LES GRANDS CLASSIQUES GAUTHIER-VILLARS

ENCYCLOPÉDIE
DES
SCIENCES MATHÉMATIQUES
PURES ET APPLIQUÉES

PUBLIÉE SOUS LES AUSPICES DES ACADÉMIES DES SCIENCES
DE GÖTTINGUE, DE LEIPZIG, DE MUNICH ET DE VIENNE
AVEC LA COLLABORATION DE NOMBREUX SAVANTS.

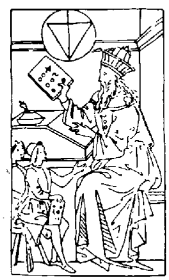
ÉDITION FRANÇAISE

RÉDIGÉE ET PUBLIÉE D'APRÈS L'ÉDITION ALLEMANDE SOUS LA DIRECTION DE

JULES MOLK,
PROFESSEUR À L'UNIVERSITÉ DE NANCY.

TOME I (DEUXIÈME VOLUME),

ALGÈBRE



ÉDITIONS
JACQUES GABAY

Abréviations.

Dans les publications de l'académie des sciences de Paris, **H.** signifie **Histoire** **M.** signifie mémoires.

I_3 = renvoi au tome premier; troisième volume.

(I 2, **19**) = renvoi au tome premier, article 2, numéro **19**.

Dans les Notes, un nombre α en exposant indique un renvoi à la note α du même article.

(2) 8 (1812), éd. 1816, p. 57 [1810] = deuxième série, tome ou volume 8, année 1812, édité en 1816, page 57, lu ou signé en 1810.

La transcription des lettres russes a lieu conformément à l'orthographe tchèque.

En particulier *č* se prononce *tch, c* se prononce *tz, š* se prononce comme *ch* dans *chat, ž* se prononce comme notre *j* dans *je, j* se prononce comme notre *y* dans *essayer.*

Abh. = Abhandlungen.
Acad. = Academie.
Accad. = Accademia.
Akad. = Akademie.
Alg. = Algèbre, Algebra.
Allg. = Allgemeine.
Amer. = American.
Ann. = Annalen, Annales, Annali.
Anw. = Anwendung.
appl. = appliqué.
arit. = aritmetica.
arith. = Arithmetik, arithmétique.
assoc. = association.
Aufs. = Aufsätze.
Avanc. = Avancement.
Ber. = Berichte.
Bibl. Congrès = bibliothèque du Congrès.
Bibl. math. = Bibliotheca mathematica.
Brit. = British.
Bull. = Bulletin.
Bull. bibl. = Bulletino bibliografico.
cah. = cahier.
Cambr. = Cambridge.
car. = carton.
cf. = comparez.
chap. = chapitre.
chim. = chimie, chimique.
circ. = circolo.
circul. = circular.
col. = colonne.
Comm. = Commentarii.
Commentat. = Commentationes.
Corresp. = Correspondance.
C. R. = Comptes rendus.
déf. = définition.
Denkschr. = Denkschriften.
Diss. = Dissertation.
Ec. = Ecole.
éd. = édité à, édité par, édition.
Edinb. = Edinburgh.
Educ. = Educational.
elem. = elementare.
élém. = élémentaire.
ex. = exemple.
extr. = extrait.
fasc. = fascicule.
fig. = figure.
fis. = fisica.
fol. = folio.
Géom. = Géométrie.
Ges. = Gesellschaft.
Gesch. = Geschichte.
Giorn. = Giornale.
Gött. = Göttingen, Göttingue.
Gymn. = Gymnasium.
Hist. = Histoire.
id. = idem, ibidem.
imp. = imprimé.
inscr. = inscription.
inst. = institution.
interméd. = intermédiaire.
intern. = international.
introd. = introduction.
Ist. = Istituto.
J. = Journal.
Jahresb. = Jahresbericht.
Lehrb. = Lehrbuch.
Leop. = Leopoldina.
Lpz., Lps. = Leipzig.
Mag. = Magazine.
Méc. = Mécanique.
med. = medicinisch.
Mém. = Mémoire.
métaph. = métaphysique.
Mitt. = Mitteilung.
Monatsh. = Monatshefte.
Monatsb. = Monatsberichte.
ms., mss. = manuscrit, manuscrits.
Nachr. = Nachrichten.
nat. = naturelle.
naturf. = naturforschende.
naturw. = naturwissenschaftlich.
norm. = normale.
nouv. = nouveau, nouvelle.
num. = numérique.
numism. = numismatique.
Op. = Opera.
Opusc. = Opuscule.
Overs. = Oversight.
p. = page.
p. ex., par ex. = par exemple.
partic. = particulier.
Petrop., Pétersb. = Saint Pétersbourg.
philol. = philologie.
philom. = philomatique.
philos. = philosophique.
phys. = physique.
pl. = planche.
polyt. = polytechnique.
pontif. = pontificia.
posth. = posthume.
Proc. = Proceeding.
progr. = programme.
prop. = proposition.
publ. = publié.
Quart. = Quarterly.
R. = reale, royal.
Recent. = Recentiores.
Rendic. = Rendiconto.
réimp. = réimprimé.
sc. = sciences.
Schr. = Schriften.
scient. = scientifique.
s. d. = sans date.
sect. = section.
Selsk. = Selskabs.
sign. = signature.
Sitzgsb. = Sitzungsberichte.
s. l. = sans lieu.
spéc. = spéciale.
suiv. = suivante.
sup. = supérieure.
suppl. = supplément.
soc. = société.
theor. = theoretische.
trad. = traduction.
Trans. = Transactions.
Unterh. = Unterhaltung.
Ver. = Vereinigung.
Verh. = Verhandlung.
Vetensk. = Vetenskabs.
Viertelj. = Vierteljahresschrift.
vol. = volume.
Vorles. = Vorlesung.
Wiss. = Wissenschaft, wissenschaftlich.
Z. = Zeitschrift.

LES GRANDS CLASSIQUES GAUTHIER-VILLARS

ENCYCLOPÉDIE
DES
SCIENCES MATHÉMATIQUES
PURES ET APPLIQUÉES

PUBLIÉE SOUS LES AUSPICES DES ACADÉMIES DES SCIENCES
DE GÖTTINGUE, DE LEIPZIG, DE MUNICH ET DE VIENNE
AVEC LA COLLABORATION DE NOMBREUX SAVANTS.

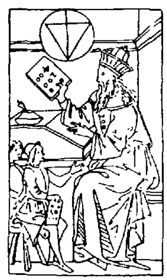
ÉDITION FRANÇAISE

RÉDIGÉE ET PUBLIÉE D'APRÈS L'ÉDITION ALLEMANDE SOUS LA DIRECTION DE

JULES MOLK,
PROFESSEUR À L'UNIVERSITÉ DE NANCY.

TOME I (DEUXIÈME VOLUME),

ALGÈBRE



ÉDITIONS
JACQUES GABAY

Avis.

Dans l'édition française, on a cherché à reproduire dans leurs traits essentiels les articles de l'édition allemande; dans le mode d'exposition adopté, on a cependant largement tenu compte des traditions et des habitudes françaises.

Cette édition française offrira un caractère tout particulier par la collaboration de mathématiciens allemands et français. L'auteur de chaque article de l'édition allemande a, en effet, indiqué les modifications qu'il jugeait convenable d'introduire dans son article et, d'autre part, la rédaction française de chaque article a donné lieu à un échange de vues auquel ont pris part tous les intéressés; les additions dues plus particulièrement aux collaborateurs français sont mises entre deux astérisques.

Réimpression autorisée de l'édition française de l'*Encyclopédie des Sciences Mathématiques Pures et Appliquées,* publiée par fascicules entre 1904 et 1916 par Gauthier-Villars et B.G. Teubner.

La publication de l'édition française a été définitivement interrompue en 1916 en raison de la guerre.

Cette réédition a été réalisée avec des volumes obligeamment prêtés par les Bibliothèques de l'École Normale Supérieure, de l'École Polytechnique et du Conservatoire National des Arts et Métiers.
De précieuses épreuves, aimablement confiées par M. Jean-Luc Verley, Maître de conférences à l'Université de Paris VII, ont permis de compléter l'article *Fonctions analytiques* écrit par W.F. Osgood, P. Boutroux et J. Chazy, et de terminer l'article *Développements concernant l'hydrodynamique* écrit par A.E.H. Love, P. Appell, H. Beghin et H. Villat.
Nous sommes particulièrement reconnaissants à la Bibliothèque de l'Institut Henri Poincaré, ainsi qu'à Mlle Karine Chemla, Chercheur au C.N.R.S., de nous avoir fourni de très utiles renseignements bibliographiques.
Nous adressons à tous nos plus sincères remerciements.

Tome I, volume 2 ISBN 2-87647-101-9
ISSN 0989-0602

ENCYCLOPÉDIE

DES

SCIENCES MATHÉMATIQUES

PURES ET APPLIQUÉES

PUBLIÉE SOUS LES AUSPICES DES ACADÉMIES DES SCIENCES
DE GÖTTINGUE, DE LEIPZIG, DE MUNICH ET DE VIENNE
AVEC LA COLLABORATION DE NOMBREUX SAVANTS.

ÉDITION FRANÇAISE

RÉDIGÉE ET PUBLIÉE D'APRÈS L'ÉDITION ALLEMANDE SOUS LA DIRECTION DE

JULES MOLK,
PROFESSEUR À L'UNIVERSITÉ DE NANCY.

TOME I (DEUXIÈME VOLUME),

ALGÈBRE

RÉDIGÉ DANS L'ÉDITION ALLEMANDE SOUS LA DIRECTION DE

FRANÇOIS MEYER,
PROFESSEUR À L'UNIVERSITÉ DE KÖNIGSBERG.

VIRIBUS UNITIS

PARIS,
GAUTHIER-VILLARS

LEIPZIG,
B. G. TEUBNER

TABLE DES MATIÈRES
des 7 premiers Tomes

Volume 2 — Fonctions de variables complexes

fasc. 1 – 23 mai 1911	II-7	Analyse algébrique **A. Pringsheim – G. Faber – J. Molk**	1-93
	II-8	Fonctions analytiques *(à suivre)* **W.F. Osgood – P. Boutroux – J. Chazy**	94-96
épreuve – 10 août 1912	II-8	*(suite)**	97-128

Volume 3 — Équations différentielles ordinaires

fasc. 1 – 22 février 1910	II-15	Existence de l'intégrale générale **P. Painlevé**	1-57
	II-16	Méthodes d'intégration élémentaires **E. Vessiot**	58-170

Volume 4 — Équations aux dérivées partielles

fasc. 1 – 30 juin 1913	II-21	Propriétés générales des systèmes d'équations aux dérivées partielles. Équations linéaires du premier ordre. **E. von Weber – G. Floquet**	1-55
	II-22	Équations non linéaires du premier ordre. Équations d'ordre plus grand que un. **E. von Weber – E. Goursat**	56-160
fasc. 2 – 17 mars 1916	II-23	Groupes de transformations continus* **H. Burkhardt – L. Maurer – E. Vessiot**	161-240

Volume 5 — Développements en séries

fasc. 1 – 31 mars 1912	II-26	Équations et opérations fonctionnelles **S. Pincherle**	1-81
	II-27	Interpolation trigonométrique **H. Burkhardt – E. Esclangon**	82-153
	II-28	Fonctions sphériques *(à suivre)* **A. Wangerin – A. Lambert**	154-160
fasc. 2 – 12 février 1914	II-28	*(suite et fin)*	161-230
	II-28a	Généralisations diverses des fonctions sphériques **P. Appell – A. Lambert**	231-268

Volume 6 — Calcul des variations. Compléments

fasc. 1 – 15 septembre 1913	II-31	Calcul des variations *(à suivre)* **A. Kneser – E. Zermelo – H. Hahn – M. Lecat**	1-128
fasc. 2 – 16 juin 1916	II-31	*(suite et fin)*	129-288

Tome III — GÉOMÉTRIE

Volume 1 — Fondements de la géométrie. Géométrie générale

fasc. 1 – 30 mars 1911	III-1	Principes de la géométrie **F. Enriques**	1-147
	III-1a	Notes sur la géométrie non-archimédienne **A. Schoenflies**	148-151
	III-2	Les notions de ligne et de surface *(à suivre)* **H. von Mangoldt – L. Zoretti**	152-160
fasc. 2 – 8 juillet 1915	III-2	*(suite et fin)*	161-184
	III-3	Exposé parallèle du développement de la géométrie synthétique et de la géométrie analytique pendant le XIXe siècle **G. Fano – S. Carrus**	185-259
	III-4	Géométrie énumérative **H.G. Zeuthen – M. Pieri**	260-331
Elie Cartan, *Œuvres complètes* Partie III, Vol. 2, G.-V., 1955	III-5	La théorie des groupes continus et la géométrie **G. Fano – E. Cartan**	1-135

Volume 2 — Géométrie descriptive. Géométrie élémentaire

fasc. 1 – 23 décembre 1913	III-8	Géométrie projective **A. Schoenflies – A. Tresse**	1-143
	III-9	Configurations* **E. Steinitz – E. Merlin**	144-160

Volume 3 — Géométrie algébrique plane

fasc. 1 – 25 juin 1911	III-17	Coniques *(à suivre)* **F. Dingeldey – E. Fabry**	1-160
fasc. 2 – 3 août 1915	III-17	*(suite et fin)*	161-162
	III-18	Systèmes de coniques **F. Dingeldey – E. Fabry**	163-256
	III-19	Théorie générale des courbes planes algébriques* **L. Berzolari**	257-304

Volume 4 — Géométrie algébrique dans l'espace

fasc. 1 – 28 avril 1914	III-22	Quadriques **O. Staude – A. Grévy**	1-164

Tome IV — MÉCANIQUE

Volume 1 — Généralités. Historique

fasc. 1 – 15 mars 1915	IV-1	Principes de la mécanique rationnelle **A. Voss – E. Cosserat – F. Cosserat**	1-187
	IV-2	Mécanique statistique **P. Ehrenfest – T. Ehrenfest – E. Borel**	188-292

** La fin de l'article n'a pas été publiée en raison de la guerre.*

I 9. LES FONCTIONS RATIONNELLES.

Exposé, d'après l'article allemand de **E. NETTO** (Giessen),
par **R. LE VAVASSEUR** (Lyon).

Préliminaires.

1. Introduction. *L'usage *exclusif* des lettres pour représenter des nombres remonte à *F. Viète*[1]); une lettre ne représentait toutefois pour lui qu'un nombre positif. Après l'introduction des nombres négatifs on a représenté par une lettre[2]) un nombre réel quelconque (positif, nul ou négatif); après l'introduction des nombres imaginaires on a représenté par une lettre un nombre complexe quelconque (réel ou imaginaire).*

*On a appelé *expression algébrique*[3]), relative à des lettres, l'indication sur ces lettres, à l'aide des signes d'addition, de soustraction, de multiplication, de division et d'extraction de racine, d'un nombre fini de calculs à effectuer[4]). On a appelé *expression rationnelle,* relative à des

1) *Pour plus de détails, et en ce qui concerne l'usage des lettres pour représenter des nombres avant *F. Viète,* voir I 1, **10**, **26** et I 3, **4**.*

2) *Chaque fois qu'on écrivait une équation ayant une racine négative et où la racine inconnue était désignée par une lettre, on avait effectivement représenté par une lettre un nombre négatif (cf. I 1 17, note 148). C'est toutefois *J. Hudde* qui a, le premier, désigné à dessein par une même lettre un nombre positif *ou* négatif [De reductione aequationum, rédigé en 1657, publié par *F. van Schooten* à la fin du tome 1 de la 2ième édition latine de la Géométrie de *R. Descartes* (Geometria a Renato Descartes 1, Amsterdam 1659, p. 439)]. Avant *J. Hudde* une lettre, par ex. p, représentait toujours une quantité positive et si dans une expression où figurait cette lettre la quantité qu'elle représentait était supposée négative on remplaçait dans l'expression envisagée p par $-p$ [cf. *R. Descartes,* Géométrie, Leyde 1637; Œuvres, éd. *Ch. Adam* et *P. Tannery* 6, Paris 1902, p. 450] (Note de *G. Eneström*).*

3) *L'emploi du mot *algébrique* dans ce sens restreint est dû à *G. W. Leibniz* [De vera proportione circuli ad quadratum circumscriptum, Acta Erud. Lps. 1682, p. 43; Werke, éd. *C. I. Gerhardt,* Math. Schr. 5, Halle 1858, p. 119] (Note de *G. Eneström*).*

4) *L'emploi de cette locution „expression algébrique“ dans ce sens restreint devrait être complètement abandonné. Les locutions „expressions rationnelles“,

lettres, toute expression algébrique relative à ces lettres ne renfermant pas de radicaux. Une expression algébrique qui n'est pas rationnelle est dite *irrationnelle*[5]). Ainsi $a+b$, $\frac{3}{2}ab$, $\frac{a^2+b^2}{a-b\sqrt{2}}$ sont des expressions rationnelles; $a+\frac{2b\sqrt[3]{a^2-b^2}}{a+b}$ est une expression algébrique irrationnelle.

On a appelé *monome*[6]) une expression algébrique dans la formation de laquelle il n'entre ni addition, ni soustraction; ainsi $4a^3b\sqrt{bc^3}$ est un monome. Un *monome entier* peut toujours s'obtenir par la multiplication de nombres et de lettres; on peut toujours l'écrire de façon qu'il soit le produit d'un nombre par des puissances entières positives de certaines lettres; ex: $\frac{2}{3}xy5xx = \frac{10}{3}x^3y$. Le nombre $\frac{10}{3}$ est ce qu'on appelle le *coefficient*[7]) du monome; le monome a^2bc a pour coefficient 1. Deux monomes entiers qui ne diffèrent que par le coefficient sont dits *semblables*; deux monomes semblables ayant même coefficient sont *identiques.**

„expressions algébriques irrationnelles“ devraient aussi être précisées. Il convient cependant de mentionner ici le sens que l'on a donné tout d'abord à ces locutions d'autant plus qu'on les rencontre encore avec cette signification imprécise dans un certain nombre de traités d'Algèbre élémentaire.*

5) *Les mots *rationnels* et *irrationnels* ont été employés pour la première fois, dans le sens que nous leur donnons actuellement (cf. I 3, **1**, **2** et **3**) en Arithmétique et en Algèbre, par *Cassiodore* (6e siècle) [voir *V. Mortet,* Revue de philologie (2) 24 (1900), p. 280] (Note de *G. Eneström*).*

6) *Le mot *monome* a été formé d'une façon assez singulière, évidemment par analogie avec le mot *binome*[12]). Il apparaît vers la fin du 17ième siècle où *J. Ozanam* en fait mention dans son Dictionnaire mathématique [éd. Amsterdam 1691, p. 63] mais il a été d'un usage peu fréquent jusqu'au début du 19ième siècle. Aux 17ième et 18ième siècles on disait ordinairement *quantité simple* [voir par ex. *E. Bartholin,* Principia matheseos universalis, publ. dans *F. van Schooten,* Geometria a Renato Descartes 2, Amsterdam 1659, p. 2] ou *grandeur incomplexe* [voir par ex. *J. Prestet,* Nouveaux élémens de math. 1, Paris 1689, p. 75] (Note de *G. Eneström*).*

7) *Le mot *coefficient* a déjà été employé par *F. Viète* [voir par ex. Ad logisticem speciosam, prop. XXIV et suiv.; Opera, éd. *F. van Schooten,* Leyde 1646, p. 23; trad. *F. Ritter,* Bull. bibl. storia mat. 1 (1868), p. 256] mais il a été peu en usage jusqu'à la fin du 17ième siècle. *R. Descartes* [Géométrie, Leyde 1637; Œuvres[2]) 6, p. 453] dit, par exemple, *la quantité connue du second* ou *du troisième terme* au lieu de dire *le coefficient du second* ou *du troisième terme*; *J. Ozanam* [Dict. math.[6]), p. 82] dit: *on apelle coëfficient du troisiéme terme la quantité connuë du troisiéme terme.* Avant *F. Viète* on désignait souvent les coefficients des termes d'une équation par les noms mêmes des puissances de l'inconnue; on rencontre ainsi le nom de *cube* (ou bien le pluriel *cubes*) et aussi de *nombre de cubes* pour désigner le coefficient de la troisième puissance de l'inconnue (Note de *G. Eneström*).*

*Le *degré*[8]) d'un monome entier est la somme des exposants des lettres qui le composent; $\frac{10}{3}x^3yz^2$ par ex. a pour degré 6. On pourra aussi parler du degré d'un monome par rapport à certaines des lettres qui y figurent; il faudra alors spécifier par rapport à quelles lettres on prend le degré; $\frac{10}{3}x^3yz^2$ est de degré 3 par rapport à x, de degré 1 par rapport à y, de degré 4 par rapport à x et y.

Un *polynome*[9]) est une somme algébrique[10]) de monomes. Les monomes, avec les signes qui y sont attachés, sont dits les *termes* du polynome. Si tous ses termes sont des monomes entiers, on dit que le polynome est *entier*. Le degré d'un polynome entier est le plus grand des degrés des monomes entiers dont le polynome est la somme algébrique.

Dans la plupart des traités d'Algèbre[11]) on a réservé les noms de *monome* et de *polynome* aux *monomes entiers* et aux *polynomes entiers*.*

---

8) *Des considérations géométriques avaient fait employer primitivement les dénominations de *quarré*, de *cube* et, par analogie, de *dimension* n au lieu des dénominations plus régulières de second degré, de troisième degré et de degré n. Voir *S. F. Lacroix*, Eléments d'Algèbre, Paris an VII; (5ième éd.) Paris an XIII (1804), p. 40; (25ième éd.) Paris 1888, p. 38. Cf. note 14.*

9) *Le mot *polynome* a été employé quelquefois par *F. Viète* dans le sens actuel [voir par ex. In artem analyticem isagoge, Tours 1591; Opera, éd. *F. van Schooten*, Leyde 1646, p. 7, 12; trad. *F. Ritter*, Bull. bibl. storia mat. 1 (1868), p. 235, 243]. Un peu avant *F. Viète*, *Simon Stevin* s'est servi du mot *multinomie* dans le même sens; mais *multinomie* a aussi signifié pendant longtemps la somme d'un certain nombre de grandeurs incommensurables entre elles [voir par ex. *A. Girard*, Invention nouvelle en l'Algèbre, Amsterdam 1629; réédité par *D. Bierens de Haan*, Leyde 1884; sign. C_1 verso, C_2 verso, F_4 recto]. Au 17ième siècle on disait ordinairement *quantité composée* ou *grandeur complexe* au lieu de *polynome* [voir par ex. *E. Bartholin*, Principia[6]), publ. dans *F. van Schooten*, Geom. Descartes[6]) 2, p. 7; *J. Prestet*, Nouveaux élémens de math. 1, Paris 1689, p. 76]. On rencontre encore à la fin du 18ième siècle plusieurs traités dans lesquels on emploie systématiquement la locution *grandeur composée* en évitant non moins systématiquement le mot *polynome* [voir par ex. *L. Euler*, Vollständige Anleitung zur Algebra 1 (sect. II, chap. 3, 4; nos 270, 273, 285, ...), St Pétersbourg 1770, p. 164, 173; trad. avec additions par *J. L. Lagrange* 1, Lyon 1774, p. 202, 204, 216, ...] et *S. F. Lacroix* dit encore à plusieurs reprises [Alg.[8]), (25ième éd.) Paris 1888, p. 31 et suiv.] *quantité complexe* au lieu de polynome (Note de *G. Eneström*).*

10) *La locution *somme algébrique* qui est d'un usage courant dans les traités de langue française a été définie dans l'article I 1, no 17.*

11) *Voir par ex. *J. Tannery*, Leçons d'Algèbre et d'Analyse 1, Paris 1906, p. 59.*

*Un *binome*[12]) est un polynome qui n'a que deux termes. Un *trinome* est un polynome qui n'a que trois termes.

On entend par *termes semblables* dans un polynome entier des termes qui ont la même partie littérale et qui ne diffèrent que par les coefficients; $+4ax^3$, $-\frac{2}{3}ax^3$ sont des termes semblables. *Réduire* des termes semblables dans un polynome entier, c'est les remplacer par un seul terme qui leur est semblable et qui a pour coefficient la somme algébrique de leurs coefficients. On appelle *polynome réduit* un polynome (entier) dans lequel la réduction des termes semblables a été effectuée et *coefficients* du polynome (entier) les coefficients des monomes qui figurent dans le polynome réduit.

Pour *faire la somme* de deux ou de plusieurs polynomes, on écrit les uns à la suite des autres tous les termes de ces polynomes, puis on fait la réduction des termes semblables. Pour *retrancher* d'un polynome un second polynome, il suffit d'ajouter au premier polynome le polynome obtenu en changeant les signes de tous les termes du second polynome.*

---

12) *Le mot *binome* avait originairement un sens plus restreint. Sa forme latine *binomium* est une traduction du terme euclidien *ἐκ δύο ὀνομάτων* qui signifie une expression de la forme $a+\sqrt{b}$ ou de la forme $\sqrt{a}+\sqrt{b}$, a et b étant rationnels. C'est dans ce sens restreint que le mot *binome* a été généralement employé depuis *Gérard de Crémone* (12ième siècle) [voir *Anaritius* (*El Nairîzî*), In decem libros priores elementorum Euclidis commentarii, éd. *M. Curtze*, Leipzig 1899, p. 331] et parfois encore jusqu'à la fin du 18ième siècle [cf. *L. Euler*, Alg.[9]) 2 (sect. I, chap. 8; no 107), p. 94; trad. 1, p. 557].

Cependant déjà *N. Tartaglia* [General trattato di numeri et misure 6, Venise 1560, fol. 4a; trad. *G. Gosselin*, Paris 1578] fait un premier pas vers une généralisation de ce sens restreint donné au mot binome. Sous le nom de *binome de dignité algébrique* il envisage en effet des binomes de la forme $a+bx^n$ et ax^m+bx^n où m et n sont des nombres naturels.

Dans le sens actuel du mot *binome*, *S. Stevin* a employé en 1585 le mot *binomie* [Œuvres math., éd. *A. Girard* 1, Leyde 1634, p. 69] et *F. Viète* a fait usage en 1591 des locutions *binomium* ou *radix binomia* [In artem analyticem isagoge[9]), Tours 1591; Ad logisticem speciosam, prop. XXV; Opera, éd. *F. van Schooten*, Leyde 1646, p. 7, 23]; *R. Descartes* a fait usage du mot même de *binome* dans le sens actuel [Géométrie, Leyde 1637, livre 3; Œuvres[2]) 6, p. 445, 454 et suiv.]. Vers la fin du 17ième siècle, *J. Ozanam* [Dict. math.[6]), p. 64] définit un binome comme une grandeur composée de deux monomes.

Ni *I. Newton*, ni *L. Euler* ne semblent avoir fait usage du mot binome dans son sens actuel. Exceptionnellement *I. Newton* a désigné par ce mot des binomes irrationnels plus compliqués comme $x^{\sqrt{2}}+x^{\sqrt{7}}$ [lettre à *H. Oldenbourg* datée du 24 octobre 1676 (epistola posterior); Opuscula, éd. *J. Castillon* 1, Lausanne et Genève 1744, Opusc. XI, p. 357; Comm. epist. *J. Collins* et aliorum, Londres 1712, éd. *J. B. Biot* et *F. Lefort*, Paris 1856, p. 145; Opera, éd. *S. Horsley* 4, Londres 1782, p. 558]. Au contraire *G. W. Leibniz* et *Jean Bernoulli* ont adopté le mot *binome* dans son sens actuel (Note de *G. Eneström*).*

*Le *produit de deux monomes entiers* est un monome entier qui a pour coefficient le produit des coefficients des deux monomes et pour partie littérale le produit des puissances des lettres qui figurent dans ces monomes, en sorte que chaque lettre est affectée d'un exposant égal à la somme des exposants qu'elle a dans les deux monomes. Bien entendu, si une lettre ne figure pas dans l'un des deux monomes, il faut la considérer comme y figurant avec l'exposant zéro. Le degré du produit de deux monomes entiers est la somme des degrés de ces deux monomes. Ainsi $(\frac{3}{2}ab^2cx) \times (\frac{1}{5}a^2y) = \frac{3}{10}a^3b^2cxy$.

On obtient le *produit de deux polynomes* en faisant la somme algébrique de tous les produits obtenus en multipliant chaque terme de l'un des polynomes par chaque terme de l'autre polynome.*

2. Fonctions rationnelles. Les lettres qui représentent des nombres complexes (réels ou imaginaires) *fixes* s'appellent des *constantes*; celles qui représentent des nombres complexes (réels ou imaginaires) susceptibles de varier s'appellent des *variables*.

Lorsqu'à chacune des valeurs que peut prendre une variable x correspond un nombre que l'on regarde comme une valeur attribuée à une variable y, on dit que la variable y est *fonction*[13]) de la variable x.

Pour désigner une fonction d'une variable x, on peut employer un symbole abrégé tel que $f(x)$ qui se lit *fonction de x* ou plus simplement *f de x*. Lorsqu'on envisagera plusieurs fonctions de x, on les appellera par ex. $f(x)$, $g(x)$, $\varphi(x)$, ... ou bien avec des indices $f_1(x)$, $f_2(x)$, $f_3(x)$, ...

On appelle *fonction rationnelle entière* d'une variable z une expression pouvant se mettre sous la forme

$$f(z) = a_0 z^n + a_1 z^{n-1} + a_2 z^{n-2} + \cdots + a_{n-1} z + a_n,$$

où n est un nombre entier, positif ou nul et où $a_0, a_1, a_2, \ldots, a_{n-1}, a_n$ sont des constantes complexes (c'est-à-dire réelles ou imaginaires). Le nombre n est le *degré*[14]) de $f(z)$; les nombres $a_0, a_1, a_2, \ldots, a_{n-1}, a_n$ sont les *coefficients* de $f(z)$.

---

13) D'après cette définition $x = \sqrt{4y^2}$ détermine *deux* fonctions de y à savoir $x = 2y$ et $x = -2y$. Pour l'origine de la notion de fonction, voir l'article II 1.

14) *Le mot *gradus* a été employé par *F. Viète* dans le sens actuel de *degré* [voir par ex. Ad logisticem speciosam prop. XXIV; Ad problema ... Adrianus Romanus responsum, chap. IV; Opera, éd. *F. van Schooten*, Leyde 1646, p. 23, 308, 309]. *R. Descartes* a donné au mot degré un sens un peu plus général [Géométrie Leyde 1637; Œuvres[2]) 6, p. 381, 392, 464] tandis qu'il appelait *dimension* [voir p. ex. Géométrie, Leyde 1637, livre 3; Œuvres[2]) 6, p. 454, 457, 464]

*Telle qu'elle est écrite ci-dessus, la fonction $f(z)$ est dite *ordonnée suivant les puissances décroissantes de z*. Elle est *complète* si elle contient effectivement des termes de tous les degrés, depuis 0 jusqu'à n avec des coefficients différents de zéro; le nombre de ces termes est alors $n+1$.*

Plus généralement, imaginons $m+1$ variables $z_0, z_1, z_2, \ldots, z_m$. Formons l'expression

$$\sum a_{\alpha_0\alpha_1\alpha_2\ldots\alpha_m} z_0^{\alpha_0} z_1^{\alpha_1} z_2^{\alpha_2} \ldots z_m^{\alpha_m},$$

dans laquelle

$$a_{\alpha_0\alpha_1\alpha_2\ldots\alpha_m}$$

désigne une constante complexe (réelle ou imaginaire), tandis que $\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_m$ sont des entiers positifs ou nuls; la somme Σ s'étend à tous les termes que l'on peut trouver en prenant pour $\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_m$ les solutions en nombres entiers, positifs ou nuls, de l'équation

$$\alpha_0 + \alpha_1 + \alpha_2 + \cdots + \alpha_m = n$$

dans laquelle n est un nombre naturel déterminé (ou à une partie de ces solutions ce qui revient à prendre quelques-uns des coefficients a égaux à zéro).

Une telle expression s'appelle[15]) fonction *rationnelle, entière et homogène de degré n*[16]) des variables $z_0, z_1, z_2, \ldots, z_m$ et nous la représenterons par un symbole tel que $f(z_0, z_1, z_2, \ldots, z_m)$. L'épithète *homogène* signifie que tous les termes de la fonction ont le même degré.

*Si l'on désigne par t une variable auxiliaire ne figurant pas dans l'expression $f(z_0, z_1, z_2, \cdots, z_m)$ on a évidemment

$$f(tz_0, tz_1, tz_2, \cdots, tz_m) = t^n f(z_0, z_1, z_2, \cdots, z_m).$$

Plus généralement nous conviendrons de dire d'une fonction quelconque F de fonctions rationnelles entières $f_0, f_1, f_2, \cdots, f_k$ qu'elle est homogène de degré r en $f_0, f_1, f_2, \cdots, f_k$ lorsque t désignant une variable auxiliaire ne figurant pas dans l'expression $F(f_0, f_1, f_2, \cdots, f_k)$, on a

$$F(tf_0, tf_1, tf_2, \cdots, tf_k) = t^r F(f_0, f_1, f_2, \cdots, f_k).$$

---

ce que nous appelons ici degré. Depuis la seconde moitié du 17e siècle la plupart des mathématiciens ont fait usage de la locution *degré n* de x dans une *équation* de dimension n (en x) [voir par ex. *J. Prestet*, Elémens de math., Paris 1675, p. 371, 382; *J. Ozanam*, Dict. math.[6]), p. 81] (Note de *G. Eneström*).*

15) *L. Euler*, Introd. in analysin infin. 1, Lausanne 1748, p. 61; trad. *J. B. Labey*, Introd. à l'analyse infinitésimale 1, Paris an IV, p. 60.

16) *On disait autrefois [14]) *dimension n* au lieu de degré n relatif à l'ensemble des variables $z_0, z_1, z_2, \cdots, z_m$. Mais depuis *S. F. Lacroix* [Alg.[8]), n° 27 en note] l'usage actuel a prévalu, en France du moins.*

Par exemple, la fonction

$$\sqrt{\frac{f_0+f_1}{f_2^{\,2}+f_3 f_4}}$$

est homogène de degré $-\frac{1}{2}$ en f_0, f_1, f_2, f_3, f_4.

Si $f_0, f_1, \ldots, f_k$ sont des fonctions homogènes de degré s de $z_0, z_1, \ldots, z_n$; si

$$F(f_0, f_1, \cdots, f_k)$$

est une fonction homogène de degré r de $f_0, f_1, \ldots, f_k$, et si l'on désigne par $\Phi(z_0, z_1, \ldots, z_n)$ la fonction dans laquelle se transforme F quand on y remplace $f_0, f_1, \ldots, f_k$ en fonction de $z_0, z_1, \ldots, z_n$, on a

$$\Phi(tz_0, tz_1, \ldots, tz_n) = t^{rs}\Phi(z_0, z_1, \ldots, z_n),$$

en sorte que Φ est homogène de degré rs en $z_0, z_1, \ldots, z_n$. Toute fonction homogène $F(f_0, f_1, \ldots, f_k)$ de degré r vérifie la *relation* dite *d'homogénéité*

$$rF = f_0\frac{\partial F}{\partial f_0} + f_1\frac{\partial F}{\partial f_1} + \cdots + f_k\frac{\partial F}{\partial f_k};$$

et réciproquement si une fonction F vérifie cette relation elle est homogène de degré r en $f_0, f_1, \ldots, f_k$.*

En particulier toute fonction rationnelle entière homogène $f(z_0, z_1, \ldots, z_m)$, de degré n, vérifie la *relation d'homogénéité*[17])

$$nf(z_0, z_1, \ldots, z_m) = z_0\frac{\partial f}{\partial z_0} + z_1\frac{\partial f}{\partial z_1} + \cdots + z_m\frac{\partial f}{\partial z_m};$$

et réciproquement si une fonction rationnelle entière $f(z_0, z_1, \ldots, z_m)$ vérifie cette relation elle est homogène de degré n en $z_0, z_2, \ldots, z_m$.

La fonction rationnelle entière homogène $f(z_0, z_1, z_2, \ldots, z_m)$ sera *complète* si aucun terme n'a un coefficient nul; le nombre des termes d'une fonction rationnelle entière homogène complète $f(z_0, z_1, \ldots, z_m)$ de degré n est[18])

17) *L. Euler* a énoncé la relation d'homogénéité dès 1729 pour une fonction (non entière) de deux variables de degré *nul* [lettre à *Jean Bernoulli* datée du 18 février 1729, publ. par *G. Eneström*, Bibl. math. (3) 4 (1903), p. 357; cf. Comm. Acad. Petrop. 3 (1728), éd. 1732, p. 120]. En 1736 *L. Euler* a énoncé la relation d'homogénéité pour une fonction de deux variables de degré *quelconque* [Mechanica 1, St Pétersb. 1736, p. 49; 2, p. 464; cf. Comm. Acad. Petrop. 7 (1734/5), éd. 1740, p. 185]. En 1755 il a énoncé et démontré la relation d'homogénéité dans le cas général d'un nombre quelconque de variables [Institutiones calculi differ., St Pétersb. 1755, n° 224, p. 189/90]. *A. Fontaine* et *A. C. Clairaut* ont trouvé indépendamment de *L. Euler* la relation dont il s'agit [voir par ex. *M. Cantor*, Vorles. Gesch. Math. (2e éd.) 3, Leipzig 1901, p. 759, 889] (Note de *G. Eneström*).*

18) *E. Bézout,* Théorie des équations algébriques, Paris 1779, p. 23.

$$\frac{(m+1)(m+2)\cdots(m+n)}{1\,.\,2\ldots n} = \frac{(m+n)!}{m!\,n!}.$$

Si, dans l'expression d'une fonction rationnelle entière et homogène de degré n des variables $z_0, z_1, z_2, \ldots, z_m$, on fait $z_0 = 1$, on obtient une fonction rationnelle, entière mais non homogène des m variables $z_1, z_2, \ldots, z_m$ de degré n, que nous représenterons aussi par un symbole tel que

$$f(z_1, z_2, \ldots, z_m).$$

Une fonction rationnelle entière *complète* non homogène de m variables, de degré n, a $\frac{(m+n)!}{m!\,n!}$ termes.

On appelle fonction rationnelle entière *identiquement nulle* une fonction rationnelle entière d'une ou de plusieurs variables telle que les coefficients de tous ses termes soient nuls. On démontre qu'une fonction rationnelle entière en z de degré n qui s'annule pour $n+1$ valeurs distinctes de z est identiquement nulle. Une fonction rationnelle entière d'un nombre quelconque de variables qui s'annule pour toutes les valeurs que l'on donne à ces variables est identiquement nulle. Deux fonctions rationnelles entières sont *identiques* lorsque leur différence est identiquement nulle[19]). Ecrire que deux fonctions rationnelles entières sont identiques c'est écrire une identité.

*On dit d'une fonction rationnelle entière f de $z_1, z_2, \ldots, z_m$ de degré n qu'elle est *régulière* relativement à l'une des variables z_i, lorsque son degré *par rapport à* z_i est égal à n, en sorte que si l'on ordonne f par rapport à z_i le coefficient de z_i^n est différent de zéro.

Une fonction rationnelle entière f de $z_1, z_2, \ldots, z_m$ est dite[20]) *régulière* (sans épithète) lorsqu'elle est régulière relativement à chacune des variables $z_1, z_2, \ldots, z_m$.*

La somme, la différence, le produit de deux fonctions rationnelles entières d'une ou de plusieurs variables sont encore des fonctions rationnelles entières des mêmes variables.

Ainsi dans le cas de fonctions d'une variable, si

$$f(z) = a_0 z^n + a_1 z^{n-1} + \cdots + a_n$$

19) *H. Dellac* [J. math. spéc. (4) 4 (1895), p. 169] cherche le nombre des conditions nécessaires et suffisantes pour qu'un polynome entier à 2 variables soit identiquement nul.*

20) *Gyula König,* Az algebrai mennyiségek általános elméletének alapvonalai, Budapest 1903, p. 70/1; éd. allemande: *J. König,* Einleitung in die allgemeine Theorie der algebraischen Grössen, Leipzig 1903, p. 67. Si la locution „*fonction régulière*“ est empruntée à *Gy.* (*J.*) *König*, la *notion* de fonction régulière est antérieure. *L. Kronecker* s'en sert couramment; cf. *J. Molk,* Thèse, Paris 1884; Acta math. 6 (1885), p. 81.*

et si

$$\varphi(z) = b_0 z^{\nu} + b_1 z^{\nu-1} + \cdots + b_{\nu},$$

le produit $f(z)\,\varphi(z)$ sera une fonction rationnelle entière de z de degré $n+\nu$

$$f(z)\,\varphi(z) = c_0 z^{n+\nu} + c_1 z^{n+\nu-1} + \cdots + c_{n+\nu}$$

dont les coefficients $c_0, c_1, \ldots, c_{n+\nu}$ sont donnés, pour $h = 0, 1, \cdots, n+\nu$, par la formule

$$c_h = a_0 b_h + a_1 b_{h-1} + \cdots + a_h b_0,$$

à condition d'y supposer nuls a_α pour $\alpha > n$, et b_β pour $\beta > \nu$.

*Si dans une fonction rationnelle entière $f(z_1, z_2, \cdots, z_m)$ on remplace les m variables $z_1, z_2, \cdots, z_m$ par des expressions linéaires et homogènes

$$(1) \qquad z_i = a_{i1} y_1 + a_{i2} y_2 + \cdots + a_{im} y_m \qquad (i = 1, 2, \ldots, m)$$

de m variables $y_1, y_2, \cdots, y_m$ à coefficients constants $a_{ik} (i, k = 1, 2, \cdots, m)$ on dit que l'on effectue sur la fonction $f(z_1, z_2, \cdots, z_m)$ une *substitution linéaire et homogène.* Le déterminant (I 2, **17**)

$$\begin{vmatrix} a_{11}, & a_{12}, & \cdots, & a_{1m} \\ a_{21}, & a_{22}, & \cdots, & a_{2m} \\ \cdot & \cdot & \cdot & \cdot \\ a_{m1}, & a_{m2}, & \cdots, & a_{mm} \end{vmatrix}$$

s'appelle le déterminant de la substitution. Si la valeur de ce déterminant est différente de zéro on peut aussi représenter les variables $y_1, y_2, \cdots, y_m$ au moyen des variables $z_1, z_2, \cdots, z_m$ par des expressions linéaires et homogènes

$$(2) \qquad y_i = b_{i1} z_1 + b_{i2} z_2 + \cdots + b_{im} z_m \qquad (i = 1, 2, \ldots, m)$$

à coefficients constants b_{ik} $(i, k = 1, 2, \cdots, m)$. On dit alors que la substitution linéaire et homogène (1) est *réversible* et que les systèmes d'équations (1) et (2) représentent des substitutions linéaires et homogènes *inverses.* Le produit des déterminants de deux substitutions linéaires et homogènes inverses est égal à 1.

Si n est le degré d'une fonction rationnelle entière de $z_1, z_2, \cdots, z_m$ cette fonction se transforme par une substitution linéaire et homogène réversible (1) en une fonction rationnelle entière de $y_1, y_2, \cdots, y_m$ de *même* degré n.

Soient $f_1, f_2, \ldots, f_k$ un nombre quelconque de fonctions rationnelles entières de $z_1, z_2, \ldots, z_m$. On peut toujours[20]) obtenir autant qu'on veut de substitutions linéaires et homogènes à coefficients entiers et à déterminant égal à 1 telles que chacune de ces fonctions $f_1, f_2, \ldots, f_k$ se transforme par ces substitutions en une fonction régulière (sans épithète).*

*Ainsi les fonctions

$$f_1(z_1, z_2, z_3) = z_1 z_2, \quad f_2(z_1, z_2, z_3) = z_1 z_3$$

se transforment par la substitution

$$z_1 = y_1 + y_2 + y_3, \quad z_2 = y_1 + 2y_2 + y_3, \quad z_3 = y_1 + y_2 + 2y_3$$

en

$$y_1^2 + 2y_2^2 + y_3^2 + 3y_1y_2 + 2y_1y_3 + 3y_2y_3$$
$$y_1^2 + y_2^2 + 2y_3^2 + 2y_1y_2 + 3y_1y_3 + 3y_2y_3.$$

Les monomes *entiers* et les polynomes *entiers* peuvent être envisagés comme des fonctions rationnelles entières d'une ou de plusieurs lettres. La plupart des auteurs ont réservé le nom de *polynome en* $z_1, z_2, \ldots, z_m$ aux polynomes (et monomes) *entiers* en $z_1, z_2, \ldots, z_m$ en sorte qu'un polynome (sans épithète) est pour eux une fonction rationnelle entière.*

3. Division. *Comme en Arithmétique (I 1, **19**), le mot division a ici deux sens bien distincts.

Voici le premier sens: *Diviser un monome ou un polynome par un monome ou un polynome*, c'est écrire une fraction dont le numérateur est le premier monome ou polynome et le dénominateur le second monome ou polynome. Pour *diviser un polynome par un monome*, il suffit de diviser par le monome chaque terme du polynome.*

Le quotient de deux fonctions rationnelles entières f et φ est la fraction $\frac{f}{\varphi}$. S'il existe une fonction rationnelle entière g telle que l'on ait $f = \varphi g$, le quotient $\frac{f}{\varphi}$ est égal à la fonction rationnelle *entière* g; dans tout autre cas ce quotient $\frac{f}{\varphi}$ prend le nom de fonction rationnelle *fractionnaire.*

Voici maintenant le second sens: Soient $f(z)$ et $\varphi(z)$ deux fonctions rationnelles entières en z; *diviser* $f(z)$ par $\varphi(z)$, c'est chercher une fonction rationnelle $g(z)$, entière en z, telle que l'expression

$$f(z) - \varphi(z)\,g(z)$$

soit une fonction $r(z)$ rationnelle entière en z, de degré inférieur au degré de $\varphi(z)$. La fonction $f(z)$ s'appelle le *dividende*, la fonction $\varphi(z)$ s'appelle le *diviseur*; $g(z)$ est le *quotient*, $r(z)$ est le *reste* de la division.

*Si le dividende $f(z)$ est de degré inférieur au degré du diviseur $\varphi(z)$, le quotient $g(z)$ est identiquement nul, et le reste $r(z)$ est identique au dividende $f(z)$.

Si le degré n de $f(z)$ est supérieur ou égal au degré p de $\varphi(z)$, $g(z)$ sera de degré $n - p$.

L'identité

$$f(z) = \varphi(z)\,g(z) + r(z)$$

permet de déterminer univoquement les coefficients de $g(z)$ et ceux de $r(z)$; il suffit pour cela d'égaler dans les deux membres de l'identité les coefficients des mêmes puissances de z.*

Si le reste $r(z)$ est identiquement nul, en sorte que

$$f(z) = \varphi(z)\,g(z),$$

on dit que $f(z)$ est (*exactement*) *divisible* par $\varphi(z)$; $\varphi(z)$ est appelé *diviseur* de $f(z)$ et $f(z)$ *multiple* de $\varphi(z)$; $f(z)$ est alors aussi (exactement) divisible par $g(z)$; $f(z)$ est un multiple de $g(z)$ et $g(z)$ un diviseur de $f(z)$.

La condition nécessaire et suffisante pour qu'une fonction rationnelle entière $f(z)$ soit divisible par $z - a$ est que $f(a)$ soit nul; par ex. $z^m - a^m$ est toujours divisible par $z - a$ quel que soit le nombre naturel m.

Plus généralement, si a est un nombre quelconque donné tel que $\varphi(a)$ ne soit pas nul, on peut se proposer de trouver une fonction rationnelle entière $g(z)$ telle que l'expression $f(z) - \varphi(z)\,g(z)$ contienne $(z-a)^{q+1}$ en facteur, q étant un nombre entier donné positif ou nul et le degré de la fonction cherchée $g(z)$ étant au plus égal à q[21]. Si a est nul, on dit qu'on fait la division de $f(z)$ par $\varphi(z)$ suivant les puissances croissantes de la variable z. Le problème n'a qu'une solution.

Si une fonction rationnelle entière f d'un nombre quelconque de variables peut être mise sous la forme d'un produit de deux fonctions rationnelles entières φ, g de ces mêmes variables (qui peuvent d'ailleurs ne pas figurer *toutes* dans chacune des deux fonctions φ, g), on dit encore que f est *divisible* par φ et par g, ou est un *multiple* de φ et de g, et aussi que φ et g sont des *diviseurs* de f.

Si une fonction rationnelle entière $f(z_1, z_2, \ldots, z_n)$ est divisible par une fonction rationnelle entière $\varphi(z_2, \ldots, z_n)$, chacun des coefficients de la fonction f ordonnée suivant les puissances de z_1 est divisible par φ.

Une fonction rationnelle entière $f(z_1, z_2, \ldots, z_n)$ qui n'est divisible par aucune fonction rationnelle entière ne dépendant que des variables $z_2, \ldots, z_n$ (ou de quelques-unes d'entre elles) est dite *primitive* par rapport à z_1. Le produit de deux fonctions primitives par rapport à z_1 est aussi une fonction primitive par rapport à z_1.

21) *Voir *H. Andoyer*, J. math. pures appl. (5) 1 (1895), p. 61/90; voir encore *C. Reuschle*, Z. Math. Phys. 41 (1896), p. 93; *W. Kretkowski*, Muzeum czasopismo Towarzystwa Nanczycieli Szkól wyższych, Lwów (Lemberg) 1887, p. 113/5; *A. V. Jamet*, Ann. Fac. sc. Marseille 8 (1898), p. 151; *F. Giudice*, Periodico mat. (2) 4 (1901/2), p. 88.*

On appelle fonctions rationnelles entières *décomposables* ou *réductibles* d'une ou de plusieurs variables celles qui peuvent se mettre sous la forme d'un produit de deux ou de plusieurs fonctions rationnelles entières des mêmes variables de degré au moins égal à 1. Les fonctions *indécomposables* ou *absolument irréductibles*[22]) sont celles pour lesquelles cette décomposition est impossible. Il y a des fonctions rationnelles entières indécomposables de *deux* et de plus de deux variables qui sont de degré > 1 par rapport à chacune de ces variables; ainsi $x^2 - y^3$ est indécomposable. Mais il n'y a pas de fonction rationnelle entière indécomposable d'une seule variable dont le degré soit > 1 (n^os **80/90**).

4. Algorithme du plus grand commun diviseur. *Deux fonctions $f_0(z)$ et $f_1(z)$ *rationnelles entières* de z, peuvent avoir un *diviseur commun*. On peut voir si elles en ont un, ou non, et, quand elles en ont un, le déterminer par des divisions successives; on forme ainsi un algorithme auquel on a donné le nom d'*algorithme d'Euclide* (cf. I 15, **1**). Voici en quoi consiste l'*algorithme d'Euclide*:

Déterminons successivement des fonctions rationnelles entières

$$g_1(z),\ f_2(z);\quad g_2(z),\ f_3(z);\quad g_3(z),\ f_4(z);\quad \ldots$$

telles que pour les valeurs successives $\lambda = 1, 2, \ldots$ de l'indice λ on ait identiquement

$$f_{\lambda-1}(z) + f_{\lambda+1}(z) = f_\lambda(z)\,g_\lambda(z)$$

et que le degré de $f_{\lambda+1}(z)$ soit inférieur au degré de $f_\lambda(z)$. Dans ces identités $f_{\lambda+1}$ est le reste, changé de signe, de la division de $f_{\lambda-1}$ par f_λ.

Les degrés des fonctions rationnelles entières $f_1(z), f_2(z), f_3(z), \ldots$ allant en diminuant, on parvient nécessairement à une fonction identiquement nulle; soit $f_{r+1}(z)$ cette fonction. Alors de deux choses l'une: ou bien dans la suite $f_1(z)$, $f_2(z)$, $f_3(z)$, ... le terme f_r qui précède immédiatement $f_{r+1}(z)$ est une fonction rationnelle entière de z de degré $\geqq 1$; cette fonction divise alors $f_{r-1}(z)$ en vertu de la dernière égalité de l'algorithme d'Euclide

$$f_{r-1}(z) = f_r(z)\,g_r(z);$$

$f_r(z)$ divise donc aussi $f_{r-2}(z)$ en vertu de l'avant-dernière égalité de

22) *Gy. (J.) König*, Alg. Grössen [20]), p. 170.*

cet algorithme, donc aussi $f_{r-3}(z), \ldots$, donc enfin $f_1(z)$ et $f_0(z)$; ainsi $f_r(z)$ est un diviseur commun de $f_0(z)$ et de $f_1(z)$. Tout diviseur commun de $f_0(z)$ et de $f_1(z)$ divise d'ailleurs $f_2(z)$ en vertu de la première égalité de l'algorithme d'Euclide, donc aussi $f_3(z)$ en vertu de la seconde égalité de cet algorithme, ..., donc enfin $f_r(z)$ en vertu de la dernière égalité de cet algorithme. C'est pourquoi on dit que $f_r(z)$ est le *plus grand commun diviseur* (p. g. c. d.) de $f_0(z)$ et de $f_1(z)$. Il est d'ailleurs commode d'appeler aussi p. g. c. d. de $f_0(z)$ et de $f_1(z)$ le produit de $f_r(z)$ par une constante quelconque différente de zéro.

Ou bien le terme f_r qui, dans la suite $f_0, f_1, f_2, \ldots$, précède immédiatement le terme nul, est une constante. Les fonctions $f_0(z)$, $f_1(z)$ n'ont alors *aucun diviseur commun* dépendant de z, car si elles en avaient un, il diviserait f_r. C'est pourquoi on dit que *les fonctions* $f_0(z)$ et $f_1(z)$ sont *premières entre elles.*

L'algorithme d'Euclide met en évidence le fait que pour $\lambda = 2, 3, \ldots, r$, chaque fonction $f_\lambda(z)$ est une fonction linéaire et homogène de $f_{\lambda-1}(z)$ et $f_{\lambda-2}(z)$ dont les coefficients sont des fonctions rationnelles entières de z en sorte que $f_\lambda(z)$ peut s'exprimer de proche en proche en fonction linéaire et homogène de $f_0(z)$ et de $f_1(z)$.

Que f_r soit le p. g. c. d. de $f_0(z)$ et de $f_1(z)$ ou que f_r soit une constante, f_r s'exprime donc de la même manière en fonction linéaire et homogène de $f_0(z)$ et de $f_1(z)$. Pour cette raison il est parfois commode de dire que quand les deux fonctions $f_0(z)$ et $f_1(z)$ sont premières entre elles, elles admettent un p. g. c. d. $f_r(z)$ de degré 0.*

Comme on vient de le voir, on peut poser[23]) pour $\lambda = 1, 2, \ldots, r$

$$f_{\lambda+1}(z) = f_1(z)\psi_\lambda(z) - f_0(z)\varphi_\lambda(z),$$

où les $\varphi_\lambda(z)$ et $\psi_\lambda(z)$ sont des fonctions rationnelles entières de z. Ces fonctions $\varphi_\lambda(z)$, $\psi_\lambda(z)$ se calculeront par récurrence au moyen des formules

$$\begin{aligned} \varphi_{\lambda+1}(z) &= \varphi_\lambda(z)g_{\lambda+1}(z) - \varphi_{\lambda-1}(z), \\ \psi_{\lambda+1}(z) &= \psi_\lambda(z)g_{\lambda+1}(z) - \psi_{\lambda-1}(z), \end{aligned} \quad (\lambda = 1, 2, \ldots, r-1)$$

avec les conditions initiales

$$\varphi_0(z) = 0, \quad \varphi_1(z) = 1, \quad \psi_0(z) = 1, \quad \psi_1(z) = g_1(z).$$

D'ailleurs on a

$$\psi_\lambda(z)\varphi_{\lambda+1}(z) - \varphi_\lambda(z)\psi_{\lambda+1}(z) = 1.$$

Le quotient $\frac{f_1(z)}{f_0(z)}$ peut s'exprimer comme il suit pour $\lambda = 1, 2, \ldots, r$:

23) Voir *E. Netto,* Vorlesungen über Algebra 1, Leipzig 1896, p. 64.

$$\begin{aligned} \frac{f_1(z)}{f_0(z)} &= \frac{\varphi_\lambda(z)}{\psi_\lambda(z)} + \frac{f_{\lambda+1}(z)}{f_0(z)\psi_\lambda(z)} \\ &= \frac{1}{\psi_0(z)\psi_1(z)} + \frac{1}{\psi_1(z)\psi_2(z)} + \cdots + \frac{1}{\psi_{\lambda-1}(z)\psi_\lambda(z)} + \frac{f_{\lambda+1}(z)}{f_0(z)\psi_\lambda(z)}; \end{aligned}$$

on a donc, en particulier,

$$\frac{f_1(z)}{f_0(z)} = \frac{1}{\psi_0(z)\psi_1(z)} + \frac{1}{\psi_1(z)\psi_2(z)} + \cdots + \frac{1}{\psi_{r-1}(z)\psi_r(z)}.$$

Si n est le degré de la fonction $f_0(z)$, et si l'on désigne par $n - n_\lambda$ le degré de la fonction $f_\lambda(z)$, les nombres naturels $n, n_1, n_2, \ldots, n_r$ vérifient les inégalités

$$0 \leqq n_1 < n_2 < \cdots < n_r \leqq n;$$

le degré de la fonction $g_1(z)$ est n_1; pour $\lambda = 2, 3, \ldots, r$ le degré de la fonction $g_\lambda(z)$ est $n_\lambda - n_{\lambda-1}$; pour $\lambda = 1, 2, 3, \ldots, r$ le degré de la fonction $\psi_\lambda(z)$ est n_λ, celui de la fonction $\varphi_\lambda(z)$ est $n_\lambda - n_1$.

Ajoutons que le développement de $\frac{f_1(z)}{f_0(z)} - \frac{\varphi_\lambda(z)}{\psi_\lambda(z)}$ suivant les puissances décroissantes de z commence par un terme en $\frac{1}{z^{n_\lambda + n_{\lambda-1}}}$, que le degré du produit $f_\lambda(z)\psi_\lambda(z)$ est égal à celui du produit de $f_{\lambda-1}(z)\psi_{\lambda-1}(z)$, et que ces deux fonctions rationnelles entières $f_\lambda(z)\psi_\lambda(z)$, $f_{\lambda-1}(z)\psi_{\lambda-1}(z)$ ont pour le terme du plus haut degré le même coefficient, savoir celui de z^n dans $f_0(z)$.

De même, les fonctions rationnelles entières $f_1(z)\varphi_1(z), \ldots$, $f_\lambda(z)\varphi_\lambda(z), \ldots$ sont de même degré, $n - n_1$, et les termes du plus haut degré en z dans chacune d'elles ont le même coefficient, celui de z^{n-n_1} dans $f_1(z)$.

*Tout ce que l'on vient de dire concernant le p. g. c. d. de deux fonctions rationnelles entières et *l'algorithme d'Euclide* s'applique aussi au cas où les coefficients des deux fonctions dépendent d'une façon quelconque de lettres $\alpha, \beta, \ldots$ que l'on envisage comme si elles étaient constantes et auxquelles on donne le nom de *paramètres.* Le p. g. c. d. des deux fonctions rationnelles entières n'est alors toutefois déterminé qu'à un facteur près qui dépend d'une façon quelconque des paramètres envisagés. Si l'on applique par exemple *l'algorithme d'Euclide* aux deux fonctions

$$\begin{aligned} f_0(z) &= \alpha z^3 + \beta z^2 + \alpha z + \beta \\ f_1(z) &= \alpha^2 z^2 + 2\alpha\beta z + \beta^2 \end{aligned}$$

on obtient

$$\begin{aligned} f_2(z) &= -\frac{\alpha^2 + \beta^2}{\alpha^2}(\alpha z + \beta) \\ f_3(z) &= 0 \end{aligned}$$

et l'on peut prendre pour p. g. c. d. de $f_0(z)$ et $f_1(z)$ aussi bien la fonction $\alpha z + \beta$ que la fonction $f_2(z)$ elle-même.*

5. Recherche et propriétés du plus grand commun diviseur et du plus petit commun multiple. On peut rechercher le p. g. c. d. de deux fonctions rationnelles entières $f_0(z)$ et $f_1(z)$ soit en s'appuyant sur l'algorithme d'Euclide soit en décomposant préalablement chacune des deux fonctions en ses facteurs indécomposables. Dans ce dernier cas on s'appuie sur le théorème fondamental d'après lequel toute fonction rationnelle entière d'un nombre quelconque de variables qui n'est pas absolument irréductible peut être décomposée, *et cela d'une seule façon,* en un produit de facteurs irréductibles.

La théorie des fonctions rationnelles entières irréductibles est d'ailleurs analogue à celle des nombres premiers[24]). En particulier si l'on sait décomposer deux fonctions rationnelles entières en produits de facteurs irréductibles on pourra trouver leur p. g. c. d. par la même règle que pour des nombres naturels décomposés en leurs facteurs premiers.

*Lorsqu'une fonction rationnelle entière des variables $z_1, z_2, \ldots, z_n, z$, primitive par rapport à z, est décomposable en un produit de deux facteurs entiers par rapport à z et rationnels par rapport à $z_1, z_2, \ldots, z_n$, elle est aussi décomposable en un produit de deux fonctions rationnelles entières par rapport aux $n+1$ variables $z_1, z_2, \ldots, z_n, z$[25]). D'après cela, deux fonctions rationnelles entières de $z_1, \ldots, z_n, z$ qui n'ont aucun diviseur commun lorsqu'on les considère comme fonctions de ces $n+1$ variables, n'admettent, non plus, aucun diviseur commun quand on les considère comme des fonctions de la seule variable z dont les coefficients dépendent des paramètres $z_1, z_2, \ldots, z_n$.

On peut reconnaître pratiquement si une fonction rationnelle entière de plusieurs variables est réductible ou irréductible à condition de savoir décomposer en facteurs linéaires une fonction rationnelle entière d'une seule variable[26]).*

24) *H. Weber,* Lehrbuch der Algebra (2e éd.) 1, Brunswick 1898, p. 72; trad. *J. Griess* 1, Paris 1898, p. 75.

25) Cf. *J. Molk,* Thèse, Paris 1884; Acta math. 6 (1885), p. 14; *F. Mertens,* Sitzgsb. Akad. Wien 101 IIa (1892), p. 1560; voir d'ailleurs déjà *C. F. Gauss,* [Disquisitiones Arithmeticae, Leipzig 1801, n° 42; trad. *A. Ch. M. Poullet-Delisle*, Recherches arithmétiques, Paris 1807; Werke 1, Göttingue 1870, p. 34] pour le théorème arithmétique correspondant dont la démonstration est identique si l'on change les locutions „fonction rationnelle“ et „fonction entière“ en „nombre rationnel“ et „nombre entier“.

26) *Il suffit pour cela, comme l'a montré *Gy. (J.) König* [Math. termész. értesitö

*Dans le cas de plus de deux fonctions, on peut pour la recherche de leur p. g. c. d. remplacer deux quelconques des fonctions données par leur p. g. c. d.

Cette façon de procéder est d'ailleurs la seule possible lorsqu'on fait usage de l'*algorithme d'Euclide* pour la recherche du p. g. c. d.

Dans ce cas, pour déterminer le p. g. c. d. de deux fonctions

$$f_0(z_1, z_2, \ldots, z_m, z), \quad f_1(z_1, z_2, \ldots, z_m, z),$$

on peut commencer par transformer, par une substitution linéaire réversible effectuée sur les variables, les deux fonctions f_0 et f_1 en deux fonctions

$$\varphi_0(y_1, y_2, \ldots, y_m, y), \quad \varphi_1(y_1, y_2, \ldots, y_m, y)$$

régulières relativement à l'une des variables y qui y figurent; cette substitution linéaire transforme le p. g. c. d. de ces fonctions dans le p. g. c. d. des fonctions transformées. On cherchera donc le p. g. c. d. des deux fonctions φ_0 et φ_1; à cet effet on envisagera pour un instant y comme seule variable, $y_1, y_2, \ldots, y_m$ comme des paramètres et l'on appliquera aux deux fonctions φ_0 et φ_1 de y l'*algorithme d'Euclide*; on divisera le p. g. c. d. $\varphi_r(y)$ ainsi obtenu par le coefficient de la puissance la plus élevée de y qui y figure (coefficient qui dépend en général de $y_1, y_2, \ldots, y_m$); le quotient ainsi obtenu, si on l'envisage de nouveau comme une fonction

$$D(y_1, y_2, \ldots, y_m, y)$$

des $m+1$ variables $y_1, y_2, \ldots, y_m, y$, est le p. g. c. d. des deux fonctions

$$\varphi_0(y_1, y_2, \ldots, y_m, y), \quad \varphi_1(y_1, y_2, \ldots, y_m, y).$$

En appliquant enfin à la fonction D la substitution inverse de la précédente on obtient le p. g. c. d. cherché des deux fonctions[27])

$$f_0(z_1, z_2, \ldots, z_m, z), \quad f_1(z_1, z_2, \ldots, z_m, z).*$$

*Voici maintenant les propriétés fondamentales du p. g. c. d.:

Désignons par $D[f_1, f_2, \ldots, f_k]$ le p. g. c. d. d'un nombre quelconque k de fonctions rationnelles entières $f_1, f_2, \ldots, f_k$ des variables $z_1, z_2, \ldots,$

2 (1883), p. 45/9], d'étendre au cas de coefficients quelconques une méthode due à *L. Kronecker* [J. reine angew. Math. 94 (1883), p. 344/8; Werke 2, Leipzig 1897, p. 411/6] et concernant le cas où les coefficients de la fonction rationnelle entière envisagée sont entiers et où l'on ne cherche à décomposer cette fonction qu'en facteurs à coefficients entiers [Note de *J. Kürschák*].*

27) Voir *E. Netto,* Vorlesungen über Algebra 2, Leipzig 1900, p. 19/21. Le procédé indiqué par *E. Netto* ne diffère de celui du texte que par la multiplication successive des fonctions $\varphi_1, \varphi_2, \ldots$ qui figurent dans l'*algorithme d'Euclide* par des facteurs convenables des paramètres $y_1, y_2, \ldots, y_n$ afin d'éviter tout dénominateur.

z_m, z; si φ désigne une fonction rationnelle entière quelconque de ces variables ou de quelques-unes d'entre elles, on a

$$D[\varphi f_1, \varphi f_2, \dots, \varphi f_k] = \varphi D[f_1, f_2, \dots, f_k],$$

et, si φ divise exactement chacune des fonctions $f_1, \dots, f_k$, on a

$$D\left[\frac{f_1}{\varphi}, \frac{f_2}{\varphi}, \dots, \frac{f_k}{\varphi}\right] = \frac{D[f_1, f_2, \dots, f_k]}{\varphi}.*$$

Supposons que $f_1, f_2, \dots, f_k$ soient des fonctions de $z_1, z_2, \dots, z_m, z$; ordonnons-les par rapport à z, et appelons $D(z)$ leur p. g. c. d. On pourra trouver des fonctions rationnelles entières $\psi_1(z), \psi_2(z), \dots, \psi_k(z), Z$, telles que l'on ait identiquement

$$\psi_1(z)f_1(z) + \psi_2(z)f_2(z) + \cdots + \psi_k(z)f_k(z) = Z \cdot D(z)$$

et, fait important, Z sera indépendant de z[28]); ce sera une fonction de $z_1, z_2, \dots, z_m$ seulement. Il peut arriver que Z ne contienne pas toutes ces variables et même se réduise à une constante. Si les fonctions $f_1, f_2, \dots, f_k$ sont premières entre elles, et si Z se réduit à une constante, on pourra écrire

$$\psi_1(z)f_1(z) + \psi_2(z)f_2(z) + \cdots + \psi_k(z)f_k(z) = 1.$$

*Si chacune des fonctions rationnelles entières $f_1, f_2, \dots, f_k$ est première avec chacune des fonctions rationnelles entières $\varphi_1, \varphi_2, \dots, \varphi_h$, les deux produits $f_1 f_2 \dots f_k$ et $\varphi_1 \varphi_2 \dots \varphi_h$ sont premiers entre eux.

Si une fonction rationnelle entière f est divisible par plusieurs fonctions rationnelles entières $\varphi_1, \varphi_2, \dots, \varphi_h$, premières entre elles deux à deux, elle est divisible par leur produit[29]).

Soit $F = f_1^{\alpha_1} f_2^{\alpha_2} \dots f_k^{\alpha_k}$, où $f_1, f_2, \dots, f_k$ désignent des facteurs irréductibles distincts; on aura tous les diviseurs de F en prenant les termes du produit

$$(1+f_1+f_1^2+\cdots+f_1^{\alpha_1})(1+f_2+f_2^2+\cdots+f_2^{\alpha_2})\cdots(1+f_k+f_k^2+\cdots+f_k^{\alpha_k}).*$$

On entend par *plus petit commun multiple* (p. p. c. m.) de k fonctions rationnelles entières $f_1, f_2, \dots, f_k$ d'un nombre quelconque de variables la fonction rationnelle entière *de moindre degré* qui est divisible à la fois par f_1, par f_2, ... et par f_k. Posons

$$P = f_1 f_2 \dots f_k;$$

$$F_1 = \frac{P}{f_1},\ F_2 = \frac{P}{f_2},\ \dots,\ F_k = \frac{P}{f_k};$$

28) *Voir *E. Lucas,* J. math spéc. (3) 3 (1889), p. 25, 49.*

29) Pour une étude détaillée de la divisibilité des polynomes, voir *F. Giudice,* Periodico mat. (1) 9 (1893/4), p. 77, 144, 175.

le p. p. c. m. des fonctions $f_1, f_2, \dots, f_k$ a pour expression

$$\frac{f_1 f_2 \cdots f_k}{D[F_1, F_2, \dots, F_k]}.$$

Tout multiple commun de $f_1, f_2, \dots, f_k$ est un multiple de leur p. p. c. m., et les quotients du p. p. c. m. de $f_1, f_2, \dots, f_k$ par f_1, par $f_2, \dots$, par f_k sont des fonctions rationnelles entières premières entre elles.*

6. Nombre de termes divisibles par $z_1^{a_1} z_2^{a_2} \dots z_k^{a_k}$, etc. Nous avons vu (n° **2**) que, si $f(z_1, z_2, \dots, z_m)$ est une fonction rationnelle entière complète de degré n, le nombre de termes de cette fonction est égal à $\frac{(m+n)!}{m!\,n!}$. Pour certaines théories, par exemple celle de l'élimination, il est utile de savoir combien de ces termes sont divisibles par un monome entier donné $z_1^{a_1} z_2^{a_2} \dots z_k^{a_k}$ formé au moyen de k des variables, où $k \leqq m$ et où $a_1, a_2, \dots, a_k$ sont des nombres naturels. Le nombre de ces termes est

$$\frac{(m+n-a_1-a_2-\cdots-a_k)!}{m!\,(n-a_1-a_2-\cdots-a_k)!}.$$

Veut-on avoir, au contraire, le nombre u des termes qui ne sont divisibles ni par $z_1^{a_1}$, ni par $z_2^{a_2}, \dots$, ni par $z_m^{a_m}$? On formera pour $k = 1, 2, \dots, m$ les expressions

$$S_k = \sum_{\alpha_1, \dots, \alpha_k} \frac{(m+n-a_{\alpha_1}-a_{\alpha_2}-\cdots-a_{\alpha_k})!}{m!\,(n-a_{\alpha_1}-a_{\alpha_2}-\cdots-a_{\alpha_k})!}$$

où, pour une valeur déterminée de k, la somme est étendue à toutes les combinaisons des valeurs

$$\alpha_1 = 1, 2, \cdots, m-k+1;\ \alpha_2 = 2, 3, \cdots, m-k+2;\ \cdots;$$
$$\alpha_k = k, k+1, \cdots, m,$$

pour lesquelles on a

$$\alpha_1 < \alpha_2 < \cdots < \alpha_k;$$

le nombre cherché est alors[30])

$$u = \frac{(m+n)!}{m!\,n!} - S_1 + S_2 - S_3 + \cdots + (-1)^m S_m.$$

Le même nombre u s'obtient encore comme il suit: Quelle que soit la fonction $F(m, n)$ que l'on envisage convenons de désigner par le symbole

$$\Delta_a F(m, n)$$

30) *J. A. Serret,* Algèbre supérieure (5e éd.) 1, Paris 1885, p. 152; *E. Netto,* Alg.[27]) 2, p. 3.

l'expression

$$\Delta_\alpha F(m,n) = F(m,n) - F(m, n-\alpha)$$

en sorte que

$$\Delta_\alpha \frac{(m+n)!}{m!\,n!}$$

désignera le nombre défini par l'égalité

$$\Delta_\alpha \frac{(m+n)!}{m!\,n!} = \frac{(m+n)!}{m!\,n!} - \frac{(m+n-\alpha)!}{m!\,(n-\alpha)!};$$

soit ensuite $\Delta^2_{\alpha,\beta}\frac{(m+n)!}{m!\,n!}$ ou $\Delta^2_{\beta,\alpha}\frac{(m+n)!}{m!\,n!}$ le nombre

$$\Delta_\alpha\left[\Delta_\beta \frac{(m+n)!}{m!\,n!}\right] = \Delta_\alpha \frac{(m+n)!}{m!\,n!} - \Delta_\alpha \frac{(m+n-\beta)!}{m!\,(n-\beta)!}$$

$$= \Delta_\beta\left[\Delta_\alpha \frac{(m+n)!}{m!\,n!}\right] = \Delta_\beta \frac{(m+n)!}{m!\,n!} - \Delta_\beta \frac{(m+n-\alpha)!}{m!\,(n-\alpha)!}$$

et ainsi de suite; on aura alors

$$u = \Delta^m_{\alpha_1, \alpha_2, \ldots, \alpha_m} \frac{(m+n)!}{m!\,n!}.$$

Voici un autre problème important: donnons-nous à l'avance $\frac{(m+n)!}{m!\,n!}$ valeurs

$$f^{(\varrho)} \qquad \left(\varrho = 1, 2, 3, \ldots, \frac{(m+n)!}{m!\,n!}\right)$$

de $f(z_1, z_2, \ldots, z_m)$; admettons que la valeur donnée $f^{(\varrho)}$ soit atteinte pour le système de valeurs également donné $z_1 = \zeta_{1,\varrho}$, $z_2 = \zeta_{2,\varrho}, \ldots,$ $z_m = \zeta_{m,\varrho}$ et cela pour $\varrho = 1, 2, 3, \ldots, \frac{(m+n)!}{m!\,n!}$; si nous voulons déterminer la fonction f pour qu'il en soit ainsi, en regardant les $\frac{(m+n)!}{m!\,n!}$ coefficients de cette fonction f comme des inconnues, nous avons précisément $\frac{(m+n)!}{m!\,n!}$ équations linéaires: il y aura donc (n° **10**) une seule solution si le déterminant des coefficients des inconnues est différent de zéro.

La proposition analogue correspondant au cas où $f^{(\varrho)} = 0$, ϱ ne devant alors prendre que les valeurs $1, 2, 3, \cdots, \frac{(m+n)!}{m!\,n!} - 1$, est fondamentale dans la Géométrie algébrique, sourtout en raison du célèbre *paradoxe d'Euler*[31]).

31) A propos du *paradoxe d'Euler* dont il sera question d'une façon détaillée dans le tome III de l'Encyclopédie, voir surtout *C. Maclaurin,* Geometria organica, Londres 1720, p. 137; *L. Euler,* Hist. Acad. Berlin 4 (1748), éd. 1750, p. 219; *G. Cramer,* Introd. à l'Analyse des lignes courbes alg., Genève 1750, p. 78; *C. G. J. Jacobi,* J. reine angew Math. 15 (1836), p. 285; Werke 3, Berlin 1884, p. 329.

7. Fonctions symétriques. Une fonction *symétrique* de n lettres $z_1, z_2, \ldots, z_n$ est une fonction dont la forme n'est pas altérée lorsqu'on y permute d'une façon quelconque les lettres $z_1, z_2, \ldots, z_n$.

Toute fonction symétrique rationnelle entière de $z_1, z_2, \ldots, z_n$ peut être mise sous la forme d'une somme de fonctions symétriques rationnelles entières *homogènes* des mêmes lettres.

Parmi ces dernières les plus simples sont celles où dans tous les termes figurent les mêmes exposants. Chaque fonction symétrique rationnelle entière homogène φ est d'ailleurs soit une telle fonction soit la somme de telles fonctions $\varphi_1, \varphi_2, \ldots$; elle peut donc toujours être mise sous la forme

$$\varphi = a_1\varphi_1 + a_2\varphi_2 + \cdots;$$

on dit alors que $a_1, a_2, \ldots$ sont les coefficients de la fonction symétrique φ.

Toute fonction rationnelle $\frac{F(z_1, z_2, \ldots, z_n)}{G(z_1, z_2, \ldots, z_n)}$ qui est symétrique peut être mise, après suppression éventuelle d'un facteur commun aux deux fonctions rationnelles entières F et G, sous la forme du quotient de deux fonctions symétriques rationnelles entières.

On appelle fonctions symétriques *élémentaires* de $z_1, z_2, \ldots, z_n$ les n fonctions symétriques rationnelles entières

$$\begin{aligned}
s_1 &= z_1 + z_2 + \cdots + z_n,\\
s_2 &= z_1z_2 + z_1z_3 + \cdots + z_{n-1}z_n,\\
s_3 &= z_1z_2z_3 + z_1z_2z_4 + \cdots + z_{n-2}z_{n-1}z_n,\\
&\cdots\cdots\cdots\cdots\cdots\\
s_n &= z_1z_2z_3\ldots z_n;
\end{aligned}$$

la $p^{\text{ième}}$ fonction symétrique élémentaire s_p est la somme des C_n^p produits de p facteurs $z_{i_1}, z_{i_2}, \ldots, z_{i_p}$ obtenus en prenant successivement pour les indices $i_1, i_2, \ldots, i_p$ les $C_n^p = \frac{n(n-1)\cdots(n-p+1)}{1\cdot 2\cdots p}$ combinaisons p à p des n nombres $1, 2, \ldots, n$.

Toute fonction symétrique rationnelle entière $\varphi(z_1, z_2, \ldots, z_n)$ est une fonction rationnelle entière $\Phi(s_1, s_2, \ldots, s_n)$ des fonctions symétriques élémentaires $s_1, s_2, \ldots, s_n$ de $z_1, z_2, \ldots, z_n$. C'est une somme de monomes de la forme $As_1^{h_1}s_2^{h_2}\ldots s_n^{h_n}$, où A est une fonction rationnelle entière à coefficients entiers des coefficients de la fonction symétrique $\varphi(z_1, z_2, \ldots, z_n)$. Ainsi la fonction symétrique rationnelle entière

$$\varphi(z_1, z_2) = a(z_1^2 + z_2^2) + bz_1z_2 + c(z_1 + z_2)$$

peut être mise sous la forme

$$\varphi(z_1, z_2) = as_1^2 + (b - 2a)s_2 + cs_1.$$

On appelle *poids* du monome $As_1^{h_1}s_2^{h_2}\dots s_n^{h_n}$ la somme

$$h_1 + 2h_2 + \cdots + nh_n$$

et l'on dit d'une fonction rationnelle entière de $s_1, s_2, \dots, s_n$ qu'elle est *isobarique*[32]) de poids ϱ lorsque chacun de ses termes a le poids ϱ[33]).

On voit immédiatement que la fonction rationnelle entière $\Phi(s_1, s_2, \dots, s_n)$ dans laquelle on peut transformer une fonction symétrique rationnelle entière homogène $\varphi(z_1, z_2, \dots, z_n)$ de degré ϱ est isobarique de poids ϱ. Si, $\Phi(s_1, s_2, \dots, s_n)$ étant isobarique de poids ϱ, on désigne par t une variable auxiliaire ne figurant pas dans $\Phi(s_1, s_2, \dots, s_n)$ on a

$$\Phi(ts_1, t^2 s_2, \dots, t^n s_n) = t^\varrho \Phi(s_1, s_2, \dots, s_n).$$

*Plus généralement, F désignant une fonction quelconque des fonctions rationnelles entières $f_0, f_1, \dots, f_k$ d'une ou de plusieurs variables, nous conviendrons d'attacher à chaque f_i un nombre ϱ_i fixé d'une façon arbitraire; nous nommerons ce nombre ϱ_i le poids de f_i et nous dirons que F est isobarique de poids ϱ en $f_0, f_1, \dots, f_k$ quand

$$F(t^{\varrho_0} f_0, t^{\varrho_1} f_1, t^{\varrho_2} f_2, \dots, t^{\varrho_k} f_k) = t^\varrho F(f_0, f_1, f_2, \dots, f_k).*$$

Soient par exemple m fonctions

$$f_1(z_1, z_2, \dots, z_m),\ f_2(z_1, z_2, \dots, z_m),\ \dots,\ f_m(z_1, z_2, \dots, z_m),$$

respectivement de degrés $n_1, n_2, \dots, n_m$. On attribue généralement[33]) au coefficient $a_\alpha^{(i)}$ du terme

$$a_\alpha^{(i)} z_1^{\nu_1} z_2^{\nu_2} \cdots z_m^{\nu_m}$$

de f_α le poids

$$p_{\alpha i} = n_\alpha - (\nu_1 + \nu_2 + \cdots + \nu_m);$$

et aux variables $z_1, z_2, \dots, z_m$ le poids 1; enfin on appelle poids d'un produit la somme des poids des facteurs de ce produit. La fonction f_α sera alors isobarique et de poids n_α. Toute fonction rationnelle entière $F(\dots a_\alpha^{(i)} \dots)$ des coefficients $a_\alpha^{(i)}$ des fonctions $f_1, f_2, \dots, f_m$ est d'ailleurs isobarique et de poids p lorsqu'on a

$$F(\dots t^{p_{\alpha i}} a_\alpha^{(i)} \dots) = t^p F(\dots a_\alpha^{(i)} \dots).$$

On peut aussi envisager des fonctions symétriques de plusieurs séries de variables. Pour fixer les idées nous raisonnerons, par exemple, sur trois séries de k variables

32) *D'après *F. Faà di Bruno* [Théorie des formes binaires, Turin 1876, p. 18] *A. Cayley* a le premier fait usage de cette locution „*isobarique*". *A. Cayley* appelle d'ailleurs [J. reine angew. Math. 47 (1854), p. 113; Papers 2, Cambr. 1889, p. 167/8] *pesanteur* ce que nous appelons *poids*.*

33) *Voir par ex. *A. E. Pellet,* Nouv. Ann. math. (2) 14 (1875), p. 259.*

$$\begin{array}{c} x_1,\ x_2,\ x_3,\ \dots,\ x_{k-1},\ x_k \\ y_1,\ y_2,\ y_3,\ \dots,\ y_{k-1},\ y_k \\ z_1,\ z_2,\ z_3,\ \dots,\ z_{k-1},\ z_k \end{array}$$

représentées par trois lettres x, y, z affectées d'indices $1, 2, 3, \dots, k-1, k$.

On appelle *fonction symétrique* toute fonction de ces trois séries de variables qui ne change pas de forme quand on effectue une permutation quelconque des nombres $1, 2, \cdots, k$ simultanément sur tous les indices de x, y et z.

Les plus simples des fonctions symétriques que l'on appelle *fonctions symétriques élémentaires* sont formées de la façon suivante.

Soient α, β, γ trois nombres fixes dont la somme h soit égale ou inférieure à k. Formons un produit tel que

$$x_1 x_2 \dots x_\alpha y_{\alpha+1} \cdots y_{\alpha+\beta} z_{\alpha+\beta+1} \cdots z_{\alpha+\beta+\gamma}$$

dans lequel figurent 1) α facteurs x; 2) β facteurs y ayant des indices distincts de ceux des α facteurs x; 3) γ facteurs z ayant des indices distincts de ceux des α facteurs x et de ceux des β facteurs y; les $\alpha + \beta + \gamma$ indices constituent alors un arrangement des nombres $1, 2, \dots, k$ pris h à h. Désignons par $c_{\alpha\beta\gamma}$ la somme

$$c_{\alpha\beta\gamma} = S(x_1 \dots x_\alpha y_{\alpha+1} \cdots y_{\alpha+\beta} z_{\alpha+\beta+1} \cdots z_{\alpha+\beta+\gamma})$$

étendue à tous les arrangements h à h des nombres $1, 2, \dots, k$ pour lesquels α, β et γ conservent la même valeur; cette somme est appelée une *fonction symétrique élémentaire* des 3 séries de variables envisagées. Ainsi l'on a

$$\begin{gathered} c_{100} = x_1 + \cdots + x_k, \quad c_{010} = y_1 + \cdots + y_k, \quad c_{001} = z_1 + \cdots + z_k, \\ c_{200} = x_1 x_2 + x_1 x_3 + \cdots + x_{k-1} x_k, \ \dots,\ c_{00k} = z_1 z_2 \dots z_k, \\ c_{110} = x_1 y_2 + \cdots + x_1 y_k + x_2 y_1 + x_2 y_3 + \cdots + x_2 y_k + \cdots \\ + x_k y_1 + \cdots + x_k y_{k-1}, \ \dots . \end{gathered}$$

Toute fonction symétrique entière est une fonction rationnelle entière des fonctions symétriques élémentaires $c_{\alpha\beta\gamma}$.[34])

Envisageons une fonction symétrique entière, homogène et de degré a par rapport aux x, homogène et de degré b par rapport aux y, homogène et de degré c par rapport aux z.

Cette fonction s'exprime[35]) au moyen des fonctions symétriques

34) *S. D. Poisson,* J. Ec. Polyt. (1) cah. 11 (an X), p. 199.

35) Pour le calcul de ces fonctions symétriques cf. *L. Schläfli,* Denkschr. Akad. Wien (math.) 4 II (1852), p. 1/74; *A. Cayley,* Philos. Trans. London 147 (1857), p. 717, Papers 2, Cambridge 1889, p. 454; *E. Betti*, Ann. mat. pura appl.

élémentaires $c_{\alpha\beta\gamma}$ sous la forme d'une somme de termes tels que

$$A c_{\alpha\beta\gamma}^{q} c_{\alpha'\beta'\gamma'}^{q'} c_{\alpha''\beta''\gamma''}^{q''} \cdots$$

où A est un coefficient constant. Pour chacun des termes la somme

$$q\alpha + q'\alpha' + q''\alpha'' + \cdots$$

que nous désignerons par $\Sigma q\alpha$ est égale à a; on l'appelle le *poids partiel* de la fonction symétrique par rapport aux x. De même pour chacun des termes on a

$$\sum q\beta = q\beta + q'\beta' + q''\beta'' + \cdots = b$$
$$\sum q\gamma = q\gamma + q'\gamma' + q''\gamma'' + \cdots = c$$

et ces deux sommes $\Sigma q\beta$, $\Sigma q\gamma$ sont appelées les *poids partiels* de la fonction symétrique par rapport aux y ou aux z. La somme

$$\sum q\alpha + \sum q\beta + \sum q\gamma$$

est appelée le *poids total* de la fonction symétrique. La fonction symétrique envisagée est *isobarique* par rapport aux poids partiels et par rapport au poids total.

*La fonction symétrique élémentaire $c_{\alpha\beta\gamma}$ est au fond identique au coefficient de $u^\alpha v^\beta w^\gamma$ dans le développement de l'expression

$$(x_1 u + y_1 v + z_1 w + 1)(x_2 u + y_2 v + z_2 w + 1) \cdots (x_k u + y_k v + z_k w + 1)$$

suivant les puissances de u, v, w.

Celles des fonctions symétriques homogènes entières qui sont homogènes et de même degré r par rapport à chacun des k systèmes

$$(x_1, y_1, z_1),\ (x_2, y_2, z_2),\ \ldots,\ (x_k, y_k, z_k)$$

s'expriment en fonction entière homogène de degré r des fonctions symétriques élémentaires $c_{\alpha\beta\gamma}$ qui figurent comme coefficients dans le développement de l'expression

$$(x_1 u + y_1 v + z_1 w)(x_2 u + y_2 v + z_2 w) \cdots (x_k u + y_k v + z_k w)$$

suivant les puissances de u, v, w[36]).*

*Si l'on envisage[37]) *deux* séries de k variables

$$x_1,\ x_2,\ x_3,\ \ldots,\ x_{k-1},\ x_k$$
$$y_1,\ y_2,\ y_3,\ \ldots,\ y_{k-1},\ y_k$$

le nombre des fonctions symétriques élémentaires est égal à $\frac{1}{2}k(k+3)$

(1) 1 (1858), p. 193; *Ch. Méray,* Ann. Ec. Norm. (1) 4 (1867), p. 159; *P. A. Mac Mahon,* Philos. Trans. London 181 (1890), p. 481; *Fr. Junker,* Math. Ann. 38 (1891), p. 92; 43 (1893), p. 225; 45 (1894), p. 1; Z. Math. Phys. 41 (1896), p. 199; Denkschr. Akad. Wien (math.) 64 (1897), p. 439; *E. Netto,* Alg.[27]) 2, p. 71/5; *Gy. (J.) König,* Alg. Grössen [20]), p. 312/23.

36) *Texte de *J. Kürschák.**

et est plus grand par conséquent que le nombre $2k$ des variables; il en résulte que ces fonctions symétriques élémentaires sont liées par des relations déterminées. Il en est de même *a fortiori* quand on envisage plus de deux séries de k variables.

Un grand nombre de ces relations ont été obtenues dans le cas de *deux* séries de k variables par *Fr. Junker*[35]); il les a établies en utilisant des tableaux fournissant les expressions de toutes les fonctions symétriques de deux séries de k variables au moyen des fonctions symétriques élémentaires de ces deux séries de k variables. Ces tableaux déjà dressés par *P. A. Mac Mahon*[35]) lorsque le poids total est inférieur à 5 ont été ensuite complétés par *Fr. Junker* lorsque le poids total est égal à 5 ou à 6.

On peut représenter[38]) sous forme d'invariants binaires toutes les relations entre les fonctions de deux séries de k variables; toutes ces relations sont alors envisagées comme des équations de condition pour la décomposition en facteurs linéaires d'une forme ternaire[39]).*

8. Décomposition des formes en général et questions connexes. *Une fonction rationnelle entière et *homogène* à plusieurs variables s'appelle aussi une *forme algébrique*[40]). Lorsqu'on emploie cette locution on s'attache plus spécialement à la nature des coefficients qu'à celle des variables. Suivant qu'il y a deux, trois, quatre, ... ou n variables on dit que la forme est *binaire*, *ternaire*, *quaternaire*, ... ou n-aire. Suivant que la forme est du premier, deuxième, troisième ou quatrième degré, on dit qu'elle est *linéaire*, *quadratique*, *cubique* ou *biquadratique*.

On dit d'une forme quelconque qu'elle est *générale* lorsqu'elle est complète et que chacun de ses coefficients est *indéterminé*. Si l'on effectue une substitution linéaire et homogène sur la forme générale $(m+1)$-aire

$$f(z_1, z_2, \cdots, z_m, z)$$

dont nous désignerons ici les coefficients par $a, b, c, \cdots$ on obtient une nouvelle forme dont nous désignerons les coefficients par $a', b', c', \cdots$. Toute fonction rationnelle entière homogène $F(a, b, c, \cdots)$ telle que, pour *chaque* substitution linéaire homogène envisagée, le quotient $\frac{F(a', b', c', \ldots)}{F(a, b, c, \ldots)}$ soit égal à une puissance du déterminant de la substitution est dite un *invariant* de la forme $f(z_1, z_2, \cdots, z_m, z)$. Toute

37) **A. Brill,* Nachr. Ges. Gött. 1893, p. 757.*

38) *Math. Ann. 50 (1898), p. 157 (Texte et notes 37/9 de *A. Brill*).*

39) *Voir les notes 56 à 60 et le texte correspondant.*

40) *Les Anglais disent „*quantic*" [voir par ex. *A. Cayley,* Philos. Trans. 144 (1854), p. 244; Papers 2, Cambridge 1889, p. 221].*

fonction rationnelle entière

$$F(a, b, c, \cdots; z_1, z_2, \cdots, z_m, z)$$

homogène en $a, b, c, \cdots$ et homogène en $z_1, z_2, \cdots, z_m, z$ telle que pour *chaque* substitution linéaire et homogène qui introduit de nouvelles variables $z_1', z_2', \cdots, z_m', z'$, le quotient

$$\frac{F(a', b', c', \cdots; z_1', z_2', \cdots, z_m', z')}{F(a, b, c, \cdots; z_1, z_2, \cdots, z_m, z)}$$

soit égal à une puissance du déterminant de la substitution envisagée, est dite un *covariant* de la forme f.

On appelle *invariants* et *covariants* d'une forme à coefficients *déterminés* les expressions que l'on obtient en remplaçant, dans les invariants et covariants de la forme générale correspondante, les indéterminées par les coefficients de la forme particulière envisagée. Lorsque les coefficients de la forme envisagée sont des nombres les invariants de cette forme sont des nombres tandis que les covariants sont des fonctions rationnelles entières à coefficients numériques.

On appelle *invariants* et *covariants* d'une fonction rationnelle entière non homogène $f(z_1, z_2, \cdots, z_m)$ des m variables $z_1, z_2, \cdots, z_m$ les invariants et covariants pour $z = 1$ de la forme $(m+1)$-aire qui pour $z = 1$ se réduit à $f(z_1, z_2, \cdots, z_m)$.

Les notions d'invariant et de covariant s'étendent immédiatement à des systèmes de formes ou de fonctions rationnelles entières; ces systèmes admettent des invariants et des covariants simultanés.

Les invariants et covariants jouent un rôle capital dans l'étude de la décomposition des formes.*

D. Hilbert[41]) a cherché la condition pour qu'une forme binaire soit une puissance donnée d'une autre forme binaire ou, ce qui revient au même, pour qu'une fonction rationnelle entière d'une variable soit une puissance donnée d'une autre fonction rationnelle de la même variable.

Soit $f(x)$ une fonction rationnelle entière de la variable x, de degré n, et $f'(x), f''(x), \ldots$ les dérivées successives de $f(x)$ par rapport à x. Convenons d'attacher aux fonctions

$$f_0 = f(x), \quad f_1 = \frac{1}{n} f'(x), \quad f_2 = \frac{1}{n(n-1)} f''(x), \quad \cdots$$

les poids $0, 1, 2, \ldots$ en sorte que f_i ait le poids i et introduisons les symboles $D(F)$, $\Delta(F)$ pour représenter les opérations suivantes effectuées sur une fonction quelconque F de $f_0, f_1, f_2, \cdots$

$$D(F) = f_0 \frac{\partial F}{\partial f_1} + 2 f_1 \frac{\partial F}{\partial f_2} + 3 f_2 \frac{\partial F}{\partial f_3} + \cdots$$

$$\Delta(F) = n f_1 \frac{\partial F}{\partial f_0} + (n-1) f_2 \frac{\partial F}{\partial f_1} + (n-2) f_3 \frac{\partial F}{\partial f_2} + \cdots;$$

représentons aussi par Δ^k l'opération Δ répétée k fois.

D. Hilbert[41]) a démontré que lorsqu'en appliquant l'opération $D(F)$ à une fonction F homogène (n° 2) et isobarique (n° 7) on obtient

$$D(F) = 0,$$

F est une fonction des invariants et covariants de la forme f. Si, μ désignant un diviseur de n, on pose $\nu = \frac{n}{\mu}$ la fonction

$$F_\nu = \Delta^{\nu+1}\left(f_0^{\frac{1}{\mu}}\right)$$

satisfait à l'équation

$$D(F_\nu) = 0;$$

d'où il résulte que F_ν et le produit[42])

$$C_\nu = f_0^{\nu - \frac{1}{\mu} + 1} \Delta^{\nu+1}\left(f_0^{\frac{1}{\mu}}\right)$$

sont des fonctions des invariants et covariants de la forme f. Enfin $C_\nu = 0$ est la condition nécessaire et suffisante pour que f soit égale à la puissance $\mu^{\text{ième}}$ d'une fonction rationnelle entière $\varphi(x)$.

C. Weltzien[43]) étend les mêmes recherches au cas des formes ternaires. *G. Giordano*[44]) cherche la condition pour qu'une forme binaire φ du quatrième degré soit (à un facteur constant près) le carré d'une forme quadratique ψ. Plus tard[45]), étant données les formes n-aires φ de degré nh et ψ de degré n, il cherche à quelles conditions on a $\varphi = A\psi^h$, A étant une constante.

M. Nöther[46]) s'est occupé de la détermination du facteur commun à deux formes binaires (cf. n° **35**). Dans le même ordre d'idées *F. Brioschi*[47]) a étudié les invariants de deux formes binaires ayant un facteur commun. Des recherches de *J. Lüroth*[48]) ont le même objet que celles de *M. Nöther*.

J. Lüroth[49]) fait aussi la remarque que, si deux fonctions rationnelles entières $f(z)$ et $\varphi(z)$ de degrés n et ν ont un p. g. c. d. de

41) Math. Ann. 27 (1886), p. 158 [1885]. *Voir déjà *F. Faà di Bruno*, Formes binaires[32]), p. 149; J. reine angew. Math. 90 (1881), p. 186; et cf. l'article I 11.*

42) Voir aussi *F. Brioschi*, Rend. Circ. mat. Palermo 10 (1896), p. 153.

43) Progr. Berlin 1892.

44) Giorn. mat. (2) 4 (1897), p. 349.

45) Id. (2) 7 (1900), p. 210.

46) Sitzgsb. phys.-medic. Soc. Erlangen 27 (1895), p. 110/5.

47) Id. 27 (1895), p. 116/8.

48) Id. 27 (1895), p. 119.

49) Z. Math. Phys. 40 (1895), p. 247.

degré p, le degré du p. p. c. m. des deux fonctions $f(z)$ et $\varphi(z)$ n'est que $n + \nu - p$. Il déduit de là une manière de retrouver les conditions pour que les deux fonctions $f(z)$ et $\varphi(z)$ aient un diviseur commun de degré p.

M. Falk [50]) a démontré que, si les r premiers coefficients de deux fonctions rationnelles entières

$$f(z) = a_0 z^n + a_1 z^{n-1} + \cdots + a_n,$$
$$\varphi(z) = b_0 z^n + b_1 z^{n-1} + \cdots + b_n$$

de même degré n sont proportionnels, en sorte que l'on ait

$$a_0 : a_1 : \cdots : a_r = b_0 : b_1 : \cdots : b_r$$

tandis que $a_0 b_{r+1} - b_0 a_{r+1}$ est différent de zéro, le plus grand commun diviseur de $f(z)$ et de $\varphi(z)$ est aussi celui des deux fonctions rationnelles entières

$$g(z) = b_0 f(z) - a_0 \varphi(z),$$
$$\psi(z) = (b_0 z^{r+1} + \cdots + b_{r+1}) f(z) - (a_0 z^{r+1} + \cdots + a_{r+1}) \varphi(z).$$

Les deux fonctions $g(z)$, $\psi(z)$ sont évidemment toutes deux de degré $< n$. Le théorème s'applique d'ailleurs aussi, en prenant $r = 0$, dans le cas où $a_0 b_1 - a_1 b_0$ est différent de zéro.

En appliquant à nouveau le théorème de *M. Falk* aux deux fonctions $g(z)$ et $\psi(z)$ [cette dernière éventuellement multipliée par une puissance convenable de z quand son degré est plus petit que celui de $g(z)$], on ramène la recherche du p. g. c. d. de ces deux fonctions, et par suite celle du p. g. c. d. de $f(z)$ et de $\varphi(z)$, à la recherche du p. g. c. d. de deux fonctions rationnelles entières de degrés encore moindres, et ainsi de suite. *M. Falk* arrive ainsi aisément à former le plus grand commun diviseur cherché.

L'étude des relations qui doivent avoir lieu entre les coefficients d'une fonction rationnelle entière $f(z)$ et un nombre α pour que $f(z)$ soit divisible par le binome $z^n - \alpha^n$ a fait l'objet de recherches de *C. F. E. Björling* [51]), de *B. C. A. M. Berloty* [52]) et de *C. J. D. Hill* [53]).

D'autres travaux relatifs à la théorie du p. g. c. d. et en particulier à la recherche des conditions pour que deux fonctions rationnelles entières aient un p. g. c. d. de degré donné seront mentionnés dans la théorie de l'élimination (nos **34** et suiv.).

50) Nova Acta Upsal. (3) 10 (1879), mém. n° 11 [1878].
51) Archiv Math. Phys. (1) 55 (1873), p. 429.
52) Nouv. Ann. math. (3) 1 (1882), p. 173.
53) J. reine angew. Math. 70 (1869), p. 103.

W. F. Meyer [54]) a obtenu le théorème suivant: Soient $f(x)$ et $\varphi(x)$ deux fonctions rationnelles entières quelconques de x. Envisageons pour $k = 1, 2, 3, \ldots$ les fonctions rationnelles entières de x définies par l'expression

$$\Delta_k = \frac{1}{k!}[f(x)]^{k+1} \frac{\partial^k}{\partial x^k}\left(\frac{\varphi(x)}{f(x)}\right);$$

l'expression

$$\Delta_n \Delta_{n-s} - \Delta_{n-s_1} \Delta_{n-s_2},$$

où s désigne l'un quelconque des nombres $2, 3, \ldots, n$ et s_1, s_2 des nombres naturels dont la somme soit s, est divisible par $[f(x)]^{n-s+1}$.

Il en est de même de l'expression

$$\Delta_n^{s-1} \Delta_{n-s} - \Delta_{n-1}^{s},$$

s désignant toujours l'un quelconque des nombres $2, 3, \ldots, n$.

La recherche des conditions nécessaires et suffisantes pour qu'une forme soit décomposable en facteurs linéaires est liée à la théorie des fonctions symétriques (n° **7**) de plusieurs séries de n variables.

*On obtient les équations de condition pour qu'une forme ternaire se décompose en facteurs linéaires en égalant identiquement à zéro certaines formes intermédiaires dites „concomitantes mixtes" de cette forme ternaire.

S. H. Aronhold [55]) a envisagé en particulier le cas des formes ternaires du troisième degré.

P. Gordan [56]) s'est occupé de la recherche des concomitants mixtes dans le cas général des formes ternaires de degré n. Il a d'ailleurs montré que quand le système des équations obtenues en égalant identiquement à zéro ces concomitants mixtes est vérifié, la forme ternaire est contenue en facteur dans son hessien (n° **76**). D'autre part, la décomposition de toute forme ternaire de degré n est une conséquence nécessaire de l'évanouissement de certains covariants simultanés des formes binaires qui figurent comme coefficients dans la forme ternaire ordonnée suivant l'une des 3 variables dont elle dépend.

C'est de cette façon que dans le cas de formes ternaires cubiques *F. Brioschi* et, dans le cas de formes ternaires de degré n, *A. Brill* ont donné un système de conditions *suffisantes* pour la décomposition de ces formes en facteurs linéaires [57]).

54) Math. Ann. 36 (1890), p. 440, 444.
55) J. reine angew. Math. 55 (1858), p. 97. Cf. *C. Weltzien*, Diss. Berlin 1882.
56) *Math. Ann. 45 (1894), p. 410.*
57) **F. Brioschi*, Ann. mat. pura appl. (2) 7 (1875/6), p. 189; Opere 2, Milan 1902, p. 137; *A. Brill*, Math. Ann. 50 (1898) p. 166.*

Quoique le nombre d'équations qui figure dans ce système de conditions suffisantes soit inférieur à celui obtenu en égalant identiquement à zéro les concomitants mixtes, il n'est cependant pas le plus petit possible.

Ainsi pour les formes ternaires cubiques[58]) le système de conditions suffisantes est formé par cinq équations dont aucune ne peut être laissée de côté quoique leur ensemble soit équivalent à trois conditions seulement[59]).*

J. Hadamard[60]) a tenté de démontrer que, du système des conditions obtenues, on n'en peut déduire aucune qui soit de degré inférieur à $n+1$; il suffirait, pour achever la démonstration, de démontrer la proposition suivante: si une fonction F de degré inférieur à $n+1$ des coefficients d'une forme de degré n s'annule toutes les fois que la forme est décomposable en facteurs linéaires, elle s'annule aussi toutes les fois que cette forme contient *un* facteur linéaire[61]).*

H. Hočevar[62]) a montré que la condition nécessaire et suffisante pour qu'une forme quelconque f de n variables soit décomposable en facteurs linéaires est que chaque mineur du troisième ordre (I 2, **20**) du *hessien* (n° **76**) de f soit divisible par f. Il y a $\frac{1}{2}(n-1)(n-2)$ conditions distinctes.

*En ce qui concerne les formes ternaires cubiques, *F. Brioschi*[63]) était parvenu au théorème suivant: Soit

$$\nu(x, y) = ax^3 + 3bx^2y + 3cxy^2 + dy^3$$

une forme *binaire* cubique en x, y; posons

$$\begin{aligned}\tau(x, y) &= \frac{1}{18}\left[\frac{\partial^2 \nu}{\partial x^2}\frac{\partial^2 \nu}{\partial y^2} - \left(\frac{\partial^2 \nu}{\partial x \partial y}\right)^2\right]\\ &= 2(ac-b^2)x^2 + 2(ad-bc)xy + 2(bd-c^2)y^2;\end{aligned}$$

l'expression la plus générale d'une forme cubique *ternaire* en x, y, z décomposable en trois facteurs linéaires, qui ne contienne pas de terme en z^2, est, en supposant que le coefficient de z^3 soit 1,

$$z^3 + 3\frac{z\tau}{\sqrt[3]{2C}} + 2\nu(x, y),$$

58) *Math. Ann. 50 (1898), p. 180.*

59) *(Texte et notes 56 à 59 de *A. Brill*).*

60) Bull. Soc. math. France 27 (1899), p. 34.

61) Voir encore *Fr. Junker*, Math. Ann. 45 (1894), p. 1; voir aussi *L. Painvin*, C. R. Acad. sc. Paris 50 (1860), p. 84, 600, 682.

62) C. R. Acad. sc. Paris 138 (1904), p. 745.

63) Opere[57]) 2, p. 137 [1875]; voir aussi *A. Thaer*, Math. Ann. 14 (1879). p. 545.

où C désigne l'expression

$$C = 4(ac-b^2)(bd-c^2) - (ad-bc)^2.$$

Une substitution linéaire permet d'ailleurs toujours de ramener une forme cubique ternaire quelconque en x, y, z à une forme cubique ternaire ne contenant pas de terme en z^2.*

Plaçons-nous maintenant dans le cas où les facteurs de décomposition peuvent être de degré quelconque et dans cet ordre d'idées citons *W. F. Meyer* qui s'est occupé de la réductibilité des fonctions entières dont les coefficients dépendent d'un ou de plusieurs paramètres[64]).

Voici encore un théorème de *E. Bertini* dont s'est également occupé *J. Lüroth*[65]). Soit $f(z_1, z_2, \dots; \lambda_1, \lambda_2, \dots)$ une fonction rationnelle entière de $z_1, z_2, \dots; \lambda_1, \lambda_2, \dots$, *linéaire* par rapport à $\lambda_1, \lambda_2, \dots$; si cette fonction $f(z_1, z_2, \dots; \lambda_1, \lambda_2, \dots)$, considérée comme fonction de $z_1, z_2, \dots$, est réductible pour des valeurs indéterminées des paramètres $\lambda_1, \lambda_2, \dots$; alors: ou bien on peut séparer de $f(z_1, z_2, \dots; \lambda_1, \lambda_2, \dots)$ un facteur qui ne contient que les variables $z_1, z_2, \dots$, et qui est indépendant des paramètres $\lambda_1, \lambda_2, \dots$, ou bien l'on a, A et B étant des fonctions rationnelles entières de $z_1, z_2, \dots$,

$$f(z_1, z_2, \dots; \lambda_1, \lambda_2, \dots) = (A + \lambda' B)(A + \lambda'' B) \dots (A + \lambda^{(n)} B),$$

$\lambda', \lambda'', \dots, \lambda^{(n)}$ étant les racines d'une équation

$$c_0\lambda^n + c_1\lambda^{n-1} + \dots + c_n = 0$$

dont les coefficients $c_0, c_1, \dots, c_n$ sont des fonctions linéaires des paramètres $\lambda_1, \lambda_2, \dots$

*Soient $P(z_1, z_2, z_3)$ et $Q(z_1, z_2, z_3)$ deux formes ternaires de même degré supposées sans facteur commun. *H. Poincaré*[66]) a démontré que si l'expression

$$P(z_1, z_2, z_3) + \lambda Q(z_1, z_2, z_3),$$

où λ désigne un paramètre, est décomposable quel que soit λ, les deux formes P et Q sont fonctions homogènes et de même degré de deux fonctions rationnelles entières Z_1, Z_2 de z_1, z_2, z_3, telles que

64) Math. Ann. 30 (1887), p. 30; Sitzgsb. Akad. München 15 (1885), p. 415; cf. Tageblatt der 58ten Versammlung deutscher Naturforscher und Ärzte in Strassburg (1885), p. 174; voir encore *J. Petersen*, De algebraiske Ligningers Theori, Copenhague 1877; trad. *H. Laurent*, Paris 1897, p. 72; *H. Wiener*, Diss. Munich 1881.

65) *E. Bertini*, Reale Ist. Lombardo, *Rendic.* (2) 15 (1882), p. 24; *J. Lüroth*, Math. Ann. 42 (1893), p. 457; 44 (1894), p. 539.

66) *Rend. Circ. mat. Palermo 5 (1891), p. 183, 187.*

l'expression

$$Z_1(z_1, z_2, z_2) + \mu Z_2(z_1, z_2, z_3),$$

où μ désigne un paramètre, ne soit plus décomposable quel que soit μ.

H. Poincaré[66]) a aussi montré, en appliquant un théorème de *G. H. Halphen*[67]), que si l'expression

$$P(z_1, z_2, z_3) + \lambda Q(z_1, z_2, z_3)$$

est indécomposable pour λ indéterminé, il n'y a jamais plus de deux valeurs de λ pour lesquelles cette expression est une puissance à exposant entier positif d'une fonction rationnelle entière homogène de z_1, z_2, z_3.*

9. Fonctions rationnelles entières qui s'annulent pour tous les systèmes de valeurs des variables qui annulent plusieurs fonctions rationnelles entières données. *Considérons d'abord les fonctions rationnelles entières non homogènes de deux variables et pour simplifier l'énoncé des théorèmes convenons d'appeler *point* (x, y) tout système de valeurs données aux deux variables x, y et *courbe algébrique plane* $f(x, y) = 0$ l'ensemble des points (x, y) pour lesquels une fonction rationnelle entière $f(x, y)$ s'annule.

M. Nöther[68]) démontre que, si les deux courbes algébriques planes

$$\varphi(x, y) = 0, \quad \psi(x, y) = 0$$

ne se coupent en aucun point coïncidant avec un des points multiples de l'une ou de l'autre courbe, chaque courbe algébrique passant par tous les points d'intersection des deux courbes envisagées peut être représentée par une équation $f(x, y) = 0$ dont le premier membre est de la forme

$$f = A\varphi + B\psi,$$

A et B étant des fonctions rationnelles entières de x et de y. *J. Bacharach*[69]) expose à nouveau cette démonstration. D'une façon plus précise, *M. Nöther*[70]) démontre le théorème suivant:

Supposons que, $\varphi(x, y)$ et $\psi(x, y)$ désignant deux fonctions rationnelles entières de x, y sans diviseur commun, à chaque point d'intersection (x_i, y_i) des deux courbes algébriques planes

$$\varphi(x, y) = 0, \quad \psi(x, y) = 0$$

67) *Mémoire sur la réduction des équations différentielles linéaires aux formes intégrables [Mém. présentés Acad. sc. Paris (2) 28 (1884), mém. n° 1, p. 19].*

68) Math. Ann. 2 (1870), p. 314.

69) Diss. Erlangen 1881, p. 7.

70) Math. Ann. 6 (1873), p. 351.

correspondent deux séries a, b entières en $x - x_i$ et $y - y_i$, telles que l'on ait identiquement

$$f = a\varphi + b\psi,$$

où f désigne une fonction rationnelle entière de x, y. Cette fonction rationnelle entière $f(x, y)$ peut alors aussi être mise sous la forme[71])

$$f = A\varphi + B\psi,$$

où A et B sont des fonctions rationnelles entières de x, y. Pour chaque point de la courbe $\psi = 0$ la fonction rationnelle

$$\frac{f(x, y)}{\varphi(x, y)}$$

se réduit à la fonction rationnelle entière $A(x, y)$.

Pour que l'on soit assuré, pour chaque point d'intersection (x_i, y_i) de $\varphi = 0$ et $\psi = 0$, de l'existence de deux séries entières a, b pour lesquelles $f = a\varphi + b\psi$, il suffit que, r_i désignant un nombre entier positif déterminé appartenant au point (x_i, y_i), on connaisse deux fonctions rationnelles entières a', b' de $x - x_i$, $y - y_i$ telles que le développement de l'expression

$$f - a'\varphi - b'\psi$$

suivant les puissances entières de $x - x_i$, $y - y_i$ ne contienne que des termes de degré supérieur à r_i.

Le *cas simple* est celui où le point (x_i, y_i) étant un point multiple d'ordre m de la courbe $\varphi = 0$, d'ordre n de la courbe $\psi = 0$ doit être compté comme mn points d'intersection des deux courbes. Dans le cas simple on a

$$r_i = m + n - 2.$$

Dans le cas général où la multiplicité de l'intersection des deux courbes est d'un ordre $\alpha \geqq mn$, on a[72])

$$r_i = (\alpha - mn) + m + n - 2.$$

M. Nöther aborde aussi le cas où les fonctions φ, ψ, f contiennent plus de deux variables; *E. Picard* et *G. Simart*[73]) réduisent ce cas à celui de deux variables.*

71) *Voir aussi *G. H. Halphen*, Bull. Soc. math. France 5 (1876/7), p. 160.*

72) *E. Bertini*, Math. Ann. 34 (1889), p. 447; *Reale Ist. Lombardo, *Rendic.* (2) 24 (1891), p. 1905; *H. F. Baker* (désigné à tort comme *H. J. Baker*), Math. Ann. 42 (1893), p. 601. Une démonstration énumérative dans le *cas simple* a été donnée par *Charlotte Angas Scott*, Math. Ann. 52 (1899), p. 593.*

73) *Théorie des fonctions algébriques de deux variables indépendantes 2, Paris 1906, p. 17 [1900]. Voir aussi *F. Severi*, Atti R. Accad. Lincei, *Rendic.* math. (5) 11 I (1902), p. 105.*

A. Voss[74]) montre que l'on peut obtenir le théorème concernant le *cas simple* en transformant seulement d'une façon convenable le résultant des deux fonctions φ et ψ. Sa démonstration, jointe à celle de *M. Nöther*[74]) concernant la possibilité de réduire le cas général au cas simple, fournit une démonstration purement algébrique du théorème de *M. Nöther* dans tous les cas.

A. Voss transforme aussi les conditions sous lesquelles le même théorème a lieu; mais cette modification l'amène à introduire des séries dans ses développements. A ces dernières recherches de *A. Voss* s'en rattachent d'analogues de *M. Nöther*, *L. Stickelberger* et *A. Brill*[75]).*

E. Netto[76]) démontre que chaque fonction f qui s'annule pour tous les zéros de φ et de ψ vérifie une équation de la forme

$$f^r = A\varphi + B\psi$$

pour un exposant entier r suffisamment grand.

Passons au cas d'un nombre quelconque de variables. Si la fonction rationnelle entière $f(z_1, z_2, \ldots, z_m)$ s'annule pour tous les systèmes de valeurs des variables annulant une autre fonction rationnelle entière $g(z_1, z_2, \ldots, z_m)$, la fonction f est divisible par chaque facteur irréductible de g. *O. Hölder* et *E. Netto* ont démontré ce théorème[77]). Il en résulte qu'une certaine puissance de f est divisible par g.

Plus généralement, si f s'annule pour tous les systèmes de valeurs de $z_1, z_2, \ldots, z_m$ annulant simultanément n fonctions rationnelles entières

$$g_1(z_1, z_2, \ldots, z_m),\ g_2(z_1, z_2, \ldots, z_m),\ \ldots,\ g_n(z_1, z_2, \ldots, z_m),$$

il existe un exposant r tel que f^r s'exprime sous la forme

$$f^r = a_1 g_1 + a_2 g_2 + \cdots + a_r g_r,$$

$a_1, a_2, \ldots, a_r$ étant des fonctions rationnelles entières de $z_1, z_2, \ldots, z_m$; *si $F, F', F'', \ldots$ sont des fonctions rationnelles entières quelconques qui s'annulent pour ces mêmes systèmes de valeurs, il est possible de déterminer un entier r assez grand pour que le produit $\Pi^{(r)}$ de r quelconques des fonctions $F, F', F'', \ldots$ puisse être mis sous la forme

$$\Pi^{(r)} = a_1 g_1 + a_2 g_2 + \ldots + a_n g_n,$$

$a_1, a_2, \ldots, a_n$ étant des fonctions rationnelles entières de $z_1, \ldots, z_m$.* Ce théorème est de *D. Hilbert*[78]).

On remarquera que les théorèmes précédents de *M. Nöther*, *E. Netto* et *D. Hilbert* s'énoncent très simplement lorsqu'on fait usage de la notion de *systèmes de modules* ou *de diviseurs* dont il sera question dans l'article I 10.

74) *A. Voss*, Math. Ann. 27 (1886), p. 527; *M. Nöther*, id. 30 (1887), p. 410; id. 40 (1892), p. 140.*

75) *M. Nöther*, Math. Ann. 30 (1887), p. 410; *L. Stickelberger*, id. p. 401; *A. Brill*, id. 39 (1891), p. 129.*

76) Acta math. 7 (1885/6), p. 101.

77) Voir *J. J. Sylvester*, Cambr. Dublin math. J. 6 (1851), p. 186; Papers 1, Cambridge 1904, p. 184; *O. Hölder*, Math.-naturw. Mitt. Würtemb. 1 (1884/6), p. 60; *E. Netto*, Algebra [27]) 2, p. 24.

Les équations linéaires. Formes linéaires.

10. Équations linéaires. *On appelle *équation linéaire* à m inconnues une équation de la forme

$$\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_m x_m = \beta,$$

$\alpha_1, \alpha_2, \ldots, \alpha_m$ et β étant des constantes. On appelle *terme constant* de cette équation linéaire la constante β qui figure dans le second membre. Si $\beta = 0$, on dit que l'équation est *linéaire et homogène.*

Considérons d'abord un système de m équations linéaires à m inconnues, mises sous la forme

$$(1)\qquad \begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1m}x_m + b_1 = 0 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2m}x_m + b_2 = 0 \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mm}x_m + b_m = 0. \end{cases}$$

Lorsque le déterminant

$$A = \begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1m} \\ a_{21} & a_{22} & \ldots & a_{2m} \\ \cdot & \cdot & \cdot & \cdot \\ a_{m1} & a_{m2} & \ldots & a_{mm} \end{vmatrix}$$

est différent de zéro, il n'existe qu'un système de valeurs de $x_1, x_2, \ldots, x_m$ satisfaisant au système d'équations (1). Pour obtenir la valeur de x_h, il suffit de former une fraction dont le dénominateur est le déterminant A et dont le numérateur est le déterminant qu'on déduit de A en y remplaçant les éléments de la $h^{\text{ième}}$ colonne par les termes constants $-b_1, -b_2, \ldots, -b_m$ correspondants. C'est dans ce procédé que consiste la règle dite *règle de Cramer.* On a ainsi

$$(2)\qquad x_h = -\frac{A_{1h}b_1 + A_{2h}b_2 + \cdots + A_{mh}b_m}{A} \qquad (h = 1, 2, \ldots, m),$$

78) Math. Ann. 42 (1893), p. 320.

A_{ih} étant le coefficient de l'élément a_{ih} dans le développement

$$A = A_{1h}a_{1h} + A_{2h}a_{2h} + \cdots + A_{mh}a_{mh}$$

du déterminant A suivant les éléments de sa $h^{\text{ième}}$ colonne.*

*E. Bézout[79]) a donné une règle d'une application facile pour le calcul du déterminant A et des déterminants

$$B_h = -(A_{1h}b_1 + A_{2h}b_2 + \cdots + A_{mh}b_m), \qquad (h = 1, 2, \ldots, m).$$

Supposons que, dans les m équations (1), les termes $b_1, b_2, \ldots, b_m$ soient remplacés respectivement par $b_1x_{m+1}, b_2x_{m+1}, \ldots, b_mx_{m+1}$. Nous formerons alors un tableau de m lignes de la manière suivante:

Dans le produit

$$x_1x_2x_3 \ldots x_mx_{m+1}$$

remplaçons successivement chacune des $m+1$ inconnues $x_1, \ldots, x_m, x_{m+1}$ soit par le coefficient de cette inconnue dans la première des équations (1), soit par ce coefficient changé de signe, suivant que l'indice correspondant de x est un nombre impair ou pair. On obtient ainsi $m+1$ termes qui constituent la première ligne du tableau de *E. Bézout.* Chacun de ces $m+1$ termes est le produit de m des $m+1$ inconnues $x_1, x_2, \ldots, x_{m+1}$ par un certain coefficient; dans chacun de ces $m+1$ termes nous rangerons ces m inconnues par ordre d'indices *croissants* et nous conviendrons de dire qu'une quantité connue remplace une inconnue de *rang pair* quand l'inconnue que l'on remplace par la quantité connue est la seconde, la quatrième, la sixième, ... des m inconnues (rangées par ordre d'indice croissant) qui figurent effectivement dans le terme envisagé.

Nous remplacerons ensuite successivement, dans chacun des termes de la première ligne, chaque inconnue par le coefficient de cette inconnue figurant dans la seconde des équations (1) en changeant toutefois le signe du coefficient lorsque la quantité connue remplace une inconnue de rang pair. On obtient ainsi la seconde ligne du tableau de *E. Bézout.*

Chacun des termes de cette seconde ligne est un produit de $m-1$ des $m+1$ inconnues $x_1, x_2, \ldots, x_{m+1}$ par un coefficient. Au moyen des termes de cette seconde ligne on formera la troisième ligne du tableau de *E. Bézout* de la même façon que l'on a formé la seconde ligne à l'aide des termes de la première ligne. Et l'on continuera

79) *E. Bézout,* Equations alg.[18]), p. 172 (Texte et note de *J. Kürschák*).*

ainsi jusqu'à la $m^{\text{ième}}$ ligne dont les termes sont chacun le produit *d'une* des $m+1$ inconnues $x_1, x_2, \ldots, x_{m+1}$ par un coefficient.

Les coefficients de $x_1, x_2, \ldots, x_m, x_{m+1}$ dans cette dernière ligne seront respectivement égaux aux déterminants $B_1, B_2, \ldots, B_m, A$.

Soient, par exemple, les quatre équations

$$\begin{aligned} 2x_1 + 3x_2 - 8 &= 0 \\ 3x_1 + 2x_3 - 9 &= 0 \\ 4x_2 + 3x_4 - 20 &= 0 \\ 2x_3 + x_4 - 10 &= 0. \end{aligned}$$

La règle de *E. Bézout* donne successivement les quatre lignes que voici:

Première ligne:

$$2x_2x_3x_4x_5 - 3x_1x_3x_4x_5 - 8x_1x_2x_3x_4;$$

Seconde ligne:

$$-4x_2x_4x_5 + 18x_2x_3x_4 - 9x_3x_4x_5 + 6x_1x_4x_5 - 27x_1x_3x_4 \\ -24x_2x_3x_4 - 16x_1x_2x_4;$$

ou, si l'on veut,

$$-4x_2x_4x_5 - 6x_2x_3x_4 - 9x_3x_4x_5 + 6x_1x_4x_5 - 27x_1x_3x_4 - 16x_1x_2x_4;$$

Troisième ligne:

$$-16x_4x_5 + 12x_2x_5 + 80x_2x_4 - 24x_3x_4 - 18x_2x_3 + 27x_3x_5 + 180x_3x_4 \\ -18x_1x_5 - 120x_1x_4 - 81x_1x_3 + 64x_1x_4 - 48x_1x_2;$$

ou, si l'on veut,

$$-16x_4x_5 + 12x_2x_5 + 80x_2x_4 + 156x_3x_4 - 18x_2x_3 + 27x_3x_5 \\ -18x_1x_5 - 56x_1x_4 - 81x_1x_3 - 48x_1x_2;$$

Quatrième ligne:

$$38x_1 + 76x_2 + 114x_3 + 152x_4 + 38x_5.$$

On a donc

$$B_1 = 38, \quad B_2 = 76, \quad B_3 = 114, \quad B_4 = 152, \quad A = 38$$

en sorte que

$$x_1 = \frac{38}{38} = 1, \quad x_2 = \frac{76}{38} = 2, \quad x_3 = \frac{114}{38} = 3, \quad x_4 = \frac{152}{38} = 4.*$$

11. Équations linéaires homogènes. Envisageons maintenant le système de k équations linéaires *et homogènes,* à m inconnues,

$$(3) \qquad a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{ih}x_h + \cdots + a_{im}x_m = 0, \\ (i = 1, 2, \ldots, k).$$

Considérons le tableau

$$(T) = \begin{cases} a_{11}\, a_{12} \,\ldots\, a_{1m} \\ a_{21}\, a_{22} \,\ldots\, a_{2m} \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ a_{k1}\, a_{k2} \,\ldots\, a_{km} \end{cases}$$

formé par les coefficients des inconnues. On appelle *déterminant principal* un déterminant déduit du tableau (T), différent de zéro, et tel que tous les déterminants de degré supérieur déduits du tableau (T) soient nuls; le degré r de ce déterminant est le *rang* (I 2, **26**) du tableau ou de la *matrice* (T). On peut d'ailleurs toujours ranger les équations et les inconnues dans un ordre tel que le déterminant

$$D = \begin{vmatrix} a_{11}\, a_{12} \,\ldots\, a_{1r} \\ a_{21}\, a_{22} \,\ldots\, a_{2r} \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ a_{r1}\, a_{r2} \,\ldots\, a_{rr} \end{vmatrix}$$

soit un déterminant principal.

Si $r = m$, il n'existe qu'une solution du système d'équations (3); c'est la solution

$$x_1 = x_2 = \cdots = x_m = 0.$$

Si $r < m$, on peut donner à $x_{r+1}, x_{r+2}, \ldots, x_m$ des valeurs arbitraires, $x'_{r+1}, x'_{r+2}, \ldots, x'_m$; alors $x_1, x_2, \ldots, x_r$ sont déterminés en fonctions de $x'_{r+1}, x'_{r+2}, \ldots, x'_m$. On dit dans ce cas que le système $(x_1, x_2, \ldots, x_r)$ admet ∞^{m-r} solutions; c'est aussi le nombre de solutions du système d'équations (3).

Si le système (3) admet deux solutions

$$(x_1', x_2', \ldots, x_m'), \quad (x_1'', x_2'', \ldots, x_m'')$$

il admet aussi la solution

$$(\lambda x_1' + \mu x_1'', \lambda x_2' + \mu x_2'', \ldots, \lambda x_m' + \mu x_m'')$$

quelles que soient les valeurs données à λ et à μ.

On dit de plusieurs solutions

$$(x_1', x_2', \ldots, x_m'), (x_1'', x_2'', \ldots, x_m''), \ldots, (x_1^{(h)}, x_2^{(h)}, \ldots, x_m^{(h)})$$

qu'elles sont *indépendantes* lorsqu'il n'existe aucun système de nombres $\mu_1, \mu_2, \ldots, \mu_h$ autres que $\mu_1 = 0,\ \mu_2 = 0, \ldots, \mu_h = 0$ pour lesquels les m équations

$$\mu_1 x_i' + \mu_2 x_i'' + \cdots + \mu_h x_i^{(h)} = 0, \qquad (i = 1, 2, \ldots, m)$$

soient satisfaites.

Désignons par k le rang de la matrice (T). Si k est plus petit que m, on peut déterminer, d'une infinité de manières, $m-k$ solutions

indépendantes du système d'équations (3); et si par un procédé quelconque on détermine $m-k+1$ solutions du système d'équations (3), ces solutions ne peuvent être indépendantes.

Si

$$(x_1', x_2', \ldots, x_m'), (x_1'', x_2'', \ldots, x_m''), \ldots, (x_1^{(m-k)}, x_2^{(m-k)}, \ldots, x_m^{(m-k)})$$

désignent $m-k$ solutions indépendantes quelconques du système (3), toute solution de ce système (3) est donnée par les formules

$$\begin{aligned} x_1 &= \mu_1 x_1' + \mu_2 x_1'' + \cdots + \mu_{m-k} x_1^{(m-k)} \\ x_2 &= \mu_1 x_2' + \mu_2 x_2'' + \cdots + \mu_{m-k} x_2^{(m-k)} \\ &\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ x_m &= \mu_1 x_m' + \mu_2 x_m'' + \cdots + \mu_{m-k} x_m^{(m-k)} \end{aligned}$$

et l'on obtient chaque solution une et une seule fois en remplaçant $\mu_1, \mu_2, \ldots, \mu_{m-k}$ par tous les systèmes de nombres possibles.

*Pour obtenir *un* système de $m-k$ solutions indépendantes du système d'équations (3) on peut appliquer la règle suivante due à *G. Frobenius*[80]):

Choisissons arbitrairement des constantes

$$\begin{matrix} u_1', u_1'', \ldots, u_1^{(m-k)} \\ u_2', u_2'', \ldots, u_2^{(m-k)} \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ u_m', u_m'', \ldots, u_m^{(m-k)} \end{matrix}$$

de façon que le déterminant

$$\Delta = \begin{vmatrix} a_{11}, & a_{12}, & \ldots, a_{1m} \\ \cdot & \cdot & \cdot \\ a_{k1}, & a_{k2}, & \ldots, a_{km} \\ u_1', & u_2', & \ldots, u_m' \\ \cdot & \cdot & \cdot \\ u_1^{(m-k)}, & u_2^{(m-k)}, & \ldots, u_m^{(m-k)} \end{vmatrix}$$

soit différent de zéro [ce qui, si k est le rang de la matrice (T), est toujours possible]. Soit alors pour $h = 1, 2, \ldots, m$ et pour $i = 1, 2, \ldots, m-k$

$$x_h^{(i)}$$

le mineur de Δ correspondant à l'élément $u_h^{(i)}$. Les $(m-k)$ solutions

$$(x_1', x_2', \ldots, x_m'), (x_1'', x_2'', \ldots, x_m''), \ldots, (x_1^{(m-k)}, x_2^{(m-k)}, \ldots, x_m^{(m-k)})$$

du système d'équations (3) forment un système de $(m-k)$ solutions *indépendantes* de ce système d'équations (3).*

---

80) **G. Frobenius*, J. reine angew. Math. 82 (1877), p. 236.*

12. Théorie générale des équations linéaires. Soit enfin un système d'équations linéaires *non homogènes,*

$$(4)\qquad a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{im}x_m + b_i = 0 \qquad (i = 1, 2, \ldots, k).$$

Considérons les tableaux[81])

$$(T) = \begin{cases} a_{11} & a_{12} & \ldots & a_{1m} \\ a_{21} & a_{22} & \ldots & a_{2m} \\ . & . & . & . \\ a_{k1} & a_{k2} & \ldots & a_{km} \end{cases} \quad \text{et} \quad (T') = \begin{cases} a_{11} & a_{12} & \ldots & a_{1m} & b_1 \\ a_{21} & a_{22} & \ldots & a_{2m} & b_2 \\ . & . & . & . & . \\ a_{k1} & a_{k2} & \ldots & a_{km} & b_k. \end{cases}$$

Soit toujours

$$D = \begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1r} \\ a_{21} & a_{22} & \ldots & a_{2r} \\ . & . & . & . \\ a_{r1} & a_{r2} & \ldots & a_{rr} \end{vmatrix}$$

un déterminant principal déduit du tableau (T). Appelons déterminant *caractéristique* relatif à D un déterminant tel que

$$\Delta_{r+h} = \begin{vmatrix} a_{11} & \ldots & a_{1r} & b_1 \\ . & . & . & . \\ a_{r1} & \ldots & a_{rr} & b_r \\ a_{r+h,1} & \ldots & a_{r+h,r} & b_{r+h} \end{vmatrix},$$

où h est un des nombres $1, 2, \ldots, k-r$. Si les $(k-r)$ déterminants caractéristiques $\Delta_{r+1}, \Delta_{r+2}, \ldots, \Delta_k$ ne sont pas tous nuls, les équations (4) n'ont pas de solution; on dit alors qu'elles sont *incompatibles.*

Au contraire, si les déterminants caractéristiques $\Delta_{r+1}, \Delta_{r+2}, \ldots, \Delta_k$ sont tous nuls, les équations (4) sont *compatibles.* On peut alors donner à $x_{r+1}, x_{r+2}, \ldots, x_m$ des valeurs arbitraires $x'_{r+1}, x'_{r+2}, \ldots, x'_m$ et $x_1, x_2, \ldots, x_r$ sont déterminés en fonction de $x'_{r+1}, x'_{r+2}, \ldots, x'_m$ en sorte que l'on peut dire que le système $(x_1, x_2, \ldots, x_r)$ admet ∞^{m-r} solutions; c'est aussi le nombre de solutions du système d'équations (4).

Les $(k-r)$ dernières équations (4) sont dites *conséquences* des r premières.

On peut ajouter que les conditions pour que les équations (4) soient compatibles sont les mêmes que celles qui expriment que les tableaux (T) et (T') ont le même rang[82]).

81) *Cf. *E. Rouché,* C. R. Acad. sc. Paris 81 (1875), p. 1050; voir aussi *G. Fontené,* Nouv. Ann. math. (3) 19 (1900), p. 188.*

82) *Voir *A. Capelli,* Rivista mat. 2 (1892), p. 54/8; Istituzioni di analisi algebrica, Naples 1902, p. 196 (Note de *G. Vivanti*).*

13. Formes linéaires. *Rappelons qu'une *forme linéaire* est une fonction rationnelle entière, homogène et du premier degré, telle que

$$a_1x_1 + a_2x_2 + \cdots + a_mx_m;$$

$a_1, a_2, \ldots, a_m$ sont les *coefficients,* $x_1, x_2, \ldots, x_m$ sont les *variables* de la forme linéaire. On sait (n° **2**) que la forme est *identiquement nulle* si l'on a

$$a_1 = 0,\ a_2 = 0,\ \ldots,\ a_m = 0.$$

Considérons k formes linéaires à m variables,

$$f_i = a_{1i}x_1 + a_{2i}x_2 + \cdots + a_{mi}x_m \qquad (i = 1, 2, \ldots, k).$$

Ces k formes $f_1, f_2, \ldots, f_k$ sont dites *linéairement indépendantes* si l'*identité*

$$\lambda_1 f_1 + \lambda_2 f_2 + \cdots + \lambda_k f_k = 0$$

ne peut avoir lieu que pour

$$\lambda_1 = \lambda_2 = \cdots = \lambda_k = 0.$$

Il faut et il suffit pour cela que si l'on déduit un déterminant principal du tableau des coefficients des formes envisagées, ce déterminant soit de degré k en sorte que le tableau lui-même soit de *rang* k.

Si ce déterminant principal est de degré $r < k$, supposons que ce soit

$$D = \begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1r} \\ a_{21} & a_{22} & \ldots & a_{2r} \\ . & . & . & . \\ a_{r1} & a_{r2} & \ldots & a_{rr} \end{vmatrix};$$

les formes $f_1, f_2, \ldots, f_r$ sont alors linéairement indépendantes, et les autres formes $f_{r+1}, f_{r+2}, \ldots, f_k$ sont exprimées au moyen de celles-là par les formules

$$f_{r+h} = \lambda_{r+h,1}f_1 + \lambda_{r+h,2}f_2 + \cdots + \lambda_{r+h,r}f_r \qquad (h = 1, 2, \ldots, k-r),$$

où les coefficients λ désignent des fonctions rationnelles des coefficients a_{ij} qui figurent dans les formes $f_1, f_2, \ldots, f_k$. On dit alors que le *système de formes* $f_1, f_2, \ldots, f_k$ *est de rang* r et aussi que le *système d'équations*

$$f_1 = 0,\ f_2 = 0,\ \ldots,\ f_k = 0$$

est de rang r.

Pour que des formes linéaires puissent prendre des valeurs arbitrairement données, il faut et il suffit qu'elles soient linéairement indépendantes.

Si des formes linéaires $f_1, f_2, \ldots, f_k$ sont des fonctions linéaires et homogènes (à coefficients constants) d'un nombre moindre de formes linéaires, $\varphi_1, \varphi_2, \ldots, \varphi_q$ $(q < k)$, elles ne sont pas linéairement indépendantes. Si les formes $\varphi_1, \varphi_2, \ldots, \varphi_q$ sont linéairement indépendantes et si le système de formes $(f_1, f_2, \ldots, f_k)$ est de rang q quand on prend pour variables $\varphi_1, \varphi_2, \ldots, \varphi_q$, il est aussi de rang q quand on prend pour variables $x_1, x_2, \ldots, x_m$; dans tous les cas le rang du système $(f_1, f_2, \ldots, f_k)$ n'est jamais plus grand que q. Si, $\varphi_1, \varphi_2, \ldots, \varphi_q$ étant des formes linéairement indépendantes, toutes les solutions du système d'équations $\varphi_1 = 0, \varphi_2 = 0, \ldots, \varphi_q = 0$ vérifient les équations $f_1 = 0, f_2 = 0, \ldots, f_k = 0$, les formes $f_1, f_2, \ldots, f_k$ sont des fonctions linéaires et homogènes (à coefficients constants) des formes $\varphi_1, \varphi_2, \ldots, \varphi_q$.

Lorsque deux systèmes de formes linéaires dépendant des mêmes variables sont tels que chaque forme de l'un des systèmes soit une fonction linéaire et homogène (à coefficients constants) des formes de l'autre système, ces deux systèmes de formes sont dits *équivalents*.*

14. Propriétés des systèmes d'équations linéaires. *Nombreuses sont les propriétés des équations linéaires; la plupart peuvent être interprétées dans le domaine de la Géométrie à m dimensions[83]). Parmi ces propriétés nous citerons les suivantes.

Soit

$$(1)\qquad \begin{cases} \xi_{11}x_1 \quad + \cdots + \xi_{1m}x_m \quad = 0 \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ \xi_{m-r,1}x_1 + \cdots + \xi_{m-r,m}x_m = 0 \end{cases}$$

un système de $m - r$ équations linéaires et homogènes. Si les premiers membres sont des formes indépendantes, à m variables $x_1, x_2, \ldots, x_m$, on dit que les $(m - r)$ équations (1) sont indépendantes. Soient $(x_{11}, \ldots, x_{1m}), \ldots, (x_{r1}, \ldots, x_{rm})$ r solutions *indépendantes* (nº **11**) du système (1).

Désignons par $a, \ldots, b, c, \ldots, d$ une permutation quelconque des nombres $1, 2, \ldots, m$; soit ω le nombre des inversions de cette permutation. La suite $a \ldots b$ contient r nombres et l'on pose

$$x_{a \ldots b} = \begin{vmatrix} x_{1a} & \cdots & x_{1b} \\ \cdot & \cdot\ \cdot & \cdot \\ x_{ra} & \cdots & x_{rb} \end{vmatrix};$$

la suite $c \ldots d$ contient $m - r$ nombres et l'on pose

$$\xi_{c \ldots d} = \begin{vmatrix} \xi_{1c} & \cdots & \xi_{1d} \\ \cdot & \cdot\ \cdot & \cdot \\ \xi_{m-r,c} & \cdots & \xi_{m-r,d} \end{vmatrix}.*$$

83) *C. Jordan*, Bull. Soc. math. France 3 (1874/5), p. 103.*

*Ceci posé, on a cette propriété que les $m!$ expressions

$$(-1)^{\omega} \frac{x_{a \ldots b}}{\xi_{c \ldots d}}$$

sont deux à deux égales entre elles[84]).

Soit maintenant

$$(2)\qquad \begin{cases} \eta_{11}x_1 \quad + \cdots + \eta_{1m}x_m \quad = 0 \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ \eta_{m-r',1}x_1 + \cdots + \eta_{m-r',m}x_m = 0 \end{cases}$$

un autre système de $m - r'$ équations indépendantes avec les mêmes inconnues $x_1, x_2, \ldots, x_m$. Si le nombre entier $r + r' - m$ est positif ou nul et si en outre aucune équation de l'un des systèmes n'est une conséquence des équations de l'autre système, les deux systèmes admettront $\infty^{r+r'-m}$ solutions communes. La condition pour qu'ils en aient un plus grand nombre, c'est-à-dire pour que les deux systèmes admettent ∞^k solutions communes, où k est un nombre naturel donné supérieur à $r + r' - m$, est que quelques-unes des équations de l'un des systèmes soient des conséquences des équations de l'autre système. Tous les déterminants d'ordre $m - k + 1$ extraits du tableau

$$\begin{matrix} \xi_{11} & \xi_{12} & \cdots & \xi_{1m} \\ \cdot & \cdot & \cdot & \cdot \\ \eta_{11} & \eta_{12} & \cdots & \eta_{1m} \\ \cdot & \cdot & \cdot & \cdot \end{matrix}$$

seront alors nuls. Les

$$C_m^{m-k+1} C_{2m-r-r'}^{m-k+1}$$

conditions que l'on trouve ainsi se réduisent à

$$k(m + k - r - r')$$

conditions indépendantes.

Le nombre k des solutions communes indépendantes est au plus égal au plus petit des deux nombres r, r' qui expriment respectivement le nombre des solutions indépendantes des systèmes (1) et (2). Si, en particulier, on suppose $r' \leqq r$ et si toutes les solutions du système (2) sont solutions du système (1) on a $k = r'$; le nombre des conditions indépendantes est alors égal à $r'(m - r)$.

Si $r' = r$ et si les conditions précédentes sont remplies, les deux systèmes sont équivalents. Le nombre des conditions pour qu'il en

84) *Cf. *A. Brill*, Math. Ann. 4 (1871), p. 530; *A. Clebsch*, Math. Ann. 5 (1872), p. 429; Abh. Ges. Gött. 17 (1872), math. mém. nº 1, § 2; *E. d'Ovidio*, Atti Accad. Torino 12 (1876/7), p. 334; *G. Frobenius*, J. reine angew. Math. 82 (1877), p. 236; *K. Bes*, Théorie générale de l'élimination, Verhand. Akad. Wetensch. Amsterdam Afdeeling Natuurkunde erste Sectie (2) 6 (1897/9), mém. nº 7, § 24.*

soit ainsi est alors $r(m-r)$. C'est ce nombre que *A. Clebsch* appelle[85]) le *poids* du système des $(m-r)$ équations (1).*

*Comme l'a montré *E. d'Ovidio*[84]), les conditions précédentes pour que les systèmes (1) et (2) aient ∞^k solutions communes (où $k > r + r' - m$) s'écrivent aussi de la façon suivante:

Prenons $m + k - r - r' - 1$ indices parmi les indices $1, 2, \ldots, m$ (soient $a \ldots b$), puis prenons $r' - k + 1$ indices parmi ceux qui restent (soient $c \ldots d$); puis enfin prenons $r - k + 1$ indices parmi ceux qui restent (soient $e \ldots f$). Alors les conditions cherchées seront

$$(3) \qquad \sum_{c\ldots de\ldots f} (-1)^{\omega} \xi_{a\ldots bc\ldots d}\, \eta_{a\ldots be\ldots f} = 0,$$

où

$$\xi_{a\ldots bc\ldots d} = \begin{vmatrix} \xi_{1a} & \cdots & \xi_{1b} & \xi_{1c} & \cdots & \xi_{1d} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \xi_{m-r,a} & \cdots & \xi_{m-r,b} & \xi_{m-r,c} & \cdots & \xi_{m-r,d} \end{vmatrix},$$

$$\eta_{a\ldots be\ldots f} = \begin{vmatrix} \eta_{1a} & \cdots & \eta_{1b} & \eta_{1e} & \cdots & \eta_{1f} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \eta_{m-r',a} & \cdots & \eta_{m-r',b} & \eta_{m-r',e} & \cdots & \eta_{m-r',f} \end{vmatrix}$$

et où le signe Σ de sommation s'étend à tous les termes que l'on obtient en laissant le groupe $a \ldots b$ fixe tandis que $c \ldots de \ldots f$ varient d'un terme à l'autre, de façon que $c \ldots de \ldots f$ coïncide successivement avec toutes les permutations d'un *même* groupe de $r + r' - 2(k-1)$ indices pris parmi $1, 2, \ldots, m$ autres que $a \ldots b$. Quant à ω, c'est le nombre des inversions de la permutation $c \ldots de \ldots f$.

Pour exprimer que les systèmes (1) et (2) sont équivalents, on a des relations de la forme

$$(4) \qquad \xi_{a\ldots bc}\, \eta_{a\ldots be} - \xi_{a\ldots be}\, \eta_{a\ldots bc} = 0,$$

où les indices $a \ldots b$ sont en nombre $m - r - 1$.

Toujours dans le cas où $r = r'$ et en supposant les systèmes équivalents, écrivons les relations (3) en y faisant $k = r - 1$; on a alors

$$\sum_{cdef} (-1)^{\omega} \xi_{a\ldots bcd}\, \eta_{a\ldots bef} = 0,$$

où le groupe $a \ldots b$ contient $m - r - 2$ indices; ceci posé éliminons les η au moyen des relations (4); en disposant des indices c, d, e, f de façon convenable, on obtient la relation

$$(5) \qquad \xi_{a\ldots bcd}\, \xi_{a\ldots bef} + \xi_{a\ldots bce}\, \xi_{a\ldots bfd} + \xi_{a\ldots bcf}\, \xi_{a\ldots bde} = 0.*$$

85) **A. Clebsch*, Abh. Ges. Gött. 17 (1872), math., mém. n° 1. p. 5.*

*Si

$$(x_{11}, x_{12}, \ldots, x_{1m}), \ldots, (x_{r1}, x_{r2}, \ldots, x_{rm})$$

sont r solutions indépendantes du système (1) et si

$$(y_{11}, y_{12}, \ldots, y_{1m}), \ldots, (y_{r'1}, y_{r'2}, \ldots, y_{r'm})$$

sont r' solutions indépendantes du système (2), on peut donner une autre forme aux conditions (4) et (5) en faisant intervenir les x_{ik} et et les y_{ik}.

Il est clair que le système d'équations

$$(1') \qquad \begin{cases} x_{11}\,\xi_1 + \cdots + x_{1m}\,\xi_m = 0 \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ x_{r1}\,\xi_1 + \cdots + x_{r,m}\,\xi_m = 0, \end{cases}$$

où $\xi_1, \ldots, \xi_m$ sont les inconnues, a le rang r et que le système d'équations

$$(2') \qquad \begin{cases} y_{11}\,\xi_1 + \cdots + y_{1m}\,\xi_m = 0 \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ y_{r'1}\,\xi_1 + \cdots + y_{r'm}\,\xi_m = 0 \end{cases}$$

a le rang r'; mais le système composé de (1′) et de (2′) n'a que le rang $r + r' - k$.

Les conditions (3) deviennent donc

$$(3') \qquad \sum_{c\ldots de\ldots f} (-1)^{\omega} x_{a\ldots bc\ldots d}\, y_{a\ldots be\ldots f} = 0$$

mais cette fois les indices $a \ldots b$ sont en nombre $k-1$, les indices $c \ldots d$ en nombre $r - k + 1$, les indices $e \ldots f$ en nombre $r' - k + 1$; le signe de sommation Σ s'étend à toutes les permutations d'un *même* groupe de $r + r' - 2(k-1)$ indices pris parmi les indices $1, 2, \ldots, m$ autres que $a \ldots b$; enfin ω est le nombre des inversions de la permutation $c \ldots de \ldots f$.

Les relations (5) deviennent

$$(5') \qquad x_{a\ldots bcd} \cdot x_{a\ldots bef} + x_{a\ldots bce} \cdot x_{a\ldots bfd} + x_{a\ldots bcf} \cdot x_{a\ldots bde} = 0$$

où le nombre des indices $a \ldots b$ est $r - 2$.*

15. Historique. *Les mathématiciens de l'antiquité et du moyen âge ont parfois résolu des systèmes d'équations linéaires à plus d'une inconnue; mais le but qu'ils se proposaient d'atteindre était toujours de trouver les *valeurs numériques* des inconnues et non la *forme* des expressions fournissant ces inconnues au moyen des coefficients; ils n'ont même jamais cherché à donner un procédé régulier permettant de calculer *méthodiquement* les inconnues. On peut citer comme tout à fait exceptionnelles les indications données par le pythagoricien

Thymaridas[86]) sur la forme des valeurs des inconnues dans un cas très spécial, celui où quelques uns des coefficients des inconnues étant égaux à 1, les autres sont tous nuls.

Ce n'est qu'au 16ième siècle qu'on a proposé des *méthodes* d'élimination des inconnues dans le cas de plusieurs équations linéaires à plusieurs inconnues. Les premiers pas dans cette voie ont été faits par *J. Butéon*[87]); *G. Gosselin* a d'ailleurs amélioré le procédé de *J. Butéon*, tout en se servant comme lui de la *méthode d'addition*.

Les mathématiciens du 17ième siècle se sont peu occupés de cette question[88]). *M. Rolle*[89]) a toutefois enseigné la *méthode de substitution* et la *méthode de combinaison*; en passant il mentionne aussi la *méthode d'addition et de soustraction*. *I. Newton*[90]) indique la *méthode d'addition*, la *méthode de combinaison* et, dans le cas d'équations n'étant pas toutes linéaires, la *méthode de substitution*[91]). Dans „l'Analyse démontrée" de *Ch. R. Reyneau*[92]) les trois méthodes sont enseignées pour des équations linéaires à plusieurs inconnues et elles le sont dans l'ordre suivant:

1) méthode de substitution;
2) méthode de combinaison;
3) méthode d'addition.

L'emploi de *multiplicateurs indéterminés* n'était point inconnu des géomètres de la fin du 17ième et du commencement du 18ième siècle[93]), mais la *méthode des coefficients indéterminés* pour résoudre les équations linéaires est due à *E. Bézout*[94]).*

---

86) **Iamblichus* in Nichomachi arith. introd. liber, éd. *H. Pistelli*, Leipzig 1894, p 62, 68. Voir aussi *M. Cantor*, Vorles. Gesch. Math. (2e éd.) 1, Leipzig 1894, p. 147/8.*

87) **J. Butéon*, Logistica, Lyon 1559, p. 193/6; *G. Gosselin*, De arte magna, Paris 1577, fol. 79b/85b.*

88) **J. Prestet* n'en parle ni dans ses „Elémens de math.", Paris 1675, ni dans ses „Nouveaux élémens de math.", Paris 1689.*

89) *Traité d'Algèbre, Paris 1690, p. 42/55.*

90) *Arithmetica universalis, rédigée vers 1685, publiée seulement à Cambridge en 1707.*

91) *Arithm. univ.[90]), Leyde 1732, p. 57/60; Opera, éd. *S. Horsley* 1, Londres 1779, p. 60/2; trad. *N. Beaudeux* 1, Paris an X, p. 78/82.

92) *Analyse démontrée ou la méthode de résoudre les problèmes des math. 1, Paris 1708, p. 14/6. Cet ouvrage a été achevé *avant* la publication de l'Arithmétique universelle de *I. Newton.**

93) *Voir par ex. Bibl. math. (2) 12 (1898), p. 58/60; (3) 6 (1905), p. 59/61 (Texte et notes 86 à 94 de *G. Eneström*).*

94) *Cours de math. à l'usage des gardes du pavillon et de la marine, et Cours de math. à l'usage du corps de l'artillerie, Paris 1764/7; (nouv. éd.) à l'usage

**G. W. Leibniz*[95]) est le premier qui ait cherché à obtenir des expressions symétriques des inconnues au moyen des coefficients. Il a été suivi par *G. Cramer*[96]), *A. T. Vandermonde*[97]) et *P. S. Laplace*[98]).*

16. Énumération de mémoires qui traitent des équations linéaires. *C. G. J. Jacobi*[99]), *A. L. Cauchy*[100]), et *H. Grassmann*[101]) étudient le cas général.

G. Frobenius introduit et utilise[102]) la notion de *rang* d'un tableau de pq grandeurs. *L. Kronecker*[103]) montre toute l'importance de cette notion de rang.

J. J. Sylvester[104]) dit d'un déterminant du $n^{\text{ième}}$ degré qu'il est un déterminant de nullité i (of nullity i), lorsque tous les mineurs du $(n-i+1)^{\text{ième}}$ degré sont nuls, mais non tous ceux du $(n-i)^{\text{ième}}$ degré.

Pour une exposition de la théorie des équations linéaires, on peut consulter *H. R. Baltzer*[105]); pour le cas des équations linéaires et homogènes, on consultera surtout *P. Gordan*[106]) et *H. Weber*[107]).

**J. D. Gergonne*[108]) expose en la complétant la théorie de *P. S. Laplace*. Citons aussi *L. H. F. X. Molins*[109]), *P. A. Hansen*[110]) et *V. von Lichtenfels*[111]).*

---

des gardes 3, Paris an VI, p. 86/9; (nouv. éd.) à l'usage de l'artillerie 2, Paris an VIII, p. 75/7.*

95) Ms. bibl. Hanovre de 1678; lettre à *G. F. A. de l'Hospital* datée du 28 avril 1693; Acta Erud. Lps. 1700, p. 206; Werke éd. *C. I. Gerhardt*, Math. Schr. 2, Berlin 1850, p. 239; 5, Halle 1858, p. 348; 7, Halle 1863, p. 5.

96) Introd.[31]), p. 657.

97) Hist. Acad. sc. Paris, 1772 II M. p. 516.

98) Hist. Acad. sc. Paris 1772 II M. p. 294; Œuvres 8, Paris 1891, p. 396.

99) J. reine angew. Math. 22 (1841), p. 285; Werke 3, Berlin 1884, p. 357.

100) Cours d'Analyse de l'Ecole polyt. 1; Analyse algébrique, Paris 1821, p. 77; Œuvres (2) 3, Paris 1897, p. 76.

101) Die lineale Ausdehnungslehre, Leipzig 1844; (2e éd.) Leipzig 1878, p. 71; Werke 1[1], Leipzig 1894, p. 100.

102) J. reine angew. Math. 86 (1879), p. 1.

103) Sitzgsb. Akad. Berlin 1884, p. 1071, 1179; Werke 3[1], Leipzig 1899, p. 33, 49.

104) Amer. J. math. 6 (1884), p. 274.

105) Theorie und Anwendungen der Determinanten, Leipzig 1857; (5e éd.) Leipzig 1881, p. 70; trad. *G. J. Hoüel*, Paris 1861, p. 64.

106) Vorlesungen über Invariantentheorie, publ. par *G. Kerschensteiner* 1, Leipzig 1885, p. 101.

107) Alg.[24]) 1, p. 96, 100; trad. *J. Griess* 1, p. 100, 106; pour les équations linéaires non homogènes voir Alg.[24]) 1, p. 104; trad. *J. Griess* 1, p. 109.

108) *Ann. math. pures appl. 4 (1813/4), p. 148/56. Les anciennes méthodes sont exposées avec détail dans plusieurs mémoires du même journal; voir en partic. *G. M. Raymond* 2 (1811/2), p. 38.*

$_*$J. Versluys[112]), *V. Valeriani*[113]), *E. Rouché*[114]), *Ch. Biehler*[115]) *G. Garbieri*[116]) donnent des discussions complètes d'un système général d'équations linéaires.

Ch. Méray[117]) précise certains points de la discussion générale. Il montre[118]) les avantages qu'il y a à fonder la théorie des déterminants sur celle des formes linéaires. De même *B. I. Clasen*[119]) résout les équations linéaires sans faire usage des déterminants, et utilise au contraire sa méthode pour le calcul des déterminants.

A. Capelli[120]) démontre les avantages didactiques de la notion du rang d'une matrice (qu'il appelle la caractéristique de la matrice).

F. J. Studnička[121]) expose systématiquement la théorie générale.

W. Veltmann[122]) montre comment on peut réduire tout système à un *système triangulaire*.

Citons encore *A. Auric*[123]) qui a fait une thèse sur la théorie d'un nombre infini d'équations linéaires à un nombre infini d'inconnues avec applications (cf. I 4, **39**), et *L. G. Gascó*[124]).

En ce qui concerne les systèmes d'équations linéaires spéciaux, nous citerons un peu au hasard les auteurs suivants:

A. Bonolis[125]) résout un système spécial se présentant dans certains problèmes de mécanique.*

109) $_*$J. math. pures appl. (1) 4 (1839), p. 509.*

110) $_*$Ber. Ges. Lpz. 1 (1846/7), math. p. 333; Abh. Ges. Lpz. (math.) 1 (1852), p. 85.*

111) $_*$Sitzgsb. Akad. Wien (math.-naturw.) 12 (1854), p. 935.*

112) $_*$Archiv Math. Phys. (1) 52 (1871), p. 257.*

113) $_*$Giorn. mat. (1) 9 (1871), p. 371.*

114) $_*$C. R. Acad. sc. Paris 81 (1875), p. 1050; J. Ec. polyt. (1) cah. 48 (1880), p. 221. Voir aussi *E. Amigues,* Nouv. Ann. math. (3) 11 (1892), p. 47.*

115) $_*$Nouv. Ann. math. (2) 19 (1880), p. 311, 356. On peut aussi citer une note de *G. Fontené,* Nouv. Ann. math. (2) 14 (1875), p. 481.*

116) $_*$Giorn. mat. (1) 30 (1892), p. 41/105.*

117) $_*$C. R. Acad. sc. Paris 81 (1875), p. 1203.*

118) $_*$J. math. pures appl. (3) 10 (1884), p. 181/281.*

119) $_*$Ann. Soc. scient. Bruxelles 12² (1887/8), p. 251; Mathesis (1) 9 (1889), suppl. n° 2, p. 1; voir aussi le rapport de *P. Mansion,* id. suppl. n° 2, p. 32; Ann. Soc. scient. Bruxelles 12¹ (1887/8), p. 50.*

120) $_*$Rivista mat. 2 (1892), p. 54.*

121) $_*$Časopis math. fys. (Prague) 6 (1877), p. 49, 97, 202 voir encore *Ed. Weyr* id. 14 (1885), p. 101.*

122) $_*$Z. Math. Phys. 31 (1886), p. 257, 272.*

123) $_*$Thèse, Grenoble (éd. Paris) 1893. *J. Collet* [Ann. Enseign. sup. Grenoble 5 (1893), p. 351] en a fait l'analyse.*

124) $_*$Archivo de mat. (Valence) 2 (1897/9), p. 124.*

125) $_*$Giorn. mat. (1) 11 (1873), p. 38.*

$_*$*P. Gordan*[126]) considère un système de s équations linéaires et homogènes à r inconnues dont les coefficients sont réels; il cherche à quelle condition le système pourra être vérifié par des valeurs *positives* de toutes les inconnues. Il cherche aussi, en supposant la condition remplie, et les coefficients entiers, quelle est la solution la plus simple en nombres entiers.

F. Unferdinger[127]) donne une nouvelle solution simple du système d'équations

$$\sum_{r=1}^{m} x_r \sin\left(\frac{rn\pi}{m+1}\right) = k_n \qquad (n = 1, 2, \ldots, m),$$

dont s'étaient déjà occupés *J. L. Lagrange*[128]) et *A. L. Crelle*[129]).

S. Günther[130]) envisage les équations

$$a_{1,\mu}x_1 + a_{2,\mu}x_2 + \cdots + a_{2n,\mu}x_{2n} = k_\mu \qquad (\mu = 1, 2, \ldots, 2n),$$

où pour $\lambda = 1, 2, \cdots, n$ et $\mu = 1, 2, \cdots, 2n$ on a

$$a_{\lambda,\mu} + (-1)^\mu a_{2n-\lambda,\mu} = 0.$$

E. Jürgens[131]) étudie le cas où dans le déterminant des coefficients des inconnues les termes de la diagonale principale sont tous positifs, les autres étant très petits. *J. Liouville*[132]) résout le système d'équations

$$\begin{aligned} \frac{x}{A-a} + \frac{y}{A-b} + \frac{z}{A-c} + \cdots &= 1, \\ \frac{x}{B-a} + \frac{y}{B-b} + \frac{z}{B-c} + \cdots &= 1, \\ \frac{x}{C-a} + \frac{y}{C-b} + \frac{z}{C-c} + \cdots &= 1, \\ \cdots\cdots\cdots\cdots\cdots& \end{aligned}$$

Citons encore *L. de Maio*[133]), *G. Bianchi*[134]), *G. Papelier*[135]),

126) $_*$Math. Ann. 6 (1873), p. 23.*

127) $_*$Archiv Math. Phys. (1) 56 (1874), p. 105.*

128) $_*$Misc. Taurinensia 1 (1759), math. p. 34; Œuvres 1, Paris 1867, p. 81.*

129) $_*$J. reine angew. Math. 43 (1852), p. 37.*

130) $_*$Archiv Math. Phys. (1) 57 (1875), p. 240.*

131) $_*$Zur Auflösung linearer Gleichungssysteme, Festschrift, Aix la Chapelle 1886.*

132) $_*$J. math. pures appl. (1) 11 (1846), p. 466; Archiv Math. Phys. (1) 22 (1854), p. 226. Voir aussi *Ubbo H. Meyer,* Archiv Math. Phys. (1) 12 (1849), p. 336/64.*

133) $_*$Memorie Accad. sc. dal 1852 in avanti (Naples) 1 (1852/4), éd. 1856, p. 101 (Note de *G. Vivanti*).*

134) $_*$Mem. mat. fis. Soc. ital. delle scienze (1) 22 (1839), p. 184 (Note de *G. Vivanti*).*

135) $_*$Revue math. spéc. 4 (1896/8), p. 81.*

J. Farkás[136]), *W. Šimerka*[137]), une remarque de *Carl Schmidt*[138]) et *E. Gelin*[139]).

T. Muir[140]) étudie des systèmes de n équations analogues au système de trois équations en x_1, x_2, x_3 que voici:

$$x_1 + g_2 x_2 + g_3 x_3 + g_1 = 0$$
$$g_1 x_1 + x_2 + g_3 x_3 + g_2 = 0$$
$$g_1 x_1 + g_2 x_2 + x_3 + g_3 = 0.$$

Voir encore *L. Heffter*[141]) et *Chr. Schmehl*[142]).

C. Prediger[143]) traite le cas où, employant la méthode des multiplicateurs indéterminés due à *E. Bézout* (n° **15**), les expressions des racines apparaissent sous forme indéterminée.

C. G. J. Jacobi[144]) exprime les valeurs des inconnues au moyen d'intégrales définies multiples d'ordre $(n-1)$; *A. L. Cauchy*[145]) emploie les racines de l'unité pour la résolution des équations linéaires.

G. Fouret[146]), *J. Massau*[147]), *F. J. van den Berg*[148]), *F. J. Vaes*[149]) résolvent *graphiquement* un système de n équations linéaires.

W. Thomson[150]), *F. Guarducci*[151]) et *F. Moth*[152]), décrivent des machines permettant de résoudre des équations linéaires simultanées.

A. Klingatsch[153]) donne une solution géométrique d'un système d'équations linéaires.*

---

136) *C. R. Acad. sc. Paris 87 (1878), p. 523.*

137) *Sitzgsb. Akad. Wien 33 (1858), p. 277.*

138) *Z. Math. Phys. 34 (1889), p. 189.*

139) *Le mat. pure appl. Città di Castello 1 (1901), p. 16, 25; Mathesis (3) 1 (1901), supplément n° 2.*

140) *Proc. R. Soc. Edinb. 23 (1899/901), p. 248/60. *Ch. Tweedie* [Proc. R. Soc. Edinb. 23 (1899/1901), p. 261/3] a ajouté quelques remarques à cet article de *T. Muir*.*

141) *J. reine angew. Math. 111 (1893), p. 59.*

142) *Z. Math.-Naturw. Unterr. 33 (1902), p. 345.*

143) *Archiv Math. Phys. (1) 70 (1884), p. 319.*

144) *J. reine angew. Math. 14 (1835), p. 51; Werke 6, Berlin 1891, p. 79.*

145) *C. R. Acad. sc. Paris 25 (1847), p. 285; Œuvres (1) 10, Paris 1897, p. 368.*

146) *Bull. Soc. math. France 3 (1874/5), p. 93.*

147) *Note sur la résolution graphique des équations du 1^er^ degré, Gand 1889.*

148) *Verslagen Meded. Akad. Wetensch. Afdeeling Natuurk. (Amsterdam) (3) 4 (1888), p. 196/252 [1887].*

149) *Nouv. Ann. math. (3) 18 (1899), p. 74.*

150) *Proc. R. Soc. London 28 (1878/9), p. 111.*

151) *Atti R. Accad. Lincei *Memorie* mat. (4) 7 (1890), éd. 1894, p. 219*

152) *Denkschr. Akad. Wien (math.) 1 I (1850), p. 105.*

153) *Monatsh. Math. Phys. 3 (1892), p. 169.*

*Citons enfin *R. Mehmke*[154]), puis *R. Mehmke* et *P. A. Nekrasov*[155]) qui se sont occupés de la résolution d'un système d'équations linéaires à un grand nombre d'inconnues par approximations successives.*

Les zéros d'une fonction rationnelle entière.

17. Continuité et dérivées d'une fonction rationnelle entière $f(z)$. Soit

$$f(z) = a_0 z^n + a_1 z^{n-1} + \cdots + a_{n-1} z + a_n$$

où $a_0, a_1, \ldots, a_{n-1}, a_n$ sont des nombres complexes (réels ou imaginaires); on peut toujours supposer que a_0 est différent de zéro. Quelle que soit la manière dont on fait tendre la variable z vers la constante complexe (réelle ou imaginaire) a, la fonction $f(z)$ tend vers la constante $f(a)$. C'est ce qu'on exprime en disant que la fonction $f(z)$ est *continue pour toute valeur* a *de* z, ou simplement que $f(z)$ est *continue*.

La valeur absolue de $f(z)$ ne peut augmenter au-delà de toute limite que si la valeur absolue de z augmente elle-même au-delà de toute limite.

La limite de $\frac{f(z)-f(z_0)}{z-z_0}$ quand z tend vers z_0 par un chemin quelconque s'appelle la *dérivée* $f'(z_0)$ de $f(z)$ pour $z = z_0$.

On a, quel que soit z,

$$f'(z) = n a_0 z^{n-1} + (n-1) a_1 z^{n-2} + \cdots + a_{n-1};$$

on appelle *dérivée seconde* de $f(z)$ et l'on désigne par $f''(z)$ la dérivée de $f'(z)$; ...; on appelle *dérivée d'ordre* α de $f(z)$ et l'on désigne par $f^{(\alpha)}(z)$ la dérivée de $f^{(\alpha-1)}(z)$. La dérivée d'ordre n de $f(z)$ est une constante

$$f^{(n)}(z) = n!\, a_0.$$

On a d'ailleurs, quel que soit h,

$$f(z+h) = f(z) + \frac{h}{1!} f'(z) + \frac{h^2}{2!} f''(z) + \cdots + \frac{h^n}{n!} f^{(n)}(z);$$

c'est la *formule de Taylor* dans le cas d'une fonction rationnelle entière.

18. Zéros d'une fonction rationnelle entière $f(z)$. L'équation

$$f(z) = a_0 z^n + a_1 z^{n-1} + \cdots + a_n = 0,$$

où a_0 est différent de zéro, s'appelle une *équation algébrique* de *degré* n. Si a est une constante complexe (réelle ou imaginaire) telle que $f(a)$

---

154) *Math. Sbornik [recueil Soc. math. Moscou] 16 (1891/3), p. 437 [1892].*

155) *Id. p. 342 [1892].*

soit nul, a s'appelle une *racine* de l'équation $f(z)=0$ ou un *zéro* de la fonction $f(z)$.

Toute fonction rationnelle entière d'une variable admet au moins *un* zéro. L'exposé des différentes démonstrations de ce *théorème fondamental* de l'Algèbre fera l'objet d'un chapitre spécial (n$^{\text{os}}$ **80/88**). Le théorème ne peut d'ailleurs être démontré qu'en faisant appel à la notion de continuité analytique.

Si on l'admet comme démontré, il est aisé de voir que toute fonction rationnelle entière $f(z)$ de degré n peut être mise sous la forme

$$f(z)=a_0(z-z_1)(z-z_2)\cdots(z-z_n),$$

où $z_1, z_2, \ldots, z_n$ sont des nombres complexes (réels ou imaginaires) distincts ou non. C'est ce qu'on exprime en disant que toute fonction rationnelle entière de degré n a *précisément* n *zéros.* Lorsque la fonction $f(z)$ est mise sous cette forme, on dit que $f(z)$ est décomposée en ses facteurs *premiers linéaires.* Cette décomposition n'est possible que d'une façon.

Si α des n zéros $z_1, z_2, \cdots, z_n$ coïncident avec le même nombre a, on dit que a est un *zéro multiple d'ordre* α de la fonction $f(z)$ ou une *racine multiple d'ordre* α de l'équation $f(z)=0$. Lorsque $\alpha=1$ on dit que a est un *zéro simple* de $f(z)$ ou une *racine simple* de l'équation algébrique $f(z)=0$.

En désignant par $a, b, \ldots, l$ des nombres complexes distincts (réels ou imaginaires), on peut mettre ainsi toute fonction rationnelle entière $f(z)$ de degré n sous la forme

$$f(z)=a_0(z-a)^\alpha(z-b)^\beta\cdots(z-l)^\lambda,$$

où $\alpha, \beta, \ldots, \lambda$ sont des nombres naturels tels que $\alpha+\beta+\cdots+\lambda=n$.

Si $s_1, s_2, \cdots, s_p, \cdots, s_n$ sont les n fonctions symétriques élémentaires (n° **7**) des n racines $z_1, z_2, \cdots, z_n$ de l'équation

$$a_0z^n+a_1z^{n-1}+\ldots+a_pz^{n-p}+\cdots+a_{n-1}z+a_n=0$$

on a

$$s_1=-\frac{a_1}{a_0},\quad s_2=\frac{a_2}{a_0},\ \cdots,\ s_p=(-1)^p\frac{a_p}{a_0},\ \cdots,\quad s_n=(-1)^n\frac{a_n}{a_0}.$$

Si les coefficients de $f(z)$ sont *réels*, la fonction $f(z)$ ne peut admettre le zéro $\alpha+\beta i$ (α et β étant réels), sans admettre le zéro conjugué $\alpha-\beta i$, avec le même ordre de multiplicité [156].

Si a et b sont réels, et si $f(a)f(b)<0$, la fonction réelle $f(z)$

156) $_*$*C. Maclaurin,* Philos. Trans. London 36 (1729), p. 59/96*; *L. Euler,* Introd. [15]) 1, p. 19; trad. *J. B. Labey* 1, p. 18.

admet dans l'intervalle (a, b) un nombre *impair* de zéros réels [157]) (chaque zéro multiple d'ordre α étant compté α fois). Si, au contraire, $f(a)f(b)>0$, la fonction réelle $f(z)$ n'admet pas de zéros (réels) dans l'intervalle (a, b) ou en admet un nombre pair.

Les racines d'une équation algébrique sont des fonctions *continues* des coefficients [158]), c'est-à-dire qu'en posant

$$f(z)=z^n+a_1z^{n-1}+\cdots+a_n=(z-a)^\alpha(z-b)^\beta\ldots(z-l)^\lambda,$$

où

$$\alpha+\beta+\cdots+\lambda=n,$$

et

$$f_1(z)=\varepsilon_1z^{n-1}+\varepsilon_2z^{n-2}+\cdots+\varepsilon_n+f(z),$$

si l'on trace des points $a, b, \ldots, l$ comme centres des cercles (ϱ_a), $(\varrho_b), \ldots, (\varrho_l)$, n'empiétant pas les uns sur les autres et de rayons *donnés* (aussi petits qu'on voudra), on pourra trouver un nombre $\eta>0$, suffisamment petit, tel que, pour $|\varepsilon_1|<\eta$, $|\varepsilon_2|<\eta, \ldots, |\varepsilon_n|<\eta$, la fonction rationnelle entière $f_1(z)$ ait exactement α zéros à l'intérieur du cercle (ϱ_a), β zéros à l'intérieur du cercle $(\varrho_b), \ldots, \lambda$ zéros à l'intérieur du cercle (ϱ_l).

19. Zéros multiples d'une fonction rationnelle entière $f(z)$. La *formule de Taylor*

$$f(z)=f(a)+\frac{z-a}{1}f'(a)+\cdots+\frac{(z-a)^\alpha}{1.2\ldots\alpha}f^{(\alpha)}(a)+\cdots+\frac{(z-a)^n}{1.2\ldots n}f^{(n)}(a)$$

montre que les égalités

$$f(a)=0,\ f'(a)=0,\ \ldots,\ f^{(\alpha-1)}(a)=0,$$

jointes à la condition que $f^{(\alpha)}(a)$ soit différent de 0, expriment que a est un zéro multiple de $f(z)$ d'ordre précisément égal à α [159]). Une racine multiple d'ordre α de l'équation $f(z)=0$ est racine multiple d'ordre $\alpha-1$ de l'équation $f'(z)=0$.

157) $_*$Cf. *B. Bolzano,* Rein analyt. Beweis . . . [Abh. böhm. Ges. Wiss. 5 (1814/7), éd. Prague 1818, phys. math., mém. n° 6, § 16, 18] réimprimé dans la collection intitulée: Classiker, wissenschaftliche, in Facsimile-Drucken 8, Berlin 1894, p. 56, 59.*

158) $_*$*O. Bonnet,* Bull. sc. math. (1) 2 (1871), p. 215; *V. Rouquet,* Nouv. Ann. math. (2) 15 (1876), p. 154; *A. Tresse,* Revue math. spéc. 4 (1896/8), p. 377; *H. Weber*, Alg. [24]) 1, p. 149; trad. *J. Griess* 1, p. 156.*

159) $_*$Cf. *J. Hudde,* De reductione aequationum (réd. en 1657); De maximis et minimis (réd. en 1658); publ. par *F. van Schooten* dans la 2$^{\text{ième}}$ éd. latine de la Géométrie de *R. Descartes* [Geom. Descartes [2]) 1, p. 433/9, 507/9]; *L. Euler,* Calc. diff. [17]), p. 577; *N. V. Bugajev,* Viestnik matem. nauk (Messager des sc. math. Vilna) 2 (1863), p. 1.*

*Désignons par Z_k le produit de ceux des facteurs distincts $(z-a)$, $(z-b)$, $\ldots$, $(z-l)$ de $f(z)$ dont l'ordre de multiplicité est égal à k. On pourra alors mettre $f(z)$ sous la forme

$$f(z) = Z_1 Z_2^2 \ldots Z_p^p.$$

On sait, par de simples divisions, trouver chacune des fonctions rationnelles entières (à zéros simples) $Z_1, Z_2, \ldots, Z_p$[160]). Si l'on désigne par $D(z)$ le plus grand commun diviseur de $f(z)$ et de $f'(z)$ et que l'on pose[161])

$$f(z) = D(z)\,\psi(z), \quad f'(z) = D(z)\,\theta(z),$$

Z_h est le plus grand commun diviseur de $\psi(z)$ et de $\theta(z) - h\psi'(z)$.

La fonction rationnelle entière $\psi(z)$ n'a aucun zéro multiple. *F. Engel*[162]) a démontré ce point sans supposer démontrée l'existence des racines de $f(z) = 0$[163]).*

Ce qui précède (n^os **17** à **19**) subsiste quand $a_0, a_1, \ldots, a_n$ au lieu de désigner des constantes complexes (réelles ou imaginaires) dépendent d'un certain nombre de paramètres ou désignent même des quantités complètement indéterminées à condition toutefois de toujours exclure les valeurs des paramètres pour lesquelles a_0 serait nul.

20. Les évectants. Si la *fonction* rationnelle entière

$$f(z) = a_0 z^n + a_1 z^{n-1} + \cdots + a_n$$

n'a que p zéros distincts, la différence $n-p$ est ce que *J. J. Sylvester*[164]) appelle la *multiplicité* de $f(z)$. Si $f(z)$ a un seul zéro d'ordre n la *multiplicité* de $f(z)$ est $(n-1)$.

*Posons $z = \frac{x}{y}$ et remplaçons $f(z)$ par la forme binaire

$$\varphi(x, y) = y^n f(z)$$

c'est-à-dire par

$$\varphi(x, y) = \sum_{p=0}^{p=n} \frac{(p+q)!}{p!\,q!}\, a_{p,q}\, x^p y^q \qquad (p+q=n),$$

où l'on a écrit

160) *J. A. Serret,* Alg. sup.[30]) 1, p. 112.*

161) *M. Ostrogradski,* C. R. Acad. sc. Paris 42 (1856), p. 930.*

162) *Ber. Ges. Lpz. 49 (1897), math. p. 603. Voir aussi *A. Tresse,* Revue math. spéc. 7 (1902/4), p. 33; *P. Mansion,* Mathesis (3) 2 (1902), p. 57.*

163) *Sur les racines doubles de l'équation $f(\mathfrak{u}, \mathfrak{v}) = 0$, f étant un polynome homogène en $\mathfrak{u}$ et $\mathfrak{v}$, $\mathfrak{u}$ et $\mathfrak{v}$ étant deux polynomes entiers en x de même degré, voir *L. Mirman,* Nouv. Ann. math. (3) 4 (1885), p. 173; voir aussi *O. Biermann,* Monatsh. Math. Phys. 13 (1902), p. 351.*

164) London Edinb. Dublin philos. mag. (4) 3 (1852), p. 375, 460; Papers 1, Cambridge 1905, p. 367, 370.

$$a_{p,q} = a_{n-q,q} = \frac{q!\,(n-q)!}{n!}\, a_q \qquad (q = 0, 1, 2, \ldots, n)$$

et convenons de dire que $\varphi(x, y)$ est de multiplicité m quand $f(z)$ est de multiplicité m.

Ceci posé, soit $\psi(a_{0,n}, a_{1,n-1}, \ldots, a_{n,0})$ une fonction quelconque des coefficients $a_{0,n}, a_{1,n-1}, \ldots, a_{n,0}$. Appelons *évectant* de ψ la forme

$$x^n \frac{\partial \psi}{\partial a_{0,n}} + x^{n-1} y \frac{\partial \psi}{\partial a_{1,n-1}} + \cdots + y^n \frac{\partial \psi}{\partial a_{n,0}}.$$

Le résultat obtenu en répétant r fois l'opération

$$x^n \frac{\partial}{\partial a_{0,n}} + x^{n-1} y \frac{\partial}{\partial a_{1,n-1}} + \cdots + y^n \frac{\partial}{\partial a_{n,0}}$$

s'appellera le $r^{\text{ième}}$ évectant.

On démontre que, si $\varphi(x, y)$ est de multiplicité m, le discriminant de $\varphi(x, y)$ [c'est-à-dire le résultat de l'élimination de x et de y entre les équations $\frac{\partial \varphi}{\partial x} = 0$ et $\frac{\partial \varphi}{\partial y} = 0$] et les $(m-1)$ premiers évectants de ce discriminant seront nuls indépendamment de x et de y, de quelque façon que la multiplicité soit distribuée. D'autre part, s'il y a r groupes de racines égales, de multiplicités $m_1, m_2, \ldots, m_r$ respectivement (où $m_1 + m_2 + \cdots + m_r = m$), le $m^{\text{ième}}$ évectant du discriminant de la forme binaire $\varphi(x, y)$ sera de la forme

$$(\beta_1 x - \alpha_1 y)^{m_1 n} (\beta_2 x - \alpha_2 y)^{m_2 n} \cdots (\beta_r x - \alpha_r y)^{m_r n}$$

où $\frac{\alpha_1}{\beta_1}, \frac{\alpha_2}{\beta_2}, \ldots, \frac{\alpha_r}{\beta_r}$ sont les valeurs de $z = \frac{x}{y}$ qui correspondent aux différentes valeurs des racines égales de l'équation $f(z) = 0$. *J. J. Sylvester*[164]) a aussi essayé d'étendre ce théorème au cas de fonctions de plusieurs variables[165]).

21. Les zéros d'une fonction rationnelle entière de plusieurs variables. Soit maintenant donnée une fonction rationnelle entière

$$f(z_1, z_2, \ldots, z_m)$$

de m variables $z_1, z_2, \ldots, z_m$ dont les coefficients soient des nombres complexes (réels ou imaginaires) dont l'un au moins soit différent de zéro.

165) *Voir aussi *H. Schramm,* Ann. mat. pura appl. (2) 3 (1869/70), p. 41; *X. Antomari,* Nouv. Ann. math. (3) 16 (1897), p. 63; *L. Baur,* Math. Ann. 50 (1898), p. 241; 52 (1899), p. 113*; *G. Salmon,* Lessons introd. to the modern higher Algebra, Dublin 1859; 4^e éd. Dublin 1885, p. 123; trad. *O. Chemin,* Paris 1890, p. 175; *P. Sondat [Nouv. Ann. math. (3) 16 (1897), p. 169; (3) 19 (1900), p. 25] cherche à quelle condition une équation de degré $2n$ a $(n+1)$ racines égales.*

Il existe des systèmes de valeurs

$$z_1 = \zeta_1, \ z_2 = \zeta_2, \ldots, z_m = \zeta_m$$

pour lesquelles cette fonction est nulle. C'est une conséquence du théorème d'après lequel chaque fonction rationnelle entière d'une variable admet un zéro. Un tel système $(\zeta_1, \zeta_2, \ldots, \zeta_m)$ s'appelle un *zéro* de la fonction rationnelle entière $f(z_1, z_2, \ldots, z_m)$ et une *racine* de l'équation algébrique

$$f(z_1, z_2, \ldots, z_m) = 0.$$

Si la fonction $f(z_1, z_2, \ldots, z_m)$ s'annulait pour tout système de valeurs $(\zeta_1, \zeta_2, \ldots, \zeta_m)$, les coefficients de la fonction f seraient tous nuls et la fonction f serait *identiquement nulle.*

On appelle $\zeta_1, \zeta_2, \ldots, \zeta_m$ les *coordonnées* de la racine $(\zeta_1, \zeta_2, \ldots, \zeta_m)$ de l'équation $f(z_1, z_2, \ldots, z_m) = 0$.

L'ensemble des racines de l'équation $f(z_1, z_2, \ldots, z_m) = 0$ forme une *variété continue* à $m-1$ dimensions dans l'espace à m dimensions. Si la fonction $f(z_1, z_2, \ldots, z_m)$ n'est pas identiquement nulle, on peut donc toujours déterminer une infinité de systèmes $(\zeta_1, \zeta_2, \ldots, \zeta_m)$, aussi voisins que l'on veut d'un système donné $(z_1, z_2, \ldots, z_m)$ et tels que $f(\zeta_1, \zeta_2, \ldots, \zeta_m)$ ait une valeur différente de zéro.

*Du fait qu'une fonction rationnelle entière d'une seule variable (qui n'est pas identiquement nulle) n'admet pas plus de racines que ne l'indique son degré, résultent les conséquences importantes que voici:

Si les coefficients de k fonctions rationnelles entières

$$f_1(z_1, z_2, \ldots, z_m), \ f_2(z_1, z_2, \ldots, z_m), \ldots, \ f_k(z_1, z_2, \ldots z_m)$$

sont des *nombres* qui, pour aucune de ces k fonctions, ne soient tous nuls, on peut toujours trouver[166]) d'une infinité de manières des valeurs de $z_1, z_2, \cdots, z_m$ pour lesquelles *aucune* des k fonctions ne s'annule.

Si ces fonctions rationnelles entières sont deux à deux sans diviseur commun, il existe des valeurs de $z_1, z_2, \ldots, z_m$ telles que l'une quelconque d'entre ces fonctions (supposée *non constante*) *soit* nulle et les autres différentes de zéro.*

Si l'on groupe les termes de même degré contenus dans une fonction rationnelle entière $f(z_1, z_2, \ldots, z_m)$ de degré n et si l'on désigne pour chaque indice k par $\varphi_k(z_1, z_2, \ldots, z_m)$ l'ensemble des termes de degré k, on a manifestement en désignant par z_0 une variable quelconque (dite *variable d'homogénéité*)

166) *Cf. *H. Weber*, Alg.[24]) 1, p. 147; trad. *J. Griess* 1, p. 154 (Texte et note de *J. Hadamard*).*

$$z_0^n f\left(\frac{z_1}{z_0}, \frac{z_2}{z_0}, \cdots, \frac{z_m}{z_0}\right) = \varphi_n(z_1, z_2, \ldots, z_m) + z_0\varphi_{n-1}(z_1, z_2, \ldots, z_m) + z_0^2\varphi_{n-2}(z_1, z_2, \ldots, z_m) + \cdots + z_0^n\varphi_0(z_1, z_2, \ldots, z_m).$$

Supposons que pour les valeurs finies

$$z_1 = \zeta_1, \quad z_2 = \zeta_2, \quad z_3 = \zeta_3, \ldots, z_m = \zeta_m,$$

la fonction $\varphi_n(z_1, z_2, \ldots, z_m)$ s'annule; l'équation homogène en $z_0, z_1, z_2, \ldots, z_m$,

$$z_0^n f\left(\frac{z_1}{z_0}, \frac{z_2}{z_0}, \ldots, \frac{z_m}{z_0}\right) = 0$$

admettra alors la racine

$$(0, \zeta_1, \zeta_2, \ldots, \zeta_m).$$

Lorsque les m dernières coordonnées $\zeta_1, \zeta_2, \ldots, \zeta_m$ de cette racine sont toutes différentes de zéro on dit que l'équation $f(z_1, z_2, \ldots, z_m) = 0$ admet la racine infinie

$$(\zeta_1 t, \zeta_2 t, \ldots, \zeta_m t) \text{ où l'on suppose } t = \infty.$$

Lorsque parmi les m dernières coordonnées de la racine envisagée

$$(0, \zeta_1, \zeta_2, \cdots, \zeta_m)$$

une, ou plusieurs, *mais non toutes*, sont nulles, on dit encore que l'équation

$$f(z_1, z_2, \cdots, z_m) = 0$$

admet la racine infinie

$$(\zeta_1 t, \zeta_2 t, \cdots, \zeta_m t), \text{ où l'on suppose } t = \infty;$$

les coordonnées de cette racine infinie qui correspondent aux ζ_i différents de zéro sont infinies, tandis que les coordonnées qui correspondent aux ζ_i égaux à zéro sont indéterminées.

L'équation

$$9z_1^2 - 4z_2^2 + z_3^2 - 2z_2z_3 - 1 = 0,$$

par exemple, admet la racine infinie

$$(2t, 3t, 0t), \quad t = \infty$$

dont les deux premières coordonnées sont infinies tandis que la troisième est indéterminée.

Toute racine infinie d'une équation

$$f(z_1, z_2, \cdots, z_m) = 0$$

dans laquelle $f(z_1, z_2, \cdots, z_m)$ est une fonction *régulière* de $z_1, z_2, \cdots, z_m$ a *au moins deux* de ses coordonnées qui sont infinies.

22. Racines multiples d'une fonction rationnelle entière. Si $(\zeta_1, \zeta_2, \ldots, \zeta_m)$ est une racine de l'équation algébrique

$$f(z_1, z_2, \ldots, z_m) = 0,$$

on peut, d'une infinité de manières, mettre la fonction $f(z_1, z_2, \ldots, z_m)$ sous la forme

$$f(z_1, z_2, \ldots, z_m) = (z_1 - \zeta_1)g_1 + (z_2 - \zeta_2)g_2 + \cdots + (z_m - \zeta_m)g_m$$

où $g_1, g_2, \ldots, g_m$ sont des fonctions rationnelles entières de $z_1, z_2, \ldots, z_m$ [167]).

Si $g_1, g_2, \ldots, g_m$ s'annulent encore pour la racine $(\zeta_1, \zeta_2, \ldots, \zeta_m)$, on pourra d'une infinité de manières mettre la fonction f sous la forme

$$f(z_1, z_2, \ldots, z_m) = \sum_{\alpha=1}^{\alpha=m} \sum_{\beta=1}^{\beta=m} (z_\alpha - \zeta_\alpha)(z_\beta - \zeta_\beta)\, g_{\alpha,\beta},$$

où les $g_{\alpha,\beta}$ sont des fonctions rationnelles entières de $z_1, z_2, \ldots, z_m$. On dit alors que $(\zeta_1, \zeta_2, \ldots, \zeta_m)$ est une *racine double* de l'équation algébrique $f(z_1, z_2, \ldots, z_m) = 0$.

En général on dit que $(\zeta_1, \zeta_2, \ldots, \zeta_m)$ est une racine d'ordre ϱ de l'équation algébrique $f(z_1, z_2, \ldots, z_m) = 0$ lorsque la fonction rationnelle entière $f(z_1, z_2, \ldots, z_m)$ peut être représentée par une fonction homogène de degré ϱ des différences $z_1 - \zeta_1, z_2 - \zeta_2, \ldots, z_m - \zeta_m$ dont les coefficients soient des fonctions rationnelles entières de $z_1, z_2, \ldots, z_m$.

Pour une racine d'ordre ϱ, non seulement $f(z_1, z_2, \ldots, z_m)$ s'annule, mais aussi toutes les dérivées partielles de f jusqu'à celles d'ordre $\varrho - 1$ inclusivement.

Problèmes d'interpolation. Fractions simples.

23. Détermination d'une fonction rationnelle entière $f(z)$ par des valeurs $u_k = f(z_k)$. La fonction rationnelle entière

$$f(z) = a_0 z^n + a_1 z^{n-1} + \cdots + a_n$$

contient $(n+1)$ constantes et sera déterminée si l'on donne les $(n+1)$ valeurs $u_0, u_1, u_2, \ldots, u_n$ de $f(z)$ pour $(n+1)$ valeurs distinctes $z = z_0,\ z = z_1,\ z = z_2, \ldots, z = z_n$ de la variable z fixées arbitrairement.

Si, avec *I. Newton* [168]), on pose

$$f(z) = c_0 + c_1(z - z_0) + c_2(z - z_0)(z - z_1) + c_3(z - z_0)(z - z_1)(z - z_2) + \cdots + c_{n+1}(z - z_0)(z - z_1)\cdots(z - z_n),$$

167) *L. Kronecker* [Monatsb. Akad. Berlin 1865, p. 687; Werke 1, Leipzig 1895, p. 136] a utilisé cette forme pour ses recherches sur l'interpolation.

168) Philos. naturalis principia math., Londres 1687 [préface 1686], (2e éd.) Cambr. 1713; (3e éd.) Londres 1726 (livre 3, lemme 5); trad. par *G. E. de Breteuil* marquise du Châtelet 2, Paris 1759, p. 120/1; Opera, éd. *S. Horsley* 3, Londres 1782, p. 128.

on a [169])

$$c_{n+1} = 0;\quad c_0 = u_0;\quad c_1 = \frac{u_0}{z_0 - z_1} + \frac{u_1}{z_1 - z_0};$$

$$c_2 = \frac{u_0}{(z_0 - z_1)(z_0 - z_2)} + \frac{u_1}{(z_1 - z_0)(z_1 - z_2)} + \frac{u_2}{(z_2 - z_0)(z_2 - z_1)};$$

et, en général, pour $k = 2, 3, \ldots, n$,

$$c_k = \frac{u_0}{(z_0 - z_1)(z_0 - z_2)\cdots(z_0 - z_k)} + \frac{u_1}{(z_1 - z_0)(z_1 - z_2)\cdots(z_1 - z_k)} + \cdots + \frac{u_k}{(z_k - z_0)(z_k - z_1)\cdots(z_k - z_{k-1})}.$$

Voici la solution du même problème due à *J. L. Lagrange* [170]): En continuant à désigner par $z_0, z_1, \ldots, z_n$, $(n+1)$ nombres distincts fixés arbitrairement, posons

$$g(z) = (z - z_0)(z - z_1)(z - z_2)\cdots(z - z_n),$$

et désignons par $g'(z)$ la dérivée de $g(z)$ prise par rapport à z. Toute fonction rationnelle entière f de z, de degré égal ou inférieur à n, peut alors être représentée par la formule d'interpolation [171])

$$f(z) = \sum_{\lambda=0}^{\lambda=n} \frac{u_\lambda g(z)}{(z - z_\lambda)\, g'(z_\lambda)},$$

où $u_\lambda = f(z_\lambda)$ pour $\lambda = 0, 1, 2, \ldots, n$ [172]).

On en déduit les formules que voici, dites *formules d'Euler* [173]),

$$\sum_{\lambda=0}^{\lambda=n} \frac{1}{g'(z_\lambda)} = 0,\quad \sum_{\lambda=0}^{\lambda=n} \frac{z_\lambda}{g'(z_\lambda)} = 0,\quad \ldots,\quad \sum_{\lambda=0}^{\lambda=n} \frac{z_\lambda^{n-1}}{g'(z_\lambda)} = 0,\quad \sum_{\lambda=0}^{\lambda=n} \frac{z_\lambda^{n}}{g'(z_\lambda)} = 1.$$

169) Voir aussi *J. F. Encke*, Berliner Astron. Jahrb. für 1830 (éd. Berlin 1828), p. 265/84 [d'après un Cours que *C. F. Gauss* avait professé en 1812].

170) Leçons élém. sur les math. données à l'Ecole normale en l'an III, leçon 5 (cf. I 21, **23** note 106); J. Ec. polyt. (1) cah. 8 (1812), p. 276; Œuvres 7, Paris 1877, p. 285. *La *formule d'interpolation de Lagrange* avait déjà été signalée par *E. Waring*, Philos. Trans. London 69 (1779), p. 59/67 (cf. I 21, **23** note 107).*

171) Voir aussi à ce sujet *E. H. Dirksen*, J. reine angew. Math. 1 (1826), p. 221; *Ch. Hermite*, id. 84 (1878), p. 70; **T. J. Stieltjes*, Verslagen Meded. Akad. Wetensch. Afdeeling Natuurk. (Amsterdam) (2) 17 (1882), p. 239/54; *F. J. Studnička*, Časopis math. fys. (Prague) 2 (1873), p. 82; *W. Levicki*, Wiadomości matematyczne 3 (1899), p. 264/74; Archiv Math. Phys. (2) 17 (1899), p. 214/74; Sammelschr. math.-naturw. ärztl. Sect. Ševčenko Ges. Wiss. Lemberg (Lwow) 4 II (1899), mém. nº 2; *J. G. Garnier*, Bull. Acad. Bruxelles 6 II (1839), p. 19/26.*

172) *La méthode de *I. Newton* donne immédiatement les conditions pour que le degré de $f(z)$ se réduise à $n - i$; il faut pour cela et il suffit que l'on ait

$$c_{n-i+1} = 0,\quad c_{n-i+2} = 0,\ \ldots,\ c_n = 0.$$

La méthode de *J. L. Lagrange* ne donne pas explicitement le degré effectif de $f(z)$. (Note de *J. Drach*).*

173) Institutiones calculi integralis 2, St Pétersb. 1769, p. 432.

De ces *formules d'Euler* on peut d'ailleurs déduire inversement la *formule d'interpolation de Lagrange*.

24. Décomposition d'une fraction rationnelle en fractions simples. Soit $\frac{f(z)}{g(z)}$ une fraction rationnelle quelconque irréductible et soit

$$g(z) = Z_1 Z_2^2 \dots Z_p^p$$

la décomposition de $g(z)$ en facteurs à zéros simples du n° **19**. *Ch. Hermite*[174]) a montré qu'on peut mettre $\frac{f(z)}{g(z)}$ sous la forme

$$\frac{Y_1}{Z_1} + \frac{Y_2}{Z_2^2} + \cdots + \frac{Y_p}{Z_p^p},$$

$Y_1, \dots, Y_p$ étant des fonctions rationnelles entières de z, et cela par des opérations rationnelles (des divisions).

Soient[175]) $a, b, \dots, l$ les zéros distincts de $g(z)$; $\alpha, \beta, \dots, \lambda$ leurs ordres de multiplicité, en sorte que, g_0 étant une constante, on ait

$$g(z) = g_0 (z-a)^\alpha (z-b)^\beta \cdots (z-l)^\lambda.$$

On pourra toujours, et d'une seule façon, mettre la fraction rationnelle $\frac{f(z)}{g(z)}$ sous la forme[176])

$$\begin{aligned}\frac{f(z)}{g(z)} = E(z) &+ \frac{A_\alpha}{(z-a)^\alpha} + \frac{A_{\alpha-1}}{(z-a)^{\alpha-1}} + \cdots + \frac{A_1}{z-a} \\ &+ \frac{B_\beta}{(z-b)^\beta} + \frac{B_{\beta-1}}{(z-b)^{\beta-1}} + \cdots + \frac{B_1}{z-b} \\ &+ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ &+ \frac{L_\lambda}{(z-l)^\lambda} + \frac{L_{\lambda-1}}{(z-l)^{\lambda-1}} + \cdots + \frac{L_1}{z-l},\end{aligned}$$

174) *Ch. Hermite*, Cours d'Analyse de l'Ec. polyt. 1, Paris 1873, p. 265/7.

175) *Le cas où $\alpha = \beta = \cdots = \lambda = 1$ a été traité à peu près simultanément par *G. W. Leibniz* et par *Jean Bernoulli* [voir *G. W. Leibniz*, Werke, éd. *C. I. Gerhardt*, Math. Schr. 3, Halle 1855/6, p. 702 (lettre de *Jean Bernoulli* datée du 10 juin 1702) et p. 703/5 (lettre de *G. W. Leibniz* datée du 24 juin 1702); voir aussi *G. W. Leibniz*, Acta Erud. Lps. 1702, p. 210; Math. Schr. 5, Halle 1858, p. 350; *Jean Bernoulli*, Hist. Acad. sc. Paris 1702, éd. 1704, M. p. 289; Opera 1, Lausanne et Genève 1742, p. 393; Acta Erud. Lps. 1703, p. 26].

Pour $\alpha, \beta, \dots, \lambda$ quelconques le problème a été résolu par *G. W. Leibniz* [Acta Erud. Lps. 1703, p. 19; Math. Schr. 5, Halle 1858, p. 361]. Voir encore *Jean Bernoulli* [Acta Erud. Lps. 1719, p. 256; Opera 2, Lausanne et Genève 1742, p. 402], *A de Moivre* [Philos. Trans. London 32 (1722/3), p. 162], *L. Euler* [lettre à *Chr. Goldbach* datée du 15 décembre 1742, publ. par *P. H. Fuss*, Corresp. math. phys. 1, St Pétersb. 1843, p. 170] (Note de *G. Eneström*).*

176) On peut aussi consulter *L. Euler*, Introd.[15]), p. 22, 161; trad. *J. B. Labey* 1, p. 21, 156; Calc. differ.[17]), p. 844; Mém. Acad. Pétersb. 1 (1803/6), éd. 1809, math. p. 3/25 [1779].

où $E(z)$ est une fonction rationnelle entière de z et $A_1, \dots, A_{\alpha-1}, A_\alpha$, $B_1, \dots, B_{\beta-1}, B_\beta, \dots\dots\dots, L_1, \dots, L_{\lambda-1}, L_\lambda$ des constantes[177]). Cela s'appelle[178]) *décomposer la fraction rationnelle en fractions simples*[179]).

Pour avoir l'ensemble des termes

$$\frac{A_\alpha}{(z-a)^\alpha} + \frac{A_{\alpha-1}}{(z-a)^{\alpha-1}} + \cdots + \frac{A_1}{z-a}$$

qui correspondent à la racine a de $g(z)$, il suffit, en désignant par $\psi(z)$ la fonction

$$\psi(z) = \frac{g(z)}{(z-a)^\alpha} = (z-b)^\beta \cdots (z-l)^\lambda,$$

de diviser $f(a+h)$ par $\psi(a+h)$, après avoir ordonné ces deux fonctions rationnelles entières suivant les puissances croissantes de h, en poussant l'opération jusqu'au premier reste qui contient h^α en facteur[180]); on obtient ainsi

$$A_\alpha + A_{\alpha-1} h + \cdots + A_1 h^{\alpha-1}.$$

Si l'on développait en série ordonnée suivant les puissances croissantes

177) *Dans son mémoire: Nova methodus integrandi formulas differentiales rationales sine subsidio quantitatum imaginariarum [Acta Acad. Petrop. 5 (1781) I, éd. 1784, math. p. 3/47] *L. Euler* décompose une fonction rationnelle fractionnaire à coefficients réels en une somme de fractions simples à dénominateurs linéaires ou quadratiques sans faire intervenir les nombres complexes (Note de *G. Vivanti*)*.

178) Pour des renseignements bibliographiques et pour un exposé complet de la théorie voir *A. L. Crelle*, J. reine angew. Math. 9 (1832), p. 231; 10 (1833), p. 42; voir en outre *E. H. Dirksen*, J. reine angew. Math. 1 (1826), p. 53; *A. L. Cauchy*, Analyse alg.[100]), p. 365; Œuvres (2) 3, p. 302; *T. Clausen*, J. reine angew. Math. 8 (1832), p. 142; *A. Beyer*, J. reine angew. Math. 7 (1831), p. 217; *G. Eisenstein*, id. 32 (1846), p. 71; *L. Öttinger*, id. 22 (1841), p. 63, 148; *J. Liouville*, J. math. pures appl. (1) 11 (1846), p. 462; *E. Rouché*, C. R. Acad. sc. Paris 46 (1858), p. 450; 49 (1859), p. 863; *J. Vieille*, id. 49 (1859), p. 746; *C. Ch. E. Gerono*, Nouv. Ann. math. (1) 18 (1859), p. 346; *S. Realis*, id. (2) 3 (1864), p. 438; *A. de Saint Germain*, id. (2) 8 (1869), p. 369; *Ch. Hermite*, Ann. Soc. scient. Bruxelles 2^2 (1877/8), p. 157; *A. V. Jamet*, Nouv. Ann. math. (3) 8 (1889) p. 228/32; *L. Saalschütz*, Monatsh. Math. Phys. 9 (1898), p. 132; *X. X.*, Bull. math. spéc. 6 (1899/1900), p. 4 (décomposition de $\frac{1}{f^2(z)}$ en fractions simples); *F. J. Studnička*, Sitzgsb. böhm. Ges. Prag 1901, mém. n° 18; Časopis math. fys. (Prague) 31 (1902), p. 1.

179) *Voir aussi *L. Rangoni*, Mem. mat. fis. Soc. ital. delle scienze (1) 21 (1836), p. 65; *N. Trudi*, Rendic. Accad. Napoli (1) 3 (1864), p. 277; Atti Accad. sc. fis. mat. (Naples) (1) 2 (1865), mém. n° 12; Giorn. mat. (1) 2 (1864), p. 225, 257; (1) 5 (1867), p. 1, 93, 257, 337 (Note de *G. Vivanti*)*.

180) *C. G. J. Jacobi*, Diss. Berlin 1825; Werke 3, Berlin 1884, p. 1. *Voir aussi Ann. math. pures appl. 10 (1819/20), p. 255*.

de h l'expression $\frac{f(a+h)}{g(a+h)}$, la partie du développement contenant les puissances négatives serait

$$\frac{A_\alpha}{h^\alpha} + \frac{A_{\alpha-1}}{h^{\alpha-1}} + \cdots + \frac{A_1}{h}.$$

*Dans le cas où $g(z) = (z-z_1)(z-z_2)\cdots(z-z_n)$ n'aurait que des zéros simples $z_1, z_2, \ldots, z_n$, *C. G. J. Jacobi*[181]) a cherché à mettre la fraction $\frac{f(z)}{g(z)}$ sous la forme

$$\frac{f(z)}{g(z)} = \sum_{h,k} \frac{A_{hk}}{(z-z_h)(z-z_k)} \qquad (h=1,2,\ldots,n;\ k=1,2,\ldots,n;\ h>k)$$

Il arrive aux identités suivantes: représentons par $M_{1,2,3,\ldots,k}$ le produit des $k(n-k)$ différences

$$\begin{aligned} M_{1,2,3,\ldots,k} = {} & (z_1 - z_{k+1})(z_1 - z_{k+2}) \cdots (z_1 - z_n) \\ & (z_2 - z_{k+1})(z_2 - z_{k+2}) \cdots (z_2 - z_n) \\ & \cdots\cdots\cdots\cdots\cdots \\ & (z_k - z_{k+1})(z_k - z_{k+2}) \cdots (z_k - z_n) \end{aligned}$$

et désignons par $p_1, p_2, \ldots, p_k$ des nombres entiers positifs ou nuls, parmi lesquels il y en ait deux au moins qui n'atteignent pas $(n-k)$, les autres ne dépassant pas $(n-k)$; on a alors

$$\sum \frac{z_1^{p_1} z_2^{p_2} \cdots z_k^{p_k}}{(z-z_1)(z-z_2)\cdots(z-z_k)} \, \frac{1}{M_{1,2,\ldots,k}} = 0,$$

la somme étant étendue à toutes les combinaisons prises k à k des n indices $1, 2, \ldots, n$. Pour tout nombre a vérifiant la condition $a \leqq n-k$ on a aussi

$$\sum \frac{z_1^{a} z_2^{n-k} z_3^{n-k} \cdots z_k^{n-k}}{(z-z_1)(z-z_2)\cdots(z-z_k)} \cdot \frac{1}{M_{1,2,\ldots,k}} = \frac{z^a}{g(z)},$$

la somme étant encore étendue aux mêmes combinaisons des indices $1, 2, \ldots, n$.*

25. La formule d'interpolation d'Hermite. *Ch. Hermite*[182]) s'est proposé de trouver une fonction rationnelle entière $F(x)$, de degré $(n-1)$, telle que, $f(x)$ désignant une fonction quelconque donnée et $a, b, \ldots, l$ des nombres quelconques donnés, on ait

181) *C. G. J. Jacobi*, Diss. Berlin 1825, § 11, 12; Werke 3, p. 18/29.

182) J. reine angew. Math. 84 (1878), p. 70. Voir aussi *Ch. Hermite*, Analyse[174]) 1, p. 265 et suiv.

$$\begin{aligned} &F(a) = f(a), \quad F'(a) = f'(a), \ \ldots, \ F^{(\alpha-1)}(a) = f^{(\alpha-1)}(a), \\ &F(b) = f(b), \quad F'(b) = f'(b), \ \ldots, \ F^{(\beta-1)}(b) = f^{(\beta-1)}(b), \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ &F(l) = f(l), \quad F'(l) = f'(l), \ \ldots, \ F^{(\lambda-1)}(l) = f^{(\lambda-1)}(l). \end{aligned}$$

En supposant $\alpha + \beta + \cdots + \lambda = n$, la question est déterminée et conduit à une généralisation de la *formule d'interpolation de Lagrange.*

Soit s une aire comprenant les points d'affixes $a, b, \ldots, l$ et x, dans laquelle $f(x)$ soit univoque, et à l'intérieur de laquelle $f(x)$ n'ait pas de pôles. On a alors

$$F(x) - f(x) = \frac{1}{2i\pi} \int_{(S)} \frac{f(z)\,(x-a)^\alpha (x-b)^\beta \cdots (x-l)^\lambda}{(x-z)\,(z-a)^\alpha (z-b)^\beta \cdots (z-l)^\lambda}\, dz,$$

l'intégrale étant prise le long du contour[183]) de l'aire s.

Il est aisé de le vérifier en remplaçant l'intégrale curviligne par la somme des résidus de l'expression

$$\frac{f(z)\,(x-a)^\alpha (x-b)^\beta \cdots (x-l)^\lambda}{(x-z)\,(z-a)^\alpha (z-b)^\beta \cdots (z-l)^\lambda}$$

à l'intérieur de l'aire s[184]).

L. Stickelberger* (nº **28) et *Gy. Zemplén*[185]) ont donné des solutions *algébriques* du problème de *Ch. Hermite.**

26. *Les formules de Brioschi. Soient $z_1, z_2, \ldots, z_n$ les zéros, supposés distincts, du polynome

$$f(z) = a_0 z^n + a_1 z^{n-1} + \cdots + a_n;$$

en désignant par $c_0, c_1, \ldots, c_n$ des nombres quelconques, posons

$$\varphi(z) = c_0 z^n + c_1 z^{n-1} + \cdots + c_n,$$

puis pour $r = 0, 1, 2, \ldots, n-1$

$$S_r = \sum_{h=1}^{h=n} \frac{z_h^r \varphi(z_h)}{f'(z_h)}, \qquad T_r = \sum_{h=1}^{h=n} \frac{z_h^r \varphi(z_h)}{(z-z_h) f'(z_h)}.$$

Alors on a[186])

183) Dans le tome II on étudiera les intégrales prises le long de lignes droites ou courbes.

184) Voir *I. Bendixson*, C. R. Acad. sc. Paris 101 (1885), p. 1050, 1129; *E. Schering*, id. 92 (1881), p. 510. *C. A. Laisant* [Assoc. fr. avanc. sc. 26 (St Etienne) 1897², p. 86] s'occupe du problème suivant: Une courbe donnée passe par n points donnés; trouver une nouvelle courbe qui passe par ces points, qui, en ces points, ait mêmes tangentes, et qui passe, en outre, par un nouveau point donné.

185) *Mathematikai és Physikai lapok 9 (1900), p. 386; Archiv Math. Phys. (3) 8 (1904), p. 214.*

186) *F. Brioschi*, J. reine angew. Math. 50 (1855), p. 239, 318.

$$S_r = (-1)^{r+1} \frac{1}{a_0^{r+2}} \begin{vmatrix} c_0 & a_0 & 0 & \dots & 0 \\ c_1 & a_1 & a_0 & \dots & 0 \\ c_2 & a_2 & a_1 & \dots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ c_r & a_r & a_{r-1} & \dots & a_0 \\ c_{r+1} & a_{r+1} & a_r & \dots & a_1 \end{vmatrix}$$

et

$$T_r = (-1)^{r+1} \frac{1}{a_0^{r+1}} \begin{vmatrix} h_0 & a_0 & 0 & \dots & 0 \\ h_1 & a_1 & a_0 & \dots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ h_{r-1} & a_{r-1} & a_{r-2} & \dots & a_0 \\ h_r & a_r & a_{r-1} & \dots & a_1 \end{vmatrix} + z^r \frac{\varphi(z)}{f(z)}$$

si l'on pose, pour $s = 0, 1, \dots, r$,

$$h_s = c_0 z^s + c_1 z^{s-1} + \dots + c_s.^*$$

27. Le problème de Cauchy. Voici en quoi consiste le problème de *A. L. Cauchy*[187]): Soit $u = \frac{N(z)}{D(z)}$ une fonction rationnelle de z, le numérateur $N(z)$ étant une fonction entière de degré $(n-1)$, le dénominateur $D(z)$ une fonction entière de degré m. On connaît les valeurs de u pour $m+n$ valeurs de z, et il s'agit de déterminer u.

Si, pour

$$z = z_1, z_2, \dots, z_{m+n},$$

on a

$$u = u_1, u_2, \dots, u_{m+n},$$

posons

$$f(z) = (z - z_1)(z - z_2) \cdots (z - z_{m+n}),$$

puis

$$v_p = \sum_{h=1}^{h=m+n} \frac{u_h z_h^p}{f'(z_h)} \qquad (p = 0, 1, 2, \dots, 2m-1);$$

on aura alors pour le dénominateur cherché $D(z)$ l'expression

$$D(z) = \begin{vmatrix} 1 & z & z^2 & \dots & z^m \\ v_0 & v_1 & v_2 & \dots & v_m \\ v_1 & v_2 & v_3 & \dots & v_{m+1} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ v_{m-1} & v_m & v_{m+1} & \dots & v_{2m-1} \end{vmatrix}.$$

Quant au numérateur cherché $N(z)$, il se déduit du dénominateur

187) Analyse alg.[100]), p. 525; Œuvres (2) 3, p. 429; voir aussi *J. Liouville*, J. math. pures appl. (1) 7 (1842), p. 361.

(au facteur $\pm u_1 u_2 \cdots u_{m+n}$ près) en remplaçant $u_1, u_2, u_3, \dots$ par $\frac{1}{u_1}, \frac{1}{u_2}, \frac{1}{u_3}, \dots$, m par $n-1$, et n par $m+1$.

Ainsi, quand $N(z)$ et $D(z)$ sont du premier degré et que pour $z = z_1, z_2, z_3$ on donne les valeurs $u = u_1, u_2, u_3$ de la fraction $u = \frac{N(z)}{D(z)}$, on a

$$u = \frac{\frac{u_2 u_3 (z - z_1)}{(z_1 - z_2)(z_1 - z_3)} + \frac{u_3 u_1 (z - z_2)}{(z_2 - z_1)(z_2 - z_3)} + \frac{u_1 u_2 (z - z_3)}{(z_3 - z_1)(z_3 - z_2)}}{\frac{u_1 (z_1 - z)}{(z_1 - z_2)(z_1 - z_3)} + \frac{u_2 (z_2 - z)}{(z_2 - z_1)(z_2 - z_3)} + \frac{u_3 (z_3 - z)}{(z_3 - z_1)(z_3 - z_2)}}.$$

Finalement, si l'on fait dans tous les cas

$$R_p = \sum_{h=1}^{h=m+n} \frac{u_h z_h^p}{(z_h - z) f'(z_h)} \qquad (p = 0, 1, 2, \dots, 2m),$$

$$w_k = \sum_{h=1}^{h=m+n} \frac{z_h^k (z_h - z) u_h}{f'(z_h)} \qquad (k = 0, 1, 2, \dots, 2m-2),$$

et que l'on désigne par $R_{\alpha,\beta}$ et $w_{\alpha,\beta}$ les expressions

$$R_{\alpha,\beta} = R_{\alpha+\beta}, \qquad (\alpha, \beta = 0, 1, 2, \dots, m),$$
$$w_{\alpha,\beta} = w_{\alpha+\beta} \qquad (\alpha, \beta = 0, 1, 2, \dots, m-1)$$

et par R, w les deux déterminants

$$R = \begin{vmatrix} R_{0,0} & R_{0,1} & \dots & R_{0,m} \\ \cdot & \cdot & \cdot & \cdot \\ R_{m,0} & R_{m,1} & \dots & R_{m,m} \end{vmatrix}, \qquad w = \begin{vmatrix} w_{0,0} & \dots & w_{0,m-1} \\ \cdot & \cdot & \cdot \\ w_{m-1,0} & \dots & w_{m-1,m-1} \end{vmatrix},$$

l'expression $-\frac{1}{f(z)} \frac{N(z)}{D(z)}$ est représentée par le quotient

$$-\frac{1}{f(z)} \frac{N(z)}{D(z)} = \frac{R}{w}.$$

C. G. J. Jacobi[188]) s'est préoccupé de savoir ce que devient la formule quand $r+1$ des quantités $z_1, z_2, \dots, z_{m+n}$ ont la même valeur a et que l'on se donne, pour $z = a$, la valeur de u et de ses r premières dérivées.

L. Kronecker[189]) a montré qu'il y a des cas où le problème n'admet pas de solution. Soit $f_1(z)$ la fonction rationnelle entière de z, de degré $(m+n-1)$, déterminée par la condition que l'on ait $f_1(z_h) = u_h$, pour $h = 1, 2, \dots, m+n$. Formons l'algorithme du p. g. c. d. $f_r(z)$

188) J. reine angew. Math. 30 (1846), p. 127; Werke 3, Berlin 1884, p. 481.

189) Monatsb. Akad. Berlin 1878, p. 95; 1881, p. 544; Werke 2, Leipzig 1897, p. 37, 126.

des deux fonctions $f(z)$ et $f_1(z)$. On aura pour $\lambda = 1, 2, \ldots, r$ des relations de la forme

$$f_{\lambda-1}(z) + f_{\lambda+1}(z) = f_\lambda(z) g_\lambda(z),$$

où $g_\lambda(z)$ est le quotient de la division de $f_{\lambda-1}(z)$ par $f_\lambda(z)$ et où $f_{\lambda+1}(z)$ est le reste de cette division changé de signe; d'ailleurs

$$f_{r+1}(z) = 0, \quad f_0(z) = f(z).$$

Il en résulte (nº **4**) que, pour $\lambda = 1, 2, \ldots, r-1$, la fonction $f_{\lambda+1}(z)$ peut être mise sous la forme

$$f_{\lambda+1}(z) = f_1(z)\psi_\lambda(z) - f(z)\varphi_\lambda(z),$$

où $\varphi_\lambda(z)$ et $\psi_\lambda(z)$ sont des fonctions rationnelles entières de z. Toutes les solutions du problème de *A. L. Cauchy* (s'il y en a) sont de la forme $\frac{f_{k+1}(z)}{\psi_k(z)}$ où $f_{k+1}(z)$ et $\psi_k(z)$ n'ont aucun diviseur commun. Si l'on fixe l'indice k de façon que, m étant le degré du numérateur $N(z)$, les degrés m_k et m_{k+1} des fonctions $\psi_k(z)$ et $\psi_{k+1}(z)$ vérifient l'inégalité

$$m_k \leqq m < m_{k+1}$$

et si, pour ce choix de k, les fonctions $f_{k+1}(z)$ et $\psi_k(z)$ ont un diviseur commun, le problème de *A. L. Cauchy* n'admet pas de solution.

E. Netto a établi la formule de *A. L. Cauchy* d'une façon élémentaire, et il a déduit de cette formule des identités dont les *formules de L. Euler* (nº **23**) ne sont qu'un cas particulier[190]).

28. Le problème de Stickelberger. Soient h fonctions rationnelles entières données $\varphi_1(z), \varphi_2(z), \ldots, \varphi_h(z)$, premières entre elles deux à deux, de degrés respectivement égaux à $n_1, n_2, \ldots, n_h$, avec $n_1 + n_2 + \cdots + n_h = n$. Posons

$$\Phi = \varphi_1\varphi_2\ldots\varphi_h \text{ et } \Phi_k = \frac{\Phi}{\varphi_k} \text{ pour } k = 1, 2, \ldots, h.$$

Appelons R_k le résultant (nº **34**) des deux fonctions rationnelles entières φ_k et Φ_k. Désignons maintenant par $\psi_1(z), \psi_2(z), \ldots, \psi_h(z)$ des fonctions rationnelles entières *arbitraires*, de degré $(n-1)$. Puisque les fonctions rationnelles entières $\varphi_1(z), \varphi_2(z), \ldots, \varphi_h(z)$ sont deux à deux premières entre elles, on peut trouver, pour $k = 1, 2, \ldots, h$, des fonctions $\mathsf{X}_k(z)$, $X_k(z)$ telles que l'on ait pour un choix convenable des constantes R_k

$$R_k\psi_k(z) = \mathsf{X}_k(z)\Phi_k(z) + X_k(z)\varphi_k(z) \qquad (k = 1, 2, \ldots, h).$$

La fonction rationnelle entière de z de degré $n-1$, définie par la relation

190) Math. Ann. 42 (1893), p. 453; Z. Math. Phys. 41 (1896), p. 107.

$$\psi(z) = \sum_{k=1}^{k=h} \frac{\mathsf{X}_k(z)}{R_k}\Phi_k(z),$$

satisfait aux h congruences[191])

$$\psi(z) \equiv \psi_k(z) \pmod{\varphi_k}, \qquad (k = 1, 2, \ldots, h).$$

En d'autres termes les h fonctions

$$\psi(z) - \psi_1(z),\ \psi(z) - \psi_2(z),\ \ldots,\ \psi(z) - \psi_h(z),$$

sont respectivement divisibles par les fonctions $\varphi_1(z), \varphi_2(z), \ldots, \varphi_h(z)$.

Dans le cas où les h fonctions $\varphi_1(z), \varphi_2(z), \ldots, \varphi_h(z)$ sont toutes du premier degré on retombe sur la *formule d'interpolation de Lagrange*.

*Si l'on pose[192])

$$\psi_i(z) = A_{i0} + \frac{z-a_i}{1}A_{i1} + \cdots + \frac{(z-a_i)^{\alpha_i - 1}}{(\alpha_i - 1)!}A_{i,\alpha_i-1}$$

et

$$\varphi_i = (z - a_i)^{\alpha_i}$$

la fonction $\psi(z)$ satisfait aux conditions suivantes

$$\psi(a_i) = A_{i0},\ \psi'(a_i) = A_{i1}, \cdots\cdots \psi^{(\alpha_i - 1)}(a_i) = A_{i,\alpha_i-1} \qquad (i = 1, 2, \cdots, h);$$

la fonction $\psi(z)$ donne donc la solution *algébrique* du problème d'interpolation de *Ch. Hermite* (nº **25**).*

29. Formules de Jacobi. *Citons encore les propositions suivantes[193]). Soit

$$\varphi(z) = (z-\alpha_1)(z-\alpha_2)\ldots(z-\alpha_n).$$

Formons la fonction alternée

$$\begin{aligned} P(\alpha_1, \alpha_2, \ldots, \alpha_k) = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)&\ldots(\alpha_1 - \alpha_k) \\ (\alpha_2 - \alpha_3)&\ldots(\alpha_2 - \alpha_k) \\ &\ldots\ldots \\ &(\alpha_{k-1} - \alpha_k) \end{aligned}$$

et l'expression

$$\begin{aligned} M_{1,2,\ldots,k} = (\alpha_1 - \alpha_{k+1})&\ldots(\alpha_1 - \alpha_n) \\ (\alpha_2 - \alpha_{k+1})&\ldots(\alpha_2 - \alpha_n) \\ &\ldots\ldots \\ (\alpha_k - \alpha_{k+1})&\ldots(\alpha_k - \alpha_n). \end{aligned}$$

Si $\beta_1, \beta_2, \ldots, \beta_k$ désignent les k indices $1, 2, \ldots, k$ rangés dans un certain ordre, représentons par β le nombre des inversions de la per-

191) *L. Stickelberger,* Math. Ann. 30 (1887), p. 405.
192) *Texte de *J. Drach.**
193) *C. G. J. Jacobi,* Nachlass; Werke 3, Berlin 1884, p. 555.

mutation $\beta_1, \beta_2 \ldots, \beta_k$. Désignons par $F(\alpha_1, \alpha_2, \ldots, \alpha_k)$ une fonction rationnelle entière quelconque donnée et formons l'expression

$$\mathrm{E} = \sum \frac{\underset{1,\ldots,k}{S}\left[(-1)^\beta F(\alpha_{\beta_1}, \alpha_{\beta_2}, \ldots, \alpha_{\beta_k})\right]}{P(\alpha_1, \alpha_2, \ldots, \alpha_k) M_{1,2,\ldots,k} (z-\alpha_1)(z-\alpha_2)\ldots(z-\alpha_k)},$$

où le signe S de sommation représente une somme qui s'étend à toutes les *permutations* $\beta_1, \beta_2, \ldots, \beta_k$ des indices $1, 2, \ldots, k$, et où le signe Σ de sommation s'étend à tous les termes obtenus en remplaçant $1, 2, \ldots, k$ par une *combinaison* quelconque des indices $1, 2, \ldots, n$ pris k à k. Considérons d'autre part la fraction

$$f = \frac{(-1)^{\frac{1}{2}k(k-1)} \underset{1,\ldots,k}{S}\left[(-1)^\beta F(z_{\beta_1}, z_{\beta_2}, \ldots, z_{\beta_k})\right]}{\varphi(z_1)\varphi(z_2)\ldots\varphi(z_k)}.$$

Si l'on développe f suivant les puissances décroissantes de $z_1, z_2, \ldots, z_{k-1}$ et si l'on fait $z_k = z$, le coefficient du terme

$$\frac{1}{z_1^{k-1} z_2^{k-2} \ldots z_{k-2}^2 z_{k-1}}$$

ne peut différer de E que par une fonction rationnelle entière de z (qui peut d'ailleurs être identique à zéro). Dans la même fraction f, développée suivant les puissances décroissantes de $z_1, z_2, \ldots, z_{k-1}, z_k$, le coefficient de

$$\frac{1}{z_k^k z_1^{k-1} z_2^{k-2} \ldots z_{k-1}}$$

sera

$$\sum \frac{\underset{1,\ldots,k}{S}\left[(-1)^\beta F(\alpha_{\beta_1}, \alpha_{\beta_2}, \ldots, \alpha_{\beta_k})\right]}{P(\alpha_1, \alpha_2, \ldots, \alpha_k) M_{1,2,\ldots,k}}.$$

Soit toujours

$$\varphi(z) = (z-\alpha_1)(z-\alpha_2)\cdots(z-\alpha_n) = z^n - A_1 z^{n-1} + A_2 z^{n-2} - \cdots + (-1)^n A_n.$$

La fraction $\frac{1}{\varphi(z)}$ peut être mise sous la forme

$$\frac{1}{\varphi(z)} = \frac{1}{z^n} + \frac{C_1}{z^{n+1}} + \frac{C_2}{z^{n+2}} + \cdots;$$

les coefficients $C_1, C_2, \ldots$ de ce développement sont alors donnés par les valeurs pour $m = 1, 2, \ldots$ du déterminant

$$C_m = \begin{vmatrix} A_1 & A_2 & \ldots & A_m \\ A_0 & A_1 & \ldots & A_{m-1} \\ A_{-1} & A_0 & \ldots & A_{m-2} \\ \cdot & \cdot & \cdot & \cdot \\ A_{-m+2} & A_{-m+3} & \ldots & A_1 \end{vmatrix}$$

à la condition d'y regarder comme nul tout élément A_m à indice $m > n$ ou à indice $m < 0$.

Cela posé, l'expression

$$\sum \frac{S[\alpha_1^{q_1} \alpha_2^{q_2} \ldots \alpha_k^{q_k}]}{M_{1,2,\ldots,k}},$$

où le signe S de sommation s'étend à toutes les permutations des nombres naturels $q_1, q_2, \ldots, q_k$, et le signe Σ de sommation à toutes les combinaisons des indices $1, 2, \ldots, n$ pris k à k, est égale à la somme des déterminants qu'on déduit du déterminant

$$\begin{vmatrix} C_{q_1+k-n} & C_{q_2+k-1-n} & \ldots & C_{q_k+1-n} \\ C_{q_1+k+1-n} & C_{q_2+k-n} & \ldots & C_{q_k+2-n} \\ \cdot & \cdot & \cdot & \cdot \\ C_{q_1+2k-1-n} & C_{q_2+2k-2-n} & \ldots & C_{q_k+k-n} \end{vmatrix}$$

en permutant de toutes les manières possibles les nombres naturels $q_1, q_2, \ldots, q_k$; dans ces déterminants on devra prendre $C_0 = 1$ et remplacer par 0 les C à indices négatifs.*

30. Développement des fonctions rationnelles en séries récurrentes. Une série

$$(1) \qquad c_0 z^k + c_1 z^{k+1} + c_2 z^{k+2} + \cdots\cdot$$

ordonnée suivant les puissances croissantes de la variable z est dite *récurrente* lorsque, pour *toutes* les valeurs entières de t supérieures à un nombre naturel donné t_0, on a identiquement une relation telle que

$$(2) \qquad b_0 c_t + b_1 c_{t+1} + b_2 c_{t+2} + \cdots + b_m c_{t+m} = 0$$

où $b_0, b_1, b_2, \ldots, b_m$ sont des nombres déterminés ne dépendant pas de t. Le nombre k peut d'ailleurs être positif ou négatif.

De même une série

$$(3) \qquad \frac{c_0}{z^k} + \frac{c_1}{z^{k+1}} + \frac{c_2}{z^{k+2}} + \cdots\cdot$$

ordonnée suivant les puissances décroissantes de la variable z est dite *récurrente* lorsque, pour *toutes* les valeurs entières de t supérieures à un nombre naturel donné t_0 on a une relation telle que (2).

La relation (2) est dite *formule linéaire de récurrence* du $m^{\text{ième}}$ ordre; les nombres $b_0, b_1, b_2, \ldots, b_m$ qui y figurent forment ce qu'on appelle l'*échelle de relation* de la série récurrente.

La condition nécessaire et suffisante pour qu'une série du type (1) ou du type (3) représente une fonction rationnelle fractionnaire est que cette série soit récurrente[194]).

194) Voir *J. A. Serret,* Alg. sup.[30]) 1, p. 522/3.

En particulier, la condition nécessaire et suffisante pour que le produit d'une fonction rationnelle entière *donnée*

$$b_0 + b_1 z + b_2 z^2 + \cdots + b_m z^m$$

(où b_m n'est pas nul) par la somme d'une série

$$\frac{c_0}{z} + \frac{c_1}{z^2} + \cdots + \frac{c_{k-1}}{z^k} + \cdots\cdots$$

soit une fonction rationnelle *entière* de z, est que les équations (2) soient vérifiées pour toute valeur $t = 0, 1, 2, 3, \ldots\ldots$ de t.

Pour que la somme de la série

$$(4) \qquad \frac{c_0}{z} + \frac{c_1}{z^2} + \frac{c_2}{z^3} + \cdots + \frac{c_{k-1}}{z^k} + \cdots\cdots$$

soit égale à une fonction rationnelle dont le dénominateur (supposé sans diviseur commun avec le numérateur) soit de degré m en z (et non inférieur à m) il faut donc qu'il existe une échelle de relation

$$b_0, b_1, b_2, \ldots, b_{m-1}, b_m$$

(où b_m est différent de zéro) vérifiant la formule linéaire de récurrence du $m^{\text{ième}}$ ordre (2) pour tout entier $t \geqq 0$, mais qu'il n'existe pas de formule linéaire de récurrence du $(m-1)^{\text{ième}}$ ordre telle que

$$(5) \qquad b_0' c_t + b_0' c_{t+1} + b_2' c_{t+2} + \cdots + b_{m-1}' c_{t+m-1} = 0,$$

en sorte qu'une relation telle que (5) ne puisse être vérifiée pour tout entier $t \geqq 0$ que si l'on a

$$b_0' = 0,\ b_1' = 0,\ b_2' = 0,\ \ldots,\ b_{m-1}' = 0.$$

Pour discerner quand ces conditions sont vérifiées, posons

$$\delta_0 = c_0, \quad \delta_1 = \begin{vmatrix} c_0 & c_1 \\ c_1 & c_2 \end{vmatrix}, \quad \delta_2 = \begin{vmatrix} c_0 & c_1 & c_2 \\ c_1 & c_2 & c_3 \\ c_2 & c_3 & c_4 \end{vmatrix}, \quad \delta_3 = \begin{vmatrix} c_0 & c_1 & c_2 & c_3 \\ c_1 & c_2 & c_3 & c_4 \\ c_2 & c_3 & c_4 & c_5 \\ c_3 & c_4 & c_5 & c_6 \end{vmatrix}, \ldots,$$

et, en général pour tout nombre naturel t

$$\delta_t = \begin{vmatrix} c_0 & c_1 & \cdots & c_t \\ c_1 & c_2 & \cdots & c_{t+1} \\ \cdot & \cdot & \cdot & \cdot \\ c_t & c_{t+1} & \cdots & c_{2t} \end{vmatrix},$$

La condition nécessaire et suffisante pour l'existence d'une formule de récurrence (2) et la non-existence d'une formule de récurrence (5)

est, comme l'a montré *L. Kronecker*[195]), que δ_{m-1} soit différent de zéro, tandis que pour tout indice $t \geqq m$ on ait $\delta_t = 0$.

Si cette double condition est vérifiée on a

$$\sum_{k=1}^{k=+\infty} \frac{c_{k-1}}{z^k} = \frac{C_m(z)}{D_m(z)},$$

où $C_m(z)$ et $D_m(z)$ désignent deux fonctions rationnelles entières définies par l'équation

$$(7) \qquad \begin{vmatrix} U & -c_0 & -c_1 & \ldots -c_{m-1} \\ -c_0 & c_0 z - c_1 & c_1 z - c_2 & \ldots c_{m-1} z - c_m \\ -c_1 & c_1 z - c_2 & c_2 z - c_3 & \ldots c_m z - c_{m+1} \\ \cdot & \cdot & \cdot & \cdot \\ -c_{m-1} & c_{m-1} z - c_m & c_m z - c_{m+1} & \ldots c_{2m-2} z - c_{2m-1} \end{vmatrix} = -C_m(z) + U D_m(z),$$

où U désigne une *indéterminée*.

De l'identité (7) il résulte que le coefficient de z^m dans $D_m(z)$ est δ_{m-1}, qu'il est donc différent de zéro, en sorte que $D_m(z)$ est bien de degré m. Les coefficients des termes de degrés les plus élevés dans $C_m(z)$ peuvent être nuls. De l'identité

$$(8) \qquad C_m(z) D_{m-1}(z) - C_{m-1}(z) D_m(z) = \delta_{m-1}^2$$

il résulte que $C_m(z)$ et $D_m(z)$ n'ont aucun facteur commun.

On doit aussi à *L. Kronecker*[195]) plusieurs propositions fondamentales reposant sur des identités intéressantes et à l'aide desquelles on peut déterminer le degré du p. g. c. d. de deux fonctions rationnelles entières données.

Désignons maintenant par ν un nombre naturel quelconque inférieur à m et demandons-nous quelles sont les conditions nécessaires et suffisantes pour que deux fonctions rationnelles entières de z

$$D_m(z) = b_0 z^m \quad + b_1 z^{m-1} + \cdots + b_m,$$
$$C_m(z) = a_0 z^{m-1} + a_1 z^{m-2} + \cdots + a_{m-1}$$

aient un p. g. c. d. de degré ν. Ces conditions sont au nombre de $\nu + 1$ et si l'on développe la fraction $\frac{C_m(z)}{D_m(z)}$ en une série de la forme

$$\frac{c_0}{z} + \frac{c_1}{z^2} + \frac{c_2}{z^3} + \cdots + \frac{c_{k-1}}{z^k} + \cdots\cdots$$

195) Monatsb. Akad. Berlin 1881, p. 535; Werke[189]) 2, p. 115.

on peut exprimer ces $\nu + 1$ conditions par les ν égalités

$$\delta_{m-1} = 0, \quad \delta_{m-2} = 0, \ldots, \delta_{m-\nu} = 0$$

jointes à l'inégalité $\delta_{m-\nu-1}$ différent de 0. Si ces conditions sont vérifiées le plus grand commun diviseur est

$$C_m(z)\,\Psi_\nu - D_m(z)\,\Phi_\nu,$$

avec

$$\Psi_\nu = \begin{vmatrix} c_0 & c_1 & \ldots & c_{\nu-1} & 1 \\ c_1 & c_2 & \ldots & c_\nu & z \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ c_\nu & c_{\nu+1} & \ldots & c_{2\nu-1} & z^\nu \end{vmatrix}$$

et

$$\Phi_\nu = \begin{vmatrix} c_0 & c_1 & \ldots & c_{\nu-1} & 0 \\ c_1 & c_2 & \ldots & c_\nu & c_0 \\ c_2 & c_3 & \ldots & c_{\nu+1} & c_0 z + c_1 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ c_\nu & c_{\nu+1} & \ldots & c_{2\nu-1} & c_0 z^{\nu-1} + c_1 z^{\nu-2} + \cdots + c_{\nu-1} \end{vmatrix}.$$

*Dans le cas où l'on pose

$$C_m(z) = \frac{d}{dz} D_m(z)$$

les équations

$$\delta_{m-1} = 0, \quad \delta_{m-2} = 0, \ldots, \delta_{m-\nu} = 0$$

sont les conditions nécessaires et suffisantes pour que l'équation

$$D_m(z) = 0,$$

de degré m, ait seulement $m - \nu$ zéros *distincts* $z_1, z_2, \ldots, z_{m-\nu}$. On a alors évidemment pour chaque indice i

$$c_i = z_1^{\,i} + z_2^{\,i} + \cdots + z^{i}_{m-\nu},$$

et δ_{m-1} se réduit au discriminant (n° **44**) de $D_m(z)$. On retrouve ainsi les conditions établies directement par *L. Baur*[196]) (n° **20**).*

E. Netto[197]) a exprimé les coefficients c_λ et les déterminants δ_t en fonction des coefficients $a_0, b_0, a_1, b_1, \ldots, a_{m-1}, b_{m-1}, b_m$ des fonctions rationnelles entières $C_m(z)$, $D_m(z)$. Ainsi l'on a $b_0 c_0 = a_0$ et pour chaque indice $\nu = 1, 2, \ldots$.

$$b_0^{\,\nu+1} c_\nu = \begin{vmatrix} b_0 & b_1 & \ldots & b_{\nu-1} & b_\nu \\ 0 & b_0 & \ldots & b_{\nu-2} & b_{\nu-1} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \ldots & b_0 & b_1 \\ a_0 & a_1 & \ldots & a_{\nu-1} & a_\nu \end{vmatrix}.$$

196) *L. Baur*, Math. Ann. 50 (1898), p. 241/6; 52 (1899), p. 113/9 (Texte et note de *J. Drach*).*

197) J. reine angew. Math. 116 (1896), p. 45.

$$(-1)^{\frac{\lambda(\lambda+1)}{2}} b_0^{\,2\lambda+1} \delta_\lambda = \begin{vmatrix} b_0 & b_1 & b_2 & \ldots & b_{2\lambda} \\ 0 & b_0 & b_1 & \ldots & b_{2\lambda-1} \\ 0 & 0 & b_0 & \ldots & b_{2\lambda-2} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \ldots & b_{\lambda+1} \\ a_0 & a_1 & a_2 & \ldots & a_{2\lambda} \\ 0 & a_0 & a_1 & \ldots & a_{2\lambda-1} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \underbrace{0 \quad 0}_{} & 0 & \ldots & a_\lambda \end{vmatrix} \begin{array}{l} \left.\vphantom{\begin{matrix} a\\a\\a\\a\\a \end{matrix}}\right\} \lambda \text{ lignes} \\ \left.\vphantom{\begin{matrix} a\\a\\a\\a \end{matrix}}\right\} (\lambda+1) \text{ lignes} \end{array}$$

$(2\lambda + 1)$ colonnes

si l'on convient de remplacer b_μ par 0 pour tout indice $\mu > m$ et a_μ par 0 pour tout indice $\mu > m - 1$. Les expressions de $\Phi_\nu(z)$ et de $\Psi_\nu(z)$ au moyen de déterminants dont les éléments sont les coefficients $a_0, b_0, a_1, b_1, \ldots, a_{m-1}, b_{m-1}, b_m$ et les puissances de la variable z, s'en déduisent immédiatement.

E. Netto a également donné diverses propriétés des déterminants δ_t[198]).

31. Autres formules de Jacobi. Dans un autre ordre d'idées *C. G. J. Jacobi*[199]) a démontré des théorèmes dans le genre du théorème que voici: Le produit

$$u = \frac{1}{ax + by - t} \cdot \frac{1}{a_1 x + b_1 y - t_1}$$

peut se mettre, quand on développe la première fraction suivant les puissances croissantes de $\frac{1}{x}$ et de y et la seconde fraction suivant les puissances croissantes de x et de $\frac{1}{y}$, sous la forme

$$(ab_1 - a_1 b)u = L_\alpha + L_\beta + L_\gamma,$$

où L_α ne contient que les termes dans lesquels x et y ont des puissances négatives, L_β contient les termes où x seul a une puissance négative, L_γ ceux où y seul a une puissance négative. On a d'ailleurs

$$L_\alpha = \frac{ab_1 - a_1 b}{(ab_1 - a_1 b)x + bt_1 - b_1 t} \times \frac{ab_1 - a_1 b}{(ab_1 - a_1 b)y + a_1 t - a t_1}$$

$$L_\beta = \frac{a_1 b - ab_1}{(ab_1 - a_1 b)x + bt_1 - b_1 t} \times \frac{b}{ax + by - t}$$

$$L_\gamma = \frac{a_1 b - ab_1}{(ab_1 - a_1 b)y + a_1 t - a t_1} \times \frac{a_1}{a_1 x + b_1 y - t_1}.$$

198) Voir à ce sujet *C. G. J. Jacobi*, J. reine angew. Math. 15 (1836), p. 119; Werke[31]) 3, p. 315; *G. Frobenius*, Sitzgsb. Akad. Berlin 1894, p. 414; *E. Netto*, J. reine angew. Math. 116 (1896), p. 45; Algebra[23]) 1, p. 75 et suiv.

199) J. reine angew. Math. 5 (1830), p. 344; Werke 3, Berlin 1884, p. 67.

C. G. J. Jacobi démontre aussi des théorèmes analogues dans le cas de plus de deux variables, et en déduit des identités.

32. Interpolation dans le cas de fonctions de plusieurs variables. Une fonction rationnelle entière $f(z_1, z_2, \dots, z_m)$ de m variables $z_1, z_2, \dots, z_m$, de degré n, contient $\frac{(m+n)!}{m!\,n!}$ constantes et sera en général déterminée si l'on se donne les $\frac{(m+n)!}{m!\,n!}$ valeurs $f^{(i)}$ que doit prendre cette fonction pour $\frac{(m+n)!}{m!\,n!}$ systèmes de nombres

$$z_1 = \zeta_{1i}, \quad z_2 = \zeta_{2i}, \quad \dots, \quad z_m = \zeta_{mi}$$
$$\left(i = 1, 2, 3, \dots, \frac{(m+n)!}{m!\,n!}\right).$$

Si l'on envisage[200] le déterminant à $\frac{(m+n)!}{m!\,n!} + 1$ lignes et colonnes

$$\Delta = \begin{vmatrix} f, & 1, & z_1, & z_2, & \dots, & z_1^{\varkappa} z_2^{\lambda} z_3^{\mu} \dots, & \dots\dots \\ f^{(1)}, & 1, & \zeta_{11}, & \zeta_{21}, & \dots, & \zeta_{11}^{\varkappa} \zeta_{21}^{\lambda} \zeta_{31}^{\mu} \dots, & \dots\dots \\ f^{(2)}, & 1, & \zeta_{12}, & \zeta_{22}, & \dots, & \zeta_{12}^{\varkappa} \zeta_{22}^{\lambda} \zeta_{32}^{\mu} \dots, & \dots\dots \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{vmatrix}$$

où $\varkappa + \lambda + \mu + \cdots \leqq n$, et si l'on désigne par $\Delta_0, -\Delta_1, -\Delta_2, \dots$ les coefficients de $f, f^{(1)}, f^{(2)}, \dots$ dans le développement

$$\Delta = f\Delta_0 - f^{(1)}\Delta_1 - f^{(2)}\Delta_2 - \cdots\cdots$$

de Δ, la fonction $f(z_1, z_2, \dots, z_m)$ est déterminée univoquement quand Δ_0 est différent de zéro et l'on a alors

$$f(z_1, z_2, \dots, z_m) = f^{(1)}\frac{\Delta_1}{\Delta_0} + f^{(2)}\frac{\Delta_2}{\Delta_0} + f^{(3)}\frac{\Delta_3}{\Delta_0} + \cdots\cdots$$

Élimination.

Cas des fonctions d'une variable.

33. Méthode de l'algorithme d'Euclide. Etant données deux fonctions rationnelles entières

$$f(z) = a_0 z^n + a_1 z^{n-1} + a_2 z^{n-2} + \cdots + a_n,$$
$$\varphi(z) = b_0 z^\nu + b_1 z^{\nu-1} + b_2 z^{\nu-2} + \cdots + b_\nu,$$

à coefficients quelconques, a_0 et b_0 étant toutefois supposés différents de zéro, on peut se proposer de rechercher les relations qui doivent exister entre les coefficients $a_0, a_1, a_2, \dots, a_n, b_0, b_1, b_2, \dots, b_\nu$ pour que les deux fonctions $f(z)$ et $\varphi(z)$ aient un diviseur commun de degré

200) *E. Netto,* Algebra [27] 2, p. 30/1.

donné q. Ces relations sont les mêmes que celles qui doivent exister pour que les deux équations $f(z) = 0$, $\varphi(z) = 0$ aient q racines communes; mais en formulant le problème comme on vient de le faire en faisant intervenir les fonctions $f(z)$ et $\varphi(z)$ au lieu des équations $f(z) = 0$ et $\varphi(z) = 0$, on a l'avantage de pouvoir si l'on veut se passer complètement du théorème fondamental de l'Algèbre, aussi bien dans l'énoncé que dans la solution du problème.

On peut trouver les relations cherchées en effectuant les divisions successives qui conduisent au plus grand commun diviseur de $f(z)$ et $\varphi(z)$. Lorsque dans *l'algorithme d'Euclide* on est arrivé à un reste de degré $(q-1)$, on écrit qu'il est identiquement nul.

Le cas le plus important est celui où $q = 1$. Il existe alors entre les coefficients $a_0, a_1, a_2, \dots, a_n, b_0, b_1, b_2, \dots, b_\nu$ une seule relation qui exprime que $f(z)$ et $\varphi(z)$ ont un diviseur commun du premier degré.

L'*opération* par laquelle on déduit des deux fonctions $f(z)$ et $\varphi(z)$ la condition pour que ces deux fonctions aient un diviseur commun s'appelle *élimination* de z entre les fonctions $f(z)$ et $\varphi(z)$, ou entre les équations $f(z) = 0$ et $\varphi(z) = 0$.

Lorsque, sans spécifier le degré q du diviseur commun que doivent avoir $f(z)$ et $\varphi(z)$, on demande seulement la condition pour que $f(z)$ et $\varphi(z)$ aient un diviseur commun, on obtient évidemment, en appliquant le même procédé, la relation unique qui exprime que $f(z)$ et $\varphi(z)$ ont un diviseur commun du premier degré[201].

*Cette méthode a déjà été utilisée dès 1585 par *S. Stevin*[202] pour trouver le p. g. c. d. d'une fonction entière du second degré et d'une fonction entière du troisième degré. Elle a été aussi employée par *G. W. Leibniz*[203] en 1683; pour déterminer une racine commune de deux équations du cinquième degré

$$f(x) = 0, \quad \varphi(x) = 0$$

il forme l'expression du p. g. c. d. des deux fonctions entières du

201) Cf. *J. J. Bret,* J. Ec. polyt. (1) cah. 15 (1809), p. 162; *N. H. Abel,* Ann. math. pures appl. 17 (1826/7), p. 204; Œuvres, éd. *L. Sylow* et *S. Lie* 1, Christiania 1881, p. 212; *M. Bloch*, Diss. Giessen (éd. Berlin) 1892.

202) *Voir *S. Stevin,* Œuvres math., éd. *A. Girard* 1, Leyde 1634, p. 56.*

203) *Brouillon d'une lettre que *G. W. Leibniz* a écrite vers le 1er juillet 1683 à *E. W. von Tschirnhausen*, mais qui n'a jamais été expédiée [Der Briefwechsel von *G. W. Leibniz* mit Mathematikern, éd. *C. I. Gerhardt* 1, Berlin 1899, p. 447/8]. *M. Rolle* [Traité d'Algèbre, Paris 1690, p. 175/6] a montré comment on peut utiliser *l'algorithme d'Euclide* pour trouver le p. g. c. d. de deux fonctions rationnelles entières mais sans se préoccuper de l'opération d'élimination proprement dite.*

cinquième degré $f(x)$ et $\varphi(x)$. On a attribué cette méthode à *J. P. de Gua*[204]) quoique ce géomètre n'en ait fait usage que bien après *S. Stevin* et *G. W. Leibniz*.*

34. Méthode des fonctions symétriques. La relation qui existe entre les coefficients $a_0, a_1, \ldots, a_n, b_0, b_1, \ldots, b_\nu$ lorsque $f(z)$ et $\varphi(z)$ ont un diviseur commun peut aussi être trouvée par la *méthode des fonctions symétriques.*

Dans cette méthode les zéros des deux fonctions envisagées vont intervenir, au début du moins.

Si $\alpha_1, \alpha_2, \ldots, \alpha_n$ désignent les zéros de la fonction rationnelle entière $f(z)$, et si $\beta_1, \beta_2, \ldots, \beta_\nu$ désignent les zéros de la fonction rationnelle entière $\varphi(z)$, on appelle *résultant*[205]) des deux fonctions $f(z)$ et $\varphi(z)$ [à proprement parler *résultant de l'élimination* de z entre les deux équations $f(z) = 0$, $\varphi(z) = 0$] l'expression

$$\begin{aligned} R(f, \varphi) = a_0^\nu b_0^n (\alpha_1 - \beta_1)(\alpha_1 - \beta_2) \cdots (\alpha_1 - \beta_\nu) \\ (\alpha_2 - \beta_1)(\alpha_2 - \beta_2) \cdots (\alpha_2 - \beta_\nu) \\ \cdots\cdots\cdots\cdots \\ (\alpha_n - \beta_1)(\alpha_n - \beta_2) \cdots (\alpha_n - \beta_\nu), \end{aligned}$$

que l'on peut aussi mettre sous la forme

$$\begin{aligned} R(f, \varphi) &= (-1)^{n\nu} b_0^n f(\beta_1) f(\beta_2) \cdots f(\beta_\nu) \\ &= a_0^\nu \varphi(\alpha_1)\varphi(\alpha_2) \cdots \varphi(\alpha_n) = (-1)^{n\nu} R(\varphi, f). \end{aligned}$$

Si $f(z)$ et $\varphi(z)$ sont du second degré, en sorte que

$$f(z) = a_0 z^2 + a_1 z + a_2,$$
$$\varphi(z) = b_0 z^2 + b_1 z + b_2,$$

on a, en particulier,

$$\begin{aligned} R(f, \varphi) &= b_0^2 f(\beta_1) f(\beta_2) = a_0^2 \varphi(\alpha_1)\varphi(\alpha_2) \\ &= (a_0 b_2 - a_2 b_0)^2 - (a_0 b_1 - a_1 b_0)(a_1 b_2 - a_2 b_1). \end{aligned}$$

Le résultant R des deux fonctions $f(z)$ et $\varphi(z)$ est toujours une fonction symétrique des racines $\alpha_1, \alpha_2, \ldots, \alpha_n$ de l'équation $f(z) = 0$ et s'exprime donc par une fonction rationnelle, entière et homogène, de degré ν, des coefficients de la fonction $f(z)$; ce même résultant R est aussi une fonction symétrique des racines $\beta_1, \beta_2, \ldots, \beta_\nu$ de l'équation

204) *Voir *J. P. de Gua,* Usage de l'analyse de Descartes, Paris 1740, p. 60, 351/2 (Texte et notes 202/4 de *G. Eneström*).*

205) **E. Bézout* [Hist. Acad. sc. Paris 1764, H. p. 89] dit de ce résultant égalé à zéro qu'il est *l'équation résultante* de l'évanouissement d'une inconnue [cf. Hist. Acad. sc. Paris M. p. 290, 301].*

$\varphi(z) = 0$ et s'exprime donc par une fonction rationnelle, entière et homogène, de degré n, des coefficients de la fonction $\varphi(z)$. On a donc, d'après la formule d'homogénéité, les deux relations

$$a_0 \frac{\partial R}{\partial a_0} + a_1 \frac{\partial R}{\partial a_1} + \cdots + a_n \frac{\partial R}{\partial a_n} = \nu R,$$
$$b_0 \frac{\partial R}{\partial b_0} + b_1 \frac{\partial R}{\partial b_1} + \cdots + b_\nu \frac{\partial R}{\partial b_\nu} = n R.$$

Les coefficients de la fonction $R(f, \varphi)$ de

$$a_0, a_1, a_2, \ldots, a_n, b_0, b_1, b_2, \ldots, b_\nu$$

sont des nombres entiers qui sont entièrement déterminés dès que l'on connaît les deux nombres naturels n et ν.

La fonction $R(f, \varphi)$ de $a_0, a_1, a_2, \ldots, a_n, b_0, b_1, b_2, \ldots, b_\nu$ est *irréductible* en ce sens qu'elle ne peut être décomposée en un produit de deux fonctions rationnelles entières de $a_0, a_1, a_2, \ldots, a_n, b_0, b_1, b_2, \ldots, b_\nu$ de degrés moindres[206]).

La condition nécessaire et suffisante pour que deux fonctions rationnelles entières $f(z)$ et $\varphi(z)$ aient au moins un zéro commun est que leur résultant $R(f, \varphi)$ soit nul[207]).

Nous avons supposé dans ce qui précède a_0 et b_0 différents de zéro. Il peut arriver que ces coefficients dépendent d'un ou de plusieurs paramètres et que, pour certaines valeurs des paramètres, l'un ou l'autre s'annule. Si $a_0 = 0$ on dit que l'équation $f(z) = 0$ a une racine infinie. Si $b_0 = 0$ on dit que l'équation $\varphi(z) = 0$ a une racine infinie. Si l'on a $a_0 = b_0 = 0$ on dit que les deux équations

$$f(z) = 0, \quad \varphi(z) = 0$$

ont *une racine infinie commune.*

Dans tous les cas

$$R(f, \varphi) = 0$$

est la condition nécessaire et suffisante pour que les deux équations

$$f(z) = 0, \quad \varphi(z) = 0$$

aient une racine commune finie ou infinie.

Si les deux fonctions $f(z)$ et $\varphi(z)$ n'ont qu'un seul zéro commun, $\alpha_1 = \beta_1$ par exemple, l'une au moins des quantités $\frac{\partial R}{\partial a_n}, \frac{\partial R}{\partial b_\nu}$ sera différente de zéro et l'on aura donc l'une au moins des deux égalités

$$\alpha_1 \frac{\partial R}{\partial a_n} = \frac{\partial R}{\partial a_{n-1}}, \quad \alpha_1 \frac{\partial R}{\partial b_\nu} = \frac{\partial R}{\partial b_{\nu-1}}.$$

206) *E. Netto,* Alg.[23]) 1, p. 169.

207) Cf. *L. Euler,* Hist. Acad. Berlin 4 (1748), éd. 1750, p. 243; *G. Cramer,* Introd.[31]), p. 660.

On aura aussi l'une au moins des deux proportions[208])

$$1:\alpha_1:\alpha_1^2:\cdots:\alpha_1^n=\frac{\partial R}{\partial a_n}:\frac{\partial R}{\partial a_{n-1}}:\frac{\partial R}{\partial a_{n-2}}:\cdots:\frac{\partial R}{\partial a_0},$$

$$1:\alpha_1:\alpha_1^2:\cdots:\alpha_1^\nu=\frac{\partial R}{\partial b_\nu}:\frac{\partial R}{\partial b_{\nu-1}}:\frac{\partial R}{\partial b_{\nu-2}}:\cdots:\frac{\partial R}{\partial b_0}.$$

J. L. Lagrange[209]) donne plus généralement les conditions nécessaires et suffisantes pour que le nombre de zéros[210]) de $\varphi(z)$ qui annulent $f(z)$ soit précisément égal à μ. En supposant b_0 différent de 0, ces conditions sont

$$R=0,\quad \frac{\partial R}{\partial a_n}=0,\quad \frac{\partial^2 R}{\partial a_n^2}=0,\quad \cdots,\quad \frac{\partial^{\mu-1}R}{\partial a_n^{\mu-1}}=0,$$

avec $\dfrac{\partial^\mu R}{\partial a_n^\mu}$ différent de 0; dans ce cas, l'équation aux racines communes s'obtient en développant l'expression symbolique qui figure dans le premier membre de l'équation symbolique

$$\left(x\frac{\partial}{\partial a_n}-\frac{\partial}{\partial a_{n-1}}\right)^\mu R=0$$

et en remplaçant dans ce développement, pour $h=0,1,2,\ldots,\mu$, le symbole

$$x^h\left(\frac{\partial}{\partial a_n}\right)^h\left(\frac{\partial}{\partial a_{n-1}}\right)^{\mu-h}R$$

par l'expression

$$x^h\frac{\partial^\mu R}{\partial a_n^h\,\partial a_{n-1}^{\mu-h}}.$$

Si $\varphi(z)$ est le produit de deux fonctions $g(z)$, $h(z)$, en désignant par $R[f,\varphi]$ le résultant de f et de φ, on a

$$R[f,gh]=R[f,g]R[f,h].$$

Pour $n=\nu$, on a

208) *F. J. Richelot,* J. reine angew. Math. 21 (1840), p. 228.

209) *J. L. Lagrange,* Nouv. Mém. Acad. Berlin 1 (1770), éd. 1772, p. 153; Œuvres 3, Paris 1869, p. 229. Voir aussi l'exposé plus symétrique et plus général de *J. J. Sylvester,* Cambr. Dublin math. J. 8 (1853), p. 64; Papers 1, Cambr. 1905, p. 403.

210) *Ici toute racine commune des deux équations $f(z)=0$ et $\varphi(z)=0$ est à compter autant de fois que l'indique son ordre de multiplicité dans l'équation $\varphi(z)=0$; son ordre de multiplicité dans l'équation $f(z)=0$ n'importe pas. Ainsi pour

$$f(z)=z^2(z-7)^2(z+8),\quad \varphi(z)=z^2(z-7)(z-9)$$

μ est égal à 3; pour

$$f(z)=z^2(z-7)(z-9),\quad \varphi(z)=z^2(z-7)^2(z+8)$$

μ est égal à 4 (Note de *J. Kürschák*).*

$$R(\lambda f+\mu g,\ \lambda' f+\mu' g)=(\lambda\mu'-\mu\lambda')^n R(f,g),$$

$\lambda,\mu,\lambda',\mu'$ étant des constantes[211]).

En désignant par $f(z)$, $\varphi(z)$, $\psi(z)$ trois fonctions rationnelles entières de z, de degrés respectivement égaux à n, ν, q, *P. Gordan*[212]) a démontré la formule

$$R[f+\varphi\psi,\varphi]=R[f,\varphi]$$

sous la restriction que l'on ait $n>\nu$ et $n-\nu-q\geqq 0$. D'autre part, pour $n-\nu-q<0$, *O. Biermann*[213]) a établi la relation

$$R[f+\varphi\psi,\varphi]=(-1)^{\nu(\nu+q-n)}b_0^{\nu+q-n}R[f,\varphi]$$

où b_0 désigne le coefficient de x^ν dans $\varphi(x)$.

35. Méthode d'Euler. On peut mettre de diverses manières le résultant R de deux fonctions rationnelles entières $f(z)$, $\varphi(z)$ et les conditions pour que $f(z)$ et $\varphi(z)$ aient un p. g. c. d. de degré donné sous forme de déterminants dont les éléments sont des fonctions rationnelles entières des coefficients de $f(z)$ et de $\varphi(z)$.

La méthode dite[214]) *méthode d'Euler*[215]) conduit au résultat suivant:

Supposons que les deux fonctions rationnelles entières $f(z)$ et $\varphi(z)$ de degré n et ν aient un plus grand commun diviseur $F(z)$ de degré q et soient $f_1(z)$ et $\varphi_1(z)$ les fonctions rationnelles entières respectivement de degré $n-q$ et $\nu-q$ que l'on obtient en divisant $f(z)$ et $\varphi(z)$ par $F(z)$. Des égalités

$$f(z)=f_1(z)F(z),\qquad \varphi(z)=\varphi_1(z)F(z)$$

on déduit immédiatement que l'on a identiquement[216])

$$f(z)\varphi_1(z)-\varphi(z)f_1(z)=0.$$

En écrivant que l'identité a lieu, quel que soit z, on obtient des

211) *C. G. J. Jacobi,* J. reine angew. Math. 15 (1836), p. 101; Werke[31]) 3, p. 295.

212) Invar.[106]) 1, p. 151.

213) Monatsh. Math. Phys. 2 (1891), p. 143. Voir aussi *M. W. Haskell,* Bull. New-York math. Soc. 1 (1891/2), p. 223.

214) *En réalité cette méthode a déjà été employée par *G. W. Leibniz* dans une note manuscrite [cf. Werke, éd. *C. I. Gerhardt,* Math. Schr. 7, Halle 1863, p. 5/7] dont la date est incertaine mais non antérieure à 1678 ni postérieure à 1693 [cf. la lettre de *G. W. Leibniz* à *G. F. A. de l'Hospital* datée du 28 avril 1693; Werke, éd. *C. I. Gerhardt,* Math. Schr. 2, Berlin 1850, p. 240] (Note de *G. Eneström*).*

215) *L. Euler,* Introd.[15]) 2, n^os^ 483/5; trad. *J. B. Labey* 2, p. 266/9; voir aussi Hist. Acad. Berlin 20 (1764), éd. 1766, p. 99.

216) **L. Euler* s'est surtout attaché au cas où l'on ne spécifie pas le degré du p. g. c. d. de $f(z)$ et de $\varphi(z)$.*

équations linéaires et homogènes par rapport aux coefficients de f_1 et de φ_1 et les conditions obtenues pour que ces équations admettent une solution où les inconnues ne sont pas toutes nulles sont précisément aussi les conditions pour que les polynomes $f(z)$ et $\varphi(z)$ admettent un diviseur commun de degré q[217]. Si l'on pose

$$R = \left.\begin{vmatrix} a_0 & 0 & \dots & b_0 & 0 & \dots \\ a_1 & a_0 & \dots & b_1 & b_0 & \dots \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ a_n & a_{n-1} & \dots & & & \dots \\ 0 & a_n & \dots & & & \dots \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{vmatrix}\right\} n + \nu \text{ lignes}$$
$$\underbrace{\qquad\qquad}_{\nu \text{ colonnes}} \underbrace{\qquad\qquad}_{n \text{ colonnes}}$$

et pour $k = 1, 2, 3, \dots$

$$R_k = \left.\begin{vmatrix} a_0 & 0 & \dots & b_0 & 0 & \dots \\ a_1 & a_0 & \dots & b_1 & b_0 & \dots \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ a_n & a_{n-1} & \dots & & & \dots \\ 0 & a_n & \dots & & & \dots \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{vmatrix}\right\} n + \nu - 2k \text{ lignes}$$
$$\underbrace{\qquad\qquad}_{\nu - k \text{ colonnes}} \underbrace{\qquad\qquad}_{n - k \text{ colonnes}}$$

la condition nécessaire et suffisante pour que les deux fonctions $f(z)$ et $\varphi(z)$ aient un p. g. c. d. de degré q est que l'on ait

$$R = 0,\ R_1 = 0,\ \dots,\ R_{q-1} = 0$$

avec R_q différent de zéro.

En particulier la condition nécessaire et suffisante pour que les deux fonctions $f(z)$ et $\varphi(z)$ aient un p. g. c. d. du premier degré est que l'on ait

$$R = 0$$

avec R_1 différent de zéro.

L'équation aux q racines communes est[218]

$$R_q z^q + R_q^{(1)} z^{q-1} + \cdots + R_q^{(q)} = 0,$$

217) Pour les développements donnés à la *méthode d'Euler*, cf. **Ch. Biehler*, Nouv. Ann. math. (3) 6 (1887), p. 67*; *W. Scheibner*, Ber. Ges. Lpz. 40 (1888), math. p. 1/13; *M. Nöther*, Sitzgsb. phys.-medic. Soc. Erlangen 27 (1895), p. 110/5; *F. Brioschi*, id. p. 116/8; *J. Lüroth*, id. p. 119.

218) *On rencontre cette formule dans divers ouvrages [voir par ex. *E. Borel* et *J. Drach*, Introd. à l'étude de la théorie des nombres d'après des conférences

si $R_q^{(i)}$ désigne le déterminant que l'on obtient en remplaçant dans le déterminant R_q les éléments de la dernière ligne par les éléments situés dans la même colonne sur la $(n + \nu - 2q + i)^{\text{ième}}$ ligne du déterminant R.

Le résultant des deux fonctions

$$f(z) = a_0 z^2 + a_1 z + a_2,$$
$$\varphi(z) = b_0 z^2 + b_1 z + b_2$$

se présente ici sous la forme

$$R = \begin{vmatrix} a_0 & 0 & b_0 & 0 \\ a_1 & a_0 & b_1 & b_0 \\ a_2 & a_1 & b_2 & b_1 \\ 0 & a_2 & 0 & b_2 \end{vmatrix}.$$

Pour $q = 1$ l'équation aux racines communes est

$$\begin{vmatrix} a_0 & b_0 \\ a_1 & b_1 \end{vmatrix} z + \begin{vmatrix} a_0 & b_0 \\ a_2 & b_2 \end{vmatrix} = 0.$$

36. Méthode de Bézout. La *méthode de Bézout* donne un déterminant d'ordre moindre que *la méthode d'Euler*. On peut la rattacher à la considération suivante qui est due elle aussi à *L. Euler*[219].

Si $f(z)$ et $\varphi(z)$ ont un diviseur commun, les deux fonctions rationnelles entières

$$b_0 f(z) - a_0 \varphi(z), \quad \frac{b_\nu f(z) - a_n \varphi(z)}{z}$$

ont le même diviseur; mais elles sont toutes deux de degré $\leqq n - 1$ si $n \geqq \nu$ ou de degré $\leqq \nu - 1$ si $n \leqq \nu$. La recherche du résultant $R(f, \varphi)$ des deux fonctions $f(z)$ et $\varphi(z)$ se ramène donc à celle du résultant de deux fonctions rationnelles entières de degrés n_1, ν_1 où, si $n_1 \geqq \nu_1$, n_1 est plus petit que n tandis que, si $n_1 \leqq \nu_1$, ν_1 est plus petit que ν. On parvient ainsi de proche en proche à ramener la recherche du résultant $R(f, \varphi)$ à celle du résultant de deux fonctions rationnelles entières dont l'une au moins est du premier degré en z. Mais on peut introduire ainsi des facteurs étrangers; ce procédé de *L. Euler* ne constitue donc pas une méthode directe de formation du résultant lui-même; aussi ne qualifierons nous pas ici ce procédé

de *J. Tannery*, Paris 1895, p. 199]. Elle est d'ailleurs une conséquence immédiate de celle donnée par *L. Heffter*, Math. Ann. 54 (1901), p. 544. Voir aussi *H. Vogt*, Revue math. spéc. 7 (1902/4), p. 105.*

219) Introd.[15] 2, n^os^ 474/82; trad. *J. B. Labey* 2, p. 254/65; Hist. Acad. Berlin 20 (1764), éd. 1766, p. 96.

du nom de *méthode*, quoique *L. Euler* se soit servi lui-même de ce mot pour le qualifier, afin de pouvoir réserver le nom de *méthode d'Euler* à la méthode du n° **35**.

E. Bézout[220]) a développé le procédé de *L. Euler* et a montré comment on peut se débarrasser des facteurs étrangers. Il a, à cet effet, ramené la formation du résultant $R(f, \varphi)$ au moyen des coefficients de $f(z)$ et de $\varphi(z)$ à un problème d'élimination entre équations *linéaires*.

*Pour $n = \nu$, il forme successivement les équations

$$a_0\varphi - b_0 f = 0,$$
$$(a_0 z + a_1)\varphi - (b_0 z + b_1) f = 0,$$
$$\cdots\cdots\cdots\cdots$$

et en général, pour $\alpha = 0, 1, 2, \ldots, n-1$,

$$f_\alpha \varphi - \varphi_\alpha f = 0,$$

où l'on a posé, pour abréger,

$$f_\alpha = a_0 z^\alpha + a_1 z^{\alpha-1} + \cdots + a_\alpha, \quad \varphi_\alpha = b_0 z^\alpha + b_1 z^{\alpha-1} + \cdots + b_\alpha;$$

il élimine ensuite entre ces n équations les puissances $z, z^2, \ldots, z^{n-1}$ envisagées comme $n-1$ inconnues distinctes.

E. Bézout[221]) aborde aussi le cas où les degrés n, ν des deux fonctions $f(z)$ et $\varphi(z)$ sont inégaux. Si $n > \nu$, il forme successivement les équations

$$a_0 z^{n-\nu}\varphi - b_0 f = 0,$$
$$(a_0 z + a_1) z^{n-\nu}\varphi - (b_0 z + b_1) f = 0,$$
$$\cdots\cdots\cdots\cdots$$

et parvient ainsi de nouveau à n équations linéaires à $n-1$ inconnues $z, z^2, \ldots, z^{n-1}$. Sa méthode a été perfectionnée par *A. L. Cauchy*[222]).

Pour trouver le résultant de deux fonctions $f(z)$ et $\varphi(z)$ de degrés n, ν, où $n \geqq \nu$, on cherche à former des combinaisons de ces deux fonctions dans lesquelles le plus haut exposant de z est $\leqq n-1$. A cet effet on forme d'abord, pour $s = 1, 2, \ldots, n-\nu$, les équations

$$(1) \qquad z^{s-1}\varphi(z) = b_0 z^{\nu+s-1} + b_1 z^{\nu+s-2} + \cdots + b_\nu z^{s-1} = 0;$$

220) Hist. Acad. sc. Paris 1764, M. p. 288, 319.

221) Id. p. 322.

222) *A. L. Cauchy*, Exercices d'Analyse et de phys. math. 1 (1840), p. 385; Nouv. Ann. math. (2) 15 (1876), p. 385, 433; Œuvres (2) 11 (sous presse); *L. Painvin*, Nouv. Ann. math. (2) 13 (1874), p. 278; *H. Lemonnier*, C. R. Acad. sc. Paris 80 (1875), p. 111, 112;* *N. von Szüts*, Monatsh. Math. Phys. 9 (1898), p. 34; *H. Weber*, Alg.[24]) 1, p. 185; trad. *J. Griess*, p. 187.

ensuite on forme, au moyen des fonctions

$$f_s(z) = a_0 z^s + a_1 z^{s-1} + \cdots + a_s,$$
$$\varphi_s(z) = b_0 z^s + b_1 z^{s-1} + \cdots + b_s,$$

les équations

$$(2) \qquad \varphi(z)\cdot f_{s-1}(z) - f(z)\cdot\varphi_{\nu-n+s-1}(z) = 0$$

pour $s = n-\nu+1, n-\nu+2, \cdots, n$. Si, pour la commodité de l'écriture, on convient de désigner par A_{ik} le coefficient de z^{n-i} dans la $k^{\text{ième}}$ des n équations (1) et (2), ces équations s'écriront

$$0 = A_{1k} z^{n-1} + A_{2k} z^{n-2} + \cdots + A_{nk} \qquad (k = 1, 2, \ldots, n),$$

où quelques-uns des A_{ik} sont nuls. Le déterminant

$$R = \begin{vmatrix} A_{11} & A_{21} & \ldots & A_{n1} \\ A_{12} & A_{22} & \ldots & A_{n2} \\ \ldots & \ldots & \ldots & \ldots \\ A_{1n} & A_{2n} & \ldots & A_{nn} \end{vmatrix}$$

est le résultant cherché des deux fonctions $f(z)$ et $\varphi(z)$.

C'est à ce déterminant que l'on donne d'après *J. J. Sylvester*[223]) le nom de *bézoutiant* ou *bézoutien*.

Si les deux fonctions $f(z)$ et $\varphi(z)$ ont un diviseur commun de degré $n-r$, tous les mineurs du déterminant R de degré $r+1$ sont nuls, et réciproquement. Ainsi en posant

$$R_r = \begin{vmatrix} A_{11} & \ldots & A_{r1} \\ \ldots & \ldots & \ldots \\ A_{1r} & \ldots & A_{rr} \end{vmatrix},$$

les conditions nécessaires et suffisantes pour que les fonctions $f(z)$ et $\varphi(z)$ aient un diviseur commun de degré $n-r$ sont

$$R_n = R_{n-1} = \cdots = R_{r+1} = 0, \quad \text{avec } R_r \text{ différent de } 0.$$

Le plus grand commun diviseur des fonctions rationnelles entières $f(z)$ et $\varphi(z)$ s'obtient alors en développant le déterminant

$$T_r = \begin{vmatrix} A_{1,1} & A_{2,1} & \ldots & A_{r-1,1} & A_{r,1} z^{n-r} + A_{r+1,1} z^{n-r-1} + \cdots + A_{n,1} \\ A_{1,2} & A_{2,2} & \ldots & A_{r-1,2} & A_{r,2} z^{n-r} + A_{r+1,2} z^{n-r-1} + \cdots + A_{n,2} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ A_{1,r} & A_{2,r} & \ldots & A_{r-1,r} & A_{r,r} z^{n-r} + A_{r+1,r} z^{n-r-1} + \cdots + A_{n,r} \end{vmatrix}.$$

37. Mémoire de Jacobi. Remarque de Cayley. Avant *A. L. Cauchy* la méthode de *E. Bézout* avait été approfondie par *C. G. J. Jacobi*[224]); c'est d'ailleurs *C. G. J. Jacobi* qui, le premier, a mis sous

223) Philos. Trans. London 143 (1853), p. 408, 516.

224) J. reine angew. Math. 15 (1836), p. 101; Werke[31]) 3, p. 295.

la forme d'un déterminant la condition que $f(z)$ et $\varphi(z)$ aient un diviseur commun.

Soient

$$f(z) = a_0 z^n + a_1 z^{n-1} + \cdots + a_n = 0,$$
$$\varphi(z) = b_0 z^n + b_1 z^{n-1} + \cdots + b_n = 0$$

deux équations algébriques de même degré n; désignons, pour $k = 0, 1, 2, \ldots, n-1$, par m_k la différence

$$m_k = (a_0 z^{n-k-1} + a_1 z^{n-k-2} + \cdots + a_{n-k-1})\varphi(z)$$
$$- (b_0 z^{n-k-1} + b_1 z^{n-k-2} + \cdots + b_{n-k+1}) f(z),$$

ordonnons m_k par rapport aux puissances croissantes de z et soit alors α_{hk} le coefficient de z^h en sorte que

(1) $$m_k = \alpha_{0,k} + \alpha_{1,k} z + \cdots + \alpha_{n-1,k} z^{n-1}.$$

On voit immédiatement que les fonctions rationnelles entières $\alpha_{h,k}$ des coefficients a et b de $f(z)$ et $\varphi(z)$ vérifient les égalités

$$\alpha_{h,k} = \alpha_{k,h} \qquad (h, k = 0, 1, 2, \ldots, n-1).$$

D'ailleurs on a identiquement

$$m_0 + m_1 z + \cdots + m_{n-1} z^{n-1} = \varphi(z)\frac{\partial f}{\partial z} - f(z)\frac{\partial \varphi}{\partial z} = \sum \alpha_{hk} z^{h+k},$$

où la somme est étendue à $h = 0, 1, 2, \ldots, n-1$ et à $k = 0, 1, 2, \ldots, n-1$.

Désignons par L le déterminant

$$L = \begin{vmatrix} \alpha_{0,0} & \alpha_{1,0} & \cdots & \alpha_{n-1,0} \\ \alpha_{0,1} & \alpha_{1,1} & \cdots & \alpha_{n-1,1} \\ \cdot & \cdot & \cdot & \cdot \\ \alpha_{0,n-1} & \alpha_{1,n-1} & \cdots & \alpha_{n-1,n-1} \end{vmatrix};$$

en résolvant par rapport à $z^0, z^1, \ldots, z^{n-1}$ les équations (1) on obtient des relations de la forme

(2) $$L z^k = \sum_{h=0}^{n-1} A_{kh} m_h \quad (k = 0, 1, 2, \ldots, n-1),$$

où les A_{kh} s'expriment aisément au moyen des α_{hk}. On a d'ailleurs $A_{h,k} = A_{h',k'}$ si $h + k = h' + k'$, de sorte que l'on pourra poser

$$A_{h,k} = A_{h+k}.$$

Ceci posé, si $f(z)$ et $\varphi(z)$ ont un facteur commun, le déterminant L est nul et la racine commune des deux équations $f(z) = 0$, $\varphi(z) = 0$ satisfait aux égalités

$$\frac{1}{A_0} = \frac{z}{A_1} = \frac{z^2}{A_2} = \cdots = \frac{z^{2n-2}}{A_{2n-2}}.$$

On a aussi, pour $h = 0, 1, 2, \ldots, n-2$, les deux systèmes d'identités

$$a_0 A_h + a_1 A_{h+1} + \cdots + a_n A_{h+n} = 0;$$
$$b_0 A_h + b_1 A_{h+1} + \cdots + b_n A_{h+n} = 0.$$

C. G. J. Jacobi en a déduit des identités de la forme

$$M_r f(z) + N_r \varphi(z) = L z^r \qquad (r = 0, 1, 2, \ldots, 2n-1);$$

il donne les expressions de M_r et de N_r; ce sont des fonctions de z entre lesquelles il indique aussi diverses relations; les suivantes,

$$A_{r+1} z M_r - (A_{r+1} + A_r z) M_{r+1} + A_r M_{r+2} = 0,$$
$$A_{r+1} z N_r - (A_{r+1} + A_r z) N_{r+1} + A_r N_{r+2} = 0,$$

permettent de calculer ces fonctions M_r et N_r de proche en proche.

C. G. J. Jacobi a aussi indiqué une méthode pour calculer les fonctions m_r; il s'est occupé des relations entre les coefficients $\alpha_{r,s}$; enfin il s'est servi de ces coefficients pour réduire la fonction rationnelle $\frac{f(z)}{\varphi(z)}$ en fraction continue.

G. Rosenhain [225]) a étendu la méthode de *C. G. J. Jacobi* au cas où les deux équations algébriques $f(z) = 0$, $\varphi(z) = 0$ n'ont pas le même degré; dans ce cas le résultant se présente avec un facteur étranger; *G. Rosenhain* a déterminé ce facteur.

A. Cayley [226]) a fait la remarque suivante: si $f(z)$ et $\varphi(z)$ sont deux fonctions rationnelles entières de z, toutes deux de degré n et que l'on envisage le quotient de l'expression $f(x)\varphi(y) - f(y)\varphi(x)$ par la différence $x - y$, ce quotient sera une fonction rationnelle entière de degré $n-1$ par rapport à chacune des deux variables; si l'on pose

$$\frac{f(x)\varphi(y) - f(y)\varphi(x)}{x - y} = \sum_{i=1}^{i=n} \sum_{k=1}^{k=n} A_{ik} x^i y^k,$$

le déterminant

$$L = \begin{vmatrix} A_{1,1} & A_{1,2} & \cdots & A_{1,n} \\ A_{2,1} & A_{2,2} & \cdots & A_{2,n} \\ \cdot & \cdot & \cdot & \cdot \\ A_{n,1} & A_{n,2} & \cdots & A_{n,n} \end{vmatrix}$$

est le *résultant de Bézout* (le bézoutien).

---

225) J. reine angew. Math. 28 (1844), p. 268.

226) J. reine angew. Math. 53 (1857), p. 366 [1855]; Papers 4, Cambr. 1891, p. 38. Voir à ce sujet *C. W. Borchardt*, J. reine angew. Math. 53 (1857), p. 367; Werke, Berlin 1888, p. 473. Voir encore *L. Schendel*, Z. Math. Phys. 38 (1893), p. 87.

38. Méthode dialytique de Sylvester. Cette méthode d'élimination de la variable z entre les deux équations algébriques

$$f(z) = 0, \quad \varphi(z) = 0$$

de degrés n et ν consiste essentiellement à former les $n + \nu$ équations

$$f(z) = 0,\ zf(z) = 0,\ z^2 f(z) = 0,\ \ldots,\ z^{\nu-1} f(z) = 0,$$
$$\varphi(z) = 0,\ z\varphi(z) = 0,\ z^2\varphi(z) = 0,\ \ldots,\ z^{n-1}\varphi(z) = 0,$$

et à les envisager comme $n + \nu$ équations linéaires en z^1, z^2, $\ldots$, $z^{n+\nu-1}$.

Si entre ces équations linéaires on élimine $z, z^2, \ldots, z^{n+\nu-1}$, on obtient un déterminant T qui est encore le résultant. Ce déterminant se présente sous la forme

$$T = \left.\underbrace{\begin{vmatrix} a_0 & a_1 & a_2 & \ldots \\ 0 & a_0 & a_1 & \ldots \\ . & . & . & . \\ b_0 & b_1 & b_2 & \ldots \\ 0 & b_0 & b_1 & \ldots \\ . & . & . & . \end{vmatrix}}_{n+\nu \text{ colonnes}}\right\} n + \nu \text{ lignes}$$

c'est le déterminant R obtenu par la *méthode d'Euler* (n° **35**), mais ce déterminant est écrit autrement.

J. J. Sylvester a appelé *dialytique* cette méthode parce qu'elle dissocie les puissances des variables.

$_*$P. de Fermat[227]) avait déjà appliqué un procédé qui est au fond la *méthode dialytique*. Si n et ν sont inégaux convenons de désigner par n le plus grand de ces deux nombres naturels. On mettra alors les équations $f(z) = 0$, $\varphi(z) = 0$ sous la forme

$$(1) \qquad a_0 z^n + a_1 z^{n-1} + \cdots + a_{n-1} z = -a_n,$$
$$(2) \qquad -b_\nu = b_0 z^\nu + b_1 z^{\nu-1} + \cdots + b_{\nu-1} z;$$

en multipliant ces deux équations membre à membre et en divisant par z les deux membres de l'équation ainsi obtenue, on aura

$$(3) \qquad b_\nu(a_0 z^{n-1} + \cdots + a_{n-1}) = a_n(b_0 z^{\nu-1} + \cdots + b_{\nu-1}).$$

227) $_*$Novus secundarum et ulterioris ordinis radicum in analyticis usus [Œuvres, éd. *Ch. Henry* et *P. Tannery* 1, Paris 1891, p. 181/8; trad. par *P. Tannery* id. 3, Paris 1896, p. 157/63]. Ce mémoire a probablement été rédigé en 1650 [cf. Œuvres 2, Paris 1894, p. 284] mais il n'a été publié qu'en 1679. *P. de Fermat* paraît d'ailleurs avoir été en possession de sa méthode dès 1638 [cf. Œuvres 2, Paris 1894, p. 177/8] (Texte et note de *G. Eneström*).*

Le degré de l'équation (3) est inférieur à celui de l'équation (1). Si l'on remplace les équations (1) et (2) par les équations (2) et (3) on obtiendra de même une équation (4) de degré inférieur au degré le plus élevé des deux équations (2) et (3). En continuant ainsi on parviendra nécessairement à une équation de la forme

$$k_0 z = k_1;$$

la valeur $\frac{k_1}{k_0}$ substituée à z dans l'équation (1) ou dans l'équation (2) donne le résultat cherché. Or si on élimine *successivement* par la méthode dialytique z^0, z^1, z^2, $\ldots$, $z^{n+\nu-4}$ entre les équations ne contenant pas $z^{n+\nu-1}$, on effectue précisément les calculs prescrits par le *procédé de Fermat* et l'on parvient à une équation de la forme

$$k_0 z^{n+\nu-2} = k_1 z^{n+\nu-3}$$

c'est-à-dire à l'équation $k_0 z = k_1$.*

$_*$*J. Hudde*[228]) a donné un procédé analogue à celui de *P. de Fermat*. Il consiste à éliminer d'abord z^n entre les deux équations

$$z^{n-\nu}\varphi(z) = 0, \quad f(z) = 0;$$

si l'on désigne par $\psi(z) = 0$ le résultat de l'élimination, $\psi(z)$ sera de degré $n - 1$ au plus. On éliminera alors z^{n-1} entre les deux équations

$$z^{n-\nu-1}\varphi(z) = 0, \quad \psi(z) = 0;$$

et ainsi de suite. On parviendra ainsi à exprimer z en fonction des coefficients a et b de $f(z)$ et $\varphi(z)$. Ce procédé qui coïncide manifestement avec la méthode dialytique de *J. J. Sylvester* diffère de celui de *P. de Fermat* en ce que l'ordre de l'élimination des puissances de z est interverti; au lieu d'éliminer successivement z^0, z^1, z^2, $\ldots$ on élimine successivement $z^{n+\nu-1}$, $z^{n+\nu-2}$, $\ldots$

I. Newton[229]) a fait usage du procédé de *J. Hudde* pour déterminer le p. g. c. d. des deux fonctions

$$x^4 - 3ax^3 - 8a^2x^2 + 18a^3x - 8a^4,$$
$$x^3 - ax^2 - 8a^2x + 6a^3.$$

228) $_*$De reductione aequationum [2]); publ. dans *F. van Schooten* [Geom. Descartes 1, p. 422/6]. Le même procédé se trouve reproduit par *E. Bartholin*, De natura aequationum, publ. dans *F. van Schooten*, Geom. Descartes [6]) 2, Amsterdam 1659, p. 114/6] et par *J. Prestet* [Nouveaux élémens de math. 2, Paris 1689, p. 359/62].*

229) $_*$Arith. univ. [90]), Leyde 1732, p. 44/6; Opera, éd. *S Horsley* 1, Londres 1779, p. 47; trad. *N. Beaudeux* 1, Paris an X, p. 58; *I. Newton* ne cite d'ailleurs pas *J. Hudde* (Texte et notes 228/9 de *G. Eneström*).*

Enfin on peut observer que la *méthode d'Euler* (n° **35**) est au fond, elle aussi, identique à la méthode dialytique. Le procédé ne diffère de ceux de *P. de Fermat* et de *J. Hudde* qu'en ceci qu'on élimine *simultanément* toutes les puissances $z^{n+\nu-1}$, $z^{n+\nu-2}$, $\ldots$, z à l'aide de multiplicateurs indéterminés.

Dans le procédé de *L. Euler* (n° **36**) qui a donné naissance à la *méthode de Bézout* l'ordre de l'élimination est le suivant:

$$z^0 \text{ et } z^{n+\nu-1},\ z^1 \text{ et } z^{n+\nu-2},\ z^2 \text{ et } z^{n+\nu-3},\ \ldots$$

mais c'est encore au fond la méthode dialytique.*

On doit à *J. J. Sylvester*[230]) un exposé très simple de cette méthode d'élimination et c'est pourquoi on l'a appelée *méthode de Sylvester*.

*Du déterminant de *J. J. Sylvester*, qu'on obtient en éliminant z entre deux fonctions rationnelles de z

$$f(z) = a_0 z^n + a_1 z^{n-1} + \cdots + a_n, \quad \varphi(z) = b_0 z^\nu + b_1 z^{\nu-1} + \cdots + b_\nu,$$

on peut déduire[231]) des identités de la forme

$$f(z)\,\Phi_{\nu-1}(z) + \varphi(z)\,F_{n-1}(z) = E_0^{(1)},$$
$$f(z)\,\Phi_{\nu-2}(z) + \varphi(z)\,F_{n-2}(z) = E_0^{(2)} + E_1^{(2)} z,$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$f(z)\,\Phi_0(z) + \varphi(z)\,F_{n-\nu}(z) = E_0^{(\nu)} + E_1^{(\nu)} z + \cdots + E_{\nu-1}^{(\nu)} z^{\nu-1};$$

dans ces identités $\Phi_i(z)$ et $F_i(z)$ désignent des fonctions entières de z, de degré i et $E_0^{(1)}$ désigne le résultant $R(f, \varphi)$ tandis que $E_0^{(2)}$, $E_1^{(2)}, \ldots, E_{\nu-1}^{(\nu)}$ se déduisent de $R(f, \varphi)$ par suppression de lignes et de colonnes. On en déduit les conditions pour que $f(z)$ et $\varphi(z)$ aient un plus grand commun diviseur de degré donné s.

L. Heffter[232]) et *H. Vogt*[233]) obtiennent encore par un autre procédé les mêmes conditions.*

Le résultant $R(f, \varphi)$ mis sous la forme du déterminant T de *J. J. Sylvester*, contient dans les ν premières lignes les coefficients a et dans les n dernières les coefficients b. Appliquant dès lors une règle

230) London Edinb. philos. mag. 16 (1840), p. 132. Voir aussi Cambr. math. J. 2 (1839/41), p. 232; Cambr. Dublin math. J. 7 (1852), p. 68; Papers 1, Cambridge 1905, p. 61, 300. *Voir encore sous la signature A. Q. G. C. un article de *A. Q. G. Craufurd*, Cambr. math. J. 2 (1841), p. 276;* *L. O. Hesse*, J. reine angew. Math. 27 (1844), p. 1; Werke, Munich 1897, p. 83.

231) *Voir par ex. *H. R. Baltzer*, Determ.[106]) (2e éd.) Leipzig 1864, p. 99; Ber. Ges. Leipzig 25 (1873), math. p. 530; *W. Kretkowski*, Prace matematyczne fizyczne (Varsovie) 2 I (1890), p. 21/32.*

232) *Math. Ann. 54 (1901), p. 541.*

233) *Revue math. spéc. 7 (1902/4), p. 105.*

donnée par *P. S. Laplace*[234]), *P. Gordan*[235]) met le résultant sous la forme d'une somme

$$\pm A_1 B_1 \pm A_2 B_2 \pm \cdots,$$

où les A_h sont des déterminants d'ordre ν formés avec les coefficients a, et les B_h des déterminants d'ordre n formés avec les coefficients b. On a ainsi une forme bilinéaire dont le déterminant a pour valeur ± 1, résultat dont *A. Hurwitz*[236]) a fait usage dans ses recherches sur la théorie des invariants (loi de réciprocité de *Ch. Hermite*).

F. J. Richelot[237]) a exposé la méthode de *J. J. Sylvester*, puis en utilisant la méthode de *L. Euler* (n° **35**) il est parvenu à la proposition suivante: Soient $f(x, y)$ et $\varphi(x, y)$ deux fonctions rationnelles entières des variables x, y, de degrés respectivement égaux à n et à ν; ordonnons-les par rapport à x, puis par rapport à y, et soient alors

$$f(x, y) = a'_m y^m + \cdots + a_0' = b_p' x^p + \cdots + b_0',$$
$$\varphi(x, y) = a''_\mu y^\mu + \cdots + a''_0 = b''_\pi x^\pi + \cdots + b''_0.$$

Soient enfin $X = 0$, $Y = 0$ les équations résultant respectivement de l'élimination de y ou de x entre les équations $f(x, y) = 0$, $\varphi(x, y) = 0$. Ceci posé, convenons de représenter par

$$(\psi)^{(\gamma, \gamma)}$$

ce que devient une fonction quelconque $\psi(x, y)$ lorsqu'on y remplace x par x_γ et y par y_γ et formons l'expression

$$\sum_\gamma x_\gamma^{\alpha-\lambda} y_\gamma^{\beta-\varkappa} \left(\frac{\dfrac{\partial X}{\partial a'_\varkappa}\dfrac{\partial Y}{\partial b''_\lambda} - \dfrac{\partial X}{\partial a''_\varkappa}\dfrac{\partial Y}{\partial b'_\lambda}}{\dfrac{\partial X}{\partial x}\dfrac{\partial Y}{\partial y}} \right)^{(\gamma, \gamma)}$$

où la somme est étendue à tous les systèmes x_γ, y_γ qui vérifient simultanément les deux équations $f(x, y) = 0$, $\varphi(x, y) = 0$; ces systèmes résultent de la résolution des équations $X = 0$, $Y = 0$. L'expression ainsi formée s'évanouit identiquement (quels que soient $\varkappa, \lambda$) pour toutes les valeurs entières de α et de β qui satisfont à la condition $\alpha + \beta + 2 < n + \nu$.

L. O. Hesse[238]) a démontré directement la coïncidence du déterminant T et du résultant $R(f, \varphi)$ obtenu par la méthode des fonctions symétriques.

234) *P. S. Laplace*, Hist. Acad. sc. Paris 1772 II, M. p. 300; Œuvres 8, Paris 1891, p. 401.

235) Math. Ann. 45 (1894), p. 405.

236) Math. Ann. 45 (1894), p. 401.

237) J. reine angew. Math. 21 (1840), p. 232.

238) Kritische Z. Chem. Phys. Math. 1858, p. 483; Werke[230]), p. 475.

C. W. Borchardt[239]) a aussi comparé avec le déterminant T le résultant obtenu par la méthode des fonctions symétriques.

$_*$H. G. Zeuthen[240]) a remarqué que si l'on forme le déterminant T par la *méthode dialytique de Sylvester*, il n'est pas démontré, par ce procédé de formation de T, que $T=0$ soit une condition *suffisante* pour que les deux équations $f=0$, $\varphi=0$ aient une racine commune[241]).*

H. R. Baltzer[242]) a établi l'identité $L=(-1)^{\frac{1}{2}n(n-1)}\,T$ pour $\nu=n$.

Si, quand n est égal à ν, on pose pour $r=0,1,2,\ldots n$,

$$T^{(r)}=\underbrace{\begin{vmatrix} a_0 & a_1 & \ldots & a_n & 0 & \ldots \\ 0 & a_0 & \ldots & a_{n-1} & a_n & \ldots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ b_0 & b_1 & \ldots & b_n & 0 & \ldots \\ 0 & b_0 & \ldots & b_{n-1} & b_n & \ldots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \end{vmatrix}}_{2n-2r \text{ colonnes}} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\end{matrix}}\right\}(n-r)\text{ lignes} \\ \left.\vphantom{\begin{matrix}a\\a\\a\end{matrix}}\right\}(n-r)\text{ lignes}\end{matrix},$$

les conditions nécessaires et suffisantes pour que les deux fonctions $f(z)$ et $\varphi(z)$ aient un diviseur commun de degré ϱ, et n'aient pas de diviseur commun de degré plus élevé, sont que l'on ait

$$T=T^{(0)}=0,\ T^{(1)}=0,\ T^{(2)}=0,\ \ldots,\ T^{(\varrho-1)}=0,$$

avec $T^{(\varrho)}$ différent de zéro.

Posons (n° **37**)

$$L^{(0)}=L$$

et pour $i=1,2,\ldots,n-1$

$$L^{(i)}=\begin{vmatrix} \alpha_{i,i}, & \alpha_{i+1,i}, & \cdots & \alpha_{n-1,i} \\ \alpha_{i,i+1}, & \alpha_{i+1,i+1}, & \cdots & \alpha_{n-1,i+1} \\ \cdot & \cdot & \cdot & \cdot \\ \alpha_{i,n-1}, & \alpha_{i+1,n-1}, & \cdots & \alpha_{n-1,n-1} \end{vmatrix}.$$

E. Netto[243]) a démontré que non seulement pour $r=0$ mais aussi

239) J. reine angew. Math. 57 (1860), p. 183; Werke[226]) 1, p. 147.

240) $_*$Tidsskrift math. Köbenhavn (Copenhague) (3) 4 (1874), p. 165.*

241) $_*$Voir aussi une remarque de *V. H. O. Madsen* [Tidsskrift math. Köbenhavn (Copenhague) (3) 5 (1875), p. 144], concernant la *méthode dialytique de Sylvester* et le procédé employé par *P. Gordan* [Verh. Ges. deutsch. Naturf. Ärzte 65, Nuremberg 1893, éd. Leipzig 1894, p. 4] pour former T par la *méthode de Sylvester*.*

242) Determ.[105]), § 11, p. 113; voir aussi l'exposé plus concis de *P. Gordan*, Invar.[106]) 1, p. 153.

243) Algebra[23]) 1, p. 160; *P. Gordan*, Sitzgsb. phys.-medic. Soc. Erlangen 37 (1905), p. 379.

pour $r=1,2,\ldots,n-1$, on a

$$T^{(r)}=(-1)^{\frac{1}{2}(n-r)(n-r-1)}L^{(r)}.$$

39. Autres expressions du résultant sous forme de déterminant. *W. Stahl*[244]) met, dans le cas où les deux fonctions rationnelles entières $f(z)$, $\varphi(z)$ sont de même degré n, le résultant $R(f,\varphi)$ de ces deux fonctions sous la forme d'un déterminant de degré $n-1$. Soient

$$f(z)=a_0z^n+a_1z^{n-1}+\cdots+a_{n-1}z+a_n,$$
$$\varphi(z)=b_0z^n+b_1z^{n-1}+\cdots+b_{n-1}z+b_n.$$

Formons $(n-1)$ fonctions linéaires indépendantes

$$f_i(z)=a_{0i}z^n+\frac{n}{1}a_{1i}z^{n-1}+\frac{n(n-1)}{1\cdot 2}a_{2i}z^{n-2}+\cdots+a_{ni}$$
$$(i=1,2,\ldots,n-1)$$

dont les n^2-1 coefficients vérifient les $2n-2$ relations

$$\left.\begin{matrix} a_na_{0i}-a_{n-1}a_{1i}+\cdots+(-1)^na_0a_{ni}=0 \\ b_na_{0i}-b_{n-1}a_{1i}+\cdots+(-1)^nb_0a_{ni}=0 \end{matrix}\right\} \quad (i=1,2,\ldots,n-1).$$

Désignons, pour $i=1,2,\ldots,n-1$, par $\alpha_{n-2,i}$ le déterminant

$$\alpha_{n-2,i}=-\begin{vmatrix} a_{n-1,i} & a_{n,1} & a_{n,2} & \cdots & a_{n,n-1} \\ a_{n-2,i} & a_{n-1,1} & a_{n-1,2} & \cdots & a_{n-1,n-1} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{0i} & a_{11} & a_{12} & \cdots & a_{1,n-1} \end{vmatrix}.$$

Appliquons $n-1$ fois l'opération

$$\Delta=\sum_{i=1}^{i=n-1}\left(a_{0i}\frac{\partial}{\partial a_{1i}}+2a_{1i}\frac{\partial}{\partial a_{2i}}+\cdots+n\,a_{n-1,i}\frac{\partial}{\partial a_{ni}}\right)$$

à la fonction $\alpha_{n-2,j}$ des coefficients a_{hj} ($h=0,1,2,\ldots n$; $j=1,2,\ldots,n-1$) et dans les résultats obtenus posons

$$\Delta\alpha_{n-2,j}=\alpha_{n-3,j},\quad \Delta^2\alpha_{n-2,j}=\Delta\alpha_{n-3,j}=2!\,\alpha_{n-4,j},\quad \ldots,$$
$$\Delta^r\alpha_{n-2,j}=r!\,\alpha_{n-2-r,j},\quad \ldots\ldots,\quad \Delta^{n-2}\alpha_{n-2,j}=(n-2)!\,\alpha_{0,j};$$

si l'on appliquait encore une fois l'opération Δ on aurait

$$\Delta^{n-1}\alpha_{n-2,j}=0.$$

On démontre que le résultant $R(f,\varphi)$ peut être mis sous la forme

$$R=\begin{vmatrix} \alpha_{0,1} & \alpha_{1,1} & \cdots & \alpha_{n-2,1} \\ \alpha_{0,2} & \alpha_{1,2} & \cdots & \alpha_{n-2,2} \\ \cdots & \cdots & \cdots & \cdots \\ \alpha_{0,n-1} & \alpha_{1,n-1} & \cdots & \alpha_{n-2,n-1} \end{vmatrix}.$$

244) Math. Ann. 35 (1890), p. 399.

Si les mineurs de degré $n-1-r$ s'annulent, les deux fonctions $f(z)$ et $\varphi(z)$ ont un diviseur de degré $r+1$ en z.

K. Bes[245]) représente le résultant des deux fonctions $f(z)$ et $\varphi(z)$ sous forme de quotient de deux déterminants que l'on peut former de diverses manières.

40. Le résultant exprimé en fonction des valeurs $f(\alpha_k)$, $\varphi(\alpha_k)$. Dans la méthode des fonctions symétriques, on forme le résultant $R(f, \varphi)$ des deux fonctions $f(z)$ et $\varphi(z)$ de degrés n et ν, au moyen des zéros de ces fonctions. *G. Rosenhain*[246]) a formé ce même résultant au moyen des valeurs de $f(z)$ et de $\varphi(z)$ pour $n+\nu$ nombres quelconques *donnés* $\alpha_1, \alpha_2, \ldots, \alpha_{n+\nu}$. Il a aussi démontré la proposition plus générale que voici:

Le résultant $R(f, \varphi)$ peut être mis sous la forme

$$R = \sum \frac{f(\alpha_1)f(\alpha_2)\cdots f(\alpha_\nu)\varphi(\alpha_{\nu+1})\varphi(\alpha_{\nu+2})\cdots\varphi(\alpha_m)}{M_{1,2,\ldots,\nu}}$$

$$= (-1)^{n\nu}\sum \frac{\varphi(\alpha_1)\varphi(\alpha_2)\cdots\varphi(\alpha_n)f(\alpha_{n+1})f(\alpha_{n+2})\cdots f(\alpha_m)}{M_{1,2,\ldots,n}}$$

où l'on a écrit, pour abréger, m au lieu de $n+\nu$ et où

$$\begin{aligned} M_{1,2,\ldots,\nu} = {} & (\alpha_1-\alpha_{\nu+1})(\alpha_2-\alpha_{\nu+1})\ldots(\alpha_\nu-\alpha_{\nu+1}) \\ & (\alpha_1-\alpha_{\nu+2})(\alpha_2-\alpha_{\nu+2})\ldots(\alpha_\nu-\alpha_{\nu+2}) \\ & \ldots\qquad\quad \ldots\qquad \ldots\qquad \ldots \\ & (\alpha_1-\alpha_m)\quad(\alpha_2-\alpha_m)\quad\ldots(\alpha_\nu-\alpha_m); \end{aligned}$$

la sommation s'étend à tous les termes obtenus en permutant les indices $1, 2, \ldots, m$ de toutes les façons possibles.

G. Rosenhain a démontré cette formule en partant de la *formule d'interpolation de Cauchy* (nº **27**). Puis il l'a démontrée directement et en a conclu la *formule de Cauchy*.

C. W. Borchardt[247]) a remarqué que dans la formule de *G. Rosenhain* les $2m$ valeurs $f(\alpha_1), \ldots, f(\alpha_m)$, $\varphi(\alpha_1), \ldots, \varphi(\alpha_m)$ ne sont pas indépendantes; $(m-1)$ d'entre elles sont déterminées par les $(m+1)$ autres. Il en résulte que cette formule ne peut servir à calculer le résultant de $f(z)$ et $\varphi(z)$ quand chacune des deux fonctions est donnée

245) Verhand. Akad. Wetensch. Amsterdam Afdeeling Natuurkunde erste Sectie (2) 6 (1897/9), mém. nº 7. Les résultats de *K. Bes* rappellent ceux de *A. Cayley* mentionnés au nº **37**; la méthode qu'il suit pour y parvenir rappelle celle de *E. Bézout* exposée au nº **36**.

246) J. reine angew. Math. 30 (1846), p. 157 [1845].

247) Monatsb. Akad. Berlin 1859, p. 376; J. reine angew. Math. 57 (1860), p. **111**; Werke[326]), p. 133.

par des valeurs interpolatoires. *C. W. Borchardt* a évité cet inconvénient au moins dans le cas où $n=\nu$; il pose dans ce cas

$$\psi(z) = (z-\alpha_0)(z-\alpha_1)\ldots(z-\alpha_n),$$

$\alpha_0, \alpha_1, \ldots, \alpha_n$ étant des nombres donnés quelconques différents; il désigne par ϖ l'expression

$$(\alpha_1-\alpha_0)^2(\alpha_2-\alpha_0)^2\ldots(\alpha_n-\alpha_0)^2(\alpha_2-\alpha_1)^2(\alpha_3-\alpha_1)^2\ldots(\alpha_n-\alpha_{n-1})^2,$$

et démontre que, si R est le résultant de $f(z)$ et de $\varphi(z)$, $\frac{(-1)^n R}{\varpi}$ peut s'exprimer simplement au moyen des $\frac{n(n+1)}{2}$ éléments

$$\frac{f(\alpha_i)\varphi(\alpha_k)-f(\alpha_k)\varphi(\alpha_i)}{\psi'(\alpha_i)\psi'(\alpha_k)(\alpha_k-\alpha_i)} \qquad (i, k = 0, 1, \ldots, n;\ i>k).$$

L. Kronecker[248]) a généralisé comme il suit ces résultats: Soit $F(z)$ une fonction entière de degré m où le coefficient de z^m est l'unité. Supposons qu'on fixe un nombre n inférieur à m et qu'on désigne par ν la différence $m-n$. Mettons, de toutes les façons possibles, $F(z)$ sous la forme d'un produit de deux facteurs, l'un $\varphi(z)$ de degré n, l'autre $\psi(z)$ de degré ν et soit alors

$$F(z) = \varphi_1(z)\psi_1(z) = \varphi_2(z)\psi_2(z) = \cdots = \varphi_\gamma(z)\psi_\gamma(z),$$

où $\gamma = C_m^n$. Désignons par $f_1, f_2, \ldots, f_\gamma$ des constantes données et par R_k le résultant de $\varphi_k(z)$ et de $\psi_k(z)$; formons enfin la fonction rationnelle entière $f(x_1, x_2, \ldots x_n)$ des variables $x_1, x_2, \ldots, x_n$,

$$f(x_1, x_2, \ldots, x_n) = \sum_{k=1}^{k=\gamma} \frac{f_k}{R_k}\,\psi_k(x_1)\psi_k(x_2)\ldots\psi_k(x_n).$$

Cette fonction $f(x_1, x_2, \ldots, x_n)$ est une fonction symétrique des variables $x_1, x_2, \ldots, x_n$, de degré ν par rapport à chacune de ces variables; elle est en outre linéaire par rapport aux γ constantes f_k. La valeur de cette fonction $f(x_1, x_2, \ldots, x_n)$ se réduit à f_k si l'on prend pour $x_1, x_2, \ldots, x_n$ les valeurs qui annulent la fonction $\varphi_k(z)$.

Cette *formule de L. Kronecker* est une généralisation de la *formule d'interpolation de Lagrange*. Elle comprend comme cas particuliers la *formule de Rosenhain* et la *formule de Borchardt*.

41. Méthode de Gordan. En se servant d'un théorème de *A. Brill*[249]), *P. Gordan*[250]) a établi ce qui suit:

248) Monatsb. Akad. Berlin 1865, p. 686; Werke[167]) 1, p. 135.

249) Math. Ann. 4 (1871), p. 530.

250) Math. Ann. 7 (1874), p. 433.

Soient

$$f(z) = a_0 z^\mu + a_1 z^{\mu-1} + \cdots + a_{\mu-1} z + a_\mu,$$
$$\varphi(z) = b_0 z^\nu + b_1 z^{\nu-1} + \cdots + b_{\nu-1} z + b_\nu,$$
$$\psi(z) = c_0 z^\varrho + c_1 z^{\varrho-1} + \cdots + c_{\varrho-1} z + c_\varrho$$

trois fonctions d'une variable z dont les degrés respectifs μ, ν, ϱ ont une somme $\mu + \nu + \varrho$ paire et qui vérifient les inégalités

$$\mu + \nu - \varrho \geqq 2, \quad \nu + \varrho - \mu \geqq 2, \quad \varrho + \mu - \nu \geqq 2.$$

Posons $N = \frac{\mu + \nu + \varrho}{2}$ et éliminons $z, z^2, \ldots, z^{N-1}$ entre les équations

$$f(z) = 0, \quad z f(z) = 0, \quad \ldots, \quad z^{N-\mu-1} f(z) = 0,$$
$$\varphi(z) = 0, \quad z\varphi(z) = 0, \quad \ldots, \quad z^{N-\nu-1}\varphi(z) = 0,$$
$$\psi(z) = 0, \quad z\psi(z) = 0, \quad \ldots, \quad z^{N-\varrho-1}\psi(z) = 0$$

dont le nombre est précisément égal à N. Le résultat de l'élimination est un déterminant que nous désignerons par S.

Si les deux fonctions $f(z)$ et $\varphi(z)$ ont plus de $\frac{\mu + \nu - \varrho}{2}$ racines communes, le déterminant S est nul *quels que soient* les coefficients $c_0, c_1, \ldots, c_\varrho$ de la fonction $\psi(z)$. Si donc on ordonne S suivant les puissances de $c_0, c_1, \ldots, c_\varrho$ et qu'on annule les coefficients des différents termes on obtient des conditions nécessaires pour que les deux fonctions $f(z)$ et $\varphi(z)$ aient un plus grand commun diviseur de degré supérieur à $\frac{\mu + \nu - \varrho}{2}$.

Le déterminant S est encore nul si les deux fonctions $f(z)$ et $\varphi(z)$ ont $\frac{\mu + \nu - \varrho}{2}$ racines communes et si l'une de ces racines communes annule la fonction $\psi(z)$.

P. Gordan utilise les résultats précédents pour déterminer le plus grand commun diviseur de deux fonctions rationnelles entières $f(z)$ et $\varphi(z)$.

42. Poids des termes du résultant. Résultant réduit. Nous avons vu que le résultant $R(f, \varphi)$ de deux fonctions rationnelles entières

$$f(z) = a_0 z^n + a_1 z^{n-1} + \cdots + a_{n-1} z + a_n,$$
$$\varphi(z) = b_0 z^\nu + b_1 z^{\nu-1} + \cdots + b_{\nu-1} z + b_\nu$$

est une fonction entière de degré n par rapport aux coefficients b_β de $\varphi(z)$ et de degré ν par rapport aux coefficients a_α de $f(z)$. C'est une somme de termes de la forme

$$A\, a_0^{h_0} a_1^{h_1} \ldots a_n^{h_n} b_0^{k_0} b_1^{k_1} \ldots b_\nu^{k_\nu} \tag{1}$$

où

$$h_0 + h_1 + \cdots + h_n = \nu,$$
$$k_0 + k_1 + \cdots + k_\nu = n.$$

Convenons d'affecter chaque coefficient a_α ou b_β d'un *poids* déterminé $p(\alpha)$ ou $q(\beta)$ et de calculer le poids d'un monome (1) par la formule

$$p(0)h_0 + p(1)h_1 + \cdots + p(n)h_n + q(0)k_0 + q(1)k_1 + \cdots + q(\nu)k_\nu.$$

Si l'on prend pour poids de chaque coefficient l'indice de ce coefficient en sorte que $p(\alpha) = \alpha$, $q(\beta) = \beta$, le résultant est isobarique (n° 7) et son poids est égal à $n\nu$.

Si l'on suppose, comme application, que chacun des coefficients $a_0, a_1, \ldots, a_n, b_0, b_1, \ldots, b_\nu$ est une fonction rationnelle entière d'un paramètre t dont le degré ne dépasse pas l'indice du coefficient, le résultant $R(f, \varphi)$ sera une fonction rationnelle entière de t dont le degré ne dépassera pas $n\nu$. Le degré de la fonction R de t atteint la valeur $n\nu$ dans le cas général où les coefficients des fonctions a_α, b_β de t sont quelconques.

W. F. Meyer[251]) a supposé que, l et λ étant des nombres naturels inférieurs à n et ν, on prenne

$$p(0) = 0, \quad p(1) = 0, \; \ldots, \; p(n-l) = 0,$$
$$p(n-l+1) = 1, \quad p(n-l+2) = 2, \ldots, p(n-1) = l-1, \quad p(n) = l;$$
$$q(0) = 0, \quad q(1) = 0, \; \ldots, \; q(\nu-\lambda) = 0,$$
$$q(\nu-\lambda+1) = 1, \quad q(\nu-\lambda+2) = 2, \ldots, q(\nu-1) = \lambda-1, \quad q(\nu) = \lambda,$$

de telle sorte qu'en posant

$$f(z) = z^{l+1} f_l(z) \;\; + g_l(z) \quad \text{avec} \quad g_l(z) = c_0 z^l \;\; + \cdots + c_l,$$
$$\varphi(z) = z^{\lambda+1}\varphi_\lambda(z) + \psi_\lambda(z) \quad \text{avec} \quad \psi_\lambda(z) = \gamma_0 z^\lambda + \cdots + \gamma_\lambda,$$

les coefficients de $\varphi_\lambda(z)$ et de $f_l(z)$ aient un poids nul et ceux de $g_l(z)$, $\psi_\lambda(z)$ un poids égal à leur indice. Dans cette hypothèse, il démontre que les termes du résultant $R(f, \varphi)$ ont un poids minimé égal à λl; l'ensemble des termes de $R(f, \varphi)$ qui ont ce poids minimé est égal à $(-1)^{\lambda(n-l)} R(g_l, \psi_\lambda) R(f_l, \varphi_\lambda)$[252]).

D'autres remarques concernant la structure du résultant $R(f, \varphi)$, dans le cas où les deux équations

$$f(z) = 0, \quad g(z) = 0$$

ont plusieurs solutions communes, ont été faites par *A. Brill*[253]).

Lorsque les coefficients a et b des fonctions $f(z)$ et $\varphi(z)$ sont quelconques, le résultant $R(f, \varphi)$ est une fonction rationnelle entière

251) Nachr. Ges. Gött. 1895, math. p. 119, 155; Acta math. 19 (1895), p. 385.
252) Cf. *E. Netto*, Nachr. Ges. Gött. 1895, math. p. 209.
253) Math. Ann. 16 (1880), p. 345 [1879].

irréductible de ces coefficients a et b[254]). Mais si les coefficients a et b sont des fonctions de certains paramètres $t, t', \ldots, u, u', \ldots$, il pourra arriver que le résultant $R(f, \varphi)$ se décompose en facteurs dont quelques-uns seront indépendants des paramètres $t, t', \ldots$, tout en contenant encore éventuellement les paramètres u, u'; *J. J. Sylvester*[255]) appelle *facteurs spéciaux* ces facteurs indépendants des paramètres $t, t', \ldots$; ces facteurs supprimés, il reste le *résultant réduit*[256]).

43. Expression du résultant dans les cas les plus simples. Le développement du résultant $R(f, \varphi)$ en fonction rationnelle entière des coefficients de $f(z)$ et de $\varphi(z)$ est laborieux; lorsque le degré de $f(z)$ et celui de $\varphi(z)$ sont tous deux égaux à 4, ce développement comprend déjà 217 termes.

I. Newton[257]) a donné le développement de $R(f, \varphi)$ dans les cas où les degrés de $f(z)$ et de $\varphi(z)$ ont respectivement les valeurs

$$(n, \nu) = (2, 2), \quad (3, 2), \quad (4, 2), \quad (3, 3).$$

E. Bézout[258]) a donné le développement de $R(f, \varphi)$ dans le cas où les degrés n et ν de $f(z)$ et de $\varphi(z)$ sont égaux à 4.

A. Cayley[259]) a donné deux méthodes pour calculer le résultant. La première, déjà employée par *G. Cramer*[260]), s'appuie sur la théorie des fonctions symétriques. La seconde utilise la forme $\sum_{(h)} \pm A_h B_h$ donnée par *P. Gordan*[261]), et dont il a été question au n° **38**. *A. Cayley* donne en particulier le résultant pour

$$(n, \nu) = (2, 2), \quad (3, 2), \quad (4, 2), \quad (3, 3), \quad (4, 3), \quad (4, 4).$$

Plus tard il donne les mêmes résultants en supposant les coefficients a, b affectés de coefficients binomiaux[262]).

254) *E. Netto*, Alg.[23]) 1, p. 169; *Gg. (J.) König*, Alg. Grössen[20]), p. 268.

255) London Edinb. philos. mag. 16 (1840), p. 132; Cambr. math. J. 2 (1839/41), p. 232; Papers 1, Cambridge 1905, p. 54, 61.

256) *A. Cayley*, J. reine angew. Math. 34 (1847), p. 30; Papers 1, Cambr. 1889, p. 337.

257) Arith. univ.[90]), Leyde 1732, p. 62/3; Opera, éd. *S. Horsley* 1, Londres 1779, p. 63/5; trad. *N. Beaudeux,* Paris an X, p. 84/6.

258) Hist. Acad. sc. Paris 1764, éd. 1767, p. 321. Pour le cas où les degrés de $f(z)$ et de $\varphi(z)$ sont égaux à 3 ou à 4 voir aussi *L. Euler*, Introd.[15]), 2, p. 261; trad. *J. B. Labey* 2, p. 260 et suiv.

259) Philos. Trans. London 147 (1857), p. 703; Quart. J. pure appl. math. 6 (1864), p. 380; Papers 2, Cambr. 1889, p. 440; 5, Cambr. 1892, p. 289.

260) Introd.[31]), p. 660.

261) Math. Ann. 45 (1894), p. 405.

262) Philos. Trans. London 158 (1868), p. 173; Proc. R. Soc. London **16** (1867/8), p. 156; Papers 6, Cambr. 1893, p. 292.

E. D. Roe[263]) utilise la même forme $\sum_{(h)} \pm A_h B_h$ dans une étude d'ensemble sur ce sujet.

F. Faà di Bruno[264]) et *G. Salmon*[265]) ont donné un tableau des résultants $R(f, \varphi)$ développés lorsque les degrés des fonctions $f(z)$ et $\varphi(z)$ sont de petits nombres. *A. Clebsch*[266]) donne le résultant $R(f, \varphi)$ sous forme de produits symboliques lorsque, le degré de $f(z)$ étant quelconque, celui de $\varphi(z)$ est égal à 2. **E. Isè*[267]) traite ce cas et aussi celui où le degré de $f(z)$ étant quelconque celui de $\varphi(z)$ est égal à 3.*

P. Gordan[268]) en partant de la théorie des invariants traite plusieurs cas déjà connus et y ajoute ceux où les degrés de $f(z)$ et de $\varphi(z)$ sont respectivement

$$(n, \nu) = (6, 2), \quad (5, 3), \quad (5, 4).$$

E. Pascal[269]) a longuement étudié le cas où le degré de $f(z)$ étant quelconque, celui de $\varphi(z)$ est égal à 3. **E. d'Ovidio*[270]) a considéré celui où les degrés de $f(z)$ et de $\varphi(z)$ sont respectivement 6 et 3; *A. Plesko*[271]) approfondit le cas où le degré de $f(z)$ étant quelconque, celui de $\varphi(z)$ est égal à 2.* Il en est de même de *E. D. Roe*[263]).

P. Gordan*[272]), en appliquant son „procédé de composition" (n° **49) à la formation du résultant de deux formes binaires f, φ de même degré, obtient une suite d'expressions faciles à évaluer et permettant d'aboutir assez rapidement à l'expression du résultant $R(f, \varphi)$ de ces deux formes quand leur degré n'est pas trop élevé.*

44. Le discriminant d'une fonction rationnelle entière d'une variable. Le résultant d'une fonction rationnelle entière

$$f(z) = a_0 z^n + a_1 z^{n-1} + \cdots + a_{n-1} z + a_n$$

263) Die Entwicklung der Sylvesterschen Determinante nach Normalformen, Diss. Erlangen (éd. Leipzig) 1898.

264) Ann. mat. pura appl. (1) 1 (1858), p. 362; Formes binaires[32]), p. 84.

265) *G. Salmon,* Alg.[165]), p. 348; trad. par *O. Chemin,* p. 500.

266) J. reine angew. Math. 58 (1861), p. 273 [1860].

267) *Giorn. mat. (1) 8 (1870), p. 1, 27.*

268) Math. Ann. 3 (1871), p. 355.

269) Giorn. mat. (1) 25 (1887), p. 257; Rendic. Accad. Napoli (2) 2 (1888), p. 67

270) *Atti Accad. Torino 28 (1892/3), p. 20.*

271) Rozpravy české Akad. 5 (1896) II, mém. n° 25; voir encore *H. S. White*, Bull. Amer. math. Soc. 1 (1894/5), p. 11.

272) **P. Gordan,* Rend. Circ. mat. Palermo 22 (1906), p. 162/3 (Texte et note de *A. Brill.*)*

et de sa dérivée

$$f'(z) = na_0 z^{n-1} + (n-1)a_1 z^{n-2} + \cdots + a_{n-1}$$

fournit, quand on l'égale à zéro, la condition nécessaire et suffisante pour que la fonction $f(z)$ ait une racine double. Ce résultant $R(f, f')$ contient a_0 en facteur et l'on est ainsi amené à envisager l'expression

$$D(f) = \frac{1}{a_0} R(f, f')$$

qui est une fonction rationnelle entière des coefficients $a_0, a_1, \cdots, a_n$ de $f(z)$ et que l'on appelle, d'après *J. J. Sylvester* [273]), le *discriminant* de $f(z)$.

C. F. Gauss [274]) l'appelle le *déterminant* de $f(z)$.

Si $\alpha_1, \alpha_2, \ldots, \alpha_n$ sont les zéros de $f(z)$ on a [275])

$$D(f) = a_0^{n-2} f'(\alpha_1) f'(\alpha_2) \ldots f'(\alpha_n) = (-1)^{\frac{1}{2}n(n-1)} a_0^{2n-2} \prod (\alpha_\lambda - \alpha_\mu)^2$$

$$(\lambda, \mu = 1, 2, \ldots, n;\ \lambda < \mu).$$

Si l'on introduit les coefficients $c_0, c_1, \ldots$ du développement de $\frac{f'(z)}{f(z)}$ suivant les puissances entières de $\frac{1}{z}$ (n° **30**)

$$\frac{f'(z)}{f(z)} = \frac{c_0}{z} + \frac{c_1}{z^2} + \cdots + \frac{c_{i-1}}{z^i} + \cdots,$$

ces coefficients seront les sommes des puissances semblables des racines, en sorte que

$$c_i = \alpha_1^{\,i} + \alpha_2^{\,i} + \cdots + \alpha_n^i;$$

A. Cayley [276]) a montré que le discriminant s'exprime au moyen de ces sommes c_i par la formule

$$D(f) = (-1)^{\frac{1}{2}n(n-1)} a_0^{2n-2}\, \mathrm{C}_n,$$

où

$$\mathrm{C}_n = \begin{vmatrix} c_0 & c_1 & \ldots & c_{n-1} \\ c_1 & c_2 & \ldots & c_n \\ \cdot & \cdot & \cdot & \cdot \\ c_{n-1} & c_n & \ldots & c_{2n-2} \end{vmatrix}.$$

Remarquons l'identité

273) London Edinb. Dublin philos. mag. (4) 2 (1851), p. 406; Papers 1, Cambr. 1905, p. 280.

274) Disq.[25]), n° 154; Werke 1, p. 122; cf. Commentat. Soc. Gott. recent. 3 (1814/5), éd. Göttingue 1816, math., mém. n° 4, p. 114; Werke 3, Göttingue 1876, p. 38.

275) *Voir *F. Joachimsthal*, J. reine angew. Math. 33 (1846), p. 371.*

276) J. math. pures appl. (1) 11 (1846), p. 297; Papers 1, Cambr. 1889, p. 306.

$$C_n = \begin{vmatrix} 1 & \alpha_1 & \alpha_1^{\,2} & \ldots & \alpha_1^{\,n-1} \\ 1 & \alpha_2 & \alpha_2^{\,2} & \ldots & \alpha_2^{\,n-1} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & \alpha_n & \alpha_n^2 & \ldots & \alpha_n^{n-1} \end{vmatrix} = \prod_{(\lambda > \mu)} (\alpha_\lambda - \alpha_\mu) \qquad (\lambda, \mu = 1, 2, \ldots, n).$$

Considérons une forme binaire

$$F(x, y) = a_0 x^n + a_1 x^{n-1} y + \cdots + a_{n-1} x y^{n-1} + a_n y^n,$$

et les deux dérivées partielles

$$F_x' = n a_0 x^{n-1} + \cdots + a_{n-1} y^{n-1},$$
$$F_y' = a_1 x^{n-1} + \cdots + n a_n y^{n-1}$$

de cette forme; formons le résultant T de ces deux dérivées partielles pour $y = 1$,

$$T = \begin{vmatrix} na_0, & (n-1)a_1, & \ldots, & a_{n-1} & , & 0, & \ldots \\ 0, & na_0 & , \ldots, & 2a_{n-2} & , & a_{n-1}, & \ldots \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ a_1, & 2a_2 & , \ldots, & na_n & , & 0, & \ldots \\ 0, & a_1 & , \ldots, & (n-1)a_{n-1}, & & na_n, & \ldots \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{vmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\end{matrix}}\right\} n-1 \text{ lignes} \\ \left.\vphantom{\begin{matrix}a\\a\\a\end{matrix}}\right\} n-1 \text{ lignes} \end{matrix}$$

$2n-2$ colonnes

On démontre que le discriminant $D(f)$ de la fonction $f(z)$ obtenue n remplaçant x par z et y par 1 dans $F(x, y)$ est égal à

$$D(f) = \frac{1}{n^{n-2}}\, T.$$

Dans cette expression de $D(f)$, le déterminant T peut d'ailleurs être remplacé par d'autres déterminants, en particulier par un déterminant de degré $n-1$ si l'on applique la méthode d'élimination de *E. Bézout* aux deux fonctions qu'on déduit de F_x', F_y' en y faisant $y = 1$.

Le discriminant $D(f)$ est une fonction rationnelle entière homogène des coefficients de $f(z)$, de degré $2n-2$. Si nous convenons de donner à chaque coefficient a_i de $f(z)$ un poids égal à $n-i$, le discriminant $D(f)$ est une fonction rationnelle entière isobarique de poids $n(n-1)$.

Si l'on fait sur les poids des coefficients les hypothèses de *W. F. Meyer* (n° **42**), de sorte qu'en posant

$$f(z) = z^{l+1} f_l(z) + g_l(z) \quad \text{avec} \quad g_l(z) = c_0 z^l + c_1 z^{l-1} + \cdots + c_l$$

les coefficients de $f_l(z)$ aient un poids nul et ceux de $g_l(z)$ un poids égal à leur indice, les termes du discriminant $D(f)$ ont un poids minimé égal à $l(l-1)$ et, comme l'a démontré *W. F. Meyer*[277]), l'ensemble des termes qui ont ce poids minimé est, abstraction faite d'un facteur numérique, égal à

$$c_0^2 D(f_l) D(g_l).$$

Si z_1 est un zéro double de $f(z)$, on a la proportion[278])

$$1 : z_1 : z_1^2 : \cdots z_1^n = \frac{\partial D}{\partial a_n} : \frac{\partial D}{\partial a_{n-1}} : \frac{\partial D}{\partial a_{n-2}} : \cdots : \frac{\partial D}{\partial a_0}.$$

F. Brioschi[279]) a considéré le cas où la fonction $f(z)$ a i groupes de zéros multiples $z_1, z_2, \ldots, z_i$ d'ordres respectifs de multiplicité $r_1, r_2, \ldots, r_i$. Dans ce cas il désigne par P_1 le résultat de l'opération symbolique

$$z^s \frac{\partial}{\partial a_n} - s z^{s-1} \frac{\partial}{\partial a_{n-1}} + \frac{s(s-1)}{1 \cdot 2} z^{s-2} \frac{\partial}{\partial a_{n-2}} + \cdots + (-1)^s \frac{\partial}{\partial a_{n-s}},$$

effectuée sur la fonction D, s étant un nombre naturel quelconque donné; il désigne par P_2 le résultat de la même opération symbolique effectuée sur P_1, etc. Si alors r représente la somme

$$r = r_1 + r_2 + \cdots + r_i,$$

on a non seulement $D = 0$, mais encore, quel que soit z,

$$P_1 = 0, \quad P_2 = 0, \ldots, P_{r-1} = 0$$

et

$$P_r = \frac{\partial^r D}{\partial a_n^r} [(z - z_1)^{r_1} (z - z_2)^{r_2} \ldots (z - z_i)^{r_i}]^s.$$

J. J. Sylvester[280]) avait énoncé le même résultat que *F. Brioschi* dans un cas particulier, celui où $s = n$.

Pour $s = 1$, l'équation

$$P_r = 0$$

donne les racines multiples de l'équation $f(z) = 0$.

Si $f(z)$ est le produit de deux fonctions rationnelles entières $f_1(z)$ et $f_2(z)$ de degrés respectifs m_1 et m_2 on a

$$D(f_1 f_2) = (-1)^{m_1 m_2} D(f_1) D(f_2) [R(f_1, f_2)]^2.$$

On a donc en particulier si m est le degré de $f(z)$

$$D[(z-a) f(z)] = (-1)^m [f(a)]^2 D[f(z)].$$

277) Nachr. Ges. Gött. 1895, math. p. 119, 155; Acta math. 19 (1895), p. 385.

278) Cf. *C. G. J. Jacobi*, J. reine angew. Math. 15 (1836), p. 106; Werke[31]) 3, p. 302; *F. J. Richelot*, J. reine angew. Math. 21 (1840), p. 228.

279) Teoria dei determinanti, Pavie 1854; trad. par *E. Combescure*, Théorie des déterminants, Paris 1856, p. 179.

280) London Edinb. Dublin philos. mag. (4) 3 (1852), p. 375, 460; Papers 1, Cambridge 1905, p. 367, 370.

45. Expression du discriminant dans les cas les plus simples. Le discriminant de la fonction

$$f(z) = a_0 z^2 + a_1 z + a_2$$

est égal à

$$D(f) = 4 a_0 a_2 - a_1^2.$$

Le discriminant de la fonction

$$f(z) = a_0 z^3 + a_1 z^2 + a_2 z + a_3$$

est égal à

$$D(f) = 27 a_0^2 a_3^2 - 18 a_0 a_1 a_2 a_3 + 4 a_0 a_2^3 + 4 a_1^3 a_3 - a_1^2 a_2^2.$$

Il est parfois utile d'écrire la fonction $f(z)$ en mettant en évidence les coefficients binomiaux. Si

$$f(z) = a z^2 + 2 b z + c,$$

on a

$$D(f) = 4(ac - b^2).$$

Si

$$f(z) = a z^3 + 3 b z^2 + 3 c z + d,$$

on a

$$D(f) = 27 [(ad - bc)^2 - 4(ac - b^2)(bd - c^2)].$$

En suivant une méthode dont le principe est dû à *G. Boole*[281]), *A. Cayley*[282]) a mis le discriminant de la fonction

$$f(z) = a z^4 + 4 b z^3 + 6 c z^2 + 4 d z + e$$

sous la forme

$$D = 256 (I^3 - 27 J^2),$$

où I et J sont les invariants

$$I = ae - 4bd + 3c^2, \qquad J = ace + 2bcd - ad^2 - eb^2 - c^3 = \begin{vmatrix} a & b & c \\ b & c & d \\ c & d & e \end{vmatrix}.$$

Dans un mémoire où il cherche d'abord le résultant de deux formes binaires cubiques, *A. Clebsch*[283]) s'est occupé de la même question.

Le même problème a été résolu pour les fonctions rationnelles du cinquième, sixième et septième degré par *G. Salmon*[284]), *F. Brioschi*[285]), *F. Faà di Bruno*[286]), *G. Maisano*[287]), *P. Gordan*[288]); ce dernier a donné une méthode générale pour former des discriminants[289]).

281) Cambr. math. J. 2 (1839/41), p. 70.

282) Cambr. math. J. 4 (1843/5), p. 208; Philos. Trans. London 148 (1858), p. 429; Papers 1 (1889), p. 94; 2, Cambr. 1889, p. 546.

283) J. reine angew. Math. 64 (1865), p. 95.

284) Cambr. Dublin math. J. 9 (1854), p. 32.

285) Ann. mat. pura appl. (2) 1 (1867/8), p. 159; Opere 2, Milan 1902, p. 77.

286) Formes binaires[32]), table IV; voir surtout la trad. allem. par *Th. Walter* publ. sous la direction de *M. Nöther*, Einleitung in die Theorie der binären Formen, Leipzig 1881, Anhang, p. 317.

A. Cayley[290]) remarque que le discriminant D de la fonction rationnelle entière

$$f(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n$$

peut être mis sous la forme

$$a_1^2 V + a_0 U,$$

V désignant le discriminant de la fonction du $(n-1)^{\text{ième}}$ degré

$$a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_{n-1} x + a_n.$$

Si $a_1 = 0$, le discriminant D est de la forme $a_0(a_2{}^3 V_1 + a_0 U)$; si $a_1 = a_2 = 0$, le discriminant D est de la forme $a_0{}^2(a_3{}^4 V_2 + a_0 U)$; etc.; $U, V_1, V_2, \ldots$ sont des fonctions rationnelles entières des coefficients de $f(x)$. *G. Bauer*[291]) a utilisé cette remarque de *A. Cayley* pour *calculer* le discriminant D d'une fonction rationnelle entière quelconque de degré n; à cet effet il met U sous la forme

$$U = \alpha + a_0^1 \beta + a_0^2 \gamma + \cdots,$$

$\alpha, \beta, \gamma \ldots$ étant indépendants de a_0, et suivant une méthode indiquée par *A. Cayley*[292]) il effectue le calcul de $\alpha, \beta, \gamma, \ldots$ en cherchant une suite de relations entre ces coefficients[293]).

46. La surface-discriminant. Si l'on suppose que $a_0 = 1$ et que les coefficients $a_1, a_2, \ldots, a_n$ de la fonction rationnelle entière

$$f(z) = z^n + a_1 z^{n-1} + \cdots + a_{n-1} z + a_n$$

sont *réels*, on peut envisager ces coefficients $a_1, a_2, \ldots, a_n$ comme les coordonnées d'un point P d'un espace à n dimensions. En égalant à zéro le discriminant $D(f)$ de la fonction $f(z)$ on obtient l'équation

$$D(a_1, a_2, \ldots, a_n) = 0$$

d'une surface dans cet espace à n dimensions. On appelle cette surface la *surface-discriminant*[294]). Quand le point P varie, le nombre des

287) Math. Ann. 30 (1887), p. 442.

288) Math. Ann. 31 (1888), p. 566.

289) Invar.[106]) 2, Leipzig 1887, p. 108. *A. Clebsch* et *P. Gordan*, Ann. mat. pura appl. (2) 1 (1867/8), p. 23.

290) Quart. J. pure appl. math. 10 (1870), p. 23; Papers 7, Cambr. 1894, p. 303.

291) Sitzgsb. Akad. München 16 (1886), p. 183.

292) J. reine angew. Math. 47 (1854), p. 109; Papers 2, Cambr. 1889, p. 164.

293) *Voir aussi, sur le discriminant, *F. Brioschi*, Ann. sc. mat. fis. 7 (1856), p. 5, 64; Opere 1, Milan 1901, p. 189; *S. R. Minich*, Atti Ist. Veneto (3) 4 (1858/9), p. 343; *G. Peano*, Giorn. mat. (1) 27 (1889), p. 226 (Note de *G. Vivanti*).*

294) *Pour $n = 2$ et $n = 3$, cf. *F. Klein* dans *W. von Dyck*, Katalog math. Modelle, Munich 1892, p. 1/15 et *S. Pincherle*, Rivista mat. 3 (1893), p. 54/6 (Note de *G. Loria*).*

racines réelles de l'équation $f(z) = 0$ ne peut changer que si le point P traverse la surface-discriminant. Si le point P est sur cette surface, l'ordre de multiplicité des racines de $f(z) = 0$ et la réalité des racines multiples restent invariantes à moins que le point P ne traverse certaines variétés situées sur cette surface.

A. Brill[295]) a démontré que dans les régions de l'espace à n dimensions où le discriminant D de l'équation algébrique envisagée $f(z) = 0$ est négatif, le nombre des couples de racines imaginaires de cette équation est impair, tandis que dans les régions où D est positif ce nombre est pair.

Le rôle de la surface-discriminant et de ses diverses variétés a été mis en pleine lumière par *L. Kronecker*[296]) qui l'a rattachée à sa théorie des *caractéristiques*. Il s'est, en particulier, servi de la surface-discriminant pour déterminer la nature des racines d'une équation du quatrième degré.

Déjà *A. Cayley*[297]) avait cherché à former les conditions nécessaires et suffisantes pour qu'une équation du cinquième degré ait deux couples de racines égales. **Ch. Hermite*, *J. J. Sylvester* et *A. Cayley* ont tous trois cherché les conditions nécessaires et suffisantes pour qu'une équation du cinquième degré ait ses cinq racines *réelles*[298]).*

D. Hilbert[299]) conserve le coefficient a_0 et regarde les nombres réels $a_0, a_1, a_2, \ldots, a_n$ comme les coordonnées *homogènes* d'un point de l'espace à n dimensions. Soit alors

$$D(a_0, a_1, a_2, \ldots, a_n) = 0$$

l'équation de la surface-discriminant. La polaire de cette surface par rapport au point $(b_0, b_1, \ldots, b_n)$ est représentée par l'équation

$$D_1 = b_0 \frac{\partial D}{\partial a_0} + b_1 \frac{\partial D}{\partial a_1} + \cdots + b_n \frac{\partial D}{\partial a_n} = 0.$$

295) Math. Ann. 12 (1877), p. 87. Voir aussi *G. Kerschensteiner*, Diss. Munich (éd. Nuremberg) 1888.

296) Monatsb. Akad. Berlin 1878, p. 119; Werke[189]) 2, p. 68; voir aussi *C. Färber*, Diss. Berlin 1889; *R. E. Hoppe*, Archiv Math. Phys. (2) 14 (1896), p. 398; *et, pour le cas d'une équation du troisième degré, *R. Le Vavasseur*, J. math. spéc. (4) 1 (1892), p. 145, 169;* pour le cas d'une équation du sixième degré, *A. Brill*, Math. Ann. 20 (1882), p. 330.

297) Philos. Trans. London 147 (1857), p. 727; Papers 2, Cambr. 1889, p. 465. Voir aussi *J. J Sylvester*, London Edinb. Dublin philos. mag. (4) 3 (1852) p. 375, 460; Papers 1, Cambridge 1905, p. 367, 370 à propos des évectants (n° 20); *puis *Ch. Hudson*, Quart. J. pure appl. math. 18 (1882), p. 215, 327.*

298) **Ch. Hermite*, Cambr. Dublin math. J. 9 (1854), p. 199; Œuvres publ. par *E. Picard* 1, Paris 1905, p. 327; *J. J. Sylvester*, Philos. Trans. London 154 (1864), p. 579; *A. Cayley*, id. 157 (1867), p. 526; Papers 6, Cambr. 1893, p. 161.*

299) Math. Ann. 30 (1887), p. 437.

Les polaires successives $D_2 = 0$, $D_3 = 0, \ldots$ de la surface $D = 0$ s'obtiennent par l'application répétée de l'opération

$$b_0 \frac{\partial}{\partial a_0} + b_1 \frac{\partial}{\partial a_1} + \cdots + b_n \frac{\partial}{\partial a_n}$$

à la fonction $D(a_0, a_1, \ldots, a_n)$, en sorte que

$$D_{k+1} = b_0 \frac{\partial D_k}{\partial a_0} + b_1 \frac{\partial D_k}{\partial a_1} + \cdots + b_n \frac{\partial D_k}{\partial a_n}.$$

Si la fonction $f(z)$ a λ zéros distincts $\alpha_1, \alpha_2, \ldots, \alpha_\lambda$ d'ordres de multiplicité $\mu_1, \mu_2, \ldots, \mu_\lambda$, le discriminant D et ses $n - \lambda - 1$ premières polaires $D_1, D_2, \ldots, D_{n-\lambda-1}$ s'évanouissent identiquement quels que soient $b_0, b_1, \ldots, b_n$, tandis que la $(n-\lambda)^{\text{ième}}$ polaire se décompose en facteurs linéaires par rapport à $b_0, b_1, \ldots, b_n$ en sorte que

$$D_{n-\lambda} = [B(\alpha_1)]^{\mu_1 - 1}[B(\alpha_2)]^{\mu_2 - 1} \ldots [B(\alpha_\lambda)]^{\mu_\lambda - 1}$$

où[300])

$$B(z) = b_0 z^n + b_1 z^{n-1} + \cdots + b_n.$$

Réciproquement, l'évanouissement identique de D et de ses $n - \lambda - 1$ premières polaires $D_1, D_2, \ldots, D_{n-\lambda-1}$ et la décomposition de la $(n-\lambda)^{\text{ième}}$ polaire $D_{n-\lambda}$ en facteurs linéaires d'ordres de multiplicité $\mu_1 - 1, \mu_2 - 1, \ldots, \mu_\lambda - 1$ entraînent l'existence de λ zéros de $f(z)$ d'ordres de multiplicité respectifs $\mu_1, \mu_2, \ldots, \mu_\lambda$.

47. Les équations aux dérivées partielles caractéristiques du résultant ou du discriminant. Le résultant $R(f, \varphi)$ de deux fonctions rationnelles entières

$$f(z) = a_0 z^n + a_1 z^{n-1} + \cdots + a_{n-1} z + a_n,$$
$$\varphi(z) = b_0 z^\nu + b_1 z^{\nu-1} + \cdots + b_{\nu-1} z + b_\nu$$

vérifie l'équation aux dérivées partielles

$$n a_0 \frac{\partial R}{\partial a_1} + (n-1) a_1 \frac{\partial R}{\partial a_2} + \cdots + a_{n-1} \frac{\partial R}{\partial a_n} + \nu b_0 \frac{\partial R}{\partial b_1} + (\nu - 1) b_1 \frac{\partial R}{\partial b_2} + \cdots + b_{\nu-1} \frac{\partial R}{\partial b_\nu} = 0.$$

Si $n > \nu$, on a aussi

$$b_0 \frac{\partial R}{\partial a_{n-\nu}} + b_1 \frac{\partial R}{\partial a_{n-\nu+1}} + \cdots + b_\nu \frac{\partial R}{\partial a_n} = 0.$$

Si $n = \nu$, on a les deux relations, rentrant l'une dans l'autre,

$$b_0 \frac{\partial R}{\partial a_0} + b_1 \frac{\partial R}{\partial a_1} + \cdots + b_n \frac{\partial R}{\partial a_n} = 0,$$
$$a_0 \frac{\partial R}{\partial b_0} + a_1 \frac{\partial R}{\partial b_1} + \cdots + a_n \frac{\partial R}{\partial b_n} = 0.$$

300) *Cf. *E. Czuber*, Monatsh. Math. Phys. 5 (1894), p. 62.*

Si $n = \nu$ et si l'on pose

$$\alpha_{s,r+1} = (b_0 a_{r+s} + b_1 a_{r+s-1} + \cdots + b_{s-1} a_{r+1}) - (a_0 b_{r+s} + a_1 b_{r+s-1} + \cdots + a_{s-1} b_{r+1}),$$

on a pour $m = 1, 2, \ldots, n$ les relations

$$\sum_{r=1}^{r=n} \alpha_{m,r} \frac{\partial R}{\partial a_r} = (n - m + 1) b_{m-1} R.$$

F. Brioschi appelle ces n équations les *équations caractéristiques* du résultant. Il établit des équations analogues pour le cas où $\varphi(z) = f'(z)$, c'est-à-dire pour le *discriminant* de $f(z)$. *F. Faà di Bruno* en donne dans ce cas une démonstration simple[301]).

Plus tard *F. Faà di Bruno* et après lui *M. Nöther* ont repris l'étude des ces équations aux dérivées partielles caractéristiques du résultant de deux fonctions rationnelles entières de degrés quelconques. *M. Nöther*[302]) démontre que la seule équation caractéristique indépendante est

$$\sum_{k=0}^{k=n-1} (a_{k+1} b_0 - a_0 b_{k+1}) \frac{\partial R}{\partial a_k} = -b_1 R.$$

De celle-là résultent toutes les autres.

Le discriminant $D(f)$ de la fonction

$$f(z) = a_0 z^n + a_1 z^{n-1} + \cdots + a_{n-1} z + a_n$$

vérifie certaines équations aux dérivées partielles, telles que, par exemple

$$n a_0 \frac{\partial D}{\partial a_1} + (n-1) a_1 \frac{\partial D}{\partial a_2} + \cdots + a_{n-1} \frac{\partial D}{\partial a_n} = 0.$$

M. Nöther[303]) a démontré que celles de ces équations aux dérivées partielles qui sont caractéristiques pour le discriminant se ramènent à une seule.

**J. A. Serret*[304]) a utilisé l'équation qui précède pour le calcul des coefficients numériques de $D(f)$.*

48. Travaux récents relatifs à l'élimination. Le grand nombre et la variété des mémoires relatifs à l'élimination rendent difficile une classification rationnelle de ces mémoires.

301) *F. Brioschi*, J. reine angew. Math. 53 (1857), p. 372; Ann. mat. pura appl. (1) 2 (1859), p. 82; Opere 2, Milan 1902, p. 17; *F. Faà di Bruno*, J. reine angew. Math. 54 (1857), p. 283.

302) *M. Nöther*, dans *F. Faà di Bruno*, Binäre Formen[286]), p. 275.

303) Id. p. 282.

304) *Alg. sup.[30]) 1, p. 461.*

Il convient toutefois de mettre en relief les recherches fondamentales de *L. Kronecker*[305]) sur l'élimination d'une variable entre deux équations algébriques et sur les séries récurrentes (nº **30**). A ces recherches se rattachent celles de *E. Netto*[306]).

Signalons ici d'autres recherches de *E. Netto* concernant la théorie de l'élimination. Reprenons, à cet effet, pour $n = \nu$, les notations du nº **35** et supposons que l'on ait

$$R = 0,\ R_1 = 0,\ R_2 = 0,\ \ldots,\ R_{q-1} = 0$$

en sorte que les deux équations

$$f(z) = a_0 z^n + a_1 z^{n-1} + \cdots + a_{n-1} z + a_n = 0,$$
$$g(z) = b_0 z^n + b_1 z^{n-1} + \cdots + b_{n-1} z + b_n = 0$$

aient q racines communes. La condition

$$R_q = 0$$

exprime la condition nécessaire et suffisante pour que les deux équations

$$f(z) = 0,\quad g(z) = 0$$

aient en outre, une $(q+1)^{\text{ième}}$ racine commune; mais alors tous les coefficients

$$R_q,\ R_q^{(1)},\ R_q^{(2)},\ \ldots,\ R_q^{(q)}$$

de l'équation aux q racines communes

$$R_q z^q + R_q^{(1)} z^{q-1} + \cdots + R_q^{(q)} = 0$$

sont aussi nuls pourvu toutefois que a_0 et b_0 ne soient pas nuls simultanément.

E. Netto[307]) s'est proposé de mettre ce fait en évidence par des transformations identiques. En s'appuyant sur le développement de certains déterminants, il démontre que, quand les coefficients

$$a_0,\ a_1,\ \ldots,\ a_n,\ b_0,\ b_1,\ \ldots,\ b_n$$

sont des variables indéterminées, les expressions

$$(a_0 u + b_0 v) R_q^{(\lambda)} \qquad (\lambda = 1, 2, \ldots, q),$$

dans lesquelles u et v désignent des indéterminées, s'expriment linéairement au moyen de

$$R_q,\ R_{q-1},\ R_{q-1}^{(1)},\ R_{q-1}^{(2)},\ \ldots,\ R_{q-1}^{(q-1)}$$

où

305) Voir surtout Monatsb. Akad. Berlin 1881, p. 535; Werke[189]) 2, p. 115.
306) J. reine angew. Math. 116 (1896), p. 33; 117 (1897), p. 57.
307) J. reine angew. Math. 104 (1889), p. 321.

$$R_{q-1},\ R_{q-1}^{(1)},\ R_{q-1}^{(2)},\ \ldots,\ R_{q-1}^{(q-1)}$$

sont les coefficients de l'équation aux $(q-1)$ racines communes

$$R_{q-1} z^{q-1} + R_{q-1}^{(1)} z^{q-2} + \cdots + R_{q-1}^{(q-1)} = 0.$$

**P. Gordan*[308]) exprime le résultant $R(f, \varphi)$ de deux fonctions rationnelles entières

$$f(z) = z^n + a_1 z^{n-1} + \cdots + a_{n-1} z + a_n = (z-\alpha_1)(z-\alpha_2)\ldots(z-\alpha_n)$$
$$\varphi(z) = z^\nu + b_1 z^{\nu-1} + \cdots + b_{\nu-1} z + b_\nu = (z-\beta_1)(z-\beta_2)\ldots(z-\beta_\nu)$$

au moyen des coefficients $c_1, c_2, \ldots, c_{n\nu}$ d'une fonction résolvante

$$\prod_{(i,\,k)} \left(z - \frac{\beta_k}{\alpha_i}\right) = z^{n\nu} + c_1 z^{n\nu-1} + \cdots + c_{n\nu-1} z + c_{n\nu};$$

ces coefficients $c_1, c_2, \ldots, c_{n\nu-1}, c_{n\nu}$, qui s'expriment rationnellement en fonction des sommes des puissances semblables des α et des β, sont donc des fonctions rationnelles de $a_1, a_2, \ldots, a_{n-1}, a_n, b_1, b_2, \ldots, b_{\nu-1}, b_\nu$ qu'il est aisé de former.

T. Muir démontre après *W. W. Taylor* que, si $f(z)$ est une fonction rationnelle entière quelconque de z de degré n, le résultant

$$R\left[f(z),\ z^n f\left(\frac{1}{z}\right)\right]$$

peut être décomposé en deux facteurs linéaires et un carré[309]). Ce théorème peut être utilisé dans l'une des démonstrations du théorème fondamental de l'algèbre [deuxième démonstration de *C. F. Gauss* modifiée par *P. Gordan*, cf. nº **85**].

D. Hilbert[310]) étudie le discriminant de la série hypergéométrique limitée à un nombre fini de termes.

S. Roberts[311]) détermine le degré du discriminant[312]) d'une forme $U + kV$ dans le cas où U, ou V, ou U et V, se décomposent en facteurs; U et V désignent des fonctions homogènes d'ordre n de 2, 3 ou 4 variables.

H. von Koch[313]) donne un procédé pour former le résultant $R(f, \varphi)$ qui s'applique au cas où l'une des deux fonctions envisagées $f(z)$ ou $\varphi(z)$ est une fonction transcendante entière.*

308) *C. R. Acad. sc. Paris 127 (1898), p. 539; voir aussi Jahresb. deutsch. Math.-Ver. 8¹ (1899), éd. 1900, p. 178.*
309) **T. Muir*, Proc. R. Soc. Edinb. 21 (1895/7), p. 360/8; *W. W. Taylor*, Proc. London math. Soc. (1) 27 (1895/6), p. 60.*
310) *J. reine angew. Math. 103 (1888) p. 337.*
311) *Quart. J. pure appl. math. 10 (1870), p. 204.*
312) *Pour l'extension de la notion de discriminant aux fonctions homogènes de trois ou quatre variables, voir nº **64**.*
313) *Öfversigt Vetensk. Akad. förhandl. (Stockholm) 50 (1893), p. 449, 453.*

Parmi les recherches sur les résultants et discriminants qui ont été plutôt faites en vue des applications géométriques nous citerons les suivantes:

Certaines recherches géométriques se ramènent finalement à la détermination du degré du résultant de deux fonctions rationnelles entières ou du discriminant d'une fonction rationnelle entière. D'autre part la superposition de deux éléments singuliers d'une courbe plane ou gauche entraîne l'existence d'un nouvel élément singulier, au moins, d'où l'on conclut que les résultants ou discriminants des équations dont dépendent les singularités les plus simples ont nécessairement des facteurs communs. Ces faits ont été étudiés par *W. F. Meyer*[314]) et *A. Brill*[315]).

W. F. Meyer[316]) a aussi traité le problème suivant: quels changements subissent les nombres des singularités réelles des courbes lorsque par la variation des coefficients deux singularités viennent à se superposer. Ces superpositions correspondent à l'évanouissement de certains facteurs des discriminants ou des résultants des équations de singularité[317]).

*Un problème spécial d'élimination auquel on a donné le nom d'*Ellipse-Glissette* a été abordé par *T. Muir*[318]), *P. H. Schoute*[319]), *E. J. Nanson*[320]), *P. G. Tait*[321]) et *J. Mc Laren*[322]). Il consiste en ceci: Une ellipse dont les demi-axes sont a, b se meut dans son plan de façon à être toujours en contact avec deux droites rectangulaires. La *glissette* en question est la courbe engendrée par un point du plan invariablement lié à l'ellipse. Au point de vue algébrique il s'agit de l'élimination d'une variable θ entre deux équations de la forme

$$-C\sin\theta\cos\theta - B\sin^2\theta + \alpha_1\cos\theta + \beta_1\sin\theta + \gamma_1 = 0$$
$$+C\sin\theta\cos\theta + B\sin^2\theta + \alpha_2\cos\theta + \beta_2\sin\theta + \gamma_2 = 0.*$$

314) Math. Ann. 38 (1891), p. 369; 43 (1893), p. 286.

315) Math. Ann. 16 (1880), p. 348.

316) Math. Ann. 38 (1891), p. 369 (courbes planes); 43 (1893), p. 286; Nachr. Ges. Gött. 1888, p. 74; 1890, p. 366, 493; 1891, p. 14, 88; Monatsh. Math. Phys. 4 (1893), p. 229, 331 (courbes gauches).

317) Voir aussi *A. Brill*, Math. Ann. 16 (1880), p. 351, 388 (courbes planes); **A. Brill* et *M. Nöther*, Die Entwicklung der Theorie der algebraischen Funktionen [Jahresb. deutsch. Math.-Ver. 3 (1892/3), éd. 1894, chap. 6 [Die Theorie der singulären Punkte], p. 367 et suiv.; voir en partic. p. 382.*

318) *Proc. R. Soc. Edinb. 17 (1889/90), p. 2; 19 (1891/2), p. 25, 89.*

319) *Wiskundige Opgaven Genootschap Amsterdam (2) 6 (1894/6), p. 42, question XX.*

320) *Proc. R. Soc. Edinb. 22 (1897/9), p. 158.*

321) *Proc. R. Soc. Edinb. 19 (1891/2), p. 131.*

322) *Proc. R. Soc. Edinb. 19 (1891/2), p. 89; 22 (1897/9), p. 379.*

L. Schendel*[323]) emploie une notation symbolique particulière au moyen de laquelle il exprime le résultant de deux fonctions rationnelles entières. Avec cette notation symbolique la *formule d'interpolation de Kronecker* (n° **40) se présente sous une forme très simple.

H. Dellac[324]) en faisant usage de considérations élémentaires [méthode du parallélogramme, annoncée par *A. L. Cauchy* comme application de ses clefs anastrophiques[325])] permettant d'exprimer le résultant des deux fonctions rationnelles entières

$$f(z) = a_0 z^n + a_1 z^{n-1} + \cdots + a_{n-1} z + a_n,$$
$$\varphi(z) = b_0 z^n + b_1 z^{n-1} + \cdots + b_{n-1} z + b_n$$

en fonction des expressions $A_{hk} = a_h b_k - a_k b_h$, remarque que des réductions ont lieu entre termes de même signe et compte le nombre total des termes *avant* la réduction, c'est-à-dire la somme des valeurs absolues des coefficients numériques qui figurent dans l'expression du résultant.*

49. Invariants ou covariants de formes binaires, divisibles par certaines puissances du résultant ou discriminant. *On appelle souvent *résultant de deux formes binaires*

$$f(x, y), \quad \varphi(x, y)$$

le résultant $R(f, \varphi)$ des deux fonctions $f(x, 1)$, $\varphi(x, 1)$. On dit de même souvent *discriminant de la forme*

$$f(x, y)$$

au lieu de dire discriminant $D(f)$ de la fonction $f(x, 1)$.*

P. Gordan[326]) a fait les remarques que voici:

Envisageons deux formes binaires

$$f(x, y), \quad \varphi(x, y)$$

et le déterminant fonctionnel (n° **73**)

$$t(x, y) = \begin{vmatrix} \dfrac{\partial f}{\partial x} & \dfrac{\partial f}{\partial y} \\ \dfrac{\partial \varphi}{\partial x} & \dfrac{\partial \varphi}{\partial y} \end{vmatrix};$$

formons aussi le résultant $R(f, \varphi)$ des deux formes binaires $f(x, y)$, $\varphi(x, y)$ et le résultant $R(t, f)$ des deux formes binaires $t(x, y)$, $f(x, y)$.

323) Z. Math. Phys. 32 (1887), p. 46, 83.

324) Ann. Fac. sc. Marseille 11 (1901), p. 141.

325) C. R. Acad. sc. Paris 44 (1857), p. 270; Œuvres (1) 12, Paris 1900, p. 420.

326) Math. Ann. 4 (1871), p. 169.

Si $D(f)$ désigne le discriminant de la forme binaire $f(x, y)$ on a

$$R(t, f) = \alpha R(f, \varphi) D(f),$$

où α est un coefficient numérique déterminé.

Envisageons de même le hessien (n° **76**)

$$h(x, y) = \begin{vmatrix} \frac{\partial^2 f}{\partial x^2} & \frac{\partial^2 f}{\partial x \partial y} \\ \frac{\partial^2 f}{\partial x \partial y} & \frac{\partial^2 f}{\partial y^2} \end{vmatrix}$$

de la forme binaire $f(x, y)$, et formons le résultant $R(f, h)$ des deux formes binaires $f(x, y)$, $h(x, y)$.. Si $D(f)$ désigne le discriminant de la forme binaire $f(x, y)$ on a

$$R(f, h) = \beta D^2(f),$$

où β est un coefficient numérique déterminé.

Si $t(x, y)$ est le déterminant fonctionnel d'une forme binaire $f(x, y)$ et de son hessien $h(x, y)$, on a aussi

$$R(t, f) = \gamma D^3(f),$$

où γ est un coefficient numérique déterminé.

D. Hilbert[327]) considère deux formes binaires $\varphi(x, y)$ et $\psi(x, y)$, toutes deux de degré ν, et envisage le discriminant de la forme $\lambda\varphi + \mu\psi$ où λ, μ désignent deux paramètres. Il se propose et résout le problème de déterminer toutes les expressions de la forme $\lambda\varphi + \mu\psi$ telles que leur discriminant soit une forme binaire *donnée* du $(2\nu - 2)^{\text{ième}}$ degré des paramètres λ, μ.

G. Kohn[328]) a indiqué un grand nombre de cas où les discriminants ou résultants de covariants de formes binaires en x et y sont divisibles par certaines puissances du discriminant ou du résultant des formes binaires elles-mêmes. *G. Kohn* a aussi étudié de nombreux cas où des invariants (autres que des discriminants ou des résultants) de covariants de formes binaires sont divisibles par des puissances déterminées des discriminants ou résultants des formes binaires elles-mêmes.

E. Waelsch[329]) a étudié des questions analogues. Il envisage aussi le résultant R des deux équations en $\frac{\lambda_1}{\lambda_2} = \lambda$

$$\lambda_2^n \varphi(\lambda) = \alpha_0 \lambda_1^n + \alpha_1 \lambda_1^{n-1} \lambda_2 + \cdots + \alpha_n \lambda_2^n = 0,$$
$$\lambda_2^n \psi(\lambda) = \beta_0 \lambda_1^n + \beta_1 \lambda_1^{n-1} \lambda_2 + \cdots + \beta_n \lambda_2^n = 0$$

et ayant rappelé que l'expression

---

327) Math. Ann. 31 (1887), p. 482.

328) Sitzgsb. Akad. Wien, 100 II^a (1891), p. 865, 1013; id. 102 II^a (1893), p. 801.

329) Id. 100 II^a (1891), p. 574; Monatsh. Math. Phys. 2 (1891), p. 421.

$$R_{ik} = \frac{\partial R}{\partial \alpha_i} \frac{\partial R}{\partial \beta_k} - \frac{\partial R}{\partial \beta_i} \frac{\partial R}{\partial \alpha_k}$$

est divisible par R il cherche le quotient de la division; il obtient pour ce quotient une expression de la forme

$$\frac{R_{ik}}{R} = (-1)^{i+k-1} n^2 P_{ik}$$

où P_{ik} est formé assez simplement au moyen des α et des β. Il en tire des conséquences géométriques.

A. Cayley[330]) donne une interprétation géométrique des équations

$$D(f) = 0, \quad D(\varphi) = 0, \quad R(f, \varphi) = 0,$$

$f(x, y)$ et $\varphi(x, y)$ désignant des formes binaires, D le discriminant et R le résultant de ces formes.

**E. Pascal* et *E. Waelsch*[331]) ont obtenu des expressions symboliques donnant sous forme finie le résultant $R(f, \varphi)$ de deux formes binaires

$$f(x, y), \qquad \varphi(y, x)$$

de même degré.

P. Gordan[332]) enfin a trouvé un „procédé de composition" permettant de construire directement le résultant $R(f, \varphi)$ de deux formes binaires de même degré n à l'aide de formes intermédiaires dont il donne dans tous les cas l'expression au moyen des coefficients de f et de φ. Le même procédé de composition lui permet aussi de former le covariant qui, égalé à zéro, donne l'équation pour la $(2n-2)^{\text{ième}}$ puissance du facteur linéaire commun aux deux équations $f(z) = 0$ et $\varphi(z) = 0$.*

50. Énumération d'autres travaux relatifs à l'élimination. Parmi les travaux relatifs à l'élimination qui, tout en cherchant à perfectionner la théorie sur quelque point de détail, ont surtout pour objet d'exposer, en les comparant entre elles, les diverses méthodes connues, ou encore s'attachent à développer plus particulièrement l'une ou l'autre de ces méthodes, nous citerons tout d'abord les traités de *F. Faà di Bruno*[333]) et de *P. Gordan*[334]), ainsi que les remarques de *W. Scheibner*[335]) et de *L. O. Hesse*[336]) au sujet du traité de *H. R. Baltzer*

---

330) *A. Cayley*, Proc. London math. Soc. (1) 5 (1873/4), p. 31/3; Papers 9, Cambridge 1896, p. 16/7.

331) **E. Pascal*, Rendic. Accad. Napoli (2) 2 (1888), p. 402; Ann. mat. pura appl. (2) 16 (1888), p. 85; *E. Waelsch*, Sitzgsb. Akad. Wien 114 II^a (1905), p. 1143/6.*

332) **P. Gordan*, Rend. Circ. mat. Palermo 22 (1906), p. 161/96 (Texte et notes 331/2 de *A. Brill*).*

333) Formes binaires[32]), p. 69 et suiv.; Binäre Formen[286]), p. 50 et suiv.

334) Invar.[106]) 1, p. 135 et suiv.

335) Ber. Ges. Lpz. 40 (1888), math. p. 1/13.

sur les déterminants. Nous citerons aussi les notes de *G. Darboux*[337]), *E. Rouché*[338]), *B. Igel*[339]), *V. Hioux*[340]), *Ventéjols*[341]) et *N. von Szüts*[342]).

*Dans la première partie de son Mémoire sur l'élimination *H. Lemonnier*[343]) montre quels liens unissent les méthodes d'élimination connues sous le nom de *méthode d'Euler, de Sylvester, de Cayley, de Bézout, de Cauchy.* Il montre ensuite comment on peut former de proche en proche les équations qui finalement conduisent aux conditions pour que deux fonctions rationnelles entières données aient un p. g. c. d. d'ordre p, et à ce p. g. c. d. lui-même. Dans une troisième partie *H. Lemonnier* applique ces procédés à la résolution de deux équations simultanées en x et en y.

A ces recherches de *H. Lemonnier* se rattachent des recherches de *H. G. Zeuthen*[344]) sur le même sujet.

Citons encore *P. Cossali*[345])[346]), *F. Chio*[347]) et *A. Cayley*[348]).*

*Soient

$$f(z) = a_0 z^n + a_1 z^{n-1} + \cdots + a_{n-1} z + a_n,$$
$$g(z) = b_0 z^n + b_1 z^{n-1} + \cdots + b_{n-1} z + b_n;$$

336) Kritische Z. Chem. Phys. Math. 1858, p. 483; Ann. mat. pura appl. (1) 2 (1859), p. 5; Werke[230]), p. 475.

337) Démonstration simple et rigoureuse des conditions nécessaires et suffisantes pour que $f(z) = 0$, $\varphi(z) = 0$ aient p racines communes [Bull. sc. math. (1) 10 (1876), p. 56; (2) 1 (1877), p. 54].

338) Nouv. Ann. math. (2) 16 (1877), p. 105.

339) Sitzgsb. Akad. Wien 76, II (1877), p. 145.

340) Nouv. Ann. math. (2) 18 (1879), p. 289; Ann. Ec. Norm. (2) 10 (1881), p. 383; (2) 11 (1882), p. 135.

341) C. R. Acad. sc. Paris 84 (1877), p. 546.

342) Monatsh. Math. Phys. 9 (1898), p. 34.

343) *Mémoire sur l'élimination, Paris 1879; Ann. Ec. Norm. (2) 7 (1878), p. 77, 151.*

344) *Tidsskrift math. Köbenhavn (Copenhague) (4) 5 (1881), p. 45, 109.*

345) *Mem. mat. fis. Soc. ital. delle scienze (1) 16 (1813), p. 272 (Note de *G. Vivanti*).*

346) **P. Cossali* s'était déjà occupé de la théorie de l'élimination dans un ouvrage dont le titre ne semblerait guère indiquer qu'on y trouve des considérations de cet ordre [Origine, trasporto in Italia, primi progressi in essa dell'Algebra 2, Parme 1799, p. 1/95; voir en partic. p. 41/6 „calcolo del *Cramer* mancante di una esatta general dimostrazione"; p. 47/51 „calcolo composto di quelli di *Eulero* e *Cramer* perfezionati"; p 51/95 „calcolo del *Lagrange* corretto e semplificato" (Note de *G. Eneström*).*

347) *Raccolta di lettere ed altri scritti fis. mat. 3 (1847), p. 193.*

348) J. reine angew. Math. 50 (1855), p. 278; 60 (1862), p. 273; Quart. J. pure appl. math. 12 (1873), p. 5; Proc. London math. Soc. (1) 11 (1879/80), p. 139; Papers 2, Cambr. 1889, p. 181; 5, Cambr. 1892, p. 157; 9, Cambr. 1896, p. 43, 11, Cambr. 1896, p. 100.

Ch. Biehler[349]) pose

$$f_1(z) = a_0 g(z) - b_0 f(z) = a_{01} z^{n-1} + a_{11} z^{n-2} + \cdots,$$
$$f_2(z) = a_0 z f_1(z) - a_{01} f(z) = a_{02} z^{n-1} + a_{12} z^{n-2} + \cdots,$$
$$f_3(z) = a_0 z f_2(z) - a_{02} f(z) = a_{03} z^{n-1} + a_{13} z^{n-2} + \cdots,$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

et il démontre que le résultant $R(f, g)$ est égal au déterminant

$$\begin{vmatrix} a_{01} & a_{02} & a_{03} & \cdots \\ a_{11} & a_{12} & a_{13} & \cdots \\ a_{21} & a_{22} & a_{23} & \cdots \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \end{vmatrix}.$$

Ventéjols[350]) revendique cette méthode comme sienne[351]).*

**C. Le Paige*[352]) donne une manière très-simple de passer du déterminant de *L. Euler* d'ordre $\nu + n$ au déterminant de *E. Bézout* d'ordre $n \geqq \nu$.

Citons aussi la méthode donnée par *A. Bonolis*[353]) pour calculer effectivement le résultant $R(f, \varphi)$ de deux fonctions données.

Worontzov[354]) rattache les diverses formes du résultant sous forme de déterminant données par *E. Bézout*, *L. Euler* et *J. J. Sylvester* au développement d'une même identité.*

**H. Laurent* s'est beaucoup occupé de la théorie de l'élimination[355]). Il montre que l'on peut déduire la théorie des fonctions symétriques de celle de l'élimination, à l'inverse de ce qu'on fait d'habitude.

Pour former le résultant $R(f, \varphi)$ de deux fonctions rationnelles entières $f(z)$, $\varphi(z)$ il observe d'abord que si $\alpha_1, \alpha_2, \ldots, \alpha_n$ sont les zéros de la fonction rationnelle entière

$$f(z) = a_0 z^n + a_1 z^{n-1} + \cdots + a_{n-1} z + a_n,$$

et si $\varphi(z)$ est une fonction rationnelle entière quelconque de z, le coefficient de $\frac{1}{z}$ dans le développement de $\frac{\varphi(z) f'(z)}{f(z)}$ ordonné suivant

349) *Nouv. Ann. math. (2) 19 (1880), p. 110, 202, 332; (3) 1 (1882), p. 529.*

350) *Nouv. Ann. math. (2) 19 (1880), p. 188.*

351) Une méthode analogue est d'ailleurs déjà exposée par *H. R. Baltzer*, Determ.[105]) § 11, p. 123/5; trad. *G. J. Hoüel*, p. 83/6.

352) *C. R. Acad. sc. Paris 90 (1880), p. 1210.*

353) *Giorn. mat. (1) 21 (1883), p. 336.*

354) *Nouv. Ann. math. (3) 11 (1892), p. 291.*

355) *J. math. spéc. (4) 2 (1893), p. 49, 217; Nouv. Ann. math. (3) 6 (1887), p. 416. Voir aussi *H. Laurent*, L'élimination, publ. dans la collection Scientia, Phys.-math. n° 7, Paris 1900, p. 40.*

les puissances décroissantes de z donne $\sum_{=1}^{n}\varphi(\alpha_p)$. D'autre part, si l'on écrit pour abréger, quels que soient $\gamma_1, \gamma_2, \ldots, \gamma_n$ et pour chaque indice $p = 1, 2, 3, \ldots$,

$$\sigma_p = \gamma_1^p + \gamma_2^p + \cdots + \gamma_n^p,$$

on a

$$\gamma_1 \gamma_2 \cdots \gamma_n = \frac{1}{n!}\begin{vmatrix} \sigma_1 & 1 & 0 & \ldots & 0 \\ \sigma_2 & \sigma_1 & 2 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \sigma_n & \sigma_{n-1} & \sigma_{n-2} & \ldots & \sigma_1 \end{vmatrix}.$$

Cela posé, connaissant $f(z)$ et $\varphi(z)$, on sait calculer les sommes σ_1, $\sigma_2, \sigma_3, \ldots$ dans lesquelles, pour chaque indice i, γ_i est remplacé par $\varphi(\alpha_i)$ en sorte que l'on connaît

$$\sigma_1 = \sum_{p=1}^{n}\varphi(\alpha_p), \quad \sigma_2 = \sum_{p=1}^{n}\varphi^2(\alpha_p), \quad \sigma_3 = \sum_{p=1}^{n}\varphi^3(\alpha_p), \ \ldots$$

et que l'on peut par suite évaluer le produit $\gamma_1\gamma_2 \ldots \gamma_n$ c'est-à-dire le produit $\varphi(\alpha_1)\varphi(\alpha_2)\ldots\varphi(\alpha_n)$ et par suite le résultant

$$R(f, \varphi) = a_0{}^\nu \varphi(\alpha_1)\varphi(\alpha_2)\ldots\varphi(\alpha_n).$$

Pour former ce résultant il montre aussi[356]) que l'on peut procéder comme il suit: Si n est le degré de $f(z)$ et si ν est le degré de $\varphi(z)$ supposons $\nu \leqq n$; déterminons alors les restes de la division par $\varphi(z)$ de $f(z)$, $zf(z)$, $z^2f(z), \ldots, z^{\nu-1}f(z)$; il suffit d'éliminer $z, z^2, \ldots, z^{\nu-1}$ entre ces divers restes pour obtenir le résultant.

H. Laurent[357]) désigne d'autre part par $\lambda_1, \lambda_2, \ldots, \lambda_n$ des indéterminées et forme les nombres

$$c_{i\gamma} = \frac{f(\lambda_\gamma)\varphi(\lambda_i) - f(\lambda_i)\varphi(\lambda_\gamma)}{\lambda_\gamma - \lambda_i}, \quad c_{ii} = f'(\lambda_i)\varphi(\lambda_i) - f(\lambda_i)\varphi_i'(\lambda_i).$$

Le déterminant

$$\begin{vmatrix} c_{11}, & c_{12}, & \cdots, & c_{1n} \\ c_{21}, & c_{22}, & \cdots, & c_{2n} \\ \cdot & \cdot & \cdot & \cdot \\ c_{n1}, & c_{n2}, & \cdots, & c_{nn} \end{vmatrix}$$

des nombres ainsi formés est le produit du résultant $R(f, \varphi)$ par une fonction entière rationnelle et symétrique de $\lambda_1, \lambda_2, \ldots, \lambda_n$ qui peut se réduire à une constante.*

356) *Nouv. Ann. math. (3) 7 (1888), p. 60, 116.*

357) *Nouv. Ann. math. (3) 11 (1892), p. 5.*

**H. W. Tyler*[358]) approfondit les relations entre les déterminants de *J. J. Sylvester* et de *E. Bézout*.

G. Garbieri[359]) démontre un théorème concernant le nombre des racines communes de deux équations; il s'appuie à cet effet sur des résultats qu'il avait établis[360]) en transformant des théorèmes connus concernant les matrices.

C. Reuschle[361]) apporte une simplification au mode de formation du résultant de *E. Bézout* (simplification déjà signalée par *A. L. Cauchy*).

E. Humbert[362]) publie une note sur le résultant de deux fonctions rationnelles entières[363]). Citons encore *F. Faà di Bruno*[364]), *G. Pittarelli*[365]) et *Ch. Forestier*[366]) qui exposent la *méthode de Bézout*, la *méthode abrégée de Bézout-Cauchy* et la *méthode de Sylvester*.

P. Mansion[367]), dans une suite d'articles réunis dans le dernier que nous citons ici, aborde successivement les diverses questions dont l'ensemble constitue la théorie de l'élimination.

Voir encore *M. Falk*[368]) et les remarques de *J. Petersen*[369]).*

**G. Vivanti*[370]) remplace les deux fonctions rationnelles entières de degré n

$$f(z) = a_0z^n + a_1z^{n-1} + \cdots + a_{n-1}z + a_n,$$
$$\varphi(z) = b_0z^n + b_1z^{n-1} + \cdots + b_{n-1}z + b_n$$

par deux fonctions rationnelles entières $F(z)$, $\Phi(z)$ de degré $n - \lambda$ (où λ est à notre choix) qui sont linéaires l'une en

358) *Diss. Erlangen 1891; Sitzgsb. phys.-medic. Soc. Erlangen 23 (1891), p. 33.*

359) *Atti Accad. Gioenia Catania (4) 6 (1893), mém. nº 16.*

360) *Giorn. mat. (1) 30 (1892), p. 41.*

361) *Z. Math. Phys. 30 (1885), p. 106, 304.*

362) *Revue math. spéc. 3 (1894/6), p. 201.*

363) *Voir encore *F. Hofmann*, Archiv Math. Phys. (2) 4 (1886), p. 325; *W. Zmurko*, Pamiętnik Akad. Umiejętności (Mém. Cracovie) 12 (1886) II, p. 1/34.*

364) *Ann. sc. mat. fis. 7 (1856), p. 76; Ann. mat. pura appl. (1) 1 (1858), p. 362.*

365) *Giorn. mat. (1) 17 (1879), p. 244 (Note de *G. Vivanti*).*

366) *Mém. Acad. sc. Toulouse (7) 9 (1877), p. 142.*

367) *C. R. Acad. sc. Paris 87 (1878), p. 975; Bull. Acad. Belgique (2) 46 (1878), p. 899 (rapport de *E. Catalan*, id. p. 880); (2) 47 (1879), p. 532 (rapport de *E. Catalan*, id. p. 490); (2) 48 (1879), p. 463, 473, 491 [théorie a posteriori de l'élimination], (rapport de *E. Catalan*, id. p. 445); Théorie de l'élimination entre deux équations algébriques, Paris 1884; Ann. Soc. scient. Bruxelles 18[1] (1893/4), p. 5. Voir encore *Simonnet*, C. R. Acad. sc. Paris 88 (1879), p. 223.*

368) *Nova Acta Upsal. (3) 10 (1879), mém. nº 2.*

369) *Tidsskrift math. Köbenhavn (Copenhague) (4) 3 (1879), p. 78.*

370) *Z. Math. Phys. 33 (1888), p. 184.*

l'autre en

$$a_\lambda,\ b_\lambda,\ a_{\lambda+1},\ b_{\lambda+1},\ \ldots,\ a_{n-\lambda+1},\ b_{n-\lambda+1}$$

$$a_{\lambda-1},\ b_{\lambda-1},\ a_\lambda,\ b_\lambda,\ \ldots,\ a_{n-\lambda},\ b_{n-\lambda}$$

et dont le résultant est le même que celui des deux fonctions $f(z)$ et $\varphi(z)$. *G. Loria*[371]) observe que c'est là précisément la méthode d'élimination de *J. J. Sylvester*. En fait, c'est la *méthode d'Euler* que *G. Vivanti* a retrouvée mais cette *méthode d'Euler* ne diffère pas, au fond, de celle de *J. J. Sylvester*.

E. Pomey[372]) discute les *méthodes d'Euler-Bézout-Sylvester*, puis la *méthode de Bézout-Cauchy*.

P. A. Mac Mahon[373]) exprime le résultant de 2 formes binaires à l'aide du symbole $(pqr\ldots)$ par lequel il désigne la fonction symétrique $\sum(\lambda^p\mu^q\nu^r\ldots)$ des racines $\lambda,\ \mu,\ \nu,\ \ldots$ d'une équation. Ainsi, $\lambda,\ \mu,\ \nu$ étant les trois racines d'une équation du troisième degré, il pose

$$\begin{aligned}
(1) &= \lambda+\mu+\nu,\quad (2)=\lambda^2+\mu^2+\nu^2,\\
(2^2) &= (2,\,2) = \mu^2\nu^2+\nu^2\lambda^2+\lambda^2\mu^2,\\
(1,\,2) &= (2,\,1) = \lambda^2\mu+\lambda^2\nu+\mu^2\nu+\mu^2\lambda+\nu^2\lambda+\nu^2\mu,\\
(1^2) &= (1,\,1) = \mu\nu+\nu\lambda+\lambda\mu,\\
(2^2,\,1) &= (2,\,2,\,1) = \lambda^2\mu^2\nu+\mu^2\nu^2\lambda+\nu^2\lambda^2\mu,\\
(2,\,1^2) &= (2,\,1,\,1) = \lambda^2\mu\nu+\mu^2\nu\lambda+\nu^2\lambda\mu,\\
(1^3) &= (1,\,1,\,1) = \lambda\mu\nu,\quad (2^3)=(2,\,2,\,2)=\lambda^2\mu^2\nu^2.
\end{aligned}$$

Ceci posé, le résultant des deux fonctions rationnelles entières

$$a_3x^3-a_2x^2+a_1x-1 \quad \text{et} \quad x^2-A_1x+A_2$$

est

$$\begin{aligned}
1-(1)A_1+(2)A_2+(1^2)A_1^2-(2\,1)A_2A_1-(1^3)A_1^3\\
+(2^2)A_2^2+(2\,1^2)A_2A_1^2-(2^2 1)A_2^2A_1+(2^3)A_2^3,
\end{aligned}$$

les symboles entre parenthèses indiquant les fonctions symétriques des racines de l'équation $x^3-a_1x^2+a_2x-a_3=0$.*

E. D. Roe[374]) calcule simultanément les fonctions symétriques et les résultants.

**A. Poussart*[375]) s'occupe des théorèmes de *E. Bézout* et de *L. Euler* relatifs au plus grand commun diviseur de deux fonctions rationnelles entières.

371) *Z. Math. Phys. 33 (1888), p. 357.*
372) *Nouv. Ann. math. (3) 7 (1888), p 66, 407.*
373) *Quart. J. pure appl. math. 23 (1889), p. 139.*
374) The Amer. math. Monthly 5 (1898), p. 1, 25, 53; 6 (1899), p. 103, 129, 161; 7 (1900), p. 59.
375) *L'Enseignement math. 2 (1900), p. 136.*

M. Martone[376]) envisage un système de m équations, chacune de degré n où $n \geqq m$, et montre que si ces équations ont au moins $n-m+2$ racines communes, certains déterminants de degré m formés à l'aide des coefficients de ces équations sont tous nuls. Mais les conditions qu'il obtient ainsi ne sont pas suffisantes pour que les m équations envisagées aient effectivement $n-m+2$ racines communes.

On peut consulter *O. Henrici*[377]) au sujet de certaines formules relatives à la théorie des discriminants.

W. K. Clifford[378]) envisage deux fonctions rationnelles entières f et φ de $\omega_1,\ \omega_2,\ \ldots,\ y,\ z,\ \ldots$ où $\omega_1,\ \omega_2,\ \ldots$ sont des produits de la forme

$$\omega_1 = x^{\alpha_1}y^{\beta_1}z^{\gamma_1}\ldots,\quad \omega_2 = x^{\alpha_2}y^{\beta_2}z^{\gamma_2}\ldots,\ \ldots\ldots$$

dans lesquels $\alpha_1+\beta_1+\gamma_1+\cdots,\ \alpha_2+\beta_2+\gamma_2+\cdots,\ \ldots\ldots$ ont la même valeur μ, et qui sont tels que f et φ envisagées comme des fonctions de $x,\ y,\ z,\ldots$ soient des fonctions homogènes de ces variables Désignons par m et n les degrés de ces fonctions homogènes et par h et k les restes de la division de m et de n par μ. Si entre les deux équations $f=0,\ \varphi=0$ on élimine x, le degré en $y,\ z,\ldots$ du résultant est égal à $\frac{mn-hk}{\mu}$.

Citons encore un peu au hasard *José Maria Piñar*[379]), *H. Nägelsbach*[380]), *J. Tœplitz*[381]), *M. A. Baraniecki*[382]), *J. J. Sylvester*[383]), *F. J. Studnička*[384]), *G. Loria*[385]).*

Élimination.

Cas des fonctions de deux variables.

51. Éliminants en x et en y. *Soient

$$f(x,y) = \sum_{(h,\,k)} a_{h,k}x^hy^k,$$

$$\varphi(x,y) = \sum_{(h,\,k)} b_{h,k}x^hy^k$$

376) *Sulle radici comuni a più equazioni, Catanzaro 1891.*
377) *Proc. London math. Soc. (1) 2 (1866/9), p. 104.*
378) *Id. (1) 3 (1869/71), p. 80.*
379) *Lecciones sobre la teoria de la eliminacion, Madrid 1864.*
380) *Z. Math. Phys. 17 (1872), p. 333.*
381) *Z. Math. Phys. 23 (1878), p. 61.*
382) *Pamiętnik towarzystwa nauk ścistych w Paryżu 10, Paris 1878, mém. n° 5.*
383) *Messenger math. (2) 9 (1879/80), p. 162.*
384) *Časopis math. fys. (Prague) 12 (1883), p. 187.*
385) *Jornal sciencias math. astr. (Coïmbre) 9 (1889), p. 33.*

deux fonctions rationnelles entières de x et de y, de degrés n et ν, en sorte que dans la première des deux fonctions les indices h et k prennent toutes les valeurs entières positives ou nulles pour lesquelles $h+k \leqq n$ et dans la seconde toutes ces valeurs pour lesquelles $h+k \leqq \nu$.

On peut se proposer de trouver les racines (ξ, η) communes aux deux équations $f(x,y)=0$, $\varphi(x,y)=0$; nous dirons de chacune de ces racines qu'elle est *racine du système d'équations* $(f=0,\ \varphi=0)$ ou encore qu'elle constitue un *zéro du système de fonctions* (f, φ).*

*Si l'on représente géométriquement $f(x,y)=0$ et $\varphi(x,y)=0$ par deux courbes algébriques planes, chaque racine (ξ, η) du système $(f=0,\ \varphi=0)$ est représentée par un point commun aux deux courbes et les nombres ξ, η sont les coordonnées de ce point.

Nous supposerons dans ce qui suit que les fonctions $f(x,y)$ et $\varphi(x,y)$ sont premières entre elles. Si des fonctions données $F(x,y)$ et $\Phi(x,y)$ ont un p. g. c. d. $\theta(x,y)$, fonction de x, ou de y, ou de x et y, on peut toujours ramener le problème au cas où elles n'en ont pas, en déterminant ce p. g. c. d. et en formant les quotients

$$f(x,y)=\frac{F(x,y)}{\theta(x,y)}, \quad \varphi(x,y)=\frac{\Phi(x,y)}{\theta(x,y)}.$$

Aux racines du système d'équations $(f=0,\ \varphi=0)$ viendront alors s'adjoindre les racines représentées par *tous* les points (ξ, η) de la courbe $\theta(x,y)=0$.

Nous supposerons que les fonctions $f(x,y)$ et $\varphi(x,y)$ soient régulières (n° **2**) de telle sorte que les coefficients a_{0n}, a_{n0}, $b_{0\nu}$, $b_{\nu 0}$ soient tous quatre différents de zéro. Si les deux fonctions données n'étaient pas régulières, on commencerait par les rendre régulières en effectuant sur les variables une substitution linéaire convenablement choisie (n° **2**). Ni l'une ni l'autre des deux courbes $f=0$, $\varphi=0$ n'a alors de direction asymptotique parallèle à l'un des axes de coordonnées.

Ordonnons $f(x,y)$ et $\varphi(x,y)$ suivant les puissances décroissantes de l'une des variables, y par exemple, et désignons par f_y, φ_y les fonctions rationnelles entières de y ainsi obtenues

$$f_y = a_0 y^n + a_1 y^{n-1} + \cdots + a_{n-1} y + a_n,$$
$$\varphi_y = b_0 y^\nu + b_1 y^{\nu-1} + \cdots + b_{\nu-1} y + b_\nu$$

où

$$a_0 = a_{0,n}, \quad a_1 = a_{0,n-1} + a_{1,n-1} x, \quad \ldots,$$
$$b_0 = b_{0,\nu}, \quad b_1 = b_{0,\nu-1} + b_{1,\nu-1} x, \quad \ldots$$

et en général

$$a_i = a_{0,n-i} + a_{1,n-i} x + \cdots + a_{i,n-i} x^i,$$
$$b_i = b_{0,\nu-i} + b_{1,\nu-i} x + \cdots + b_{i,\nu-i} x^i.\text{*}$$

*Formons le résultant $R(f_y, \varphi_y)$; c'est une fonction rationnelle entière de x que l'on appelle *l'éliminant* en x des deux fonctions $f(x,y)$ et $\varphi(x,y)$; nous le désignerons par $E_1(x)$. Nous désignerons de même par $E_2(y)$ l'éliminant en y obtenu en formant le résultant $R(f_x, \varphi_x)$ des deux fonctions f_x, φ_x de x obtenues en ordonnant $f(x,y)$, $\varphi(x,y)$ suivant les puissances décroissantes de x.

Les fonctions $E_1(x)$, $E_2(y)$ sont homogènes de degré ν par rapport aux $a_{h,k}$, homogènes de degré n par rapport aux $b_{h,k}$. Si l'on donne à chaque $a_{h,k}$ le poids $n-h-k$, à chaque $b_{h,k}$ le poids $\nu-h-k$ et à chacune des deux variables x, y le poids 1, les fonctions $f(x,y)$ et $\varphi(x,y)$ sont isobariques (n° **7**) de poids respectifs n et ν tandis que les fonctions $E_1(x)$ et $E_2(y)$ sont isobariques de poids $n\nu$ en sorte que leurs degrés par rapport à x ou à y sont $\leqq n\nu$.

Si (ξ, η) est une racine du système $(f=0,\ \varphi=0)$, les équations en y

$$f(\xi, y)=0, \quad \varphi(\xi, y)=0$$

ont la solution commune $y=\eta$ et ξ annule l'éliminant $E_1(x)$. Inversement, si $x=\xi$ est une racine de l'équation $E_1(x)=0$, les deux fonctions $f(\xi, y)$ et $\varphi(\xi, y)$ de y ont un p. g. c. d. et si η est un zéro de ce p. g. d. c., (ξ, η) est une racine du système d'équations $(f=0, \varphi=0)$. On voit donc que la recherche des racines d'un système d'équations $(f=0,\ \varphi=0)$ revient à la résolution de l'équation $E_1(x)=0$. En transposant x et y on verrait de même qu'elle revient aussi, si l'on veut, à la résolution de l'équation $E_2(y)=0$.

Désignons par f_n et φ_ν l'ensemble des termes des fonctions $f(x,y)$ et $\varphi(x,y)$ de degré respectivement égal à n et à ν et convenons (n° **49**) d'appeler *résultant* $R(f_n, \varphi_\nu)$ des deux fonctions homogènes f_n et φ_ν le résultant des deux fonctions d'une variable que l'on obtient en faisant $y=1$ dans f_n et dans φ_ν.

Quand les coefficients $a_{00}, a_{01}, \ldots, a_{nn}, b_{00}, b_{01}, \ldots, b_{\nu\nu}$ sont déterminés nous dirons que nous sommes dans le *cas général* lorsque le résultant $R(f_n, \varphi_\nu)$ est différent de zéro. Dans le cas général les courbes $f(x,y)=0$, $\varphi(x,y)=0$ n'ont donc aucune direction asymptotique commune; la seule solution qui annule f_n et φ_ν simultanément est $x=0$, $y=0$.

Quand les coefficients $a_{00}, a_{10}, \ldots, a_{nn}, b_{00}, b_{10}, \ldots, b_{\nu\nu}$ des fonctions rationnelles entières $f(x,y)$, $\varphi(x,y)$ dépendent de paramètres indéterminés $\lambda_1, \lambda_2, \ldots$, nous dirons que nous sommes dans le cas général lorsque le résultant $R(f_n, \varphi_\nu)$ ne s'annule pas identiquement en $\lambda_1, \lambda_2, \ldots$.

Quand les coefficients $a_{00}, a_{10}, \ldots, a_{nn}, b_{00}, b_{10}, \ldots, b_{\nu\nu}$ sont des indéterminées indépendantes les unes des autres on est donc dans le cas général.

Plaçons-nous dans le cas général. Les degrés des deux éliminants $E_1(x)$, $E_2(y)$ sont alors tous deux égaux à $n\nu$. Prenons l'une quelconque de ces deux fonctions, $E_1(x)$ par exemple; soient $\xi_1, \xi_2, \ldots$ les racines distinctes de l'équation $E_1(x) = 0$ et soient $\alpha_1, \alpha_2, \ldots$ les ordres respectifs de multiplicité de ces racines, en sorte que $\alpha_1 + \alpha_2 + \cdots = n\nu$.

A la racine ξ_i correspond un p. g. c. d. des deux fonctions $f(\xi_i, y)$ et $\varphi(\xi_i, y)$ de y qui est de degré α_i en y; si l'on égale à zéro ce p. g. c. d. on a α_i valeurs

$$\eta_{i1}, \; \eta_{i2}, \; \cdots$$

distinctes ou non. Le nombre total des racines (ξ, η) du système d'équations $(f = 0, \; \varphi = 0)$ sera égal à $n\nu$; les deux courbes $f(x, y) = 0$, $\varphi(x, y) = 0$ ont $n\nu$ points communs, distincts ou non, tous à distance finie.*

Le théorème fondamental, d'après lequel le nombre des racines du système d'équations $(f = 0, \; \varphi = 0)$ est égal à $n\nu$ dans le cas général, a d'abord été énoncé par *C. Maclaurin*[386]); *G. Cramer*[387]) et *L. Euler*[388]) ont essayé d'en donner une démonstration, sans d'ailleurs préciser ce qu'il faut entendre par cas général. La première démonstration est due à *E. Bézout*[389]).

52. Eliminant en $ux + vy$. La détermination *simultanée* des deux coordonnées des points communs aux deux courbes $f(x, y) = 0$, $\varphi(x, y) = 0$ peut être obtenue par une méthode due à *S. D. Poisson*[390]) *et employée systématiquement par *J. Liouville*[391])*. Cette méthode consiste essentiellement à former une combinaison linéaire des variables x et y avec des coefficients *indéterminés*. Soit

$$z = ux + vy;$$

posons

$$v^n f\left(x, \frac{z - ux}{v}\right) = g(x, z),$$

$$v^\nu \varphi\left(x, \frac{z - ux}{v}\right) = \psi(x, z)$$

386) Geometria organica, Londres 1720, p. 136.

387) Introd. [31]), p. 673/6.

388) Hist. Acad. Berlin 4 (1748), éd. 1750, p. 234.

389) Cours de math. à l'usage des gardes du pavillon et de la marine 3, Paris 1766, p. 209 et suiv.

390) J. Ec. polyt. (1) cah. 11 (an X), p. 199.

391) *J. math. pures appl. (1) 12 (1847), p. 68.*

et formons l'éliminant en z des deux fonctions rationnelles entières $g(x, z)$, $\psi(x, z)$. Le degré de cet éliminant que nous désignerons par $E(z)$ est $n\nu$ comme ceux de $E_1(x)$ et de $E_2(y)$ et l'éliminant $E(z)$ peut jouer le même rôle que $E_1(x)$ ou $E_2(y)$ dans la recherche des racines du système d'équations $(f = 0, \; \varphi = 0)$; mais le calcul de ces racines est notablement simplifié par la présence des indéterminées u et v.

*Ordonnons $E(z)$ suivant les puissances décroissantes de z

$$E(z) = \varrho_0 z^{n\nu} + \varrho_1 z^{n\nu - 1} + \cdots + \varrho_{n\nu - 1} z + \varrho_{n\nu};$$

le coefficient ϱ_0 de $z^{n\nu}$ est indépendant de u et de v; c'est le résultant de f_n et φ_ν; le coefficient ϱ_i de $z^{n\nu - i}$ est homogène de degré i en u, v. Chaque coefficient ϱ est homogène de degré ν par rapport aux $a_{h,k}$ et homogène de degré n par rapport aux $b_{h,k}$. Si l'on donne aux indéterminées u, v le poids 0, z aura comme x et y le poids 1 et $E(z)$ sera isobarique de poids $n\nu$ comme précédemment $E_1(x)$ et $E_2(y)$.

Toute racine ζ_i de l'équation $E(z) = 0$ sera une *forme linéaire* de u et de v

$$\zeta_i = u\xi_i + v\eta_i$$

et les coefficients ξ_i, η_i de u et de v dans cette forme linéaire seront les coordonnées d'une des racines du système d'équations $(f = 0, \; \varphi = 0)$. Aux $n\nu$ racines ζ_i distinctes ou non de l'équation $E(z) = 0$ correspondent ainsi univoquement les $n\nu$ racines distinctes ou non du système d'équations $(f = 0, \; \varphi = 0)$.

Lorsque l'éliminant $E(z)$ égalé à zéro admet une racine

$$\zeta_i = u\xi_i + v\eta_i$$

d'ordre de multiplicité q, on dit que le point correspondant (ξ_i, η_i) est un *point multiple* d'ordre q. *Le système d'équations* $(f = 0, \; \varphi = 0)$ *a alors une racine multiple* (ξ_i, η_i) *d'ordre* q.

Supposons maintenant que l'on ne soit pas dans le cas général. On a alors toujours

$$\varrho_0 = R(f_n, \varphi_\nu) = 0;$$

les deux courbes $f(x, y) = 0$ et $\varphi(x, y) = 0$ ont des directions asymptotiques communes et des points communs à l'infini. Le degré de l'éliminant $E(z)$ s'abaisse; si les deux fonctions $f(x, y)$ et $\varphi(x, y)$ sont toutes deux régulières les degrés de $E_1(x)$ et de $E_2(y)$ s'abaissent aussi.

J. Liouville[391]) a démontré que, les deux fonctions $f(x, y)$ et $\varphi(x, y)$ étant supposées sans diviseur commun, à chaque diminution d'une unité dans le degré $n\nu$ de l'éliminant en z correspond une racine infinie du système d'équations ($f=0$, $\varphi=0$) en sorte que le nombre de racines finies, distinctes ou non, du système d'équations ($f=0$, $\varphi=0$) est précisément égal au degré de l'éliminant en z [et aussi, quand les fonctions $f(x, y)$, $\varphi(x, y)$ sont toutes deux *régulières*, aux degrés des éliminants $E_1(x)$ et $E_2(y)$].

Ce fait se présente et ne se présente que quand les deux fonctions $f_n(x, y)$ et $\varphi_\nu(x, y)$ ont un p. g. c. d.; soit $\alpha y - \beta x$ un des facteurs de ce p. g. c. d. et q son ordre de multiplicité; $\frac{\beta}{\alpha}$ est le coefficient angulaire d'une direction asymptotique d'ordre q commune aux deux courbes $f(x, y)=0$, $\varphi(x, y)=0$. On dit dans ce cas que *le système d'équations* ($f=0$, $\varphi=0$) *a une racine infinie* de la forme

$$x=\alpha t, \quad y=\beta t, \quad \text{où } t=+\infty$$

et que cette racine est *d'ordre de multiplicité* q. Si s est la somme des ordres de multiplicité q des facteurs du p. g. c. d. de f_n et φ_ν, les coefficients $\varrho_0, \varrho_1, \ldots, \varrho_{s-1}$ de l'éliminant $E(z)$ sont nuls, en sorte que les éliminants sont de degré $(n\nu - s)$.*

*Si l'on compte chaque racine infinie autant de fois que l'indique son ordre de multiplicité, tout système d'équations

$$f(x, y)=0, \quad \varphi(x, y)=0,$$

où $f(x, y)$ et $\varphi(x, y)$ sont deux fonctions rationnelles entières sans diviseur commun, se trouve avoir exactement $n\nu$ racines.

Si l'éliminant $E(z)$ est de degré $n\nu-\sigma$ les coefficients

$$\varrho_{\sigma+1}, \varrho_{\sigma+2}, \ldots, \varrho_n$$

envisagés comme des fonctions de u et v sont divisibles par ϱ_σ. Les racines infinies du système d'équations ($f=0$, $\varphi=0$) s'obtiennent si l'on veut en décomposant ϱ_σ en ses facteurs linéaires. A chaque facteur linéaire $\alpha u+\beta v$ figurant q fois dans ϱ_σ correspond la racine infinie d'ordre de multiplicité q

$$x=\alpha t, \quad y=\beta t \quad \text{où } t=\infty$$

de ce système d'équations ($f=0$, $\varphi=0$).

L'éliminant $E(z)$ d'un système quelconque d'équations ($f=0$, $\varphi=0$) détermine ainsi les $n\nu$ racines de ce système, aussi bien ses racines infinies que ses racines finies, chacune avec son ordre de multiplicité[392]).*

392) *Cf. *Gy. (J.) König*, Alg. Grössen[20]), p. 305, où le même fait est mis en évidence dans le cas où l'on a un nombre quelconque m d'équations algébriques entre le même nombre m de variables (Texte et note de *J. Kürschák*).*

En ce qui concerne les racines multiples, on peut, en s'appuyant sur les résultats obtenus par *W. F. Meyer* dans l'étude de la structure des résultants des formes binaires (nº **42**), non seulement démontrer que, si (ξ, η) est une racine multiple d'ordre m de l'équation $f(x, y)=0$ et une racine multiple d'ordre μ de l'équation $\varphi(x, y)=0$ (nº **22**), la racine (ξ, η) est multiple d'ordre $m\mu$ au moins du système d'équations

$$(f=0, \ \varphi=0),$$

mais encore trouver aisément les conditions pour que cet ordre de multiplicité soit précisément égal à $m\mu$.[393])

Les éliminants ne peuvent jamais être identiquement nuls puisqu'on a supposé que les deux fonctions $f(x, y)$ et $\varphi(x, y)$ n'ont pas de diviseur commun.

53. Méthode de Labatie. Comme on vient de le voir, le degré de l'éliminant $E(z)$, où $z=ux+vy$, de deux fonctions rationnelles entières $f(x, y)$, $\varphi(x, y)$ *à coefficients donnés*, indique *exactement* le nombre de racines finies du système d'équations ($f=0$, $\varphi=0$), et ces racines elles-mêmes sont données par celles de l'équation $E(z)=0$.

Le calcul effectif de ces racines offre toutefois, le plus souvent, de grandes difficultés; c'est pourquoi divers auteurs ont cherché des procédés directs permettant d'obtenir pratiquement ces racines quand les coefficients ont des valeurs numériques données. Ces procédés ne supposent pas que les fonctions données soient régulières; il en résulte que, les éliminants $E(z)$, $E_1(x)$, $E_2(y)$ n'étant plus forcément du même degré, les coordonnées de certaines racines peuvent être l'une finie l'autre infinie; cela se présente quand les courbes $f(x, y)=0$, $\varphi(x, y)=0$ ont des asymptotes communes parallèles aux axes.

Soient $F(x, y)$, $\Phi(x, y)$ les deux fonctions données, $D(F, \Phi)$ leur p. g. c. d., en sorte que

$$F(x, y)=D(F, \Phi)\,F_1(x, y),$$
$$\Phi(x, y)=D(F, \Phi)\,\Phi_1(x, y).$$

Les racines du système d'équations

$$(F=0, \ \Phi=0)$$

se composent des racines de l'équation $D(F, \Phi)=0$ qui forment une variété à une dimension (ou courbe algébrique) et des racines du système d'équations

$$(F_1=0, \ \Phi_1=0)$$

où les deux fonctions $F_1(x, y)$ et $\Phi_1(x, y)$ sont premières entre elles.

393) *E. Netto*, Alg.[27]) 2, p. 49; *W. F. Meyer*, Nachr. Ges. Gött. 1895, math. p. 119, 155.

Désignons par $g(x)$ et $l(y)$ les p. g. c. d. des coefficients de la fonction F_1 supposée ordonnée respectivement suivant les puissances de y et de x, et par $\gamma(x)$ et $\lambda(y)$ les p. g. c. d. des coefficients de la fonction Φ_1 supposée ordonnée respectivement suivant les puissances de y et de x, en sorte que

$$F_1(x, y) = g(x)\, l(y)\, f(x, y),$$
$$\Phi_1(x, y) = \gamma(x) \lambda(y) \varphi(x, y).$$

Les solutions des systèmes

$$(g(x) = 0,\ \lambda(y) = 0), \quad (\gamma(x) = 0,\ l(y) = 0)$$
$$(g(x) = 0,\ \varphi(x, y) = 0), \quad (\gamma(x) = 0,\ f(x, y) = 0)$$

sont immédiates; on est donc finalement ramené à rechercher les racines du système d'équations

$$(f = 0,\ \varphi = 0),$$

où $f(x, y)$ et $\varphi(x, y)$ sont des fonctions rationnelles entières primitives (n° **3**) par rapport à chacune des deux variables x, y.

Effectuons[394] sur les deux fonctions $f(x, y)$ et $\varphi(x, y)$ ordonnées suivant les puissances décroissantes de y les opérations du p. g. c. d. Cette opération introduit des dénominateurs fonctions de x seulement, et en multipliant par des fonctions rationnelles entières de x convenables on obtient l'algorithme

$$\begin{aligned}
u_1 f &= \varphi q + \varphi_1 v_1, \\
u_2 \varphi &= \varphi_1 q_1 + \varphi_2 v_2, \\
u_3 \varphi_1 &= \varphi_2 q_2 + \varphi_3 v_3, \\
&\cdots\cdots\cdots \\
u_{n-1} \varphi_{n-3} &= \varphi_{n-2} q_{n-2} + \varphi_{n-1} v_{n-1}, \\
u_n \varphi_{n-2} &= \varphi_{n-1} q_{n-1} + v_n,
\end{aligned}$$

où $q, q_1, q_2, \ldots, q_{n-2}, q_{n-1}, \varphi_1, \varphi_2, \varphi_3, \ldots, \varphi_{n-3}, \varphi_{n-2}, \varphi_{n-1}$ sont des fonctions rationnelles entières de x et de y, tandis que $u_1, u_2, u_3, \ldots, u_{n-1}, u_n, v_1, v_2, v_3, \ldots, v_{n-1}, v_n$ sont des fonctions rationnelles entières de x seulement; on choisira $v_1, v_2, \ldots, v_n$ de façon que $\varphi_1, \varphi_2, \ldots, \varphi_{n-1}$ soient des fonctions primitives en y.

Déterminons ensuite successivement le p. g. c. d. d_1 de u_1 et de v_1, le p. g. c. d. d_2 de $\frac{u_1 u_2}{d_1}$ et de v_2, le p. g. c. d. d_3 de $\frac{u_1 u_2 u_3}{d_1 d_2}$ et de $v_3, \ldots$, enfin le p. g. c. d. d_n de $\frac{u_1 u_2 u_3 \ldots u_n}{d_1 d_2 \ldots d_{n-1}}$ et de v_n.

394) *Labatie* (de Douai) Méthode d'élimination par le p. g. c. d. entièrement rectifiée et appliquée ... Paris 1835. *Une première édition (anonyme) signée *L.* avait paru à Paris en 1832 sous le titre: Méthode d'élimination par le p. g. c. d.*

Ceci posé, les racines du système d'équations

$$(f = 0,\ \varphi = 0)$$

sont précisément les racines des n systèmes

$$\left(\varphi = 0,\ \frac{v_1}{d_1} = 0\right), \quad \left(\varphi_1 = 0,\ \frac{v_2}{d_2} = 0\right), \quad \ldots, \quad \left(\varphi_{n-1} = 0,\ \frac{v_n}{d_n} = 0\right).$$

Chacun de ces n systèmes se compose d'une équation en x seulement et d'une équation en x et y. A chacune des racines de l'équation en x d'un système, correspondent autant de valeurs de y qu'il y a d'unités dans le degré, par rapport à y, de l'équation en x et y du même système[395].

54. Règle de Minding. La *règle de Minding*[396] a pour objet de permettre de déterminer avec précision dans chaque cas particulier le degré de l'éliminant; elle repose sur le développement en séries en x des différentes racines y d'une équation algébrique $f(x, y) = 0$, développement déjà indiqué par *I. Newton.*

Ces séries en x peuvent s'obtenir à l'aide d'une correspondance entre les termes de $f(x, y)$ et les points d'un plan à coordonnées entières: au terme

$$a_{\alpha\beta} x^\alpha y^\beta$$

de $f(x, y)$ on fait correspondre le point de coordonnées α, β et on se sert d'une ligne polygonale dite *ligne polygonale de Newton*[397].

395) Voir *J. J. Bret,* J. Ec. polyt. (1) cah. 15 (1809), p. 162; *J. Petersen,* Tidsskrift math. Köbenhavn (Copenhague) (3) 4 (1874), p. 83.

396) *E. F. A. Minding,* J. reine angew. Math. 22 (1841), p. 178; J. math. pures appl. (1) 6 (1841), p. 412.

397) Lettre à *H. Oldenbourg*[12]) datée du 24 octobre 1676 (epistola posterior); De Analysi per aequationes numero terminorum infinitas, Londres 1711 [1669]; Methodus fluxionum [cf. I 1, **26** note 186], Londres 1736; Opuscula, éd. *J. Castillon* 1, Lausanne et Genève 1744, Opusc. I, II, XI, p. 13, 39, 351/2; Opera, éd. *S. Horsley* 1, Londres 1779, p. 257; 4, Londres 1782, p. 540. Voir, à ce sujet, *J. Wallis,* A treatise of algebra, Londres 1685, p. 339/40; *Brook Taylor,* Methodus incrementorum directa et inversa, Londres 1715, p. 28; *J. P. de Gua,* Analyse de Descartes[204]), p. 24; *G. Cramer,* Introd.[31]), p. 165; *A. G. Kästner,* Anfangsgründe der Analysis endlicher Grössen, Göttingue 1759; (3e éd.) Göttingue 1794, p. 419/87; *V. Puiseux,* J. math pures appl. (1) 15 (1850), p. 365; *A. Clebsch,* Vorles. über Geometrie, publ. par *F. Lindemann,* Leipzig 1876, p. 331; trad. *Ad. Benoist* 2, Paris 1880, p. 37; *H. R. Baltzer,* Analyt. Geom., Leipzig 1882, p. 295; *E. Cosserat,* Ann. Fac. sc. Toulouse 4 (1890), mém. n° 15, p. 1/16; *C. Jordan,* Cours d'Analyse (2e éd.) 1, Paris 1895, p. 90; *E. Vessiot,* Bull. sc. math. (2) 20 (1896), p. 29; *E. Netto,* Alg.[27]) 2, p. 51; *K. Hensel* et *G. Landsberg,* Theorie der algebraischen Functionen einer Variabeln und ihre Anwendung auf algebraische Kurven und Abelsche Integrale, Leipzig 1903, p. 39 et suiv.

C'est une ligne polygonale convexe vers l'origine dont tous les sommets sont des points (α, β) et qui est telle que chacun de ses côtés prolongé indéfiniment laisse ceux des points (α, β) qu'il ne contient pas dans la région du plan qui ne renferme pas l'origine des coordonnées.

La *règle de Minding* consiste à calculer les premiers termes des développements de $y_1, y_2, \ldots, y_n$ suivant les puissances *décroissantes* de x. Les exposants $h_1, h_2, \ldots$ du premier terme dans les développements des racines $y_1, y_2, \ldots$ sont alors les inverses, changés de signe, des coefficients angulaires des côtés successifs de la *ligne polygonale de Newton*; ce sont des nombres positifs entiers ou fractionnaires.

*Soient deux équations algébriques

$$f(x, y) = 0, \quad \varphi(x, y) = 0;$$

désignons par f_y et φ_y les fonctions $f(x, y)$ et $\varphi(x, y)$ ordonnées suivant les puissances décroissantes de y et soit

$$f_y = a_0 y^n + a_1 y^{n-1} + \cdots + a_{n-1} y + a_n = 0,$$
$$\varphi_y = b_0 y^\nu + b_1 y^{\nu-1} + \cdots + b_{\nu-1} y + b_\nu = 0,$$

$a_0, a_1, \ldots, a_{n-1}, a_n$; $b_0, b_1, \ldots, b_{\nu-1}, b_\nu$ désignant des fonctions rationnelles entières en x. Soient $y_1, y_2, \ldots, y_\nu$ les racines de l'équation en y

$$\varphi_y = b_0 y^\nu + b_1 y^{\nu-1} + \cdots + b_\nu = 0.$$

Soient enfin $c_1 x^{h_1}, c_2 x^{h_2}, \ldots, c_\nu x^{h_\nu}$ les premiers termes des développements de $y_1, y_2, \ldots, y_\nu$ suivant les puissances décroissantes de x.

Pour calculer le degré du résultant

$$\psi(x) = b_0{}^n f(x, y_1)\, f(x, y_2) \ldots f(x, y_\nu),$$

obtenu en éliminant y entre les deux équations $f(x, y) = 0$, $\varphi(x, y) = 0$, on détermine les degrés $k_1, k_2, \ldots, k_\nu$ de $f(x, y_1), f(x, y_2), \ldots, f(x, y_\nu)$ et le degré b de b_0; le degré de $\psi(x)$ est alors égal à

$$nb + k_1 + k_2 + \cdots + k_\nu.$$

En général pour déterminer le degré k_α de $f(x, y_\alpha)$ il suffit de déterminer le degré de $f(x, c_\alpha x^{h_\alpha})$. Quelquefois cependant, pour avoir le degré k_α du facteur $f(x, y_\alpha)$, il est nécessaire de calculer *plusieurs* termes du développement de y_α; cela arrive lorsque en remplaçant y par son développement

$$y = c_i x^{h_i} + \cdots$$

dans $f(x, y)$, le terme de degré le plus élevé en x s'annule par suite de la valeur particulière de c_i.

L. J. Magnus[398]) a cru trouver la méthode en défaut. *E. F. A. Minding*[399]) montre que l'objection de *L. J. Magnus* tombe si l'on a soin de calculer dans le développement de y_α un nombre suffisant de termes.*

398) *J. reine angew. Math. 26 (1843), p. 365.*

Dans un autre mémoire[400]) *E. F. A. Minding* utilise *simultanément* les zéros de f_y et de φ_y considérées comme des fonctions de y et emploie la forme du résultant

$$\psi(x) = R(f_y, \varphi_y) = a_0{}^\nu b_0{}^n \prod_{(i,k)} (\eta_i - y_k),$$

où $y_1, y_2, \ldots, y_\nu$ continuent à désigner les racines de l'équation

$$\varphi_y = b_0 y^\nu + b_1 y^{\nu-1} + \cdots + b_{\nu-1} y + b_\nu = 0$$

tandis que $\eta_1, \eta_2, \ldots$ sont les racines de l'équation

$$f_y = a_0 y^n + a_1 y^{n-1} + \cdots + a_n = 0.$$

*Si l'on remplace les η_i et les y_k par leurs développements suivant les puissances décroissantes de x et si, dans ces développements, le degré du premier terme de η_i est égal au nombre entier ou fractionnaire ε_i, tandis que le degré du premier terme de y_k est égal au nombre entier ou fractionnaire h_k, le développement de $\eta_i - y_k$ commence par un terme dont le degré est le plus grand des deux nombres ε_i, h_k lorsque ces nombres sont distincts, tandis qu'il est plus petit quand ces deux nombres sont égaux et que les coefficients de x^{ε_i}, x^{h_k} sont égaux dans les développements de η_i, y_k.

Rangeons les nombres $\varepsilon_1, \varepsilon_2, \ldots, h_1, h_2, \ldots$ par ordre de grandeurs croissantes; si deux de ces nombres sont égaux, l'ordre dans lequel ils sont placés est indifférent; désignons par s_i le nombre des ε qui suivent h_i et par σ_i le nombre des h qui suivent ε_i dans la suite des ε et h ainsi formée; désignons enfin par α_0 et β_0 les degrés en x de a_0 et b_0. Le degré de $\psi(x)$ est, en général,

$$\nu\alpha_0 + n\beta_0 + \sum s_i h_i + \sum \sigma_i \varepsilon_i;$$

ce nombre est réellement atteint lorsque aucun des ε n'est égal à l'un des h; il peut être diminué quand l'un au moins des ε est égal à l'un des h, et dans ce cas il est nécessaire de calculer dans les développements de η_i et de y_k assez de termes pour que l'on connaisse le terme de degré le plus élevé dans la différence $\eta_i - y_k$.

P. J. E. Finck[401]) essaie d'éviter l'emploi des séries dont on fait usage pour appliquer la *règle de Minding*.*

399) *J. reine angew. Math. 27 (1844), p. 379. Cf. *J. A. Serret*, Alg. sup.[30]) 1, p. 636.*

400) J. reine angew. Math. 31 (1846), p. 1.

401) *J. math. pures appl. (1) 9 (1844), p. 334.*

55. Cas de trois fonctions de deux variables. *Envisageons trois fonctions rationnelles entières

$$f(x, y), \quad \varphi(x, y), \quad \psi(x, y)$$

de deux variables x, y, à coefficients indéterminés; désignons par n, ν, σ leurs degrés respectifs; et convenons de donner aux coefficients du terme $x^h y^k$ dans ces trois fonctions respectivement les poids

$$n - (h + k), \qquad \nu - (h + k), \qquad \sigma - (h + k)$$

conformément à la règle du nº 7. Soient alors

$$(\xi_1, \eta_1), (\xi_2, \eta_2), \ldots, (\xi_{n\nu}, \eta_{n\nu})$$

les $n\nu$ racines du système d'équations $(f = 0, \ \varphi = 0)$ et soit ϱ_0 le résultant des deux fonctions homogènes f_n et φ_ν des deux variables x et y, formées respectivement par l'ensemble des termes de degré n de f et par l'ensemble des termes de degré ν de φ.

Ceci posé, on appelle *résultant* des trois fonctions envisagées l'expression

$$R(f, \varphi, \psi) = \varrho_0{}^\sigma \prod_{\alpha=1}^{\alpha=n\nu} \psi(\xi_\alpha, \eta_\alpha).$$

L'expression $R(f, \varphi, \psi)$ ainsi définie est une fonction rationnelle entière irréductible des coefficients des trois fonctions $f(x, y)$, $\varphi(x, y)$, $\psi(x, y)$.

Le résultant $R(f, \varphi, \psi)$ est homogène de degré $\nu\sigma$ par rapport aux coefficients de $f(x, y)$, homogène de degré σn par rapport aux coefficients de $\varphi(x, y)$, homogène de degré $n\nu$ par rapport aux coefficients de $\psi(x, y)$, isobarique de poids $n\nu\sigma$ par rapport aux coefficients de $f(x, y)$, $\varphi(x, y)$ et $\psi(x, y)$ réunis.

Lorsque les coefficients des trois fonctions $f(x, y)$, $\varphi(x, y)$, $\psi(x, y)$ sont des nombres déterminés ou dépendent de paramètres déterminés, on appelle *résultant* de ces trois fonctions l'expression que l'on obtient en formant d'abord le résultant des mêmes fonctions dans lesquelles les coefficients sont remplacés par des indéterminées et remplaçant ensuite dans la fonction $R(f, \varphi, \psi)$ ainsi formée les coefficients indéterminés par les coefficients déterminés donnés.

La condition nécessaire et suffisante pour que les trois équations

$$f(x, y) = 0, \quad \varphi(x, y) = 0, \quad \psi(x, y) = 0$$

aient une racine commune finie ou infinie est que l'on ait

$$R(f, \varphi, \psi) = 0.$$

Les recherches qui seront mentionnées au nº **59** dans le cas général, où il s'agit du résultant de $m + 1$ fonctions de m variables, s'appliquent ici pour $m = 2$.*

Élimination.

Cas des fonctions de plus de deux variables.

56. Cas de m équations à m variables. Soient maintenant

$$f_1(z_1, z_2, \ldots, z_m), \quad f_2(z_1, z_2, \ldots, z_m), \ldots, \quad f_m(z_1, z_2, \ldots, z_m)$$

m fonctions rationnelles entières de m variables $z_1, z_2, \ldots, z_m$ de degrés respectifs $n_1, n_2, \ldots, n_m$. On appelle *racines du système d'équations* $(f_1 = 0, \ f_2 = 0, \ \ldots, \ f_m = 0)$ les racines communes aux m équations algébriques $f_1 = 0$, $f_2 = 0$, $\ldots$, $f_m = 0$.

Pour trouver les racines du système $(f_1 = 0, f_2 = 0, \ldots, f_m = 0)$, la première méthode qui se présente à l'esprit, comme généralisation de celle que l'on a suivie dans le cas de deux variables, consiste à éliminer une des variables, z_1 par exemple, entre la première équation $f_1 = 0$ et chacune des suivantes $f_2 = 0, \ldots, f_m = 0$; on forme ainsi $m - 1$ équations contenant $m - 1$ variables

$$g_2(z_2, z_3, \ldots, z_m) = 0, \quad g_3(z_2, z_3, \ldots, z_m) = 0, \ldots, \quad g_m(z_2, z_3, \ldots z_m) = 0$$

dont les degrés respectifs sont égaux ou inférieurs à

$$n_1 n_2, \quad n_1 n_3, \quad \ldots, \quad n_1 n_m.$$

Entre l'équation $g_2 = 0$ et chacune des $(m - 2)$ équations suivantes $g_3 = 0, \ldots, g_m = 0$ on élimine ensuite z_2 et l'on forme ainsi $(m - 2)$ équations à $(m - 2)$ inconnues dont les degrés respectifs sont égaux ou inférieurs à

$$n_1{}^2 n_2 n_3, \quad n_1{}^2 n_2 n_4, \quad \ldots, \quad n_1{}^2 n_2 n_m.$$

Et ainsi de suite. Finalement on parvient ainsi à une seule équation à une seule inconnue dont le degré est égal ou inférieur à

$$n_1{}^{2^{m-2}} \cdot n_2{}^{2^{m-3}} \cdots n_{m-2}^2 n_{m-1} n_m.$$

Mais la fonction $F(z_m)$ ainsi obtenue ne saurait jouer un rôle analogue à celui que joue l'*éliminant* dans le cas de deux variables parce qu'elle contient, en général, des facteurs fournissant des solutions étrangères à la question. Ce n'est que dans le cas où les m équations algébriques données sont *linéaires* que cette méthode peut s'appliquer sans inconvénient dans tous les cas.

On pourrait être tenté de croire que *l'artifice de Poisson-Liouville* (nº **52**) qui consiste essentiellement à introduire, *avant* l'élimination successive de $z_1, z_2, \ldots, z_{m-1}$, au lieu de z_m une variable

$$z = \lambda_1 z_1 + \lambda_2 z_2 + \cdots + \lambda_m z_m$$

où $\lambda_1, \lambda_2, \ldots, \lambda_m$ désignent des indéterminées, permet de se débarrasser des facteurs étrangers. Il n'en est rien, comme on peut aisément le constater sur un exemple[402]).

57. Méthode de Bézout. *E. Bézout* semble avoir le premier reconnu que la fonction $F(z_m)$ contient des facteurs étrangers à la question. Pour obvier à cet inconvénient il cherche à éliminer *simultanément*[403]), au lieu de *successivement*, les $(m-1)$ variables $z_1, z_2, \ldots, z_{m-1}$. Il se place dans le cas où les coefficients des fonctions $f_1, f_2, \ldots, f_m$ sont indéterminés et il cherche alors à déterminer m fonctions rationnelles entières $\varphi_1, \varphi_2, \ldots, \varphi_m$ de façon que la somme $f_1\varphi_1 + f_2\varphi_2 + \cdots + f_m\varphi_m$ soit indépendante de $z_1, z_2, \ldots, z_{m-1}$. En comptant le nombre des coefficients inconnus, il constate que la détermination des fonctions φ_λ dépend d'équations linéaires dont le nombre ne dépasse pas celui des inconnues, en sorte que ces fonctions $\varphi_1, \varphi_2, \ldots, \varphi_m$ peuvent être déterminées d'une infinité de manières; φ_α peut en général[404]) être choisie de degré $n_1 n_2 \ldots n_m - n_\alpha$.

J. A. Serret[405]) a essayé de montrer que les équations linéaires envisagées sont toujours compatibles; à cet effet il se place dans un cas particulier, ce qui est insuffisant comme l'a montré *Carl Schmidt*[406]). Ce dernier remarque aussi que, dans l'exposé de *J. A. Serret*[407]), φ_m n'est pas la fonction rationnelle entière la plus générale de degré $n_1 n_2 \ldots n_m - n_m$, et il montre qu'il faut lever cette restriction.

E. Bézout[408]) a démontré que, quand les coefficients des fonctions $f_1, f_2, \ldots, f_m$ sont indéterminés, le degré de la fonction de z_m (indépendante de $z_1, z_2, \ldots, z_{m-1}$)

$$R(z_m) = f_1\varphi_1 + f_2\varphi_2 + \cdots + f_m\varphi_m$$

est précisément égal à $n_1 n_2 \ldots n_m$; il en conclut que le nombre des racines du système d'équations

402) *E. Netto*, Alg.[27]) 2, p. 99.

403) Equations alg.[18]), préface et livre 2; cf. *E. Netto*, Alg.[27]) 2, p. 98.

404) *E. Netto*, Alg.[27]) 2, p. 100.

405) Alg. sup.[30]) 1, p. 158/9.

406) Z. Math. Phys. 31 (1886), p. 214.

407) Alg. sup.[30]) 1, p. 156.

408) *Voir à ce sujet *S. Roberts*, Proc. London math. Soc. (1) 2 (1866/9), p. 8/20; *E. Isé*, Giorn. mat. (1) 11 (1873), p. 253; *L. Saltel*, Nouv. Ann. math. (2) 12 (1873), p. 565; C. R. Acad. sc. Paris 81 (1875), p. 884; *G. Fouret*, C. R. Acad. sc. Paris 78 (1874), p. 183; Bull. Soc. math. France 2 (1873/4), p. 127; *V. Janni*, Giorn. mat. (1) 12 (1874), p. 27; *H. Laurent*, Nouv. Ann. math. (3) 5 (1886), p. 432, 456; (3) 12 (1893), p. 305, 355; J. math. spéc. (4) 2 (1893), p. 97, 121; J. Ec. polyt. (1) cah. 60 (1890), p. 107; Scientia, Phys.-math. nº 7, Paris 1900, p. 33; *R. Lachlan*, Proc. Cambr. philos. Soc. 9 (1895/8), p. 313.*

$$(f_1 = 0,\ f_2 = 0,\ \ldots,\ f_m = 0)$$

est précisément égal à $n_1 n_2 \ldots n_m$. C'est là le théorème fondamental que l'on a appelé *théorème de Bézout*. En appliquant la *méthode de Bézout*, *J. Liouville*[409]) a complété le *théorème de Bézout* en donnant un procédé qui permet de calculer $z_1, z_2, \ldots, z_{m-1}$ quand on connaît z_m.

Pour que la dernière conclusion de *E. Bézout* fût légitime et le calcul de *J. Liouville* suffisant, il faudrait montrer que à chaque racine ζ_m de l'équation $R(z_m) = 0$ correspondent des valeurs $z_1 = \zeta_1$, $z_2 = \zeta_2, \ldots, z_{m-1} = \zeta_{m-1}$ telles que $(\zeta_1, \zeta_2, \ldots, \zeta_{m-1}, \zeta_m)$ soit une racine du système d'équations $(f_1 = 0, f_2 = 0, \ldots, f_m = 0)$. *J. A. Serret*[410]) s'est le premier aperçu de la nécessité de cette démonstration complémentaire, mais la démonstration qu'il a donnée suppose que z_m ne peut vérifier une équation algébrique de degré moindre que $n_1 n_2 \ldots n_m$ ce qui n'est pas légitime. *Carl Schmidt*[411]) a critiqué la démonstration de *J. A. Serret* et en a donné une autre qui est entièrement rigoureuse. Le *théorème de Bézout* se trouve ainsi établi lui aussi en toute rigueur. Dans le cas où les coefficients des fonctions $f_1, f_2, \ldots, f_m$ sont indéterminés, la fonction

$$R(z_m) = f_1\varphi_1 + f_2\varphi_2 + \cdots + f_m\varphi_m$$

dont le degré est précisément égal à $n_1 n_2 \ldots n_m$ est déterminée *univoquement* à un facteur numérique près et est une fonction *irréductible* des coefficients indéterminés de $f_1, f_2, \ldots, f_m$ et de z_m. A chaque racine $z_m = \zeta_m$ de l'équation algébrique $R(z_m) = 0$ correspond une racine $(\zeta_1, \zeta_2, \ldots, \zeta_m)$ du système

$$(f_1 = 0,\ f_2 = 0,\ \ldots,\ f_m = 0).$$

Dans le cas où les coefficients des fonctions $f_1, f_2, \ldots, f_m$ ont des valeurs particulières données numériquement ou en fonction de paramètres, on peut utiliser le calcul précédent fait avec des coefficients indéterminés et y remplacer ensuite les coefficients par les valeurs données. Il peut alors arriver que le degré de la fonction $R(z_m)$ s'abaisse d'une ou de plusieurs unités; cette fonction $R(z_m)$ peut même s'annuler identiquement.

Lorsque les coefficients des fonctions $f_1, f_2, \ldots, f_m$ ne sont plus indéterminés *le théorème de Bézout* ne s'applique plus: le nombre des racines du système $(f_1 = 0, f_2 = 0, \ldots, f_m = 0)$ peut être inférieur

409) J. math. pures appl. (1) 12 (1847), p. 68.

410) Alg. sup.[30]) 1, p. 164.

411) Z. Math. Phys. 31 (1886), p. 214.

à $n_1 n_2 \dots n_m$; mais il ne peut être supérieur à ce nombre sans être infini.

Pour $m = 2$, la fonction $R(z_m)$ est identique, à un facteur numérique près, à l'éliminant $E_2(z_2)$.

Quel que soit m la fonction $R(z_m)$ jouit de propriétés analogues à celles de l'éliminant pour $m = 2$; c'est pourquoi nous l'appellerons dans tous les cas *l'éliminant* en z_m du système d'équations

$$(f_1 = 0,\ f_2 = 0,\ \dots,\ f_m = 0).$$

On formerait de même les éliminants en z_1, en $z_2, \dots,$ en z_{m-1} du même système d'équations.

Un théorème important est celui-ci[412]: toute fonction rationnelle entière d'une racine $(\zeta_1, \zeta_2, \dots, \zeta_m)$ du système d'équations $(f_1 = 0,\ f_2 = 0,\ \dots,\ f_m = 0)$ peut être réduite de façon à contenir ζ_1 au plus au degré $n_1 - 1$, ζ_2 au plus au degré $n_2 - 1, \dots, \zeta_m$ au plus au degré $n_m - 1$.

Voici un autre théorème souvent utile[413]: Supposons que, pour des fonctions quelconques $f_1, f_2, \dots, f_m$ des m variables $z_1, z_2, \dots, z_m$ dont les coefficients sont des nombres rationnels ou des fonctions rationnelles (à coefficients rationnels) d'un nombre fini de paramètres $\lambda_1, \lambda_2, \dots,$ on puisse, par un procédé quelconque, déterminer des fonctions rationnelles entières $\psi_1, \psi_2, \dots, \psi_m$ des m variables $z_1, z_2, \dots, z_m$ (dont les coefficients sont des nombres rationnels ou des fonctions rationnelles des paramètres $\lambda_1, \lambda_2, \dots$) telles que l'expression

$$f_1 \psi_1 + f_2 \psi_2 + \cdots + f_m \psi_m$$

soit une fonction $F(z_m)$ ne dépendant que de z_m. Il peut arriver que cette fonction $F(z_m)$ soit *irréductible*[414]) par rapport à z_m. Dans ce cas la fonction $G(z_m)$, formée par la *méthode de Bézout* à l'aide de fonctions $\varphi_1, \varphi_2, \dots, \varphi_m$ de façon que

412) *J. A. Serret* a le premier posé ce théorème et s'est rendu compte de la difficulté qu'il y a à le démontrer par un procédé analogue à celui qui permet de démontrer le même théorème pour $m = 1$ [cf. Alg. sup.[30]) 1, p. 151]. L'essai de démonstration de *H. Laurent* [Traité d'Analyse 1, Paris 1885, p. 307] peut être envisagé comme manqué. On trouvera une démonstration complète et rigoureuse dans *E. Netto,* Alg.[27]) 2, p. 114.

413) Cf. *E. Netto*, Alg.[27]) 2, p. 112.

414) Une fonction rationnelle entière de z_m, dont les coefficients sont des nombres rationnels ou des fonctions rationnelles (à coefficients rationnels) d'un nombre fini de paramètres $\lambda_1, \lambda_2, \dots,$ est dite *irréductible* par rapport à z_m lorsqu'on ne peut la mettre sous la forme d'un produit de fonctions rationnelles entières (égales ou inégales) de z_m dont les coefficients soient des nombres rationnels ou des fonctions rationnelles (à coefficients rationnels) de $\lambda_1, \lambda_2, \dots$

$$G(z_m) = f_1 \varphi_1 + f_2 \varphi_2 + \cdots + f_m \varphi_m$$

soit indépendant de $z_1, z_2, \dots, z_{m-1}$, est, à un facteur près qui ne dépend pas de z_m, une puissance entière positive de $F(z_m)$. On en conclut que si $E_m(z_m)$ est l'éliminant en z_m du système d'équations

$$(f_1 = 0,\ f_2 = 0,\ \dots,\ f_m = 0)$$

et si l'on suppose que les coefficients de $f_1, f_2, \dots, f_m$ sont indéterminés, l'éliminant en z_m du système d'équations

$$(\varphi_1 = 0,\ \varphi_2 = 0,\ \dots,\ \varphi_m = 0)$$

est égal à

$$[E_m(z_m)]^q$$

où l'on a posé pour abréger

$$q = \left(\frac{k}{n_1} - 1\right)\left(\frac{k}{n_2} - 1\right) \cdots \left(\frac{k}{n_m} - 1\right)$$

en désignant par k le produit

$$k = n_1 n_2 \dots n_m.$$

58. Méthode d'élimination de Poisson ou méthode des fonctions symétriques. Dans la méthode d'élimination de *S. D. Poisson*[415]) on s'appuie sur la théorie des fonctions symétriques de plusieurs séries de variables (nº 7); on se trouve ainsi généraliser la méthode d'élimination de *J. L. Lagrange* pour $m = 1$.

Reprenons les m équations

$$f_1(z_1, z_2, \dots, z_m) = 0,\ f_2(z_1, z_2, \dots, z_m) = 0,\ \dots,\ f_m(z_1, z_2, \dots, z_m) = 0,$$

de degrés respectivement égaux à $n_1, n_2, \dots, n_m$. Plaçons-nous d'abord dans le cas où les coefficients des m fonctions envisagées

$$f_\alpha(z_1, z_2, \dots, z_m)$$

sont indéterminés et donnons alors au coefficient de $z_1^{h_1} z_2^{h_2} \dots z_m^{h_m}$ dans f_α le poids

$$n_\alpha - (h_1 + h_2 + \cdots + h_m).$$

Posons pour abréger $k = n_1 n_2 \dots n_m$, et soient pour $h = 1, 2, \dots, k$

$$[z_{1h}, z_{2h}, \dots, z_{mh}]$$

les k solutions du système $(f_1 = 0,\ f_2 = 0,\ \dots,\ f_m = 0)$.

On démontre que toute fonction F symétrique entière de degré p des m séries de variables

$$[z_{i1}, z_{i2}, \dots, z_{ik}] \qquad (i = 1, 2, \dots, m)$$

s'exprime par une fonction rationnelle des coefficients des m fonctions $f_1, f_2, \dots, f_m$. Le numérateur de cette fonction rationnelle est iso-

415) J. Ec. polyt. (1) cah. 11 (an X), p. 199. Cf. nº **52** note 390.

barique de poids p par rapport aux coefficients de $f_1, f_2, \ldots, f_m$; le dénominateur est isobarique de poids nul par rapport à ces coefficients.

Ceci posé, formons avec *S. D. Poisson*[415]) et *J. Liouville*[416]) l'expression

$$z = \lambda_1 z_1 + \lambda_2 z_2 + \cdots + \lambda_m z_m,$$

dans laquelle $\lambda_1, \lambda_2, \ldots, \lambda_m$ désignent des paramètres indéterminés dénués de poids, en sorte que z soit, comme $z_1, z_2, \ldots, z_m$, de poids 1; posons aussi pour $h = 1, 2, \ldots, k$,

$$\zeta_h = \lambda_1 z_{1h} + \lambda_2 z_{2h} + \cdots + \lambda_m z_{mh}.$$

Toute fonction symétrique de $\zeta_1, \zeta_2, \ldots, \zeta_k$ entière homogène de degré l s'exprime au moyen des fonctions symétriques des z_{ih} avec des coefficients fonctions rationnelles entières de degré l par rapport à $\lambda_1, \lambda_2, \ldots, \lambda_m$. Il en résulte que $\zeta_1, \zeta_2, \ldots, \zeta_k$ sont racines d'une équation

$$\varrho_0 z^k - \varrho_1(\lambda_1, \ldots, \lambda_m) z^{k-1} + \cdots + (-1)^k \varrho_k(\lambda_1, \ldots, \lambda_m) = 0;$$

dans cette équation ϱ_0 est indépendant des paramètres $\lambda_1, \lambda_2, \ldots, \lambda_m$; en général ϱ_i est une fonction rationnelle entière homogène de degré i par rapport à $\lambda_1, \lambda_2, \ldots, \lambda_m$.

ϱ_0 est une fonction irréductible des coefficients des termes de degré n_α dans $f_\alpha(z_1, z_2, \ldots, z_m)$ pour $\alpha = 1, 2, \ldots, m$[417]); ϱ_0 est de poids 0 et ϱ_i est isobarique de poids i par rapport aux coefficients des fonctions $f_1, f_2, \ldots, f_m$.

On appelle *éliminant* du système de fonctions $(f_1, f_2, \ldots, f_m)$ et l'on représente par $E(z)$ le premier membre de l'équation de degré k en z que l'on vient de former, en sorte que

$$E(z) = \varrho_0 z^k - \varrho_1 z^{k-1} + \cdots + (-1)^k \varrho_k.$$

L'éliminant $E(z)$ est homogène par rapport aux coefficients de l'une quelconque des m fonctions $f_\alpha(z_1, z_2, \ldots, z_m)$, et il est d'un degré égal à $\frac{k}{n_\alpha}$ par rapport à ces coefficients. L'éliminant $E(z)$ est irréductible[418]). Chaque zéro ζ_α de l'éliminant $E(z)$ est de la forme

$$\zeta_\alpha = \lambda_1 z_{1\alpha} + \lambda_2 z_{2\alpha} + \cdots + \lambda_m z_{m\alpha},$$

$z_{1\alpha}, z_{2\alpha}, \ldots, z_{m\alpha}$ étant les coordonnées d'une même racine du système $(f_1 = 0, f_2 = 0, \ldots, f_m = 0)$.

416) J. math. pures appl. (1) 12 (1847), p. 68. Cf. n° **52** note 391.

417) *E. Netto*, Alg.[23]) 1, p. 169.

418) Cf. *H. Laurent*, Traité d'Algèbre 4, Paris 1894, p. 16 et suiv. et *E. Netto*, Alg.[27]) 2, p. 79; Oberhessische Gesellschaft für Natur- und Heilkunde Giessen 32 (1897/9), p. 37/41.

Si l'on suppose $\lambda_\alpha = 1$, et tous les autres λ nuls, l'éliminant $E(z)$ se réduit à l'éliminant $R_\alpha(z_\alpha)$ en z_α de *E. Bézout.* L'avantage qu'offre la *substitution de Poisson-Liouville* est de pouvoir calculer toutes les coordonnées d'une même racine au moyen de la seule valeur de $z = \lambda_1 z_1 + \cdots + \lambda_m z_m$ relative à cette racine. Soit k le degré de l'éliminant $E(z)$. Pour calculer les coordonnées $z_{1\alpha}, z_{2\alpha}, \ldots, z_{m\alpha}$ correspondant à la même racine

$$\zeta_\alpha = \lambda_1 z_{1\alpha} + \lambda_2 z_{2\alpha} + \cdots + \lambda_m z_{m\alpha},$$

on peut prendre successivement tous les λ nuls excepté celui qui multiplie la coordonnée que l'on veut calculer.

La méthode d'élimination employée par *J. Liouville* a d'ailleurs été déjà donnée par *E. Waring*[419]).

Si, par un procédé quelconque, on a formé l'éliminant $E(z)$, on peut utiliser les relations qui existent entre les coefficients et les racines de l'équation $E(z) = 0$ pour calculer les fonctions symétriques des racines

$$(z_{1\alpha}, z_{2\alpha}, \ldots, z_{m\alpha}) \qquad (\alpha = 1, 2, \ldots, k).$$

Ces relations entre les coefficients et les racines de l'équation $E(z) = 0$ subsistent d'ailleurs quelles que soient les indéterminées $\lambda_1, \lambda_2, \ldots, \lambda_m$ et elles fournissent pour des valeurs particulières de ces indéterminées des expressions de fonctions symétriques des $z_{1\alpha}, z_{2\alpha}, \ldots, z_{m\alpha}$ au moyen des coefficients de $f_1, f_2, \ldots, f_m$. Si les fonctions symétriques calculées sont entières par rapport aux $z_{1\alpha}, z_{2\alpha}, \ldots, z_{m\alpha}$ leurs expressions au moyen des coefficients de $f_1, f_2, \ldots, f_m$ ne renferment au dénominateur que ϱ_0 et ses puissances.

Dans le cas où les coefficients de $f_1, f_2, \ldots, f_m$ sont indéterminés, *L. Kronecker*[420]) a mis les coordonnées z_{ih} des différentes racines du système $(f_1 = 0, f_2 = 0, \ldots, f_m = 0)$ sous la forme que voici:

Formons, pour $i = 1, 2, \ldots, m$, les expressions

$$H_i(z) = E(z) \sum_{\alpha=1}^{\alpha=k} \left(\frac{z_{i\alpha}}{z - \zeta_\alpha}\right) \qquad (i = 1, 2, \ldots, m);$$

chacune de ces m fonctions $H_i(z)$ est une fonction rationnelle entière de z dont les coefficients sont des fonctions symétriques des ζ_α et des $z_{i\alpha}$, et s'exprimeront par suite en fonction des coefficients de $f_1, f_2, \ldots, f_m$. En faisant $z = \zeta_h$ dans $H_i(z)$ on aura, puisque $E'(\zeta_h)$

419) Miscellanea analytica de aequationibus algebraicis et de curvarum proprietatibus, Cambridge 1762, p. 55.

420) J. reine angew. Math. 91 (1881), p. 307; Werke 2, Leipzig 1897, p. 203.

n'est pas nul dans le cas des coefficients indéterminés dans lequel nous nous sommes placés,

$$z_{ih} = \frac{H_i(\zeta_h)}{E'(\zeta_h)}.$$

Ces expressions des coordonnées des différentes racines d'un système d'équations données s'étendent d'ailleurs au cas où les coefficients des fonctions $f_1, f_2, \ldots, f_m$ sont des constantes ou des fonctions rationnelles entières d'un ou de plusieurs paramètres, pourvu toutefois que la dérivée, prise par rapport à z, de l'éliminant $E(z)$ ne s'annule pour aucune des racines z_h de l'équation $E(z) = 0$.

59. Résultant. Plaçons-nous toujours dans le cas où les coefficients de $f_1, f_2, \ldots, f_m$ sont indéterminés, et envisageons maintenant le cas où l'on aurait une $(m+1)^{\text{ième}}$ équation $f_{m+1} = 0$ à coefficients indéterminés entre les m variables $z_1, z_2, \ldots, z_m$. Les coefficients étant indéterminés, les fonctions $f_1, f_2, \ldots, f_m$ sont sans diviseur commun. Formons le produit

$$\prod_{\alpha=1}^{\alpha=k} f_{m+1}(z_{1\alpha}, z_{2\alpha}, \ldots, z_{m\alpha}),$$

où $k = n_1 n_2 \ldots n_m$. Ce produit s'exprime en fonction rationnelle entière des coefficients des $(m+1)$ fonctions $f_1, f_2, \ldots, f_{m+1}$ avec un dénominateur qui est une puissance de ϱ_0. *L. Schläfli*[421]) a démontré que cette puissance a pour exposant le degré n_{m+1} de la fonction f_{m+1}.

On est ainsi amené à définir, avec *S. D. Poisson*, comme *résultant* des $(m+1)$ fonctions $f_1, f_2, \ldots, f_{m+1}$ des m variables $z_1, z_2, \ldots, z_m$ l'expression

$$R = R(f_1, f_2, \ldots, f_{m+1}) = \varrho_0^{n_{m+1}} \prod_{\alpha=1}^{\alpha=k} f_{m+1}(z_{1\alpha}, z_{2\alpha}, \ldots, z_{m\alpha}),$$

où ϱ_0 est le coefficient de la plus haute puissance de z dans l'éliminant $E(z)$ du système de fonctions $(f_1, f_2, \ldots, f_m)$. Si l'on convient d'appeler *résultant* de m fonctions *homogènes* $\varphi_1, \varphi_2, \ldots, \varphi_m$ de m variables $z_1, z_2, \ldots, z_m$, le résultant des m fonctions $t_1, t_2, \ldots, t_m$ de $m-1$ variables que l'on obtient en remplacant dans $\varphi_1, \varphi_2, \ldots, \varphi_m$ l'une des variables, z_m par exemple, par 1, on démontre que ϱ_0 est le résultant des m fonctions homogènes $\varphi_1, \varphi_2, \ldots, \varphi_m$ formées par les termes de $f_1, f_2, \ldots, f_m$ de degré respectivement égaux à $n_1, n_2, \ldots, n_m$.

Le résultant $R(f_1, f_2, \ldots, f_{m+1})$ ainsi défini est une fonction rationnelle entière des coefficients indéterminés des fonctions $f_1, f_2, \ldots, f_{m+1}$.

On entend par *résultant* de $m+1$ fonctions quelconques données $f_1, f_2, \ldots, f_{m+1}$ de m variables $z_1, z_2, \ldots, z_m$, à coefficients *déterminés*,

421) Denkschr. Akad. Wien (math.) 4 II (1852), p. 7.

la fonction que l'on obtient en formant le résultant des $m+1$ fonctions $f_1, f_2, \ldots, f_{m+1}$ comme si les coefficients de ces fonctions étaient indéterminés et en remplaçant dans la fonction rationnelle entière R ainsi obtenue les coefficients indéterminés par les coefficients déterminés des fonctions données $f_1, f_2, \ldots, f_{m+1}$.

Dans le cas où les coefficients de $f_1, f_2, \ldots, f_{m+1}$ sont *indéterminés*, le résultant $R(f_1, f_2, \ldots, f_{m+1})$ est une fonction *irréductible* de ces coefficients; il est homogène par rapport aux coefficients de chacune des fonctions f_α et son degré par rapport à ces coefficients est égal à

$$n_1 n_2 \ldots n_{\alpha-1} n_{\alpha+1} \ldots n_{m+1};$$

de plus le résultant $R(f_1, f_2, \ldots, f_{m+1})$ est isobarique de poids $n_1 n_2 \ldots n_{m+1}$ par rapport aux coefficients de *toutes* les fonctions f_α.

Si la fonction rationnelle entière $f_1(z_1, z_2, \ldots, z_m)$ se décompose en un produit de deux fonctions rationnelles entières

$$f_1(z_1, z_2, \ldots, z_m) = f_{11}(z_1, z_2, \ldots, z_m) f_{12}(z_1, z_2, \ldots, z_m),$$

on a

$$R(f_1, f_2, \ldots, f_{m+1}) = R(f_{11}, f_2, \ldots, f_{m+1})\, R(f_{12}, f_2, \ldots, f_{m+1}).$$

La condition nécessaire et suffisante pour que $m+1$ équations aient une racine commune (finie ou infinie) est que leur résultant soit nul.

De ce théorème fondamental et de ce que le résultant R de m fonctions rationnelles entières $f_1, f_2, \ldots, f_m$ à coefficients indéterminés est irréductible, on déduit aisément que le résultant du système de fonctions

$$f_1, \quad f_2 + q_{21} f_1, \quad f_3 + q_{32} f_2 + q_{31} f_1, \quad \ldots,$$

où $q_{21}, q_{32}, q_{31}, \ldots$ désignent des fonctions rationnelles entières de degrés $n_{21}, n_{32}, n_{31}, \ldots$, coïncide avec le résultant R du système de fonctions $f_1, f_2, \ldots, f_m$ lorsque

$$n_{21} + n_1 \leqq n_2, \; n_{32} + n_2 \leqq n_3, \; n_{31} + n_1 \leqq n_3, \ldots$$

*Dans le cas où le résultant $R(f_1, f_2, \ldots, f_{m+1})$ est égal à zéro, *C. Russĭjan*[422]) détermine les racines communes des équations

$$f_1 = 0, \quad f_2 = 0, \ldots, f_{m+1} = 0$$

à l'aide des dérivées partielles de la fonction R prises par rapport aux coefficients des fonctions $f_1, f_2, \ldots, f_{m+1}$.*

A l'occasion d'une méthode de *O. Biermann*[423]), *J. Hadamard*[424]) s'est occupé des différentes formes du résultant que l'on obtient en

422) *Zapiski novoross. universit. (Mém. Odessa) 57 (1892), p. 313.*

423) Monatsh. Math. Phys. 5 (1894), p. 17.

424) Acta math. 20 (1896/7), p. 201.

appliquant la *méthode de Poisson*, suivant l'ordre dans lequel on range les fonctions données, c'est-à-dire suivant celle des fonctions $f_1, f_2, \ldots, f_{m+1}$ dans laquelle on substitue à $z_1, z_2, \ldots, z_m$ les zéros $(z_{1h}, z_{2h}, \ldots, z_{mh})$ du système formé par les m autres fonctions.

Si $\alpha_1, \alpha_2, \ldots, \alpha_{m+1}$ sont les nombres $1, 2, \ldots, m+1$ rangés dans un certain ordre, on a

$$R(f_{\alpha_1}, f_{\alpha_2}, \ldots, f_{\alpha_{m+1}}) = (-1)^{\omega n_1 n_2 \cdots n_{m+1}} R(f_1, f_2, \ldots, f_{m+1}),$$

ω étant égal au nombre des inversions de la permutation

$$(\alpha_1, \alpha_2, \ldots, \alpha_{m+1}).$$

Si donc on range de deux façons différentes les fonctions données on obtient des résultants égaux en valeur absolue qui sont de même signe ou de signes contraires suivant que dans les façons de ranger ces fonctions le produit $\omega n_1 n_2 \ldots n_{m+1}$ a, ou non, même parité.

Etant données m équations

$$f_1(z_1, z_2, \ldots, z_m) = 0, \quad f_2(z_1, z_2, \ldots, z_m) = 0, \quad \ldots, \quad f_m(z_1, z_2, \ldots, z_m) = 0$$

entre m variables $z_1, z_2, \ldots, z_m$, si l'on forme le résultant des m fonctions $f_1, f_2, \ldots, f_m$ envisagées comme des fonctions de $z_1, z_2, \ldots, z_{m-1}$ seulement, ce résultant sera l'éliminant $E_m(z_m)$ par rapport à z_m, tel qu'il a été défini plus haut, des m fonctions $f_1, f_2, \ldots, f_m$ des m variables $z_1, z_2, \ldots, z_m$.

L'éliminant $E(z)$ des m fonctions $f_1, f_2, \ldots, f_m$ qui a été défini au n° **58** est le résultant des $m+1$ fonctions

$$f_1, f_2, \ldots, f_m, \; \lambda_1 z + \lambda_2 z_2 + \cdots + \lambda_m z_m - z$$

envisagées comme des fonctions de $z_1, z_2, \ldots, z_m$.

60. Expression du résultant due à Perrin. *R. Perrin*[425]) considère p fonctions entières $u, v, w, \ldots$ des $(p-1)$ variables $x, y, z, \ldots$ et leur résultant R. *Il montre qu'on peut mettre ce résultant sous la forme

$$R = R_{100\ldots} u + R_{010\ldots} v + R_{001\ldots} w + \cdots$$
$$- \frac{1}{2!}(R_{200\ldots} u^2 + R_{020\ldots} v^2 + \cdots + 2 R_{110\ldots} uv + \cdots)$$
$$+ \frac{1}{3!}(R_{300\ldots} u^3 + \cdots + 3 R_{210\ldots} u^2 v + \cdots + 6 R_{1110\ldots} uvw + \cdots) - \cdots$$

où l'on a posé pour abréger

$$R_{qrs\ldots} = \frac{\partial^{q+r+s\cdots} R}{\partial a^q \partial b^r \partial c^s \ldots},$$

$a, b, c, \ldots$ désignant les termes tout connus de $u, v, w, \ldots$*

425) C. R. Acad. sc. Paris 106 (1888), p. 1789; 107 (1888), p. 22, 219.

*Prenons par exemple deux fonctions u, v d'une variable x. Le résultant peut alors toujours être mis sous la forme

$$(1) \quad R = (R_{10} u + R_{01} v) - \frac{1}{2!}(R_{20} u^2 + 2 R_{11} uv + R_{02} v^2)$$
$$+ \frac{1}{3!}(R_{30} u^3 + 3 R_{21} u^2 v + 3 R_{12} uv^2 + R_{03} v^3) + \cdots$$

Cette relation se réduisant à une simple identité quand on y remplace u et v par les fonctions de x que ces lettres représentent, on a aussi les relations

$$\frac{\partial R}{\partial x} = 0, \quad \frac{\partial^2 R}{\partial x^2} = 0, \quad \frac{\partial^3 R}{\partial x^3} = 0, \quad \ldots$$

Si dans ces dernières relations on fait $u = v = 0$, on obtient des relations entre les valeurs particulières que prennent les dérivées

$$u' = \frac{\partial u}{\partial x}, \quad v' = \frac{\partial v}{\partial x}, \quad u'' = \frac{\partial^2 u}{\partial x^2}, \quad v'' = \frac{\partial^2 v}{\partial x^2}, \ldots$$

pour une solution $x = \xi$ commune aux deux équations $u = 0$, $v = 0$. Nous nous contenterons de citer les trois premières de ces relations dans le cas où les deux fonctions de la variable x ont un ou plusieurs facteurs communs. Ce sont les relations

$$(2) \quad \begin{cases} R_{10} u' + R_{01} v' = 0 \\ R_{10} u'' + R_{01} v'' = R_{20} u'^2 + 2 R_{11} u' v' + R_{02} v'^2 \\ R_{10} u''' + R_{01} v''' = 3[R_{20} u'' u' + R_{11}(u'' v' + v'' u') + R_{02} v'' v'] \\ \qquad - [R_{30} u'^3 + 3 R_{21} u'^2 v' + 3 R_{12} u' v'^2 + R_{03} v'^3]. \end{cases}$$

En combinant convenablement des relations du type (1) et du type (2) on parvient à préciser les conditions d'existence des divers genres de solutions multiples d'un système donné d'équations $u(x) = 0$, $v(x) = 0$.* Pour fixer les idées cherchons les conditions pour que u et v soient de la forme

$$u = \alpha^2 \beta^2 u_1, \quad v = \alpha^2 \beta v_1,$$

où α, β désignent deux fonctions linéaires de x et u_1, v_1 deux fonctions rationnelles entières de x premières entre elles et premières avec α, β. Il faut pour cela non seulement que le résultant $R(u, v)$ ainsi que les coefficients

$$R_{10}, \quad R_{01}, \quad R_{20}, \quad R_{02}, \quad R_{03}$$

soient nuls comme il résulte du *théorème de Lagrange* sur les racines communes à plusieurs équations (n° **34**; voir en partic. note 210), mais encore que l'on ait les identités

$$R_{11} = 0, \quad 3 R_{21}^2 - 4 R_{30} R_{12} = 0$$

en sorte que le second membre de la relation (1) commence par un groupe de termes du 3ième degré en u et v et que ce groupe de termes se décompose en un produit de deux facteurs l'un du premier et l'autre du second degré.

Réciproquement, si l'on a deux fonctions données u et v, les conditions énoncées sont suffisantes pour que u et v soient de la forme envisagée.

*Dans le cas de trois fonctions u, v, w de deux variables x, y, le résultant peut toujours être mis sous la forme

$$R = (R_{100}u + R_{010}v + R_{001}w) \tag{3}$$
$$-\frac{1}{2!}(R_{200}u^2 + 2R_{110}uv + R_{020}v^2 + 2R_{101}uw + R_{002}w^2 + 2R_{011}vw) + \cdots$$

Supposons que l'ensemble des termes de degrés $1, 2, \ldots, q-1$ soit identiquement nul en u, v, w et que l'ensemble des termes de degré q ne le soit pas. On démontre que les courbes

$$u = 0, \quad v = 0, \quad w = 0$$

ont alors q points communs et que l'ensemble des termes de degré q du second membre de (3) se décompose en q facteurs linéaires; chacun de ces facteurs correspond à l'un des q points communs aux trois courbes $u = 0$, $v = 0$, $w = 0$; les divers cas possibles d'égalité de ces q facteurs linéaires correspondent d'ailleurs aux divers cas possibles de coïncidence des q points entre eux.*

61. Essai d'extension de la méthode d'Euler au cas de plusieurs variables. *A. Cayley*[426]) a cherché à étendre le *procédé d'Euler* qui a donné naissance à la *méthode de Bézout* (nº **36**) pour former le résultant dans le cas d'une variable, à un système d'équations à plusieurs variables.

Multiplions à cet effet les $(m+1)$ fonctions données

$$f_1(z_1, z_2, \ldots, z_m),\ f_2(z_1, z_2, \ldots, z_m),\ \ldots,\ f_{m+1}(z_1, z_2, \ldots, z_m)$$

par des produits de puissances des inconnues, c'est-à-dire par des termes tels que $z_1^{\alpha_1} z_2^{\alpha_2} \ldots z_m^{\alpha_m}$, où $\alpha_1, \alpha_2, \ldots, \alpha_m$ désignent des nombres naturels ou nuls, jusqu'à ce qu'on ait obtenu un nombre d'équations égal au nombre de ces produits de puissances des inconnues. On regarde alors les équations obtenues comme linéaires par rapport à ces produits de puissances, et en écrivant qu'elles sont compatibles on obtient un multiple du résultant. Il faut toutefois

426) Cambr. Dublin math. J. 2 (1847), p. 52; 3 (1848), p. 116; Papers 1, Cambr. 1889, p. 259, 370.

encore débarrasser le résultat des facteurs étrangers. *A. Cayley*[427]) a montré comment on peut y arriver[428]).

J. J. Sylvester[429]) emploie un autre procédé qui convient au cas de trois équations

$$f_1(z_1, z_2) = 0, \quad f_2(z_1, z_2) = 0, \quad f_3(z_1, z_2) = 0$$

de même degré, ou au cas de quatre équations

$$f_1(z_1, z_2, z_3) = 0, \qquad f_2(z_1, z_2, z_3) = 0,$$
$$f_3(z_1, z_2, z_3) = 0, \qquad f_4(z_1, z_2, z_3) = 0$$

toutes quatre du second degré; ce procédé donne le résultant débarrassé de tout facteur étranger.

62. Théorème de Liouville. Voici un théorème de *J. Liouville*[430]) très important par ses nombreuses applications géométriques et que *G. Fouret*[431]) énonce ainsi: Dans l'équation

$$E(z_{m+1}) = 0$$

de degré $k = n_1 n_2 \ldots n_{m+1}$, résultant de l'élimination de m variables entre $m+1$ équations algébriques à $m+1$ variables dont les degrés sont respectivement $n_1, n_2, \ldots, n_{m+1}$, le coefficient du terme de degré $k-i$ dépend exclusivement des coefficients des termes des $m+1$ équations données qui sont d'un degré égal ou supérieur à $n_1 - i$

427) Voir *E. Netto* [Alg.[27]) 2, p. 146 et suiv.]; *G. Salmon* [Alg.[165]), p. 88/9; trad. *O. Chemin*, p. 126], avait déjà exposé la méthode de *A. Cayley*, mais l'exposé n'est pas à l'abri de toute critique; cf. *E. Netto*, Alg.[27]) 2, p. 152; voir aussi *K. Bes*, Verhand. Akad. Wetensch. Amsterdam, Afdeeling Natuurkunde erste Sectie (2) 6 (1897/9), mém. nº 7, p. 1; (2) 8 (1901/4), mém. nº 1; K. Akad. Wetensch. Amsterdam, Verslagen natuurk. Afdeeling 8 (1898/9), p. 173; *F. S. Macaulay*, Proc. London math. Soc. (1) 35 (1902/3), p. 3/27.

428) Parmi les anciens mémoires conçus dans cet ordre d'idées, on peut citer: *L. Euler*, Hist. Acad. Berlin 4 (1748), éd. 1750, p. 219; *G. Cramer*, Introd.[31]), p. 660 (appendice); *J. Plücker*, Ann. math. pures appl. 19 (1828/9), p. 97, 129; J. reine angew. Math. 16 (1837), p. 47 [1836]; Wiss. Abh. 1, Leipzig 1895, p. 76, 323; *C. G. J. Jacobi*, J. reine angew. Math. 15 (1836), p. 101; Werke[31]) 3, p. 297; *L. O. Hesse*, J. reine angew. Math. 20 (1840), p. 285; 26 (1843), p. 147; Werke[230]), p. 23, 73; cf. *A. Cayley*[426]).

429) Cambr. Dublin math. J. 7 (1852), p. 68; Papers 1, Cambridge 1905, p. 298. Ce procédé est exposé dans *E. Netto*, Alg.[27]) 2, p. 152. Voir, à ce propos, *J. J. Sylvester*, Cambr. math. J. 2 (1839/41), p. 232; Papers 1, Cambridge 1905, p. 61; *T. Muir*, Proc. R. Soc. Edinb. 20 (1892/5), p. 300, 371; Trans. R. Soc. Edinb. 39 (1900), p. 667 [1899]; 40 (1903), p. 23/38 [1899]; et *A. Cayley*, Proc. R. Soc. Edinb. 20 (1892/5), p. 306/8; Papers 13, Cambr. 1897, p. 545/7, pour un problème particulier.

430) J. math. pures appl. (1) 6 (1841), p. 359.

431) Nouv. Ann. math. (3) 9 (1890), p. 258.

pour la première équation, à $n_2 - i$ pour la deuxième équation, ..., à $n_{m+1} - i$ pour la dernière équation.

Les conséquences géométriques de ce *théorème de Liouville* sont développées par *E. Laguerre*[432]), *E. B. Holst*[433]), *G. Humbert*[434]) et *J. Hadamard*[435]).

63. Cas des équations homogènes. Dans le cas où l'on a m équations *homogènes*

$$\varphi_1(z_1, z_2, \ldots, z_m) = 0, \quad \ldots, \quad \varphi_m(z_1, z_2, \ldots, z_m) = 0,$$

la condition nécessaire et suffisante pour que le système d'équations ($\varphi_1 = 0,\ \varphi_2 = 0,\ \ldots,\ \varphi_m = 0$) admette une racine commune autre que $z_1 = 0,\ z_2 = 0,\ \ldots,\ z_m = 0$ est que le résultant (n° **59**) des fonctions homogènes $\varphi_1, \varphi_2, \ldots, \varphi_m$ soit nul.

Dans un long mémoire, *L. Schläfli*[436]) passe en revue les propriétés du résultant. Il démontre, par exemple, ceci: soit un système de $(n+1)$ équations homogènes, $\varphi = 0,\ \varphi_1 = 0, \ldots, \varphi_n = 0$, entre les $(n+1)$ variables $x, y, z, \ldots$ respectivement de degrés $m, m_1, \ldots, m_n$, soit a le coefficient de x^m dans φ; posons

$$m_1 m_2 \ldots m_n = \mu$$

a^μ est la plus haute puissance de a qui se trouve dans le résultant et l'ensemble des termes du résultant divisibles par a^μ est $a^\mu A$, où A représente la $m^{\text{ième}}$ puissance du résultant des fonctions homogènes $\varphi_1, \varphi_2, \ldots, \varphi_n$ quand on y fait $x = 0$.

F. Mertens[437]) a étudié la structure du résultant des formes homogènes. Soient

$$\varphi_1(z_1, z_2, \ldots, z_m), \quad \ldots, \quad \varphi_m(z_1, z_2, \ldots, z_m)$$

des formes homogènes de m variables $z_1, z_2, \ldots, z_m$, respectivement de degrés $n_1, n_2, \ldots, n_m$. Désignons pour abréger par $\nu_1, \nu_2, \ldots, \nu_m$ les nombres définis par les égalités $n_1 n_2 \ldots n_m = n_1\nu_1 = n_2\nu_2 = \cdots = n_m\nu_m$. Si a_{ih} est le coefficient de $z_h^{n_i}$ dans φ_i, le résultant $R(\varphi_1, \varphi_2, \ldots, \varphi_m)$ contient le terme $a_{11}^{\nu_1} a_{22}^{\nu_2} \ldots a_{mm}^{\nu_m}$ avec le coefficient 1.

Si les formes $\varphi_1, \varphi_2, \ldots, \varphi_m$ sont des puissances entières de formes $\psi_1, \psi_2, \ldots, \psi_m$ de telle sorte que

$$\varphi_i = \psi_i^{\nu_i} \qquad (i = 1, 2, \ldots, m)$$

432) C. R. Acad. sc. Paris 60 (1865), p. 70.

433) Math. Ann. 11 (1877), p. 341; Bull. soc. math. France 8 (1879/80), p. 52.

434) J. math. pures appl. (4) 3 (1887), p. 327; (4) 5 (1889), p. 81; (4) 6 (1890), p. 233; (5) 1 (1895), p. 131; voir aussi Nouv. Ann. math. (3) 6 (1887), p. 526.

435) Acta math. 20 (1896/7), p. 201.

436) Denkschr. Akad. Wien, (math.) 4, II (1852), p. 1/74.

437) Sitzgsb. Akad. Wien 93 II (1886), p. 527; 108 IIa (1899), p. 1173, 1344.

on a

$$R(\varphi_1, \varphi_2, \ldots, \varphi_m) = [R(\psi_1, \psi_2, \ldots, \psi_m)]^{\nu_1 \nu_2 \cdots \nu_m}.$$

Si $\varphi_1, \varphi_2, \ldots, \varphi_m$ s'expriment d'une façon linéaire et homogène au moyen de $(m-1)$ formes $g_1, g_2, \ldots, g_{m-1}$ des mêmes variables $z_1, z_2, \ldots, z_m$ en sorte que l'on ait

$$\varphi_\alpha = p_{\alpha,1} g_1 + \cdots + p_{\alpha,m-1} g_{m-1},$$

où les $p_{\alpha\beta}$ sont des fonctions homogènes de $z_1, z_2, \ldots, z_m$, le résultant $R(\varphi_1, \varphi_2, \ldots, \varphi_m)$ s'évanouit identiquement.

Si chacune des fonctions $\varphi_1, \varphi_2, \ldots, \varphi_m$ s'exprime d'une manière linéaire et homogène au moyen de m fonctions $g_1, \ldots, g_m$ des mêmes variables $z_1, z_2, \ldots, z_m$, en sorte que l'on ait

$$\varphi_\alpha = p_{\alpha,1} g_1 + \cdots + p_{\alpha,m} g_m \qquad (\alpha = 1, 2, \ldots, m),$$

le résultant des formes φ_α est divisible par le résultant des formes g.

Si dans $\varphi_1, \ldots, \varphi_m$ on remplace $z_1, z_2, \ldots, z_m$ par des formes homogènes de même degré n de nouvelles variables $x_1, \ldots, x_m$, et si l'on désigne par

Δ le résultant des z par rapport aux x,

R le résultant des φ par rapport aux z,

S le résultant des φ par rapport aux x,

on a

$$S = R^{n^{m-1}} \Delta^k.$$

64. Discriminant d'une fonction de plusieurs variables. Soit $\varphi(z_1, z_2, \ldots, z_m)$ une fonction rationnelle entière homogène des variables $z_1, z_2, \ldots, z_m$. Le résultant des dérivées partielles $\frac{\partial\varphi}{\partial z_1}, \frac{\partial\varphi}{\partial z_2}, \ldots, \frac{\partial\varphi}{\partial z_m}$ s'appelle le *discriminant de* φ.

C'est là (à un facteur numérique près qui ne dépend que du degré de φ) une généralisation de la notion de discriminant donnée au n° **44**. Si le discriminant de φ s'annule, les équations

$$\frac{\partial\varphi}{\partial z_1} = 0, \ \frac{\partial\varphi}{\partial z_2} = 0, \ \ldots, \ \frac{\partial\varphi}{\partial z_m} = 0$$

admettent au moins une racine commune $(\zeta_1, \ldots, \zeta_m)$ autre que la racine dont toutes les coordonnées sont nulles; cette racine annule aussi la fonction φ.

Envisageons $z_1, z_2, \ldots, z_m$ comme les coordonnées homogènes du point ayant pour coordonnées ordinaires $\frac{z_1}{z_m}, \frac{z_2}{z_m}, \ldots, \frac{z_{m-1}}{z_m}$. Le point qui a pour coordonnées homogènes $\zeta_1, \zeta_2, \ldots, \zeta_m$ est alors un point *singulier* de la variété définie par l'équation $\varphi(z_1, z_2, \ldots, z_m) = 0$; en ce point il n'y a pas de *plan tangent* à la variété $\varphi(z_1, z_2, \ldots, z_m) = 0$.

Si φ est de degré n, le discriminant de φ est homogène de degré $m(n-1)^{m-1}$ par rapport aux coefficients de φ; si l'on donne à chacun des coefficients de la fonction φ un poids égal à la puissance de la variable z_m par laquelle il est multiplié, le poids du discriminant de φ est égal à $n(n-1)^{m-1}$.

Si, par une substitution linéaire et homogène

$$z_i = \gamma_{i1} x_1 + \gamma_{i2} x_2 + \cdots + \gamma_{im} x_m$$
$$(i = 1, 2, \ldots, m)$$

à déterminant

$$\Delta = \begin{vmatrix} \gamma_{11}, & \gamma_{12}, & \ldots, & \gamma_{1m} \\ \gamma_{21}, & \gamma_{22}, & \ldots, & \gamma_{2m} \\ \cdot & \cdot & \cdot & \cdot \\ \gamma_{m1}, & \gamma_{m2}, & \ldots, & \gamma_{mm} \end{vmatrix}$$

différent de zéro, la fonction envisagée $\varphi(z_1, z_2, \ldots, z_m)$ se transforme en une fonction $\Phi(x_1, x_2, \ldots, x_m)$, le discriminant de cette fonction $\Phi(x_1, x_2, \ldots, x_m)$ est égal au produit de $\Delta^{n(n-1)^{m-1}}$ par le discriminant de $\varphi(z_1, z_2, \ldots, z_m)$.

On appelle *discriminant* de la fonction rationnelle entière non homogène $f(z_1, z_2, \ldots, z_{m-1})$ de degré n le discriminant de la fonction rationnelle entière homogène

$$\varphi(z_1, z_2, \ldots, z_m) = z_m^n f\left(\frac{z_1}{z_m}, \frac{z_2}{z_m}, \ldots, \frac{z_{m-1}}{z_m}\right).$$

Si un système d'équations $(f_1 = 0, f_2 = 0, \ldots, f_m = 0)$ admet une infinité de racines, le discriminant d'une fonction quelconque φ homogène et non-linéaire de $f_1, f_2, \ldots, f_m$ est identiquement nul.

Si $f_1, f_2, \ldots$ désignent des fonctions rationnelles entières homogènes de $x, y, z, \ldots$ en nombre moindre que celui des variables et si une fonction homogène $\varphi(x, y, z, \ldots)$ peut être mise sous la forme $F(f_1, f_2, \ldots)$ homogène ou non, mais ne contenant pas de terme du premier degré, le discriminant de φ est identiquement nul.

65. Racines infinies. Si $\varphi_\alpha(z_1, z_2, \ldots, z_m)$ désigne pour chacun des indices $\alpha = 1, 2, \ldots, m$ l'ensemble des termes de degré n_α de la fonction $f_\alpha(z_1, z_2, \ldots, z_m)$, le résultant $R(\varphi_1, \varphi_2, \ldots, \varphi_m)$ des m fonctions homogènes $\varphi_1, \varphi_2, \ldots, \varphi_m$ des m variables $z_1, z_2, \ldots, z_m$ est le coefficient ϱ_0 de la plus haute puissance de z dans l'éliminant $E(z)$. Il en résulte que la condition nécessaire et suffisante pour que les m équations homogènes $\varphi_1 = 0, \varphi_2 = 0, \ldots, \varphi_m = 0$ aient au moins une solution commune (autre que $z_1 = 0, z_2 = 0, \ldots, z_m = 0$) est que ϱ_0 soit égal à zéro; si le système d'équations

$$(\varphi_1 = 0, \varphi_2 = 0, \ldots, \varphi_m = 0)$$

admet d'autres racines que la racine $(0, 0, \ldots, 0)$ le nombre de racines finies du système d'équations

$$(f_1 = 0, f_2 = 0, \ldots, f_m = 0)$$

est donc nécessairement inférieur à $n_1 n_2 \ldots n_m$.

Si l'éliminant $E(z)$ d'un système de fonctions $(f_1, f_2, \ldots, f_m)$ se présente sous la forme

$$E(z) = (-1)^i \varrho_i z^{k-i} + (-1)^{i+1} \varrho_{i+1} z^{k-i-1} + \cdots + (-1)^k \varrho_k,$$

en sorte que dans l'expression générale de l'éliminant les coefficients $\varrho_0, \varrho_1, \ldots, \varrho_{i-1}$ soient nuls, le système d'équations

$$(f_1 = 0, f_2 = 0, \ldots, f_m = 0)$$

n'admet plus que $k - i$ racines; on dit alors que ce système d'équations $(f_1 = 0, f_2 = 0, \ldots, f_m = 0)$ admet *i racines infinies.* L'éliminant $E(z)$ a alors i facteurs linéaires de la forme

$$\alpha_1 \lambda_1 + \alpha_2 \lambda_2 + \cdots + \alpha_m \lambda_m$$

et à chacun de ces i facteurs linéaires correspond une racine infinie du système d'équations

$$f_1 = 0, f_2 = 0, \ldots, f_m = 0;$$

au facteur $\alpha_1 \lambda_1 + \alpha_2 \lambda_2 + \cdots + \alpha_m \lambda_m$ correspond la racine[438])

$$z_1 = \alpha_1 t, \; z_2 = \alpha_2 t, \ldots, z_m = \alpha_m t \qquad (\text{où } t = \infty).$$

Il peut arriver qu'une ou plusieurs des racines aient certaines de leurs coordonnées infinies, les autres étant indéterminées; les premières correspondent à des valeurs de α différentes de zéro, les autres à des valeurs de α égales à zéro.

Déjà *L. Euler*[439]) compte les racines infinies dans le nombre total des racines. *C. Arzelà*[440]) s'est occupé de la réduction possible du degré de l'éliminant et calcule ce degré par la *règle de Minding.*[441])

Si, pour un système particulier d'équations, les coefficients $\varrho_0, \varrho_1, \ldots, \varrho_{\mu-1}$ de l'éliminant $E(z)$ sont identiquement nuls, le coefficient ϱ_μ envisagé comme une fonction de $\lambda_1, \lambda_2, \ldots, \lambda_m$ divise exactement les coefficients suivants $\varrho_{\mu+1}, \varrho_{\mu+2}, \ldots$ en sorte qu'on peut supprimer les facteurs de ϱ_μ dans l'expression de l'éliminant $E(z)$[442]) quand on ne cherche que les solutions finies du système d'équations envisagées.

---

438) *Gy. (J.) König,* Alg. Grössen[20]), p. 304.

439) Hist. Acad. Berlin 4 (1748), éd. 1750, p. 234.

440) Giorn. mat. (1) 15 (1877), p. 62, 154.

441) Pour le cas de deux variables, voir *J. Zaluski,* Prace matematyczne-fizyczne (Varsovie) 8 (1897), p. 129/138.

442) *E. Netto,* Alg.[27]) 2, p. 86.

L'éliminant $E(z)$ du système de fonctions rationnelles entières

$$f_1,\ f_2,\ f_3,\ \ldots,\ f_m$$

ne s'annule identiquement que quand le système d'équations

$$f_1 = 0,\ f_2 = 0,\ \ldots,\ f_m = 0$$

a un nombre infini de racines finies ou infinies[443]). Quand on se trouve dans ce cas on dit que le système d'équations est *indéterminé*.

66. Racines multiples. Si l'éliminant $E(z)$ d'un système de fonctions $(f_1, f_2, \ldots, f_m)$ admet un zéro multiple $z = \xi_1$, d'ordre α, la racine $(z_{11}, z_{21}, \ldots, z_{m1})$ correspondante sera dite *racine multiple d'ordre* de multiplicité α du système d'équations $(f_1 = 0, f_2 = 0, \ldots, f_m = 0)$.

Le théorème de *Bézout* d'après lequel quand ϱ_0 n'est pas nul le système $(f_1 = 0, f_2 = 0, \ldots, f_m = 0)$ admet précisément $k = n_1 n_2 \ldots n_m$ racines n'est vrai, dans chaque cas particulier qui se présente, qu'à condition de compter chaque racine finie ou infinie avec son ordre de multiplicité.

La condition nécessaire et suffisante pour que $(z_{11}, z_{12}, \ldots, z_{1m})$ soit une racine finie multiple d'ordre 2, au moins, d'un système d'équations

$$f_1(z_1, z_2, \ldots, z_m) = 0,\ f_2(z_1, z_2, \ldots, z_m),\ \ldots,\ f_m(z_1, z_2, \ldots, z_m) = 0$$

est que l'on ait

$$f_1(z_{11}, z_{12}, \ldots, z_{1m}) = 0,\ f_2(z_{11}, z_{12}, \ldots, z_{1m}),\ \ldots,\ f_m(z_{11}, z_{12}, \ldots, z_{1m}) = 0$$

et que le *déterminant fonctionnel de Jacobi* (cf. nº **73**)

$$J(z_1, z_2, \ldots, z_m) = \begin{vmatrix} \frac{\partial f_1}{\partial z_1} & \frac{\partial f_1}{\partial z_2} & \cdots & \frac{\partial f_1}{\partial z_m} \\ \cdot & \cdot & \cdot & \cdot \\ \frac{\partial f_m}{\partial z_1} & \frac{\partial f_m}{\partial z_2} & \cdots & \frac{\partial f_m}{\partial z_m} \end{vmatrix}$$

s'annule[444]) quand on y remplace $z_1, z_2, \ldots, z_m$ respectivement par $z_{11}, z_{12}, \ldots, z_{1m}$.

Il semble très difficile d'énoncer des conditions nécessaires et suffisantes pour que $(z_{11}, z_{12}, \ldots, z_{1m})$ soit une racine multiple d'ordre 3, au moins, d'un système d'équations

$$f_1(z_1, z_2, \ldots, z_m) = 0,\ \ldots,\ f_m(z_1, z_2, \ldots, z_m) = 0.$$

Si $(z_{11}, z_{12}, \ldots, z_{1m})$ est une racine d'ordre q_1 de l'équation $f_1(z_1, z_2, \ldots, z_m) = 0$, d'ordre q_2 de l'équation $f_2(z_1, z_2, \ldots, z_m) = 0$,

443) *Gy. (J.) König*, Alg. Grössen[20]), p. 304.

444) *E. Netto*, Alg.[27]) 2, p. 90.

$\ldots$, d'ordre q_m de l'équation $f_m(z_1, z_2, \ldots, z_m) = 0$, ce sera une racine dont l'ordre sera au moins $q_1 q_2 \ldots q_m$ pour le système total

$$(f_1 = 0,\ f_2 = 0,\ \ldots,\ f_m = 0).$$

Si en particulier, pour $i = 1, 2, \ldots, m$, la fonction rationnelle entière f_i se réduit à l'ensemble de ceux de ses termes qui sont de degré plus élevé que q_i, la racine

$$z_1 = 0,\ z_2 = 0,\ \ldots,\ z_m = 0$$

du système $(f_1 = 0, f_2 = 0, \ldots, f_m = 0)$ sera donc une racine multiple d'ordre $q_1 q_2 \ldots q_m$ au moins; cet ordre est effectivement égal à $q_1 q_2 \ldots q_m$ quand, pour $i = 1, 2, \ldots, m$, les coefficients des termes de degré plus élevé que q_i dans f_i sont indéterminés. *E. Netto*[445]) le prouve en introduisant la notion de *limite inférieure du poids* d'une somme: si l'on donne un poids arbitraire à chaque terme d'une somme, la limite inférieure du poids de la somme sera définie par le poids de celui ou de ceux des termes de la somme qui ont le moindre poids[446]).

La notion d'*ordre* peut être étendue aux racines infinies d'un système d'équations algébriques. On dit que la racine

$$z_1 = \alpha_1 t,\ z_2 = \alpha_2 t,\ \ldots,\ z_m = \alpha_m t \qquad (\text{où } t = \infty)$$

est d'ordre q lorsque le facteur correspondant

$$\alpha_1 \lambda_1 + \alpha_2 \lambda_2 + \cdots + \alpha_m \lambda_m$$

de l'éliminant $E(z)$ y figure exactement à la $q^{\text{ième}}$ puissance.

Pour distinguer les cas où le système d'équations

$$f_1 = 0,\ f_2 = 0,\ \ldots,\ f_m = 0$$

a des racines multiples de ceux où il n'en a pas, il est commode d'introduire la notion de *discriminant d'un système de fonctions* $(f_1, f_2, \ldots, f_m)$.

Plaçons-nous d'abord dans le cas où les coefficients de $f_1, f_2, \ldots, f_m$ sont des indéterminées et envisageons alors l'expression

$$\varrho_0^{n_1 + n_2 + \cdots + n_m - m - 1} \prod_{\lambda=1}^{\lambda=k} J(\xi_{1\lambda}, \xi_{2\lambda}, \ldots, \xi_{m\lambda})$$

où ϱ_0 continue à désigner le coefficient de z^k dans l'éliminant $E(z)$

445) Alg.[27]) 2, p. 90; Oberhess. Ges.[418]) 32 (1897/9), p. 78/83.

446) Voir aussi *P. Gordan*, Invar.[106]) 1, p. 148; *J. J. Sylvester*[164]); *G. Salmon*, Alg.[165]); trad. *O. Chemin*, p. 145; *E. Amigues*, Nouv. Ann. math. (3) 14 (1895), p. 447; *L. Berzolari*, Ann. mat. pura appl. (2) 24 (1896), p. 165; *W. Mantel*, Nieuw Archief voor Wiskunde (1) 16 (1889), p. 203/8; *E. F. A. Minding*, J. math. pures appl. (1) 6 (1841), p. 412; *E. Combescure*, C. R. Acad. sc. Paris 62 (1866), p. 383.

du système $f_1, f_2, \dots, f_m$ et où le produit est étendu aux $k = n_1 n_2 \cdots n_m$ racines $(\zeta_{1\lambda}, \zeta_{2\lambda}, \dots, \zeta_{m\lambda})$ du système d'équations $(f_1 = 0, f_2 = 0, \dots, f_m = 0)$. Cette expression peut être mise sous la forme d'une fonction rationnelle entière D des coefficients des fonctions $f_1, f_2, \dots, f_m$; cette fonction D est irréductible; c'est elle qu'on appelle le *discriminant*[447]) du système $(f_1, f_2, \dots, f_m)$.

On entend par *discriminant* de m fonctions rationnelles entières quelconques données

$$f_1(z_1, z_2, \dots, z_m),\ f_2(z_1, z_2, \dots, z_m), \dots, f_m(z_1, z_2, \dots, z_m)$$

à coefficients *déterminés*, le nombre (ou la fonction des paramètres) que l'on obtient en formant le discriminant du système $(f_1, f_2, \dots, f_m)$ comme si les coefficients des fonctions étaient indéterminés et en remplaçant dans la fonction rationnelle entière ainsi obtenue les indéterminées par les coefficients déterminés des fonctions données $f_1, f_2, \dots, f_m$.

Le discriminant D d'un système quelconque de fonctions données $f_1, f_2, \dots, f_m$ s'annulera et ne s'annulera que si le système d'équations

$$f_1(z_1, z_2, \dots, z_m) = 0,\ \dots,\ f_m(z_1, z_2, \dots, z_m) = 0$$

a au moins une racine multiple (finie ou infinie) ou si $E(z)$ s'annule identiquement en z[448]).*

Dans le cas où les coefficients des fonctions rationnelles entières $f_1, f_2, \dots, f_m$ sont indéterminés, si l'on pose

$$\Delta = \begin{vmatrix} 1 & \zeta_{11} & \zeta_{12} & \zeta_{11}\zeta_{12} & \dots & \zeta_{11}^{n_1-1} & \dots & \zeta_{12}^{n_2-1} & \dots \\ 1 & \zeta_{21} & \zeta_{22} & \zeta_{21}\zeta_{22} & \dots & \zeta_{21}^{n_1-1} & \dots & \zeta_{22}^{n_2-1} & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \end{vmatrix},$$

où dans les $k = n_1 n_2 \dots n_m$ colonnes de ce déterminant figurent toutes les combinaisons $\zeta_{i1}^{\mu} \zeta_{i2}^{\nu} \dots \zeta_{im}^{\varrho}$ pour lesquelles $\mu \leqq n_1 - 1$, $\nu \leqq n_2 - 1$, $\dots$, $\varrho < n_m - 1$, on aura

$$\Delta^2 = G \prod_{\lambda=1}^{\lambda=k} J(\zeta_{1\lambda}, \zeta_{2\lambda}, \dots, \zeta_{m\lambda}),$$

G étant une fonction rationnelle des coefficients des termes du plus haut degré des fonctions

$$f_1, f_2, \dots, f_m$$ [449]).

*On appelle *discriminant* d'un système de m fonctions rationnelles entières homogènes $F_1, F_2, \dots, F_m$ de $m+1$ variables $z_1, z_2, \dots, z_{m+1}$ le discriminant du système de m fonctions $f_1, f_2, \dots, f_m$ de m variables

447) *Gy. (J.) König,* Alg. Grössen [20]), p. 323, 329.*

448) *Id. p. 338 (Texte et notes 447/8 de *Gy. (J.) König* et *J. Kürschák*).*

449) Cf. *H. Laurent,* Traité d'Analyse [412]) 1, p. 305.

que l'on obtient en faisant $z_{m+1} = 1$ dans $F_1, F_2, \dots, F_m$. Si l'on envisage une $(m+1)^{\text{ième}}$ fonction rationnelle entière homogène

$$F_{m+1}(z_1, z_2, \dots, z_{m+1})$$

et le déterminant fonctionnel

$$J = \begin{vmatrix} \dfrac{\partial F_1}{\partial z_1}, & \dfrac{\partial F_1}{\partial z_2}, & \dots, & \dfrac{\partial F_1}{\partial z_m}, & \dfrac{\partial F_1}{\partial z_{m+1}} \\ \dfrac{\partial F_2}{\partial z_1}, & \dfrac{\partial F_2}{\partial z_2}, & \dots, & \dfrac{\partial F_2}{\partial z_m}, & \dfrac{\partial F_2}{\partial z_{m+1}} \\ \dots & \dots & \dots & \dots & \dots \\ \dfrac{\partial F_m}{\partial z_1}, & \dfrac{\partial F_m}{\partial z_2}, & \dots, & \dfrac{\partial F_m}{\partial z_m}, & \dfrac{\partial F_m}{\partial z_{m+1}} \\ \dfrac{\partial F_{m+1}}{\partial z_1}, & \dfrac{\partial F_{m+1}}{\partial z_2}, & \dots, & \dfrac{\partial F_{m+1}}{\partial z_m}, & \dfrac{\partial F_{m+1}}{\partial z_{m+1}} \end{vmatrix},$$

le discriminant $D(F_1, F_2, \dots, F_m)$ et les résultants $R(F_1, F_2, \dots, F_{m+1})$, $R(F_1, F_2, \dots, F_m, J)$ sont liés par la relation[450])

$$R(F_1, F_2, \dots, F_m, J) = n_{m+1}^k R(F_1, F_2, \dots, F_{m+1})\, D(F_1, F_2, \dots, F_m)$$

où $n_1, n_2, \dots, n_{m+1}$ désignent les degrés de $F_1, F_2, \dots, F_{m+1}$ et k le produit $n_1 n_2 \dots n_m$.

Lorsque les coefficients des fonctions rationnelles entières homogènes $F_1, F_2, \dots, F_{m+1}$ sont indéterminés on peut donc obtenir le discriminant de $F_1, F_2, \dots, F_m$, à un facteur numérique près, en décomposant le résultant $R(F_1, F_2, \dots, F_m, J)$ en deux facteurs dont l'un dépende de coefficients de F_{m+1} tandis que l'autre en est indépendant; c'est ce dernier facteur qui est alors le discriminant de $F_1, F_2, \dots, F_m$. C'est ainsi que *L. Kronecker* définit le discriminant[451])

$$D(f_1, f_2, \dots, f_m).*$$

67. Recherches spéciales. Des recherches spéciales relatives à l'élimination ont été faites pour certains cas particuliers. Ainsi le cas de trois équations du second degré à trois inconnues a été traité par *L. O. Hesse*[452]) et par *J. A. Serret*[453]).

A. Clebsch[454]) a résolu le cas de m équations homogènes dont $(m-2)$ linéaires, une quadratique et la dernière de degré quelconque.

450) *Gy. (J.) König,* Alg. Grössen [20]), p. 333.*

451) *Festschrift [451]) § 10; J. reine angew. Math. 92 (1882), p. 27; Werke 2, Leipzig 1897, p. 276 (Texte et notes 450/1 de *Gy. (J.) König* et *J. Kürschák*).*

452) J. reine angew. Math. 28 (1844), p. 68; Werke [230]), p. 89.

453) Alg. sup. [30]) 1, p. 168.

454) J. reine angew. Math. 58 (1860), p. 273.

J. Versluys[455]) résout un système d'équations dont l'une est du second degré, tandis que les autres sont linéaires. *P. Mansion*[456]) simplifie la solution de *J. Versluys*; *C. W. Baur*[457]), *E. J. Nanson*[458]) traitent le même problème.

S. Gundelfinger[459]) envisage $n-1$ équations homogènes à n variables dans le cas où deux de ces équations sont quadratiques et les $n-3$ autres linéaires.

H. R. Baltzer[460]) discute le cas de deux équations à deux inconnues.

R. Radau[461]) forme le résultant de trois formes quadratiques ternaires.

H. Lemonnier[462]) s'occupe de la résolution de trois équations quadratiques à trois inconnues.

V. Mollame[463]) étudie le système d'une équation quadratique, et d'une ou de deux équations linéaires et homogènes, à n inconnues[464]).*

K. Th. Vahlen[465]) démontre le théorème suivant: le nombre des systèmes de valeurs qui vérifient les $m+n$ équations

$$f_i(\overset{\mu_i}{x_1, \ldots, x_m}; \overset{\nu_i}{y_1, \ldots, y_n}) = 0$$

obtenues en prenant successivement $i = 1, 2, \ldots, m+n$ et dont la $i^{\text{ème}}$ est de degré μ_i par rapport aux x et de degré ν_i par rapport aux y, est égal à

$$\sum \mu_1 \mu_2 \ldots \mu_m \nu_{m+1} \nu_{m+2} \ldots \nu_{m+n},$$

où le signe Σ s'étend à tous les produits qu'on peut former avec m des $m+n$ nombres μ et n des $m+n$ nombres ν.

E. Hess[466]) remarque que les sommes de la forme $\sum x_i^p y_i^q$ étendues

455) *Archiv Math. Phys. (1) 60 (1877), p. 128.*

456) *Nouv. Corresp. math. 3 (1877), p. 376.*

457) *Z. Math. Phys. 14 (1869), p. 130.*

458) *Proc. R. Soc. Edinb. 22 (1897/9), p. 353.*

459) *Z. Math. Phys. 18 (1873), p. 543.*

460) *Progr. Dresde, 1868.*

461) *Nouv. Ann. math. (2) 8 (1869), p. 358; C. R. Acad. sc. Paris 68 (1869), p. 327.*

462) *Bull. Soc. math. France 7 (1878/9), p. 16; Bull. Soc. philom. Paris (7) 3 (1878/9), p. 73/5.*

463) *Atti Accad. Gioenia Catania (3) 18 (1885), p. 53/9.*

464) *Voir encore *H. Andoyer*, Nouv. Ann. math. (3) 15 (1896), p. 153 (intersection de deux quadriques); *T. Muir*, Proc. R. Soc. Edinb. 21 (1895/7), p. 220, 328; *E. J. Nanson*, id. 22 (1897/9), p. 150, 353; *J. McLaren*, id. 19 (1891/2), p. 264; *E. Amigues*, Nouv. Ann. math. (3) 13 (1894), p. 81 (intersection de deux coniques).*

465) J. reine angew. Math. 113 (1894), p. 348.

466) *Z. Math. Phys. 15 (1870), p. 326.*

aux racines communes (x_i, y_i) de deux équations algébriques

$$\varphi(x, y) = 0, \quad \psi(x, y) = 0$$

s'expriment simplement par des sommes de produits de certains déterminants dont les éléments sont formés au moyen des coefficients des équations proposées; il remarque aussi qu'on peut les exprimer par voie récurrente sous forme de sommes de produits de déterminants de même nature, multipliées par des fonctions analogues de degrés inférieurs.*

P. Gordan[467]) s'occupe du résultant de formes ternaires. Il traite en particulier le cas d'une forme ternaire cubique et de deux formes quadratiques au point de vue du calcul symbolique.

Fr. Junker[468]) calcule les fonctions symétriques des coordonnées des points d'intersection de deux courbes planes; il cherche les conditions pour que trois courbes planes aient des points communs et les conditions pour qu'une courbe plane ait des points singuliers.

A. Cayley[469]) considère quatre formes ternaires P, Q, U, V, les deux premières de même degré, et cherche la forme de la relation qui doit exister entre les coefficients des fonctions P, Q, U, V pour qu'il existe dans le faisceau $\lambda P + \mu Q = 0$ une courbe qui passe par deux des points d'intersection des courbes $U = 0$, $V = 0$.

A. Brill[470]) cherche la condition pour que trois courbes planes qui ont déjà un certain nombre de points communs se coupent encore en un point de plus. En formant dans le cas de trois fonctions de deux variables

$$f(x, y), \quad \varphi(x, y), \quad \psi(x, y)$$

l'expression à laquelle il donne le nom de *résultant réduit* (et qui n'est autre que celle déjà introduite par *A. Cayley*[471]) sous le nom de *résultant spécial*) il cherche à déterminer une fonction entière F des

467) Math. Ann. 50 (1898), p. 113; J. math. pures appl. (5) 3 (1897), p. 195; Verh. des ersten intern. Math.-Kongr. Zürich 1897, publ. par *F. Rudio*, Leipzig 1898, p. 143.

468) Neues Korrespondenzblatt für die Gelehrten- und Realschulen Württembergs 3 (1896), p. 434, 476.

469) Quart. J. pure appl. math. 11 (1871), p. 99, 132; Papers 8, Cambr. 1895, p. 22, 29.

470) Math. Ann. 4 (1871), p. 510; Abh. Akad. München 17 I (1888/9), éd. 1892, p. 89.

471) J. reine angew. Math. 34 (1847), p. 30; Papers 1, Cambr. 1889, p. 337. Voir aussi J. reine angew. Math. 63 (1864), p. 34; 64 (1865), p. 167; Quart. J. pure appl. math. 11 (1871), p. 211; Papers 5, Cambridge 1892, p. 162, 416; 8, Cambridge 1895, p. 46.

coefficients de f, φ et ψ telle que, quand les trois équations

$$f(x, y) = 0, \quad \varphi(x, y) = 0, \quad \psi(x, y) = 0$$

sont identiquement vérifiées par un ou plusieurs systèmes de valeurs (x, y), la condition $F = 0$ entraîne encore de nouveaux systèmes de solutions de ces mêmes équations.

Il démontre que si les trois équations

$$f(x, y) = 0, \quad \varphi(x, y) = 0, \quad \psi(x, y) = 0$$

représentent trois courbes, de degrés respectivement égaux à n, p, q, ayant en α un point multiple d'ordre ν pour la courbe $f(x, y) = 0$, d'ordre π pour la courbe $\varphi(x, y) = 0$, d'ordre ϱ pour la courbe $\psi(x, y) = 0$, le degré du résultant réduit par rapport aux coefficients des trois fonctions $f(x, y)$, $\varphi(x, y)$ et $\psi(x, y)$ est respectivement égal à $pq - \nu$, $qn - \pi$ et $np - \varrho$.

L. Berzolari[472]) a démontré que, étant données trois surfaces algébriques d'ordres l, m, n, simples ou composées d'une façon quelconque, pouvant posséder une infinité de points singuliers mais ne passant pas par la même courbe, la condition nécessaire et suffisante pour qu'un point O, commun à ces trois surfaces et ayant respectivement les multiplicités λ, μ, ν pour chacune des trois surfaces prise isolément, soit un point commun de multiplicité $\lambda\mu\nu$ et non davantage, est que les trois cônes tangents aux trois surfaces au point O n'aient aucune génératrice commune.*

68. Mémoires divers relatifs à l'élimination ou à la divisibilité. *R. F. Davis*[473]) appelle équations *porismatiques*[473a]) un système de n équations à n variables qui n'ont pas de racines finies ou sont indéterminées suivant qu'une certaine relation entre les coefficients (dite relation porismatique) n'est pas vérifiée ou est vérifiée. L'auteur ne considère d'ailleurs que des équations de la forme

$$F(y, z) = 0, \quad F(z, x) = 0, \quad F(x, y) = 0$$

où F désigne une fonction rationnelle entière de deux variables dont la forme ne change pas quand on transpose ces deux variables.

L. Saltel[474]) donne une méthode qui permet d'éliminer *successivement*, par la simple résolution de l'équation $ax^n + b = 0$, $(k-1)$ inconnues entre k équations, en étudiant les solutions étrangères qui

472) *Ann. mat. pura appl. (2) 24 (1896), p. 165/91.*

473) *The mathematical gazette, cah. 17 (1899), p. 252; cah. 18 (1899), p. 273.*

473a) *Probablement d'après *J. Wolstenholme*, Math. problems, (3e éd.) Londres 1891, p. 85 [poristic systems of equations] (Note de *G. Loria*).*

474) *Nouv. Ann. math. (3) 2 (1883), p. 554.*

s'introduisent nécessairement dans les autres équations par la substitution de la valeur $x^n = -\frac{b}{a}$ tirée de la première équation, et en indiquant le moyen de supprimer, dans la suite des calculs, ces solutions étrangères.

Ch. Méray[475]) tente un essai de décomposition symbolique d'un polynome entier à plusieurs variables en éléments linéaires.

J. Kürschák[476]) obtient sous une forme assez simple la condition nécessaire et suffisante pour que deux fonctions rationnelles entières

$$f(x_1, x_2, \ldots, x_m), \quad \varphi(x_1, x_2, \ldots, x_m)$$

admettent un diviseur commun. Si $y_1, y_2, \ldots, y_m$ désignent m variables auxiliaires et λ un paramètre, il faut et il suffit qu'en envisageant

$$f(x_1 + \lambda y_1, x_2 + \lambda y_2, \ldots, x_m + \lambda y_m), \quad g(x_1 + \lambda y_1, \ldots, x_m + \lambda y_m)$$

comme des fonctions de λ et $x_1, x_2, \ldots, x_m$, $y_1, y_2, \ldots, y_m$ comme des indéterminées, le résultant de ces deux fonctions de λ s'annule identiquement en $x_1, x_2, \ldots, x_m$, $y_1, y_2, \ldots, y_m$.*

Citons encore *L. Zmurko*[477])*, *F. Mertens*[478]), *K. Bes*[479]), enfin *D. André*[480]) qui cherche à obtenir des fonctions rationnelles entières $f(x_1, x_2, \ldots, x_n)$ telles que si l'on détermine $y_1, y_2, \ldots, y_n$ par les égalités

$$\frac{f(x_1, x_2, \ldots, x_n)}{y_1} = \frac{f(x_2, x_3, \ldots, x_n, x_1)}{y_2} = \cdots = \frac{f(x_n, x_1, x_2, \ldots, x_{n-1})}{y_n}$$

on ait en retour

$$\frac{f(y_1, y_2, \ldots, y_n)}{x_1} = \frac{f(y_2, y_3, \ldots, y_n, y_1)}{x_2} = \cdots = \frac{f(y_n, y_1, y_2, \ldots, y_{n-1})}{x_n}.$$

Théorie générale de l'élimination.

69. Méthode d'élimination de Kronecker. Nous n'avons envisagé jusqu'ici que des systèmes d'équations algébriques où le nombre des équations est égal au nombre des variables ou le surpasse d'une unité.

475) *Ann. Ec. Norm. (3) 2 (1885), p. 289.*

476) *Math. Ann. 60 (1905), p. 317.*

477) *Denkschr. Akad. Wien (math.) 30 II (1870), p. 217 [1869].*

478) Pamiętnik Akad. Umiejętności (Mém. Cracovie) 17 (1890), p. 143/65; Rozprawy Akad. Umiejętności (2) 1 (1891), p. 333/52; Bull. intern. Acad. sc. Cracovie 1890 (éd. 1891), p. 57, 285.

479) Verhand. Akad. Wetensch. Amsterdam Afdeeling Naturkunde erste Sectie (2) 8 (1901/4), mém. n° 2; Handelingen van het 8ste Nederlandsch Natuur.-Geneeskundig Congres, Rotterdam avril 1901, p. 152/5.

480) Bull. Soc. math. France 24 (1896), p. 136.

Dans ce dernier cas nous avons surtout cherché à obtenir les conditions sous lesquelles le système d'équations admet des solutions; dans tous les cas nous n'avons appris à déterminer les solutions du système que quand ces solutions sont en nombre *fini.*

Dans la *théorie générale de l'élimination* on abandonne toute restriction concernant le nombre des variables, le nombre des équations, ou encore le nombre des solutions du système d'équations que l'on envisage. Lorsque le nombre de ces solutions est infini on cherche avant tout à grouper ces solutions d'une façon naturelle.

*Pour trois variables x, y, z par exemple et un nombre quelconque m d'équations algébriques

$$f_1(x, y, z) = 0, \quad f_2(x, y, z) = 0, \ \dots, \quad f_m(x, y, z) = 0,$$

à chaque racine (ξ, η, ζ) du système correspond, dans l'espace orienté par un trièdre de référence donné, un *point* de coordonnées ξ, η, ζ; nous l'appellerons *point-racine* (ξ, η, ζ) du système d'équations algébriques envisagé. Le problème qu'il s'agit de résoudre dans la théorie générale de l'élimination consiste à grouper les différentes solutions du système en ensembles correspondant à des points-racines du système formant des surfaces, des courbes non situées sur ces surfaces et des points isolés. L'ensemble des trois variables x, y, z constitue une variété à 3 dimensions; l'ensemble des solutions qui correspond à chacune des surfaces ainsi obtenues constitue une variété à 2 dimensions, l'ensemble des solutions qui correspond à chacune des courbes ainsi obtenues constitue une variété à 1 dimension, enfin chaque solution qui correspond à l'un des points isolés constitue une variété à 0 dimension. Chacune de ces variétés à 2, 1 ou 0 dimensions est dite située dans la variété envisagée à 3 dimensions.

Dans le cas d'un nombre quelconque n de variables nous ferons usage de la même terminologie et nous serons ainsi amenés à introduire des variétés de $n-1, n-2, \dots, 3, 2, 1, 0$ dimensions situées dans une variété donnée à n dimensions. Chacune de ces variétés est formée de solutions du système de m équations algébriques envisagées; chacune de ces solutions $(\xi_1, \xi_2, \dots, \xi_n)$ correspond à un *point-racine* de *coordonnées* $\xi_1, \xi_2, \dots, \xi_n$.*

On doit à *L. Kronecker*[481]) une méthode générale qui permet de classer les racines communes d'un système quelconque d'équations

481) Grundzüge einer arithmetischen Theorie der algebraischen Grössen, Festschrift zu Herrn Kummers Doctorjubiläum, Berlin 1881, § 10, 20, 21; J. reine angew. Math. 92 (1882), p. 27, 70; Werke 2, Leipzig 1897, p. 275, 326; voir aussi J. reine angew. Math. 99 (1886), p. 336; Werke 3¹, Leipzig 1899, p. 156.

données suivant la variété à laquelle elles appartiennent. Cette méthode a été exposée tout au long et commentée par *J. Molk*[482]); on la retrouve modifiée et complétée dans l'ensemble des recherches de *Gy. (J.) König*[483]).

Soient

$$f_1(x_1, x_2, \dots, x_n), \quad f_2(x_1, x_2, \dots, x_n), \quad \dots, \quad f_m(x_1, x_2, \dots, x_n)$$

m fonctions de n variables, dont les coefficients sont donnés. *Ces coefficients peuvent être soit des indéterminées, soit des fonctions données d'un certain nombre de paramètres.* *L. Kronecker* se propose de déterminer les limitations qu'apporte à la variété à n dimensions constituée par les variables $x_1, x_2, \dots, x_n$ le système des m équations

$$f_1 = 0, \ f_2 = 0, \ \dots, \ f_m = 0.$$

*On peut d'abord, au moyen d'une substitution linéaire

$$x_h = \sum_{i=1}^{i=n} \alpha_{ih} x_i' \qquad (h = 1, 2, \dots, n),$$

faire en sorte que chacune des m fonctions $f_1, f_2, \dots, f_m$ soit *régulière.* Alors, si les m fonctions $f_1, f_2, \dots, f_m$ ont un diviseur commun, ce diviseur sera une fonction rationnelle entière de *toutes* les variables.

Effectuons la substitution de *Liouville* (n° **58**)

$$x = u_1 x_1 + u_2 x_2 + \cdots + u_{n-1} x_{n-1} + u_n x_n;$$

elle transforme chacune des fonctions $f_\alpha(x_1, \dots, x_n)$, multipliée par une puissance convenable de u_n, en une fonction rationnelle entière de $x, x_1, \dots, x_{n-1}, u_1, u_2, \dots, u_n$ que nous désignerons par

$$K_\alpha(x, x_1, x_2, \dots, x_{n-1}; \ u_1, u_2, \dots, u_{n-1}, u_n).$$

Soit $D_1(x, x_1, \dots, x_{n-1})$ le plus grand commun diviseur des fonctions K_α.

Soit aussi, pour chaque indice $\alpha = 1, 2, \dots, m$,

$$K_\alpha = D_1 L_{1\alpha},$$

et envisageons le système

$$(L_{11}, L_{12}, \dots, L_{1m}).$$

Désignons par $R_1(x, x_1, x_2, \dots, x_{n-1})$ le produit des facteurs irréductibles *distincts* (chacun pris une seule fois) qui figurent dans la fonction

$$D_1(x, x_1, x_2, \dots, x_{n-1}).$$

482) Thèse, Paris 1884; Acta math. 6 (1885), p. 107.
483) Alg. Grössen [20]), p. 199.

Les coordonnées $\xi_1, \xi_2, \ldots, \xi_n$ de chaque point-racine $(\xi_1, \xi_2, \ldots, \xi_n)$ du système d'équations

$$f_1(x_1, x_2, \ldots, x_n) = 0, \quad f_2(x_1, x_2, \ldots, x_n) = 0, \quad \ldots, \quad f_m(x_1, x_2, \ldots, x_n) = 0$$

vérifient ou bien l'équation $R_1 = 0$ ou bien le système d'équations

$$L_{11} = 0, \; L_{12} = 0, \; \ldots, \; L_{1m} = 0,$$

si l'on n'envisage la lettre x dans R_1 et dans $L_{11}, L_{12}, \ldots, L_{1m}$ que comme un symbole abrégé qui représente l'expression $u_1 x_1 + u_2 x_2 + \cdots + u_n x_n$. Inversement chaque système $(\xi_1, \xi_2, \ldots, \xi_n)$ qui vérifie soit l'équation $R_1 = 0$ soit le système d'équations

$$L_{11} = 0, \; L_{12} = 0, \; \ldots, \; L_{1m} = 0$$

est une racine du système d'équations

$$f_1(x_1, x_2, \ldots, x_n) = 0, \; f_2(x_1, x_2, \ldots, x_n) = 0, \; \ldots, \; f_m(x_1, x_2, \ldots, x_n) = 0.$$

Il est d'ailleurs sous-entendu que $\xi_1, \xi_2, \ldots, \xi_n$ ne dépendent pas des indéterminées $u_1, u_2, \ldots, u_n$.

Pour obtenir les solutions $(\xi_1, \xi_2, \ldots, \xi_n)$ de l'équation $R_1 = 0$ on peut opérer comme il suit:

Les valeurs $x_1 = \xi_1, x_2 = \xi_2, \ldots, x_{n-1} = \xi_{n-1}$ étant fixées arbitrairement, de façon toutefois à être indépendantes des indéterminées $u_1, u_2, \ldots, u_n$, on détermine les valeurs ξ de x pour lesquelles la fonction R_1 s'annule; ces valeurs ξ sont en nombre fini et elles sont de la forme

$$u_1 \xi_1 + u_2 \xi_2 + \cdots + u_n \xi_n;$$

on peut donc en déduire les valeurs correspondantes de x_n. On voit ainsi que l'équation $R_1 = 0$ représente une *variété* de dimension $n - 1$ dont tous les points sont des points-racines du système d'équations proposées.*

L'ensemble des points-racines du système d'équations proposées, abstraction faite de l'ordre de multiplicité de ces points-racines, est ainsi formé de l'ensemble des points constituant la variété $R_1 = 0$ à $n-1$ dimensions et de l'ensemble des points-racines du système d'équations

$$L_{11} = 0, \; L_{12} = 0, \; \ldots, \; L_{1m} = 0.$$

Rien ne dit d'ailleurs que, parmi les points de ce dernier ensemble, il n'y en a pas plusieurs, ou même une infinité, faisant partie de la variété $R_1 = 0$. Mais les points cherchés, racines du système donné, qui ne sont pas sur la variété $R_1 = 0$ sont certainement des points-racines du système

$$L_{11} = 0, \; L_{12} = 0, \; \ldots, \; L_{1m} = 0.$$

Ceci posé désignons par $U_1, U_2, \ldots, U_m$ et par $V_1, V_2, \ldots, V_m$ deux systèmes d'indéterminées et formons les deux fonctions

$$\sum_{i=1}^{i=m} U_i L_{1i} \quad \text{et} \quad \sum_{i=1}^{i=m} V_i L_{1i}.$$

Toute racine commune du système d'équations

$$L_{11} = 0, \; L_{12} = 0, \; \ldots, \; L_{1m} = 0$$

annule ces deux fonctions; inversement toute solution

$$x = \xi, \quad x_1 = \xi_1, \quad x_2 = \xi_2, \quad \ldots, \quad x_{n-1} = \xi_{n-1}$$

qui annule ces deux fonctions, quelles que soient les indéterminées U et V, fournit une racine commune $(\xi, \xi_1, \ldots, \xi_{n-1})$ du système d'équations

$$L_{11} = 0, \; L_{12} = 0, \; \ldots, \; L_{1m} = 0$$

si nous y considérons $x, x_1, x_2, \ldots, x_{n-1}$ comme les variables.

Ceci posé formons le résultant E_1 des deux fonctions

$$U_1 L_{11} + U_2 L_{12} + \cdots + U_m L_{1m}$$
$$V_1 L_{11} + V_2 L_{12} + \cdots + V_m L_{1m}$$

envisagées comme des fonctions de x_{n-1}, en supposant les $L_{11}, L_{12}, \ldots, L_{1m}$ exprimés en fonction de $x, x_1, x_2, \ldots, x_{n-1}$ et en faisant abstraction de ce que, au fond, x dépend aussi de x_{n-1}. Ordonnons le résultant E_1 ainsi formé suivant les produits des puissances des indéterminées U et V et désignons alors par $s_{11}, s_{12}, \ldots, s_{1\mu}$ les coefficients de E_1 pris dans un ordre quelconque. Chaque racine du système d'équations $L_{11} = 0, L_{12} = 0, \ldots, L_{1m} = 0$ fournit une racine commune du système d'équations

$$\begin{cases} s_{11}(x, x_1, x_2, \ldots, x_{n-2}) = 0, \\ s_{12}(x, x_1, x_2, \ldots, x_{n-2}) = 0, \\ \cdots\cdots\cdots\cdots \\ s_{1\mu}(x, x_1, x_2, \ldots, x_{n-2}) = 0; \end{cases}$$

inversement à chaque racine $(\xi, \xi_1, \xi_2, \ldots, \xi_{n-2})$ de ce dernier système correspond une valeur ξ_{n-1} telle que $(\xi, \xi_1, \xi_2, \ldots, \xi_{n-1})$ soit racine du système d'équations

$$L_{11} = 0, \; L_{12} = 0, \; \ldots, \; L_{1m} = 0;$$

d'ailleurs ξ_{n-1} est nécessairement indépendante des indéterminées U et V.

Une analyse plus précise met en évidence que l'ensemble des racines des équations données

$$f_1 = 0, \; f_2 = 0, \; \ldots, \; f_m = 0$$

est aussi fourni, abstraction faite de l'ordre de multiplicité de ces racines, par la variété $R_1 = 0$ de dimension $n - 1$ et par les racines du système d'équations

$$s_{11} = 0, \; s_{12} = 0, \; \ldots, \; s_{1\mu} = 0,$$

si l'on suppose $s_{11}, s_{12}, \ldots, s_{1\mu}$ exprimées *en fonction de*

$$x_1, x_2, \ldots, x_n$$

et que l'on n'envisage que les racines indépendantes de $u_1, u_2, \ldots, u_n$.

Si D_2 est le p. g. c. d. des fonctions $s_{11}, s_{12}, \ldots, s_{1\mu}$ de $x, x_1, x_2, \ldots, x_{n-2}$ nous désignerons par $R_2(x, x_1, x_2, \ldots, x_{n-2})$ le produit des facteurs irréductibles distincts (chacun pris une seule fois) qui figurent dans la fonction D_2; d'autre part nous poserons

$$s_{11} = D_2\Lambda_{11}, \; s_{12} = D_2\Lambda_{12}, \; \ldots, \; s_{1\mu} = D_2\Lambda_{1\mu}.$$

L'ensemble des points-racines du système d'équations

$$s_{11} = 0, \; s_{12} = 0, \; \ldots, \; s_{1\mu} = 0$$

est alors formé, abstraction faite de l'ordre de multiplicité de ces racines, par l'ensemble des points-racines de l'équation $R_2 = 0$ et par l'ensemble des points-racines du système

$$\Lambda_{11} = 0, \; \Lambda_{12} = 0, \; \ldots, \; \Lambda_{1\mu} = 0;$$

un même point-racine peut d'ailleurs faire partie des deux ensembles.

*Envisageons d'abord les points-racines de $R_2 = 0$; à cet effet fixons arbitrairement les coordonnées $x_1 = \xi_1, x_2 = \xi_2, \ldots, x_{n-2} = \xi_{n-2}$; chaque racine $x = \xi$ de l'équation en x

$$R_2(x, \xi_1, \xi_2, \ldots, \xi_{n-2}) = 0$$

est de la forme

$$\xi = u_1\xi_1 + u_2\xi_2 + \cdots + u_{n-2}\xi_{n-2} + u_{n-1}\xi_{n-1} + u_n\xi_n;$$

elle fournit donc les valeurs ξ_{n-1}, ξ_n qui jointes à $\xi_1, \xi_2, \ldots, \xi_{n-2}$ vérifient $R_2 = 0$ si l'on n'envisage x que comme une notation abrégée pour désigner $u_1x_1 + u_2x_2 + \cdots + u_nx_n$; les points-racines de l'équation $R_2 = 0$ forment donc une variété à $n-2$ dimensions satisfaisant au système d'équations

$$f_1 = 0, \; f_2 = 0, \ldots, f_m = 0.$$

Quant au système

$$\Lambda_{11} = 0, \; \Lambda_{12} = 0, \; \ldots, \; \Lambda_{1\mu} = 0,$$

on le traitera comme on a traité plus haut le système

$$L_{11} = 0, \; L_{12} = 0, \; \ldots, \; L_{1m} = 0;$$

il en diffère seulement par ce qu'il contient *une variable de moins;* le nombre m d'équations n'ayant d'ailleurs joué aucun rôle, la valeur du nombre naturel μ importe peu.*

Finalement en continuant ainsi, on forme successivement des fonctions $R_1, R_2, \ldots, R_{n-1}, R_n$, à $n, n-1, \ldots, 2, 1$ variables. *L. Kronecker* a appelé R_k le *résolvant de rang k* du système envisagé et

$$R = R_1R_2R_3 \ldots R_{n-1}R_n$$

le *résolvant total* de ce système. (Un ou plusieurs des résolvants partiels R_k peuvent d'ailleurs se réduire à des constantes).

L'équation $R_k = 0$ est l'*équation résolvante de rang k* du système d'équations algébriques envisagée (ou simplement *le résolvant* de rang k).

L'équation unique

$$R = R_1R_2R_3 \ldots R_n = 0$$

est le *résolvant total* du système d'équations algébriques[484])

$$f_1 = 0, \; f_2 = 0, \; \ldots, \; f_m = 0.$$

Si, dans les expressions de $R_1, R_2, \ldots, R_n$, on envisage la lettre x comme une notation abrégée pour

$$u_1x_1 + u_2x_2 + \cdots + u_nx_n$$

et si l'on ne tient compte que des solutions indépendantes de $u_1, u_2, \ldots, u_n$, le système d'équations ($f_1 = 0, f_2 = 0, \ldots, f_m = 0$) et l'équation unique $R = 0$ fournissent *exactement* les mêmes racines à condition de faire abstraction de l'ordre de multiplicité de ces racines.

Observons ici que la substitution linéaire

$$x_h = \alpha_{1h}x_1' + \alpha_{2h}x_2' + \cdots + \alpha_{nh}x_n' \qquad (h = 1, 2, \ldots, n)$$

dont il a été fait mention plus haut et qu'il est indispensable d'effectuer avant de commencer le calcul du résolvant total d'un système d'équations algébriques données doit être choisie telle que non seulement les fonctions rationnelles entières sur lesquelles on effectue les transformations indiquées soient *régulières* mais encore telles que les fonctions $E_1, E_2, \ldots$ rencontrées dans le courant des calculs soient *régulières* par rapport aux variables $x, x_1, x_2, \ldots$ qui y figurent, en sorte que E_1 soit régulière en $x, x_1, x_2, \ldots, x_{n-1}$, que E_2 soit régulière en $x, x_1, x_2, \ldots, x_{n-2}$, et ainsi de suite.

Si le résolvant R_1 de rang *un* d'un système d'équations algébriques données ($f_1 = 0, f_2 = 0, \ldots, f_m = 0$) ne se réduit pas à une constante on dit que le système de fonctions ($f_1, f_2, \ldots, f_m$) est de *rang un.* Plus généralement si R_k est le premier des résolvants $R_1, R_2, R_3, \ldots$ du système d'équations algébriques

$$f_1 = 0, \; f_2 = 0, \; \ldots, \; f_m = 0$$

données qui ne se réduise pas à une constante on dit que le système de fonctions ($f_1, f_2, \ldots, f_m$) est de rang k.

On dit qu'un système ($f_1, f_2, \ldots, f_m$) est *simple* quand un seul des résolvants $R_1, R_2, R_3, \ldots, R_n$ ne se réduit pas à une constante. Dans le cas contraire on dit que ce système est *mêlé.*

---

484) *L. Kronecker*, Festschr.[481]); *J. Molk,* Thèse, Paris 1884; Acta math. 6 (1885), p. 126, 131.

*Si l'on décompose le résolvant R_k de rang k en ses facteurs irréductibles $R_k^{(1)}$, $R_k^{(2)}, \ldots$ et que dans l'un quelconque de ces facteurs $R_k^{(i)}$ on remplace x par la fonction linéaire $u_1x_1 + u_2x_2 + \cdots + u_nx_n$ que cette lettre représente, l'ensemble des points-racines dont les coordonnées $\xi_1, \xi_2, \ldots, \xi_n$ vérifient l'équation $R_k^{(i)} = 0$ pour toutes les valeurs possibles de $u_1, u_2, \ldots, u_n$ forme une variété *irréductible* de dimension $n - k$ et de rang k.

Au résolvant R_k de rang k d'un système d'équations algébriques données (que R_k soit d'ailleurs irréductible ou non), on peut faire correspondre un système d'équations algébriques $\varphi_1 = 0$, $\varphi_2 = 0, \ldots$, en nombre égal, au plus, à $n+1$ et tel que tout point-racine de ce système

$$\varphi_1 = 0, \quad \varphi_2 = 0, \ldots$$

soit un point de la variété $R_k = 0$ et qu'inversement tout point de cette variété $R_k = 0$ soit point-racine du système $\varphi_1 = 0$, $\varphi_2 = 0, \ldots$

Le système d'équations algébriques ainsi formé $\varphi_1 = 0$, $\varphi_2 = 0, \ldots$ est ce que *J. Molk* appelle la *figuration complète* de la variété correspondante $R_k = 0$.*

K. Th. Vahlen[485]) a montré pourquoi $n+1$ équations sont parfois nécessaires pour définir une variété à ν dimensions dans une variété à n dimensions.

Il n'est pas toujours possible de représenter une variété de dimension $n-k$ dans un espace à n dimensions par k équations entre n variables sans introduire des points formant d'autres variétés de même dimension $n-k$. Ainsi quand on se propose de représenter une courbe gauche du troisième ordre par deux surfaces, il arrive que ces deux surfaces de quelque manière qu'on les choisisse se coupent non seulement suivant la courbe gauche mais aussi en une courbe ou une droite étrangère à cette courbe gauche du troisième ordre.

Il est possible que le système $(f_1 = 0, f_2 = 0, \ldots, f_m = 0)$ n'ait aucune racine finie. Chacun des résolvants $R_1, R_2, \ldots, R_n$ se réduit alors à une constante et réciproquement. Un tel système est de rang $n+1$; en voici un exemple:

$$f_1(z_1, z_2) = 0, \quad f_2(z_1, z_2) = f_1(z_1, z_2) + a = 0,$$

a étant une constante différente de zéro.

70. Recherches de König[486]). *Dans la théorie générale de l'élimination de *L. Kronecker* on fait abstraction de l'ordre de multiplicité des points-racines du système d'équations algébriques envi-

485) J. reine angew. Math. 108 (1891), p. 346.

486) *Ce numéro est dû à *J. Kürschák*.*

sagées. Pour pouvoir tenir compte de cet ordre de multiplicité *Gy. (J.) König* envisage, outre l'équation résolvante totale

$$R = R_1 R_2 R_3 \ldots R_n = 0$$

de *L. Kronecker* qu'il appelle le résolvant total *réduit*[487]) du système d'équations algébriques

(1) $f_1(x_1, x_2, \ldots, x_n) = 0$, $f_2(x_1, x_2, \ldots, x_n) = 0, \ldots, f_m(x_1, x_2, \ldots, x_n) = 0$,

la fonction

$$D = D_1 D_2 D_3 \ldots D_n$$

dont les facteurs $D_1, D_2, D_3, \ldots$ ont été définis au nº **69** et l'équation correspondante

$$D = 0;$$

il appelle D le *résolvant total complet*[488]) et $D = 0$ l'*équation résolvante totale complète*[489]) du système d'équations (1).

Chaque *résolvant partiel complet* D_k a les mêmes facteurs irréductibles $\varrho_{k1}, \varrho_{k2}, \ldots$ que le résolvant partiel réduit R_k, mais dans R_k chacun de ces facteurs irréductibles ϱ_{ki} ne figure qu'une fois tandis qu'il peut figurer plusieurs fois dans D_k. L'exposant auquel ϱ_{ki} figure dans D_k est la *multiplicité* de la variété irréductible représentée par l'équation $\varrho_{ki} = 0$.

Lorsque le système $(f_1, f_2, \ldots, f_m)$ est de rang n, on a $D = D_n$ et à chaque facteur irréductible ϱ de D correspond alors un point-racine du système d'équations algébriques

$$(f_1 = 0, \; f_2 = 0, \; \ldots, \; f_m = 0).$$

Il resterait à voir si, dans le cas où $m = n$, chacun des points-racines de ce système d'équations algébriques a le même ordre de multiplicité au sens actuel de *Gy. (J.) König* et au sens donné à ce mot au nº **66** dans le cas particulier où $m = n$.

Si dans la fonction D on remplace $u_1, u_2, \ldots, u_{n-1}$ par 0 et u_n par 1 on obtient la fonction rationnelle entière

$$r(x_1, x_2, \ldots, x_n)$$

que *Gy. (J.) König* appelle la *forme résolvante*[490]) du système $(f_1, f_2, \ldots, f_m)$

487) **Gy. (J.) König*, Alg. Grössen[20]), p. 214.*

488) *Id., p. 207.*

489) *On rencontre déjà le résolvant total complet D dans des recherches antérieures à celles de *Gy. (J.) König;* mais dans ces recherches la différence essentielle entre ce résolvant D et le résolvant R de *L. Kronecker* n'avait pas été mise en pleine lumière; les résolvants D et R ont été souvent désignés [voir par ex. *E. Delassus*[499])] tous deux sous le nom commun de *résolvant de Kronecker*.*

490) **Gy. (J.) König*, Alg. Grössen[20]), p. 107.*

relativement à $x_1, x_2, \ldots, x_n$. A chaque fonction rationnelle entière $r(x_1, x_2, \ldots, x_n)$ on peut faire correspondre univoquement, par un procédé facile à appliquer, m fonctions rationnelles entières

$$X_1(x_1, x_2, \ldots, x_n),\ X_2(x_1, x_2, \ldots, x_n),\ \ldots,\ X_m(x_1, x_2, \ldots, x_n),$$

telles que l'on ait

$$f_1 X_1 + f_2 X_2 + \cdots + f_m X_m = r.$$

Soit ϱ_{ki} un des facteurs irréductibles du résolvant partiel réduit R_k d'un système $(f_1, f_2, \ldots, f_m)$. Il peut arriver que *tous* les points de la variété irréductible représentée par l'équation $\varrho_{ki} = 0$ fassent déjà partie de l'une ou l'autre des variétés

$$R_1 = 0,\ R_2 = 0,\ \ldots,\ R_{k-1} = 0.$$

S'il en est ainsi on peut, en écrivant le résolvant total réduit, laisser de côté ce facteur irréductible ϱ_{ki} sans que l'on perde par là aucun des points-racines du système d'équations

$$(f_1 = 0,\ f_2 = 0,\ \ldots,\ f_m = 0).$$

Gy. (J.) König appelle *résolvant minimé*[491]) du système

$$(f_1 = 0,\ f_2 = 0,\ \ldots,\ f_m = 0)$$

le résolvant total réduit débarrassé de tous les facteurs ϱ_{ki} du type que l'on vient de signaler

$$(k = 2, 3, \ldots, n;\ i = 1, 2, \ldots).$$

L'équation résolvante minimée s'obtient en égalant le résolvant minimé à zéro.

L'équation *résolvante minimée* a, tout comme l'équation *résolvante totale réduite*, pour points-racines exactement ceux du système

$$(f_1 = 0,\ f_2 = 0,\ \ldots,\ f_m = 0)$$

si l'on fait abstraction de l'ordre de multiplicité de ces points-racines.

A chaque système d'équations algébriques

$$(f_1 = 0,\ f_2 = 0,\ \ldots,\ f_m = 0)$$

on peut faire correspondre un système déterminé d'équations algébriques

$$\varphi_1 = 0,\quad \varphi_2 = 0,\ \ldots$$

en nombre égal *au plus* à $n + 1$, qui a *même résolvante minimée* que le premier[492]). *Gy. (J.) König* dit du second système qu'il est la *figuration complète* du premier quand bien même ce second système n'est pas simple mais mêlé.

491) *Gy. (J.) König*, Alg. Grössen [20]), p. 235.*

492) *Id. p. 234/8.*

L'ensemble des points communs à deux variétés constitue l'*intersection* de ces deux variétés. *Gy. (J.) König*[493]) a démontré que si une variété irréductible ϱ_k de rang k (de dimension $n - k$) n'est pas contenue tout entière dans une variété donnée w_k de même rang k, l'intersection des deux variétés forme une ou plusieurs variétés chacune de rang supérieur à k. Ainsi se trouve précisé un théorème énoncé par *L. Kronecker*[494]) sous la forme que voici: Lorsqu'un système d'équations algébriques représente une variété irréductible de dimension $n - k$, il n'y a aucun système d'équations algébriques qui permette de représenter *une partie seulement* de cette variété irréductible de dimension $n - k$.

En modifiant légèrement la démonstration de *Gy. (J.) König* on peut aussi démontrer que si une variété algébrique irréductible ϱ_k de rang k (de dimension $n - k$) n'est pas contenue tout entière dans une variété algébrique donnée w_h de rang $h \leq k$, l'intersection des deux variétés est formée de variétés algébriques chacune de rang supérieur à k. Pour $h = 1$ on a donc en particulier le théorème: Lorsque tous les points d'une variété algébrique irréductible de rang k (de dimension $n - k$) sont points-racines d'une certaine équation *réductible*

$$A(x_1, x_2, \ldots, x_n)\, B(x_1, x_2, \ldots, x_n) = 0$$

(en sorte que les coordonnées de chacun de ces points vérifient cette équation réductible) il faut que ces points soient ou bien *tous* des points-racines de $A = 0$ ou bien *tous* des points-racines de $B = 0$. Ce théorème admet une réciproque. On peut donc aussi définir l'irréductibilité de la façon suivante (cf. nº **72**):

Une *variété algébrique* (c'est-à-dire l'ensemble des points-racines d'un système d'équations algébriques) sera dite *irréductible* si chaque fois que les coordonnées $x_1, x_2, \ldots, x_n$ de chacun des points-racines qui constituent cette variété vérifient une équation réductible de la forme

$$A(x_1, x_2, \ldots, x_n)\, B(x_1, x_2, \ldots, x_n) = 0,$$

ces points-racines sont nécessairement ou bien *tous* des points-racines de l'équation

$$A(x_1, x_2, \ldots, x_n) = 0$$

ou bien *tous* des points-racines de l'équation

$$B(x_1, x_2, \ldots, x_n) = 0.$$

Voici encore un autre théorème de *L. Kronecker* que *Gy. (J.) König* a précisé en lui donnant la forme suivante:

493) *Gy. (J.) König*, Alg. Grössen [20]), p. 223.*

494) *L. Kronecker*, Festschrift [481]) § 10; J. reine angew. Math. 92 (1882), p. 30; Werke 2, Leipzig 1897, p. 280.*

Si l'on connaît le résolvant réduit R_k (de rang k, de dimension $n-k$) d'un système *simple*

$$f_1(x_1, x_2, \ldots, x_n),\ f_2(x_1, x_2, \ldots, x_n),\ \ldots,\ f_m(x_1, x_2, \ldots, x_n)$$

de rang k, on peut toujours former des fonctions rationnelles entières

$$\Delta(x_k, x_{k+1}, \ldots, x_n),\ f(x_k, x_{k+1}, \ldots, x_n),\ \varphi(x_k, x_{k+1}, \ldots, x_n),$$
$$\psi_1(x_k, x_{k+1}, \ldots, x_n),\ \psi_2(x_k, x_{k+1}, \ldots, x_n),\ \ldots,\ \psi_{k-1}(x_k, x_{k+1}, \ldots, x_n)$$

telles que d'une part le système d'équations

$$(1) \qquad f=0,\ x_1\varphi+\psi_1=0,\ \ldots,\ x_{k-1}\varphi+\psi_{k-1}=0$$

admette comme points-racines *tous* les points racines du système d'équations ($f_1=0, f_2=0, \ldots, f_m=0$) et que d'autre part ce système d'équations (1) n'admette comme points-racines vérifiant l'inégalité $\Delta \gtrless 0$ *que* des points-racines du système d'équations ($f_1=0, f_2=0, \ldots, f_m=0$). Il peut y avoir des points-racines du système d'équations ($f_1=0, f_2=0, \ldots, f_m=0$) qui vérifient à la fois le système d'équations (1) et l'égalité $\Delta=0$; l'ensemble de ces points ne saurait toutefois former qu'une ou plusieurs variétés de rangs au moins égaux à $k+1$. Il peut aussi y avoir des points-racines du système (1) qui ne soient pas points-racines du système d'équations ($f_1=0, f_2=0, \ldots, f_m=0$); ces points-racines forment alors une variété de rang 2.

Gy. (J.) König[495]) appelle *figuration principale* du système *simple* ($f_1, f_2, \ldots, f_m$) de rang k la variété représentée par les égalités (1) jointes à l'inégalité $\Delta \gtrless 0$. Cette *figuration principale* d'un système simple ne comprend pas les variétés particulières de rangs au moins égaux à $k+1$ signalées plus haut (pour lesquelles $\Delta=0$) qui peuvent cependant faire partie de ce système simple; ces variétés particulières quand elles existent doivent être envisagées à part.

On rencontre déjà dans des recherches antérieures à celles de *Gy. (J.) König* relatives à la théorie de l'élimination des figurations de variétés analogues à cette figuration principale. C'est ainsi par ex. que *M. Nöther*[496]), en faisant usage d'une figuration convenable des variétés algébriques, démontre un théorème de *G. H. Halphen*[497]) d'après lequel quand dans un espace à $r-1$ dimensions on se donne deux variétés algébriques de degrés μ et ν et de dimensions m et n, l'intersection de ces deux variétés est une variété de dimension $m+n-(r-1)$ et de degré $\mu\nu$, quand on a $m+n \geqq r-1$ et quand les deux variétés envisagées n'ont pas un système commun de dimension égale ou supérieure à $m+n-r+2$.*

495) *Gy. (J.) König,* Alg. Grössen [30]), p. 229.*
496) *Math. Ann. 11 (1877), p. 571.*
497) *Bull. Soc. math. France 2 (1873/4), p. 34.*

71. Forme canonique des systèmes d'équations algébriques.[498]) *E. Delassus*[499]) a appliqué aux systèmes d'équations algébriques homogènes une méthode calquée sur celle qu'il avait précédemment imaginée pour la réduction et l'étude des systèmes d'équations aux dérivées partielles.

Si l'on groupe les monomes $x_1^{\alpha_1}x_2^{\alpha_2}\ldots x_n^{\alpha_n}$ de degré m (c'est-à-dire pour lesquels $\alpha_1+\alpha_2+\cdots+\alpha_n=m$, où m est un nombre naturel donné) formés avec les variables $x_1, x_2, \ldots, x_n$, d'après les valeurs décroissantes de α_1 puis, dans chaque groupe, d'après les valeurs décroissantes de α_2 et ainsi de suite, on obtient un mode de rangement des monomes qui donne à l'expression „le $p^{\text{ième}}$ monome de degré m" un sens précis et qui, en outre, possède des propriétés spéciales sur lesquelles repose en grande partie la méthode dont il s'agit.

En y joignant la considération des *déduites* d'une équation $F(x_1, x_2, \ldots, x_n)=0$ [on entend par là les équations que l'on *déduit* de l'équation $F=0$ en multipliant ses deux membres successivement par les différentes variables; cette opération joue ici un rôle analogue à celui des dérivations dans le cas des équations aux dérivées partielles], puis enfin la considération d'une substitution linéaire de variables à coefficients uniquement assujettis à ne pas vérifier certaines conditions se traduisant par des égalités [cette substitution permet d'éviter des cas exceptionnels], on montre que tout système (S) d'équations algébriques entières et homogènes peut se remplacer par un système analogue et équivalent (Σ) satisfaisant aux conditions suivantes:

1) Les p équations qui composent (Σ) sont toutes d'un même degré m et sont résolues par rapport aux p premiers monomes de degré m.

2) Les équations de degré $m+1$ *déduites* des équations (Σ) sont alors résolues par rapport aux monomes de degré $m+1$ *déduits* des p monomes précédents de degré m. Certains de ces monomes peuvent être obtenus plusieurs fois, mais *les diverses expressions obtenues pour un même monome sont identiques.*

Cette forme *canonique* (Σ) permet d'étudier les solutions du système (S) et conduit au *résolvant total complet* [au sens de *Gy. (J.) König*]. Elle met en évidence deux nombres m et p et, par suite, les $n-1$ exposants de $x_1, x_2, \ldots, x_{n-1}$ dans le $p^{\text{ième}}$ monome

498) *Ce numéro est dû à *E. Delassus.**
499) *Ann. Ec. Norm. (3) 13 (1896), p. 421; (3) 14 (1897), p. 21; C. R. Acad. sc. Paris 122 (1896), p. 772; 123 (1896), p. 546, 1246/8.*

de degré m. Ces exposants sont précisément les degrés des différents facteurs $D_1, D_2, \ldots, D_{n-1}$ du résolvant total complet [au sens de *Gy. (J.) König*] du système canonique (Σ) pour $x_n = 1$.

E. Delassus[500]) a montré ensuite que cette *forme canonique* (Σ) du système (S) permet de former toutes les équations algébriques d'un degré donné μ qui sont les conséquences du système (S) et par suite de trouver, dans une variété à un nombre quelconque n de dimensions, l'équation générale des variétés algébriques de dimension $n-1$ de degré donné μ passant par l'intersection complète de plusieurs variétés algébriques données de dimension $n-1$ ou, plus généralement, contenant un système quelconque de variétés algébriques de dimensions quelconques données à l'avance.*

72. Décomposition en variétés irréductibles d'après Lasker[501]). *Soit

$$f_1(z_1, z_2, \ldots, z_n),\ f_2(z_1, z_2, \ldots, z_n),\ \ldots,\ f_m(z_1, z_2, \ldots, z_n)$$

un système quelconque donné de fonctions rationnelles entières homogènes des coordonnées homogènes $z_1, z_2, \ldots, z_n$. *E. Lasker*[502]) s'est proposé de décomposer en variétés de dimensions distinctes les ensembles de points-racines du système d'équations algébriques

$$f_1 = 0,\ f_2 = 0,\ \ldots,\ f_m = 0$$

en ne faisant intervenir les n variables que d'une façon symétrique. A cet effet il utilise, au lieu du résultant obtenu par élimination d'une seule variable comme l'avait fait *L. Kronecker,* le résultant plus général de n fonctions de n variables homogènes défini au n° **59**.

Soient

$$u_{rs} \qquad (r = 1, 2, \ldots, n-m;\ s = 1, 2, \ldots, n)$$

$n(n-m)$ indéterminées et posons, pour abréger, pour $r = 1, 2, \ldots, n-m$,

$$l_r = u_{r1} z_1 + u_{r2} z_2 + \cdots + u_{rn} z_n.$$

Supposons que les fonctions données $f_1, f_2, \ldots, f_m$ soient telles que le résultant ϱ des n fonctions homogènes $f_1, f_2, \ldots, f_m, l_1, l_2, \ldots, l_{n-m}$ ne soit pas nul identiquement; ce résultant ϱ est alors une fonction rationnelle entière homogène des indéterminées $u_{11}, \ldots, u_{n-m,m}$; décomposons-le en ses facteurs irréductibles $\varrho_1, \varrho_2, \ldots, \varrho_k$ et soit

$$\varrho = \varrho_1^{\alpha_1} \varrho_2^{\alpha_2} \ldots \varrho_k^{\alpha_k}.$$

500) *Bull. sc. math. (2) 21 (1897), p. 59.*

501) *Ce numéro (texte et notes) est dû à *J. Kürschák*.*

502) *Math. Ann. 60 (1905), p. 20.*

Désignons enfin par $(F_1^{(h)}, F_2^{(h)}, \ldots)$ l'ensemble (infini) formé par les fonctions rationnelles entières homogènes de $z_1, z_2, \ldots, z_n$ telles que, pour chacune d'entre elles $F_i^{(h)}$ $(i = 1, 2, \ldots)$, le résultant des n fonctions

$$f_1, f_2, \ldots, f_{m-1}, F_i^{(h)}, l_1, l_2, \ldots, l_{n-m}$$

soit divisible par le facteur ϱ_h de ϱ.

Si *tous* les points-racines du système d'équations algébriques

$$F_1^{(h)} = 0,\ F_2^{(h)} = 0, \ldots$$

vérifient une équation algébrique *réductible* quelconque

$$A(z_1, z_2, \ldots, z_n) B(z_1, z_2, \ldots, z_n) = 0,$$

il faut que ces points soient ou bien *tous* des points-racines de l'équation

$$A(z_1, z_2, \ldots, z_n) = 0$$

ou bien *tous* des points-racines de l'équation

$$B(z_1, z_2, \ldots, z_n) = 0;$$

c'est pourquoi l'on dit de l'ensemble des points-racines du système d'équations algébriques

$$F_1^{(h)} = 0,\ F_2^{(h)} = 0, \ldots$$

qu'il forme une *variété algébrique irréductible.* Cette variété algébrique irréductible *correspond* à l'équation $\varrho_h = 0$; elle est de dimension $n-m-1$.

Cette définition d'une variété irréductible ne diffère pas au fond de celles qui ont été données au n° **70**.

On dit aussi que la variété irréductible qui correspond à l'équation $\varrho_h = 0$ forme une *section irréductible* de l'ensemble des variétés défini par le système d'équations

$$f_1 = 0,\ f_2 = 0,\ \ldots,\ f_m = 0.$$

La variété irréductible qui correspond à $\varrho_h = 0$ n'a en général qu'un nombre fini de points-racines situés sur les $n-m-1$ variétés linéaires

$$\lambda_r = a_{r1} z_1 + a_{r2} z_2 + \cdots + a_{rn} z_n = 0 \qquad (r = 1, 2, \ldots, n-m-1)$$

à coefficients *déterminés*

$$a_{rs} \qquad (r = 1, 2, \ldots, n-m-1;\ s = 1, 2, \ldots, n).$$

Pour obtenir ces points-racines il suffit de remplacer dans la fonction ϱ_h les indéterminées u_{rs} $(r = 1, 2, \ldots, n-m-1;\ s = 1, 2, \ldots, n)$ par les coefficients déterminés a_{rs} ayant mêmes indices et de décomposer la fonction de $u_{n-m,1}, u_{n-m,2}, \ldots, u_{n-m,n}$ ainsi obtenue en ses facteurs irréductibles qui sont tous linéaires; à chacun de ces facteurs linéaires

$$c_1 u_{n-m,1} + c_2 u_{n-m,2} + \cdots + c_n u_{n-m,n}$$

correspond un point de coordonnées homogènes

$$z_1 = c_1,\ z_2 = c_2,\ \ldots,\ z_n = c_n$$

qui se trouve à la fois sur la variété algébrique irréductible correspondant à $\varrho_h = 0$ et sur chacune des $n - m - 1$ variétés linéaires

$$\lambda_1 = 0,\ \lambda_2 = 0,\ \ldots,\ \lambda_{n-m-1} = 0.$$

Ce n'est que quand ϱ_h s'annule identiquement en $u_{n-m,1}, u_{n-m,2}, \ldots, u_{n-m,n}$, après qu'on y a remplacé les u_{rs} ($r = 1, 2, \ldots, n-m-1$; $s = 1, 2, \ldots, n$) par les a_{rs} ayant mêmes indices, qu'il y a une *infinité* de *points-racines* communs à la variété algébrique irréductible correspondant à $\varrho_h = 0$ et aux $n - m - 1$ variétés linéaires $\lambda_1 = 0$, $\lambda_2 = 0, \ldots, \lambda_{n-m-1} = 0$.

Ceci posé, envisageons un système quelconque de fonctions rationnelles entières homogènes données

$$f_1(z_1, z_2, \ldots, z_n),\ f_2(z_1, z_2, \ldots, z_n),\ \ldots,\ f_j(z_1, z_2, \ldots, z_n)$$

où j peut être supérieur, égal ou inférieur à n. Si le système d'équations algébriques

$$f_1 = 0,\ f_2 = 0,\ \ldots,\ f_j = 0$$

a des points-racines, on peut grouper ces points-racines en variétés irréductibles de la façon suivante:

Décomposons f_1 en ses facteurs irréductibles; rangeons dans un premier groupe G_1 les variétés irréductibles obtenues en égalant à zéro ceux de ces facteurs qui divisent chacune des fonctions données $f_1, f_2, \ldots, f_j$; les variétés irréductibles obtenues en égalant à zéro les autres facteurs irréductibles de f_1 formeront un second groupe G'.

Soit $F = 0$ une quelconque des variétés du groupe G' et f_i une quelconque des fonctions données qui ne soit pas divisible par F; formons les variétés algébriques irréductibles *sections* du système d'équations

$$F = 0,\quad f_i = 0$$

[ici m étant égal à 2, ces sections seront de dimension $n - 3$]; répétons la même chose pour la fonction envisagée F et successivement pour chacune des fonctions données f_i non divisibles par F; répétons ensuite la même chose successivement pour toutes les variétés $F = 0$ du groupe G'. Enfin rangeons dans un groupe G_2 toutes celles des *sections* ainsi obtenues qui sont contenues dans chacune des variétés $f_2 = 0, f_3 = 0, \ldots, f_j = 0$; les autres formeront un groupe G''.

Maintenant reprenons le même procédé successivement pour toutes les variétés du groupe G'' et cherchons les sections de chacune de ces variétés du groupe G'' et de la variété $f_i = 0$, où f_i est successivement chacune des fonctions données qui égalées à zéro ne contiennent pas la variété envisagée du groupe G''. Les sections ainsi obtenues sont de dimension $n - 4$. Nous rangerons en un groupe G_3 celles qui sont contenues dans chacune des variétés $f_2 = 0, \ldots, f_j = 0$; les autres formeront un groupe G'''[503]).

En continuant ainsi, l'ensemble des groupes

$$G_1,\quad G_2,\quad G_3,\ \ldots$$

formera un groupe G qui comprendra précisément l'ensemble des

---

503) *Si, dans ce calcul, l'équation $\varrho_h = 0$ par ex. représente une variété irréductible du groupe G''', on peut déterminer les *sections* irréductibles de cette variété $\varrho_h = 0$ et de $f_i = 0$ de la manière suivante:

Soient

$$\begin{matrix} u_{11} & u_{12} & \ldots u_{1n} \\ u_{21} & u_{22} & \ldots u_{2n} \\ \cdot & \cdot & \cdot \\ u_{n-4,1} & u_{n-4,2} & \ldots u_{n-4,n} \\ u_{n-3,1} & u_{n-3,2} & \ldots u_{n-3,n} \end{matrix}$$

les indéterminées dont dépend ϱ_h. Envisageons ϱ_h comme une fonction de

$$u_{n-3,1},\ u_{n-3,2},\ \ldots,\ u_{n-3,n}$$

seulement, en faisant jouer aux autres indéterminées $u_{11}, \ldots, u_{n-4,n}$ le rôle de paramètres; la fonction ϱ_h peut alors être décomposée en facteurs linéaires de la forme

$$c_{g1} u_{n-3,1} + c_{g2} u_{n-3,2} + \cdots + c_{gn} u_{n-3,n} \qquad (g = 1, 2, \ldots).$$

Si l'on forme le produit

$$\prod_{(g)} f_i(c_{g1}, c_{g2}, \ldots, c_{gn})$$

étendu aux valeurs $g = 1, 2, \ldots$ qui correspondent à *tous* ces facteurs linéaires de ϱ_h on sait, d'après la théorie des fonctions symétriques de plusieurs séries de variables (n° 7), que ce produit peut être mis sous la forme d'une fonction rationnelle entière φ des indéterminées

$$\begin{matrix} u_{11}, & u_{12}, & \ldots, u_{1n} \\ u_{21}, & u_{22}, & \ldots, u_{2n} \\ \cdot & \cdot & \cdot \\ u_{n-4,1}, & u_{n-4,2}, & \ldots, u_{n-4,n}. \end{matrix}$$

Si cette fonction rationnelle entière φ des indéterminées $u_{11}, \ldots, u_{n-4,n}$ s'annule *identiquement par rapport à ces indéterminées*, la variété $\varrho_h = 0$ est contenue tout entière dans la variété $f_i = 0$. Si φ ne s'annule pas identiquement on peut décomposer cette fonction des indéterminées $u_{11}, \ldots, u_{n-4,n}$ en facteurs irréductibles; chacun de ces facteurs irréductibles égalé à zéro fournit alors une des sections cherchées de $\varrho_h = 0$ et de $f_i = 0$.*

points-racines du système donné

$$f_1 = 0,\ f_2 = 0,\ \ldots,\ f_j = 0$$

et ces points-racines seront distribués en variétés irréductibles.*

Les déterminants fonctionnels.

73. Propriétés du déterminant fonctionnel. Soient

$$f_1(z_1, z_2, \ldots, z_m),\ f_2(z_1, z_2, \ldots, z_m),\ \ldots,\ f_m(z_1, z_2, \ldots, z_m)$$

m fonctions des m variables $z_1, z_2, \ldots, z_m$. On appelle *déterminant fonctionnel* de ces m fonctions le déterminant [504]

$$\begin{vmatrix} \frac{\partial f_1}{\partial z_1} & \frac{\partial f_2}{\partial z_1} & \cdots & \frac{\partial f_m}{\partial z_1} \\ \frac{\partial f_1}{\partial z_2} & \frac{\partial f_2}{\partial z_2} & \cdots & \frac{\partial f_m}{\partial z_2} \\ \cdots & \cdots & \cdots & \cdots \\ \frac{\partial f_1}{\partial z_m} & \frac{\partial f_2}{\partial z_m} & \cdots & \frac{\partial f_m}{\partial z_m} \end{vmatrix};$$

on représente souvent, avec *W. F. Donkin* [505]), ce déterminant fonctionnel par la notation abrégée

$$\frac{\partial(f_1, f_2, \ldots, f_m)}{\partial(z_1, z_2, \ldots, z_m)}$$

ou encore, avec *P. Gordan* [506]), par le symbole $\binom{f_1, \ldots, f_m}{z_1, \ldots, z_m}$; *L. O. Hesse* écrit simplement $(f_1, f_2, \ldots, f_m)$, mais cela peut prêter à confusion.

A. Cayley [507]) a appelé *jacobien* le déterminant fonctionnel et ce nom lui est resté.

J. Bertrand [508]) donne du déterminant fonctionnel une autre définition: soient $f_1, \ldots, f_m$ des fonctions de $z_1, \ldots, z_m$; désignons par $d_1, d_2, \ldots, d_m$ des accroissements indépendants et envisageons l'expression R définie comme quotient de deux déterminants par l'égalité

$$\begin{vmatrix} d_1 z_1 & d_1 z_2 & \ldots & d_1 z_m \\ d_2 z_1 & d_2 z_2 & \ldots & d_2 z_m \\ \cdots & \cdots & \cdots & \cdots \\ d_m z_1 & d_m z_2 & \ldots & d_m z_m \end{vmatrix} \times R = \begin{vmatrix} d_1 f_1 & d_1 f_2 & \ldots & d_1 f_m \\ d_2 f_1 & d_2 f_2 & \ldots & d_2 f_m \\ \cdots & \cdots & \cdots & \cdots \\ d_m f_1 & d_m f_2 & \ldots & d_m f_m \end{vmatrix}.$$

504) *C. G. J. Jacobi,* J. reine angew. Math. 22 (1841), p. 319; Werke [99]) 3, p. 395; voir aussi Vorlesungen über Dynamik, réd. par *A. Clebsch,* Berlin 1866, p. 100.

505) Philos. Trans. London 144 (1854), p. 72.

506) Invar. [106]) 1, p. 121.

507) J. reine angew. Math. 52 (1856), p. 276; Papers 4, Cambr. 1891, p. 30.

508) J. math. pures appl. (1) 16 (1851), p. 212; C. R. Acad. sc. Paris 32 (1851), p. 134.

R s'appellera d'après *J Bertrand* le déterminant fonctionnel des m fonctions $f_1, f_2, \ldots, f_m$. Cette manière de définir le déterminant fonctionnel est critiquée par *G. Peano* [509]).

Voici, d'après *C. G. J. Jacobi* [510]), les principales propriétés du déterminant fonctionnel.

1. Si l'on envisage simultanément les m fonctions $f_1, f_2, \ldots, f_m$ de $z_1, z_2, \ldots, z_m$ et les m fonctions inverses $z_1, z_2, \ldots, z_m$ de $f_1, f_2, \ldots, f_m$, on a la relation fondamentale

$$(1) \qquad \frac{\partial(z_1, z_2, \ldots, z_m)}{\partial(f_1, f_2, \ldots, f_m)} = \frac{1}{\frac{\partial(f_1, f_2, \ldots, f_m)}{\partial(z_1, z_2, \ldots, z_m)}}.$$

2. Si l'on forme

$$\frac{\partial(z_1, z_2, \ldots, z_k)}{\partial(f_1, f_2, \ldots, f_k)},\quad \frac{\partial(f_{k+1}, \ldots, f_m)}{\partial(z_{k+1}, \ldots, z_m)}$$

en envisageant $z_1, z_2, \ldots, z_k, f_{k+1}, f_{k+2}, \ldots, f_m$ comme des fonctions de $f_1, f_2, \ldots, f_k, z_{k+1}, z_{k+2}, \ldots, z_m$, on a aussi pour $k = 1, 2, \ldots, m-1$, les relations

$$(2) \qquad \frac{\partial(f_1, f_2, \ldots, f_m)}{\partial(z_1, z_2, \ldots, z_m)} \cdot \frac{\partial(z_1, \ldots, z_k)}{\partial(f_1, \ldots, f_k)} = \frac{\partial(f_{k+1}, \ldots, f_m)}{\partial(z_{k+1}, \ldots, z_m)}.$$

3. Supposons que $f_1, f_2, \ldots, f_m$ soient fonctions de $\varphi_1, \varphi_2, \ldots, \varphi_p$, et que $\varphi_1, \varphi_2, \ldots, \varphi_p$ soient elles-mêmes fonctions de $z_1, z_2, \ldots, z_m$. Si alors $p < m$, on a toujours

$$(3^a) \qquad \frac{\partial(f_1, f_2, \ldots, f_m)}{\partial(z_1, z_2, \ldots, z_m)} = 0;$$

si $p = m$, on a

$$(3^b) \qquad \frac{\partial(f_1, f_2, \ldots, f_m)}{\partial(z_1, z_2, \ldots, z_m)} = \frac{\partial(f_1, f_2, \ldots, f_m)}{\partial(\varphi_1, \varphi_2, \ldots, \varphi_m)} \cdot \frac{\partial(\varphi_1, \varphi_2, \ldots, \varphi_m)}{\partial(z_1, z_2, \ldots, z_m)};$$

si enfin $p > m$, on a

$$(3^c) \qquad \frac{\partial(f_1, f_2, \ldots, f_m)}{\partial(z_1, z_2, \ldots, z_m)} = \sum \frac{\partial(f_1, f_2, \ldots, f_m)}{\partial(\varphi_{h_1}, \varphi_{h_2}, \ldots, \varphi_{h_m})} \cdot \frac{\partial(\varphi_{h_1}, \varphi_{h_2}, \ldots, \varphi_{h_m})}{\partial(z_1, z_2, \ldots, z_m)},$$

où la somme s'étend à toutes les combinaisons $h_1, h_2, \ldots, h_m$ des nombres $1, 2, \ldots, p$ pris m à m.

4. Si $f_1, f_2, \ldots, f_m$ sont données en fonctions de $z_1, z_2, \ldots, z_m$ au moyen des formules

509) Voir *A. Genocchi*, Calcolo differenziale, Turin 1884, p. XXVII des Annotazioni de *G. Peano.* *Voir aussi *G. Peano,* Giorn. mat. (1) 27 (1889), p. 226 (Note de *G. Vivanti*).*

510) J. reine angew. Math. 22 (1841), p. 319/59; Werke [99]) 3, p. 395/438.

$$\begin{aligned}F_1(f_1, f_2, \ldots, f_m;\quad z_1, z_2, \ldots, z_m) &= 0,\\ F_2(f_1, f_2, \ldots, f_m;\quad z_1, z_2, \ldots, z_m) &= 0,\\ \cdots\cdots\cdots\cdots\cdots\cdots&\\ F_m(f_1, f_2, \ldots, f_m;\quad z_1, z_2, \ldots, z_m) &= 0,\end{aligned}$$

on a

$$(4)\qquad \frac{\partial(f_1, f_2, \ldots, f_m)}{\partial(z_1, z_2, \ldots, z_m)} = (-1)^m \frac{\dfrac{\partial(F_1, F_2, \ldots, F_m)}{\partial(z_1, z_2, \ldots, z_m)}}{\dfrac{\partial(F_1, F_2, \ldots, F_m)}{\partial(f_1, f_2, \ldots, f_m)}}.$$

5. Supposons que les fonctions $f_1, f_2, \ldots, f_m$ de $z_1, z_2, \ldots, z_m$ soient données par $m + \mu$ équations $F_1 = 0$, $F_2 = 0, \ldots, F_{m+\mu} = 0$ entre $z_1, z_2, \ldots, z_m$, $f_1, f_2, \ldots, f_m$, $f_{m+1}, \ldots, f_{m+\mu}$. Le déterminant fonctionnel est alors donné par l'expression

$$(5)\qquad \frac{\partial(f_1, f_2, \ldots, f_m)}{\partial(z_1, z_2, \ldots, z_m)} = (-1)^m \frac{\dfrac{\partial(F_1, F_2, \ldots, F_m, F_{m+1}, \ldots, F_{m+\mu})}{\partial(z_1, z_2, \ldots, z_m, f_{m+1}, \ldots, f_{m+\mu})}}{\dfrac{\partial(F_1, F_2, \ldots, F_m, F_{m+1}, \ldots, F_{m+\mu})}{\partial(f_1, f_2, \ldots, f_m, f_{m+1}, \ldots, f_{m+\mu})}}.$$

6. Soient $f, f_1, f_2, \ldots, f_m, f_{m+1}, \ldots, f_{m+\mu}$ des fonctions de $z, z_1, z_2, \ldots, z_m, z_{m+1}, \ldots, z_{m+\mu}$. Posons, pour $i, k = 0, 1, 2, \ldots, \mu$,

$$\frac{\partial(f, f_1, f_2, \ldots, f_{m-1}, f_{m+i})}{\partial(z, z_1, z_2, \ldots, z_{m-1}, z_{m+k})} = b_{i,k}$$

puis

$$B = \frac{\partial(f, f_1, \ldots, f_{m-1})}{\partial(z, z_1, \ldots, z_{m-1})};$$

on aura alors

$$(6)\qquad \begin{vmatrix} b_{00}, & b_{01}, & \ldots, & b_{0\mu}\\ b_{10}, & b_{11}, & \ldots, & b_{1\mu}\\ \cdot & \cdot & \cdot & \cdot\\ b_{\mu 0}, & b_{\mu 1}, & \ldots, & b_{\mu\mu}\end{vmatrix} = \frac{\partial(f, f_1, f_2, \ldots, f_{m+\mu})}{\partial(z, z_1, z_2, \ldots, z_{m+\mu})} B^{\mu}.$$

Si l'on suppose $m = 1$, on a en particulier

$$b_{ik} = \frac{\partial(f, f_{i+1})}{\partial(z, z_{k+1})}, \quad B = \frac{\partial f}{\partial z}$$

et par conséquent

$$(6\mathrm{a})\qquad \begin{vmatrix} b_{00}, & b_{01}, & \ldots, & b_{0\mu}\\ b_{10}, & b_{11}, & \ldots, & b_{1\mu}\\ \cdot & \cdot & \cdot & \cdot\\ b_{\mu 0}, & b_{\mu 1}, & \ldots, & b_{\mu\mu}\end{vmatrix} = \frac{\partial(f, f_1, \ldots, f_{\mu+1})}{\partial(z, z_1, \ldots, z_{\mu+1})} B^{\mu}.$$

7. Supposons que z soit une fonction de $z_1, z_2, \ldots, z_m$, déterminée par l'équation

$$f(z, z_1, z_2, \ldots, z_m) = 0.$$

Posons

$$\frac{\partial(f, f_1, \ldots, f_m)}{\partial(z, z_1, \ldots, z_m)} = A\frac{\partial f}{\partial z} + A_1\frac{\partial f}{\partial z_1} + \cdots + A_m\frac{\partial f}{\partial z_m}$$

où

$$A = \frac{\partial(f_1, f_2, \ldots, f_m)}{\partial(z_1, z_2, \ldots, z_m)}$$

et où, pour chaque indice k, A_k se déduit de A en y substituant aux dérivées partielles par rapport à z_k les dérivées partielles par rapport à z et en changeant le signe du résultat.

Désignons aussi, pour chaque indice h, par (f_h) ce que devient la fonction f_h quand on y remplace z en fonction de $z_1, z_2, \ldots, z_m$. On a alors

$$(7)\qquad \frac{\partial((f_1), (f_2), \ldots, (f_m))}{\partial(z_1, z_2, \ldots, z_m)} = A - A_1\frac{\partial z}{\partial z_1} - A_2\frac{\partial z}{\partial z_2} - \cdots - A_m\frac{\partial z}{\partial z_m}.$$

D'après *C. G. J. Jacobi*[511]) cette formule est due à *J. L. Lagrange*.

8. Supposons que les inconnues $z, z_1, z_2, \ldots, z_m$ soient liées par un système d'équations

$$f = \alpha,\quad f_1 = \alpha_1,\quad f_2 = \alpha_2,\quad \ldots,\quad f_m = \alpha_m$$

où $\alpha, \alpha_1, \alpha_2, \ldots, \alpha_m$ désignent des constantes. De la première de ces équations tirons z pour porter cette valeur de z dans $f_1, f_2, \ldots, f_m$; puis de la deuxième tirons z_1 pour porter cette valeur de z_1 dans $f_2, \ldots, f_m$; et ainsi de suite. Alors f_m ne contiendra que z_m et les constantes $\alpha, \alpha_1, \ldots, \alpha_{m-1}$; f_{m-1} ne contiendra que z_{m-1}, z_m et les constantes $\alpha, \alpha_1, \ldots, \alpha_{m-2}$; en général f_i contiendra $z_i, z_{i+1}, \ldots, z_m$, et les constantes $\alpha, \alpha_1, \alpha_2, \ldots, \alpha_{i-1}$. On a alors la formule remarquable

$$(8)\qquad \frac{\partial(f, f_1, \ldots, f_m)}{\partial(z, z_1, \ldots, z_m)} = \left(\frac{\partial f}{\partial z}\right)\left(\frac{\partial f_1}{\partial z_1}\right)\cdots\left(\frac{\partial f_m}{\partial z_m}\right).$$

Dans le premier membre de cette formule, $f, f_1, f_2, \ldots, f_m$ sont fonctions de $z, z_1, z_2, \ldots, z_m$ tandis que dans le second membre (et c'est pour l'indiquer qu'on a mis les dérivées partielles entre parenthèses) f_i est une fonction de $z_i, z_{i+1}, \ldots, z_m$ contenant comme paramètres $\alpha, \alpha_1, \alpha_2, \ldots, \alpha_{i-1}$.

9. Si $u, u_1, u_2, \ldots, u_m$ désignent des fonctions quelconques de $z_1, z_2, \ldots, z_m$, et si l'on pose

$$\frac{u_1}{u} = v_1,\quad \frac{u_2}{u} = v_2,\quad \ldots,\quad \frac{u_m}{u} = v_m,$$

---

511) *C. G. J. Jacobi*, J. reine angew. Math. 22 (1841), p. 353; Werke[99]) 3, p 431 (n° 17).

le déterminant fonctionnel des fonctions $v_1, v_2, \ldots, v_m$ de $z_1, z_2, \ldots, z_m$ s'exprime par la relation

$$(9)\qquad \frac{\partial(v_1, v_2, \ldots, v_m)}{\partial(z_1, z_2, \ldots, z_m)} = \frac{1}{u^{m+1}} \begin{vmatrix} u & \frac{\partial u}{\partial z_1} & \cdots & \frac{\partial u}{\partial z_m} \\ u_1 & \frac{\partial u_1}{\partial z_1} & \cdots & \frac{\partial u_1}{\partial z_m} \\ \cdots & \cdots & \cdots & \cdots \\ u_m & \frac{\partial u_m}{\partial z_1} & \cdots & \frac{\partial u_m}{\partial z_m} \end{vmatrix}.$$

Si aux fonctions $u, u_1, u_2, \ldots, u_m$ on substitue leurs produits ut, $u_1 t$, $u_2 t, \ldots, u_m t$ par une fonction quelconque t, cette formule montre que le déterminant

$$\begin{vmatrix} u & \frac{\partial u}{\partial z_1} & \cdots & \frac{\partial u}{\partial z_m} \\ u_1 & \frac{\partial u_1}{\partial z_1} & \cdots & \frac{\partial u_1}{\partial z_m} \\ \cdots & \cdots & \cdots & \cdots \\ u_m & \frac{\partial u_m}{\partial z_1} & \cdots & \frac{\partial u_m}{\partial z_m} \end{vmatrix}$$

qui figure dans son second membre est simplement multiplié par t^{m+1}, comme si t était une constante.

74. Déterminants fonctionnels de fonctions rationnelles entières homogènes. Si $\varphi_1, \ldots, \varphi_m$ désignent des fonctions rationnelles entières *homogènes* des variables $z_1, \ldots, z_m$, le produit de chacune des variables z_i par le déterminant fonctionnel

$$\frac{\partial(\varphi_1, \varphi_2, \ldots, \varphi_m)}{\partial(z_1, z_2, \ldots, z_m)}$$

s'exprime par des fonctions linéaires et homogènes de $\varphi_1, \varphi_2, \ldots, \varphi_m$ dont les coefficients sont des fonctions rationnelles entières de $z_1, \ldots, z_m$.

Par conséquent le déterminant fonctionnel

$$\frac{\partial(\varphi_1, \varphi_2, \ldots, \varphi_m)}{\partial(z_1, z_2, \ldots, z_m)}$$

s'annule pour chaque racine autre que la racine $(0, 0, \ldots, 0)$ du système d'équations

$$\varphi_1 = 0, \quad \varphi_2 = 0, \quad \ldots, \quad \varphi_m = 0.$$

Si les fonctions $\varphi_1, \varphi_2, \ldots, \varphi_m$ sont de même degré, les dérivées du déterminant fonctionnel

$$\frac{\partial(\varphi_1, \varphi_2, \ldots, \varphi_m)}{\partial(z_1, z_2, \ldots, z_m)}$$

prises par rapport à chacune des variables $z_1, z_2, \ldots, z_m$ s'annulent aussi pour chaque racine du système d'équations

$$\varphi_1 = 0, \ \varphi_2 = 0, \ \ldots, \ \varphi_m = 0$$[512]).

Considérons $(m+1)$ équations homogènes

$$\varphi_1 = 0, \quad \varphi_2 = 0, \quad \ldots, \quad \varphi_{m+1} = 0$$

entre les m variables $z_1, z_2, \ldots, z_m$; avec les m fonctions qu'on obtient en supprimant successivement $\varphi_1, \varphi_2, \ldots, \varphi_{m+1}$, formons les $m+1$ déterminants fonctionnels $R_1, R_2, \ldots, R_{m+1}$. Prenons m d'entre eux, par exemple ceux qu'on obtient en supprimant R_α, et soit S_α le déterminant fonctionnel de ces m déterminants fonctionnels: on a alors pour le quotient $\frac{S_\alpha}{\varphi_\alpha}$ une expression qui ne dépend pas de α. *A. Clebsch* a établi ce théorème [513]); puis il a donné d'après les indications de *P. Gordan* un moyen de trouver l'expression M des $m+1$ quotients [514])

$$M = \frac{S_1}{\varphi_1} = \frac{S_2}{\varphi_2} = \cdots = \frac{S_{m+1}}{\varphi_{m+1}}.$$

75. Fonctions dépendantes. Fonctions indépendantes. Soient

$$f_1(z_1, z_2, \ldots, z_m), \quad f_2(z_1, z_2, \ldots, z_m), \quad \ldots, \quad f_q(z_1, z_2, \ldots, z_m)$$

q fonctions rationnelles et entières des m variables $z_1, z_2, \ldots, z_m$. Lorsqu'il existe entre $f_1, f_2, \ldots, f_q$ au moins une relation de la forme

$$F(f_1, f_2, \ldots, f_q) = 0,$$

[où F désigne une fonction rationnelle et entière dont les coefficients sont indépendants des variables $z_1, z_2, \ldots, z_m$] et que cette relation n'est pas une identité en $f_1, f_2, \ldots, f_q$, c'est-à-dire n'est pas vérifiée quelles que soient les valeurs que l'on donne à $f_1, f_2, \ldots, f_q$, on dit, d'après *C. G. J. Jacobi* [515]), que ces fonctions sont *dépendantes* [algébriquement] les unes des autres. S'il n'existe *aucune* relation de cette forme on dit que ces fonctions sont [algébriquement] *indépendantes.*

Il résulte de cette définition que, si q est plus grand que m, les fonctions envisagées $f_1, f_2, \ldots, f_q$ ne sont jamais indépendantes. Si au contraire $q \leqq m$, il peut arriver que ces fonctions soient indépendantes mais il peut aussi arriver qu'elles soient dépendantes. Pour voir si elles sont indépendantes, ou non, on peut envisager

512) Cf. *L. O. Hesse*, J. reine angew. Math. 28 (1844) p. 68; Werke [250]), p. 89.

513) J. reine angew. Math. 69 (1868), p. 355.

514) J. reine angew. Math. 70 (1869), p. 175. Consulter l'exposé de la théorie du déterminant fonctionnel dû à *P. Gordan*, Invar. [106]) 1, p. 120.

515) J. reine angew. Math. 22 (1841), p. 319; Werke [99]) 3, p. 395.

le système d'équations

$$f_1(z_1, z_2, \dots, z_m) = \varphi_1, \quad f_2(z_1, z_2, \dots, z_m) = \varphi_2, \quad \dots, \quad f_q(z_1, z_2, \dots, z_m) = \varphi_q,$$

où $\varphi_1, \varphi_2, \dots, \varphi_q$ désignent des indéterminées, puis former les résultants du système constitué par les équations

$$f_\alpha(z_1, \dots, z_m) - \varphi_\alpha = 0 \qquad (\alpha = 1, 2, \dots q)$$

en éliminant successivement de toutes les manières possibles $q-1$ des m variables $z_1, z_2, \dots, z_m$. Si l'un de ces résultants est indépendant des $m-q+1$ variables z non éliminées, les fonctions f_α ne sont pas indépendantes. Elles sont indépendantes dans le cas contraire [516].

Comme l'a démontré *C. G. J. Jacobi* [515]) dans le cas où $m = q$, la condition nécessaire et suffisante pour que les m fonctions $f_\alpha(z_1, z_2, \dots, z_m)$ ne soient pas indépendantes est que le déterminant fonctionnel $\frac{\partial(f_1, f_2, \dots, f_m)}{\partial(z_1, z_2, \dots, z_m)}$ s'évanouisse identiquement.

La distinction précédente entre fonctions dépendantes et indépendantes s'étend d'ailleurs à des fonctions analytiques quelconques $f_1, f_2, \dots, f_q$ et le théorème de *C. G. J. Jacobi* s'applique encore, dans ce cas plus général que celui que nous envisageons ici, en prenant pour F une fonction analytique quelconque de $f_1, f_2, \dots, f_q$.

Si l'on considère q fonctions rationnelles entières $f_1, f_2, \dots, f_q$ de $m = q + \mu$ variables et si ces q fonctions ne sont pas indépendantes, les déterminants fonctionnels que l'on peut former en prenant les variables q à q sont tous nuls, et réciproquement si ces C_m^q déterminants sont nuls les fonctions ne sont pas indépendantes. On aura alors nécessairement entre ces q fonctions une relation de la forme

$$F(f_1, f_2, \dots, f_q) = 0$$

où F désigne une fonction rationnelle entière de $f_1, f_2, \dots, f_q$ à coefficients indépendants des m variables. *Gy. (J.) König* [517]) a donné une démonstration purement algébrique de ce théorème et il a montré comment on obtient effectivement, dans le cas où les C_m^q déterminants sont nuls, une relation de la forme $F(f_1, f_2, \dots, f_q) = 0$.

D'après *C. G. J. Jacobi* [518]) les équations

$$f_1 = 0, \quad f_2 = 0, \quad \dots, \quad f_q = 0$$

sont dites *indépendantes* si (supposant $m \geqq q$) il est possible de tirer de ces équations q des variables en fonction des $m-q$ autres variables.

516) Cf. *E. Netto,* Alg. [27]) 2, p. 135.
517) Alg. Grössen [20]), p. 247.
518) J. reine angew. Math. 22 (1841), p. 321; Werke [99]) 3, p. 397.

E. Netto [519]) fait observer qu'il peut être utile de préciser cette définition de *C. G. J. Jacobi* en lui substituant celle que voici: On dit que l'équation $f_q(z_1, z_2, \dots, z_m) = 0$ *dépend* du système des équations

$$f_1(z_1, z_2, \dots, z_m) = 0, \quad f_2(z_1, z_2, \dots, z_m) = 0, \quad \dots, \quad f_{q-1}(z_1, z_2, \dots, z_m) = 0,$$

ou encore *est une conséquence* de ce système, lorsque toute solution de ce système

$$f_1(z_1, z_2, \dots, z_m) = 0, \quad f_2(z_1, z_2, \dots, z_m) = 0, \quad \dots, \quad f_{q-1}(z_1, z_2, \dots, z_m) = 0$$

satisfait aussi à l'équation $f_q(z_1, z_2, \dots, z_m) = 0$; dans tout autre cas on dit que l'équation $f_q(z_1, z_2, \dots, z_m) = 0$ ne dépend pas du système d'équations

$$f_1(z_1, z_2, \dots, z_m) = 0, \quad f_2(z_1, z_2, \dots, z_m) = 0, \quad \dots, f_{q-1}(z_1, z_2, \dots, z_m) = 0.$$

76. Le hessien. Soit $f(z_1, z_2, \dots, z_m)$ une fonction homogène de $z_1, z_2, \dots, z_m$. Le *jacobien* des m fonctions

$$\frac{\partial f}{\partial z_1}, \quad \frac{\partial f}{\partial z_2}, \quad \dots, \quad \frac{\partial f}{\partial z_m}$$

s'appelle le *hessien* de la fonction f; ce nom lui a été donné par *A. Cayley* et par *J. J. Sylvester* [520]).

Si l'on désigne par

$$H = H(z_1, z_2, \dots, z_m)$$

le hessien d'une fonction homogène $f(z_1, z_2, \dots, z_m)$ on a donc

$$H = \begin{vmatrix} \frac{\partial^2 f}{\partial z_1^2} & \frac{\partial^2 f}{\partial z_1 \partial z_2} & \dots & \frac{\partial^2 f}{\partial z_1 \partial z_m} \\ \frac{\partial^2 f}{\partial z_1 \partial z_2} & \frac{\partial^2 f}{\partial z_2^2} & \dots & \frac{\partial^2 f}{\partial z_2 \partial z_m} \\ \dots & \dots & \dots & \dots \\ \frac{\partial^2 f}{\partial z_1 \partial z_m} & \frac{\partial^2 f}{\partial z_2 \partial z_m} & \dots & \frac{\partial^2 f}{\partial z_m^2} \end{vmatrix}.$$

Si l'on fait sur une fonction rationnelle entière homogène $f(z_1, z_2, \dots, z_m)$ une substitution linéaire,

$$z_\alpha = a_{\alpha 1} y_1 + \dots + a_{\alpha m} y_m \quad (\alpha = 1, 2, \dots, m),$$

où $a_{11}, a_{12}, \dots, a_{mm}$ sont des constantes telles que le déterminant de la substitution soit différent de zéro, elle se transforme en une fonc-

519) Alg. [27]) 2, p. 143.
520) *A. Cayley,* Philos. Trans. London 146 (1856), p. 636; Papers 2, Cambridge 1889, p. 319; *J. J. Sylvester,* Cambr. Dublin math. J. 6 (1851), p. 194; Papers 1, Cambr. 1905, p. 193; voir d'ailleurs *L. O. Hesse,* J. reine angew. Math. 28 (1844), p. 68; Werke [230]), p. 89.

tion $F(y_1, y_2, \ldots, y_m)$ qui dépend en général des m variables $y_1, y_2, \ldots, y_m$. Si l'on peut choisir cette substitution linéaire de façon que la fonction transformée F soit indépendante d'une au moins des m variables $y_1, y_2, \ldots, y_m$, le hessien H de la fonction $f(z_1, z_2, \ldots, z_m)$ est identiquement nul.

A deux reprises différentes *L. O. Hesse*[521]) a cherché à démontrer la réciproque de ce théorème. *M. Pasch*[522]) a démontré l'exactitude de cette réciproque pour les formes cubiques ternaires et quaternaires. *P. Gordan*[523]) l'a établie pour les formes ternaires, *M. Nöther* et *P. Gordan*[524]) pour les formes quaternaires. Enfin *P. Gordan* et *M. Nöther*[525]) ont établi que cette réciproque n'est pas exacte pour plus de quatre variables.

Si $(\zeta_1, \zeta_2, \ldots, \zeta_m)$ est une racine d'ordre de multiplicité k de l'équation algébrique homogène $f(z_1, z_2, \ldots, z_m) = 0$ supposée de degré supérieur à 2, cette racine $(\zeta_1, \zeta_2, \ldots, \zeta_m)$ sera nécessairement une racine d'ordre de multiplicité $k + (m-1)(k-2)$ de l'équation

$$H(z_1, z_2, \ldots, z_m) = 0$$

formée en égalant à zéro le hessien H de la fonction $f(z_1, z_2, \ldots, z_m)$.

Dans la variété à $m-1$ dimensions constituée par les rapports des variables $z_1, z_2, \ldots, z_m$, les *tangentes* à la variété[526])

$$f(z_1, z_2, \ldots, z_m) = 0$$

au point multiple $(\zeta_1, \zeta_2, \ldots, \zeta_m)$, d'ordre de multiplicité k, sont aussi, en ce même point $(\zeta_1, \zeta_2, \ldots, \zeta_m)$, tangentes à la variété

$$H(z_1, z_2, \ldots, z_m) = 0.$$

Pour $m = 3$, le nombre de ces tangentes communes aux courbes

$$f(z_1, z_2, z_3) = 0, \qquad H(z_1, z_2, z_3) = 0$$

au point $(\zeta_1, \zeta_2, \zeta_3)$ est fini et égal à k; en prenant $k = 2$ on voit ainsi que tout point double de la courbe $f(z_1, z_2, z_3) = 0$ compte pour

521) J. reine angew. Math. 42 (1851), p. 117; 56 (1859), p. 263; Werke[230]), p. 288, 481.

522) J. reine angew. Math. 80 (1875), p. 169.

523) Sitzgsb. phys.-medic. Soc. Erlangen 8 (1875/6), p. 89.

524) id. 8 (1875/6), p. 51.

525) Math. Ann. 10 (1876), p. 547. Cf. *N. L. W. A. Gravelaar*, Nieuw Archief voor Wiskunde (1) 3 (1877), p. 193; *E. C. Valentiner*, Tidsskrift math. Köbenhavn (Copenhague) (5) 6 (1888), p. 49.

526) Cf. *A. Voss*, Math. Ann. 27 (1886), p. 526. Voir aussi le tome III de l'Encyclopédie.

six points parmi les points communs aux deux courbes[527])

$$f(z_1, z_2, z_3) = 0, \ H(z_1, z_2, z_3) = 0.$$

Pour $m > 3$, les tangentes communes aux deux variétés

$$f(z_1, z_2, \ldots, z_m) = 0, \ H(z_1, z_2, \ldots, z_m) = 0$$

au point $(\zeta_1, \zeta_2, \ldots, \zeta_m)$ forment un cône (ou un hypercône) d'ordre égal à k.

La condition nécessaire et suffisante pour qu'un *point simple* de la courbe

$$f(z_1, z_2, z_3) = 0$$

soit aussi situé sur la courbe

$$H(z_1, z_2, z_3) = 0$$

est que la courbe $f(z_1, z_2, z_3) = 0$ ait en ce point simple une tangente d'inflexion. De même la condition nécessaire et suffisante pour qu'un *point simple* de la variété

$$f(z_1, z_2, \ldots, z_m) = 0 \qquad \text{où } m \geqq 4$$

soit situé sur la variété

$$H(z_1, z_2, \ldots, z_m) = 0$$

est que la variété $f(z_1, z_2, \ldots, z_m) = 0$ ait en ce point simple une variété linéaire tangente à $m-2$ dimensions [un plan pour $m = 4$, un hyperplan pour $m > 4$] qui soit *stationnaire* c'est-à-dire qui soit aussi tangente à la variété $f(z_1, z_2, \ldots, z_m) = 0$ en un certain point

$$z_1 + dz_1, \ z_2 + dz_2, \ \ldots, \ z_m + dz_m$$

infiniment voisin du point $(z_1, z_2, \ldots, z_m)$.

77. Formule de Jacobi. Généralisation de Liouville. Soient

$$f_1(z_1, z_2, \ldots, z_m), \quad f_2(z_1, z_2, \ldots, z_m), \quad \ldots, \quad f_m(z_1, z_2, \ldots, z_m)$$

m fonctions rationnelles entières (non homogènes) à coefficients indéterminés, de degrés respectifs

$$n_1, n_2, \ldots, n_m.$$

Comme l'ont déjà fait observer *L. Euler*[528]) et *G. Cramer*[529]), les

527) Voir à ce sujet *L. O. Hesse*, J. reine angew. Math. 28 (1844), p. 68, 97; 38 (1849), p. 257; 40 (1850), p. 316; 41 (1851), p. 272; Werke[230]) p. 89, 123, 211, 257, 263; *A. Clebsch*, J. reine angew. Math. 58 (1860), p. 229; *A. Cayley*, id. 34 (1847) p. 30; Papers 1, Cambridge 1889, p. 337; *A. Clebsch*, Geom.[397]) 1, p. 176, 312, 318, 381; 325, 326, 327, 356, 360, 377 etc.; trad. *Ad. Benoist* 1, Paris 1879, p 219; 2, Paris 1880, p. 11, 18, 102; 27, 29, 30, 72, 77, 97 etc.

528) Hist. Acad. Berlin 4 (1748), éd. 1750, p. 219.

529) Introd.[31]), p. 78.

racines du système formé par les m équations

$$f_1 = 0, \quad f_2 = 0, \quad \ldots, \quad f_m = 0$$

ou, si l'on veut, les points communs aux m variétés $f_1 = 0, f_2 = 0, \ldots, f_m = 0$, ne peuvent pas être arbitrairement choisis.

Supposons que les m équations $f_1 = 0, f_2 = 0, \ldots, f_m = 0$ n'aient que des racines *finies* et *distinctes*, en sorte que le nombre k de ces racines soit égal au produit $k = n_1 n_2 \ldots n_m$. Soit alors $g(z_1, z_2, \ldots, z_m)$ une fonction rationnelle, entière, quelconque de degré

$$\mu < n_1 + n_2 + \cdots + n_m - m.$$

Si alors

$$J(z_1, z_2, \ldots, z_m) = \frac{\partial(f_1, f_2, \ldots, f_m)}{\partial(z_1, z_2, \ldots, z_m)}$$

et si

$$(\zeta_{11}, \zeta_{21}, \ldots, \zeta_{m1}), \quad (\zeta_{12}, \zeta_{22}, \ldots, \zeta_{m2}), \quad \ldots, \quad (\zeta_{1k}, \zeta_{2k}, \ldots, \zeta_{mk})$$

désignent les k racines finies des équations

$$f_1 = 0, \quad f_2 = 0, \quad \ldots, \quad f_m = 0,$$

on a la formule

$$\sum_{h=1}^{h=k} \frac{g(\zeta_{1h}, \zeta_{2h}, \ldots, \zeta_{mh})}{J(\zeta_{1h}, \zeta_{2h}, \ldots, \zeta_{mh})} = 0$$

qui, pour $m = 1$, se réduit à la *formule d'Euler* (nº **23**). Cette formule a été trouvée dans le cas où $m = 2$ par *C. G. J. Jacobi*[530]); elle a été ensuite étendue sans difficulté au cas général par *E. Betti*[531]) et *A. Clebsch*[532]).

Dans le cas où $m = 2$ et où les degrés n_1 et n_2 des deux courbes algébriques

$$f_1(z_1, z_2) = 0, \quad f_2(z_1, z_2) = 0$$

sont tous deux égaux au même nombre n, *C. G. J. Jacobi*[530]) déduit de cette relation appliquée à la fonction rationnelle entière

$$g(z_1, z_2) = z_1^{\alpha_1} z_2^{\alpha_2},$$

où α_1, α_2 sont des nombres naturels donnés, les relations qui existent entre les coordonnées des n^2 points d'intersection des deux courbes $f_1 = 0$, $f_2 = 0$; *C. G. J. Jacobi* a aussi étudié de plus près les relations qui existent entre les coordonnées des points d'intersection de

530) J. reine angew. Math. 14 (1835), p. 281; 15 (1836), p 285; Werke[31]) 3, p. 287, 331; voir aussi p. 610 pour ce qui concerne le cas où le nombre des racines finies (égales ou inégales) $k < n_1 n_2 \ldots n_m$, cas auquel la *formule de Jacobi* peut être en défaut; cf. *E. Netto*, Alg.[27]) 2, p. 168.

531) Ann. mat. pura appl. (1) 1 (1858), p. 1.

532) J. reine angew. Math. 63 (1864), p. 189.

trois surfaces algébriques

$$f_1(z_1, z_2, z_3) = 0, \quad f_2(z_1, z_2, z_3) = 0, \quad f_3(z_1, z_2, z_3) = 0.$$

J. Plücker[533]) s'est ensuite occupé de la même question qui a d'ailleurs fait l'objet de nombreux travaux[534]).

W. End[535]) envisage trois surfaces algébriques

$$f_1(z_1, z_2, z_3) = 0, \quad f_2(z_1, z_2, z_3) = 0, \quad f_3(z_1, z_2, z_3) = 0$$

qui se coupent suivant une même courbe gauche (C) n'ayant ni point double ni point de rebroussement et qui ont de plus μ points isolés $P_1, P_2, \ldots, P_\mu$ en commun. Convenons de ranger ces trois surfaces dans un ordre tel que, si n_1, n_2, n_3 sont les degrés des fonctions rationnelles entières

$$f_1(z_1, z_2, z_3), \; f_2(z_1, z_2, z_3), \; f_3(z_1, z_2, z_3),$$

on ait

$$n_1 \geqq n_2 \geqq n_3.$$

Par la courbe (C) faisons passer une surface algébrique quelconque

$$\varphi(z_1, z_2, z_3) = 0$$

telle toutefois que, si n est le degré de la fonction rationnelle entière $\varphi(z_1, z_2, z_3)$, on ait

$$n + \mu \geqq n_2 + n_3 - 3.$$

Désignons enfin par

$$r(z_1) = 0$$

l'équation de degré μ dont les racines fournissent la première coordonnée de chacun des μ points isolés $P_1, P_2, \ldots, P_\mu$. On peut alors mettre le produit $r(z_1) \cdot \varphi(z_1, z_2, z_3)$ sous la forme

$$r \cdot \varphi = A_1 f_1 + A_2 f_2 + A_3 f_3,$$

où A_1, A_2, A_3 désignent des fonctions rationnelles entières de z_1, z_2, z_3.

Ceci posé, soit $g(z_1, z_2, z_3) = 0$ une surface algébrique passant deux fois par (C) et dont le degré soit égal à $n_1 + n_2 + n_3 - 4$. Si, en prenant pour $\varphi(z_1, z_2, z_3)$ une fonction de degré le moins élevé possible, on peut mettre g sous la forme

$$g = \sum_{(i)} [(A_1^{(i)} f_1 + A_2^{(i)} f_2 + A_3^{(i)} f_3 + A_4^{(i)} \varphi)\,(B_1^{(i)} f_1 + B_2^{(i)} f_2 + B_3^{(i)} f_3 + B_4^{(i)} \varphi)],$$

où les coefficients $A_1^{(i)}, A_2^{(i)}, A_3^{(i)}, A_4^{(i)}, B_1^{(i)}, B_2^{(i)}, B_3^{(i)}, B_4^{(i)}$ désignent

533) J. reine angew. Math. 16 (1837), p. 47 [1836]; Wiss. Abh. 1, Leipzig 1895, p. 323.

534) Pour renseignements bibliographiques, voir *A. Brill* et *M. Nöther*, Jahresb. deutsch. Math.-Ver. 3 (1892/3), éd. 1894, p. 347.

535) Diss. Tubingue 1887; Math. Ann. 35 (1890), p. 82.

des fonctions rationnelles entières de z_1, z_2, z_3, on a la relation

$$\sum_{h=1}^{h=\mu} \frac{g(\zeta_{1h}, \zeta_{2h}, \zeta_{3h})}{J(\zeta_{1h}, \zeta_{2h}, \zeta_{3h})} = 0,$$

où $J(z_1, z_2, z_3)$ est le déterminant fonctionnel des trois fonctions $f_1(z_1, z_2, z_3)$, $f_2(z_1, z_2, z_3)$, $f_3(z_1, z_2, z_3)$ et où la somme est étendue aux μ points-racines *discrets* $(\zeta_{11}, \zeta_{21}, \zeta_{31})$, $(\zeta_{12}, \zeta_{22}, \zeta_{32})$, $\ldots$, $(\zeta_{1\mu}, \zeta_{2\mu}, \zeta_{3\mu})$ communs aux trois surfaces

$$f_1(z_1, z_2, z_3) = 0,\ f_2(z_1, z_2, z_3) = 0,\ f_3(z_1, z_2, z_3) = 0.$$

E. Betti[531]) a déduit la *formule de Jacobi* de la théorie des fonctions symétriques de plusieurs variables; *L. Kronecker*[536]) l'obtient en généralisant, d'une façon distincte de celle qui a été indiquée au n° **40**, la *formule d'interpolation de Lagrange.* Dans cette nouvelle généralisation les $(\zeta_{1h}, \zeta_{2h}, \ldots, \zeta_{mh})$ au lieu d'être, comme dans celle du n° **40**, des systèmes *donnés* sont définis comme racines des systèmes d'équations données[537]).

L. Kronecker insiste sur ce que cette *formule de Jacobi* suppose essentiellement soit que les coefficients de $f_1, f_2, \ldots, f_m$ sont indéterminés, soit que pour des coefficients déterminés le nombre des racines finies et distinctes du système $(f_1 = 0,\ f_2 = 0,\ \ldots,\ f_m = 0)$ est précisément égal à $n_1 n_2 \cdots n_m$.

J. Liouville[538]) a démontré une formule qui semble tout d'abord plus générale que la *formule de Jacobi* mais qu'on peut en réalité déduire aisément de cette dernière comme l'a montré *L. Kronecker*[539]). Les développements de *J. Liouville* fournissent donc finalement une nouvelle démonstration de la *formule de Jacobi.* Voici le résultat auquel est parvenu *J. Liouville*:

Soient

$$f_1(z_1, z_2, \ldots, z_m),\ f_2(z_1, z_2, \ldots, z_m),\ \ldots,\ f_{m+1}(z_1, z_2, \ldots, z_m)$$

$(m+1)$ fonctions rationnelles entières des m variables $z_1, z_2, \ldots, z_m$. Désignons par R et S les déterminants fonctionnels

$$R = \frac{\partial(f_1, f_2, \ldots, f_m)}{\partial(z_1, z_2, \ldots, z_m)},\quad S = (-1)^m \frac{\partial(f_2, f_3, \ldots, f_m, f_{m+1})}{\partial(z_1, z_2, \ldots, z_{m-1}, z_m)}$$

536) Monatsb. Akad. Berlin 1865, p. 687; Werke[167]) 1, p. 135.

537) Au sujet de la généralisation de la *formule de Lagrange*, on peut consulter *H. Laurent*, Traité d'Algèbre (5e éd.) 3, Paris 1894, p. 198.

538) J. math. pures appl. (1) 6 (1841), p. 345; C. R. Acad. sc. Paris 13 (1841), p. 467, 412.

539) Monatsb. Akad. Berlin 1865, p. 690; Werke[167]) 1, p. 140.

et envisageons une fonction rationnelle entière quelconque $f(z_1, z_2, \ldots, z_m)$ de degré moindre que le degré de la fonction f_{m+1}. On a alors nécessairement une relation de la forme

$$\sum_h \frac{f(\alpha_{1h}, \ldots, \alpha_{mh})}{f_{m+1}(\alpha_{1h}, \ldots, \alpha_{mh})} = \sum_k \frac{f(\beta_{1k}, \ldots, \beta_{mk})\ R(\beta_{1k}, \ldots, \beta_{mk})}{f_1(\beta_{1k}, \ldots, \beta_{mk}) S(\beta_{1k}, \ldots, \beta_{mk})},$$

où $(\alpha_{1h}, \ldots, \alpha_{mh})$ est l'une quelconque des racines du système d'équations $(f_1 = 0, f_2 = 0, \ldots, f_m = 0)$ et où $(\beta_{1k}, \beta_{2k}, \ldots, \beta_{mk})$ est l'une quelconque des racines du système d'équations $(f_2 = 0, \ldots, f_m = 0, f_{m+1} = 0)$; dans le premier membre la somme est étendue à toutes les racines du système $(f_1 = 0,\ f_2 = 0,\ \ldots,\ f_m = 0)$, dans le second membre la somme est étendue à toutes les racines du système $(f_2 = 0, \ldots, f_m = 0, f_{m+1} = 0)$.

On retombe sur la *formule de Jacobi* en faisant

$$f_{m+1} = R(z_1, z_2, \ldots, z_m).$$

A. Harnack[540]) considère une expression qui dans la notation symbolique dont on fait usage dans la théorie des invariants (I 11) se présente sous la forme

$$D = \frac{U_x^{n+n'+n''-3}}{(a\,b\,c)\,a_x^{n-1}\,b_x^{n'-1}\,c_x^{n''-1}}.$$

Les symboles $a_x^n, b_x^{n'}, c_x^{n''}$ représentent trois fonctions rationnelles entières homogènes de trois variables x_1, x_2, x_3 de degrés respectivement égaux à n, n', n''. Le produit symbolique qui figure au dénominateur de D représente le déterminant fonctionnel des trois fonctions $a_x^n, b_x^{n'}, c_x^{n''}$ divisé par $n\,n'\,n''$. Le symbole qui figure au numérateur de D représente une fonction rationnelle entière homogène quelconque de x_1, x_2, x_3, de degré $n + n' + n'' - 3$.
Alors on a identiquement

$$n'' \sum_{\substack{a_x^n = 0,\\ b_x^{n'} = 0,}} D = n \sum_{\substack{b_x^{n'} = 0,\\ c_x^{n''} = 0,}} D = n' \sum_{\substack{c_x^{n''} = 0,\\ a_x^n = 0,}} D,$$

le premier signe Σ étant étendu aux valeurs de D pour tous les points d'intersection des courbes $a_x^n = 0$, $b_x^{n'} = 0$, le second aux valeurs de D pour tous les points d'intersection des courbes $b_x^{n'} = 0$, $c_x^{n''} = 0$, le troisième aux valeurs de D pour tous les points d'intersection des courbes $c_x^{n''} = 0$, $a_x^n = 0$.

78. Théorie des caractéristiques. De même que la connaissance du signe de la dérivée $f'(x)$ d'une fonction $f(x)$ d'une seule variable est utile pour l'étude des variations de cette fonction, de

540) Math. Ann. 9 (1876), p. 371.

même celle du signe du déterminant fonctionnel de m fonctions de m variables intervient dans certains problèmes relatifs à ces m fonctions. Des remarques à ce sujet ont été faites par *J. J. Sylvester*[541]).

Dans la théorie des *caractéristiques* de *L. Kronecker*[542]), le rôle du déterminant fonctionnel est très important. Dans cette théorie on se propose de *séparer* les racines réelles d'un système d'équations algébriques à plusieurs inconnues et à coefficients réels; c'est le même problème pour les systèmes d'équations à plusieurs inconnues que celui que résout le *théorème de Sturm* pour le cas d'une seule équation algébrique à une seule inconnue (à coefficients réels).

Pour parvenir à ce résultat on introduit la notion de *caractéristique* d'un système de $m+1$ fonctions de m variables. Supposons à cet effet, que

$$f_0(z_1, z_2, \ldots, z_m),\ f_1(z_1, z_2, \ldots, z_m),\ \ldots,\ f_m(z_1, z_2, \ldots, z_m)$$

désignent $m+1$ fonctions rationnelles entières des m variables $z_1, z_2, \ldots, z_m$ à coefficients *réels*, ne s'annulant chacune que pour des valeurs *finies* des variables et ayant chacune une valeur positive dès que les valeurs absolues de toutes les variables dépassent un nombre positif déterminé. Désignons par

$$f_{0\alpha}, f_{1\alpha}, \ldots, f_{m\alpha} \quad (\alpha = 1, 2, \ldots, m)$$

les dérivées partielles, prises par rapport à z_α, des fonctions $f_0, f_1, \ldots, f_m$ et par

$$f_{00}, f_{10}, \ldots, f_{m0}$$

des indéterminées. Formons le déterminant

$$\Delta = \begin{vmatrix} f_{00}, & f_{10}, & \ldots, & f_{m0} \\ f_{01}, & f_{11}, & \ldots, & f_{m1} \\ \cdot & \cdot & \cdot & \cdot \\ f_{0m}, & f_{1m}, & \ldots, & f_{mm} \end{vmatrix}$$

et désignons par Δ_k la dérivée

$$\Delta_k = \frac{\partial \Delta}{\partial f_{k0}};$$

c'est, au signe près, le déterminant fonctionnel des m fonctions f_0, $f_1, \ldots, f_{k-1}, f_{k+1}, \ldots, f_m$. Désignons enfin par D le déterminant

541) Philos. Trans. London 143 (1853), p. 407; Papers 1, Cambridge 1905, p. 429.

542) Monatsb. Akad. Berlin 1869, p. 159, 688; 1873, p. 153; 1878, p. 145; Werke 1, Leipzig 1895, p. 177, 215, 346; 2, Leipzig 1897, p. 73; C. R. Acad. sc. Paris 113 (1891), p. 1006/12.

$$D = \begin{vmatrix} f_0, & f_1, & \ldots, & f_m \\ f_{01}, & f_{11}, & \ldots, & f_{m1} \\ \cdot & \cdot & \cdot & \cdot \\ f_{0m}, & f_{1m}, & \ldots, & f_{mm} \end{vmatrix}$$

qui n'est autre que le déterminant Δ dans lequel les indéterminées $f_{00}, f_{10}, \ldots, f_{m0}$ sont remplacées par les fonctions envisagées $f_0, f_1, \ldots, f_m$.

Si l'on convient que $\operatorname{sgn} A = +1$ si $A > 0$ et que $\operatorname{sgn} A = -1$ si $A < 0$ on démontre que la somme

$$\text{(I)} \qquad \sum \operatorname{sgn} D(z_1, z_2, \ldots, z_m),$$

étendue à toutes les racines du système de m équations

$$(f_0 = 0,\ f_1 = 0,\ \ldots,\ f_{k-1} = 0,\ f_{k+1} = 0,\ \ldots,\ f_m = 0),$$

a la même valeur, que l'on choisisse k égal à 0, à 1, à 2, ... ou à m. De même la somme

$$\text{(II)} \qquad \sum \operatorname{sgn} \Delta_k(z_1, z_2, \ldots, z_m),$$

étendue à toutes celles des racines du système de m équations

$$(f_0 = 0,\ f_1 = 0,\ \ldots,\ f_{k-1} = 0,\ f_{k+1} = 0,\ \ldots,\ f_m = 0)$$

pour lesquelles $f_k < 0$, a la même valeur, que l'on prenne k égal à 0, à 1, à 2, ... ou à m. Et il en est encore ainsi pour la somme

$$\text{(III)} \qquad \sum \operatorname{sgn} \Delta_k(z_1, z_2, \ldots, z_m)$$

étendue à toutes celles des racines du même système d'équations pour lesquelles $f_k > 0$.

Si l'on désigne par χ chacune des sommes (II), chacune des sommes (I) sera égale à $-\frac{1}{2}\chi$ et chacune des sommes (III) sera égale à $-\chi$.

On appelle χ la *caractéristique* du système de $m+1$ fonctions $f_0, f_1, \ldots, f_m$ des m variables $z_1, z_2, \ldots, z_m$.

La propriété fondamentale de la caractéristique χ consiste en ce que, si l'on fait varier d'une façon continue les coefficients des fonctions $f_0, f_1, \ldots, f_m$, la caractéristique χ de ces fonctions ne varie que quand les coefficients de $f_0, f_1, \ldots, f_m$ prennent des valeurs telles que les $m+1$ fonctions aient un zéro commun; pour ces valeurs des coefficients le déterminant D est nul. S'il devient nul en passant du positif au négatif, la caractéristique χ augmente de 1; si, au contraire, il devient nul en passant du négatif au positif, la caractéristique χ diminue de 1.

La théorie des caractéristiques a été perfectionnée par *E. Picard*[543]) et *W. von Dyck*[544]).

E. Picard[545]) démontre le théorème que voici: soient $f_1(x, y)$, $f_2(x, y)$ deux fonctions continues ainsi que leurs dérivées partielles du premier ordre par rapport à x et à y. Posons

$$(f_1^2 + f_2^2)\, P = f_1 \frac{\partial f_2}{\partial x} - f_2 \frac{\partial f_1}{\partial x},$$

$$(f_1^2 + f_2^2)\, Q = f_1 \frac{\partial f_2}{\partial y} - f_2 \frac{\partial f_1}{\partial y};$$

alors l'intégrale, prise le long d'une courbe fermée C,

$$J = \frac{1}{2\pi} \int_{(C)} (P\, dx + Q\, dy)$$

donne l'excès du nombre des racines incluses dans l'intérieur de la courbe (C) pour lesquelles le déterminant fonctionnel est positif sur le nombre de ces racines pour lesquelles le déterminant fonctionnel est négatif. Le *théorème de Picard* s'étend d'ailleurs au cas d'un nombre quelconque de variables.

W. von Dyck[544]), après avoir démontré le même théorème que *E. Picard* par un procédé un peu différent, établit une proposition plus générale dont il déduit d'une part le *théorème de Picard* et d'autre part les expressions des zéros eux-mêmes du système de fonctions envisagées.

79. Autres mémoires sur les déterminants fonctionnels. *T. Muir*[546]) fait une remarque sur l'une des propositions de *C. G. J. Jacobi*[547]) signalées au nº **73.**

E. Combescure[548]) démontre à nouveau la formule de *C. G. J. Jacobi*

$$\frac{\partial (f_1, \ldots, f_n)}{\partial (x_1, \ldots, x_n)} \cdot \frac{\partial (x_1, \ldots, x_n)}{\partial (f_1, \ldots, f_n)} = 1$$

qui a été également signalée au nº **73.**

A. Levi[549]) et *F. Gerbaldi*[550]) s'occupent des singularités de la

543) J. math. pures appl. (4) 8 (1892), p. 5; C. R. Acad. sc. Paris 113 (1891), p. 356, 669, 1012.

544) C. R. Acad. sc. Paris 119 (1894), p. 1254; 120 (1895), p. 34; Sitzgsb. Akad. München 28 (1898), p. 203. Voir aussi *A. Vasiliev*, Učenyja Zapiski Kazan Univ. 41 (1874), p. 631/56.

545) Nouv. Ann. (3) 8 (1889), p. 5/13.

546) Proc. R. Soc. Edinb. 23 (1899/1901), p. 423.

547) J. reine angew. Math. 22 (1841), p. 319; Werke[99]) 3, p. 395.

548) Ann. Ec. Norm. (1) 4 (1867), p. 93.

549) Atti Accad. Torino 31 (1895/6), p. 502; Giorn. mat. (2) 3 (1896), p. 215.

550) *Rend. Circ. mat. Palermo 10 (1896), p. 158 (Note de *G. Loria*).*

jacobienne de quatre surfaces; on entend par là la surface dont l'équation en coordonnées homogènes est

$$\frac{\partial (f_1, f_2, f_3, f_4)}{\partial (z_1, z_2, z_3, z_4)} = 0,$$

si $f_i(z_1, z_2, z_3, z_4) = 0$ $(i = 1, 2, 3, 4)$ sont les équations, en coordonnées homogènes, des quatre surfaces envisagées.

W. Trzaska[551]) remarque qu'étant données k fonctions $f_1, f_2, \ldots f_k$ de m variables indépendantes $z_1, z_2, \ldots, z_m$, on peut chercher s'il existe des relations indépendantes des variables entre ces fonctions, en appliquant le théorème suivant: pour que k fonctions

$$f_1(z_1, z_2, \ldots, z_m),\ f_2(z_1, z_2, \ldots, z_m),\ \ldots,\ f_k(z_1, z_2, \ldots, z_m)$$

de m variables indépendantes satisfassent à p relations indépendantes de ces variables, il faut et il suffit que parmi les k fonctions $f_1, f_2, \ldots, f_k$ il y en ait $k-p$, par ex. $f_1, f_2, \ldots, f_{k-p}$ telles que leur déterminant fonctionnel

$$\frac{\partial (f_1, f_2, \ldots, f_{k-p})}{\partial (z_1, z_2, \ldots, z_{k-p})}$$

soit différent de zéro, et que les p^2 déterminants fonctionnels

$$\frac{\partial (f_1, f_2, \ldots, f_{k-p}, f_i)}{\partial (z_1, z_2, \ldots, z_{k-p}, z_h)},$$

où i et h prennent toutes les valeurs entières vérifiant les inégalités

$$k - p + 1 \leqq i \leqq k, \quad k - p + 1 \leqq h \leqq k,$$

soient identiquement nuls pour toutes les valeurs des variables $z_1, z_2, \ldots, z_m$. Ce théorème n'a toutefois lieu que pour $m > k - p > 0$.

M. Falk[552]) démontre par induction en passant de $n-1$ à n, sans faire d'ailleurs usage de la multiplication des déterminants, le théorème connu sur la dépendance entre des fonctions quand leur déterminant fonctionnel s'évanouit. Il donne aussi une démonstration de ce théorème, ordinairement admis comme évident: les équations qui définissent les variables dépendantes en fonctions des variables indépendantes peuvent, quand le déterminant fonctionnel n'est pas nul, être résolues par rapport à ces dernières variables. Pour terminer, il donne une règle à l'aide de laquelle on peut s'assurer si une variable dépendante désignée peut s'exprimer ou non en fonction des autres variables.

551) Pamiętnik towarzystwa nauk ścisłych w Paryżu 1 (1871), p. 113 [1870].

552) Tidskrift for math. och fys. (Upsal) 5 (1874), p. 193/206.

F. Casorati[553]) s'occupe 1°) des déterminants fonctionnels de $n+1$ fonctions de $n+1$ variables, 2°) des déterminants de degré $n+1$ dont la première ligne contient $n+1$ fonctions de n variables et les lignes suivantes les dérivées de ces $n+1$ fonctions par rapport aux n variables, 3°) des déterminants de degré $n+1$ dont la première ligne contient $n+1$ fonctions d'une variable, les autres lignes contenant les dérivées successives de ces fonctions par rapport à la variable; ces déterminants portent le nom de *wronskiens* (cf. I 2, **32**).

F. Casorati[554]) étudie le déterminant fonctionnel de fonctions ayant un facteur commun, question qui a été reprise par *G. Torelli*[555]). Dans ce même travail *F. Casorati*[554]) calcule le hessien $H(\xi_1, \xi_2, \ldots, \xi_\nu)$ d'une fonction

$$f(x_1, x_2, \ldots, x_n) = \varphi(\xi_1, \xi_2, \ldots, \xi_\nu)$$

dans le cas où $x_1, x_2, \ldots, x_n$ dépendent linéairement d'un nombre moindre de quantités $\xi_1, \xi_2, \ldots, \xi_\nu$.

Sur les wronskiens on peut consulter *G. Peano*[556]), *A. Demoulin*[557]), *S. Dickstein*[558]), *S. Pincherle*[559]), *G. Vivanti*[560]), *E. Bortolotti*[561]).

N. L. W. A. Gravelaar[562]) démontre que le hessien $H(z_1, z_2, \ldots, z_m)$ d'une fonction homogène de m variables s'évanouit identiquement ainsi que ses mineurs, jusqu'à ceux de degré $(m-r+1)$, quand au moyen d'une substitution linéaire la fonction donnée peut se transformer en une fonction de $(m-r)$ variables seulement.

E. J. Nanson[563]) étudie les effets du changement des variables indépendantes sur le hessien d'une fonction de plusieurs variables et considère[564]) le hessien d'une fonction implicite.

---

553) Memorie Reale Ist. Lombardo (3) 4 (1877), p. 181/7 [1874].

554) Reale Ist. Lombardo, *Rendic.* (2) 7 (1874), p. 846.

555) Rend. Circ. mat. Palermo 7 (1893), p. 75.

556) Mathesis (1) 9 (1889), p. 75, 110; Atti R. Accad. Lincei, *Rendic.* mat. (5) 6 I (1897), p. 413.

557) Mathesis (1) 9 (1889), p. 136; (2) 7 (1897), p. 62.

558) Prace matematyczne fizyczne 1 (1888), p. 5/25; Archivo de mat. (Valence) 2 (1897/9), p. 102, 122, 141 (traduction inachevée du polonais).

559) Atti R. Accad. Lincei, *Rendic.* mat. (5) 6, I (1897), p. 301.

560) *Atti Accad. R. Lincei *Rendic.* mat. (5) 7 I (1898), p. 194/7.*

561) *Id. (5) 7 I (1898), p. 45/50 (Notes 560 et 561 de *G. Vivanti*).*

562) Nieuw Archief voor Wiskunde (1) 3 (1877), p. 193/202.

563) Messenger math. (2) 25 (1895/6), p. 133.

564) Id. (2) 25 (1895/6), p. 137; voir aussi *F. de Ponte Horta*, Estudo elementar dos determinantes, seguido de uma parte complementar relativa principalmente aos determinantes funccionaes, Lisbonne 1889.

A. Brill[565]) démontre que le résultant obtenu en éliminant $n-1$ variables entre n fonctions rationnelles entières à n variables a pour discriminant une fonction entière des coefficients qui admet comme facteur le résultant des n fonctions et de leur déterminant fonctionnel.

Considérons, avec *H. Laurent*[566]), m fonctions rationnelles entières de m variables

$$f_1(z_1, z_2, \ldots, z_m), f_2(z_1, z_2, \ldots, z_m), \ldots, f_m(z_1, z_2, \ldots, z_m)$$

et soit $(\xi_1, \xi_2, \ldots, \xi_m)$ une racine du système d'équations

$$f_1 = 0,\ f_2 = 0,\ \ldots,\ f_m = 0.$$

En désignant par $u_1, u_2, \ldots, u_m$ de nouvelles variables posons

$$f_1 = u_1,\ f_2 = u_2,\ \ldots,\ f_m = u_m$$

et envisageons $z_1, z_2, \ldots, z_m$ comme des fonctions de $u_1, u_2, \ldots, u_m$ définies par ces équations. Formons l'intégrale multiple d'ordre m

$$(1) \qquad \int\!\!\int\!\!\int \ldots \frac{F(z_1, z_2, \ldots, z_m)}{u_1 u_2 \ldots u_m}\, du_1\, du_2 \ldots du_m,$$

où F désigne une fonction quelconque de $z_1, z_2, \ldots, z_m$; les intégrales doivent être étendues aux points $(u_1, u_2, \ldots, u_m)$ d'une variété fermée (W) suffisamment petite de forme quelconque entourant le point de coordonnées

$$u_1 = 0,\ u_2 = 0,\ \ldots,\ u_m = 0.$$

Nous allons transformer cette intégrale de deux manières différentes. D'une part nous prendrons $z_1, z_2, \ldots, z_m$ comme nouvelles variables indépendantes; l'intégrale envisagée se transforme alors en l'intégrale multiple d'ordre m

$$\int\!\!\int\!\!\int \ldots J \cdot F(z_1, z_2, \ldots, z_m)\, \frac{dz_1\, dz_2 \ldots dz_m}{f_1 f_2 \ldots f_m},$$

où J désigne le déterminant fonctionnel

$$J = \frac{\partial(f_1, f_2, \ldots, f_m)}{\partial(z_1, z_2, \ldots, z_m)}$$

et dans laquelle ne figurent plus les indéterminées $u_1, u_2, \ldots, u_m$. Cette intégrale est étendue à une variété fermée entourant le point $(\xi_1, \xi_2, \ldots, \xi_m)$ et ne contenant aucune autre solution des équations données si l'on a eu soin de choisir pour (W) une variété fermée suffisamment petite.

D'un autre côté, si pour $u_1 = r_1 e^{\theta_1 i}$, $u_2 = r_2 e^{\theta_2 i}, \ldots, u_m = r_m e^{\theta_m i}$ on intègre la même expression différentielle en prenant pour chaque

---

565) Nachr. Ges. Gött. 1889, p. 89/92.

566) C. R. Acad. sc. Paris 67 (1868), p. 491.

point $(z_1, z_2, \ldots, z_m)$ correspondant au point $(u_1, u_2, \ldots, u_m)$ celui qui est dans le *voisinage* du point déterminé ayant pour coordonnées $z_1 = \zeta_1$, $z_2 = \zeta_2$, $\ldots$, $z_m = \zeta_m$, puis qu'on fasse tendre $r_1, r_2, \ldots, r_m$ vers zéro, donc z_1 vers ζ_1, z_2 vers ζ_2, $\ldots$, z_m vers ζ_m, on trouve, comme limite de l'intégrale multiple envisagée, l'expression

$$(2i\pi)^m F(\zeta_1, \zeta_2, \ldots, \zeta_m).$$

On a donc la relation

$$(2i\pi)^m F(\zeta_1, \zeta_2, \ldots, \zeta_m) = \int\!\!\int\!\!\int \ldots J \cdot F(z_1, z_2, \ldots, z_m)\, \frac{dz_1\, dz_2 \ldots dz_m}{f_1 f_2 \ldots f_m}$$

qui permet de déterminer $F(\zeta_1, \zeta_2, \ldots, \zeta_m)$ tant que J ne s'annule pas, c'est-à-dire tant que $(\zeta_1, \zeta_2, \ldots, \zeta_m)$ n'est pas une racine multiple du système d'équations envisagées[567].

Le théorème fondamental.

80. Énoncé du théorème fondamental. Toute fonction rationnelle entière d'une variable z

$$f(z) = a_0 z^n + a_1 z^{n-1} + \cdots + a_{n-1} z + a_n,$$

à coefficients complexes (réels ou imaginaires) $a_0, a_1, \ldots, a_{n-1}, a_n$, admet un zéro au moins. On en déduit immédiatement (nº **18**) qu'elle admet exactement n zéros, chaque zéro d'ordre de multiplicité α étant compté pour α zéros.

Tel est l'énoncé que l'on donne généralement du théorème fondamental de l'Algèbre. Les démonstrations de ce théorème sont nombreuses. Elles diffèrent d'ailleurs *essentiellement* suivant le point de vue auquel on se place, suivant la doctrine que l'on professe sur les fondements de l'Arithmétique. Suivant ce point de vue, telle démonstration est rigoureuse ou ne l'est pas; au point de vue purement arithmétique de *L. Kronecker* le théorème tel qu'on vient de l'énoncer n'est même pas exact et il convient de le remplacer par un autre théorème[568] concernant la possibilité, dans le cas où les coefficients a_0, $a_1, a_2, \ldots, a_{n-1}, a_n$ sont réels, de *déterminer* pour chaque nombre positif (rationnel) arbitrairement fixé ε des intervalles dans lesquels la valeur absolue de $f(z)$ reste inférieure à ε et aux deux extrémités desquels $f(z)$ soit de signes contraires; si n est pair on peut déterminer suivant les cas $0, 2, 4, \ldots, n-2$ ou n de ces intervalles; si n est impair on peut suivant les cas en déterminer $1, 3, 5, \ldots, n-2$ ou n; c'est l'existence de ces intervalles qui permet de *définir* les racines irrationnelles de l'équation algébrique $f(z) = 0$. Au point de vue intuitif au contraire (cf. I 3, **9**), ou lorsqu'on admet comme évident a priori qu'à chaque segment de droite correspond nécessairement un nombre déterminé, le théorème fondamental est, au moins relativement, assez facile à démontrer.

567) Au sujet des déterminants fonctionnels, voir encore *C. Neumann*, Math. Ann. 1 (1869), p. 208; *Ph. Gilbert*, Mém. Acad. Belgique 38 (1871), mém. nº 7, p. 1/12 [1869]; rapport de *M. Steichen*, Bull. Acad. Belgique (2) 28 (1869), p. 528.

568) Cf. *L. Kronecker*, J. reine angew. Math. 101 (1887) p. 337; Werke 3^1, Leipzig 1899, p. 251.

Suivant que l'on suppose connue, ou non, la notion *analytique* du continu, suivant aussi que l'on estime, ou non, que toute démonstration du théorème fondamental doit fournir pour être légitime un procédé permettant de calculer au moyen des coefficients de $f(z)$ et avec telle approximation que l'on veut les racines (dont l'existence résulte alors, en dernière analyse, de ce procédé même), l'objet même de la démonstration du théorème fondamental sera changé.

Nous allons passer en revue[569] les principales démonstrations du théorème fondamental que l'on a données en se plaçant tour à tour à l'un ou à l'autre de ces points de vue.

81. Démonstrations anciennes. Démonstrations de d'Alembert, d'Euler, de Daviet de Foncenex, de Lagrange, de Laplace. *Les mathématiciens grecs semblent avoir ignoré qu'une équation peut admettre plus d'une racine. Au point de vue de l'interprétation des résultats, les équations les plus simples que l'on rencontre parmi celles qui ont plus d'une racine sont les équations du second degré dont les deux racines sont positives; même dans ce cas très simple il semble qu'ils n'aient jamais envisagé qu'une seule des deux racines. On sait, par contre, que les mathématiciens hindous[570] et arabes[571] connaissaient certaines équations du second degré ayant deux racines.

H. Cardan[572] fait observer que les équations du troisième degré peuvent avoir trois racines et que les équations du quatrième degré peuvent en avoir quatre. *F. Viète*[573] construit une équation du cinquième degré ayant cinq racines, et il sait évidemment qu'on peut

569) *G. Loria*, Rivista mat. 1 (1891), p. 185 et suiv.; voir aussi Bibl. math. (2) 5 (1891), p. 99.

570) *Voir *H. T. Colebrooke*, Algebra with arithmetic, (Algèbre de *Bhâscara*), Londres 1817, p. 135.*

571) *Voir *F. Rosen*, The algebra of Mohammed ben Musa (Algèbre d'*Alkhovaresmî*), Londres 1831, p. 18.*

572) *Ars magna, Nuremberg 1545; nouv. éd. Bâle 1570, p. 6/7; Opera 4, Lyon 1663, p. 223/4.*

573) *De emendatione aequationum; Opera, éd. *F. van Schooten*, Leyde 1646, p. 158 (Texte et notes 570 à 573 de *G. Eneström*).*

miner suivant les cas $0, 2, 4, \ldots, n-2$ ou n de ces intervalles; si n est impair on peut suivant les cas en déterminer $1, 3, 5, \ldots, n-2$ ou n; c'est l'existence de ces intervalles qui permet de *définir* les racines irrationnelles de l'équation algébrique $f(z)=0$. Au point de vue intuitif au contraire (cf. I 3, **9**), ou lorsqu'on admet comme évident a priori qu'à chaque segment de droite correspond nécessairement un nombre déterminé, le théorème fondamental est, au moins relativement, assez facile à démontrer.

Suivant que l'on suppose connue, ou non, la notion *analytique* du continu, suivant aussi que l'on estime, ou non, que toute démonstration du théorème fondamental doit fournir pour être légitime un procédé permettant de calculer au moyen des coefficients de $f(z)$ et avec telle approximation que l'on veut les racines (dont l'existence résulte alors, en dernière analyse, de ce procédé même), l'objet même de la démonstration du théorème fondamental sera changé.

Nous allons passer en revue[569]) les principales démonstrations du théorème fondamental que l'on a données en se plaçant tour à tour à l'un ou à l'autre de ces points de vue.

81. Démonstrations anciennes. Démonstrations de d'Alembert, d'Euler, de Daviet de Foncenex, de Lagrange, de Laplace. *Les mathématiciens grecs semblent avoir ignoré qu'une équation peut admettre plus d'une racine. Au point de vue de l'interprétation des résultats, les équations les plus simples que l'on rencontre parmi celles qui ont plus d'une racine sont les équations du second degré dont les deux racines sont positives; même dans ce cas très simple il semble qu'ils n'aient jamais envisagé qu'une seule des deux racines. On sait, par contre, que les mathématiciens hindous[570]) et arabes[571]) connaissaient certaines équations du second degré ayant deux racines.

H. Cardan[572]) fait observer que les équations du troisième degré peuvent avoir trois racines et que les équations du quatrième degré peuvent en avoir quatre. *F. Viète*[573]) construit une équation du cinquième degré ayant cinq racines, et il sait évidemment qu'on peut

569) *G. Loria*, Rivista mat. 1 (1891), p. 185 et suiv.; voir aussi Bibl. math. (2) 5 (1891), p. 99.

570) *Voir *H. T. Colebrooke,* Algebra with arithmetic, (Algèbre de *Bhâscara*), Londres 1817, p. 135.*

571) *Voir *F. Rosen,* The algebra of Mohammed ben Musa (Algèbre d'*Alkhovaresmî*), Londres 1831, p. 18.*

572) *Ars magna, Nuremberg 1545; nouv. éd. Bâle 1570, p. 6/7; Opera 4, Lyon 1663, p. 223/4.*

573) *De emendatione aequationum; Opera, éd. *F. van Schooten,* Leyde 1646, p. 158 (Texte et notes 570 à 573 de *G. Eneström*).*

construire de la même façon une équation du $n^{\text{ième}}$ degré ayant n racines.

Albert Girard[574]) affirme déjà que, puisque certaines équations algébriques (à coefficients réels rationnels) admettent autant de racines que l'indique leur degré, il est utile, quand on a affaire à une équation algébrique admettant moins de racines que ne l'indique son degré, d'introduire autant de *solutions impossibles* qu'il lui en manque pour que le nombre total des racines et des solutions impossibles soit dans tous les cas précisément égal au degré de l'équation.*

**J. Prestet*[575]) et *M. Rolle*[576]) se placent encore à ce même point de vue. *R. Descartes*[577]) et *I. Newton*[578]) se contentent d'affirmer qu'une équation du $n^{\text{ième}}$ degré peut avoir au plus n racines. *J. Ozanam*[579]) et *Ch. R. Reyneau*[580]) disent par contre expressément qu'une équation „a autant de racines qu'elle a de degré" et ils prétendent même avoir démontré ce théorème; leurs soi-disant démonstrations reviennent toutefois à affirmer que toute fonction rationnelle entière du $n^{\text{ième}}$ degré peut être conçue comme un produit de n facteurs linéaires.*

*En 1741, *J. P. de Gua*[581]) démontre que toute équation algébrique, de degré n, a n racines, en supposant que toute équation algébrique puisse se résoudre formellement au moyen de radicaux. En 1742 *Nicolas Bernoulli*[582]) refuse d'admettre que toute fonction rationnelle entière à coefficients réels puisse être représentée par un produit de facteurs du premier et du second degré à coefficients réels.

L. Euler, le premier, se place au point de vue moderne, en affir-

574) Invention nouvelle en l'Algèbre, Amsterdam 1629; réédité par *D. Bierens de Haan,* Leyde 1884; sign. E_4 recto à F_1 verso.

575) *Nouveaux élémens de math. 2, Paris 1689, p. 353/4.*

576) *Traité d'Algèbre, Paris 1690, p. 124. D'autre part (id. p. 230) *M. Rolle* annonce que $\sqrt[n]{a}$ a effectivement n valeurs distinctes ce qui signifie que l'équation $x^n - a = 0$ a précisément n racines.*

577) *Géométrie, Leyde 1637; Œuvres[2]) 6, p. 444.*

578) *Arith. univ.[90]), Leyde 1732, p. 181; trad. *N. Beaudeux* 2, Paris an X, p. 4; Opera, éd. *S. Horsley* 1, Londres 1779, p. 167.*

579) *Nouveaux elemens d'algèbre 1, Amsterdam 1702, p. 173/4.*

580) *Analyse démontrée[92]) 1, p. 63, 74 (Texte et notes 575 à 580 de *G. Eneström*).*

581) *Hist. Acad. sc. Paris 1741, éd. 1744, M. p. 480. On trouvera dans ce même mémoire des renseignements historiques (p. 436/58).*

582) *Lettre à *L. Euler* datée du 24 octobre 1742, publ. par *P. H. Fuss,* Corresp. math. phys. 2, St. Pétersbourg 1843, p. 695; voir aussi la lettre de *L. Euler* à *Chr. Goldbach* datée du 15 décembre 1742, publ. par *P. H. Fuss,* Corresp. math. phys. 1, St. Pétersbourg 1843, p. 170 (Texte et note de *E. Cartan*).*

mant que l'on peut *démontrer* le théorème d'après lequel toute fonction rationnelle entière d'une variable à coefficients réels peut être décomposée en facteurs réels linéaires ou quadratiques[583]).*

(*Jean le Rond*) *d'Alembert*[584]) a donné une première démonstration de ce théorème; il dit même explicitement que si aucun nombre réel n'est racine d'une équation algébrique à coefficients réels il y a toujours un nombre de la forme $a + b\sqrt{-1}$, où a et b sont réels, qui vérifie l'équation algébrique. *Cette démonstration parut rigoureuse à l'époque où elle fut publiée ce qui valut au théorème de garder, en France du moins, le nom de *théorème de d'Alembert.**

C. F. Gauss a toutefois critiqué à juste titre[585]) le mode de démonstration dont *J. d'Alembert* a fait usage; il montre que la démonstration de *J. d'Alembert* repose au fond sur l'inversion de la relation

$$y = f(x) = a_0 x^m + a_1 x^{m-1} + \cdots + a_{m-1} x + a_m;$$

or pour *J. d'Alembert* la possibilité de cette inversion résulte elle-même de considérations ayant un caractère essentiellement géométrique; au point de vue arithmétique la démonstration de *J. d'Alembert* est donc insuffisante; *C. F. Gauss* a d'ailleurs montré comment l'inversion dont il s'agit peut être légitimée d'une façon rigoureuse[586]).

*Après *J. d'Alembert*, *L. Euler* a publié deux démonstrations[587]) du théorème fondamental. Voici en quoi consiste la première de ces deux démonstrations: Si l'on envisage la fonction rationnelle entière

$$Z = z^{2m} + c_2 z^{2m-2} + c_3 z^{2m-3} + \ldots + c_{2m-1} z + c_{2m}$$

à coefficients *réels* $c_2, c_3, \ldots, c_{2m-1}, c_{2m}$, on peut toujours la décomposer en un produit de deux fonctions rationnelles entières à coefficients réels

$$z^m - u z^{m-1} + a_2 z^{m-2} + a_3 z^{m-3} + \ldots + a_{m-1} z + a_m$$

et

$$z^m + u z^{m-1} + b_2 z^{m-2} + b_3 z^{m-3} + \ldots + b_{m-1} z + b_m.$$

Pour qu'il en soit ainsi il suffit que les $2m - 1$ coefficients $u, a_2, a_3, \ldots, a_{m-1}, a_m, b_2, b_3, \ldots, b_{m-1}, b_m$ de ces deux fonctions rationnelles

583) *Misc. Berolin. 7 (1743), p. 202.*

584) Hist. Acad. Berlin 2 (1746), éd. 1748, p. 183. *Un peu plus tard *J. d'Alembert* examine aussi [Hist. Acad. sc. Paris 1769, éd. 1772, M. p. 74] le cas général d'une équation à coefficients complexes (Note de *E. Cartan*).*

585) Demonstratio nova ..., Diss. Helmstedt 1799, § 6; Werke 3, Göttingue 1876, p. 9.

586) Diss.[585]) § 23/4; Werke 3, p. 29.

587) *Hist. Acad. Berlin 5 (1749), éd. 1751, p. 223 et suiv.*

entières vérifient $2m - 1$ relations qu'il est aisé de former. *L. Euler* essaie de démontrer que l'on peut attribuer à $u, a_2, a_3, \ldots, a_m, b_2, b_3, \ldots, b_m$ des valeurs réelles satisfaisant à ces $2m - 1$ relations dans lesquelles $c_2, c_3, \ldots, c_{2m}$ sont supposés avoir des valeurs réelles quelconques déterminées. *C. F. Gauss* après avoir exposé cette première[588]) démonstration de *L. Euler* en a fait la critique[589]); il fait remarquer en particulier qu'au cours de sa démonstration *L. Euler* suppose tacitement que l'équation $Z = 0$ admet $2m$ racines dont la somme est nulle par suite de ce fait que le second terme manque dans Z.

La seconde démonstration de *L. Euler*[590]) repose sur l'hypothèse inexacte que les racines des équations algébriques de tous les degrés ne sauraient être formées qu'à l'aide d'additions, de soustractions, de multiplications, de divisions et d'extractions de racines; on sait depuis *N. H. Abel* que cette proposition n'est vraie en général que pour les équations dont le degré ne dépasse pas quatre.*

C. F. Gauss[591]) a aussi exposé une démonstration due à *F. Daviet de Foncenex*[592]) et lui a adressé les mêmes objections à peu près qu'à la première démonstration de *L. Euler*.

J. L. Lagrange[593]) a, lui aussi, proposé deux démonstrations, non sans faire quelques pétitions de principes.

**P. S. Laplace*[594]) enfin a publié une autre démonstration qu'on retrouve exposée dans beaucoup d'ouvrages postérieurs[595]); elle donne lieu aux mêmes objections que les précédentes.*

588) *Diss.[585]) § 7; Werke 3, p. 11.*

589) *Diss.[585]) § 8; Werke 3, p. 13; voir aussi *F. Daviet de Foncenex*, Misc. Taurinensia 1 (1759), math. p. 113 et suiv.*

590) *Hist. Acad. Berlin 5 (1749), éd. 1751, p. 263.*

591) Diss.[585]) § 10; Werke 3, p. 18.

592) Misc. Taurinensia 1 (1759), math. p. 120.

593) Nouv. Mém. Acad. Berlin 3 (1772), éd. 1774, p. 222; Œuvres 3, Paris 1869, p. 479; voir aussi: Traité de la résolution numérique des équations de tous les degrés, Paris an VI; (2e éd.) Paris 1808, note X; (3e éd.) Paris 1826; Œuvres 8, Paris 1879, p. 234.

594) *Leçons de math. données à l'Ecole normale en l'an III; ces leçons ont paru dans les deux éditions des Séances des Ecoles Normales recueillies par des sténographes et revues par les professeurs (1e éd.) 2, Paris (s. d.) [an III], p. 315 (5ième leçon); J. Ec. polyt. (1) cah. 7 (1812), p. 56.*

595) *Voir par ex. *S. F. Lacroix*, Compléments des éléments d'Algèbre, Paris an VIII, p. 78; (4e éd.) Paris 1817, p. 80; *J. Hymers*, A treatise on the theory of alg. equat., Cambridge 1837; (2e éd.) Cambridge 1840, p. 187; (3e éd.) Cambridge 1858.*

82. Première démonstration de Gauss. Voici en quoi consiste essentiellement la première démonstration de *C. F. Gauss*[596]):

Envisageons une fonction rationnelle entière

$$f(z) = a_0 z^n + a_1 z^{n-1} + \cdots + a_{n-1} z + a_n$$

d'une variable complexe $z = x + iy$, à coefficients complexes (réels où imaginaires) $a_0, a_1, \ldots, a_{n-1}, a_n$; on suppose que a_0 est différent de zéro et que le nombre naturel n est plus grand que 1. La fonction $f(z)$ peut être mise sous la forme

$$f(x+iy) = \varphi(x,y) + i\psi(x,y),$$

où $\varphi(x,y)$ et $\psi(x,y)$ sont des fonctions rationnelles entières des variables réelles x et y, à coefficients réels.

*Ceci posé, si dans le plan représentatif des nombres complexes on trace de l'origine O des coordonnées comme centre un cercle (C) de rayon $R > 1$ et tel que l'on ait

$$R > \sqrt{2}\,[|a_1| + |a_2| \cdots + |a_n|],$$

la circonférence du cercle (C) peut être partagée en $2n$ arcs le long desquels la fonction $\varphi(x,y)$ est alternativement positive et négative; aux $2n$ extrémités E_i $(i = 1, 2, \ldots, 2n)$ de ces arcs on a $\varphi(x,y) = 0$. De chacun des $2n$ points E_i on peut mener une ligne (T) située tout entière à l'*intérieur* du cercle (C) aboutissant à un autre des points $E_1, E_2, \ldots, E_{2n}$ et le long de laquelle $\varphi(x,y)$ est *partout* nulle.

La même circonférence du cercle (C) peut aussi être partagée en $2n$ arcs le long desquels la fonction $\psi(x,y)$ est alternativement positive et négative; aux $2n$ extrémités ε_i $(i = 1, 2, \ldots, 2n)$ de ces arcs on a $\psi(x,y) = 0$. De chacun des $2n$ points ε_i on peut mener une ligne (U) située tout entière à l'*intérieur* du cercle (C) aboutissant à un autre des points $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{2n}$ et le long de laquelle $\psi(x,y)$ est partout nulle.

D'ailleurs chaque point E_i est situé sur la circonférence du cercle (C) entre deux des points $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{2n}$ et chaque point ε_i est situé entre deux des points $E_1, E_2, \ldots, E_{2n}$[597]).* Il en résulte qu'à l'intérieur du cercle envisagé le système formé par les courbes (T) et le système formé par les courbes (U) ont nécessairement *au moins un*

596) Diss.[585]) § 19; Werke 3, p. 25.

597) Au sujet des propriétés de ces courbes (T) et (U), voir *W. Walton,* Quart. J. pure appl. math. 11 (1871), p. 178; Nouv. Ann. math. (2) 10 (1871), p. 509; *A. Raabe*, Sitzgsb. Akad. Wien 63 II (1871), p. 733; *C. F. E. Björling,* K. Svenska Vetenskaps Acad. handligar 10 (1871/2), mém. n° 3, éd. Stockholm 1871 [Diss. Lund 1871].

point commun; si ξ, η sont les coordonnées de ce point et si l'on pose $\zeta = \xi + i\eta$, la fonction $f(z)$ s'annule pour $z = \zeta$.

Cette démonstration est à l'abri de toute objection si l'on suppose légitime l'usage que *C. F. Gauss* y fait de la notion analytique du continu.

Cinquante ans après avoir donné cette première démonstration, *C. F. Gauss* l'a reprise à nouveau et l'a quelque peu modifiée[598]).

*La circonférence du cercle (C) est encore partagée en $2n$ arcs le long desquels la fonction $\varphi(x,y)$ est alternativement positive et négative, mais au lieu de faire jouer ensuite à la fonction $\psi(x,y)$ un rôle parallèle à celui de la fonction $\varphi(x,y)$, *C. F. Gauss* partage la *surface* du cercle (C) en régions (analogues aux cases d'un échiquier) dans chacune desquelles la fonction $\varphi(x,y)$ est ou bien toujours positive ou bien toujours négative; le long des lignes (U) qui séparent ces régions les unes des autres on a $\varphi(x,y) = 0$. On peut parcourir toujours dans le même sens ces lignes (U) en partant d'un point de la circonférence du cercle (C) où $\psi(x,y)$ est positif et en aboutissant en un point de cette circonférence où $\psi(x,y)$ est négatif; il faut donc qu'en *un point au moins* des lignes (U) la fonction $\psi(x,y)$ s'annule; si ξ, η sont les coordonnées de ce point et si l'on pose $\zeta = \xi + i\eta$, la fonction $f(z)$ s'annule pour $z = \zeta$.

L'avantage que présente cette modification de la *première démonstration de Gauss* consiste en ce que *C. F. Gauss* met ainsi en évidence qu'il est inutile d'envisager les deux systèmes de courbes (T) et (U) et qu'un seul de ces systèmes suffit[599]).*

L. Kronecker[600]) a présenté la première démonstration de *C. F. Gauss* (celle de 1799) en se plaçant au point de vue de sa théorie des caractéristiques.

*De cette première démonstration de *C. F. Gauss* il faut rapprocher celle plus récente de *J. Perott*[601]) et celle de *H. Dutordoir*[602]).*

83. Démonstrations d'Argand, de Legendre, de Cauchy. *La démonstration de *J. R. Argand*[603]) est entièrement indépendante de

598) Abh. Ges. Gött. 4 (1850), math. p. 3/34; Werke 3, Göttingue 1876, p. 73.

599) *L'exposé des modifications apportées par *C. F. Gauss* en 1849 à sa démonstration de 1799 et le parallèle entre ces deux façons de présenter cette première démonstration de *C. F. Gauss* sont dus à *H. Weber*.*

600) Monatsb. Akad. Berlin 1878, p. 145; Werke[189]) 2, p. 73.

601) *J. reine angew. Math. 99 (1886), p. 14.*

602) *C. R. Acad. sc. Paris 97 (1883), p. 742; Ann. Soc. scient. Bruxelles 7² (1882/3), p. 437/49; Mathesis (1) 3 (1883) supplément, p. 1/20.*

603) *Essai sur une manière de représenter les quantités imaginaires dans

celle de *C. F. Gauss.* Dans sa démonstration, *J. R. Argand* insiste sur ce qu'il est nécessaire non seulement de trouver des suites de points à coordonnées x, y telles que la valeur absolue de $f(x+iy)$ aille sans cesse en décroissant et en tendant asymptotiquement vers zéro, mais qu'il faut encore que *la loi du décroissement amène nécessairement* $f(x+iy)$ *à zéro.*

Cette démonstration a été exposée par *G. J. Hoüel*[604]. L'exposition de *J. C. Fields*[605]) ne diffère guère de celle de *G. J. Hoüel*; celle de *A. Transon*[606]), qui est antérieure à celle de *G. J. Hoüel*, est sans doute analogue mais elle est cependant moins réussie[607]).*

Il existe aussi une démonstration de *A. M. Legendre*[608]) qui s'étend d'ailleurs à des classes étendues d'équations transcendantes. Cette démonstration a été modifiée par *G. Foscolo*[609]). Dans la démonstration analogue de *A. L. Cauchy*[610]), on envisage la surface dont l'équation en coordonnées cartésiennes orthogonales (x, y, u) est

$$u = \varphi^2(x, y) + \psi^2(x, y),$$

où $\varphi(x, y)$ et $i\psi(x, y)$ continuent à désigner respectivement la partie réelle et la partie purement imaginaire de $f(x+iy)$. La variable u ne pouvant prendre de valeur négative, on suppose qu'elle atteint nécessairement une valeur minimée positive ou nulle pour un couple déterminé x_1, y_1 de valeurs de x, y. Il est alors aisé de démontrer que ce minimé ne peut être que zéro, en sorte que l'on a

$$f(x_1 + iy_1) = \varphi(x_1, y_1) + i\psi(x_1, y_1) = 0.$$

Mais cette hypothèse de l'existence d'un minimé de u constitue un point faible de la démonstration de *A. L. Cauchy.* *Ce point faible a été signalé pour la première fois, suivant *G. Darboux*[611]), par *O. Bonnet;*

les constructions géométriques, (sans nom d'auteur) Paris 1806; (2e éd.) publ. par *G. J. Hoüel,* Paris 1874; Ann. math. pures appl. 4 (1813/4), p. 133; 5 (1814/5), p. 197.*

604) *Cours de calcul infinitésimal 1, Paris 1878, p. 47.*

605) *Amer. J. math. 8 (1886), p. 178.*

606) *Nouv. Ann. math. (2) 7 (1868), p. 97. Cf. *H. Lamb,* Mem. and proc. of Manchester liter. and philos. Soc. 43 (1898/9), mém. n° 7.*

607) *Au sujet des démonstrations de *C. F. Gauss* et de *J. R. Argand* et d'une variante apportée à cette dernière démonstration par *W. Scheibner,* voir *H. Hankel,* Theorie der complexen Zahlsysteme, Leipzig 1867, p. 93/5.*

608) Essai sur la théorie des nombres, Paris an VI; (2e éd.) Paris 1808, p. 153; (3e éd.) Théorie des nombres 1, Paris 1830, p. 178.

609) Giorn. mat. (1) 2 (1864), p. 13.

610) J. Ec. polyt. (1) cah. 18 (1820), p. 411; Analyse alg.[100]), p. 329; Exercices math. 4, Paris 1829, p. 217, 253; Œuvres (2) 1, Paris 1905, p. 258; (2) 3, Paris 1897, p. 274; (2) 9, Paris 1891, p. 259, 298.

611) *Bull. sc. math. (1) 3 (1872), p. 307.*

on peut d'ailleurs y remédier[612]).* La démonstration rendue rigoureuse suppose toujours la notion analytique du continu.

*On a, à plusieurs reprises, essayé de simplifier l'exposé de cette démonstration de *A. L. Cauchy*[613]). Un essai dans cette voie a été tenté, avec un succès médiocre, par *A. Burg*[614]), puis par *J. Sussmann*[615]); *W. Walton*[616]) a fait aboutir cet essai. Dans le même ordre d'idées on peut signaler encore une seconde tentative malheureuse de *A. Burg*[617]).*

84. Les démonstrations basées sur le calcul des racines. *L'objection de *O. Bonnet* à la démonstration de *A. L. Cauchy* ne porte pas seulement sur l'existence d'un minimé de $|f(z)|^2$. Pour que la démonstration de *A. L. Cauchy* puisse être envisagée comme rigoureuse il faut encore montrer qu'on peut trouver une suite infinie de nombres z satisfaisant aux deux conditions suivantes: 1°) ils devront tendre vers une limite déterminée; 2°) ils devront faire prendre à $|f(z)|^2$ des valeurs toujours décroissantes devenant plus petites que toute valeur positive donnée.*

Le problème ainsi posé a été traité par *R. Lipschitz*[618]). *L'existence d'une suite infinie satisfaisant aux deux conditions précédentes résulte pour lui implicitement de la méthode qu'il donne pour obtenir avec

612) *Cf. *A. Genocchi,* Calcolo differenziale, publié par *G. Peano,* Turin 1884, p. 131; *H. Weber,* Alg.[24]) 1, p. 137, trad. *J. Griess,* 1, p. 143; voir aussi *J. Thomae,* Elementare Theorie der analyt. Functionen, (1e éd.) Halle 1880, p. 82, 88; *P. du Bois-Reymond,* Die allgemeine Functionentheorie 1, Tubingue 1882, p. 248; trad. *G. Milhaud* et *A. Girod,* Nice 1887, p. 191; *O. Stolz,* Vorles. über allg. Arith. 2, Leipzig 1886, p. 117; *W. Scheibner,* Ber. Ges. Lpz. 40 (1888), math. p. 4; *A. Cayley,* C. R. Acad. sc. Paris 110 (1890), p. 174, 215; Papers 13, Cambr. 1897, p. 33.*

613) *Citons *M. A. Stern,* J. reine angew. Math. 23 (1842), p. 370 et *E. Amigues,* C. R. Acad. sc. Paris 112 (1891), p. 212; Nouv. Ann. math. (3) 9 (1890), p. 116; J. math. spéc. (3) 4 (1890), p. 145; puis *H. R. Baltzer,* Die Elemente der Math. 1, Leipzig 1860; (7e éd.) Leipzig 1885; trad. par *L. Cremona,* Elementi di matematica 3, Gênes 1875, p. 125; *J. A. Serret,* Alg. sup.[30]) 1, p. 99/102.*

614) *Ausführliches Lehrbuch der höheren Math. 1, Vienne 1832, p. 57/69; voir aussi Compendium der höheren Math., Vienne 1836; (2e éd.) Vienne 1851.*

615) *J. reine angew. Math. 44 (1852), p. 57.*

616) *Quart. J. pure appl. math. 11 (1871), p. 178; Nouv. Ann. math. (2) 10 (1871), p. 509.*

617) *J. reine angew. Math. 5 (1830), p. 182.*

618) Lehrb. der Analysis 1, Bonn 1877, p. 248, § 61. Voir aussi l'article de *C. Juel,* Tidsskrift math. København (Copenhague) (5) 5 (1887), p. 161/9 et surtout, d'une part l'exposition de *P. Mansion* [Ann. Soc. scient. Bruxelles 4² (1879/80), p. 99; 14¹ (1889/90), p. 46; Mélanges math., Gand 1882], d'autre part celle de *H. Weber* [Alg.[24]) 1, p. 143, 147; trad. *J. Griess* 1, p. 150] qui contient quelques simplifications dues à *R. Dedekind* et à *G. Frobenius.*

une approximation indéfinie l'une des racines de l'équation envisagée $f(z) = 0$.

Une autre méthode d'approximation a été donnée par *F. Mertens*[619]) dans le cas où la fonction $f(z)$ n'a pas de zéros multiples et où ses coefficients sont des nombres complexes *rationnels*. Cette démonstration du théorème fondamental a été d'ailleurs complétée plus tard[620]) par *F. Mertens* lui-même.

K. Weierstrass[621]) s'est à plusieurs reprises occupé de la recherche d'un développement convergent formé *explicitement* au moyen des coefficients de $f(z)$ et qui mis à la place de z annule $f(z)$; il est parvenu à résoudre complètement ce problème. *Ch. Méray*[622]) a, de son côté, et d'une façon tout à fait indépendante, résolu le même problème.

85. Deuxième démonstration de Gauss. Quand on se place au point de vue purement arithmétique de *L. Kronecker*, la deuxième démonstration de *C. F. Gauss*[623]) est la plus parfaite de toutes.

C. F. Gauss établit tout d'abord une suite de théorèmes concernant les fonctions rationnelles entières obtenues en effectuant et ordonnant le produit

$$\varphi(z) = (z - z_1)(z - z_2)\cdots(z - z_n) = z^n - f_1 z^{n-1} + f_2 z^{n-2} - \cdots + (-1)^n f_n,$$

où $z_1, z_2, \ldots, z_n$ désignent des nombres *indéterminés*; dans l'énoncé de ces théorèmes ne figurent que des fonctions rationnelles symétriques des indéterminées $z_1, z_2, \ldots, z_n$, en d'autres termes des fonctions rationnelles des indéterminées $f_1, f_2, \ldots, f_n$. Si dans les relations qui expriment ces théorèmes on remplace $-f_1, +f_2, \ldots, (-1)^n f_n$ par les coefficients $a_1, a_2, \ldots, a_n$ d'une fonction rationnelle entière quelconque donnée

$$f(z) = z^n + a_1 z^{n-1} + a_2 z^{n-2} + \cdots + a_n,$$

on obtient des relations entre ces coefficients $a_1, a_2, \ldots, a_n$; on peut en conclure parfois que $f(z)$ jouit des mêmes propriétés que le produit $\varphi(z)$. Ainsi *C. F. Gauss* démontre par ce mode de raisonnement que la condition nécessaire et suffisante pour qu'une fonction rationnelle

619) Sitzgsb. Akad. Wien 97 II^a (1888), p. 1505.

620) Sitzgsb. Akad. Wien 101 II^a (1892), p. 415.

621) Sitzgsb. Akad. Berlin 1891, p. 1085; voir déjà Monatsb. Akad. Berlin 1859, p. 758; id. 1868, p. 428. Les résultats obtenus par *K. Weierstrass* ont été exposés par *C. Bourlet*, Ann. Ec. Norm. (3) 12 (1895), p. 317.

622) Bull. sc. math. (2) 15 (1891), p. 236; Leçons nouvelles sur l'Analyse infin. 2, Paris 1895, p. 13.

623) Commentat. Soc. Gott. recent. 3 (1814/5), éd. Göttingue 1816, math., mém. n° 4, p. 107; Werke 3, Göttingue 1876, p. 33.

entière quelconque donnée $f(z)$ et sa dérivée $f'(z)$ aient un diviseur commun est que le discriminant de $f(z)$ s'annule, et il l'établit[624]) *sans supposer l'existence des zéros de* $f(z)$. C'est en s'appuyant sur ce théorème que *C. F. Gauss* a donné sa seconde démonstration du théorème fondamental de l'Algèbre. Cette démonstration elle-même consiste à prouver que la solution d'une équation quelconque à coefficients réels dont le degré est un nombre *pair* de la forme

$$2^\mu(2h+1) \qquad (\mu \geqq 1)$$

se ramène à la solution d'une autre équation à coefficients réels de degré

$$2^\nu(2k+1)$$

où $\nu < \mu$. De proche en proche, en appliquant le même procédé on arrive à une équation de degré impair à coefficients réels.

Sur les mêmes principes sont fondées les démonstrations de *K. G. Chr. von Staudt*[625]), de *P. Gordan*[626]), de *Gy.* (*J.*) *König*[627]), de *E. Netto*[628]), de *Ch. Brisse*[629]), de *K. Th. Vahlen*[630]) et celle que *L. Kronecker* a exposée en 1870/1 dans son Cours professé à l'Université de Berlin[631]).

*La démonstration de *F. Walecki*[632]) se rattache à celle de *W. K. Clifford*[633]).*

Toutes ces démonstrations permettent de conclure, de l'existence de racines des équations de degré $(2m+1)2^\nu$ où m est un nombre naturel quelconque inférieur à un nombre déterminé n et où ν est l'un quelconque des nombres $0, 1, 2, \cdots$ inférieurs ou égaux à un

624) Voir à ce sujet *J. Molk*, Thèse, Paris 1884; Acta math. 6 (1885), p. 22.

625) J. reine angew. Math. 29 (1845), p. 97.

626) Math. Ann. 10 (1876), p. 572; Invar.[106]) 1, p. 166; en ce qui concerne les Vorlesungen la remarque de *F. von Dalwigk* [Math. Ann. 34 (1889), p. 158] est sans objet; la lacune signalée dans l'article de 1876 pouvait d'ailleurs être comblée en quelques mots. Voir aussi *E. B. Elliott*, Proc. London math. Soc. (1) 25 (1893/4), p. 173.

627) Math. Ann. 15 (1879), p. 161.

628) J. reine angew. Math. 88 (1880), p. 14 [1879].

629) J. Ec. polyt. (1) cah. 56 (1886), p. 163.

630) Acta math. 21 (1897), p. 287.

631) Festschrift[481]) § 13; J. reine angew. Math. 92 (1882), p. 42; Werke 2, p. 294.

632) *C. R. Acad. sc. Paris 96 (1883), p. 772; Nouv. Ann. math. (3) 2 (1883), p. 241.*

633) *Proc. Cambr. philos. Soc. 2 (1864/76), p. 156 [1870]; Papers, Londres 1882, p. 20.*

nombre fini déterminé, à l'existence de racines des équations de degré $(2n+1)\,2^{\nu+1}$. Le cas général est ainsi ramené au cas où le degré de $f(z)$ est un nombre *impair* sans que l'on fasse appel à la notion de continuité.

Toute cette partie de la démonstration a un caractère purement arithmétique au sens de *L. Kronecker.* Elle est nettement séparée de la partie *transcendante* de la question [selon l'expression de *P. Gordan* [634])]; elle revient en somme à démontrer que toute équation a une racine du moment que le théorème est admis pour une équation à coefficients réels de degré impair.

La partie transcendante de la question consiste ensuite à démontrer que toute équation de degré impair a au moins une racine.

86. Troisième démonstration de Gauss. La troisième démonstration de *C. F. Gauss* [635]) s'appuie sur des considérations de calcul intégral [636]).

*Supposons que les coefficients $a_1, a_2, \ldots, a_n$ d'une fonction rationnelle entière de la variable complexe z, de degré n,

$$f(z) = z^n + a_1 z^{n-1} + a_2 z^{n-2} + \cdots + a_n$$

soient réels. Désignons par r la valeur absolue et par φ l'argument de z en sorte que

$$z = r\,(\cos\varphi + i\sin\varphi);$$

soient alors $t(r,\varphi)$ la partie réelle et $u(r,\varphi)$ le coefficient de i dans la partie purement imaginaire de $f(z)$, en sorte que

$$f(z) = t(r,\varphi) + iu\,(r,\varphi).$$

Pour abréger l'écriture désignons aussi par t_1, u_1, y les valeurs communes des expressions

$$t_1 = r\frac{\partial t}{\partial r} = \frac{\partial u}{\partial \varphi}$$

$$u_1 = r\frac{\partial u}{\partial r} = -\frac{\partial t}{\partial \varphi}$$

$$y = \frac{\partial}{\partial \varphi}\left[\frac{tu_1 - ut_1}{r(t^2+u^2)}\right] = \frac{\partial}{\partial r}\left[\frac{tt_1 + uu_1}{t^2+u^2}\right].$$

634) Invar. [106]) 1, p. 116.

635) Commentat. Soc. Gott. recent. 3 (1814/5), éd. Göttingue 1816, math., mém. n° 5, p. 135; Werke 3, Göttingue 1876, p. 59. Cette démonstration est légèrement modifiée par *M. Bôcher,* Amer. J. math. 17 (1895), p. 266; Bull. Amer. math. Soc. 1 (1894/5), p. 205.

636) Les quatre démonstrations de *C. F. Gauss* (la quatrième est celle de 1849, cf. n° **82**) ont été publiées en allemand par *E. Netto* [Ostwalds Klassiker der exakten Wiss. n° 14, Leipzig 1890].

Enfin envisageons, dans le plan de la variable z, un cercle de centre O et de rayon R arbitrairement fixé.

Si l'expression

$$t^2 + u^2$$

ne s'annulait pour aucun point situé à l'intérieur de ce cercle (C), l'intégrale double étendue à toute l'aire de (C) serait finie, déterminée et aurait une valeur égale à chacune des deux intégrales itérées

$$\int_{r=0}^{r=R} dr\left[\int_{\varphi=0}^{\varphi=2\pi} y\,d\varphi\right],\quad \int_{\varphi=0}^{\varphi=2\pi} d\varphi\left[\int_{r=0}^{r=R} y\,dr\right].$$

Or en évaluant directement chacune de ces deux intégrales itérées on trouve que la première a une valeur nulle quel que soit R, tandis que, pour des valeurs de R plus grandes que le plus grand des nombres

$$\alpha_1,\ \sqrt{\alpha_2},\ \sqrt[3]{\alpha_3},\ \ldots,\ \sqrt[n]{\alpha_n},$$

où

$$\alpha_1 = n\sqrt{2}\,|\,a_1\,|,\quad \alpha_2 = n\sqrt{2}\,|\,a_2\,|,\ \ldots,\ \alpha_n = n\sqrt{2}\,|\,a_n\,|,$$

la seconde des intégrales itérées a une valeur positive.

Pourvu que le rayon R du cercle (C) soit fixé suffisamment grand, il faut donc qu'en un point z au moins, situé dans ce cercle (C), l'expression t^2+u^2 s'annule et que par suite $f(z)$ s'annule.*

De cette troisième démonstration de *C. F. Gauss* on peut rapprocher celle de *T. J. Stieltjes* [637]). Les démonstrations de *C. F. Gauss* et *T. J. Stieltjes* ont été exposées par *G. Loria* [638]).

*Une autre démonstration très simple fondée sur les principes de la théorie des fonctions analytiques, mais rentrant au fond dans le même ordre d'idées que la troisième démonstration de *C. F. Gauss,* a été donnée par *K. Weierstrass* [639]) dans ses Cours professés à l'Université de Berlin. Toute fonction rationnelle entière $f(z)$ a pour $z=\infty$ un pôle; en d'autres termes $\frac{1}{f(z)}$ est une fonction analytique *régulière* aux environs du point analytique $z=\infty$; mais une fonction analytique qui ne se réduit pas à une constante ne peut être régulière aux environs de chaque point analytique du plan des z; la

637) Nieuw Archief voor Wiskunde (1) 9 (1882), p. 196.

638) Rivista mat. 1 (1891), p. 220/2. Voir déjà *L. Kronecker,* Monatsb. Akad. Berlin 1878, p. 151/2; Werke [189]) 2, p. 79/82.

639) *Cette démonstration se trouve sous une forme un peu différente dans *O. Biermann,* Theorie der analyt. Funct., Leipzig 1887, p. 34. (Texte et note de *G. Vivanti*).*

fonction analytique $\frac{1}{f(z)}$ aura donc au moins un point singulier a à distance finie. Ce point singulier a de $\frac{1}{f(z)}$ ne peut être qu'un pôle puisque la fonction rationnelle entière $f(z)$ est régulière aux environs de tout point fini z. Donc $f(z)$ s'annule pour $z = a$.*

87. Deuxième démonstration de Cauchy. Tout autre est le point de départ et le fondement de la seconde démonstration de *A. L. Cauchy* [640]) qui établit le moyen de calculer le nombre des zéros de la fonction $f(z)$ inclus dans une aire donnée [641]).

Si dans le plan des x, y on envisage un contour fermé simplement connexe (C) et qu'un observateur parcoure ce contour (C) dans un sens tel que l'intérieur de (C) soit toujours à sa gauche, le nombre de fois que le quotient $\frac{\varphi(x, y)}{\psi(x, y)}$ s'annule en passant des valeurs positives aux valeurs négatives, diminué du nombre de fois que ce même quotient s'annule en passant des valeurs négatives aux valeurs posives, est égal au double du nombre des racines de l'équation

$$f(x + iy) = \varphi(x, y) + i\psi(x, y) = 0$$

situées à l'intérieur du contour (C). Par un choix convenable du contour (C) on déduit aisément de ce théorème une démonstration du théorème fondamental de l'Algèbre. Cette démonstration suppose évidemment la notion analytique du continu [642]).

Il faut rapprocher de cette démonstration de *A. L. Cauchy* celles de *J. Ch. F. Sturm* et *J. Liouville* [643]), *de *C. Ullherr* [644]), de *A. de Morgan* [645]), de *G. B. Airy* [646]), de *J. Sokotski* [647]), de *C. A. Laisant* [648]), de *G. Lery* [649]), de *E. Pomey* [650]).*

---

640) Le mémoire de *A. L. Cauchy* a été lithographié à Turin, le 27 septembre 1831; voir aussi J. Ec. polyt. (1) cah. 25 (1837), p. 176; Œuvres (2) 1, Paris 1905, p. 416. A propos de cette démonstration de *A. L. Cauchy*, voir *J. Ch. F. Sturm* et *J. Liouville*, J. math. pures appl. (1) 1 (1836), p. 278, 290.

641) Cf. *F. N. M. Moigno,* J. math. pures appl. (1) 5 (1840), p. 75.

642) On doit à *F. Rudio* [Viertelj. Naturf. Ges. Zürich 39 (1894), p. 345] une remarque signalant une lacune dans cette démonstration.

643) J. math. pures appl. (1) 1 (1836), p. 278.

644) *J. reine angew. Math. 31 (1846), p. 231.*

645) *Trans. Cambr. philos. Soc. 10, I (1858), p. 261 [1857].*

646) *Id. 10, I (1858), p. 283 [1858].*

647) *Rozwiczywanie równán liczebnyck, Varsovie 1884; cette démonstration est exposée par *G. Loria*, Rivista mat. 1 (1891), p. 185.*

648) *Bull. Soc. math. France 15 (1886/7), p. 42; J. math. spéc. (3) 3 (1889), p. 77.*

649) *Nouv. Ann. math. (4) 5 (1905), p. 385/7.*

650) *Id. p. 388/94.*

*Citons ici une démonstration de *A. Cayley* [651]).

La démonstration de *Ch. A. A. Briot* et *J. C. Bouquet* [652]) repose sur l'étude de la variation éprouvée par l'argument d'une fonction d'une variable complexe quand la variable décrit une ligne donnée. Elle se rattache donc au théorème fondamental de *A. L. Cauchy* sur lequel on peut faire reposer toute la théorie des fonctions.

On peut citer encore *E. Carvallo* [653]), *E. Jablonski* [654]), *E. Guitton* [655]) *A. V. Jamet* [656]), et l'exposé de la démonstration de *Ch. A. A. Briot* et *J. C. Bouquet* par *Fleurot* [657]).*

88. Démonstrations de Mourey, Collins etc. *Une démonstration géométrique très curieuse du théorème fondamental de l'Algèbre a été donnée par *C. V. Mourey* [658]) qui ramène la question à prouver que le problème suivant admet une solution: Étant donnés en position n points $a_1, a_2, \ldots, a_n$ dans un plan, trouver dans ce plan un point A tel que le produit géométrique des vecteurs $a_1A, a_2A, \ldots, a_nA$ soit équipollent à un vecteur donné (dans le même plan). Si l'on représente ce vecteur donné par $\varrho e^{i\omega}$ et les vecteurs a_kA par $\varrho_k e^{i\omega_k}$, où $\omega, \omega_1, \omega_2, \ldots, \omega_n, \varrho, \varrho_1, \varrho_2, \ldots, \varrho_n$ sont réels et $\varrho > 0, \varrho_1 > 0, \varrho_2 > 0, \ldots, \varrho_n > 0$, cela revient à faire voir qu'il est toujours possible de satisfaire aux deux conditions [659])

$$\varrho_1\varrho_2 \ldots \varrho_n = \varrho, \quad \omega_1 + \omega_2 + \cdots + \omega_n \equiv \omega \pmod{2\pi}.$$

La démonstration de *E. B. Holst* [660]) a de grandes ressemblances avec celle de *C. V. Mourey* ainsi que l'a constaté *G. Loria* [661]). Il en est de même de celle de *F. Mangeot* [662]).

Citons ici parmi les démonstrations de caractère géométrique celles de *H. Hocks* [663]), *L. Woodhouse* [664]), *K. Küpper* [665]).*

---

651) *Trans. Cambr. philos. Soc. 12 II (1879), p. 395 [1874]; Papers 9, Cambridge 1896, p. 21.*

652) *Théorie des fonctions elliptiques, (2e éd.) Paris 1875, p. 22.*

653) *Nouv. Ann. math. (3) 10 (1891), p. 109.*

654) *Id. (3) 12 (1893), p. 301.*

655) *J. math. spéc. (4) 2 (1893), p. 180.*

656) *Mathesis (2) 4 (1894), p. 5; Nouv. Ann. math. (3) 14 (1895), p. 437/42.*

657) *J. math. spéc. (4) 4 (1895), p. 145.*

658) *La vraie théorie des quantités négatives et des quantités prétendues imaginaires, (1re éd.) Paris 1828; (2e éd.) Paris 1861.*

659) *Cf. *J. Liouville*, J. math. pures appl. (1) 4 (1839), p. 501; (1) 5 (1840), p. 31.*

660) *Acta math. 8 (1886), p. 155; Forhandlinger Videnskabs-Selskabet Christiania 1886, éd. 1887, mém. n° 1.*

661) *Acta math. 9 (1886/7), p. 71/2.*

662) *J. math. spéc. (3) 3 (1889), p. 121, 162.*

663) *Z. Math. Phys. 28 (1883), p. 123 avec une remarque de *F. von Dalwigk* [id. 34 (1889) p. 185].*

*Certaines tentatives de démonstration sont basées sur la transformation de l'équation proposée; c'est le cas, par exemple, de celle de *A. Burg*[666]), reproduite plus tard par *L. Matthiessen*[667]) quoiqu'elle ne soit pas très heureuse; c'est aussi le cas de celle de *J. Macnie*[668]) et de celle de *J. C. Malet*[669]).

E. Collins[670]) a eu l'idée de réduire la recherche des racines d'une équation à la recherche d'un trinome du second degré qui divise le premier membre de l'équation. Cette même idée a guidé *Ch. Jourjon*[671]) qui, pour éviter les imaginaires, se sert des «clefs algébriques» de *A. L. Cauchy*[672]).

Il y a lieu de signaler une démonstration très simple donnée par *H. G. Zeuthen*[673]).*

E. Phragmén[674]) se sert simplement de la divisibilité des polynomes, en introduisant deux séries de fonctions définies algébriquement par voie récurrente.

Pour *F. Mertens*[675]), qui adopte un point de vue purement arithmétique au sens de *L. Kronecker*, une racine existe dès qu'on a une méthode pour déterminer une valeur complexe *rationnelle* de z qui rende $|f(z)|$ aussi petit qu'on voudra. *D. Hilbert*[676]) critique à la fois cette définition de l'existence d'une racine et la définition de *L. Kronecker* (n° **80**).

*Nous citerons seulement les démonstrations plus ou moins originales et de valeurs très inégales de *P. Franchini*[677]), *K. Hubbe*[678]), *F. Deahna*[679]), *A. Faure*[680]), *A. von Ettinghausen*[681]), *A. Cayley*[682]), *N. V. Bugajev*[683]), *V. Valeriani*[684]), *A. Schmitz*[685]), *G. Kreuzberg*[686]), *L. Gérard*[687]), *F. Giudice*[688]), *T. Takagi*[689]), *C. A. dell'Agnola*[690]).

Comme type même de cercle vicieux, on peut citer l'essai de démonstration de *J. B. E. Dubourguet*[691]).*

664) *Jornal sciencias math. astr. (Coïmbre) 6 (1885), p. 177/82.*

665) *Časopis math. fys. (Prague) 14 (1885), p. 28.*

666) *Jahrb. Polyt. Inst. Wien 17 (1832), p. 141. Voir aussi Lehrb.[614]) 1, p. 57/69.*

667) *Grundzüge der antiken und modernen Algebra, Leipzig 1878, p. 11.*

668) *The Analyst (Des Moines) 5 (1878), p. 80/2.*

669) *Trans. Irish Acad. 26 (1879), p. 453 [1878].*

670) *J. reine angew. Math. 18 (1838), p. 119.*

671) *La divisibilité des fonctions entières démontrée sans les imaginaires, Paris 1886.*

672) *C. R. Acad. sc. Paris 36 (1853), p. 70, 129, 161; id. 37 (1853), p. 38, 57; Œuvres (1) 11, Paris 1899, p. 439; (1) 12, Paris 1900, p. 12, 21, 46, 54.*

673) *Nyt Tidsskrift mat. Köbenhavn (Copenhague) Afd. B. 1 (1890), p. 65 *

674) Öfversigt Vetensk. Akad. förhandl. (Stockholm) 48 (1891), p. 113. Voir aussi *D. Selivanov,* Bull. Soc. math. France 13 (1884/5), p. 119.

675) Monatsh. Math. Phys. 3 (1892), p. 293.

676) Jahrb. Fortsch. Math. 24 (1892), p. 87.

677) *Saggi di algebra transcendente e di meccanica [Mem. mat. fis. Soc. ital. delle scienze (1) 16 (1813), p. 223] (Note de *G. Vivanti*).*

678) *Rocznik Uniwers. Krakowsk. (Cracovie) 3 (1818), p. 92/115.*

Réductibilité; irréductibilité.

89. Réductibilité dans le domaine des nombres rationnels. D'après le théorème fondamental de l'Algèbre, toute fonction rationnelle entière d'une variable

$$f(z) = a_0 z^n + a_1 z^{n-1} + \cdots + a_{n-1} z + a_n,$$

de degré $n > 1$, peut être mise sous la forme

$$f(z) = a_0 (z - z_1)(z - z_2) \cdots (z - z_n),$$

où $z_1, z_2, \ldots, z_n$ sont des nombres complexes (réels ou imaginaires); elle est donc *décomposable* ou *réductible* au sens que nous avons donné à ce mot (n° **3**). Mais dans un grand nombre de recherches il importe de savoir si une fonction rationnelle entière donnée peut être mise sous la forme d'un produit de fonctions rationnelles entières *dont les coefficients satisfont à certaines conditions déterminées.* Ainsi il peut y avoir intérêt à savoir si une fonction rationnelle entière à coefficients *réels* est décomposable, ou non, en fonctions rationnelles entières ayant des coefficients *réels.* Pour les fonctions d'une variable, à coefficients réels, le théorème fondamental indique que ces fonctions

679) *J. reine angew. Math. 20 (1840), p. 337.*

680) *Essai sur la théorie et l'interprétation des quantités dites imaginaires 1, Paris 1845.*

681) *Sitzgsb. Akad. Wien 5 II (1850), p. 31/7.*

682) *London, Edinb., Dublin philos. mag. (4) 18 (1859), p. 436; Papers 4, Cambridge 1891, p. 116.*

683) *Věstnik matem. nauk (Messager des sc. math. Vilna) 1 (1862), p. 118.*

684) *Giorn. mat. (1) 13 (1875), p. 33.*

685) *Blätter für das bayr. Gymnasialschulwesen 21 (1885), p. 47/9.*

686) *Diss. Bonn 1896.*

687) *Bull. math. spéc. 4 (1897/8), p. 45/7.*

688) *Rend. Circ. mat. Palermo 16 (1902), p. 180.*

689) *Tōkyō Sūgaku-Buturigaku kwai Hōkoku 1, n° 9 (1902), p. 56/8.*

690) *Atti Ist. Veneto (8) 8 II (1905/6), p. 551/6 (Note de *G. Loria*).*

691) *Ann. mat. pures appl. 2 (1811/2), p. 338/40. Voir d'ailleurs la critique que *J. J. Bret* [id. 3 (1812/3), p. 33] fait de cette démonstrations et les réponses de *J. B. E. Dubourguet.*

peuvent être décomposées en facteurs du premier ou du second degré, en sorte que le problème ne diffère guère de celui de la recherche générale des racines d'une équation algébrique à coefficients quelconques.

La condition nécessaire et suffisante pour qu'une de ces fonctions du second degré

$$ax^2 + bx + c$$

soit décomposable en facteurs réels du premier degré est que les coefficients a, b, c vérifient l'inégalité

$$4ac - b^2 \leqq 0.$$

Quand ces coefficients vérifient l'inégalité

$$4ac - b^2 > 0$$

la fonction $ax^2 + bx + c$ est *irréductible dans le domaine des nombres réels.*

Mais il peut aussi y avoir intérêt à savoir si une fonction rationnelle entière à coefficients *rationnels* (ou même *entiers*) est décomposable, ou non, en fonctions rationnelles entières ayant des coefficients *rationnels* (ou *entiers*). Lorsqu'on se place au point de vue purement arithmétique de *L. Kronecker* (I 3, **10**) cette question est de la plus haute importance. Au point de vue pratique des applications de l'Algèbre il est d'ailleurs non moins important de pouvoir résoudre cette question directement.

Lorsqu'une fonction rationnelle entière

$$f(z) = a_0 z^n + a_1 z^{n-1} + \cdots + a_{n-1} z + a_n,$$

dont les coefficients $a_0, a_1, \ldots, a_{n-1}, a_n$ sont des *nombres rationnels*, peut être mise sous la forme d'un produit $f_1(z) f_2(z)$ de fonctions rationnelles entières de z *à coefficients rationnels*, on dit que la fonction $f(z)$ est *réductible dans le domaine des nombres rationnels* et que chacun des facteurs $f_1(z)$, $f_2(z)$ est un *véritable diviseur*[692]) de $f(z)$. Dans le cas contraire, où la fonction $f(z)$ ne peut pas être mise sous la forme d'un produit de deux fonctions rationnelles entières de z, à coefficients rationnels, la fonction $f(z)$ est dite *irréductible dans le domaine des nombres rationnels.*

Si $f_1(z)$ est un diviseur de $f(z)$ dans le domaine des nombres rationnels, le produit $cf_1(z)$ de $f_1(z)$ par un nombre rationnel quelconque c est aussi un diviseur de $f(z)$. Tous les diviseurs $cf_1(z)$ qui ne diffèrent que par la valeur attribuée au nombre rationnel c sont dits *équivalents* et on ne les envisage pas ici comme distincts.

692) *Si c est un nombre rationnel, $f_1 = c$, $f_2 = \frac{1}{c} f(z)$ ne sont pas de *véritables diviseurs* de $f(z)$; ces types de pseudo-diviseurs sont ici exclus.*

Lorsqu'une fonction rationnelle entière $f(z)$ dont les coefficients sont des *nombres rationnels entiers* peut être mise sous la forme d'un produit $f_1(z) f_2(z)$ de fonctions rationnelles entières *à coefficients entiers*, on dit que la fonction $f(z)$ est *réductible dans le domaine des nombres (rationnels) entiers* et que chacun des facteurs $f_1(z)$, $f_2(z)$ est un véritable diviseur de $f(z)$. Cette définition subsiste si l'un des deux facteurs $f_1(z)$, $f_2(z)$ se réduit à un nombre entier autre que ± 1. Dans le cas contraire où la fonction $f(z)$ ne peut être mise ni sous la forme d'un produit de deux fonctions rationnelles entières de z à coefficients entiers, ni sous celle du produit d'une fonction rationnelle entière à coefficients entiers par un nombre entier différant de $+1$ et de -1, on dit que la fonction $f(z)$ est *irréductible dans le domaine des nombres (rationnels) entiers.*

Si $f_1(z)$ qui peut se réduire à un nombre entier est un diviseur de $f(z)$ dans le domaine des nombres (rationnels) entiers il en est de même de $-f_1(z)$. On dit que $f_1(z)$ et $-f_1(z)$ sont des diviseurs *équivalents* de $f(z)$ et on ne les envisage pas ici comme distincts.

La notion d'équivalence est donc toute autre suivant que le domaine dans lequel on effectue la décomposition de $f(z)$ est celui des nombres rationnels ou celui des nombres entiers.

Dans le domaine des nombres rationnels à chaque diviseur correspondent une infinité de diviseurs équivalents; dans le domaine des nombres (rationnels) entiers à chaque diviseur $f_1(z)$ ne correspond que le seul diviseur équivalent $-f_1(z)$.

Tandis qu'il n'y a pas de fonction rationnelle entière d'une variable, de degré plus grand que 1, qui soit *absolument* irréductible (n° **3**), il y a des fonctions rationnelles entières d'une variable, de degré plus grand que 1, qui sont irréductibles dans le domaine des nombres rationnels ou dans le domaine des nombres (rationnels) entiers.

C. F. Gauss[693]) a montré que, si une fonction rationnelle entière d'une variable à coefficients (rationnels) entiers est réductible dans le domaine des nombres rationnels, elle est aussi réductible dans le domaine des nombres (rationnels) entiers. A l'aide de ce théorème on peut toujours ramener la détermination, dans le domaine des nombres rationnels, des diviseurs d'une fonction rationnelle entière à coefficients rationnels, à la détermination, dans le domaine des nombres (rationnels) entiers, des diviseurs d'une fonction rationnelle entière à coefficients (rationnels) entiers.

693) Disq.[25]) n^os^ 42, 226; Werke 1, p. 34, 226. Voir aussi *H. Weber*, Alg.[24]) 1, p. 27; trad. *J. Griess* 1, p. 27.

L. Kronecker [694]) a donné une méthode qui permet de reconnaître si une fonction rationnelle entière $f(z)$ à coefficients rationnels entiers donnés est réductible ou irréductible dans le domaine des nombres entiers.

Au point de vue de *L. Kronecker* (I 3, **10**) la *définition* de l'irréductibilité des fonctions rationnelles entières (dont les coefficients sont des nombres rationnels) en d'autres termes la *distinction* entre fonctions rationnelles entières (à coefficients rationnels) réductibles et fonctions rationnelles entières (à coefficients rationnels) irréductibles n'est d'ailleurs légitime (en mathématiques) que parce qu'on peut établir une méthode permettant de concevoir au moins la possibilité de distinguer, après un nombre *fini* d'opérations réalisables, si une fonction rationnelle entière (à coefficients rationnels) donnée rentre dans le type réductible ou dans le type irréductible [695]). Les seules opérations réalisables sont d'ailleurs celles qui se ramènent à un nombre *fini* d'additions, de soustractions, de multiplications et de divisions.

La méthode de *L. Kronecker* ne suppose naturellement pas connu le théorème fondamental (n° **80**) de l'Algèbre.

Si $F(x)$ désigne une fonction rationnelle entière de degré donné n et dont les coefficients sont des nombres (rationnels) entiers donnés, il s'agit de montrer que l'on peut former un nombre *fini* de fonctions rationnelles entières $f(x)$ à coefficients (rationnels) entiers hors desquelles il ne saurait y avoir de diviseurs, à coefficients (rationnels) entiers, de $F(x)$.

On peut d'abord observer que, si n est un nombre pair $2m$ ou un nombre impair $2m+1$, il suffit d'envisager les fonctions $f(x)$ de degrés $\leqq m$, car si l'on peut former un tableau de telles fonctions hors desquelles il ne saurait y avoir de diviseur (à coefficients rationnels entiers) de $F(x)$, de degrés $\leqq m$, il est aisé d'en déduire, en divisant successivement $F(x)$ par chacune des fonctions de ce tableau, le tableau des fonctions $f(x)$ hors desquelles il ne saurait y avoir de diviseur de $F(x)$ de degré $> m$.

Désignons par $\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_m$ des nombres (rationnels) entiers *arbitrairement fixés,* formons le produit

$$\varphi(x) = (x-\alpha_0)\ (x-\alpha_1)\ (x-\alpha_2)\ \ldots\ (x-\alpha_m)$$

et les $m+1$ fonctions rationnelles entières

$$g_i(x) = \frac{\varphi(x)}{(x-\alpha_i)\ \varphi'(\alpha_i)} \qquad (i = 0, 1, 2, \ldots, m).$$

694) Festschr. [481]) § 4; J. reine angew. Math. 92 (1882), p. 11; Werke 2, p. 257; voir aussi *J. Molk,* Thèse, Paris 1884, Acta math. 6 (1885), p. 11.

695) Cf. *J. Molk,* Thèse, Paris 1884; Acta math. 6 (1885), p. 8.

On sait [voir la *formule d'interpolation de Lagrange,* n° **23**] que toute fonction rationnelle entière de x à coefficients rationnels entiers dont le degré ne dépasse pas m peut être mise sous la forme

$$(1)\qquad f(x) = A_0 g_0(x) + A_1 g_1(x) + A_2 g_2(x) + \cdots + A_m g_m(x),$$

où

$$A_i = f(\alpha_i) \qquad (i = 0, 1, 2, \ldots, m).$$

Si $f(x)$ divise $F(x)$, A_i divise nécessairement $F(\alpha_i)$; or $F(\alpha_i)$ est un nombre rationnel entier qui est connu puisqu'on connaît les coefficients de $F(x)$ et qu'on a fixé α_i; un nombre *fini* d'opérations donne donc tous les A_i possibles; en répétant la même chose pour $i = 0, 1, 2, \ldots, m$ on a donc tous les diviseurs possibles de degré $\leqq m$ de la fonction $F(x)$.

*Pour déterminer les facteurs linéaires [696]) ou quadratiques, à coefficients entiers, contenus dans une fonction rationnelle entière donnée, à coefficients entiers, *G. W. Leibniz* [697]) transforme tout d'abord, par une substitution linéaire, la fonction donnée en une autre

$$a_0 x^n + a_1 x^{n-1} + \cdots + a_n$$

dont tous les coefficients $a_0, a_1, \ldots, a_n$ sont *positifs*; dans cette dernière fonction il remplace la variable x par un nombre h fixé arbitrairement parmi ceux qui sont plus grands que tous les coefficients de la fonction; il détermine ensuite tous les facteurs $H_1, H_2, \ldots$ du nombre

$$F(h) = a_0 h^n + a_1 h^{n-1} + \cdots + a_n$$

ainsi obtenu. Chacun de ces facteurs H_i peut être mis sous la forme

$$\alpha_{0i} h^{r_i} + \alpha_{1i} h^{r_i - 1} + \cdots + \alpha_{ri}$$

696) *Cette question a d'ailleurs, en fait, été abordée longtemps avant *G. W. Leibniz* et *I. Newton*, puisqu'elle est manifestement résolue dès qu'on a trouvé toutes les racines rationnelles de l'équation obtenue en égalant la fonction à zéro et que ce problème a été traité par plusieurs mathématiciens du 17ième siècle, en particulier par *J. Hudde.* Dans son „Epistola prima" intitulée De reductione aequationum [2]), écrite en 1657 [publ. en 1659 dans *F. van Schooten,* Geom. Descartes (2e éd. latine) 1, p. 407/506], *J. Hudde* enseigne [id. p. 466] un procédé pour trouver par tâtonnements les diviseurs rationnels d'une équation; il envisage l'équation

$$x^3 - 21ax^2 - (b^2 - 20a^2)x + 20ab^2 = 0$$

et trouve que le seul diviseur linéaire du premier membre est $x - 20a$.*

697) *Lettre à *J. Hermann* datée du 6 septembre 1708; Werke, éd. *C. I. Gerhardt,* Math. Schr. 4, Halle 1859, p. 335/9. Un passage de cette lettre montre clairement que *G. W. Leibniz* n'avait en vue que les fonctions rationnelles entières dont tous les zéros sont réels. Il est toutefois évident que son procédé s'applique au cas où ces zéros sont soit réels soit de la forme $-a + bi$ (où $a > 0$, $b \neq 0$) et dans tout autre cas on peut [cf. note 704] transformer la fonction donnée en une autre jouissant de cette propriété.*

où $\alpha_{0i}, \alpha_{1i}, \ldots, \alpha_{ri}$ sont des nombres positifs déterminés. Les diviseurs de la fonction à coefficients positifs se trouvent donc tous parmi les fonctions rationnelles entières de la forme

$$(1) \qquad \alpha_{0i} x^{r_i} + \alpha_{1i} x^{r_i - 1} + \cdots + \alpha_{ri} \qquad (i = 1, 2, \ldots).$$

Les coefficients $\alpha_{01}, \alpha_{02}, \ldots$ doivent d'ailleurs être des diviseurs de a_0 et les coefficients $\alpha_{r1}, \alpha_{r2}, \ldots$ doivent être des diviseurs de a_n, ce qui permet déjà d'exclure un certain nombre des fonctions rationnelles entières figurant dans le tableau (1). De plus, à chaque diviseur

$$\alpha_{0i} x^{r_i} + \alpha_{1i} x^{r_i - 1} + \cdots + \alpha_{ri}$$

de la fonction $F(x)$ doit correspondre non seulement un diviseur de $F(h)$ de la forme

$$\alpha_{0i} h^{r_i} + \alpha_{1i} h^{r_i - 1} + \cdots + \alpha_{ri}$$

mais aussi un diviseur de $F(h)$ de la forme

$$\alpha_{0k} h^{r_k} + \alpha_{1k} h^{r_k - 1} + \cdots + \alpha_{rk}$$

tel que l'on ait

$$r_i + r_k = n, \quad \alpha_{0i}\alpha_{0k} = a_0, \quad \alpha_{ri}\alpha_{rk} = a_n;$$

cette remarque permet de réduire encore sensiblement le nombre des diviseurs possibles de $F(x)$. On vérifiera enfin, en effectuant la division de $F(x)$ par chacun des diviseurs possibles restants, si chacun de ces diviseurs possibles (1) est, ou non, un diviseur effectif de $F(x)$. La substitution, inverse de la première, fournit immédiatement les diviseurs de la fonction donnée. Pour chacun de ces diviseurs on peut répéter ce qu'on vient de dire pour la fonction donnée, en sorte que l'on obtient finalement tous les diviseurs quadratiques et linéaires de la fonction donnée[698]).*

I. Newton[699]) avait aussi cherché à déterminer les facteurs *linéaires*, à coefficients entiers, contenus dans une fonction rationnelle entière donnée à coefficients entiers[699a]); il y est parvenu par un procédé[700]) qui

698) *Texte et notes 696 à 698 de *G. Eneström.**

699) Arithm. univ.[90]), Leyde 1732, p. 37/44; Opera éd. *S. Horsley* 1, Londres 1779, p. 40; trad. *N. Beaudeux* 2, Paris an X, p. 47/56.

699a) *Dans le cas où tous les facteurs linéaires sont de la forme $x + k$, un procédé, au fond absolument identique à celui de *I. Newton*, avait été indiqué, dès 1649, par *J. Waessenaer* [voir *F. van Schooten,* Geometria a Renato Descartes (1re éd. latine) Leyde 1649, p. 262/4 (Note de *G. Eneström*).*

700) **I. Newton* a exposé son procédé sans démonstration. La démonstration a été donnée en 1708 par *Nicolas Bernoulli* dans une note rédigée pour être publiée immédiatement mais qui n'a paru que dans le „Commercium philosophicum et mathematicum" de *G. W. Leibniz* et *Jean Bernoulli* 2, Lausanne et Genève 1745, p. 189/209. Une démonstration absolument identique à celle de *Nicolas Bernoulli* fut communiquée en 1708 par *J. Hermann* à *G. W. Leibniz* [Werke, éd. *C. I. Gerhardt,* Math. Schr. 4, Halle 1859, p. 329/31] (Note de *G. Eneström*).*

diffère essentiellement de celui de *G. W. Leibniz*; il a d'ailleurs essayé plus tard d'étendre ce même procédé à la recherche de facteurs de degrés quelconques et l'ordre d'idées dans lequel il se meut alors, apparaît comme identique à celui qui a guidé plus tard *L. Kronecker*[701]).

Parmi tous les nombres (rationnels) entiers A_i possibles on peut évidemment rejeter tout de suite ceux pour lesquels $f(\alpha_i)$ évalué au moyen de la formule d'interpolation (1) n'est pas un nombre entier. En utilisant cette remarque, *C. Runge*[702]) a notablement perfectionné la méthode de *L. Kronecker.* Il l'a rendue pratiquement réalisable dans tous les cas où le degré et les coefficients de la fonction donnée ne sont pas de trop grands nombres.

En s'appuyant sur le théorème fondamental de l'Algèbre, on peut d'ailleurs fixer aisément une borne supérieure pour les valeurs absolues des coefficients des facteurs irréductibles de $f(z)$; cette borne s'exprime[703]) au moyen des valeurs absolues des coefficients de $f(z)$.

M. Mandl[704]) démontre d'abord qu'au moyen d'une transformation linéaire $z = t + h$ on peut, en choisissant convenablement h, rendre positifs tous les coefficients, tant ceux de la fonction transformée

$$\varphi(t) = f(t+h) = d_0 t^n + d_1 t^{n-1} + d_2 t^{n-2} + \cdots + d_{n-1} t + d_n$$

que ceux des facteurs de décomposition; cette transformation une fois effectuée, il ramène le problème à trouver deux systèmes de nombres entiers positifs $b_0, b_1, b_2, \ldots, b_n$; $c_0, c_1, c_2, \ldots, c_n$ tels que l'on ait, pour $r = 0, 1, 2, \ldots, n$,

$$d_r = b_0 c_r + b_1 c_{r-1} + b_2 c_{r-2} + \cdots + b_r c_0.$$

En résumé on voit qu'une fonction rationnelle entière dont les coefficients sont des nombres rationnels peut toujours être décomposée dans le domaine des nombres rationnels en un produit de facteurs irréductibles. De même une fonction rationnelle entière dont les coefficients sont des nombres (rationnels) entiers peut toujours être décomposée, dans le domaine des nombres (rationnels) entiers, en un produit de facteurs irréductibles[705]).

701) *Festschrift[481]), § 4; J. reine angew. Math. 92 (1882), p. 11; Werke 2, p. 257.*

702) J. reine angew. Math. 99 (1886), p. 89 [1884]. Voir aussi *F. Mertens* Sitzgsb. Akad. Wien 97 IIa (1888), p. 618.

703) *C. Runge,* J. reine angew. Math. 99 (1886), p. 93, 94.

704) J. reine angew. Math. 113 (1894), p. 252; Jahresb. deutsch. Math.-Ver. 4 (1894/5), éd. 1897, p. 95.

705) Cf. *H. E. Heine,* J. reine angew. Math. 48 (1854), p. 267. Consulter aussi *M. L. Maleyx*, Nouv. Ann. math. (2) 14 (1875), p. 97; *H. F. Talbot,* Trans. R. Soc. Edinb. 27 (1876), p. 303/12; *V. Murer,* Periodico mat. (1) 2 (1886/7), p. 72; *P. J. E. Finck,* J. math. pures appl. (1) 10 (1845), p. 171.

Il est essentiel d'observer[706]) que cette décomposition d'une fonction rationnelle entière d'une variable est *univoque* si l'on convient de ne pas envisager comme distincts, dans le domaine des nombres rationnels, deux facteurs dont le quotient est un nombre rationnel et, dans le domaine des nombres (rationnels) entiers, deux facteurs dont le quotient est égal à -1. C'est ce théorème qui donne aux facteurs irréductibles de la fonction rationnelle entière le caractère de *facteurs premiers.*

90. Théorème d'Eisenstein. Généralisations. *G. Eisenstein*[707]) a démontré que, si les coefficients $a_1, a_2, \ldots, a_{n-1}, a_n$ d'une fonction rationnelle entière

$$f(z) = z^n + a_1 z^{n-1} + a_2 z^{n-2} + \cdots + a_{n-1} z + a_n$$

sont des nombres entiers divisibles par le nombre premier p et si a_n n'est pas divisible par p^2, la fonction $f(z)$ est irréductible dans le domaine naturel d'intégrité.

E. Netto[708]) a généralisé ce théorème en démontrant que toute fonction rationnelle entière de la forme

$$z^{2k+1} + \gamma_1 p z^{2k} + \cdots + \gamma_k p z^{k+1} + \gamma_{k+1} p^2 z^k + \cdots + \gamma_{2k+1} p^2,$$

où $\gamma_1, \ldots, \gamma_k, \gamma_{k+1}, \ldots, \gamma_{2k+1}$ désignent des nombres entiers dont le dernier γ_{2k+1} n'est pas divisible par le nombre premier p, est irréductible. Il a aussi démontré que, si une fonction rationnelle entière de la forme

$$z^{2k+2} + \gamma_1 p z^{2k+1} + \cdots + \gamma_{k+1} p z^{k+1} + \gamma_{k+2} p^2 z^k + \cdots + \gamma_{2k+2} p^2,$$

où γ_{2k+2} n'est pas divisible par p, est réductible, elle ne peut se décomposer qu'en deux facteurs irréductibles, chacun de degré égal à $k+1$.

On peut même aller plus loin et démontrer que, si tous les coefficients $a_1, a_2, \ldots, a_{n-1}, a_n$ d'une fonction rationnelle entière

$$f(z) = z^n + a_1 z^{n-1} + a_2 z^{n-2} + \cdots + a_{n-1} z + a_n$$

sont divisibles par un nombre premier p et si a_{n-1} n'est pas divisible par p^2, la fonction rationnelle entière $f(z)$, si elle n'est pas irréductible, n'admet certainement qu'un facteur du premier degré et un facteur irréductible de degré $n-1$.

706) Cf. *J. Molk*, Thèse, Paris 1884; Acta math. 6 (1885), p. 12.

707) J. reine angew. Math. 39 (1850), p. 160. *Ce théorème se déduit d'ailleurs immédiatement d'un théorème sur les congruences dû à *Th. Schönemann* [J. reine angew. Math. 32 (1846), p. 100].*

708) Alg.[23]) 1, p. 61; Math. Ann. 48 (1897), p. 81; Oberhess. Ges.[418]) 31 (1896), p. 113.

Dans ses recherches sur l'irréductibilité, *L. Königsberger*[709]) part d'une certaine *surface de Riemann* évidemment indécomposable et cherche tout d'abord la forme de l'équation $f(x, y) = 0$ qui définit la fonction algébrique y correspondant à cette *surface de Riemann*; la fonction $f(x, y)$ ne pouvant être décomposée en fonctions rationnelles entières de y dont les coefficients soient des fonctions rationnelles entiè es de x, sa forme permet à *L. Königsberger* de déduire par analogie la forme des fonctions rationnelles entières à coefficients entiers qu'il prévoit devoir être irréductibles et dont il démontre ensuite directement l'irréductibilité.

Ainsi, en désignant par $[h]$ le plus grand entier contenu dans le nombre positif h, on trouve que la fonction rationnelle entière de z

$$\begin{aligned} a_0 z^n &+ p^{\left[\frac{r}{n}\right]+1} \cdot a_1 \cdot z^{n-1} \\ &+ p^{\left[\frac{2r}{n}\right]+1} \cdot a_2 \cdot z^{n-2} \\ &+ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ &+ p^{\left[\frac{(n-1)r}{n}\right]+1} \cdot a_{n-1} z \\ &+ p^r \cdot a_n, \end{aligned}$$

où p est un nombre premier, où r est premier avec n, où enfin ni a_0 ni a_n ne sont divisibles par p, est irréductible, comme est irréductible la fonction rationnelle entière de y

$$\begin{aligned} y^n F_0(x) &+ y^{n-1}(x-\alpha)^{\left[\frac{r}{n}\right]+1} F_1(x) \\ &+ y^{n-2}(x-\alpha)^{\left[\frac{2r}{n}\right]+1} F_2(x) \\ &+ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ &+ y(x-\alpha)^{\left[\frac{(n-1)r}{n}\right]+1} F_{n-1}(x) \\ &+ (x-\alpha)^r F_n(x), \end{aligned}$$

où $F_0(x), F_1(x), \ldots, F_n(x)$ sont des fonctions rationnelles entières de x à coefficients entiers, les fonctions $F_0(x)$ et $F_n(x)$ ne s'annulant d'ailleurs pas quand on y remplace x par le nombre entier α.

L. Königsberger envisage aussi le cas d'une *surface de Riemann* à n feuillets avec deux points de ramification. Il revient sur le même sujet dans un autre mémoire[710]).

709) Sitzgsb. Akad. Berlin 1894, p. 1135; J. reine angew. Math. 115 (1895), p. 53.

710) Sitzgsb. Akad. Berlin 1898, p. 737.

91. Irréductibilité de $\frac{x^n-1}{x-1}=0$ quand n est premier. Si n est premier, l'équation

$$\frac{x^n-1}{x-1}=x^{n-1}+x^{n-2}+\cdots+x+1=0$$

est irréductible dans le domaine naturel de rationalité. Une démonstration de ce théorème a été donnée par *C. F. Gauss*[711]. Une autre qui s'étend aussi au cas où n est une puissance d'un nombre premier est due à *L. Kronecker*[712], qui démontre plus généralement pour chaque nombre entier positif n l'irréductibilité de l'équation dont les racines sont les $\varphi(n)$ *racines primitives* $n^{\text{ièmes}}$ de l'unité, c'est-à-dire les nombres a pour lesquels on a

$$a^n=1$$

mais a^m différant de 1 pour tout entier positif m plus petit que n. *L. Kronecker* généralise même encore ce théorème[713].

D'autres démonstrations du même théorème ont été données par *J. A. Serret*[714], *Th. Schönemann*[715], *R. Dedekind*[716], *G. Eisenstein*[717], *F. Arndt*[718] et par *V. A. Lebesgue*[719] qui refait la démonstration de *F. Arndt.*

K. Th. Vahlen[720] démontre que dans le domaine des nombres rationnels les seuls binomes réductibles se déduisent du binome z^m-1 où m est un nombre naturel quelconque et du binome z^4+4, par la substitution de $\frac{z^n}{c}$ à la place de z, c étant un nombre rationnel et n un nombre naturel.

92. Réductibilité et irréductibilité des fonctions de plusieurs variables dans le domaine des nombres rationnels. Le théorème de *C. F. Gauss*[721], cité au n° **89**, s'étend immédiatement aux fonctions rationnelles entières d'un nombre quelconque de variables. On peut

711) Disq.[25] n° 341; Werke 1, p. 417.

712) J. reine angew. Math. 29 (1845), p. 280; J. math pures appl. (2) 1 (1856) p. 399; Werke 1, Leipzig 1895, p. 100.

713) J. math. pures appl. (1) 19 (1854), p. 177; Werke 1, Leipzig 1895, p. 77.

714) J. math. pures appl. (1) 15 (1850), p. 296.

715) J. reine angew. Math. 32 (1846), p. 93.

716) J. reine angew. Math. 54 (1857), p. 27.

717) J. reine angew. Math. 39 (1850), p. 160.

718) J. reine angew. Math. 56 (1859), p. 178 [1857].

719) J. math. pures appl. (2) 4 (1859), p. 105.

720) Acta math. 19 (1895), p. 195.

721) Disq.[25] n° 42; Werke 1, p. 34. Cf. note 693.

donc toujours ramener la détermination, dans le domaine des nombres rationnels, des diviseurs d'une fonction rationnelle entière de n variables, à coefficients rationnels, à la détermination, dans le domaine des nombres (rationnels) entiers, des diviseurs d'une fonction rationnelle entière de n variables, à coefficients (rationnels) entiers. Soit donc

$$f(z_1, z_2, \ldots, z_n)$$

une fonction rationnelle de plusieurs variables $z_1, z_2, \ldots, z_n$ ayant pour coefficients des nombres entiers. Pour reconnaître si cette fonction rationnelle entière à coefficients entiers d'un nombre quelconque de variables est réductible ou irréductible dans le domaine des nombres rationnels, posons

$$(1)\qquad z_1=t,\quad z_2=t^q,\quad z_3=t^{q^2},\quad \ldots,\quad z_n=t^{q^{n-1}},$$

ce qui transforme le monome

$$a_{h_1 h_2 \ldots h_n} z_1^{h_1} z_2^{h_2} \cdots z_n^{h_n}$$

en

$$a_{h_1 h_2 \ldots h_n} t^k$$

où

$$(2)\qquad k=h_1+h_2 q+h_3 q^2+\cdots+h_n q^{n-1}.$$

En prenant le nombre naturel q de façon que $q-1$ ne soit inférieur ni au degré de f par rapport à z_1, ni au degré de f par rapport à $z_2, \ldots,$ ni au degré de f par rapport à z_n, tous les monomes $a_{h_1 h_2 \ldots h_n} t^k$ de f, considérés comme des fonctions de t, ont des exposants k différents[722]. Les exposants k sont d'ailleurs tous inférieurs à q^n et tout nombre k inférieur à q^n peut être mis d'une seule façon sous la forme (2).

On a ainsi transformé $f(z_1, z_2, \ldots, z_n)$ en une fonction $\Phi(t)$ d'une seule variable t de degré inférieur à q^n. Si par un procédé quelconque on a déterminé un facteur $f_1(z_1, z_2, \ldots, z_n)$ de $f(z_1, z_2, \ldots, z_n)$ à coefficients rationnels, les substitutions (1) transforment ce facteur $f_1(z_1, z_2, \ldots, z_n)$ en une fonction $\Phi_1(t)$, à coefficients rationnels, qui est un diviseur de $\Phi(t)$. Inversement de cette fonction $\Phi_1(t)$ on déduit à nouveau $f_1(z_1, z_2, \ldots, z_n)$ au moyen des substitutions (1) et (2). Il suffit donc de chercher tous les diviseurs à coefficients rationnels de la fonction $\Phi(t)$ d'une seule variable t et de les transformer au moyen des substitutions (1) et (2) en fonctions $F_1, F_2, \ldots$ de $z_1, z_2, \ldots, z_n$ pour être sûr que ces dernières fonctions $F_1, F_2, \ldots,$ qui sont nécessairement en nombre *fini*, contiennent tous les diviseurs,

722) Voir *L. Kronecker,* Festschrift[481] § 4; J. reine angew. Math. 92 (1882), p. 11/2; Werke 2, p. 258.

à coefficients rationnels, de $f(z_1, z_2, \ldots, z_n)$. Mais chacune de ces fonctions $F_1, F_2, \ldots$ n'est pas nécessairement un diviseur de la fonction $f(z_1, z_2, \ldots, z_n)$ car, si la fonction en t est toujours réductible quand la fonction $f(z_1, z_2, \ldots, z_n)$ est réductible, la réciproque n'a pas toujours lieu; ainsi pour $z_1 = t$, $z_2 = t^g$ la fonction irréductible $z_1 - z_2$ se transforme en une fonction réductible $t(1 - t^{g-1})$. Après avoir obtenu tous les facteurs irréductibles de la fonction en t, il faudra donc examiner si les fonctions de $z_1, z_2, \ldots, z_n$ qui correspondent à ces facteurs irréductibles en t sont, ou non, des facteurs de la fonction $f(z_1, z_2, \ldots, z_n)$; cela n'exige d'ailleurs qu'un nombre fini d'opérations rationnelles.

Observons ici que pour obtenir un système de valeurs pour $z_1, z_2, \ldots, z_n$ tel que $f(z_1, z_2, \ldots, z_n)$ ne s'annule pas, il suffit de choisir une valeur de t pour laquelle $\Phi(t)$ ne s'annule pas et d'appliquer la substitution (1).

Ici encore la décomposition d'une fonction rationnelle entière en ses facteurs irréductibles, dans le domaine des nombres rationnels, est *univoque*[723]).

*Cette façon d'obtenir les diviseurs de $f(z_1, z_2, \ldots, z_n)$ est due à *L. Kronecker*[724]). On doit d'ailleurs encore à *L. Kronecker*[725]) une seconde méthode permettant de décider si une fonction rationnelle entière de plusieurs variables est irréductible ou non, et, si elle est réductible, de trouver ses facteurs irréductibles. Cette méthode repose sur l'emploi de la *formule d'interpolation de Lagrange* et elle est directe. Pour l'appliquer à une fonction rationnelle entière donnée

$$f(z_1, z_2, \ldots, z_{n-1}, z_n),$$

à coefficients (rationnels) entiers, nous envisagerons $f(z_1, z_2, \ldots, z_{n-1}, z_n)$ comme une fonction rationnelle entière $F(z_n)$ de z_n seulement dont les coefficients dépendent de $z_1, z_2, \ldots, z_{n-1}$ et nous chercherons les diviseurs de $F(z_n)$ dont le degré m soit inférieur au degré de la fonction $F(z_n)$. A cet effet, désignons par $\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_m$ des nombres (rationnels) entiers *arbitrairement fixés* et formons, comme au nº **89**, $m+1$ fonctions rationnelles entières d'une variable quelconque x,

723) *J. Molk,* Thèse, Paris 1884; Acta math. 6 (1885) p. 16/8; *H. Weber,* Alg.[24]) 1, p. 74; trad. *J. Griess* 1, p. 75; *E. Netto,* Alg.[27]) 2, p. 23.

724) *Festschrift[481]), § 4; J. reine angew. Math. 92 (1882), p. 10/3; Werke 2, p. 256/60.*

725) **L. Kronecker,* J. reine angew. Math. 94 (1883), p. 344; Werke 2, Leipzig 1897, p. 412; voir aussi *E. Netto,* Alg.[27]) 2, p. 17; *H. Laurent,* Nouv. Ann. math. (3) 12 (1893), p. 315.*

$$g_0(x) = \frac{\varphi(x)}{(x-\alpha_0)\,\varphi'(\alpha_0)},\ g_1(x) = \frac{\varphi(x)}{(x-\alpha_1)\,\varphi'(\alpha_1)}, \ldots, g_m(x) = \frac{\varphi(x)}{(x-\alpha_m)\,\varphi'(\alpha_m)},$$

où l'on a posé pour abréger

$$\varphi(x) = (x-\alpha_0)(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_m).$$

Toute fonction rationnelle entière $F_1(z_n)$ dont le degré, par rapport à z_n, ne dépasse pas m peut être mise sous la forme

$$(3)\quad F_1(z_n) = F_1(\alpha_0)\,g_0(z_n) + F_1(\alpha_1)\,g_1(z_n) + \cdots + F_1(\alpha_m)\,g_m(z_n).$$

Si $F_1(z_n)$ divise $F(z_n)$, $F_1(\alpha_i)$ divise nécessairement $F(\alpha_i)$, pour $i = 0, 1, 2, \ldots, m$. Or $F(\alpha_i)$ est une fonction rationnelle entière de $z_1, z_2, \ldots, z_{n-1}$ à coefficients (rationnels) entiers; si donc on sait déjà distinguer les fonctions rationnelles entières de $n-1$ variables en fonctions irréductibles et réductibles et obtenir par un nombre fini d'opérations les diviseurs de celles de ces fonctions qui sont réductibles, on obtiendra aussi par un nombre fini d'opérations les diviseurs de chacune des fonctions $F(\alpha_0), F(\alpha_1), \ldots, F(\alpha_m)$ des $n-1$ variables $z_1, z_2, \ldots, z_{n-1}$; on obtiendra donc par un nombre fini d'opérations tous les coefficients possibles $F_1(\alpha_0), F_1(\alpha_1), \ldots, F_1(\alpha_m)$ de l'expression (3) de $F_1(z_n)$. En d'autres termes on aura ainsi toutes les fonctions $F_1(z_n)$ qui *peuvent* diviser la fonction donnée $F(z_n)$ et sont de degré $\leqq m$.

Pour $n = 1$ la recherche des diviseurs d'une fonction rationnelle entière à coefficients (rationnels) entiers s'effectue à l'aide d'un nombre fini d'opérations. La méthode précédente permet donc aussi de trouver tous ces diviseurs quand $n = 2$, donc aussi quand $n = 3, \ldots$, donc aussi quand il s'agit d'une fonction rationnelle entière d'un nombre quelconque de variables, à coefficients (rationnels) entiers.

H. Hancock[726]) a étendu à la recherche des diviseurs des fonctions rationnelles entières d'un nombre quelconque de variables, à coefficients (rationnels) entiers, la méthode donnée par *M. Mandl*[704]) dans les cas des fonctions rationnelles entières d'une seule variable, à coefficients (rationnels) entiers. Il fait voir comment on peut transformer la fonction rationnelle entière donnée, à coefficients entiers, de façon que tous les coefficients deviennent des entiers *positifs*, et ce sont les fonctions rationnelles entières à coefficients entiers positifs ainsi obtenues qu'il décompose en facteurs irréductibles.*

*Une autre méthode due à *Gy. (J.) König*[727]) repose sur le théorème suivant qui est dû à *L. Kronecker*[728]) et que l'on peut énoncer, en en modifiant légèrement les termes, de la façon que voici:

726) *Ann. Éc. Norm. (3) 17 (1900), p. 89.*

727) *Alg. Grössen[20]), p. 128 (Texte et notes 727 et 728 de *J. Kürschák*).*

Soient F et G deux fonctions rationnelles entières de $z_1, z_2, \ldots, z_n$, à coefficients indéterminés $A_1, A_2, \ldots, B_1, B_2, \ldots$ Chacun des produits $Z_{ik} = A_i B_k$ de l'un des coefficients de F par l'un des coefficients de G est racine d'une équation algébrique de la forme

$$(1) \qquad Z_{ik}^{\nu} + A_{ik}^{(1)} Z_{ik}^{\nu-1} + A_{ik}^{(2)} Z_{ik}^{\nu-2} + \cdots + A_{ik}^{(\nu)} = 0$$

dont les coefficients $A_{ik}^{(1)}, A_{ik}^{(2)}, \cdots, A_{ik}^{(\nu)}$ sont des fonctions rationnelles entières (à coefficients numériques rationnels entiers) des coefficients du produit FG.

Si donc on envisage une fonction rationnelle entière

$$f(z_1, z_2, \ldots, z_n)$$

à coefficients (rationnels) entiers déterminés, et si, f étant de degré μ, on veut savoir si f peut être mis sous la forme

$$f(z_1, z_2, \ldots, z_n) = F(z_1, z_2, \ldots, z_n)\, G(z_1, z_2, \ldots, z_n)$$

où

$$F(z_1, z_2, \ldots, z_n) = \sum_{(i)} a_i z_1^{r_{1i}} z_2^{r_{2i}} \ldots z_n^{r_{ni}}$$

$$G(z_1, z_2, \ldots, z_n) = \sum_{(k)} b_k z_1^{s_{1k}} z_2^{s_{2k}} \ldots z_n^{s_{nk}}$$

sont des fonctions rationelles entières de degrés *donnés* μ_1 et $\mu - \mu_1$, à coefficients (rationnels) entiers a_i et b_k, il suffira de former pour chaque combinaison des indices i et k, l'équation (1). Les coefficients A_{ik} de cette équation seront des nombres (rationnels) entiers que l'on peut évaluer au moyen des coefficients de $f(z_1, z_2, \ldots, z_n)$. Puisque le produit $a_i b_k$ doit vérifier cette équation, a_i et b_k ne peuvent être choisis que parmi les diviseurs du nombre $A_{ik}^{(\nu)}$ si ce nombre est différent de zéro; si au contraire ce nombre $A_{ik}^{(\nu)}$ est égal à zéro, chacun des deux nombres a_i et b_k ne peut être choisi que ou bien égal à zéro, ou bien parmi les diviseurs du dernier de ceux des nombres $A_{ik}^{(1)}, A_{ik}^{(2)}, \ldots, A_{ik}^{(\nu-1)}$ qui ne sont pas nuls. Tous les nombres a_i ne peuvent d'ailleurs être nuls non plus que tous les nombre b_k. On obtient donc finalement un nombre *fini* de fonctions $F(z_1, z_2, \ldots z_n)$ et de fonctions $G(z_1, z_2, \ldots, z_n)$ hors desquelles une décomposition de $f(z_1, \ldots, z_n)$ en un produit de deux fonctions rationnelles entières à coefficients (rationnels) entiers, l'une de degré μ_1, l'autre de degré $\mu - \mu_1$, est impossible. Une simple division de $f(z_1, z_2, \ldots, z_n)$ par chacune des fonctions $F(z_1, z_2, \ldots, z_n)$ ainsi obtenues permet enfin de reconnaître parmi ces fonctions $F(z_1, z_2, \ldots, z_n)$ celles qui divisent effectivement $f(z_1, z_2, \ldots, z_n)$.

728) *Monatsb. Akad. Berlin 1883, p. 957; Werke[189]) 2, p 417; voir aussi *Gy. (J.) König,* Alg. Grössen[20]), p. 178.*

Pour voir si une fonction rationnelle entière de n variables, à coefficients entiers, est réductible ou irréductible dans le domaine des nombres (rationnels) entiers, on est ainsi conduit à chercher si certaines équations à coefficients entiers admettent, ou non, pour racines des nombres entiers.*

Citons ici un théorème important de *D. Hilbert*[729]). Soit

$$f(z_1, z_2, \ldots, z_n;\, p, q, \ldots)$$

une fonction rationnelle entière, à coefficients (rationnels) entiers, des variables $z_1, z_2, \ldots, z_n$ et des paramètres $p, q, \ldots$, *irréductible* par rapport à $z_1, z_2, \ldots, z_n, p, q, \ldots$: il est toujours possible, et cela d'une infinité de manières, de remplacer les paramètres $p, q, \ldots$ par des nombres rationnels entiers de façon que la fonction se présente comme une fonction rationnelle entière *irréductible* (à coefficients entiers) des variables $z_1, z_2, \ldots, z_n$.

*Envisageons, par exemple, l'expression[730])

$$z^3 - 3pz^2 - 3z + p$$

qui est une fonction *irréductible* des deux variables z, p. Si dans cette expression on remplace p par un nombre entier divisible par 3 sans être divisible par 9, elle se réduit à une fonction de l'unique variable z qui, en vertu du théorème de *G. Eisenstein* (n° **90**), est *irréductible.**

93. Réductibilité et irréductibilité dans un domaine quelconque de rationalité. Il y a souvent lieu de rechercher si une fonction rationnelle entière donnée peut être mise sous la forme d'un produit de fonctions rationnelles entières dont les coefficients soient des fonctions rationnelles à coefficients entiers de certains éléments arbitrairement fixés; ces éléments peuvent être des nombres donnés, ils peuvent aussi être des paramètres ou des fonctions de paramètres donnés.

*Il y a grand intérêt à s'attacher en particulier au cas où ces éléments sont en nombre *fini*; au point de vue auquel s'est placé *L. Kronecker* ce cas est même le seul qu'il y ait lieu d'envisager, au moins en algèbre. Afin de conserver ici le point de vue le plus général possible nous supposerons toutefois que ces éléments peuvent aussi bien être en nombre infini qu'en nombre fini; le cas où, comme aux n^os **1** à **88**, ces éléments sont tous les nombres complexes ordinaires (réels ou imaginaires) est alors compris parmi les cas possibles.

Tout en réservant pour l'article suivant (I 10) le développement

729) J. reine angew. Math. 110 (1892), p. 104.

730) *En égalant cette expression à zéro, on obtient l'équation à la résolution de laquelle se ramène le problème de la trisection d'un angle quelconque donné u, si l'on pose $u = \operatorname{arctg} p$.*

systématique des notions qui interviennent dans cet ordre de recherches, nous allons cependant donner ici quelques-uns des principaux résultats obtenus.* Pour énoncer ces résultats, les différents auteurs n'ont pas toujours employé la même terminologie. Nous adopterons celle de *L. Kronecker*; voici en quoi elle consiste[731]):

Etant donnés des symboles R', R'', R''', ... (représentant des nombres, des paramètres ou des fonctions de paramètres) en nombre fini ou infini on appelle *domaine de rationalité* et l'on représentera par le symbole $(R', R'', R''', \ldots)$ l'ensemble des fonctions rationnelles à coefficients rationnels de $R', R'', R''', \ldots$ On dit de chacun de ces symboles $R', R'', R''', \ldots$ qu'il est un *élément* du domaine. On définit de même le *domaine d'intégrité* $[R', R'', R''', \ldots]$ en remplaçant dans la définition précédente les locutions „fonction rationnelle" et „coefficients rationnels" par les locutions „fonction entière" et „coefficients entiers".

Si l'on ne se donne qu'un seul symbole R' et que l'on ait $R' = 1$, ou que l'on se donne un nombre fini de symboles $R', R'', R''', \ldots$ représentant des paramètres indépendants les uns des autres (l'un d'eux peut être égal à 1) le domaine de rationalité $(R', R'', R''', \ldots)$ s'appelle *domaine naturel de rationalité.*

On définit de même le *domaine naturel d'intégrité* $[R', R'', R''', \ldots]$.

*Nous représenterons par $\mathfrak{R}$ le domaine naturel de rationalité formé par le seul symbole $R' = 1$. Ce domaine est formé par l'ensemble des nombres rationnels.

Nous représenterons par $R_{\mathfrak{R}}$ tout autre domaine naturel de rationalité.

L'ensemble des fonctions rationnelles d'un nombre fini de paramètres indépendants les uns des autres, à coefficients complexes (réels ou imaginaires) rationnels, forme aussi un domaine de rationalité. Parfois on dit aussi de ce domaine qu'il est un domaine *naturel* de rationalité et on le représente par le symbole R en réservant le symbole $R_{\mathfrak{R}}$ pour désigner les domaines naturels de rationalité au sens plus restreint indiqué plus haut.*

Si $z_1, z_2, \ldots, z_n$ sont des variables indépendantes, on appelle fonction rationnelle entière de $z_1, z_2, \ldots, z_n$ dans le domaine de rationalité $(R', R'', R''', \ldots)$ [ou dans le domaine d'intégrité $[R', R'', R''', \ldots]$] toute fonction rationnelle entière de $z_1, \ldots, z_n$ dont les coefficients font partie de ce domaine de rationalité [ou d'intégrité].

731) *L. Kronecker,* Ber. Akad. Berlin 1853, p. 365; Monatsb. Akad. Berlin 1873, p. 117; Werke[167]) 1, p. 303; Monatsb. Akad. Berlin 1879, p. 205; Festschr.[481]) § 1; J. reine angew. Math. 92 (1882), p. 4; 94 (1883), p. 344; Werke[189]) 2, p. 249, 411; voir aussi *J. Molk,* Thèse, Paris 1884, chap. 2; Acta math. 6 (1885), p. 10.

Si une telle fonction $f(z_1, z_2, \ldots, z_n)$ peut se mettre sous la forme d'un produit $f_1 f_2$ de deux fonctions rationnelles entières *dans le même domaine de rationalité,* on dit que f est *réductible* dans ce domaine de rationalité. Si non, on dit que f est *irréductible* dans le domaine de rationalité envisagé.

*Si $f_1(z_1, z_2, \ldots, z_n)$ est un diviseur de $f(z_1, z_2, \ldots, z_n)$ dans un domaine de rationalité donné, le produit de $f_1(z_1, z_2, \ldots, z_n)$ par une quantité quelconque C faisant partie de ce même domaine de rationalité est aussi un diviseur de $f(z_1, z_2, \ldots, z_n)$. Deux diviseurs tels que

$$Cf_1(z_1, z_2, \ldots, z_n), \qquad C_1 f_1(z_1, z_2, \ldots, z_n),$$

dont le quotient fait partie du domaine de rationalité donné, sont dits *équivalents* dans ce domaine. Ils ne sont pas, en général, envisagés ici comme distincts.*

On dit de même qu'une fonction rationnelle entière $f(z_1, z_2, \ldots, z_n)$ dont les coefficients font partie d'un domaine d'intégrité $[R', R'', R''', \ldots]$ est *réductible* ou *irréductible* dans ce domaine, suivant qu'elle peut, ou non, se mettre sous la forme d'un produit $f_1 f_2$ de deux fonctions rationnelles entières dans le même domaine d'intégrité; les deux fonctions f_1, f_2 ne dépendent d'ailleurs pas nécessairement de toutes les variables $z_1, z_2, \ldots, z_n$; une de ces deux fonctions (par ex. f_1) peut même ne dépendre d'aucune des n variables: il suffit que $\frac{1}{f_1}$ ne soit pas une quantité faisant partie du domaine d'intégrité.

*Si E et $\frac{1}{E}$ appartiennent tous deux à un domaine d'intégrité donné, et si, dans ce domaine, $f_1(z_1, z_2, \ldots, z_n)$ est un diviseur de $f(z_1, z_2, \ldots, z_n)$, la fonction $Ef_1(z_1, z_2, \ldots, z_n)$ est aussi, dans ce même domaine, un diviseur de $f(z_1, z_2, \ldots, z_n)$. On dit que les deux fonctions

$$Ef_1(z_1, z_2, \ldots, z_n) \quad \text{et} \quad f_1(z_1, z_2, \ldots, z_n)$$

sont *équivalentes* dans ce domaine.

Ces définitions conviennent aussi bien au cas où $n = 1$ qu'à celui où $n > 1$.*

*Nous allons maintenant[732]) énoncer plusieurs théorèmes qui ont lieu quel que soit le domaine de rationalité Ω que l'on envisage.

I. Toute fonction rationnelle entière

$$f(z_1, z_2, \ldots, z_n)$$

dont les coefficients font partie d'un domaine Ω est ou bien *irréductible,* ou bien contient un nombre *fini* de diviseurs non équivalents.

732) *A partir d'ici et jusqu'à la fin des additions du n° **93**, texte et notes de *J. Kürschák.**

II. Si l'on envisage deux fonctions rationnelles entières

$$f(z_1, z_2, \ldots, z_n), \quad \varphi(z_1, z_2, \ldots, z_n)$$

dont les coefficients fassent partie d'un même domaine Ω, on peut toujours former une fonction rationnelle entière

$$D(z_1, z_2, \ldots, z_n)$$

dont les coefficients fassent aussi partie de Ω et qui soit telle que chacun des diviseurs communs de $f(z_1, z_2, \ldots, z_n)$ et de $\varphi(z_1, z_2, \ldots, z_n)$ soit, dans Ω, un diviseur de $D(z_1, z_2, \ldots, z_n)$ et que, dans le domaine Ω, $D(z_1, z_2, \ldots, z_n)$ ne contienne pas d'autre diviseur que ces diviseurs communs de $f(z_1, z_2, \ldots, z_n)$ et de $\varphi(z_1, z_2, \ldots, z_n)$.

On appelle $D(z_1, z_2, \ldots, z_n)$ le *plus grand commun diviseur* (p. g. c. d.) des deux fonctions $f(z_1, z_2, \ldots, z_n)$ et $\varphi(z_1, z_2, \ldots, z_n)$.

Le procédé indiqué aux n[os] **4** et **5** s'applique encore et permet de déterminer le p. g. c. d. $D(z_1, z_2, \ldots, z_n)$ de deux fonctions $f(z_1, z_2, \ldots, z_n)$ et $\varphi(z_1, z_2, \ldots, z_n)$ dans un domaine Ω.

Si les deux fonctions $f(z_1, z_2, \ldots, z_n)$ et $\varphi(z_1, z_2, \ldots, z_n)$ n'ont aucun diviseur commun dans un domaine Ω, on prendra $D = 1$.

III. Si une fonction $f(z_1, z_2, \ldots, z_n)$ est *irréductible* dans un domaine Ω et si le produit

$$A(z_1, z_2, \ldots, z_n)\, B(z_1, z_2, \ldots, z_n)$$

de deux fonctions rationnelles entières, à coefficients faisant partie de Ω, est divisible par $f(z_1, z_2, \ldots, z_n)$, il faut que l'une au moins des deux fonctions $A(z_1, z_2, \ldots, z_n)$, $B(z_1, z_2, \ldots, z_n)$ soit divisible par $f(z_1, z_2, \ldots, z_n)$.

IV. Si, dans un domaine Ω, une fonction $f(z_1, z_2, \ldots, z_n)$ est réductible, elle peut être répresentée *d'une* et *d'une seule manière* par un produit de fonctions rationnelles entières irréductibles dans Ω, à condition toutefois de ne pas envisager comme distincts deux produits dont les facteurs soient respectivement équivalents.

Dans le domaine $\mathfrak{R}$ on peut toujours, à l'aide d'un nombre *fini* d'opérations, reconnaître (n[os] **89** et **92**) si une fonction rationnelle entière donnée $f(z_1, z_2, \ldots, z_n)$ est irréductible ou non et quand elle est réductible obtenir effectivement ses diviseurs. Quoiqu'il en soit de même pour un grand nombre d'autres domaines de rationalité, il n'en est pas de même pour tous les domaines de rationalité. On a toutefois pu démontrer le théorème suivant qui a lieu quel que soit le domaine Ω que l'on envisage:

V. Lorsqu'on sait trouver dans un domaine Ω, à l'aide de procédés déterminés, tous les diviseurs de chaque fonction rationnelle

entière d'une seule variable z, on peut aussi, à l'aide de ces mêmes procédés et d'un nombre fini d'additions, de soustractions, de multiplications et de divisions, trouver tous les diviseurs de chaque fonction rationnelle entière d'un nombre quelconque de variables.

Si, en effet[733]), la fonction $f(z_1, z_2, \ldots, z_n)$ est régulière en z_1, ce qu'on peut toujours supposer en appliquant préalablement (n° **2**) s'il y a lieu une substitution linéaire convenablement choisie, tout diviseur de $f(z_1, z_2, \ldots, z_n)$ est aussi une fonction régulière en z_1. Rien n'empêche, d'autre part, de supposer que le coefficient c de la plus haute puissance de z_1 dans f est égal à 1, car s'il n'est pas égal à 1 il suffit d'envisager au lieu de $f(z_1, z_2, \ldots, z_n)$ le quotient de cette fonction par c; on peut alors se borner à envisager les diviseurs de $f(z_1, z_2, \ldots, z_n)$ dont le coefficient de la plus haute puissance en z_1 est aussi égal à 1. Dès lors la seconde méthode de *L. Kronecker*, exposée au n° **92**, s'applique et il suffit de répéter ce qui a été dit à ce sujet au n° **92** en remplaçant seulement les coefficients $F(\alpha_0)$, $F(\alpha_1), \ldots, F(\alpha_m)$ respectivement par des diviseurs de

$$f(z_1, z_2, \ldots, z_{n-1}, \alpha_0),\ f(z_1, z_2, \ldots, z_{n-1}, \alpha_1), \ldots f(z_1, z_2, \ldots, z_{n-1}, \alpha_m)$$

dont les coefficients appartiennent au domaine Ω, le coefficient de la puissance la plus élevée en z_1 dans chacun de ces diviseurs étant égal à 1.

Plaçons-nous par exemple dans le cas où Ω représente le domaine de tous les nombres complexes (réels ou imaginaires) et envisageons comme possible la résolution de toutes les équations algébriques $\varphi(z) = 0$ à coefficients numériques quelconques donnés. Les procédés qui permettent d'obtenir ainsi les racines de toutes les équations $\varphi(z) = 0$ suffiront alors pour déterminer dans le domaine Ω les diviseurs de chaque fonction rationnelle entière $f(z_1, z_2, \ldots, z_n)$ à coefficients numériques quelconques donnés.

Il convient toutefois d'observer qu'au point de vue de *L. Kronecker* cette façon de présenter les choses est précaire et ne saurait être admise qu'à titre provisoire (cf. I 3, **10** et I 9, **89**).

Si l'on continue à envisager comme possible la résolution de toutes les équations algébriques $\varphi(z) = 0$ à coefficients numériques, on peut aussi déterminer, dans le domaine naturel de rationalité au sens étendu du mot, domaine que nous désignons ici par R, les diviseurs de chaque fonction rationnelle entière $f(z_1, z_2, \ldots, z_n)$ à coefficients situés dans ce domaine R. A cet effet, on remarque que si les coefficients de $f(z_1, z_2, \ldots, z_n)$ font partie du domaine R formé par

733) *Cf. *Gy. (J.) König,* Math. termész. értesitö 2 (1883), p. 46.*

toutes les fonctions rationnelles entières, à coefficients complexes (réels ou imaginaires), de ϱ paramètres $R', R'', \ldots, R^{(\varrho)}$, on peut toujours former une fonction rationnelle entière

$$C(R', R'', \ldots, R^{(\varrho)}),$$

à coefficients numériques, telle que la fonction rationnelle F des $n + \varrho$ quantités

$$z_1, z_2, \ldots, z_n, R', R'', \ldots, R^{(\varrho)},$$

définie par l'expression

$$F(z_1, z_2, \ldots, z_n, R', R'', \ldots, R^{(\varrho)}) = C.\ f(z_1, z_2, \ldots, z_n),$$

soit une fonction rationnelle *entière* de ces $n + \varrho$ quantités. Ceci posé, déterminons tous les diviseurs de F, c'est-à-dire toutes les fonctions rationnelles entières de $z_1, z_2, \ldots, z_n, R', R'', \ldots, R^{(\varrho)}$, à coefficients numériques, qui divisent F; ce seront aussi les diviseurs de $f(z_1, z_2, \ldots, z_n)$ dans le domaine envisagé R, à condition toutefois d'envisager comme équivalents dans ce domaine R deux des diviseurs de F quand leur quotient ne dépend d'aucune des n variables $z_1, z_2, \ldots, z_n$.

Des considérations analogues montrent que, dans le domaine $R_{\mathfrak{R}}$, les diviseurs d'une fonction rationnelle entière

$$f(z_1, z_2, \ldots, z_n)$$

peuvent être formés à l'aide d'un nombre *fini* d'opérations *sans qu'il soit ici nécessaire de supposer possible la résolution des équations algébriques* $\varphi(z) = 0$ *à coefficients numériques.*

On appelle *domaines clos*[734]) les domaines Ω tels que si $F(x)$ est une fonction rationnelle entière de x dont les coefficients font partie de Ω, il existe dans Ω une quantité x au moins (soit un nombre, soit une fonction rationnelle entière d'un ou de plusieurs paramètres) qui annule $F(x)$.

Toute fonction rationnelle entière de x, à coefficients faisant partie d'un domaine clos Ω, se décompose, dans ce domaine clos, en facteurs linéaires.

Si, par contre, on envisage les fonctions rationnelles entières de x, à coefficients faisant partie d'un domaine non clos Ω arbitrairement fixé, il y a toujours une infinité de fonctions de degrés plus grands que 1 qui sont irréductibles dans ce domaine non clos Ω.

734) *C'est *L. Kronecker* qui a, le premier, désigné sous le nom de „geschlossene Bereiche" [Festschrift[481]), § 3; J. reine angew. Math. 92 (1882), p. 10; Werke 2, p. 255] certains domaines jouissant de cette propriété.

L'ensemble des nombres complexes (réels et imaginaires) constitue un domaine clos. L'ensemble des nombres réels constitue un domaine non clos.

Soit Ω un domaine non clos arbitrairement fixé. Envisageons une fonction rationnelle entière

$$F(x),$$

de degré au moins égal à 2, à coefficients appartenant au domaine Ω, et qui soit irréductible dans ce domaine Ω. Désignons par η une racine de l'équation

$$F(x) = 0.$$

L'ensemble des fonctions rationnelles entières de η dont les coefficients appartiennent au domaine Ω constituent un nouveau domaine que nous désignerons par

$$\Omega' = (\Omega, \eta)$$

et que nous dirons *dérivé* du domaine Ω par *adjonction* de η.

Le domaine des nombres complexes

$$\Omega' = (\Omega, i)$$

peut ainsi être envisagé comme le domaine dérivé du domaine Ω des nombres réels par adjonction de la racine i de l'équation

$$x^2 + 1 = 0.$$

L. Kronecker[735]) et *H. Weber*[736]) ont montré que quand on connaît un procédé permettant de former les diviseurs de chaque fonction rationnelle entière $f(z_1, z_2, \ldots, z_n)$ dans un domaine Ω, ce même procédé (et de simples additions, soustractions, multiplications et divisions en nombre fini) permet aussi de former les diviseurs de $f(z_1, z_2, \ldots, z_n)$ dans un domaine quelconque $\Omega' = (\Omega, \eta)$ *dérivé* du domaine Ω. La méthode que *H. Weber* a imaginée pour réaliser cette décomposition sera exposée au n° **94**.*

A chaque fonction rationnelle entière $f(x)$ d'*une seule* variable x correspond un domaine de rationalité Ω dans lequel cette fonction $f(x)$ se décompose en facteurs linéaires.

Au contraire certaines fonctions rationnelles entières de deux ou de plusieurs variables non linéaires sont irréductibles quel que soit

735) Festschrift[481]), § 4; J. reine angew. Math. 92 (1882), p. 12/3; Werke 2, p. 258/9; *J. Molk,* Thèse, Paris 1884; Acta math. 6 (1885), p. 41/8.

736) *A proprement parler, la méthode de *H. Weber,* comme celle de *L. Kronecker,* suppose que Ω est un domaine *naturel* de rationalité. Toutefois le procédé de *H. Weber,* comme celui de *L. Kronecker,* s'applique tout aussi bien pour tout autre domaine Ω. Voir aussi *J. Molk,* Thèse, Paris 1884; Acta math. 6 (1885), p. 65/79; *E. Borel* et *J. Drach,* Théorie des nombres[218]), p. 184/7, 234/7.*

le domaine de rationalité dont font partie leurs coefficients. Ce sont les fonctions *indécomposables* (nº **3**) ou *absolument irréductibles* non linéaires. La fonction $x_1 x_2 - 1$ est absolument irréductible.

Les théorèmes relatifs à la décomposition des fonctions rationnelles entières dans un *domaine de rationalité* ne peuvent, en général, être étendus à la décomposition de ces fonctions dans un *domaine d'intégrité*. Mais dans le domaine d'intégrité constitué par l'ensemble des nombres (rationnels) entiers, et aussi dans le domaine naturel d'intégrité $[R', R'', \ldots, R^{(\nu)}]$ où $R' = 1$ tandis que $R'', \ldots, R^{(\nu)}$ désignent des paramètres indépendants, les théorèmes I à IV cités plus haut, ont encore lieu.

94. Méthode de Weber pour reconnaître si une fonction est réductible ou irréductible dans un domaine de rationalité dérivé d'un domaine donné[737]. *Proposons-nous tout d'abord de reconnaître à l'aide d'un nombre *fini* d'opérations réalisables si une fonction rationnelle entière donnée $F(z)$ d'une seule variable z est réductible ou irréductible dans un domaine de rationalité

$$(1, \theta_1)$$

où θ_1 est l'un des zéros d'une fonction rationnelle entière donnée $\psi(t)$ d'une variable t ayant pour coefficients des nombres rationnels connus.

Nous pouvons toujours supposer que les coefficients de $F(z)$ sont des nombres rationnels, car s'ils étaient des fonctions rationnelles de θ_1, il nous suffirait d'appliquer à la norme de $F(z)$ prise par rapport à θ_1 le procédé que nous allons indiquer pour la fonction $F(z)$ à coefficients rationnels. Cette norme est par définition le produit de $F(z)$ par les fonctions que l'on en déduit en y remplaçant successivement θ_1 par chacune des racines de l'équation $\psi(t) = 0$; d'après la théorie des fonctions symétriques (nº **7**) c'est donc une fonction rationnelle entière de z à coefficients rationnels; et, d'autre part, il est clair que dans le domaine de rationalité $(1, \theta_1)$ les facteurs irréductibles d'une fonction $F(z)$ à coefficients fonctions rationnelles de θ_1 sont compris parmi les facteurs irréductibles, dans ce même domaine de rationalité $(1, \theta_1)$, de la norme de $F(z)$ prise par rapport à θ_1.

Nous pourrions aussi, dans cette recherche, éviter de supposer connu le théorème fondamental de l'Algèbre (nº **80**) car la question de savoir si $F(z)$ peut, ou non, être mis sous la forme d'un produit

$$F(z) = f(z, \theta_1) f_1(z, \theta_1) \tag{1}$$

737) *Ce numéro est dû à *H. Weber*.*

de deux fonctions rationnelles entières f et f_1 de z ayant pour coefficients des fonctions rationnelles (à coefficients entiers) de θ_1 est, au fond, identique à celle de savoir si la fonction $F(z)$ d'une variable z peut, ou non, être mise sous la forme

$$F(z) = f(z, t) f_1(z, t) + \psi(t)\, g(z, t) \tag{2}$$

c'est-à-dire si, pour deux fonctions données, $F(z)$ et $\psi(t)$, dépendant la première de l'unique variable z et la seconde de l'unique variable t, on peut trouver trois fonctions des *deux* variables z et t vérifiant identiquement cette équation (2).

Pour abréger l'exposé de la méthode de *H. Weber* nous introduirons cependant les zéros de la fonction $\psi(t)$ et, au lieu de raisonner sur l'équation (2), nous raisonnerons sur l'équation (1); chacun rétablira aisément l'exposé correspondant.

D'après ce qui a été démontré (nº **89**), on peut toujours supposer que les fonctions $F(z)$ et $\psi(t)$ sont *irréductibles* dans le domaine naturel de rationalité. Si $F(z)$ est de degré m en z et si $\psi(t)$ est de degré μ en t nous désignerons par

$$\zeta_1, \zeta_2, \ldots, \zeta_m$$

les zéros de $F(z)$ et par

$$\theta_1, \theta_2, \ldots, \theta_\mu$$

les zéros de $\psi(t)$.

Ceci posé envisageons une fonction rationnelle entière des deux variables z et t,

$$y = \varphi(z, t)$$

de degré inférieur à m par rapport à z, inférieur à μ par rapport à t et dont les coefficients sont des nombres (rationnels) entiers fixés arbitrairement sauf parmi ceux dont nous allons parler.

Soit

$$\eta_{i\varkappa} = \varphi(\zeta_i, \theta_\varkappa) \qquad \begin{pmatrix} i = 1, 2, \ldots, m \\ \varkappa = 1, 2, \ldots, \mu \end{pmatrix};$$

nous supposerons les coefficients de φ choisis de façon que les $m\mu$ nombres $\eta_{i\varkappa}$ soient distincts; en d'autres termes nous les supposerons tels que le discriminant

$$D = \prod [\eta_{i\varkappa} - \eta_{i'\varkappa'}]^2$$

soit différent de zéro; le produit qui figure ici dans le second membre est étendu aux indices $i, i' = 1, 2, \ldots, m$; $\varkappa, \varkappa' = 1, 2, \ldots, \mu$, pour lesquels $i \leqq i'$ et, dans le cas où $i = i'$, pour lesquels $\varkappa < \varkappa'$. Cette restriction est légitime car on peut exprimer, à l'aide d'un nombre *fini* d'opérations réalisables, D en fonction rationnelle des coefficients de φ et l'on peut ensuite, à l'aide d'un nombre *fini* d'opérations réalisables, trouver pour les coefficients de φ des valeurs telles que cette fonction rationnelle D ne soit pas nulle.

Si l'équation

$$\Phi(y, \theta_\varkappa) = 0 \tag{3}$$

est le résultat de l'élimination de z entre les deux équations

$$F(z) = 0, \qquad y - \varphi(z, \theta_\varkappa) = 0, \tag{4}$$

les racines de l'équation (3) envisagée comme une équation en y sont les m nombres

$$\eta_{i\varkappa} = \varphi(\xi_i, \theta_\varkappa) \qquad (i = 1, 2, \ldots, m).$$

D'ailleurs les μ fonctions de y

$$\Phi(y, \theta_1), \quad \Phi(y, \theta_2), \quad \ldots, \quad \Phi(y, \theta_\mu)$$

sont deux à deux sans diviseur commun. Ces fonctions peuvent être obtenues à l'aide d'un nombre *fini* d'opérations quand on se donne les équations (4).

Pour trouver les facteurs irréductibles de la fonction $\Phi(y, \theta_\varkappa)$ envisagée comme une fonction de y, on formera la norme

$$N(y) = \Phi(y, \theta_1)\, \Phi(y, \theta_2) \ldots \Phi(y, \theta_\mu);$$

on l'exprimera par une fonction rationnelle de y dont les coefficients sont des nombres rationnels, ce qui est possible (nº **7**) à l'aide d'un nombre fini d'opérations; on décomposera cette fonction rationnelle $N(y)$ en ses facteurs irréductibles $N_1(y), N_2(y), \ldots$, dans le domaine naturel de rationalité, ce qui est possible (nº **89**) à l'aide d'un nombre fini d'opérations; enfin on cherchera pour $\nu = 1, 2, \ldots$ le plus grand commun diviseur des deux fonctions de y

$$\Phi(y, \theta_\varkappa), \quad N_\nu(y),$$

ce qui est encore possible à l'aide d'un nombre fini d'opérations, en appliquant l'*algorithme d'Euclide.*

Il suffit maintenant pour trouver les facteurs irréductibles de $F(z)$ dans le domaine de rationalité $(1, \theta_\varkappa)$ de remplacer, dans les facteurs irréductibles $\Phi_1(y, \theta_\varkappa)$, $\Phi_2(y, \theta_\varkappa), \ldots$ de $\Phi(y, \theta_\varkappa)$ ainsi obtenus, la variable y par son expression

$$y = \varphi(z, \theta_\varkappa)$$

et de chercher les plus grands communs diviseurs des fonctions de z

$$\Phi_1[\varphi(z, \theta_\varkappa), \theta_\varkappa], \qquad \Phi_2[\varphi(z, \theta_\varkappa), \theta_\varkappa], \qquad \ldots$$

et de la fonction donnée $F(z)$.

On démontre d'ailleurs aisément que, si $F(z)$ contient un facteur $f_1(z, \theta_1)$ irréductible dans le domaine $(1, \theta_1)$, il contiendra aussi les facteurs irréductibles $f_1(z, \theta_2), \ldots, f_1(z, \theta_\nu)$.

La même méthode s'applique lorsqu'au lieu du domaine de rationalité $(1, \theta_1)$ on envisage un domaine de rationalité

$$(R', R'', \ldots, R^{(\nu)}, \theta_1)$$

formé par un domaine quelconque donné $(R', R'', \ldots, R^{(\nu)})$ [naturel ou non] auquel on a *adjoint* une racine θ_1 d'une équation algébrique donnée $\psi(t) = 0$ dont les coefficients fassent partie du domaine

$$(R', R'', \ldots, R^{(\nu)}).$$

Enfin on montre sans peine[738]) que l'*adjonction* au domaine $(R', R'', \ldots, R^{(\nu)})$ d'un nombre fini quelconque de racines $\theta_1, \eta_1, \ldots$ d'équations algébriques $\psi_1(t) = 0$, $\psi_2(t) = 0, \ldots$ distinctes données dont les coefficients font partie du domaine $(R', R'', \ldots, R^{(\nu)})$, revient à l'adjonction au domaine $(R', R'', \ldots, R^{(\nu)})$ de la racine d'une seule équation algébrique déterminée dont les coefficients font partie de ce même domaine $(R', R'', \ldots, R^{(\nu)})$; on peut d'ailleurs les obtenir à l'aide d'un nombre *fini* d'opérations rationnelles.

On pourrait aussi opérer de proche en proche en appliquant la méthode précédente pour trouver d'abord les facteurs irréductibles de $F(z)$ dans le domaine $(R', R'', \ldots, R^{(\nu)}, \theta_1)$, puis les facteurs irréductibles de chacun de ces facteurs irréductibles dans le domaine $(R', R'', \ldots, R^{(\nu)}, \theta_1, \eta_1)$, et ainsi de suite.

Les résultats obtenus dans la théorie générale de l'élimination permettent d'appliquer la méthode de *H. Weber* au cas où l'on adjoint au domaine de rationalité donné les zéros d'un système quelconque d'équations algébriques (en nombre fini) dont les coefficients font partie du domaine de rationalité donné.

Ce que l'on a dit au nº **92** suffit pour étendre au cas d'un nombre quelconque de variables la méthode de réduction exposée ici pour le cas d'une seule variable.

De tout ce qui précède on peut conclure que chaque fonction rationnelle entière d'une ou de plusieurs variables, dont les coefficients appartiennent à un domaine de rationalité quelconque donné, peut être décomposée en facteurs irréductibles dans ce domaine de rationalité. Mais il n'en résulte pas que la décomposition de chaque fonction rationnelle entière en facteurs irréductibles dans ce domaine est *univoque*, en sorte qu'on ne peut conclure de ce qui précède que les facteurs irréductibles obtenus ont le caractère de *facteurs premiers* de la fonction rationnelle envisagée, au sens de la Théorie des nombres.

Pour démontrer que la décomposition est *univoque*, il faut dé-

738) *L. Kronecker*, Festschrift[481]) § 3; J. reine angew. Math. 92 (1882), p. 8; Werke 2, p. 254; *J. Molk*, Thèse, Paris 1884; Acta math. 6 (1885), p. 38.*

montrer que, si un produit de deux fonctions rationnelles entières d'un nombre quelconque de variables est divisible, dans un domaine de rationalité donné, par une fonction rationnelle f *irréductible dans ce domaine*, un au moins des deux facteurs est divisible par f dans ce domaine.

On trouvera la démonstration de ce théorème dans le mémoire de *J. Molk*[739]) et dans le traité d'algèbre de *H. Weber*[740]). C'est par *induction* qu'on parvient à le démontrer et la chaîne de raisonnements que l'on est amené à faire revient à ceci:

Supposons le théorème exact pour toutes les fonctions rationnelles entières de n variables $z_1, z_2, \ldots, z_n$. Envisageons des fonctions rationnelles entières d'une nouvelle variable t dont les coefficients soient des fonctions rationnelles entières de $z_1, z_2, \ldots, z_n$ et convenons d'appeler pour un instant diviseur d'une telle fonction de t le p. g. c. d. de ses coefficients. On démontre alors tout d'abord que le diviseur d'un produit est égal au produit des diviseurs des facteurs de ce produit. On en conclut que si une fonction

$$\Phi\,(t, z_1, z_2, \ldots, z_n)$$

envisagée comme une fonction de t seulement peut être décomposée en facteurs à coefficients rationnels en $z_1, z_2, \ldots, z_n$, cette même fonction Φ peut aussi être décomposée en facteurs fonctions rationnelles entières des $n+1$ variables $t, z_1, z_2, \ldots, z_n$. De là résulte que si les deux fonctions rationnelles entières

$$f(t, z_1, z_2, \ldots, z_n), \qquad \varphi\,(t, z_1, z_2, \ldots, z_n),$$

envisagées comme des fonctions de t, sont premières entre elles et si le produit

$$f(t, z_1, z_2, \ldots, z_n)\, F(t, z_1, z_2, \ldots, z_n),$$

envisagé comme une fonction de t, est divisible par $\varphi\,(t, z_1, z_2, \ldots, z_n)$ envisagé comme une fonction de t, la fonction $F\,(t, z_1, z_2, \ldots, z_n)$ envisagée comme une fonction de t est divisible par $\varphi\,(t, z_1, z_2, \ldots, z_n)$. D'où le théorème annoncé.

Il est maintenant aisé d'établir que la décomposition d'une fonction rationnelle entière, dans un domaine de rationalité fixé à l'avance, est *univoque* si l'on convient toutefois de ne pas envisager comme distincts (au point de vue de cette décomposition) deux facteurs dont le quotient est une quantité faisant partie du domaine de rationalité envisagé.*

95. Réductibilité de $x^n - a$ dans un domaine quelconque de rationalité. Si p est un nombre premier et si, dans le domaine de

739) *Thèse, Paris 1884; Acta math. 6 (1885), p. 16/8.*

740) **H. Weber*, Alg.[24]) 1, p. 74; trad. *J. Griess* 1, p. 75.*

rationalité choisi, a n'est pas une puissance $p^{\text{ième}}$ d'une quantité faisant partie de ce domaine, le binome $x^p - a$ est irréductible. C'est là un théorème dû à *N. H. Abel*[741]), dont *F. Mertens*[742]) et *A. Kneser*[743]) ont donné des démonstrations purement arithmétiques.

L. Kronecker[744]) a cherché la condition pour que l'équation aux racines primitives qui est irréductible dans le domaine naturel de rationalité devienne réductible dans le domaine de rationalité (R', R'') où $R' = 1$ et où R'' désigne une racine primitive de l'unité.

A. Capelli[745]) s'est occupé de la réductibilité de $x^n - a$, quand n est un nombre entier positif quelconque. Supposant que $\theta_1(x)$ et $\theta_2(x)$ sont des fonctions rationnelles et entières de x, dont les coefficients appartiennent à un certain domaine de rationalité Ω, pour que la fonction $\theta_1(\theta_2(x))$ soit irréductible dans le domaine Ω, il faut et il suffit que la fonction $\theta_1(x)$ soit irréductible dans le domaine Ω, et que, y_h étant une racine choisie à volonté de l'équation $\theta_1(y) = 0$, la fonction $\theta_2(x) - y_h$ soit irréductible dans le domaine (Ω, y_h). Cela posé, *A. Capelli* démontre que le théorème de *N. H. Abel* s'applique au binome $x^n - a$, pourvu que n soit impair. Il examine aussi[746]) le cas d'exception où n est une puissance de 2 en sorte que le binome est de la forme $x^{2^\lambda} - a$; ce binome est réductible si a est le carré d'une des quantités faisant partie du domaine Ω, ou si $(-a)$ est le quadruple de la quatrième puissance d'une des quantités faisant partie du domaine Ω[747]).

Les fonctions rationnelles entières à coefficients rationnels qui sont réductibles dans le domaine des nombres rationnels sont aussi réductibles quel que soit le domaine de rationalité dans lequel on cherche à les décomposer.

96. Théorème de Kronecker. *Dans un tout autre ordre d'idées, envisageons, avec *L. Kronecker*[748]), une fonction rationnelle entière de x

741) J. reine angew. Math. 1 (1826), p. 71 et mém. posth. nº 18; Œuvres éd. *L. Sylow* et *S. Lie* 1, Christiania 1881, p. 72; 2, Christiania 1881, p. 217.

742) Monatsh. Math. Phys. 2 (1891), p. 291.

743) J. reine angew. Math. 106 (1890), p. 48.

744) J. reine angew. Math. 100 (1887), p. 79; Werke 3[1], Leipzig 1899, p. 243; voir aussi *N. L. W. A. Gravelaar*, Nieuw Archief voor Wiskunde (1) 20 (1893), p. 7.

745) Rendic. Accad. Napoli (3) 3 (1897), p. 243; (3) 4 (1898), p. 84, 243; Math. Ann. 54 (1901), p. 602.

746) Rendic. Accad. Napoli (3) 4 (1898), p. 84.

747) Cf. *E. Wendt*, Math. Ann. 53 (1900), p. 450.

748) J. reine angew. Math. 100 (1887), p. 490; Mathesis (1) 5 (1885), p. 102 (extrait d'une lettre à *P. Mansion*); Werke 3[1], Leipzig 1899, p. 211.

$$F(x) = x^n - c_1 x^{n-1} + c_2 x^{n-2} - \cdots + (-1)^n c_n$$

dont les coefficients $c_1, c_2, \ldots, c_n$ soient des fonctions rationnelles *entières* des éléments d'un certain domaine naturel d'intégrité $[1, R', R'', \ldots]$ et qui n'ait aucun diviseur commun avec sa dérivée $\frac{\partial F}{\partial x}$.

Désignons par $x_1, \ldots, x_n, u_1, \ldots, u_n$ des indéterminées, et formons le produit

$$\text{(I)} \qquad \prod_{(i)} (z - u_1 x_{i_1} - u_2 x_{i_2} - \cdots - u_n x_{i_n}),$$

étendu aux $n!$ permutations $(i_1, i_2, \ldots, i_n)$ des nombres $1, 2, \ldots, n$. Si l'on représente par $f_1, \ldots, f_n$ les fonctions symétriques élémentaires des indéterminées $x_1, x_2, \ldots, x_n$ définies par l'identité

$$(x - x_1)(x - x_2) \cdots (x - x_n) = x^n - f_1 x^{n-1} + f_2 x^{n-2} - \cdots + (-1)^n f_n,$$

le produit (I) est une fonction $G(z, f_1, f_2, \ldots, f_n)$ dont les coefficients dépendent des indéterminées $u_1, u_2, \ldots, u_n$. Dans cette fonction remplaçons $f_1, f_2, \ldots, f_n$ par les coefficients $c_1, c_2, \ldots, c_n$ de la fonction $F(x)$ et les indéterminées $u_1, u_2, \ldots, u_n$ par des nombres (rationnels) entiers arbitrairement fixés parmi ceux pour lesquels le discriminant de la fonction $G(z, c_1, c_2, \ldots, c_n)$ n'est pas nul. Si alors $G_1(z)$ est un des facteurs irréductibles de la fonction $G(z; c_1, c_2, \ldots, c_n)$ dans le domaine naturel d'intégrité $[1, R', R'', \ldots]$, la fonction $F(x)$ pourra être décomposée, relativement au module *premier* $G_1(z)$, en un produit de facteurs *linéaires*; en d'autres termes la différence entre le produit de $F(x)$ par une quantité convenablement choisie faisant partie du domaine naturel d'intégrité $[1, R', R'', \ldots]$ et le produit de $G_1(z)$ par une fonction rationnelle entière de x convenablement choisie est un produit de facteurs linéaires en x; les coefficients de toutes les fonctions étant des fonctions rationnelles entières de $z, R', R'', \ldots$

Exemple: Envisageons la fonction

$$F(x) = x^3 - a^3$$

dont les coefficients 1 et a^3 sont des fonctions rationnelles entières des éléments du domaine naturel d'intégrité $[1, a]$ et dont les trois racines sont distinctes si l'on suppose a différent de zéro. Relativement au module premier $G_1(z) = z^2 + 3a^2$, on a identiquement

$$4(x^3 - a^3) \equiv (x - a)(2x + z + a)(2x - z + a) \;[\text{mod.}\,(z^2 + 3a^2)].^*$$

„Presque tous les nombreux renseignements bibliographiques complémentaires contenus dans cet exposé français sont dus à *R. Le Vavasseur.* L'exposé des théories générales a été rédigé à nouveau et complété par *J. Kürschák*-Budapest, *J. Molk* et *H. Vogt*-Nancy."

I 10. PROPRIÉTÉS GÉNÉRALES DES CORPS ET DES VARIÉTÉS ALGÉBRIQUES.

Exposé, d'après l'article allemand de **G. LANDSBERG** (Kiel),

par **J. HADAMARD** (Paris) et **J. KÜRSCHÁK** (Budapest).

Notion de corps.

1. Introduction des considérations arithmétiques dans l'Algèbre. Dans l'article précédent (I 9), on a étudié les polynomes ou fonctions rationnelles entières en se plaçant successivement à des points de vue bien distincts. Parmi ces points de vue il en est deux qui ont un caractère extrême et qui ont particulièrement retenu notre attention.

C'est au premier de ces deux points de vue extrêmes qu'on s'est placé dans la première partie de l'article I 9 (nos **1** à **88**); il consiste à prendre pour coefficients des fonctions rationnelles entières envisagées des quantités *absolument quelconques.* Si, par exemple, ces coefficients sont des nombres, ces nombres peuvent être aussi bien fractionnaires qu'entiers, rationnels qu'irrationnels, complexes que réels. Une seule propriété essentielle leur est imposée: celle d'être constants, indépendants des variables par rapport auxquelles les fonctions rationnelles entières sont ordonnées.

Dans la plus grande partie des nos **89** à **92** de l'article I 9 il en est tout autrement. Les seuls nombres que l'on envisage et que l'on se donne le droit d'employer sont les nombres entiers (réels, rationnels); par conséquent aussi les seules fonctions rationnelles entières qu'on prenne en considération sont celles dont les coefficients sont des nombres entiers, toutes les autres fonctions rationnelles entières étant regardées comme inexistantes. En un mot, lorsqu'on se place à ce second point de vue extrême, tout se passe comme si la théorie des nombres complexes, celle des nombres irrationnels et même celle des nombres fractionnaires n'était point faite.

Un point de vue intermédiaire, qui a été lui aussi mentionné aux n^{os} **89** à **92** de l'article I 9, consiste à n'admettre comme coefficients que des nombres réels et rationnels. C'est l'Algèbre telle qu'elle aurait pu être constituée avant l'invention des nombres irrationnels.

2. Influence de ces considérations arithmétiques sur l'irréductibilité. Il est essentiel de remarquer immédiatement que certains des mots employés dans ce qui précède ont un sens tout différent suivant qu'on se place à l'un ou à l'autre de ces points de vue. Tel est avant tout le cas pour le mot *irréductibilité.*

Soit par exemple une fonction rationnelle entière de deux variables x et y. Cette fonction

$$f(x,\ y)$$

de degré n sera dite *réductible* sous notre premier point de vue si elle peut être mise sous la forme du produit de deux fonctions rationnelles entières de degrés inférieurs à n. Cette affirmation est rigoureusement équivalente à celle-ci: la courbe algébrique

$$f(x,\ y) = 0$$

est décomposable en courbes algébriques (distinctes ou non) d'ordres inférieurs.

Ainsi toute fonction rationnelle entière homogène de x et y (de degré supérieur à 1), par exemple la fonction

$$ax^2 + bxy + cy^2,$$

est réductible: car l'équation obtenue en égalant cette fonction rationnelle entière à zéro représente, quels que soient les coefficients a, b, c, un système de droites issues de l'origine.

Il n'en est pas de même à notre second point de vue, c'est-à-dire si nous imposons aux coefficients la condition d'être réels, rationnels et entiers. La fonction rationnelle entière

$$ax^2 + bxy + cy^2$$

ne sera alors réductible que si les droites représentées par l'équation

$$ax^2 + bxy + cy^2 = 0$$

ont leurs coefficients angulaires réels et rationnels, c'est-à-dire si le nombre entier

$$b^2 - 4ac$$

est positif et carré parfait.

Le premier point de vue, qui est, comme on le voit, celui de la géométrie analytique, est généralement considéré en France comme appartenant seul à l'algèbre proprement dite. Le second ainsi que ceux dont il nous reste à parler représente ce que l'on appellera l'*arithmético-algèbre.*

Toute opposée est l'opinion de *L. Kronecker*[1]). Pour lui l'idée de fonction rationnelle implique que les coefficients sont eux aussi des nombres rationnels. De même *L. Kronecker* ne considère aucun polynome comme fonction rationnelle entière si ses coefficients, lorsqu'ils sont numériques, ne sont pas des nombres entiers. Nous ne nous placerons pas en général à ce point de vue et pour plus de clarté nous encadrerons du signe [ ] tout ce qui s'y rapporte.

3. Les „quantités connues“ en général. Les points de vue mentionnés au n° **1** sont loin d'être les seuls auxquels on puisse se placer. Il en existe une infinité d'autres analogues (cf. I 9, n^{os} **93** à **95**) auxquels on s'est trouvé nécessairement conduit dès qu'on a voulu étudier d'une façon un peu approfondie la résolution des équations[2]).

On est alors amené, en effet, à distinguer entre les quantités connues et celles qui ne le sont point ou ne le sont point encore. La connaissance d'une ou de plusieurs quantités entraîne d'ailleurs celle de toutes leurs combinaisons *rationnelles*, c'est-à-dire de toutes les quantités que l'on en déduit par addition, soustraction, multiplication et division. Par exemple la détermination des côtés des deux décagones réguliers inscrits au cercle de rayon 1 exige la connaissance de la quantité $\sqrt{5}$; cette quantité une fois connue, les côtés des deux décagones doivent être nécessairement envisagés comme connus puisqu'ils sont égaux l'un à $\frac{\sqrt{5}-1}{2}$, l'autre à $\frac{\sqrt{5}+1}{2}$.

Soit maintenant une équation algébrique à une inconnue

$$f(x) = 0$$

de degré n. On dira que cette équation est *réductible* si la fonction rationnelle entière $f(x)$ est décomposable en deux fonctions rationnelles entières de degrés inférieurs à n ayant pour coefficients des combinaisons *rationnelles* des quantités connues, toute fonction rationnelle entière qui ne satisfait pas à cette condition étant, jusqu'à nouvel ordre, laissée hors de considération. Nous avons considéré précédemment le cas où l'on ne regarde comme quantités connues que les nombres entiers et les nombres fractionnaires.

L'équation du second degré

$$ax^2 + bx + c = 0$$

---

1) Grundzüge einer arithmetischen Theorie der algebraischen Grössen, Festschrift zu *E. E. Kummer*'s 50tem Doctor-Jubiläum 1881, éd. Berlin 1882; J. reine angew. Math. 92 (1882), p. 1; Werke 2, Leipzig 1897, p. 245.

2) Voir I 13 et, dans l'article actuel I 10, le n° **14**.

est en général irréductible. Elle est, au contraire, réductible si l'on suppose connue la différence des racines.

4. Aperçu historique. La distinction précédente apparaît pour la première fois dans les travaux de *N. H. Abel*[3]) qui donne aux quantités connues le nom de *quantités constantes*; elle forme la base de l'analyse de *E. Galois*[4]) auquel est due la dénomination plus juste de *quantités connues.* Mais dans le même temps des considérations purement arithmétiques conduisaient *C. F. Gauss* à une conception presque identique.

C. F. Gauss[5]) définit, dans l'introduction des „Disquisitiones arithmeticae" la théorie des nombres comme la partie des mathématiques qui traite des nombres entiers à l'exclusion des nombres fractionnaires et surtout des nombres irrationnels. Mais il remarqua lui-même que cette définition était trop étroite: il fut, en effet, amené, par ses recherches sur la loi de réciprocité des résidus biquadratiques, à étudier[6]) les lois de la divisibilité dans le domaine constitué par les nombres de la forme

$$a + ib$$

que l'on obtient en combinant aux deux nombres entiers a et b l'unité imaginaire $i = \sqrt{-1}$, laquelle joue par conséquent dans cette étude le rôle de quantité connue; il constata que ces lois étaient toutes semblables à celles qui gouvernent la divisibilité des nombres entiers eux-mêmes.

Après que *G. Eisenstein*[7]) eut traité au même point de vue certains domaines quadratiques et cubiques, *E. E. Kummer*[8]) fit intervenir comme quantités connues les racines de l'unité d'ordre convenablement choisi. Par là il peut être regardé comme ayant fondé définitivement la théorie qui nous occupe, car le cas ainsi traité présente toutes les circonstances essentielles du cas général et l'on y rencontre en particulier les difficultés qui nous occuperont aux n^{os} 24 et suiv.

---

3) Mém. posth. [1828]; Œuvres, éd. *L. Sylow* et *S. Lie* 2, Christiania 1881, p. 220.

4) Mém. posth. daté du 16 janvier 1831, publ. par *J. Liouville,* J. math. pures appl. (1) 11 (1846), p. 418; Œuvres, publ. par *E. Picard,* Paris 1897, p. 34.

5) Disquisitiones arithmeticae, Leipzig 1801, préface; trad. *A. Ch. M. Poullet-Delisle,* Recherches arithmétiques, Paris 1807, p. XI; Werke 1, Göttingue 1870, p. 5.

6) Theoria residuorum biquadraticorum (commentatio secunda) [Commentat. Soc. Gott. recent. 7 (1828/31), éd. Göttingue 1832, math. p. 98 [1831]; Werke 2, Göttingue 1876, p. 104].

L'idée directrice de *C. F. Gauss* dans cette difficile généralisation a été sans nul doute tirée de la théorie des fonctions lemniscatiques (fonctions inverses de l'intégrale $u = \int\limits_0^x \frac{dx}{\sqrt{1-x^4}}$) pour lesquelles il a dû connaître l'existence du théorème d'addition et celle d'une multiplication complexe permettant d'exprimer $\mathrm{sn}(\mu u; i)$ en fonction rationnelle de $\mathrm{sn}(u; i)$, $\mathrm{cn}(u; i)$, $\mathrm{dn}(u; i)$ pour $\mu = a + ib$.

7) J. reine angew. Math. 27 (1844), p. 80, 289, 311; 28 (1844), p. 28, 53, 289; 29 (1845), p. 19, 177/84 (fonction lemniscatique); Math. Abh., Berlin 1847, p. 1/120, 121/8.

8) J. reine angew. Math. 35 (1847), p. 319, 327.

5. Corps ou Domaine orthoïde. Domaine de rationalité. Au lieu de *quantités connues* on emploie aujourd'hui la locution équivalente de *corps* proposée par *R. Dedekind*[9]). Un *corps,* ou d'après *Gy. (J.) König*[10]) un *domaine orthoïde,* est un système de quantités telles qu'en additionnant, soustrayant multipliant ou divisant deux quelconques d'entre elles (pourvu que le diviseur ne soit pas nul) on retombe toujours sur une quantité appartenant au système.

L'ensemble des nombres réels rationnels (entiers et fractionnaires) de l'arithmétique constitue un corps $\mathfrak{R}$ et l'on voit aisément que ce corps est contenu dans tous les autres.

μ étant un entier choisi une fois pour toutes et non carré parfait, l'ensemble des quantités de la forme

$$a + b\sqrt{\mu},$$

où l'on donne à a et à b toutes les valeurs rationnelles possibles, constitue un corps car la somme, le produit, le quotient de deux quantités de cette nature est encore une quantité de la même espèce. Ce corps peut encore être défini comme formé par toutes les quantités qui deviennent rationnellement connues lorsque outre tous les nombres rationnels on considère comme connue l'irrationnelle $\sqrt{\mu}$.

Le *corps de Gauss* (n° 4) est celui qui correspond à $\mu = -1$,

L'expression de *domaine de rationalité* employée par *L. Kronecker*

---

9) *R. Dedekind* dans *G. Lejeune Dirichlet,* Vorlesungen über Zahlentheorie, (4e éd.) Brunswick 1894, p. 452 (Suppl. XI, sur la théorie des nombres algébriques, n° 160). Les principes sur lesquels reposent ces recherches ont été développés par *R. Dedekind* dans la seconde édition [Brunswick 1871, p. 423/97] de ce cours professé par *G. Lejeune Dirichlet*; voir aussi *R. Dedekind,* Bull. sc. math. (1) 11 (1876), p 278/88; (2) 1 (1877), p. 17/41, 69/92, 144/64, 207/48. Dans ce dernier article la définition des *corps* se trouve p. 150. Il faut entendre ici le mot *corps* dans le sens qu'on lui donne dans la locution *corps d'armée* par exemple.

10) *Gyula König,* Az algebrai mennyiségek általános elméletének alapvonalai, Budapest 1903; éd. allemande: *J. König,* Einleitung in die allgemeine Theorie der algebraischen Grössen, Leipzig 1903, p. 8. Les citations ultérieures se rapportent à l'édition allemande.

a sensiblement le même sens que *corps*; d'une manière plus précise[11]) elle est synonyme de *corps fini* (n° 7).

6. Corps de fonctions. Nous nous sommes bornés jusqu'ici au cas où les quantités connues étaient purement numériques. Mais l'hypothèse contraire s'est déjà présentée dans l'article I 9 où, en même temps que les fonctions rationnelles entières qui ont pour coefficients des nombres rationnels, on a considéré (n° **93**) les fonctions rationnelles entières dont les coefficients sont eux-mêmes des fonctions rationnelles de variables indépendantes auxiliaires et où l'on a constaté que les deux théories étaient entièrement parallèles.

Nous conviendrons dès lors que dans les définitions précédentes le mot *quantité* désigne indistinctement un *nombre* ou une fonction quelconque d'une ou de plusieurs variables. Il y a, d'après cela, deux sortes de corps: les *corps de nombres* et les *corps de fonctions.*

Le corps de fonctions le plus simple est le corps R qui est constitué par les fonctions rationnelles des variables envisagées.

On remarquera toutefois qu'il y a plusieurs corps de cette espèce suivant la nature des coefficients numériques qui doivent figurer dans les fonctions rationnelles en question. On peut admettre pour ces coefficients toutes les valeurs numériques possibles (point de vue de l'algèbre pure), mais on peut aussi les assujettir à appartenir à un certain corps de nombres K, par exemple à être rationnels. Nous considérerons les corps obtenus dans le premier cas comme devant seuls à proprement parler être désigné par R; il n'y a qu'un corps R de fonctions d'une variable, un corps R de fonctions de deux variables, ..., un corps R de fonctions de *n* variables. Tout corps qu'on obtient en astreignant les coefficients des fonctions rationnelles qui le constituent à faire partie du corps numérique K sera toujours désigné par R_{K}. Ainsi $\mathrm{R}_{\mathfrak{R}}$ est le corps constitué par les fonctions rationnelles des variables envisagées ayant pour coefficients des nombres rationnels ordinaires.

[Bien entendu (cf. n° 2) pour *L. Kronecker* il en serait tout autrement. Le corps qui devrait être à son point de vue désigné par R est celui qui dans notre terminologie est représenté par $\mathrm{R}_{\mathfrak{R}}$].

Il nous arrivera d'employer la locution de *corps général* R lorsque nous voudrons spécifier d'une manière formelle qu'aucune restriction de nature arithmétique n'est imposée aux coefficients numériques. C'est ce qui aura lieu toutes les fois que nous aurons en vue des interprétations analytiques ou géométriques (cf. n° 7).

11) *Gy.* (*J.*) *König,* Alg. Grössen [10]), p. 182/4.

Contrairement à ce qui avait lieu pour les nombres, le corps R n'est pas contenu dans tous les autres corps de fonctions. On peut former des corps de fonctions transcendantes, par exemple le corps de toutes les fonctions elliptiques aux mêmes périodes, celui des fonctions modulaires, etc qui ne contiennent pas le corps R. On peut même former des corps ne contenant que des fonctions rationnelles et ne contenant cependant pas le corps R. C'est le cas, par exemple, pour les fonctions symétriques rationnelles de *n* variables qui à elles seules forment un corps.

7. Adjonction. Nombres algébriques. Fonctions algébriques. Après s'être astreint jusqu'à un certain moment à n'introduire dans les calculs que les quantités appartenant à un certain corps (de nombres ou de fonctions) K, on peut convenir, à partir de ce moment, de regarder en outre comme connues une ou plusieurs quantités n'appartenant pas à K. On dit alors qu'on *adjoint* ces quantités. On forme ainsi un nouveau corps K′ comprenant outre les quantités du *corps générateur* K les quantités adjointes et leurs combinaisons rationnelles entre elles ou avec les premières.

L. Kronecker[12]) dit, dans ce cas, que K′ contient K ou est engendré par K. D'autres disent que K′ est un *multiple*[13]) de K, ou un *corps supérieur*[14]) à K [Körper über K[14]); Oberkörper[15])]. Ce dernier est un *diviseur*[13]) de K′ [Divisor[13]), Teiler[14])] ou encore un *sous-corps*[15]) de K′.

On peut désigner le corps supérieur K′ par la notation

$$\mathrm{K}' = (\mathrm{K}, \eta_1, \eta_2, \ldots)$$

$\eta_1, \eta_2, \ldots$ étant les quantités adjointes.

La notion d'adjonction et la découverte de son importance pour la théorie des équations algébriques sont dues à *E. Galois*[16]).

L'ensemble des quantités communes à deux corps K et K′ forme évidemment lui-même un corps, le *plus grand commun diviseur*[17]) ou l'*intersection*[17]) [Durchschnitt[18])] des deux premiers.

12) Festschrift [1]) § 2; J. reine angew. Math. 92 (1882), p. 5/7; Werke 2, p. 251/3.

13) *R. Dedekind* dans *G. Lejeune Dirichlet,* Zahlenth. [9]), (4ᵉ éd.) p. 453 (Suppl. XI, n° 160); *R. Dedekind,* Bull. sc. math. (2) 1 (1877), p. 150.

14) *H. Weber,* Lehrbuch der Algebra (2ᵉ éd.) 1, Brunswick 1898, p. 492; trad. *J. Griess* 1, Paris 1898, p. 524.

15) *D. Hilbert,* Jahresb. deutsch. Math.-Ver. 4 (1894/5), éd. Berlin 1897, p. 203.

16) *E. Galois,* Bull. sc. math. astron. phys. chim. 13 (1830), p. 271; J. math. pures appl. (1) 11 (1846), p. 395; Œuvres [4]), p. 11; voir aussi *E. Galois,* mém. posth. [4]); J. math. pures appl. (1) 11 (1846), p. 417; Œuvres [4]), p. 33.

17) *R. Dedekind* dans *G. Lejeune Dirichlet,* Zahlenth. [9]), (4ᵉ éd.), p. 454 (Suppl. XI, n° 160).

L'ensemble des quantités que l'on peut exprimer rationnellement à l'aide des éléments de K et de ceux de K′ forme aussi un corps, le *plus petit commun multiple*[17]) ou le *corps composé*[19]) de K et de K′.

Les corps les plus intéressants sont les *corps algébriques* ou *corps finis*[20]).

Un corps K′ supérieur à K est dit *fini* ou *algébrique* relativement à K si chacune des quantités adjointes est racine d'une équation algébrique ayant pour coefficient des quantités appartenant à K. On peut toujours[21]) dans ces conditions passer de K à K′ par l'adjonction d'une quantité unique ξ.

On caractérise encore[22]) les corps finis par cette condition qu'il existe un nombre fini n des quantités $\eta_1, \eta_2, \ldots, \eta_n$ appartenant à K′ et telles que tout autre élément y de K′ puisse se mettre sous la forme

$$y = u_1\eta_1 + u_2\eta_2 + \cdots + u_n\eta_n \tag{1}$$

$u_1, u_2, \ldots, u_n$ étant rationnels en K. On dit alors[22]) que l'ensemble $(\eta_1, \eta_2, \ldots, \eta_n)$ forme une *base* du corps K′.

Les quantités $\eta_1, \eta_2, \ldots, \eta_n$ seront par exemple les puissances $0, 1, 2, \ldots, n-1$ de celle que nous avons désignée tout à l'heure par ξ, si n est le degré de l'équation algébrique en ξ dont les cofficients sont fonctions des éléments de K.

Les corps finis ou algébriques *au sens absolu du mot* sont ceux

18) *E. Zermelo*, Math. Ann. 65 (1908), p. 107. *E. Zermelo* emploie d'ailleurs le mot „Durchschnitt" dans le sens indiqué, non pas seulement dans le cas où l'on envisage des *corps* déterminés, mais pour tous les *ensembles* possibles.

19) *D. Hilbert*, Jahresb. deutsch. Math.-Ver. 4 (1894/5), éd. Berlin 1897, p. 247.

20) *R. Dedekind* dans *G. Lejeune Dirichlet*, Zahlenth.[9]), (4e éd.) p. 466 (Suppl. XI, n° 164); *R. Dedekind*, Bull. sc. math. (2) 1 (1877), p. 150.

21) Ce fait est implicitement contenu dans *E. Galois* [mém. posth.[4]); J. math. pures appl. (1) 11 (1846), p. 419/20; Œuvres[4]), p. 35/6] et dans *N. H. Abel* [Précis d'une théorie des fonctions elliptiques, chap. 2 § 1, mém. posth. publié dans ses Œuvres (1re éd.) rédigée par *B. M. Helmboë* 1, Christiania 1839, p. 351; réimpr. dans ses Œuvres, éd. *L. Sylow* et *S. Lie* 1, Christiania 1881, p. 546]. Un cas particulier du même fait est même implicitement contenu dans *J. L. Lagrange*, Réflexions sur la résolution algébrique des équations (nos 103, 104) [Nouv. Mém. Acad. Berlin 2 (1771), éd. 1773, p. 218/21; Œuvres publ. par *J. A. Serret* 3, Paris 1869, p. 385/8].

Voir *J. A. Serret*, Algèbre supérieure (6e éd.) 2, Paris 1910, p. 433/46; *H. Weber*, Alg.[14]) 1, p. 499 (n° 150); trad. *J. Griess* 1, p. 531; *J. Molk*, Thèse, Paris 1884; Acta math. 6 (1885), p. 38/40.

22) *R. Dedekind* dans *G. Lejeune Dirichlet*, Zahlenth.[9]), (4e éd.), p. 466/74 (Suppl. XI, n° 164); *R. Dedekind*, Bull. sc. math. (2) 1 (1877), p. 150/1.

pour lesquels le *corps* dont ils procèdent par adjonction de ξ est l'un des domaines $\mathfrak{R}$, $R_{\mathfrak{R}}$ ou R définis aux nos **5** et **6**. *L. Kronecker*[23]) donne à ces derniers la dénomination commune de *domaines naturels de rationalité* et leur oppose les corps algébriques considérés comme *corps dérivés* (*Gattungsbereiche*) engendrés dans les corps naturels de rationalité.

[Si l'on se place au point de vue de l'Arithmético-algèbre les domaines $\mathfrak{R}$ et $R_{\mathfrak{R}}$ doivent seuls être envisagés comme des domaines *naturels* de rationalité et l'on n'a donc à tenir compte ici que des corps dérivés dont le corps générateur est soit $\mathfrak{R}$ soit $R_{\mathfrak{R}}$].

L'étude des corps dérivés engendrés dans un domaine $\mathfrak{R}$ fait l'objet de la théorie des *nombres algébriques*. L'étude des corps dérivés engendrés dans un domaine R fait l'objet de la théorie ordinaire des *fonctions algébriques*. L'étude des corps dérivés engendrés dans un domaine $R_{\mathfrak{R}}$ fait l'objet de l'arithmético-algèbre des *fonctions algébriques*.

On dit qu'un nombre (réel ou imaginaire) est un *nombre algébrique* lorsque ce nombre est racine d'une équation algébrique, à coefficients *rationnels*,

$$f(x) = 0.$$

On dit qu'une fonction y des variables indépendantes $x_1, x_2, \ldots, x_n$ est une fonction algébrique de n variables indépendantes quand y est racine d'une équation algébrique

$$f(y) = 0$$

dont les coefficients sont des *fonctions rationnelles* de $x_1, x_2, \ldots, x_n$.

On appelle nombres *transcendants* les nombres qui ne sont pas algébriques, et *fonctions transcendantes* les fonctions qui ne sont pas algébriques.

Si K est un corps algébrique au sens absolu du mot et si K′ est un corps algébrique relativement à K, le corps K′ peut être dérivé du domaine $\mathfrak{R}$, d'un domaine R ou d'un domaine $R_{\mathfrak{R}}$; le corps K′ est donc aussi un corps algébrique au sens absolu du mot.

L'étude des propriétés de K′ est toutefois différente suivant que nous envisageons K′ comme dérivé de K ou comme dérivé directement du domaine naturel de rationalité.

Ainsi dans la première alternative une *base* de K′ (dans le sens précédent) est formée par un nombre moindre d'éléments que dans la seconde alternative; en effet, dans la première alternative $u_1, u_2, \ldots, u_n$

23) *L. Kronecker*, Festschrift[1]) § 2, 3; J. reine angew. Math. 92 (1882), p. 5/10; Werke 2, p. 251/6.

peuvent être des quantités quelconques dans K, tandis que dans la seconde alternative ils font nécessairement partie du domaine naturel de rationalité. De ces deux façons d'envisager les choses, celle où l'on envisage K' comme dérivé de K conduit à des recherches plus difficiles que l'autre mais elle permet de pénétrer davantage dans l'étude des propriétés des corps algébriques.

Observons encore que certains corps jouissent de la propriété que voici: chaque équation algébrique dont les coefficients appartiennent à un tel corps est satisfaite *au moins* par l'*une* des quantités qui appartiennent à ce corps. *L. Kronecker*[24]) a mentionné l'existence de ces corps qu'il a désignés sous le nom de *domaines clos* (*geschlossene Grössenbereiche*) [I 9, **93**] sans toutefois sembler attacher une grande importance à leur introduction systématique en Algèbre.

L'ensemble des nombres naturels n'est pas clos, mais l'ensemble des nombres algébriques est clos.

L'ensemble des nombres réels n'est pas clos, mais l'ensemble des nombres complexes (réels et imaginaires) est clos.

Le corps R n'est pas clos, mais l'ensemble des fonctions algébriques d'une ou de plusieurs variables indépendantes est un corps clos.

Toute fonction rationnelle entière $f(x)$ d'*une seule* variable dont les coefficients font partie d'un corps clos peut être, dans ce corps clos, décomposée en facteurs *linéaires*. Toutes les racines de l'équation

$$f(x) = 0$$

appartiennent donc au même corps clos que les coefficients de $f(x)$.

Les corps *algébriques* ou *finis* au sens absolu ne sont pas clos.

Un exemple de corps *non fini* et cependant non clos est celui qui est formé par tous les nombres réels.

8. Interprétation fonctionnelle. Fonctions rationnelles sur une courbe ou sur une surface algébrique. Comme nous l'avons dit, l'étude des corps algébriques, le corps générateur étant le corps *général* R (n° **6**), est l'objet de la théorie des fonctions algébriques. Cette théorie fait partie de l'Analyse et est aussi intimement liée à la Géométrie algébrique.

Tout résultat de la théorie des corps aura ainsi une signification analytique et géométrique que nous indiquerons sous la rubrique *interprétation fonctionnelle.*

Soit

$$f(x_1, x_2, \ldots, x_n, y)$$

24) Festschrift[1]) § 3; J. reine angew. Math. 92 (1882), p. 10; Werke 2, p. 255/6.

une fonction rationnelle entière de $x_1, x_2, \ldots, x_n, y$ qui ne puisse être décomposée en facteurs de degré inférieur, même quand on admet que les coefficients de chaque facteur puissent être des nombres quelconques réels ou imaginaires. L'équation

$$(1) \qquad f(x_1, x_2, \ldots, x_n, y) = 0$$

qui définit y comme une fonction algébrique de $x_1, x_2, \ldots, x_n$ est considérée en géométrie algébrique pour $n = 1$ comme l'équation d'une courbe plane algébrique irréductible et pour $n > 1$ comme celle d'une surface algébrique irréductible dans l'espace à $n + 1$ dimensions. Les fonctions rationnelles de la forme

$$\frac{\mathrm{P}(x_1, x_2, \ldots, x_n, y)}{\mathrm{Q}(x_1, x_2, \ldots, x_n, y)},$$

où P et Q sont des fonctions rationnelles entières quelconques, sont dites en géométrie algébrique fonctions rationnelles *attachées* pour $n = 1$ à la courbe (1), ou pour $n > 1$ à la surface (1). A notre point de vue actuel elles forment le *corps*[25]) qu'on obtient en adjoignant y à l'ensemble des fonctions rationnelles des variables indépendantes $x_1, x_2, \ldots, x_n$ c'est-à-dire au corps *général* R (n° **6**).

9. Généralisations. Domaines hyperorthoïdes. Domaines pseudo-orthoïdes. On peut étendre la notion de *corps* ou de *domaine orthoïde* au cas où les opérations fondamentales de l'arithmétique sont prises dans un sens généralisé. La notion de *corps* apparaît alors comme une spécialisation de celle de *groupe*, et la notion de *domaine orthoïde* comme une spécialisation de celle de *corps.*

*On dit[26]) d'un ensemble d'objets qu'il forme un *groupe* dans le sens le plus général du mot, lorsqu'on se donne une règle permettant de déduire de deux quelconques A et B des objets de l'ensemble un troisième objet C de ce même ensemble. Chacun des objets de l'ensemble prend alors le nom d'*élément* du groupe, et l'on dit de l'élément C qu'il est obtenu par *composition* des éléments A et B. Dans un même groupe on peut d'ailleurs en général composer les éléments de diverses manières; ainsi dans le groupe formé par l'ensemble des nombres naturels la composition peut se faire par addition, multiplication et exponentiation.

25) On trouve aussi chez les auteurs allemands la dénomination de *genre* (*genus, Gattung*) ou encore celle de *système* [cf. *B. Riemann*, J. reine angew. Math. 54 (1857), p. 133; Werke, (2e éd.), publ. par *H. Weber*, Leipzig 1892, p. 119; trad. *L. Laugel*, Paris 1898, p. 131] appliqué à un tel ensemble de fonctions algébriques.

26) *Ce numéro 9 a été rédigé par *J. Kürschák* en utilisant le texte correspondant de l'article allemand de *G. Landsberg*. Malgré leur importance il n'a pu être tenu compte des recherches en cours de publication de *E. Steinitz* [cf. J. reine angew. Math. 137 (1910), p. 167].*

Un groupe prend le nom de *corps* lorsque les éléments de ce groupe se composent de deux façons distinctes, auxquelles on donne le nom d'*addition* et de *multiplication*, satisfaisant aux six premières des conditions que voici:

1°) Les deux modes de composition (l'addition et la multiplication) sont liés par la loi de *distribution* en sorte que si A, B, C désignent trois éléments quelconques du groupe on a, en convenant d'employer les symboles d'addition et de multiplication de l'arithmétique élémentaire pour représenter les deux modes de composition nommés ici addition et multiplication,

$$A(B+C) = AB + AC$$
$$(A+B)C = AC + BC.$$

2°) L'addition est *associative* et *commutative*, en sorte que l'on a

$$A + (B + C) = (A + B) + C$$
$$A + B = B + A.$$

3°) L'opération inverse de l'addition, à laquelle on donne le nom de *soustraction*, est *univoque* et *toujours possible*, en sorte que, quels que soient les deux éléments A, B du groupe que l'on envisage, il existe dans le groupe un et un seul élément X satisfaisant à la relation

$$A + X = B;$$

on représente cet élément par le symbole

$$X = B - A.$$

Des conditions précédentes on déduit immédiatement que l'élément $A - A$ est indépendant du choix que l'on fait pour A dans le groupe envisagé et que cet élément $A - A$, auquel on donne le nom de *zéro* et qu'on représente par le symbole 0, vérifie les relations

$$0 \cdot A = A \cdot 0 = 0$$

pour tout élément A du groupe envisagé.

Lorsqu'à un certain élément D d'un groupe on peut faire correspondre au moins un élément D', différent de 0, du même groupe, tel que l'une au moins des deux égalités

$$D \cdot D' = 0, \qquad D' \cdot D = 0$$

soit vérifiée, on dit que D est un *diviseur de zéro.* Tout diviseur de zéro est dit *diviseur propre de zéro* lorsqu'il n'est pas lui-même égal à zéro.

Si l'élément A d'un groupe n'est pas diviseur de zéro, on déduit des conditions précédentes que chacune des deux équations

$$A \cdot X = B, \qquad Y \cdot A = B$$

admet, quel que soit l'élément B du groupe que l'on envisage, au plus une seule solution.

4°) La multiplication est *associative*, en sorte que l'on a, quels que soient les éléments A, B, C du groupe que l'on envisage,

$$A(B \cdot C) = (A \cdot B)C.$$

5°) L'équation

$$X \cdot X = X$$

est vérifiée par un élément X du groupe envisagé qui n'est pas diviseur de zéro.

On déduit des conditions précédentes que cet élément X composé par multiplication avec un quelconque des éléments A du groupe vérifie les relations

$$X \cdot A = A \cdot X = A$$

et que cet élément X est *unique* dans le groupe. On désigne cet élément unique par le symbole 1 et on le nomme l'*unité absolue* du corps.

6°) Si l'élément A du groupe n'est pas diviseur de zéro, chacune des deux équations

$$A \cdot X = B, \qquad Y \cdot A = B$$

admet une solution pour chaque élément B du groupe.

On déduit des conditions précédentes que, A étant arbitrairement fixé parmi les non-diviseurs de zéro du groupe, les solutions des deux équations

$$A \cdot X = 1, \qquad Y \cdot A = 1$$

sont égales; on les désigne toutes deux par le symbole

$$\frac{1}{A}.$$

La solution de l'équation

$$A \cdot X = B$$

est alors

$$X = \frac{1}{A} \cdot B$$

et celle de l'équation

$$Y \cdot A = B$$

est

$$Y = B \cdot \frac{1}{A};$$

ces deux solutions peuvent d'ailleurs être distinctes.

C'est ainsi encore que *K. Hensel*[27]) a pu considérer des *corps de*

27) J. reine angew. Math 127 (1904), p. 116/166.

matrices, l'addition et la multiplication de deux matrices étant prises au sens défini par *A. Cayley*[28]).

H. Weber[29]) emploie la notion de *corps* dans un sens plus restreint. Pour qu'un groupe constitue un corps au sens de *H. Weber,* il faut que ses éléments satisfassent non seulement aux six conditions précédentes mais encore aux deux conditions que voici:

7⁰) La multiplication est *commutative,* en sorte que l'on a

$$AB = BA$$

quels que soient les éléments A, B du groupe que l'on envisage.

8⁰) Le groupe ne contient aucun diviseur propre de zéro, en sorte qu'un produit ne peut être égal à zéro que si l'un de ses facteurs est égal à zéro.

Pour les corps au sens de *H. Weber* on a toujours

$$\frac{1}{A} \cdot B = B \cdot \frac{1}{A}$$

en sorte qu'il n'y a qu'une seule opération inverse de la multiplication; on lui donne le nom de *division* et au lieu de $\frac{1}{A} \cdot B$ et de $B \cdot \frac{1}{A}$ on écrit simplement $\frac{B}{A} \cdot$ Si le diviseur est différent de zéro, la division est univoque et toujours possible.

Gy. (J.) König[30]) appelle *domaines orthoïdes* les groupes dont les éléments satisfont en premier lieu aux huit conditions précédentes et en outre à la condition que voici:

9⁰) Une somme

$$1 + 1 + 1 + \cdots + 1$$

d'un nombre quelconque d'éléments, chacun égal à 1, n'est jamais égale à zéro.

Les domaines orthoïdes constituent donc une partie seulement des corps au sens de *H. Weber.* L'ensemble des nombres rationnels est un domaine orthoïde tout comme chacun des corps de nombres ou de fonctions dont nous avons parlé dans les n^os^ 5, 6 et 7.

Gy. (J.) König appelle *domaines hyperorthoïdes* les groupes dont les éléments satisfont aux conditions 1⁰) à 7⁰) et à la conditions 9⁰) sans satisfaire à la condition 8⁰).

---

28) Philos. Trans. London 148 (1858), p. 17/37, en partic. p. 19, 21; Papers 2, Cambridge 1889, p. 475/96, en partic. p. 477, 479.

29) Math. Ann. 43 (1893), p. 521/49; voir en partic. p. 526.

30) Alg. Grössen[10]), p. 8, 148, 408.

On obtient[31]) par exemple un domaine hyperorthoïde en composant par addition et multiplication les expressions linéaires de la forme

$$a + bx,$$

où a et b désignent des nombres complexes (réels ou imaginaires) quelconques, si l'on convient de supprimer dans chaque élément les termes où x figure à une puissance supérieure à la première. Dans ce domaine hyperorthoïde les diviseurs de zéro sont les éléments de la forme

$$bx.$$

Les domaines hyperorthoïdes sont des corps au sens général du mot, mais non au sens de *H. Weber.*

Gy. (J.) König appelle *domaine pseudo-orthoïde* les groupes dont les éléments satisfont aux conditions (1⁰) à (8⁰) sans satisfaire à la condition (9⁰).

Pour obtenir un domaine pseudo-orthoïde il suffit de composer par addition et multiplication le groupe des nombres rationnels entiers en convenant d'envisager comme identiques les nombres qui sont congrus suivant un module déterminé p, où p est un nombre premier. Nous désignerons dans ce numéro ce domaine par le symbole $\mathfrak{R}_p$.

Le domaine $\mathfrak{R}_2$ ne comprend que les deux éléments 0 et 1 et ces éléments vérifient les relations

$$0 + 0 = 1 + 1 = 0, \qquad 1 + 0 = 0 + 1 = 1,$$
$$0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0, \qquad 1 \cdot 1 = 1.$$

Les domaines pseudo-orthoïdes sont compris parmi les corps au sens de *H. Weber.* Un corps au sens de *H. Weber* forme soit un domaine orthoïde, soit un domaine pseudo-orthoïde suivant que la condition (9⁰) est vérifiée ou non.

Parmi les corps au sens de *H. Weber,* les plus remarquables sont ceux qu'il appelle[32]) *corps congruentiels.* Voici comment on peut les définir:

Si Ω représente un corps quelconque au sens de *H. Weber* et si t désigne une variable indépendante ne faisant pas partie de Ω, envisageons les fonctions rationnelles entières de t

$$A_0 + A_1 t + A_2 t^2 + \cdots + A_m t^m$$

dont les coefficients sont des éléments quelconques de Ω et convenons que les compositions par addition et par multiplication de deux quel-

---

31) *Gy. (J.) König,* Alg. Grössen[10]), p. 227; *E. Study,* Geometrie der Dynamen, Leipzig 1903, p. 195.

32) Math. Ann. 43 (1893), p. 534.

conques de ces fonctions rationnelles entières de t

$$A_0 + A_1 t + A_2 t^2 + \cdots + A_m t^m, \qquad B_0 + B_1 t + B_2 t^2 + \cdots + B_n t^n$$

donnent naissance, comme en algèbre élémentaire, respectivement aux fonctions rationnelles entières

$$(A_0 + B_0) + (A_1 + B_1)t + (A_2 + B_2)t^2 + \cdots$$
$$A_0 B_0 + (A_0 B_1 + A_1 B_0)t + (A_0 B_2 + A_1 B_1 + A_2 B_0)t^2 + \cdots$$

Parmi les fonctions de t ainsi obtenues, envisageons en particulier celles dont le coefficient de la puissance la plus élevée de t est égal à 1 (c'est-à-dire à l'unité absolue du corps Ω). Nous dirons d'une telle fonction quelle est *irréductible* dans Ω, si elle ne peut être mise sous la forme d'un produit de deux fonctions rationnelles entières de t ayant chacune pour coefficients des éléments de Ω et pour coefficient de la puissance la plus élevée de t l'unité absolue de Ω.

Convenons enfin, après avoir fixé une fonction rationnelle entière irréductible en Ω,

$$g(t) = t^\nu + \omega_1 t^{\nu-1} + \cdots + \omega_\nu$$

à laquelle nous donnerons le nom de *module*, d'envisager comme identiques deux fonctions rationnelles entières de t dont les coefficients sont des éléments de Ω, lorsque la différence de ces deux fonctions est divisible par $g(t)$. L'ensemble des fonctions rationnelles entières de t,

$$\varphi(t) = A_0 + A_1 t + A_2 t^2 + \cdots + A_{\nu-1} t^{\nu-1}$$

de degrés plus petits que le degré ν du module $g(t)$, et dans lesquelles les coefficients $A, A_1, A_2, \ldots, A_{\nu-1}$ sont des éléments du corps Ω, constitue alors un corps au sens de *H. Weber*. On représente ce corps par le symbole

$$\Omega(t)$$

et on l'appelle *corps supérieur à Ω congruentiel relativement au module $g(t)$*.

Suivant que le corps Ω forme un domaine orthoïde ou pseudo-orthoïde le corps congruentiel $\Omega(t)$ formera aussi un domaine orthoïde ou pseudo-orthoïde et cela quel que soit le module $g(t)$ envisagé.

Si l'on prend, en particulier, pour Ω le corps $\mathfrak{R}$ formé par l'ensemble des nombres rationnels, la composition des éléments du corps $\Omega(t)$ congruentiel à Ω relativement au module $g(t)$, est identique à celle des éléments du domaine orthoïde $(\mathfrak{R}, \eta)$ que l'on obtient en *adjoignant* au corps $\mathfrak{R}$ une des racines η de l'équation irréductible

$$g(t) = 0.$$

Si l'on prend pour Ω le corps représenté plus haut par le symbole $\mathfrak{R}_p$, la composition des éléments du corps $\Omega(t)$ supérieur à Ω

congruentiel relativement au module $g(t)$ est identique à celle des *imaginaires de Galois*[33]. [Cf. I 15].

Soient Ω et Ω' deux groupes, chacun à deux compositions distinctes de ses éléments. On dit que ces deux groupes sont *identiques abstraitement parlant* lorsque leurs éléments se correspondent parfaitement (cf. I 1, **1**) et de telle façon que si dans le groupe Ω on a

$$C = A + B \quad \text{ou} \quad C = A \cdot B$$

on ait aussi entre les éléments correspondants du groupe Ω'

$$C' = A' + B' \quad \text{ou} \quad C' = A' \cdot B'.$$

Si un corps, au sens de *H. Weber*, ne comprend qu'un nombre *fini* d'éléments, il est identique, abstraitement parlant[34]), à un domaine pseudo-orthoïde dont les éléments sont des imaginaires de Galois.

Chaque domaine orthoïde est identique, abstraitement parlant, à un domaine orthoïde dont les éléments sont constitués par des nombres, des variables indépendantes et certaines fonctions algébriques de ces variables indépendantes. *Gy. (J.) König* n'a d'ailleurs jamais envisagé d'autres domaines orthoïdes.

Toutes les recherches concernant la réductibilité des fonctions rationnelles entières dont les coefficients sont des éléments d'un domaine orthoïde K ne dépendent finalement que de la façon dont les éléments du domaine K se composent par addition et multiplication. *Dans ces recherches* on peut donc toujours remplacer chaque domaine orthoïde par un quelconque des domaines orthoïdes qui lui sont identiques, abstraitement parlant, à la seule condition de remplacer les éléments de l'ancien domaine par les éléments correspondants du nouveau domaine envisagé.

Dans toute recherche algébrique, on peut ainsi, en particulier, comme l'a fait observer *L. Kronecker*[35]), éviter l'emploi des nombres transcendants. Soit, en effet, K un domaine orthoïde ayant pour éléments des nombres algébriques et soient $\eta_1, \eta_2, \eta_3, \ldots$ des nombres transcendants entre lesquels nous supposerons d'abord qu'il n'y ait aucune relation algébrique à coefficients rationnels. Désignons par

$$\mathrm{K}' = (\mathrm{K}, \eta_1, \eta_2, \eta_3, \ldots)$$

---

33) *E. Galois*, Bull. sc. math. astron. phys. chim. 13 (1830), p. 428; J. math. pures appl. (1) 11 (1846), p. 399; Œuvres[4]), p. 15.

34) *E. H. Moore*, Mathematical papers of the Chicago Congress 1893, éd. New-York 1896, p. 210; *L. E. Dickson*, Linear groups with an exposition of the Galois Field theory, Leipzig 1901, p. 13.

35) Festschrift[1]), § 3; J. reine angew. Math. 92 (1882), p. 7; Werke 2, p. 253.

le domaine orthoïde formé en adjoignant aux éléments de K les nombres transcendants $\eta_1, \eta_2, \eta_3, \ldots$ Envisageons une relation de la forme

$$F(\eta_1, \eta_2, \ldots; x, y, \ldots) = F_1(\eta_1, \eta_2, \ldots; x, y, \ldots) F_2(\eta_1, \eta_2, \ldots; x, y, \ldots)$$

où F, F_1, F_2 désignent des fonctions rationnelles entières de $x, y, \ldots$ dont les coefficients sont des éléments du domaine K′; toute relation de cette forme continuera à avoir lieu quand on y remplace $\eta_1, \eta_2, \eta_3, \ldots$ par des variables indépendantes. Rien n'est donc changé aux recherches concernant la réductibilité des fonctions rationnelles entières si l'on envisage les nombres transcendants $\eta_1, \eta_2, \eta_3, \ldots$ comme s'ils étaient des variables indépendantes.

Le même fait a encore lieu lorsque les nombres transcendants envisagés $\eta_1, \eta_2, \eta_3, \ldots$ sont liés par une ou plusieurs relations algébriques à coefficients rationnels ou même par une ou plusieurs relations algébriques dont les coefficients font partie du domaine orthoïde K, à condition seulement de remplacer $\eta_1, \eta_2, \eta_3, \ldots$ non plus par des variables indépendantes, mais par des variables satisfaisant aux mêmes relations algébriques que $\eta_1, \eta_2, \eta_3, \ldots$

Dans d'autres recherches mathématiques, en particulier dans celles où le fait pour une des grandeurs envisagées d'être plus grande ou plus petite qu'une autre joue un rôle essentiel, on parviendrait au contraire à des résultats faux ou absurdes en remplaçant par des variables les nombres transcendants que l'on rencontre dans la suite des raisonnements. Il n'est donc permis de remplacer ainsi les nombres transcendants par des variables que dans des recherches où seule joue un rôle la façon dont les éléments du domaine envisagé se composent par addition et multiplication.

E. Maillet[36]) a constitué des corps avec des nombres transcendants.

Dans toute recherche algébrique, on peut de même remplacer les fonctions transcendantes par de nouvelles variables. Si l'on envisage, par exemple, le domaine orthoïde K dont les éléments sont les fonctions rationnelles de $\sin t$ et de $\cos t$, on peut, dans toute recherche concernant la réductibilité dans ce domaine K des fonctions rationnelles entières dont les coefficients sont des éléments de K, remplacer $\sin t$ et $\cos t$ par deux nouvelles variables u et v liées par la relation

$$u^2 + v^2 = 1.$$

Les domaines orthoïdes K formés d'une partie seulement des

36) **E. Maillet,* Introduction à la théorie des nombres transcendants et des propriétés arithmétiques des fonctions, Paris 1906, p. 25/56 (chap. 3).*

éléments du corps R méritent de fixer aussi notre attention. Dans toute recherche algébrique on peut, en effet, si l'on veut, envisager chacun de ces domaines orthoïdes comme constitué par *toutes* les fonctions rationnelles de certaines nouvelles variables et, éventuellement, de certaines fonctions algébriques de ces nouvelles variables.

Si l'on se donne, par exemple, le domaine orthoïde K formé par l'ensemble des fonctions *symétriques* rationnelles de k variables $x_1, x_2, \ldots, x_k$, on peut aussi envisager K comme formé par l'ensemble de *toutes* les fonctions rationnelles des nouvelles variables $c_1, c_2, \ldots, c_k$ définies comme fonctions symétriques élémentaires (I 9, **7**) de $x_1, x_2, \ldots, x_k$. Ces nouvelles variables $c_1, c_2, \ldots, c_k$ sont indépendantes les unes des autres; il n'y a aucune relation algébrique entre elles.

Si l'on se donne le domaine orthoïde K formé par les fonctions symétriques rationnelles des systèmes

$$(x_1, y_1, z_1), (x_2, y_2, z_2), \ldots, (x_k, y_k, z_k),$$

on peut envisager K comme formé par l'ensemble de *toutes* les fonctions rationnelles des nouvelles variables $c_{\alpha\beta\gamma}$ définies comme fonctions symétriques élémentaires (I 9, **7**) des systèmes

$$(x_1, y_1, z_1), (x_2, y_2, z_2), \ldots, (x_k, y_k, z_k);$$

ici ces nouvelles variables $c_{\alpha\beta\gamma}$ ne sont pas indépendantes; elles sont liées par certaines relations algébriques déterminées.

Dans tout ce qui suit nous entendrons en général par „corps“ un corps de nombres ou un corps de fonctions dans le sens qui a été fixé aux n^os **5** et **6**, en d'autres termes un „domaine orthoïde.“

10. Équations irréductibles. Étant donné un corps K, la définition de l'irréductibilité doit être formulée ainsi:

Une équation algébrique $f(x) = 0$ dont les coefficients appartiennent au corps K est dite *irréductible dans ce corps* quand son premier membre ne peut pas être considéré comme le produit de deux fonctions rationnelles entières en x, à coefficients *rationnels en* K et de degrés différents de zéro.

Il est clair qu'une équation irréductible dans un certain corps peut être réductible dans un corps supérieur.

Dans les corps *naturels* [n° **7**] $\mathfrak{R}$ et $\mathrm{R}_{\mathfrak{R}}$ on sait toujours [cf. I 9, **89**, **92** et **93** V], comme le demandait *L. Kronecker*[37]), reconnaître par

37) *L. Kronecker* [voir par exemple Festschr.[1]) § 4; J. reine angew. Math. 92 (1882), p. 10/13; Werke 2, p. 256/60] considérait cette condition comme indispensable à la légitimité d'une définition. Cette opinion est opposée à celle de beaucoup de mathématiciens; voir par exemple *R. Dedekind,* Was sind und was sollen die Zahlen, (1^e éd.), Brunswick 1888; (2^e éd.) Brunswick 1893, p. 2 en note.

un nombre fini d'essais si une équation donnée est irréductible et, dans le cas contraire, décomposer son premier membre en facteurs irréductibles[38].

Dans tout corps dérivé engendré dans $\mathfrak{R}$ ou $R_{\mathfrak{R}}$ on parvient aussi au même résultat par un nombre fini d'essais[39] [cf. I 9, **94**].

Il n'en est pas de même pour le corps R du moins en ce qui concerne la formation des deux facteurs. Toutefois si l'on suppose que toute équation algébrique à coefficients numériques puisse être résolue numériquement, on peut (I 9, **93** V), à l'aide du procédé permettant cette résolution numérique, joint à un nombre fini d'opérations rationnelles, décider si une équation quelconque donnés est réductible ou irréductible dans le corps R.

Dans tout corps *dérivé* engendré dans R on parvient de même, par un nombre fini d'essais, à ramener toute recherche concernant la réductibilité d'une fonction rationnelle entière à celle de la réductibilité des fonctions dans le domaine R lui-même.

Dans un corps quelconque K la décomposition d'une fonction rationnelle entière réductible $f(x)$ en un produit de fonctions irréductibles est *unique* si l'on convient de ne pas considérer comme distinctes deux fonctions rationnelles entières qui ne diffèrent que par un facteur indépendant de x[40].

Une équation algébrique (E) irréductible dans un corps K n'a avec une autre équation, de degré fini, (E′) à coefficients rationnels en K aucune racine commune à moins que toutes les racines de (E) n'appartiennent à (E′). Cette proposition ne s'étend pas au cas où

38) Voir *L. Kronecker,* J. reine angew. Math. 94 (1883), p. 344/8; Werke 2, Leipzig 1897, p. 411/6; *E. Picard,* Traité d'Analyse (2ᵉ éd.) 3, Paris 1908, p. 465; *C. Runge,* J. reine angew. Math. 99 (1886), p. 89; *M. Mandl,* id. 113 (1894), p. 252; *W. F. Meyer,* Math. Ann. 30 (1887), p. 30; *Gy. (J.) König,* Alg. Grössen[10], p. 128.
Critères particuliers d'irréductibilités dans *Th. Schönemann,* J. reine angew. Math. 32 (1846), p. 100; *G. Eisenstein,* id. 39 (1850), p. 166; cf. *J. A. Serret,* Algèbre supérieure (6ᵉ éd.) 1, Paris 1910, p. 244; *L. Königsberger,* J. reine angew. Math. 115 (1895), p. 53; Sitzgsb. Akad. Berlin 1894, p. 1135; J. reine angew. Math. 121 (1900), p. 320; *E. Netto,* Vorlesungen über Algebra 1, Leipzig 1896, p. 56/64; Math. Ann. 48 (1896), p. 82; *L. Kronecker,* Vorlesungen über die Theorie der Determinanten, publ. par *K. Hensel,* Leipzig 1903, p. 248/62; *Michael Bauer,* J. reine angew. Math. 128 (1905), p. 87, 298; 134 (1908), p. 15; *G. Dumas,* J. math. pures appl. (6) 2 (1906), p. 191; *O. Dorner,* Diss. Königsberg 1908; Monatsh. Math. Phys. 20 (1909), p. 242; *O. Perron,* Math. Ann. 60 (1905), p. 448.

39) *L. Kronecker,* Festschrift[1]) § 4; J. reine angew. Math. 92 (1882), p. 12/3; Werke 2, p. 258/9; *J. Molk,* Thèse, Paris 1884; Acta math. 6 (1885), p. 41/8.

40) *L. Kronecker,* J. reine angew. Math. 94 (1883), p. 344/8; Werke 2, Leipzig 1897, p. 411/6; *J. Molk,* Thèse, (chap. 2, § 1); Acta math. 6 (1885), p. 10.

(E′) est une équation de degré infini obtenue en égalant à zéro une série de Maclaurin[41]).

La définition de l'irréductibilité s'étend aux équations algébriques à plusieurs inconnues et aux systèmes de telles équations. Une équation algébrique

$$f(x_1, x_2, \ldots, x_n) = 0$$

dont les coefficients appartiennent au corps K est dite irréductible dans ce corps quand son premier membre ne peut pas être envisagé comme le produit de deux fonctions rationnelles entières de $x_1, x_2, \ldots, x_n$ à coefficients rationnels (de degrés différents de zéro). Quand, en particulier, K est formé par l'ensemble des nombres complexes (réels et imaginaires) on dit d'une équation irréductible

$$f(x_1, x_2, \ldots, x_n) = 0$$

qu'elle est *absolument* irréductible.

Un système (S) d'équations à n variables dont les coefficients appartiennent à un corps déterminé K est dit *irréductible* si son *résolvant total complet*

$$D(x, x_1, x_2, \ldots, x_{n-1};\, u_1, u_2, \ldots, u_n) = 0$$

(I 9, **70**) est irréductible dans le corps R_K formé par l'ensemble de celles des fonctions rationnelles de $u_1, u_2, \ldots, u_n$ dont les coefficients appartiennent au corps K.

Parmi les $n-1$ premiers résolvants totaux partiels [I 9, **70**]

$$D_1, D_2, \ldots, D_{n-1}$$

d'un tel système irréductible (S), un seul peut dépendre de $x, x_1, x_2, \ldots, x_{n-1}$ ou de quelques-unes de ces quantités; tous les autres, ainsi d'ailleurs que le $n^{\text{ième}}$ résolvant total partiel D_n, en sont indépendants. Si D_r dépend de $x, x_1, x_2, \ldots, x_{n-1}$ ou de quelques-unes de ces quantités on dit que le système irréductible (S) est de rang r. Si, au contraire, aucun des résolvants totaux partiels ne dépend de ces quantités, on dit que le système irréductible (S) est de rang n; il n'admet alors aucune solution.

D. Hilbert a prouvé que, dans une fonction rationnelle entière de n variables à coefficients entiers qui est irréductible, on peut toujours, d'une infinité de façons, donner à un nombre quelconque $k < n$ de ces variables des valeurs numériques entières telles qu'il en résulte une fonction *irréductible* des $n-k$ variables restantes. Cette pro-

41) *R. Dedekind,* Jahresb. deutsch. Math.-Ver. 1 (1890/1), éd. Berlin 1892, p. 33. Voir aussi *A. Hurwitz,* Acta math. 14 (1890/1), p. 211.

position reste vraie si le domaine de rationalité imposé aux coefficients est un corps algébrique quelconque[42]).

Interprétation fonctionnelle. Supposons que K représente l'ensemble des nombres complexes (réels ou imaginaires). Lorsqu'un système d'équations (S) est irréductible et de rang r, il définit un système de $n-r$ fonctions algébriques de r variables dans l'ensemble K *unique* au sens de la théorie générale des fonctions, c'est-à-dire tel que ses différentes déterminations sont les prolongements analytiques les unes des autres. Par exemple pour $n=3$, $r=2$ ce qui précède définit la notion de *courbe gauche algébrique irréductible* de l'espace ordinaire.

Corps conjugués. Discriminant d'un système de quantités.

11. Corps conjugués. Soient $F(x)=0$ une équation de degré n, irréductible dans un corps Ω (dans lequel il est implicitement supposé que ses coefficients sont rationnels en Ω) et ξ une racine de cette équation. L'ensemble des fonctions rationnelles de ξ à coefficients rationnels en Ω définit un corps K supérieur à Ω et qui est dit du $n^{\text{ième}}$ degré (par rapport à Ω).

Remarquons ici une fois pour toutes que dans ce qui suit Ω désignera toujours un corps rentrant dans l'un des trois types suivants (dont le premier est d'ailleurs compris dans le troisième mais est mentionné spécialement en raison de son importance):

1) le corps $\mathfrak{R}$ ou R ou $R_{\mathfrak{R}}$

2) un corps dont toutes les quantités sont contenues dans R ou $R_{\mathfrak{R}}$ (ex: le corps des fonctions symétrique de $x_1, x_2, \ldots, x_n$).

3) un corps dérivé (n° 7) engendré dans $\mathfrak{R}$, R ou $R_{\mathfrak{R}}$.

Soient $\xi', \xi'', \ldots, \xi^{(n-1)}$ les racines de l'équation $F(x)=0$ distinctes de ξ. Si l'on remplace partout ξ par ξ', ou par ξ'', ..., ou par $\xi^{(n-1)}$, on obtient les corps K′, K″, ..., $K^{(n-1)}$ *conjugués* de K formés respectivement par les quantités

$$\varphi(\xi'),\ \varphi(\xi''),\ \ldots,\ \varphi(\xi^{(n-1)})$$

conjuguées d'une quantité quelconque $\varphi(\xi)$ appartenant au corps K. Le passage d'un corps à l'un de ses conjugués peut être considéré comme un mode de représentation dans lequel toutes les relations rationnelles se conservent, pourvu que leurs coefficients soient rationnels dans le domaine Ω[43]).

42) J. reine angew. Math. 110 (1892), p. 104. Par contre *D. Hilbert* [Nachr. Ges. Gött. 1897, p. 53] a aussi démontré qu'il existe des fonctions (d'une seule variable) rationnelles entières irréductibles, à coefficients entiers, qui sont décomposables en facteurs suivant tout module égal à un nombre premier ou à une puissance d'un nombre premier. Cf. *Michael Bauer*, J. reine angew. Math. 128 (1905), p. 87.

Interprétation fonctionnelle. Dans le cas où ξ est une *fonction* algébrique et Ω le corps général R, les quantités $\xi', \xi'', \ldots, \xi^{(n-1)}$ ne sont autres que les diverses déterminations ou *branches* de la fonction multiforme ξ.

Mais si Ω était un corps R_K (n° 6) les quantités conjuguées ainsi obtenues pourraient ne pas être les seules.

12. Trace. Norme. Discriminant d'un système. Toutes les fonctions symétriques des n quantités conjuguées

$$\varphi(\xi),\ \varphi(\xi'),\ \ldots,\ \varphi(\xi^{(n-1)})$$

sont des éléments du domaine Ω envisagé au n° **11**.

En particulier la somme $S(\eta)$ d'une quantité η appartenant à K et de ses $n-1$ conjuguées est dite la *trace* (die *Spur*) de η et le produit $N(\eta)$ des mêmes quantités est dite la *norme* de η[44]).

Dans le *corps de Gauss* (n° 4) la norme d'un nombre n'est autre chose que le carré de la valeur absolue de ce nombre.

Si $\eta_1, \eta_2, \ldots, \eta_n$ sont des éléments de K, le carré du déterminant formé par ces quantités et leurs conjuguées, à savoir le déterminant

$$\Delta[\eta_1, \eta_2, \ldots, \eta_n] = \begin{vmatrix} \eta_1 & \eta_1' & \eta_1'' & \cdots & \eta_1^{(n-1)} \\ \eta_2 & \eta_2' & \eta_2'' & \cdots & \eta_2^{(n-1)} \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ \eta_n & \eta_n' & \eta_n'' & \cdots & \eta_n^{(n-1)} \end{vmatrix}$$

carré qui est également rationnel en Ω, se nomme le *discriminant* Δ du système $\eta_1, \eta_2, \ldots, \eta_n$. Suivant qu'il est nul ou non, il existe ou non, entre $\eta_1, \eta_2, \ldots, \eta_n$, une relation linéaire et homogène à coefficients rationnels en Ω. C'est seulement quand Δ est différent de zéro que toute quantité appartenant à K peut s'exprimer à l'aide de $\eta_1, \eta_2, \ldots, \eta_n$ sous la forme

$$y = u_1\eta_1 + u_2\eta_2 + \cdots + u_n\eta_n$$

$u_1, u_2, \ldots, u_n$ étant rationnels en Ω.

43) *R. Dedekind* dans *G. Lejeune-Dirichlet*, Zahlenth.[9]), (4e éd.) p. 456/64. (Suppl. XI, n° 161); *R. Dedekind*, Bull. sc. math. (2) 1 (1877), p. 151 et suiv.

44) Le mot *Spur* est employé pour la première fois par *R. Dedekind* et *H. Weber* [J. reine angew. Math. 92 (1882), p. 188] et par *R. Dedekind* [Abh. Ges. Gött. 29 (1882) math. mém. n° 2, p. 5]; le mot *norme* remonte à *C. F. Gauss* [Commentat. Soc. Gott. recent. 7 (1828/31), éd. Göttingue 1832, p. 97; Werke 2, Göttingue 1876, p. 103] et à *E. E. Kummer*, [J. math. pures appl. (1) 12 (1847), p. 187].

*On peut encore dire, en considérant avec *Ch. Hermite*[45]) n variables indépendantes $x_1, x_2, \ldots, x_n$, que le carré de Δ est égal au discriminant de la forme quadratique

$$\begin{gathered}(x_1\eta_1 + x_2\eta_2 + \cdots + x_n\eta_n)^2 \\ + (x_1\eta_1' + x_2\eta_2' + \cdots + x_n\eta_n')^2 + \cdots \\ + (x_1\eta_1^{(n-1)} + x_2\eta_2^{(n-1)} + \cdots + x_n\eta_n^{(n-1)})^2.\end{gathered}$$

Cette conception est la base des recherches de *Ch. Hermite* sur les formes quadratiques à un nombre quelconque n d'indéterminées et des formes du $n^{\text{ième}}$ degré décomposables en n facteurs linéaires.*

Si $\eta_1, \eta_2, \ldots, \eta_n$ sont les n premières puissances $1, \eta, \eta^2, \ldots, \eta^{n-1}$ de la quantité η, le déterminant $\Delta[1, \eta, \eta^2, \ldots, \eta^{n-1}]$ est le *discriminant* de η; il est égal, au signe près, à la norme de la quantité suivante [où $\eta', \eta'', \ldots, \eta^{(n-1)}$ sont toujours les conjuguées de η]:

$$(\eta - \eta')(\eta - \eta'') \ldots (\eta - \eta^{(n-1)});$$

cette dernière quantité appartient également à K et on la nomme avec *D. Hilbert*[46]) la *différente* de η.

Si le corps générateur Ω est quelconque les normes, traces etc. qui viennent d'être définies seront, lorsqu'une confusion est à craindre, dites *relatives*[47]), les dénominations de normes, traces, ... *absolues* étant réservées au cas où Ω est un corps naturel $\mathfrak{R}$, $R_{\mathfrak{R}}$ ou R.

13. Corps primitifs et non primitifs. Toute quantité

$$\eta = \varphi(\xi)$$

de K satisfait à une certaine équation du $n^{\text{ième}}$ degré

$$\begin{aligned}\Phi(x) &= N[x - \varphi(\xi)] \\ &= [x - \varphi(\xi)][x - \varphi(\xi')][x - \varphi(\xi'')] \ldots [x - \varphi(\xi^{(n-1)})] = 0.\end{aligned}$$

La différente de η n'est autre que $\Phi'(\eta)$; le discriminant de η n'est autre que le discriminant au sens algébrique [voir I 9, **44**] de $\Phi(x)$.

L'équation

$$\Phi(x) = 0$$

peut ou bien être irréductible dans le domaine Ω, ou bien avoir pour premier membre la puissance $e^{\text{ième}}$ d'une fonction rationnelle entière de degré f en x [avec $ef = n$][48]). Ce dernier cas se présente lorsque l'on a

$$\Delta[1, \eta, \eta^2, \ldots, \eta^{n-1}] = 0.$$

Si, pour toute quantité η qui appartient au corps K sans appartenir à Ω, l'équation

$$\Phi(x) = 0$$

est irréductible, le corps K est dit *primitif*[49]); il est dit *non primitif* dans le cas contraire, c'est-à-dire s'il existe au moins une quantité η de K (non appartenant à Ω) pour laquelle la décomposition se produit à la manière indiquée ci-dessus. Dans cette dernière hypothèse les fonctions rationnelles de η forment un corps $\overline{\text{K}}$ supérieur à Ω de degré f et K est un corps supérieur à $\overline{\text{K}}$ de degré e par rapport à $\overline{\text{K}}$.

Prenons par exemple pour domaine générateur Ω le corps des fonctions rationnelles symétriques de ν variables $x_1, x_2, \ldots, x_\nu$, lequel est identique avec le corps de toutes les fonctions rationnelles des combinaisons symétriques élémentaires

$$f_1, f_2, \ldots, f_\nu$$

de ces ν variables, et prenons pour corps supérieur K le corps de toutes les fonctions rationnelles de $x_1, x_2, \ldots, x_\nu$. Dans le cas où $\nu = 2$, ce corps dérive de Ω par adjonction de la racine $\xi = x_1 - x_2$ de l'équation

$$x^2 - (f_1^2 - 4f_2) = 0$$

et est évidemment primitif. Pour $\nu > 2$, le corps K est constitué de la façon que voici:

Posons

$$\xi = a_1x_1 + a_2x_2 + \cdots + a_\nu x_\nu,$$

où $a_1, a_2, \ldots, a_\nu$ sont des nombres rationnels inégaux arbitrairement fixés. En permutant de toutes les manières possibles les ν lettres $x_1, x_2, \ldots, x_\nu$ on obtient $n = \nu!$ fonctions linéaires distinctes

$$\xi^{(i)} = a_1x_{i_1} + a_2x_{i_2} + \cdots + a_\nu x_{i_\nu}$$

et le produit

$$(x - \xi)(x - \xi')(x - \xi'') \ldots (x - \xi^{(n-1)})$$

peut se mettre sous la forme d'une fonction de x

$$F(x; f_1, f_2, \ldots, f_\nu)$$

45) J. reine angew. Math. 47 (1854), p. 330; Œuvres publ. par *E. Picard* 1, Paris 1905, p. 221.

46) Jahresb. deutsch. Math.-Ver. 4 (1894/5), éd. Berlin 1897, p. 179 (n° 3).

47) *D. Hilbert*, id. 4, p. 203/5 (n° 14).

48) *Th. Schönemann*, [J. reine angew. Math. 31 (1846), p. 273] paraît être le premier qui ait établi explicitement dans toute sa généralité cette proposition, bien des fois démontrée depuis, de la théorie des corps de nombres algébriques. Mais elle est au fond due à *J. L. Lagrange* car elle se ramène immédiatement à celle qui fait l'objet de la note 50.

49) *H. Weber*, Alg.[14]) 1, p. 501, (n° 151); trad. *J. Griess* 1, p. 533; cette dénomination est tirée de la propriété correspondante du groupe (voir plus loin n° **14**).

de degré n, à coefficients rationnels en Ω. L'équation

$$F(x;\, f_1, f_2, \ldots, f_\nu) = 0$$

est irréductible dans le corps Ω. Le corps envisagé K dérive de Ω par adjonction de la racine ξ de cette équation irréductible $F = 0$.

Toute quantité

$$\eta = \varphi(\xi) = \theta(x_1, x_2, \ldots, x_\nu)$$

du corps K et les quantités conjuguées

$$\eta^{(i)} = \varphi(\xi^{(i)}) = \theta(x_{i_1}, x_{i_2}, \ldots, x_{i_\nu})$$

de η vérifient l'équation

$$\Theta(x;\, f_1, f_2, \ldots, f_\nu) = N[x - \varphi(\xi)] = 0$$

à coefficients rationnels en Ω. Cette équation est irréductible dans le corps Ω quand les $n = \nu!$ fonctions $\varphi(\xi^{(i)})$ obtenues en permutant $x_1, x_2, \ldots, x_\nu$ de toutes les façons possibles dans $\theta(x_1, x_2, \ldots, x_\nu)$ sont distinctes; dans ce cas le corps dérivé du corps Ω par adjonction de η est identique au corps dérivé de Ω par adjonction de ξ, c'est-à-dire à K. Mais si $\theta(x_1, x_2, \ldots, x_\nu)$ reste inaltérée par un groupe de e substitutions et par conséquent ne prend, par toutes les substitutions possibles, que $f = \frac{\nu!}{e}$ valeurs, la fonction

$$\Theta(x, f_1, f_2, \ldots, f_\nu)$$

sera la $e^{\text{ième}}$ puissance d'une fonction entière

$$\Theta_1(x, f_1, f_2, \ldots, f_\nu)$$

irréductible en Ω. Le corps K est donc un corps non primitif. Ces résultats sont tous compris dans le théorème suivant énoncé par *J. L. Lagrange*[50]):

Si la fonction

$$\psi(x_1, x_2, \ldots, x_\nu)$$

reste inaltérée par toutes les substitutions qui ne changent pas $\theta(x_1, x_2, \ldots, x_\nu)$, elle appartient au corps (Ω, θ) défini en adjoignant à Ω la fonction θ. Si alors m est le nombre de fonctions distinctes dans lesquelles se transforme $\theta(x_1, \ldots, x_\nu)$ lorsqu'on applique les substitutions qui laissent invariable la fonction $\psi(x_1, x_2, \ldots, x_\nu)$, la fonction $\theta(x_1, x_2, \ldots, x_\nu)$ vérifie une équation de degré m dont les coefficients

50) Nouv. Mém. Acad. Berlin 1 (1770), éd. 1772, p. 134; 2 (1771), éd. 1773, p. 138; Œuvres 3, Paris 1869, p. 205; voir en part. p. 385/8 (§ 103/4). Cf. *C. Jordan,* Traité des substitutions et des équations algébriques, Paris 1870, p. 50/2; *E. Netto,* Substitutionentheorie und ihre Anwendungen auf die Algebra, Leipzig 1882, p. 55 (§ 51) et p. 108/9 (§ 99/100).

sont rationnels dans le corps (Ω, ψ) obtenu en adjoignant ψ au corps Ω.

On peut envisager ces résultats comme contenant en germe la théorie de *E. Galois* sur les équations algébriques; mais il ne faut pas oublier qu'elles ont cependant encore un caractère très particulier puisqu'ici l'équation de degré ν irréductible dans Ω, dont $x_1, x_2, \ldots, x_\nu$ sont les racines, est une équation sans *affect* (n° **14**).

14. Relations avec la théorie des équations de Galois. Comme on l'a dit (n° **4**) la distinction des corps est dans les idées actuelles la base de la *théorie des équations algébriques de Galois* (I 13). A toute équation donnée du $n^{\text{ième}}$ degré $F(x) = 0$, laquelle peut même être réductible en Ω mais qui ne doit pas avoir de racines égales, appartiennent n corps K, K′, K″, …, $\mathrm{K}^{(n-1)}$ formés chacun par adjonction à Ω d'une des racines de $F(x) = 0$, et l'on peut toujours déterminer le corps L du moindre degré possible qui comprend tous ces n corps, autrement dit le *corps composé* (n° **7**) de K, K′, K″, …, $\mathrm{K}^{(n-1)}$[51]).

On obtient ce corps L en envisageant l'expression

$$\Theta = u\xi + u'\xi' + \cdots + u^{(n-1)}\xi^{(n-1)},$$

où $u, u', \ldots, u^{(n-1)}$ désignent des indéterminées ne figurant pas parmi les éléments du corps Ω et où $\xi, \xi', \ldots, \xi^{(n-1)}$ désignent les n racines de l'équation $F(x) = 0$; on formera ensuite l'équation

$$(1) \qquad P(z, u, u', u'', \ldots, u^{(n-1)}) = 0$$

dont les $n!$ racines sont les $n!$ quantités que l'on déduit de Θ en permutant de toutes les manières possibles les n racines $\xi, \xi', \ldots, \xi^{(n-1)}$. Dans cette équation (1) de degré $n!$ on remplace les indéterminées $u, u', \ldots, u^{(n-1)}$ par des nombres rationnels arbitrairement fixés parmi ceux pour lesquels toutes les $n!$ racines de l'équation sont distinctes. On obtient ainsi une équation

$$Q(z) = 0$$

de degré $n!$, à coefficients rationnels, dont le premier membre $Q(z)$ est ou bien irréductible dans le domaine Ω ou bien se décompose dans ce domaine Ω en facteurs tous de même degré ϱ (en sorte que ϱ divise $n!$). Désignons par $G(z)$ un quelconque de ces facteurs irréductibles de degré ϱ de $Q(z)$ en convenant que, si $Q(z)$ est irréductible dans Ω, on prendra pour $G(z)$ la fonction $Q(z)$ elle-même. Si alors θ désigne une quelconque des racines de l'équation $G(z) = 0$, on obtient le corps L en adjoignant θ au corps Ω.

51) *E. Galois,* mém. posth.[4]) [1831]; J. math. pures appl. (1) 11 (1846), p. 420; Œuvres, p. 36.

On appelle *résolvante de Galois* de l'équation $F(x) = 0$ l'équation envisagée

$$G(z) = 0$$

ainsi que toutes celles des équations de degré ϱ, irréductibles dans le corps Ω, dont il suffit d'adjoindre une des racines au corps Ω pour obtenir le corps L.

Le corps L qui appartient à la résolvante de Galois est un *corps normal* ou *corps de Galois*, c'est-à-dire qu'il est identique avec ses conjugués. Toute fonction rationnelle de $\xi, \xi', \ldots, \xi^{(n-1)}$ est une quantité de L, et inversement.

Comme les corps conjugués du corps L ne sont autres que le corps L lui-même, on peut toujours construire $\varrho - 1$ fonctions rationnelles entières $\varphi_1, \varphi_2, \ldots, \varphi_{\varrho-1}$ dont les coefficients fassent partie de Ω, telles que toutes les racines de la résolvante de Galois envisagée $G(z) = 0$ se déduisent de l'une d'entre elles au moyen des relations

$$\theta_0 = \theta,\ \theta_1 = \varphi_1(\theta),\ \theta_2 = \varphi_2(\theta),\ \ldots,\ \theta_{\varrho-1} = \varphi_{\varrho-1}(\theta).$$

De la définition même du corps L il résulte que chaque élément η du corps L peut être mis sous la forme d'une fonction rationnelle entière

$$\eta = \varphi(\theta)$$

dont les coefficients sont rationnels en Ω; si l'on remplace θ par

$$\theta_i = \varphi_i(\theta)$$

cet élément $\eta = \varphi(\theta)$ du corps L se transforme dans l'élément

$$\eta_i = \varphi(\theta_i) = \varphi[\varphi_i(\theta)]$$

du même corps.

Si, ayant fixé l'indice i (parmi les nombres $0, 1, 2, \ldots, \varrho - 1$) on remplace chacun des éléments η du corps L par l'élément correspondant η_i on retrouve le même corps L, on exprime ce fait en disant que le corps L se transforme en lui-même. Pour $i = 0, 1, 2, \ldots, \varrho - 1$ on obtient ainsi ϱ transformations de L en lui-même. Ces ϱ transformations forment un groupe car le résultat obtenu en effectuant successivement deux de ces transformations peut aussi être obtenu en effectuant une seule des transformations convenablement choisie.

Les racines $\xi, \xi', \ldots, \xi^{(n-1)}$ de l'équation donnée $F(x) = 0$ subissent, par ces ϱ transformations, ϱ permutations dont l'ensemble forme un groupe $\mathfrak{G}$. Ce groupe $\mathfrak{G}$ se nomme le *groupe de l'équation.* Toute fonction rationnelle des quantités $\xi, \xi', \ldots, \xi^{(n-1)}$ qui ne change de

valeur par aucune des permutations de $\mathfrak{G}$ est une quantité de Ω et inversement toute fonction rationnelle de $\xi, \xi', \ldots, \xi^{(n-1)}$ qui est une quantité rationnelle en Ω admet les substitutions du groupe $\mathfrak{G}$ de l'équation dont $\xi, \xi', \ldots, \xi^{(n-1)}$ sont les racines.

Le groupe de toute équation irréductible est *transitif*, c'est-à-dire que, si x_i et x_k désignent deux quelconques des racines de l'équation, il existe toujours dans le groupe de cette équation au moins une substitution qui transforme x_i en x_k.

*Le groupe de la *résolvante de Galois* n'est autre que l'isomorphe holoédrique transitif de $\mathfrak{G}$ dont l'*ordre*, c'est-à-dire le nombre des permutations, et le *degré*, c'est-à-dire le nombre des éléments permutés, sont égaux[52]).*

La théorie algébrique des équations se fonde sur la connaissance des propriétés du corps normal L[53]).

Le groupe de l'équation générale du $n^{\text{ième}}$ degré à coefficients indéterminés est le *groupe symétrique*; c'est le groupe formé par toutes les $n!$ substitutions.

Il y a des équations spéciales caractérisées par ce fait qu'une certaine catégorie de fonctions non symétriques des racines est connue rationnellement en Ω, à savoir les fonctions qui admettent les ϱ substitutions du groupe de l'équation.

On dit avec *L. Kronecker* que ces équations ont un *affect*[54]), et une fonction φ des racines telle que son groupe soit le groupe de l'équation est nommée une *fonction d'affect.* Le nombre $\frac{n!}{\varrho}$ est le *degré de l'affect*[55]).

L. Kronecker[56]) a indiqué comment on peut, dans tous les cas, former une fonction d'affect φ d'une équation donnée $F(x) = 0$, et par suite obtenir le groupe de cette équation.

52) Pour les propriétés des groupes transitifs dont l'ordre et le degré sont égaux, voir *C. Jordan,* Traité des substitutions[50]), p. 58/60 et en partic. *E. Maillet,* Thèse, Paris 1892, p. 9/19.

53) *R. Dedekind* dans *G. Lejeune Dirichlet,* Zahlenth.[9]), (4e éd.) p. 482/5 (Suppl. XI, nº 166); *H. Weber*, Alg.[14]) 1, p. 517/22, 548/58; trad. *J. Griess* 1, p. 551/6, 584/94.

54) *L. Kronecker* [Monatsb. Akad. Berlin 1858, p. 288; cf. I 13] emploie ce terme pour la première fois.

55) La locution *degré de l'affect* est employée ici d'après *H. Weber* [Alg.[14]) 1, p. 521; trad. *J. Griess* 1, p. 555]. *L. Kronecker* [Festschrift[1]) § 12; J. reine angew. Math. 92 (1882), p. 34/42; Werke 2, p. 285/94] désigne par *ordre de l'affect* le nombre ϱ.

56) Festschrift[1]) § 11; J. reine angew. Math. 92 (1882), p. 34; Werke 2, p. 284.

Quand l'équation $F(x) = 0$ est sans affect, le premier membre de l'équation
$$P(z, u, u', u'', \ldots, u^{(n-1)}) = 0,$$
à l'aide duquel on vient de construire la *résolvante de Galois* de l'équation $F(x) = 0$ et dans lequel nous laisserons ici $u, u', u'', \ldots, u^{(n-1)}$ *indéterminés,* est une fonction rationnelle entière, irréductible dans Ω, de $z, u, u', u'', \ldots, u^{(n-1)}$. Quand au contraire le groupe de l'équation $F(x) = 0$ a un degré ϱ inférieur à $n!$, la fonction $P(z, u, u', \ldots, u^{(n-1)})$ se décompose dans Ω en facteurs *irréductibles*
$$Q_1(z; u_1, u_2, \ldots, u_n), \quad Q_2(z; u_1, u_2, \ldots, u_n) \ldots,$$
tous de même degré ϱ, et chacun de ces facteurs irréductibles envisagé comme une fonction de
$$u, u', u'', \ldots, u^{(n-1)}$$
est une fonction d'affect de l'équation $F(x) = 0$.

Le paramètre z qui figure dans le facteur envisagé
$$Q(z; u_1, u_2, \ldots, u_n)$$
peut d'ailleurs être remplacé par un nombre rationnel quelconque tel que toutefois le groupe de Q ne soit pas augmenté.

D'après cela, le problème de trouver *l'affect* (ou, ce qui revient au même, le groupe) *d'une équation donnée* se ramène (théoriquement) au problème dont on a parlé précédemment (n° **10**) qui consiste à reconnaître si une équation est irréductible et, dans le cas contraire, à trouver ses facteurs irréductibles[57]).

On peut encore définir la *fonction d'affect* de la manière suivante[58]). Soit
$$F(x) = x^n - c_1 x^{n-1} + c_2 x^{n-2} - \cdots + (-1)^n c_n = 0$$
l'équation donnée et soient
$$f_1, f_2, \ldots, f_n$$
les fonctions symétriques élémentaires des racines. Le système d'équations
$$f_1 = c_1, f_2 = c_2, \ldots, f_n = c_n$$
peut être réductible même si F ne l'est pas. Mais si l'on ajoute l'équation
$$\varphi = c$$

57) Voir l'exposé de *E. Picard,* Traité d'Analyse[38]), (2e éd.)3, p. 472/81.

58) *L. Kronecker,* Festschrift[1]) § 12; J. reine angew. Math. 92 (1882), p. 34/42; 100 (1887), p. 490; Werke 2, Leipzig 1897, p. 285/94; 3[1], Leipzig 1899, p. 211/40.

qui donne la valeur rationnelle c de la *fonction d'affect* φ, le système d'équations
$$f_1 = c_1, f_2 = c_2, \ldots, f_n = c_n, \varphi = c$$
est toujours irréductible quand F est irréductible et cette propriété caractérise la *fonction d'affect.*

D'après le théorème de *D. Hilbert* (n° **10**) on peut, d'une infinité de manières, dans le corps $\mathfrak{R}$ ou plus généralement dans un corps algébrique quelconque, engendré dans $\mathfrak{R}$, former des équations ayant pour groupe le groupe symétrique ou le groupe alterné.

Les notions introduites par la théorie des équations se transportent d'elles-mêmes à la théorie des corps. C'est ce qui arrive pour les dénominations des *corps* engendrés directement dans les domaines naturels de rationalité et aussi pour celles des *corps* relativement algébriques à un corps lui-même déjà dérivé.

Quand on peut distribuer les éléments permutés d'un groupe transitif en s systèmes $A_0, A_1, A_2, \ldots, A_{s-1}$ de r éléments chacun de façon que chaque permutation ne fasse que permuter entre eux les r éléments d'un même système et permuter entre eux les s systèmes eux-mêmes, en sorte que pour aucune des permutations deux éléments d'un même système ne deviennent éléments de deux systèmes distincts, on dit que le groupe envisagé est *imprimitif* (ou *non primitif*). On appelle *primitif* tout groupe transitif pour lequel une telle distribution de ses éléments n'est pas possible. Une équation est dite primitive ou non primitive (n° **13**) suivant que son groupe est primitif on non primitif.

On désigne par *corps quadratiques* les corps de degré 2; ils sont dits absolument ou relativement quadratiques suivant que le domaine générateur Ω est un domaine naturel ou un domaine dérivé. Un corps de nombres absolument quadratique est dit *réel* ou *imaginaire* suivant qu'on l'obtient en adjoignant au corps $\mathfrak{R}$ la racine carrée d'un nombre positif ou la racine carrée d'un nombre négatif.

On désigne par *corps circulaires,* au sens restreint du mot, les corps que l'on déduit du corps $\mathfrak{R}$ par adjonction d'une racine de l'unité, et par *corps circulaires,* au sens général du mot, tous les corps inférieurs qui sont contenus dans un corps circulaire au sens restreint du mot.

C'est ainsi également que l'on parle de *corps abéliens:* ce sont ceux que l'on obtient en adjoignant à un corps Ω une quantité ξ racine d'une équation abélienne. Autrement dit: les *corps abéliens* sont des corps normaux dont le groupe est composé de substitutions toutes permutables deux à deux.

Lorsque Ω est le corps naturel $\mathfrak{R}$, les corps abéliens sont absolument abéliens; chacun de ces corps est alors un corps circulaire, au moins au sens général du mot[59]. Il en est autrement pour les corps *relativement abéliens*, c'est-à-dire pour les corps abéliens où Ω n'est pas un corps naturel.

La théorie de la multiplication complexe fournit des corps abéliens relativement aux corps de nombres absolument quadratiques. (Voir I 19).

Inversement, et comme *L. Kronecker*[60]) le soupçonnait déjà dans ses „rêves de jeunesse", toute équation algébrique dont les coefficients sont des éléments d'un corps quadratique imaginaire et qui possède dans ce corps un groupe abélien, peut être résolue rationnellement à l'aide de racines de l'unité et de racines des équations de la multiplication complexe[61]).

**Interprétation fonctionnelle.* Supposons que l'équation algébrique donnée soit celle d'une courbe algébrique

$$F(x, y) = 0,$$

de sorte que les coefficients de l'équation algébrique en x donnée soient des fonctions rationnelles entières de y (ou plus généralement supposons que l'équation donnée soit celle d'une surface algébrique dans un espace à un nombre quelconque de dimensions, de sorte que les coefficients de l'équation algébrique en x donnée soient des fonctions rationnelles entières de deux ou de plus de deux variables $y_1, y_2, \ldots$). Considérons cette équation dans le corps général R (n° **6**).

Le groupe de l'équation précédente n'est alors autre que le *groupe de monodromie* de x considéré comme fonction de y (ou des variables $y_1, y_2, \ldots$), c'est-à-dire que ses substitutions sont celles qui correspondent[62]) aux différents contours fermés décrits par la variable y (ou les variables $y_1, y_2, \ldots$).

Il n'en est pas de même, bien entendu, si l'équation est considérée dans un des corps que nous avons appelé $\mathrm{R_K}$ au n° **6**.

59) Ce théorème énoncé par *L. Kronecker* [Abh. Akad. Berlin 1853, math. p. 373] a été démontré par *H. Weber*, Acta math. 8 (1886), p. 193/236; Lehrbuch der Algebra (1re éd.) 2, Brunswick 1895, p. 648/69 (chap. 20); (2e éd.) 2, Brunswick 1899, p. 762/83; J. reine angew. Math. 132 (1907), p. 167/88; *D. Hilbert*, Nachr. Ges. Gött. 1896, p. 29/39; Jahresb. deutsch. Math.-Ver. 4 (1894/5), éd. Berlin 1897, p. 339 (n° 100); *F. Mertens*, J. reine angew. Math. 131 (1906), p. 87/112.

60) Monatsb. Akad. Berlin 1877, éd. 1878, p. 851.

61) *R. Fueter*, J. reine angew. Math. 132 (1907), p. 255/69. *Et aussi, dans un cas particulier, *T. Takagi*, Journal of the College of science Tokyo 19 (1903), p. 42 (n° 5).*

A. Kneser[62]) a démontré que, pour une courbe algébrique donnée, le groupe de monodromie est toujours le groupe symétrique si les axes n'ont pas été choisis d'une manière particulière.*

Quantités entières d'un corps. Discriminant d'un corps.

15. Quantités entières rationnelles. Dans les domaines naturels $\mathfrak{R}$, R et $\mathrm{R}_{\mathfrak{R}}$, on peut mettre à part l'ensemble des quantités *entières*: dans $\mathfrak{R}$ ce sont les nombres entiers, dans R les nombres complexes (réels et imaginaires) et les fonctions rationnelles entières, dans $\mathrm{R}_{\mathfrak{R}}$ les nombres rationnels entiers et les *fonctions rationnelles entières* dont les coefficients sont des nombres rationnels entiers que l'on considérera ainsi par opposition aux quantités qui ne sont que rationnelles.

Ces quantités entières forment des *domaines holoïdes* contenus dans $\mathfrak{R}$, dans R ou dans $\mathrm{R}_{\mathfrak{R}}$. Elles se reproduisent par les trois opérations de l'addition, de la soustraction et de la multiplication.

*On appelle[63]) *domaine holoïde proprement dit* un ensemble de nombres ou plus généralement de quantités ayant toutes les propriétés des domaines orthoïdes [n° **9**] sauf toutefois (ce qui le distingue des domaines *holoïdes improprement dits* ou *orthoïdes* précédemment définis) que la division n'y est pas toujours possible, en sorte que, deux quantités α, β du domaine étant données, l'équation du premier degré

$$\alpha\xi = \beta \tag{1}$$

n'admet *pas* toujours pour solution une quantité du domaine.

De tout domaine holoïde on peut déduire un domaine orthoïde correspondant dans lequel figurent tous les éléments du domaine holoïde, à savoir celui qui est formé par les symboles $\frac{\beta}{\alpha}$ où α et β sont des éléments du domaine holoïde, α étant supposé différent de zéro. On suppose que ces éléments $\frac{\beta}{\alpha}$ jouissent des propriétés que voici:

1°) $\frac{\beta}{1}$ représente l'élément β du domaine holoïde;

2°) on a $\frac{\beta}{\alpha} = \frac{\delta}{\gamma}$ quand $\alpha\delta - \beta\gamma = 0$ et dans ce cas seulement;

3°) l'addition et la multiplication ont lieu conformément aux formules

$$\frac{\beta}{\alpha} + \frac{\delta}{\gamma} = \frac{\beta\gamma + \alpha\delta}{\alpha\gamma},$$

$$\frac{\beta}{\alpha} \cdot \frac{\delta}{\gamma} = \frac{\beta\delta}{\alpha\gamma};$$

62) Diss. Berlin 1884; Math. Ann. 28 (1887), p. 125/32.

63) **Gy.* (*J.*) *König*, Alg. Grössen[10]), p. 1/30 (chap. 1).*

le nouveau domaine ainsi défini a effectivement toutes les propriétés d'un domaine orthoïde, et de la condition 1°) on voit immédiatement qu'il contient tous les éléments du domaine holoïde envisagé.*

Dans la terminologie de *R. Dedekind* un domaine holoïde s'appelle[64]) un *ordre (Ordnung).*

16. Nombres premiers. Fonctions premières. Un nombre entier rationnel est dit *premier* si on ne peut le décomposer en deux facteurs entiers différents de ± 1.

Dans le domaine R des fonctions rationnelles entières de n variables une fonction rationnelle entière sera dite *première* ou *irréductible* si elle ne peut se décomposer en deux facteurs qui soient des fonctions rationnelles entières; il s'agit ici, bien entendu, de véritables fonctions rationnelles dépendant d'une ou de plusieurs variables et non de nombres constants.

Dans le domaine $R_{\mathfrak{R}}$ des fonctions rationnelles entières *à coefficients entiers* de n variables une fonction rationnelle entière sera dite *première* ou *irréductible* si elle ne peut se décomposer en deux facteurs différents de ± 1 qui soient des quantités entières du domaine c'est-à-dire des nombres entiers ou des fonctions rationnelles entières à coefficients entiers.

L'expression „fonction rationnelle entière *irréductible*“ reçoit ainsi deux sens différents déjà distingués au n° **2**. Le premier sens revient à celui d'*équation absolument irréductible* (n° **10**). Le second sens est voisin de celui d'*équation irréductible dans* $\mathfrak{R}$, mais ne lui est pas identique vu la circonstance suivante: Une fonction rationnelle entière $f(x_1, x_2, \ldots, x_n)$ qui égalée à zéro donne une équation irréductible dans $\mathfrak{R}$, n'est cependant pas une fonction rationnelle entière irréductible si les nombres rationnels entiers qui figurent comme coefficients dans $f(x_1, x_2, \ldots, x_n)$ ont un diviseur commun différent de ± 1.

17. Entiers algébriques. Jusqu'ici la qualité d'*entier* a été inséparable de celle de *rationnel.*

L'un des plus grands progrès de la théorie qui nous occupe consiste à étendre la notion de quantité algébrique entière à des quantités *irrationnelles.*

Considérons une équation algébrique irréductible $f(x) = 0$ à coefficients entiers en $\mathfrak{R}$ ou en R. Les racines de cette équation sont dans le premier cas, des *nombres algébriques*, dans le second cas, les

64) *R. Dedekind* dans *G. Lejeune Dirichlet*, Zahlenth.[9]), (4e éd.) p. 505 (Suppl. XI, n° 170); Bull. sc. math. (2) 1 (1877), p. 217.

diverses déterminations d'une *fonction algébrique* x d'une ou de plusieurs variables.

Si dans cette équation le coefficient de la plus haute puissance de x (que nous appellerons *premier* coefficient) est égal à l'unité, x est une *quantité algébrique entière* (nombre ou fonction).

Pour que x soit une quantité algébrique entière, il suffit qu'il existe *une* équation algébrique (irréductible ou réductible) à coefficients entiers en $\mathfrak{R}$, ou en R, ayant pour racine x et pour premier coefficient l'unité; mais il revient au même de dire que dans la seule équation irréductible en $\mathfrak{R}$, ou en R, qui a x pour racine et l'unité pour premier coefficient, les autres coefficients sont aussi des entiers en $\mathfrak{R}$, ou en R.

D'ailleurs une quantité algébrique entière qui est en même temps rationnelle est une quantité rationnelle et entière, au sens primitif du mot[65]).

Les quantités algébriques entières forment un domaine holoïde[66]) car la somme ou le produit de deux d'entre elles est encore un entier algébrique.

De plus, on n'arriverait pas à des quantités distinctes des précédentes en procédant à l'aide des entiers algébriques comme nous avons procédé à l'aide des entiers ordinaires: toute quantité x racine d'une équation dont les coefficients sont des entiers algébriques, le premier d'entre eux étant égal à l'unité, est elle-même un entier algébrique[67]).

On a cru tout d'abord ne pouvoir définir les entiers algébriques que comme résultant, par additions, soustractions, multiplications, de certaines quantités *conventionnellement* choisies et regardées *a priori* comme entières. Ce fut un des grands progrès de l'Arithmetico-algèbre que la découverte des entiers algébriques au sens *absolu* du mot[68]).

Interprétation fonctionnelle. Les fonctions algébriques entières peuvent être caractérisées par ce fait qu'elles ne sont jamais infinies à distance finie.

*[Lorsqu'on adopte le point de vue de *L. Kronecker* on doit ne considérer comme *fonctions rationnelles et entières* que celles à coefficients *entiers.* La définition des fonctions algébriques entières devrait

65) D'après le théorème fondamental de la *théorie des racines commensurables*: cf. *J. A. Serret*[38]) 1, p. 321 et tous les Cours d'Algèbre.

66) *R. Dedekind,* Bull. sc. math. (2) 1 (1877), p. 144; *en germe dans *G. Eisenstein,* J. reine angew. Math. 39 (1850), p. 236.*

67) Voir par exemple *R. Dedekind*, Bull. sc. math. (2) 1 (1877), p. 146; *P. Bachmann,* Allgemeine Arithmetik der Zahlenkörper, Leipzig 1905, p. 6.

68) *L. Kronecker*, J. reine angew. Math. 91 (1881), p. 301 [1862]; Werke 2, Leipzig 1897, p. 195; *R. Dedekind* dans *G. Lejeune Dirichlet,* Zahlenth.[9]), (4e éd.) p. 524 (Suppl. XI, n° 173).

être, dans ce cas, modifiée en conséquence de façon que les quantités entières de R soient remplacées par les quantités entières de $R_{\mathfrak{R}}$, et la propriété *analytique* d'être toujours finie à distance finie ne suffirait plus à caractériser ces fonctions; il faudrait ajouter des propriétés purement arithmétiques].*

18. Divisibilité. Unités. Une quantité algébrique entière β est dite *divisible* par une autre α si le quotient $\frac{\beta}{\alpha}$ est lui-même entier.

*Il existe des quantités algébriques entières, appelées *unités,* dont les inverses sont aussi des entières et par lesquelles par conséquent toute autre grandeur algébrique entière est divisible.

Tels sont déjà dans le domaine $\mathfrak{R}$ les nombres $+1$ et -1.

Plus généralement, est une *unité* tout nombre racine d'une équation algébrique à coefficients entiers dans laquelle les coefficients extrêmes sont égaux à $+1$ ou à -1; autrement dit encore, est une *unité* tout nombre algébrique entier dont la norme absolue [n° **12**] est égale à $+1$ ou à -1.

Si un nombre algébrique est une unité, il en est de même de tous ses conjugués, toujours au sens absolu [n° **12**]. Si toutes ces unités conjuguées ont pour valeur absolue 1, ce sont des racines de l'unité ordinaire[69]).

Dans l'étude des *fonctions algébriques* on doit [si l'on ne se place pas au point de vue de *L. Kronecker*] considérer comme unité:

1°) toute quantité purement numérique différente de zéro;

2°) toute fonction qui est racine d'une équation algébrique dont les coefficients sont des fonctions rationnelles entières, les coefficients extrêmes étant numériques et différents de zéro; en d'autres termes toute fonction qui, pour des valeurs finies quelconques données à la variable, n'est ni nulle ni infinie.

Deux quantités algébriques dont le quotient est une unité sont dites *associées*[70]). Chacune d'elles est divisible par l'autre. Deux quantités associées ont par conséquent les *mêmes* diviseurs.

19. Unités contenues dans un corps de nombres. Soit $f(x)=0$ une équation algébrique, à coefficients rationnels entiers, irréductible

---

69) *L. Kronecker,* J. reine angew. Math. 53 (1857), p. 173; Werke 1, Leipzig 1895, p. 105; *H. Minkowski,* Geometrie der Zahlen 1, Leipzig 1896, p. 135; *D. Hilbert,* Jahresb. deutsch. Math.-Ver. 4 (1894/5), éd. Berlin 1897, p. 221 (n° 21).

70) *R. Dedekind* dans *G. Lejeune Dirichlet,* Zahlenth.[9]), (4e éd.) p. 532 (Suppl. XI, n° 174); Bull. sc. math. (2) 1 (1877), p. 148.

dans $\mathfrak{R}$. Soient r_1 le nombre de ses racines réelles et $2r_2$ le nombre de ses racines imaginaires conjuguées (r_1 ou r_2 peuvent être nuls).

Le corps algébrique K que l'on obtient en adjoignant à $\mathfrak{R}$ une racine ξ de l'équation $f(x)=0$ renferme, en général, un nombre infini d'unités ε, mais elles peuvent toutes s'exprimer à l'aide d'un certain nombre fini d'entre elles

$$\varepsilon_0,\ \varepsilon_1,\ \varepsilon_2,\ \ldots,\ \varepsilon_r$$

par des formules de la forme

$$\varepsilon = \varepsilon_0^{h_0}\varepsilon_1^{h_1}\varepsilon_2^{h_2}\ldots\varepsilon_r^{h_r}, \tag{1}$$

où $h_0, h_1, h_2, \ldots, h_r$ sont des entiers.

L'une de ces unités ε_0 est une racine de l'unité ordinaire[71]) contenue dans le corps; $\varepsilon_0 = -1$ si le corps ne contient pas de racines imaginaires de l'unité ordinaire: c'est ce qui arrive nécessairement pour $r_2 = 0$. On peut toujours[72]) déterminer $r = r_1 + r_2 - 1$ unités $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_r$ de K de façon que chaque unité ε de K s'exprime univoquement au moyen de $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_r$ par une expression de la forme

$$\varepsilon = \varrho\,\varepsilon_1^{h_1}\varepsilon_2^{h_2}\ldots\varepsilon_r^{h_r},$$

où $h_1, h_2, \ldots, h_r$ désignent des nombres rationnels entiers et ϱ une racine ordinaire de l'unité contenue dans K. On dit que $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_r$ forment un *système d'unités fondamentales.*

D'un système fondamental d'unités $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_r$ on peut déduire une infinité d'autres systèmes équivalents. Il suffit pour cela de définir r unités par la formule

$$\varepsilon = \varepsilon_1^{h_1}\varepsilon_2^{h_2}\ldots\varepsilon_r^{h_r} \tag{3}$$

en donnant aux exposants $h_1, h_2, \ldots, h_r$ successivement r systèmes de valeurs dont le déterminant soit égal à ± 1.

Si α et β sont les logarithmes de deux unités de K, $\alpha+\beta$ et $\alpha-\beta$ sont aussi des logarithmes d'unités de K.

---

71) Toutes les racines de l'unité contenues dans un corps sont évidemment des puissances de l'une d'entre elles convenablement choisie.

72) *G. Lejeune Dirichlet,* C. R. Acad. sc. Paris 10 (1840), p. 285/8; Ber. Akad. Berlin 1841, p. 280/5; 1842, p. 93/5; 1846, p. 103/7; Werke 1, Berlin 1889, p. 621/3, 627/32, 635/8, 641/4. *Ch. Hermite,* Lettres sur la théorie des nombres (quatrième lettre) [J. reine angew. Math. 40 (1850), p. 312; Œuvres[45]) 1, p. 160]; *L. Kronecker,* C. R. Acad. sc. Paris 96 (1883), p. 93, 148, 216; 99 (1884), p. 765; Werke 3^1, Leipzig 1899, p. 3/30; *J. Molk,* Bull. sc. math. (2) 7 (1883), p. 133; *H. Minkowski,* Geom. der Zahlen[69]) 1, p. 137/47; *R. Dedekind* dans *G. Lejeune Dirichlet,* Zahlenth.[9]), (4e éd.) p. 590/603 (Suppl. XI, n° 183); *D. Hilbert,* Jahresb. deutsch. Math.-Ver. 4 (1894/5), éd. Berlin 1897, p. 214.

*On peut exprimer le même fait d'une manière différente en introduisant l'idée de *module* dont il sera question plus loin. Il suffit alors de dire que les logarithmes des unités forment un module. Ce module est *fini.*

Quant aux unités elles-mêmes on peut dire qu'elles forment un *module logarithmique*[73]) en appelant ainsi un système de nombres tels que le produit ou le quotient de deux quelconques d'entre eux appartienne encore au système.

On dit que deux nombres appartenant au corps sont *associés* (n° **18**) lorsque leur quotient appartient au module logarithmique formé par les unités du corps ou, ce qui revient au même, lorsque ces deux nombres sont congrus relativement à ce module.*

Désignons par $\xi_1, \xi_2, \ldots, \xi_{r_1}$ les racines réelles de l'équation $f(x)=0$ et par

$$\xi_{r_1+1}=u_1+iv_1,\quad \xi_{r_1+2}=u_2+iv_2,\quad \ldots,\quad \xi_{r_1+r_2}=u_{r_2}+iv_{r_2},$$
$$\xi_{r_1+r_2+1}=u_1-iv_1,\quad \xi_{r_1+r_2+2}=u_2-iv_2,\quad \ldots,\quad \xi_{r_1+2r_2}=u_{r_2}-iv_{r_2}$$

les racines imaginaires de cette équation. Soit K_s le corps déduit de $\mathfrak{R}$ par adjonction de ξ_s. Si l'on désigne par ε une unité quelconque de K et par ε_s l'unité conjuguée dans K_s et si l'on entend par $l_s(\varepsilon)$ soit la fonction

$$\log|\varepsilon_s|$$

soit

$$2\log|\varepsilon_s|$$

suivant que ξ_s est réel ou imaginaire, le déterminant

$$R=\begin{vmatrix} l_1(\varepsilon_1), & l_1(\varepsilon_2), & \ldots, & l_1(\varepsilon_r)\\ l_2(\varepsilon_1), & l_2(\varepsilon_2), & \ldots, & l_2(\varepsilon_r)\\ \cdot & \cdot & \cdot & \cdot\\ l_r(\varepsilon_1), & l_r(\varepsilon_2), & \ldots, & l_r(\varepsilon_r)\end{vmatrix}$$

formé à l'aide d'un système fondamental $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_r$ d'unités du corps K_s est, au signe près, univoquement déterminé par K. Ce nombre R est ce que *R. Dedekind* appelle le *régulateur* du corps K[74]).

---

73) *Nous proposons cette dénomination de préférence à „*Aequivalenzbereich*"; dans un „Aequivalenzbereich" [*Gy.* (*J.*) *König*, Alg. Grössen[10]), p. 27] le quotient ne figure d'ailleurs pas nécessairement. La locution „*Strahl*" [*R. Fueter*, Diss. Göttingue 1903; J. reine angew. Math. 130 (1905), p. 197] pourrait être traduite par „*rayon*".*

74) *R. Dedekind* dans *G. Lejeune Dirichlet*, Zahlenth.[9]), (4e éd.) p. 597 (Suppl. XI, n° 183); voir aussi *G. Eisenstein* [J. reine angew. Math. 28 (1844), p. 313] où cette même locution est employée dans un sens voisin de celui du texte.

*Dans un corps normal (n° **14**) on peut se demander s'il existe un système fondamental formé d'une unité et de ses conjuguées. La réponse est affirmative[75]).*

20. Quantités entières d'un corps. Systèmes fondamentaux. Discriminant d'un corps. Considérons maintenant les quantités algébriques qui font partie d'un corps donné K, celui-ci étant lui-même envisagé comme corps supérieur à un corps Ω par rapport auquel il est d'ordre n.

On pourra toujours dans le corps K trouver m quantités entières $y_1, y_2, \ldots, y_m$ telles que tout entier algébrique appartenant à K puisse se mettre sous la forme

$$(1)\qquad y=u_1y_1+u_2y_2+\cdots+u_my_m,$$

où $u_1, u_2, \ldots, u_m$ sont des *entiers* appartenant au corps Ω. Un tel système $(y_1, y_2, \ldots, y_m)$ s'appelle d'après *L. Kronecker*[76]) un *système fondamental*, ou d'après *R. Dedekind* une *base* des quantités entières du corps K[77]).

Le nombre m n'est pas nécessairement égal à n; il peut lui être supérieur. Toutefois l'égalité $m=n$ a certainement lieu (et par conséquent les valeurs de $u_1, u_2, \ldots, u_n$ dans la relation (1) sont déterminées quand on se donne y) dans quelques cas assez généraux tels que les suivants:

1°) si le corps K est un corps algébrique de nombres, avec[78])

$$\Omega=\mathfrak{R};$$

[si au contraire on envisage K comme un *corps relativement algébrique* à un corps Ω supposé lui-même dérivé de $\mathfrak{R}$, c'est-à-dire si

$$\Omega \text{ est différent de } \mathfrak{R} \text{ et si } K \text{ est différent de } \Omega,$$

le théorème n'est plus vrai];

2°) si K est un corps algébrique de fonctions d'*une* variable[79]), avec

$$\Omega=\mathrm{R};$$

---

75) **H. Minkowski*, Nachr. Ges. Gött. 1900, p. 90/3*.

76) Festschr.[1]), § 8; J. reine angew. Math. 92 (1882), p. 20; Werke 2, Leipzig 1897, p. 267.

77) *R. Dedekind* dans *G. Lejeune Dirichlet*, Zahlenth.[9]), (4e éd.), p. 494, 537 (Suppl. XI, nos 168, 175); Bull. sc. math. (2) 1 (1877), p. 23, 161; *Gy.* (*J.*) *König*, [Alg. Grössen[10]), p. 495 et suiv.] donne la marche à suivre pour déterminer effectivement cette base par résolution d'équations indéterminées du premier degré.

78) *R. Dedekind* dans *G. Lejeune Dirichlet*, Zahlenth.[9]), (4e éd.) p. 537 (Suppl. XI, n° 175; *R. Dedekind*, Bull. sc. math. (2) 1 (1877), p. 158.

79) *L. Kronecker*, J. reine angew. Math. 91 (1881), p. 308 et suiv.; Werke

[pour les fonctions algébriques de plusieurs variables, ce n'est pas certain; *K. Hensel*[80]) prétend cependant que pour les fonctions algébriques de *deux* variables il existe un système fondamental de n éléments].

3°) si Ω est le corps des fonctions symétriques de ν variables $x_1, x_2, \ldots, x_\nu$ à coefficients numériques rationnels et si K est le corps des fonctions rationnelles des mêmes variables (à coefficients rationnels) qui admettent un groupe donné; $u_1, u_2, \ldots, u_n$ sont alors des fonctions entières (à coefficients rationnels) des fonctions symétriques élémentaires[81]).

Si $m = n$ le discriminant du système fondamental

$$D[y_1, y_2, \ldots, y_n] = \begin{vmatrix} y_1 & y_1' & y_1'' & \cdots & y_1^{(n-1)} \\ y_2 & y_2' & y_2'' & \cdots & y_2^{(n-1)} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ y_n & y_n' & y_n'' & \cdots & y_n^{(n-1)} \end{vmatrix}^2$$

est une quantité entière de Ω qui est invariante lorsqu'on change le système fondamental des quantités entières. Ce discriminant du système fondamental est le plus grand commun diviseur des discriminants de tous les systèmes de n entiers du corps; il divise par suite le discriminant de toute quantité entière du corps. On appelle

$$D[y_1, y_2, \ldots, y_n]$$

le *discriminant du corps.*

Le discriminant d'un corps est un multiple du discriminant de tout corps inférieur[82]).

Considérons, par exemple, les corps formés de fonctions rationnelles de ν variables $x_1, x_2, \ldots, x_\nu$ admettant un groupe donné de $\frac{\nu!}{n}$ substitutions. Si ce groupe ne contient que la substitution identique, le corps se compose de toutes les fonctions rationnelles de $x_1, x_2, \ldots, x_\nu$; si l'on désigne par ϑ le produit des différences des variables $x_1, x_2, \ldots, x_\nu$, le discriminant du corps est $\vartheta^{\frac{1}{2}\nu!}$. Dans tous les autres cas on a des corps inférieurs au premier; le discriminant d'un quelconque de ces corps est donc aussi une puissance de ϑ; l'exposant de cette

2, Leipzig 1897, p. 203 et suiv.; *R. Dedekind* et *H. Weber,* J. reine angew. Math. 92 (1882), p. 193 et suiv.

80) „Jahresb. deutsch. Math.-Ver. 8^1 (1899), éd. Leipzig 1900, p. 229."

81) *L. Kronecker*[1]), § 12; J. reine angew. Math. 92 (1882), p. 39; Werke 2, Leipzig 1897, p. 290.

82) *L. Kronecker*[1]), § 9; J. reine angew. Math. 92 (1882), p. 26, Werke 2, Leipzig 1897, p. 274; *R. Dedekind,* Bull. sc. math. (2) 1 (1877), p. 158.

puissance est, d'après *E. Netto*[83]), égal à

$$\frac{1}{2}n - \frac{nq}{\nu(\nu-1)},$$

où q désigne le nombre des transpositions du groupe.

Si deux corps numériques K_1, K_2 ont pour degrés absolus m_1, m_2 et pour discriminants deux nombres d_1, d_2 premiers entre eux, le *corps composé* (n° 7) qui en résulte a[84]) pour degré $m_1 m_2$ et pour discriminant $d_1^{m_2} d_2^{m_1}$. Les conclusions sont beaucoup moins simples si d_1 et d_2 ne sont pas premiers entre eux[85]).

Le discriminant absolu d'un corps numérique (autre que $\mathfrak{R}$) est toujours[86]) plus grand que 1. Le nombre des corps de degré donné pour lesquels ce discriminant a une valeur donnée est toujours fini[87]).

21. Forme discriminante. Discriminant d'un corps. Si $m > n$ on ajoutera à la matrice

$$\begin{Vmatrix} y_1, & y_2, & y_3, & \ldots, & y_m \\ y_1', & y_2', & y_3', & \ldots, & y_m' \\ y_1'', & y_2'', & y_3'', & \ldots, & y_m'' \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ y_1^{(n-1)}, & y_2^{(n-1)}, & y_3^{(n-1)}, & \ldots, & y_m^{(n-1)} \end{Vmatrix}$$

$m - n$ lignes composées d'indéterminées.

Le carré du déterminant ainsi obtenu est la *forme discriminante.* Le plus grand commun diviseur des coefficients de cette forme s'appelle le *discriminant du corps.*

Seulement ici rien ne dit que le discriminant du corps est une quantité de Ω; il peut n'être représentable qu'en faisant intervenir la notion des systèmes de diviseurs; c'est un *idéal* de Ω (voir plus loin n^os^ **24** et suiv.).

83) J. reine angew. Math. 90 (1881), p. 171.

84) *D. Hilbert,* Jahresb. deutsch. Math.-Ver. 4 (1894/5), éd. Berlin 1897, p. 266 (n° 52).

85) *K. Hensel,* J. reine angew, Math. 105 (1889), p. 329.

86) *H. Minkowski,* J. reine angew. Math. 107 (1891), p. 278; C. R. Acad. sc. Paris 112 (1891), p. 209; Geom. der Zahlen[69]) 1, p. 130; *D. Hilbert,* Jahresb. deutsch. Math.-Ver. 4 (1894/5), éd. Berlin 1897, p. 211 (n° 18).

87) *Ch. Hermite* [J. reine angew. Math. 47 (1854), p. 335; Œuvres[45]) 1, p. 225; (lettre à *C. W. Borchardt*) J. reine angew. Math. 53 (1857), p. 182; Œuvres[45]) 1, p. 415, voir aussi C. R. Acad. sc. Paris 40 (1855), p. 786; Œuvres[45]) 1, p. 477 en note] a démontré le théorème analogue relatif au discriminant *algébrique* de l'équation, théorème de portée moindre puisque le discriminant d'une équation est un multiple du discriminant du corps correspondant.

Voir aussi *H. Minkowski,* C. R. Acad. sc. Paris 112 (1891), p. 209; *D. Hilbert,* Jahresb. deutsch. Math.-Ver. 4 (1894/5), éd. Berlin 1897, p. 212 (n° 18).

Contrairement à ce qui a lieu (n° **20**) pour les discriminants absolus, le discriminant relatif d'un corps supérieur K peut[88]) être égal à 1 sans que K coïncide avec le corps Ω.

22. Anneaux, espèces ou domaines d'intégrité. Les entiers algébriques contenus dans un corps donné K forment évidemment un domaine holoïde. De ce domaine holoïde on peut extraire des domaines plus restreints, mais également holoïdes.

On obtient de tels domaines en partant de k quantités entières quelconques

$$\Theta_1,\ \Theta_2,\ \ldots,\ \Theta_k$$

de K et en formant toutes les fonctions entières de $\Theta_1, \Theta_2, \ldots, \Theta_k$ à coefficients entiers et empruntés à K ou à un corps Ω inférieur à K.

L. Kronecker[89]) a donné à un tel domaine le nom d'*espèce (Art; species)*; *R. Dedekind*[90]) l'a désigné sous le nom *d'ordre* d'un module fini; *D. Hilbert*[91]) l'a appelé *anneau (Ring)* ou *domaine d'intégrité (Integritätsbereich)*.

L'*espèce principale (Hauptart)* est celle qui est composée de tous les entiers contenus dans K.

Comme l'espèce principale, toutes les autres espèces admettent chacune un système fondamental, un discriminant qui est le discriminant du système fondamental[92]), etc.

Mais l'espèce principale se distingue des autres dans la théorie de la divisibilité (voir plus loin n° **24**).

R. Fueter*[93]) étudie d'une manière analogue les *modules logarithmiques* (n° **19). Le plus simple qu'il considère est formé de quantités η appartenant à un corps donné K et telles que $\eta - 1$ soit divisible soit par un nombre soit par un idéal (n° **26**) donné, appelé *guide* du module logarithmique.

Il faut remarquer qu'ici un nombre fractionnaire a est dit *divisible* par un nombre entier b lorsque en multipliant a par un nombre premier relatif à b on obtient un nombre entier divisible par b. Dans

88) Exemples dans *D. Hilbert,* Nachr. Ges. Gött. 1898, p. 377/80.

89) Festschr.[1]), § 5; J. reine angew. Math. 92 (1882), p. 15; Werke 2, Leipzig 1897, p. 261.

90) *R. Dedekind* dans *G. Lejeune Dirichlet*, Zahlenth.[9]), (4e éd.) p. 505 (Suppl. XI, n° 170); Bull. sc. math. (2) 1 (1877), p. 217.

91) Jahresb. deutsch. Math.-Ver. 4 (1894/5), éd. Berlin 1897, p. 237 (n° 31). Le mot allemand „Ring" a un sens analogue à celui du mot anglais „trust".

92) *L. Kronecker,* Festschr.[1]), § 8; J. reine angew. Math. 92 (1882), p. 20/5; Werke 2, Leipzig 1897, p. 267/74; *D. Hilbert,* Jahresb. deutsch. Math.-Ver. 4 (1894/5), éd. Berlin 1897, p. 237 (n° 31).

93) *Diss. Göttingue 1903; J. reine angew. Math. 130 (1905), p. 197.*

le corps R des nombres rationnels, les nombres entiers impairs et leurs quotients forment un module logarithmique du type envisagé ayant pour *guide* 2.*

23. Applications aux invariants. *D. Hilbert*[94]) a appliqué la théorie des corps à celle des invariants [I 9, 8] appartenant à un système de formes générales

$$f_1,\ f_2,\ \ldots,\ f_\varrho.$$

Parmi les invariants du système de formes $(f_1, f_2, \ldots, f_\varrho)$ on peut toujours extraire $\varkappa$ invariants

$$J_1,\ J_2,\ \ldots,\ J_\varkappa$$

qui ne soient liés par aucune relation algébrique et qui soient tels que tout autre invariant du système de formes $f_1, f_2, \ldots, f_\varrho$ soit une fonction algébrique entière de $J_1, J_2, \ldots, J_\varkappa$.

Le nombre $\varkappa$ est égal à l'excès du nombre des coefficients des formes sur celui du nombre des paramètres du groupe continu des transformations linéaires. Si, par exemple, le système de formes $f_1, f_2, \ldots, f_\varrho$ se réduit à une seule forme binaire de degré n, le nombre des coefficients de cette forme étant $n+1$, le nombre des paramètres du groupe continu des transformations linéaires est $4-1=3$ et l'on a donc $\varkappa = n-2$.

Aux invariants $J_1, J_2, \ldots J_\varkappa$ on peut toujours adjoindre un invariant J tel que tous les autres invariants du système $(f_1, f_2, \ldots, f_\varrho)$ soient fonctions rationnelles de $J_1, J_2, \ldots, J_\varkappa, J$. D'après ce qui précède, J ne peut être qu'une fonction algébrique entière de $J_1, J_2, \ldots, J_\varkappa$.

Si nous envisageons les invariants $J_1, J_2, \ldots, J_\varkappa$ comme des variables indépendantes, le corps algébrique K formé par les fonctions rationnelles de $J_1, J_2, \ldots, J_\varkappa$ après adjonction de J jouira de la propriété que voici: tout invariant du système $(f_1, f_2, \ldots, f_\varrho)$ envisagé comme une fonction de $J_1, J_2, \ldots, J_\varkappa$ est égal à un entier de K. Inversement tout entier de K envisagé comme une fonction des coefficients de $f_1, f_2, \ldots, f_\varrho$ représente un *invariant* du système $(f_1, f_2, \ldots, f_\varrho)$ (à condition toutefois d'être homogène dans les coefficients de chacune des ϱ fonctions $f_1, f_2, \ldots, f_\varrho$).

Pour obtenir un *système complet d'invariants* de $(f_1, f_2, \ldots, f_\varrho)$, c'est-à-dire un système d'invariants $i_1, i_2, \ldots, i_\sigma$ tel que tout autre invariant de $(f_1, f_2, \ldots, f_\varrho)$ s'exprime en fonction rationnelle entière de $i_1, i_2, \ldots, i_\sigma$, il suffit de déterminer une *base* des quantités entières (n° **20**) du corps K. L'ensemble de $J_1, J_2, \ldots, J_\varkappa$ et des éléments

94) Math. Ann. 42 (1893), p. 313.

de cette base, envisagés comme fonctions des coefficients de $f_1, f_2, \ldots, f_\varrho$, forme un système complet d'invariant.

Si l'on donne aux coefficients de $f_1, f_2, \ldots, f_\varrho$ des valeurs telles que les invariants $J_1, J_2, \ldots, J_\varkappa$ s'annulent, tous les invariants du système $(f_1, f_2, \ldots, f_\varrho)$ s'annulent.

Dans le cas où $\varrho = 1$, on dit de toute forme dont tous les invariants s'annulent qu'elle est une *forme nulle*.

La détermination des „formes nulles" se ramène à celle de certaines „formes canoniques".

Idéaux.

24. *Domaines holoïdes complets et incomplets de quantités algébriques entières. Parmi les diverses propriétés de la divisibilité, il en est un certain nombre qui s'étendent sans modification aux entiers algébriques contenus dans un corps déterminé quelconque. Ainsi toute quantité (entière) qui en divise une autre divise ses multiples, et toute quantité qui en divise deux autres divise leur somme et leur différence; etc. De plus, parmi les quantités entières d'un corps, il en est qui sont *premières dans ce corps*, c'est-à-dire qui ne peuvent être décomposés en facteurs entiers contenus dans ce corps et dont aucun ne soit une unité[95]); et tout entier d'un corps est décomposable en facteurs premiers dans ce corps.

Mais, pour d'autres propriétés de la divisibilité, l'analogie ne subsiste plus d'une manière générale. Les deux théorèmes que nous allons énoncer concernent exclusivement les quantités entières des domaines *naturels* de rationalité $\mathfrak{R}$ ou $R_{\mathfrak{R}}$; ils ne peuvent être étendus aux quantités entières de corps dérivés quelconques de ces domaines.

I. Dans les corps $\mathfrak{R}$ et $R_{\mathfrak{R}}$, la décomposition d'un nombre entier ou d'une fonction entière en ses facteurs premiers est *unique* lorsqu'on convient de ne pas envisager comme distinctes deux quantités égales et de signes contraires[96]).

II. Deux quantités entières quelconques du corps $\mathfrak{R}$ ou du corps $R_{\mathfrak{R}}$ admettent toujours un *plus grand commun diviseur*; en d'autres termes: si l'on envisage soit dans le corps $\mathfrak{R}$ soit dans le corps $R_{\mathfrak{R}}$ deux quantités entières quelconques, il existe toujours dans le corps envisagé

95) *Cette définition n'est pas identique à celle de *R. Dedekind* et de *Gy. (J.) König* (voir plus loin, note 101). Une quantité première dans un corps peut bien entendu cesser de l'être dans un corps supérieur.*

96) **L. Kronecker*, Vorlesungen über Zahlentheorie, publ. par *K. Hensel* 1, Leipzig 1901, p. 176 (15ième leçon); J. reine angew. Math. 94 (1883), p. 344; Werke 2, Leipzig 1897, p. 411.*

$\mathfrak{R}$ ou $R_{\mathfrak{R}}$ une quantité entière admettant pour diviseurs tous les diviseurs communs aux deux premières quantités et ceux-là seulement.

Si l'on ne considère pas comme distincts deux polynomes ne différant l'un de l'autre que par un facteur numérique autre que zéro, les deux théorèmes I et II ont encore lieu pour les fonctions entières dans le corps R.

Dans la terminologie de *Gy. (J.) König* le théorème II s'énonce ainsi:

Chacun des trois ensembles constitué par les quantités entières du corps $\mathfrak{R}$, du corps $R_{\mathfrak{R}}$ et du corps R forme un *domaine holoïde complet.*

Gy. (J.) König[97]) dit, en effet, d'un domaine holoïde qu'il est *complet* lorsqu'à deux éléments quelconques A_1, A_2 de ce domaine correspond toujours un élément D du même domaine, (on l'appelle le plus grand commun diviseur de A_1 et A_2) dont les diviseurs soient précisément les diviseurs communs des deux éléments A_1 et A_2. La notion de *diviseur* est prise ici dans le sens ordinaire du mot qui est celui-ci:

La condition nécessaire et suffisante pour qu'un élément A du domaine soit „diviseur" d'un élément B de ce domaine est que, dans ce domaine, il y ait un élément X tel que AX soit *égal* à B.

On remarquera que dans la définition des domaines holoïdes *complets* ne figure pas la condition de l'existence, dans le domaine, de diviseurs premiers, et bien moins encore celle que chaque élément du domaine soit décomposable en un produit de facteurs premiers.

Le plus remarquable de tous les domaines holoïdes complets ne contenant aucun diviseur premier est celui qui est constitué par l'ensemble de tous les nombres algébriques. Dans cet ensemble tout élément peut être décomposé en facteurs d'une infinité de manières; car A et $\sqrt[n]{A}$ désignant des nombres algébriques entiers, on a $A = (\sqrt[n]{A})^n$.

Cependant cet ensemble constitue un domaine holoïde complet comme il résulte du théorème suivant que *R. Dedekind*[98]) à démontré en se servant de la théorie des idéaux dont il sera question plus loin:

Deux nombres entiers algébriques α et β (non tous deux nuls) admettent toujours un diviseur commun δ représentable sous la forme

$$\delta = \alpha\alpha' + \beta\beta'$$

(où α' et β' sont des entiers), tel par conséquent que tout autre diviseur commun de α et de β soit diviseur de δ. Ce *plus grand commun diviseur* est unique si l'on convient de ne pas regarder

97) *Alg. Grössen[10]), p. 13/5 (Texte et note de *J. Kürschák*).*

98) **R. Dedekind* dans *G. Lejeune Dirichlet,* Zahlenth.[9]), (4e éd.) p. 577 (Suppl. XI, n° 181); *R. Dedekind,* Bull. sc. math. (2) 1 (1877), p. 246.*

comme distincts deux diviseurs associés. [Il n'appartient toutefois en général qu'à un corps supérieur au corps $(\mathrm{R}, \alpha, \beta)$].

Pour chacun des domaines $\mathfrak{R}$, $\mathrm{R}_{\mathfrak{R}}$ et R le théorème I peut se déduire du théorème II joint au fait que les quantités entières de chacun de ces domaines sont décomposables en facteurs irréductibles.

Ce dernier fait résulte si l'on veut des théorèmes suivants:

1°) Si un domaine holoïde complet contient des quantités irréductibles, chacune de ces quantités irréductibles qui divise un produit divise aussi nécessairement un au moins des facteurs de ce produit.

2°) Une quantité quelconque d'un domaine holoïde complet n'est décomposable en facteurs irréductibles que d'une seule manière.

3°) Inversement quand chaque quantité d'un domaine holoïde est décomposable d'une et d'une seule manière en facteurs irréductibles, ce domaine holoïde est un domaine holoïde *complet.*

Les théorèmes I et II ont aussi lieu pour certains corps algébriques si l'on ne regarde pas comme distinctes deux décompositions dont les facteurs sont *associés* (n° **18**) chacun à chacun. Tel est, par exemple, le corps des nombres rationnels complexes

$$a+b\sqrt{-1}$$

(où a et b sont des nombres rationnels ordinaires), considéré par *C. F. Gauss.*

Mais lorsque *E. E. Kummer*[99]) entreprit de généraliser les recherches de *C. F. Gauss* en remplaçant $\sqrt{-1}$ par d'autres racines de l'unité, il rencontra des circonstances toutes différentes. Dans les corps ainsi obtenus, comme dans une infinité d'autres dont les quantités entières ne forment pas de domaines holoïdes complets, les lois énoncées pour les domaines $\mathfrak{R}$, $\mathrm{R}_{\mathfrak{R}}$, R ne sont plus exactes. Deux entiers peuvent n'avoir pas de p. g. c. d.[100]) appartenant au corps; dès lors il n'est plus vrai qu'un entier premier qui divise un produit de deux facteurs divise nécessairement l'un de ces facteurs[101]). En fait, il arrive que,

99) *J. reine angew. Math. 35 (1847), p. 319, 327; 40 (1850), p. 93; 53 (1857), p. 142; J. math. pures appl. 16 (1851), p. 377; Abh. Akad. Berlin 1856, math. p. 1; 1857, math. p. 41; 1859, math. p. 19; 1861, math. p. 81.*

100) *On ne doit pas confondre, bien entendu, deux nombres qui n'ont pas de p, g. c. d. avec deux nombres premiers entre eux (lesquels admettent pour p. g. c. d. l'unité).*

101) *Les *nombres premiers* sont pris ici dans les sens indiqués note 97. *R. Dedekind* [Bull. sc. math. (2) 1 (1877), p. 75] et *Gy. (J.) König* [Alg. Grössen[10]), p. 23] désignent au contraire l'un par *nombres indécomposables* l'autre par *nombres irréductibles* les nombres ainsi définis en réservant la dénomination de *nombres premiers* à ceux qui ne peuvent diviser un produit de deux facteurs sans diviser l'un d'eux.*

dans les corps en question, un nombre peut être décomposé en un produit de deux ou de plusieurs facteurs premiers non associés.

L'exemple le plus simple de corps dont les entiers ne forment pas de domaine holoïde complet a été indiqué par *R. Dedekind*[102]): c'est le corps obtenu en adjoignant à R l'irrationnelle $\sqrt{-5}$. Dans ce corps les nombres 9 et $3(1-2\sqrt{-5})$ ont des diviseurs communs autres que 1 (savoir les nombres 3 et $2-\sqrt{-5}$), mais pas de p. g. c. d.; les nombres 3 et $2-\sqrt{-5}$ n'ont pas de p. p. c. m.; le nombre 9 admet les deux décompositions, essentiellement distinctes, en facteurs premiers

$$9 = 3^2 = (2+\sqrt{-5})(2-\sqrt{-5});$$

le nombre $3-6\sqrt{-5}$ admet les deux décompositions

$$3(1-2\sqrt{-5}) = (2-\sqrt{-5})(4-\sqrt{-5}),$$

de sorte que le nombre 3, qui est premier dans le corps en question, et qui ne divise ni $2+\sqrt{-5}$, ni $2-\sqrt{-5}$, ni $4-\sqrt{-5}$, divise cependant le produit des deux premiers et celui des deux derniers. Enfin, quoique les deux nombres 3 et $1-2\sqrt{-5}$ soient premiers entre eux, leurs carrés ne le sont point et admettent le diviseur commun $2-\sqrt{-5}$.

La distinction fondamentale entre les domaines holoïdes *complets* et les domaines holoïdes *incomplets* apparaît naturellement dans toutes les recherches où les domaines holoïdes jouent un rôle quelconque.

Ainsi *R. Bricard*[103]), en étudiant la réduction des formes quadratiques binaires [cf. I 16, en partic. n^os **13** et suiv.] dont les coefficients sont des entiers d'un corps quadratique, constate que la théorie est, dans ce cas, toute parallèle à ce qu'elle est dans le cas des entiers ordinaires si les entiers du corps quadratique forment un domaine holoïde *complet*; mais qu'il en est tout autrement dans les corps quadratiques dont les entiers forment un domaine holoïde *incomplet.**

25. Nombres idéaux de Kummer. Quoique les principaux théorèmes concernant la divisibilité ne s'appliquent plus aux corps dérivés du domaine naturel $\mathfrak{R}$ par adjonction d'une racine de l'unité, *E. E. Kummer* est cependant parvenu à étendre à tous ces corps dérivés de $\mathfrak{R}$ la théorie de la divisibilité. A cet effet, à défaut d'un p. g. c. d. entre deux ou plusieurs nombres d'un tel corps, il a introduit un être

102) **R. Dedekind* dans *G. Lejeune Dirichlet*, Zahlenth.[9]), (4^e éd.) p. 451 (Suppl. XI, n° 159); Bull. sc. math. (2) 1 (1877), p. 73.*

103) *Bull. Soc. math. France 35 (1907), p. 161 (communication verbale faite le 2 mai 1907, non publiée).*

fictif destiné à jouer le rôle de ce p. g. c. d.; à cet être fictif il a donné le nom de *nombre idéal.*

*Voici en quoi consiste essentiellement la théorie de *E. E. Kummer* dans le cas où la racine de l'unité qu'on a adjointe est d'ordre premier λ.

Soit q un nombre premier (ordinaire) distinct de p; désignons par f le plus petit entier positif pour lequel on ait

$$q^f \equiv 1 \qquad (\text{mod. } p);$$

on sait que le quotient

$$e = \frac{\lambda - 1}{f}$$

est un nombre entier. Rappelons aussi que *C. F. Gauss*[104]) a montré que pour un choix convenable du nombre naturel γ, on peut toujours distribuer les $\lambda - 1$ racines de l'équation

$$x^{\lambda-1} + x^{\lambda-2} + \cdots + x + 1 = 0,$$

mises sous la forme

$$\alpha, \alpha^{\gamma}, \alpha^{\gamma^2}, \alpha^{\gamma^3}, \ldots, \alpha^{\gamma^{ef-1}},$$

en e périodes

$$\eta_0, \eta_1, \eta_2, \ldots, \eta_{e-1}$$

contenant chacune f termes, telles que l'on ait, pour $k = 0, 1, 2, \ldots, e-1$,

$$\eta_k = \alpha^{\gamma^k} + \alpha^{\gamma^{e+k}} + \alpha^{\gamma^{2e+k}} + \cdots + \alpha^{\gamma^{(f-1)e+k}}.$$

Le produit des deux périodes η_0, η_k peut se mettre sous la forme

$$(1) \qquad \eta_0\eta_k = \mu^{(k)}f + m_0^{(k)}\eta_0 + m_1^{(k)}\eta_1 + \cdots + m_{e-1}^{(k)}\eta_{e-1},$$

où, pour $k = 0, 1, 2, \ldots, e-1$, les coefficients $\mu^{(k)}, m_0^{(k)}, m_1^{(k)}, \ldots, m_{e-1}^{(k)}$ sont des nombres rationnels entiers. Le coefficient $\mu^{(k)}$ est d'ailleurs nul sauf quand, f étant pair, $k = 0$ ou que, f étant impair, $k = \frac{e}{2}$, auxquels cas $\mu^{(k)} = 1$.

Ceci rappelé, *E. E. Kummer* démontre que le système de congruences

$$(2) \qquad U_0U_k \equiv \mu^{(k)}f + m_0^{(k)}U_0 + m_1^{(k)}U_1 + \cdots + m_{e-1}^{(k)}U_{e-1} \qquad (\text{mod. } q),$$
$$(k = 0, 1, 2, \ldots, e-1),$$

où $U_0, U_1, \ldots, U_{e-1}$ sont les inconnues, a exactement e solutions distinctes (mod. q). Si

$$(u_0, u_1, u_2, \ldots, u_{e-1})$$

est l'une de ces e solutions, les $e-1$ autres s'en déduisent aisément par permutations circulaires.

Parmi les fonctions linéaires homogènes, à coefficients rationnels

104) *Disq.[5]) n° 343; Werke 1, p. 420 (Texte et note de *J. Kürschák*).*

entiers, des périodes $\eta_0, \eta_1, \ldots, \eta_{e-1}$ il en existe une, au moins,

$$L(\eta_0, \eta_1, \ldots, \eta_{e-1})$$

telle que le nombre rationnel entier N défini par le produit

$$(3) \qquad N = \prod_{k=0}^{k=e-1} L(\eta_k, \eta_{k+1}, \ldots, \eta_{e-1}, \eta_0, \ldots, \eta_{k-1})$$

soit divisible par q sans être divisible par q^2. Pour une telle fonction L, un et un seul des e nombres

$$(4) \qquad L(u_k, u_{k+1}, \ldots, u_{e-1}, u_0, \ldots, u_{k-1}) \qquad (k = 0, 1, 2, \ldots, e-1)$$

est divisible par q. On peut d'ailleurs exprimer $L(\eta_0, \eta_1, \ldots, \eta_{e-1})$ en fonction rationnelle (à coefficients rationnels) de l'unique période η_0; soit $\psi(\eta_0)$ cette fonction rationnelle. On a alors évidemment, pour $k = 0, 1, 2, \ldots, e-1$,

$$L(\eta_k, \eta_{k+1}, \ldots, \eta_{e-1}, \eta_0, \ldots, \eta_{k-1}) = \psi(\eta_k).$$

On peut faire se correspondre de e façons distinctes les périodes $\eta_0, \eta_1, \ldots, \eta_{e-1}$ et les systèmes de e nombres $u_0, u_1, \ldots, u_{e-1}$ rangés circulairement

$$(u_k, u_{k+1}, \ldots, u_{k-1}), \quad (u_{k+1}, u_{k+2}, \ldots, u_k), \quad \ldots, \quad (u_{k-1}, u_k, \ldots, u_{k-2});$$

nous désignerons par le symbole

$$\eta_k \mid u_r$$

celle de ces e correspondances distinctes pour laquelle à η_k correspond $(u_r, u_{r+1}, \ldots, u_{r-1})$.

Dans le corps circulaire défini par l'équation

$$\frac{x^{\lambda} - 1}{x - 1} = 0,$$

E. E. Kummer fait correspondre à chacune des correspondances $\eta_k \mid u_r$ un facteur premier (effectif ou idéal) de q.

Quand q peut être mis sous la forme d'un produit (3), chacun des facteurs

$$(5) \qquad L(\eta_k, \eta_{k+1}, \ldots, \eta_{k-1})$$

de q est un nombre premier algébrique du corps circulaire envisagé. Dans ce cas, si $L(u_r, u_{r+1}, \ldots, u_{r-1})$ est divisible par q on dit que le nombre (5) est le facteur premier effectif de q correspondant à $\eta_k \mid u_r$.

Quand, au contraire, q ne peut pas être mis sous la forme d'un produit (5), les facteurs premiers de q introduits par *E. E. Kummer* ne sont que des êtres fictifs auxquels il donne le nom de *facteurs idéaux.*

Pour déterminer les facteurs premiers (effectifs ou idéaux) d'un nombre algébrique entier donné

$$\beta = F(\alpha)$$

on procède de la façon suivante:

Soit

$$L(\eta_0, \eta_1, \ldots, \eta_{e-1}) = \psi(\eta_0)$$

une fonction linéaire et homogène (à coefficients rationnels et entiers) des périodes, telle que le produit (3) soit divisible par q sans l'être par q^2. Et soit

$$(u_0, u_1, \ldots, u_{e-1})$$

celle des solutions du système de congruences (2) pour laquelle on ait

$$L(u_0, u_1, \ldots, u_{e-1}) \equiv 0 \qquad (\text{mod. } q).$$

Formons alors la suite infinie

$$F(\alpha)\left(\frac{\Psi(\eta_\nu)}{q}\right), \quad F(\alpha)\left(\frac{\Psi(\eta_\nu)}{q}\right)^2, \quad \ldots, \quad F(\alpha)\left(\frac{\Psi(\eta_\nu)}{q}\right)^\mu, \quad \ldots\ldots,$$

où l'on a posé pour abréger

$$\Psi(\eta_0) = \psi(\eta_1)\,\psi(\eta_2)\ldots\psi(\eta_{e-1}),$$

$\Psi(\eta_1)$, $\Psi(\eta_2), \ldots, \Psi(\eta_\nu), \ldots\ldots$ s'en déduisant par permutations circulaires.

Quelques termes de cette suite infinie peuvent être des nombres algébriques entiers. Si le $(\mu + 1)^{\text{ième}}$ terme de cette suite infinie est le premier qui ne soit pas un nombre algébrique entier, le nombre algébrique donné β contient exactement μ fois le facteur premier (effectif ou idéal) de q correspondant à $\eta_\nu \mid u_0$.

On peut d'ailleurs envisager ce facteur premier comme le plus grand commun diviseur (effectif ou idéal) de $\psi(\eta_\nu)$ et de q.

Si l'on détermine ainsi tous les facteurs premiers de q, un produit $\beta_1\beta_2$ de deux nombres algébriques entiers du corps circulaire envisagé ne peut être divisible par un facteur premier de q que si l'un au moins, β_1 ou β_2, des deux facteurs du produit est divisible par ce facteur premier de q.

La notion de facteur premier idéal est particulière aux corps circulaires. Elle a été étendue par *E. E. Kummer* au cas où le degré de la racine de l'unité qu'on a adjointe est un nombre composé, mais on ne peut l'étendre à des corps algébriques quelconques.

Pour étendre la théorie de la divisibilité à des corps algébriques numériques ou fonctionnels quelconques, on dispose aujourd'hui de deux méthodes principales, à savoir: la théorie des idéaux de *R. Dedekind* et la théorie des diviseurs algébriques de *L. Kronecker.* Pour les recherches concernant les corps de nombres les suites p-adiques

introduites par *K. Hensel* permettent aussi d'étendre la théorie de la divisibilité. Nous examinerons d'abord les deux méthodes de *R. Dedekind* et de *L. Kronecker*; nous envisagerons ensuite un peu plus loin les suites p-adiques de *K. Hensel.**

26. Théorie de Dedekind[105]). Pour *R. Dedekind*, un *idéal* du corps K est un ensemble de quantités entières appartenant à ce corps et possédant les propriétés suivantes:

1°) Si deux quantités α, β appartiennent à l'idéal, il en est de même de leur somme;

2°) Si une quantité α appartient à l'idéal, il en est de même du produit $\alpha\lambda$, en désignant par λ un entier quelconque de K.

Ces deux propriétés appartiennent évidemment à l'ensemble des entiers du corps K qui sont divisibles par un entier déterminé α_0 du même corps; un tel ensemble constitue l'espèce la plus simple d'idéal; c'est ce que l'on nomme un *idéal principal*; on le désigne par le symbole (α_0).

L'idéal principal (1) est donc formé de tous les entiers de K.

Les idéaux principaux (qui correspondent, comme on le voit, aux quantités entières de K) sont les seuls qui existent dans un corps dont les éléments entiers forment un domaine holoïde complet; il en existe au contraire une infinité d'autres dans tout corps dont les éléments forment un domaine holoïde incomplet.

Plus généralement, plusieurs entiers $\alpha, \beta, \gamma \ldots$ de K définissent un idéal de K, à savoir celui qui est formé par tous les nombres représentables sous la forme

$$\lambda\alpha + \mu\beta + \nu\gamma + \cdots,$$

où λ, μ, ν sont des entiers de K; on le désignera par la notation $(\alpha, \beta, \gamma, \ldots)$.

Inversement, tout idéal de K peut être défini aussi par un nombre *fini* d'éléments fondamentaux $\alpha, \beta, \gamma, \ldots$ Autrement dit, non seulement (d'après la première propriété que nous avons prise pour définition) un idéal est un *module*; mais c'est un module *fini.*

On peut même préciser et ajouter [en se bornant, pour le moment, aux corps numériques] qu'il existe toujours[106]) n entiers η_1, $\eta_2, \ldots, \eta_n$ appartenant à l'idéal (où n est le degré absolu de K)

105) Pour les nombres algébriques, voir *R. Dedekind*, dans *G. Lejeune Dirichlet*, Zahlenth.[9]), (4e éd.) p. 550 (Suppl. XI, n° 177); Bull. sc. math. (2) 1 (1877), p. 207. Pour les fonctions algébriques d'une variable, voir *R. Dedekind* et *H. Weber*, J. reine angew. Math. 92 (1882), p. 181.

106) *D. Hilbert*, Jahresb. deutsch. Math.-Ver. 4 (1894/5), éd. Berlin 1897, p. 182, (théorème 6, n° 4).

et qui en forment la *base*, c'est-à-dire qui sont tels que tout autre élément de l'idéal puisse se mettre sous la forme

$$u_1\eta_1 + u_2\eta_2 + \cdots + u_n\eta_n,$$

$u_1, u_2, \ldots, u_n$ étant cette fois des entiers *rationnels.*

Une quantité qui fait partie d'un idéal (c'est-à-dire qui peut se représenter sous la forme indiquée) est encore dite *divisible* par cet idéal. Un idéal $\mathfrak{b}$ est *divisible* par un idéal $\mathfrak{a}$, si tout élément de $\mathfrak{b}$ est divisible par $\mathfrak{a}$ (il suffit évidemment qu'il en soit ainsi pour les éléments qui définissent $\mathfrak{b}$).

Un idéal apparaît ainsi comme le p. g. c. d. des éléments qui le définissent. Le p. g. c. d. de deux idéaux est défini par l'ensemble des quantités qui définissent les deux premiers.

Le *produit* de deux idéaux

$$\mathfrak{a} = (\alpha_1, \alpha_2, \ldots, \alpha_r), \quad \mathfrak{b} = (\beta_1, \beta_2, \ldots, \beta_s)$$

est l'idéal

$$\mathfrak{c} = \mathfrak{a}\mathfrak{b} = (\alpha_1\beta_1, \alpha_1\beta_2, \ldots, \alpha_i\beta_k, \ldots, \alpha_r\beta_s).$$

Un idéal qui n'est pas le produit de deux idéaux, dont l'un au moins serait l'idéal principal (1), est dit un idéal premier. Dans ces conditions, *tout idéal est décomposable, et d'une seule manière, en idéaux premiers.*

Si l'idéal $\mathfrak{c}$ est égal au produit $\mathfrak{a}\mathfrak{b}$, $\mathfrak{c}$ est évidemment divisible par $\mathfrak{a}$ et par $\mathfrak{b}$.

*Mais la démonstration de la proposition inverse:

3°) *Tout idéal* $\mathfrak{c}$ *qui est divisible par un idéal* $\mathfrak{a}$ *est égal au produit de* $\mathfrak{a}$ *par un troisième idéal* $\mathfrak{b}$[107])

constitue la plus sérieuse difficulté de la théorie des idéaux.

Cela tient à ce que la proposition précédente ne serait pas vraie si l'on considérait les idéaux, non du corps K, mais d'une espèce [n° **22**] intérieure à ce corps et autre que l'espèce principale. Les idéaux de cette espèce (anneau) sont formés [n° **31**] à l'aide des nombres de l'espèce envisagée de la façon même dont les idéaux du corps K sont formés à l'aide des nombres de l'espèce principale (en d'autres termes à l'aide des nombres *entiers* du corps K).*

*La proposition 3°) n'aurait par exemple, pas lieu entre les idéaux que l'on peut former avec les nombres de la forme $x + y\sqrt{-3}$, où x et y sont deux entiers rationnels, parce que le corps $(\mathrm{R}, \sqrt{-3})$

107) *D. Hilbert* [Jahresb. deutsch. Math.-Ver. 4 (1894/95), éd. Berlin 1897, p. 183] prend l'égalité $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$ comme *définition* de la divisibilité de $\mathfrak{a}$ par $\mathfrak{b}$. Dans cette terminologie le théorème à démontrer est: *Si tous les éléments de l'idéal* $\mathfrak{a}$ *font partie de l'idéal* $\mathfrak{b}$, $\mathfrak{a}$ *est divisible par* $\mathfrak{b}$.

contient des entiers qui ne sont pas de cette forme, à savoir les nombres $\frac{x + y\sqrt{-3}}{2}$, *où x et y désignent deux entiers rationnels impairs.**

*Dans la démonstration de la proposition 3°) il faut donc tenir compte de ce que le système d'idéaux que l'on considère contient *tous* les idéaux d'un même corps.

Il suffit d'ailleurs, comme on le voit aisément, de prouver la proposition suivante:

Tout idéal $\mathfrak{a}$ peut être multiplié par un idéal $\mathfrak{b}$ de manière que le produit soit un idéal principal.

C'est à quoi l'on peut arriver par plusieurs voies. On y arrive, par exemple, avec *R. Dedekind*[108]), en faisant usage de la théorie des modules et démontrant qu'un idéal est un module *propre.* On y arrive aussi[109]) en faisant usage d'un lemme relatif au produit de deux polynomes.*

Dès que la proposition 3°) est démontrée, la théorie de la divisibilité dans les corps quelconques devient, moyennant l'intervention des idéaux, toute semblable à ce qu'elle est dans les corps dont les entiers ne forment pas de domaine holoïde complet et, en particulier, dans la doctrine des entiers ordinaires.

27. Théorie de Kronecker et modifications apportées à cette théorie. *L. Kronecker*[110]) a fondé sa théorie sur les deux notions de *forme* et de *diviseur algébrique.* *D. Hilbert*[111]) a modifié cette théorie, au moins en ce qui concerne les corps de nombres, de façon à ne plus avoir à s'appuyer que sur la notion de forme. *H. Weber*[112]) et *Gy. (J.) König*[113]) ont, au contraire, modifié la théorie de *L. Kronecker* en y remplaçant la notion de diviseur par une autre plus générale; *H. Weber,* se borne au cas des corps de nombres et appelle *fonctional* le diviseur généralisé; *Gy. (J.) König* le désigne sous le nom de

108) *R. Dedekind* dans *G. Lejeune Dirichlet*, Zahlenth.[9]), (4° éd.) p. 553 (Suppl. XI, n° 177). Cf. *R. Dedekind*, Nachr. Ges. Gött. 1895, p. 106.*

109) *Voir *A. Hurwitz*, Nachr. Ges. Gött. 1894, p. 291; *D. Hilbert*, Jahresb. deutsch. Math.-Ver. 4 (1894/5), éd. Berlin 1897, p. 184 (n° 5); *P. Bachmann*, Zahlenkörper[67]), Leipzig 1905, p. 169. On trouvera d'autres méthodes dans le mémoire de *D. Hilbert* que l'on vient de citer, p. 247 (n° 36) et dans *A. Hurwitz*, Nachr. Ges. Gött. 1895, p. 324.*

110) Festschrift[1]), § 14/18; J. reine angew. Math. 92 (1882), p. 45/63; Werke 2, Leipzig 1897, p. 297/319.

111) Jahresb. deutsch. Math.-Ver. 4 (1894/5), éd. Berlin 1897, p. 186/8 (n° 6).

112) Alg.[14]), (1re éd.) 2, p. 489/526; (2e éd.) 2, p. 553/95.

113) Alg. Grössen[10]), p. 461/552 (chap. 9).

quantité idéale en envisageant d'ailleurs des corps algébriques quelconques au sens absolu du mot.

Une *forme* entière algébrique *du corps* K est un polynome entier (qui n'est nullement supposé homogène, contrairement à ce qui a lieu dans d'autres parties de l'algèbre où le même mot intervient) par rapport à un certain nombre d'indéterminées $u_1, u_2, \ldots$, les coefficients étant des quantités entières de K. Les éléments entiers du domaine K doivent être ici envisagés comme des formes de degré zéro. Soit Ω le corps *naturel* ($\mathfrak{R}$ ou $\mathrm{R}_{\mathfrak{R}}$ ou R) qui a donné naissance à K, et par rapport auquel K est un corps de degré n; soit F une forme de K. Le produit de F et de ses $n-1$ conjuguées $F', F'', \ldots, F^{(n-1)}$, produit qui, d'après la terminologie présente, doit s'appeler la norme de F et que nous désignerons par $N(F)$, est une forme de Ω, c'est-à-dire une forme dont les coefficients sont des (nombres ou polynomes) entiers ordinaires; d'où résulte en particulier qu'ils admettent un p. g. c. d. P qui est un entier de Ω. Si ce p. g. c. d. est égal à 1, la forme est dite une forme *primitive* ou une *forme-unité*. *L. Kronecker* désigne le quotient

$$\frac{N(F)}{P}$$

par le symbole

$$Fm(F).$$

L. Kronecker entend par *diviseurs algébriques* du corps K tous les quotients

$$\frac{F}{Fm(F)}.$$

Ces diviseurs algébriques sont, après les formes elles-mêmes, les types les plus simples des expressions que *H. Weber* désigne sous le nom de *fonctionaux entiers* et *Gy. König* sous celui de *quantités* (ou *grandeurs*) *idéales entières*. On entend, en effet, par „fonctional“ ou „quantité idéale“ tout quotient

$$\frac{F}{G}$$

de deux formes algébriques entières quelconques F et G du corps K. Quand G est une forme-unité, le „fonctional“ est dit *entier* la „quantité idéale“ est dite *entière*.

Plaçons-nous d'abord au point de vue général de *Gy.* (*J.*) *König*.

Si deux quantités idéales entières de K (par exemple deux diviseurs algébriques, deux formes entières, ou encore un diviseur algébrique et une forme entière) sont entre elles comme deux formes-unités, elles sont dites *équivalentes* ou, conformément à la terminologie précédente [n° **18**], *associées* et, au sens de la divisibilité, ne sont pas

considérées comme distinctes: c'est le cas, en particulier, pour deux quantités idéales entières dont les numérateurs ont les mêmes coefficients et ne diffèrent que par les variables ou puissances de variables affectées de ces coefficients. Les quantités idéales dont les numérateurs et les dénominateurs sont des formes-unités sont équivalentes à 1.

On dit qu'une quantité idéale entière $\mathfrak{A}$ est *divisible* par une quantité idéale entière $\mathfrak{B}$ lorsque le quotient $\frac{\mathfrak{A}}{\mathfrak{B}}$ est égal à une quantité idéale entière $\mathfrak{C}$.

Une quantité idéale entière est dite *irréductible* ou *première* (ou encore un *diviseur premier*) si elle n'est pas équivalente au produit de deux quantités idéales entières dont aucune ne soit équivalente à 1.

Dans ces conditions, on a ce théorème: *Toute* quantité idéale entière *du corps* K *est égale* à un *produit de diviseurs premiers, et cette décomposition est unique si l'on ne considère pas comme distincts deux diviseurs équivalents.*

Deux quantités idéales entières $\mathfrak{A}$ et $\mathfrak{B}$ admettent toujours un p. g. c d. c'est-à-dire un diviseur divisible par les diviseurs communs de $\mathfrak{A}$ et de $\mathfrak{B}$ et par ceux là seulement. Pour obtenir un p. g. c. d. de $\mathfrak{A}$ et $\mathfrak{B}$, il suffit de construire une quantité idéale entière $\mathfrak{C}$ dont le numérateur ait pour coefficients les éléments de K qui figurent parmi les coefficients de $\mathfrak{A}$ et de $\mathfrak{B}$. Tout p. g. c. d. de $\mathfrak{A}$ et $\mathfrak{B}$ est d'ailleurs équivalent à $\mathfrak{C}$.

Les définitions et les théorèmes concernant la divisibilité, la décomposition, etc. des quantités idéales entières s'appliquent encore lorsqu'on y remplace la notion de quantité idéale entière par celle de *diviseur algébrique*, ou encore par celle de *forme*, à condition toutefois de remplacer en même temps les *égalités* par des *équivalences*. On parvient ainsi d'une part à la théorie de *L. Kronecker* telle qu'il l'avait énoncée et d'autre part à la modification de cette théorie due à *D. Hilbert*. Au lieu d'„équivalent“ *L. Kronecker* dit d'ailleurs „absolument équivalent“, tandis que *D. Hilbert* dit „de même contenu (inhaltsgleich)“.

La théorie de *R. Dedekind* correspond à celle de *L. Kronecker* de la manière suivante: à tout diviseur algébrique de K correspond *l'idéal* qui est défini par les coefficients de son numérateur; à des diviseurs algébriques équivalents correspond le même idéal; à tout diviseur algébrique qui est équivalent à une quantité de K correspond un idéal principal. Au produit de deux diviseurs algébriques correspond le produit des deux idéaux respectifs; aux diviseurs premiers correspondent les idéaux premiers. Les deux théories sont donc bien équivalentes.

En comparant la théorie de *R. Dedekind* aux diverses modifications de la théorie de *L. Kronecker* dont on vient de parler, on parvient à des résultats analogues aux précédents. Pour bien mettre en évidence le lien des *idéaux* et des différentes quantités qui leur correspondent ainsi, il est commode de faire usage de la terminologie suivante:

Un diviseur algébrique, une forme et plus généralement un fonctional entier ou une quantité idéale entière sont dits des *représentations* de l'idéal correspondant, et ce dernier est dit[114]) le *contenu* de ce diviseur algébrique, de cette forme et plus généralement de ce fonctional entier ou de cette quantité idéale entière.

L'une ou l'autre des théories précédentes nous montre que deux ou plusieurs entiers de K ont toujours pour p. g. c. d. soit un véritable élément de K, soit au moins un idéal de K.

On démontre[115]) que tout idéal de K peut s'obtenir comme p. g. c. d. de *deux* entiers de K.

Deux idéaux sont dits *premiers* entre eux, s'ils n'ont aucun diviseur (idéal) commun que l'idéal (1).

28. *__Ensemble des quantités idéales entières d'un corps.__* Dans la théorie de *R. Dedekind* les idéaux d'un corps K ne forment pas un domaine holoïde; on ne peut, en effet, que multiplier mais non additionner ces idéaux. Dans la théorie de *L. Kronecker* les diviseurs algébriques ne forment pas non plus un domaine holoïde; la somme de deux diviseurs algébriques ne peut, en effet, pas toujours être mise sous la forme $\frac{F}{Fm(F)}$. Dans la théorie de *D. Hilbert* les formes entières du corps K forment au contraire un domaine holoïde; mais ce domaine n'est pas toujours complet; cela tient à ce que, pour les formes, les notions de divisibilité et de p. g. c. d. sont introduites de façon à n'exiger que l'équivalence là où au n° **24** figurait l'égalité.

Dans la théorie de *H. Weber* les fonctionaux entiers forment un domaine holoïde complet. Dans la théorie de *Gy. (J.) König* les quantités idéales entières forment de même un domaine holoïde complet. En effet, la somme de deux fonctionaux entiers est un fonctional entier; la somme de deux quantités idéales entières est une quantité

114) Pour le cas d'un idéal et d'une forme, voir *D. Hilbert,* Jahresb. deutsch. Math.-Ver. 4 (1894/5), éd. Berlin 1897, p. 186/8 (n° 6).

115) *R. Dedekind* dans *G. Lejeune Dirichlet*, Zahlenth.[9]), (4e éd.) p. 559 (Suppl. XI, n° 178) [pour les corps de nombres]; *R. Dedekind* et *H. Weber*, J. reine angew. Math. 92 (1882), p. 213 (cf. n° 9) [pour les corps de fonctions]; *D. Hilbert*, Jahresb. deutsch. Math.-Ver. 4 (1894/5), éd. Berlin 1897, p. 186 (théorème 12, n° 5); *Gy. (J.) König,* Alg. Grössen[10]), p. 494.

idéale entière; et, d'autre part, dans ces deux théories, les notions de divisibilité et de p. g. c. d. sont établies conformément à la définition des domaines holoïdes complets donnée au n° **24**.*

29. Norme d'un idéal. Congruence suivant des idéaux. *Désignons par Ω l'un quelconque des trois corps R, $\mathfrak{R}$ ou $R_{\mathfrak{R}}$ et par K un corps dérivé de Ω. Soient $\mathfrak{a}$ un idéal de K, $\mathfrak{A}$ une représentation (n° **27**) de $\mathfrak{a}$ (c'est-à-dire une quantité idéale de K dont $\mathfrak{a}$ est le contenu), F le numérateur, E le dénominateur de $\mathfrak{A}$; on a alors entre les normes de $\mathfrak{A}$, F et E la relation

$$N(\mathfrak{A}) = \frac{N(F)}{N(E)}.$$

Les coefficients du numérateur et du dénominateur de $N(\mathfrak{A})$ appartiennent au domaine Ω. Les coefficients de $N(F)$ ont donc pour p. g. c. d. un élément entier M de Ω et la quantité idéale entière $N(\mathfrak{A})$ est équivalente à M. La quantité M ne dépend que du choix de $\mathfrak{a}$ et non de celle des quantités entières idéales $\mathfrak{A}$ que l'on a choisie parmi celles en nombre infini, et équivalentes entre elles, qui sont des représentations de $\mathfrak{a}$.

On appelle M la norme de $\mathfrak{a}$ et on écrit

$$M = N(\mathfrak{a}).$$

Dans le cas où Ω est soit $R_{\mathfrak{R}}$ soit $\mathfrak{R}$, N n'est déterminé qu'au signe près. Dans le cas où Ω est R, N n'est même déterminé qu'à un facteur numérique près. Nous supposerons, dans ce qui suit, que, dans le cas où Ω est $\mathfrak{R}$, le signe de N est positif.

Si α est un élément entier du domaine K, la norme de l'idéal principal (α) formé par les nombres divisibles par α est égale à la norme (n° **12**) de α.

La norme d'un produit d'idéaux est le produit des normes des facteurs. Il résulte de là que la norme d'un idéal divise la norme de tout entier appartenant à cet idéal.

Prenons en particulier un idéal *premier* $\mathfrak{p}$. Il existe alors un élément P (un nombre ou une fonction), et un seul, *premier* rationnel dans Ω, divisible par $\mathfrak{p}$; c'est le p. g. c. d. de ceux des éléments entiers de Ω qui sont divisibles par $\mathfrak{p}$. La norme de $\mathfrak{p}$ est une puissance P^f de cet élément. On appelle f le *degré* de l'idéal premier $\mathfrak{p}$[116]). Dans la théorie des fonctions algébriques d'une seule variable chaque idéal premier est de degré $f = 1$.

116) **Gy. (J.) König,* Alg. Grössen[10]), p. 492. En ce qui concerne les corps de nombres cf. *R. Dedekind,* dans *G. Lejeune Dirichlet,* Zahlenth.[9]), (4e éd.) p. 565 (Suppl. XI, n° 180); *R. Dedekind*, Bull. sc. math. (2) 1 (1877), p. 213.*

Dans le cas des domaines de nombres, l'importance du rôle joué par les normes des idéaux doit être tout particulièrement signalée.*

Deux entiers α et β de K seront dits *congrus* suivant un idéal $\mathfrak{a}$ et, conformément à la définition générale des congruences suivant un module, on écrira

$$\alpha \equiv \beta \qquad (\mathfrak{a})$$

si la différence $\alpha - \beta$ est divisible par $\mathfrak{a}$. On considérera tous les nombres congrus entre eux suivant un idéal comme formant une même *classe* par rapport à cet idéal. Le nombre des classes qui sont distinctes suivant cet idéal, autrement dit le nombre d'entiers de K incongrus entre eux par rapport à $\mathfrak{a}$, est précisément égal à $N(\mathfrak{a})$[117]). On peut même, avec *R. Dedekind*[118]), définir directement $N(\mathfrak{a})$ par la somme de ces classes.

Si l'idéal d'un corps de nombres est considéré comme dérivé d'une base $(\eta_1, \eta_2, \ldots, \eta_n)$ [n° **26**] et si les n éléments de cette base sont eux-mêmes liés à une base $(y_1, y_2, \ldots, y_n)$ des nombres entiers du corps [n° **20**] par les formules

$$\eta_i = \omega_{i1} y_1 + \omega_{i2} y_2 + \cdots + \omega_{in} y_n \qquad (i = 1, 2, \ldots, n),$$

les ω_{ik} étant des entiers rationnels, la norme ne sera autre[119]) que la valeur absolue du déterminant $|\omega_{ik}|$.

Le degré f d'un idéal premier $\mathfrak{p}$ est[120]) le nombre maximé des entiers $y_1, y_2, \ldots$ de K entre lesquels on ne peut établir aucune relation de la forme

$$a_1 y_1 + a_2 y_2 + \cdots + a_f y_f \equiv 0 \qquad (\mathfrak{p}),$$

$a_1, a_2, \ldots, a_f$ étant des entiers rationnels non tous divisibles par p.

La norme p^f d'un idéal premier $\mathfrak{p}$ donne lieu à un théorème analogue au *théorème de Fermat* qui concerne les nombres premiers ordinaires [cf. I 18].

30. Classes d'idéaux. Deux idéaux $\mathfrak{a}$, $\mathfrak{b}$ d'un corps de *nombres* sont dits *équivalents* s'il existe un troisième idéal $\mathfrak{c}$ tel que les deux produits $\mathfrak{ac}$, $\mathfrak{bc}$ soient des idéaux principaux. On constate aisément qu'alors, si $\mathfrak{d}$ est un idéal tel que $\mathfrak{ad}$ soit un idéal principal, il en est de même de $\mathfrak{bd}$ (on peut encore dire que le rapport $\frac{\mathfrak{a}}{\mathfrak{b}}$ est égal au rapport de deux entiers de K).

117) *D. Hilbert*, Jahresb. deutsch. Math.-Ver. 4 (1894/5), éd. Berlin 1897, p. 190 (théorème 20, n° 7).

118) *R. Dedekind* dans *G. Lejeune Dirichlet*, Zahlenth.[9]), (4e éd.) p. 564/73 (Suppl. XI, n° 180), Bull. sc. math. (2) 1 (1887), p. 211.

119) *D. Hilbert*[117]), p. 189 (théorème 19, n° 7).

120) *D. Hilbert*[117]), p. 189 (théorème 17, n° 7).

Deux idéaux équivalents à un troisième sont équivalents entre eux, de sorte qu'on peut considérer tous les idéaux équivalents entre eux comme formant une même *classe* (un quelconque d'entre eux pouvant être considéré comme un *représentant* de cette classe.) La classe la plus simple est évidemment la classe *principale*, formée de tous les idéaux principaux.

Si deux idéaux $\mathfrak{a}$ et $\mathfrak{a}'$ sont équivalents, ce que l'on écrira

$$\mathfrak{a} \sim \mathfrak{a}'$$

et si l'on a de même

$$\mathfrak{b} \sim \mathfrak{b}',$$

on aura aussi

$$\mathfrak{ab} \sim \mathfrak{a}'\mathfrak{b}'.$$

On peut donc parler de la classe, *produit* de deux classes d'idéaux; et cette multiplication est commutative et associative.

A toute classe A correspond une classe *opposée*[121]) ou *réciproque*[122]) B, définie par cette condition que AB soit la classe principale.

Le nombre de classes d'idéaux d'un corps de nombres est fini[123]): c'est ce que l'on démontre en montrant que toute classe renferme au moins un représentant dont la norme [n° **12**] ne dépasse pas une certaine constante[124]), qui n'est autre que la racine carrée du discriminant du corps[125]).

Si h est le nombre de classes pour le corps K, la puissance $h^{\text{ième}}$ de tout idéal de K est un idéal principal[126]).

Les classes d'idéaux forment un groupe abélien fini, c'est-à-dire [n° **9**] un groupe d'éléments tels que la composition (ici la multiplication) de ces éléments soit commutative. Il existe un certain nombre q de *classes fondamentales* à l'aide desquelles on peut exprimer toutes les autres (d'une manière et d'une seule) par des produits formés de classes fondamentales[127]).

121) *R. Dedekind* dans *G. Lejeune Dirichlet*, Zahlenth.[9]), (4e éd.) p. 574 (Suppl. XI, n° 181); Bull. sc. math. (2) 1 (1877), p. 242.

122) *D. Hilbert*[117]), p. 223 (n° 22).

123) *L. Kronecker,* De unitatibus complexis, Diss. Berlin 1845 (§ 6); Werke 1, Berlin 1895, p. 25; *R. Dedekind* dans *G. Lejeune Dirichlet,* Zahlenth.[9]), (4e éd.) p. 575 (Suppl. XI, n° 181); Bull. sc. math. (2) 1 (1877), p. 242; *A. Hurwitz*, Nachr. Ges. Gött. 1895, p. 230/40.

124) *R. Dedekind,* Bull. sc. math. (2) 1 (1877), p. 242.

125) *H. Minkowski,* J. reine angew. Math. 107 (1891), p. 785.

126) *R. Dedekind* dans *G. Lejeune Dirichlet*, Zahlenth.[9]), (4e éd.) p. 576 (Suppl. XI, n° 181); Bull. sc. math. (2) 1 (1877), p. 245.

127) *E. Schering,* Abh. Ges. Gött. 14 (1868/9), éd. 1869, math. mém. n° 1, p. 3/16; Werke 1, Berlin 1902, p. 135/48; *L. Kronecker,* Monatsb. Akad. Berlin 1870, p. 881; Werke 1, Leipzig 1895, p. 271; *D. Hilbert*[117]), p. 232/3 (n° 28).

*Il importe parfois d'introduire des notions plus restreintes d'*équivalence* et de *classe*. Ainsi *D. Hilbert* a été amené à n'envisager deux idéaux comme équivalents que quand leur quotient est un nombre *positif total* du corps K. Pour éviter toute confusion il dit que deux idéaux vérifiant cette condition sont *équivalents au sens restreint du mot*. On pourrait aussi pour préciser davantage dire que ces idéaux sont des *idéaux positivement équivalents*. Tous les idéaux équivalents dans ce sens restreint forment une *classe*[128]) au sens restreint du mot.

On entend d'ailleurs par nombre *positif total* de K un nombre entier ou fractionnaire de K qui, quand K est un corps réel, est *positif*, et dont les nombres conjugués sont aussi positifs chaque fois que les corps conjugués de K dont ils font partie sont réels[129]).

31. *Idéaux d'un anneau. Le conducteur d'un anneau. Si dans un corps K dérivé de $\mathfrak{R}$ on envisage un anneau A, on appelle „idéal de cet anneau" tout système infini $\alpha_1, \alpha_2, \ldots\ldots$ d'éléments algébriques de l'anneau dont une combinaison linéaire quelconque

$$\lambda_1\alpha_1 + \lambda_2\alpha_2 + \cdots\cdots$$

reproduise un des éléments du système, et cela quels que soient les entiers de l'anneau A par lesquels on remplace $\lambda_1, \lambda_2, \ldots\ldots$

Un idéal de l'anneau A n'est pas nécessairement un idéal du corps K, (c'est-à-dire un idéal dans le sens toujours donné à ce mot jusqu'ici). Mais, dans l'anneau A, il y a toujours certains idéaux qui sont idéaux du corps K. On appelle[130]) *conducteur* (*Führer*) de l'anneau, le p. g. c. d. de ceux des idéaux de l'anneau qui sont aussi des idéaux du corps K.*

32. Interprétation fonctionnelle. Notion de diviseur rationnel. Nous avons vu [n° 8] que la théorie des corps de fonctions algébriques, considérés comme dérivés du corps général R, est identique à celle des fonctions attachées à une courbe ou à une surface algébrique.

L'identité des deux théories cesse toutefois d'être complète lorsqu'on fait intervenir la notion d'entier algébrique.

En effet, les *fonctions algébriques entières* sont définies [n° **17**]

128) *R. Dedekind* dans *G. Lejeune Dirichlet*, Zahlenth.[9]), (4e éd.) p. 578 (Suppl. XI, n° **181**) envisage le cas où pour considérer deux idéaux comme équivalents on exigerait que leur rapport fût celui de deux nombres à *normes positives*. Ceci n'a d'ailleurs de sens que dans des corps convenablement choisis (toujours de degré pair) où il existe des nombres à norme négative mais non d'unité à norme négative: tel est le corps $(\mathrm{R}, \sqrt{3})$.

129) *D. Hilbert*, Nachr. Ges. Gött. 1898, p. 374.

130) **R. Dedekind* dans *G. Lejeune Dirichlet*, Zahlenth.[9]), (4e éd.) p. 572 Suppl. XI, n° 180).*

par la condition d'être toujours finies *à distance finie*. De même, dans le domaine des fonctions, les unités algébriques sont les fonctions qui ne sont ni nulles ni infinies à *distance finie*. Or une telle définition ne saurait prendre place dans la théorie des fonctions algébriques, telle qu'on la considère habituellement: celle-ci est en effet invariante par une transformation birationnelle quelconque et ne distingue pas entre les points à distance finie et les points à l'infini. C'est précisément pour cela que dans la théorie des fonctions algébriques d'une variable (fonctions rattachées à une courbe) les notions d'entier algébrique et d'idéal ne jouent qu'un rôle secondaire. Le rôle principal est rempli par la notion toute distincte du *diviseur*[131]).

*Cette notion de *diviseur* apparaît déjà dans la théorie des fonctions rationnelles d'une variable indépendante x.

A chaque valeur α de x convenons de faire correspondre un *symbole* $\mathfrak{p}$ que nous appellerons le „diviseur premier rationnel de α". Dans la représentation des nombres complexes par les points d'une sphère, nous représenterons $\mathfrak{p}$ par le même point de la sphère que α lui-même.

A chaque fonction rationnelle $\frac{P(x)}{Q(x)}$ d'une variable x correspond un nombre entier ϱ (positif, nul ou négatif) tel que, pour des valeurs suffisamment petites de $|x - \alpha|$, on ait

$$\frac{P(x)}{Q(x)} = (x - \alpha)^\varrho\,[A_0 + A_1(x - \alpha) + A_2(x - \alpha)^2 + \cdots\cdots],$$

où $A_0, A_1, A_2, \ldots\ldots$ désignent des constantes, A_0 étant différent de zéro. Ce nombre entier ϱ est ce qu'on appelle l'*ordre* de la fonction rationnelle $\frac{P(x)}{Q(x)}$ de la variable x relativement au diviseur premier *rationnel* $\mathfrak{p}$ correspondant à α.

Au pôle $x = \infty$ de la sphère correspond de même un diviseur premier rationnel $\mathfrak{p}_\infty$ que nous appellerons le „diviseur premier de $x = \infty$". L'ordre de la fonction rationnelle $\frac{P(x)}{Q(x)}$ relativement au diviseur premier rationnel $\mathfrak{p}_\infty$ est le nombre ϱ pour lequel $\frac{P(x)}{Q(x)}$ peut être mis sous la forme

$$\frac{P(x)}{Q(x)} = \left(\frac{1}{x}\right)^\varrho \left[A_0 + \frac{A_1}{x} + \frac{A_2}{x^2} + \cdots\cdots\right],$$

où $A_0, A_1, A_2, \ldots$ désignent des constantes, A_0 étant différent de zéro.

En désignant par $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_h$ un nombre quelconque h de diviseurs premiers rationnels de $\frac{P(x)}{Q(x)}$, et par $\sigma_1, \sigma_1, \ldots, \sigma_h$ des entiers

131) *Ce qui suit dans ce numéro **32**, ainsi que le texte et les notes des numéros **33** à **41**, est presque entièrement dû à *J. Kürschák*.*

quelconques (positifs, nuls ou négatifs), le symbole

$$d = \mathfrak{p}_1^{\sigma_1}\mathfrak{p}_2^{\sigma_2}\ldots\mathfrak{p}_h^{\sigma_h}$$

est désigné par *K. Hensel* et *G. Landsberg*[132]) sous le nom de *diviseur rationnel* de $\frac{P(x)}{Q(x)}$. L'introduction de ce symbole est souvent commode dans les théories qui nous occupent et cela principalement parce qu'il permet de faire usage de la terminologie suivante:

On dit qu'une fonction rationnelle $\frac{P(x)}{Q(x)}$ est divisible par d *relativement* au diviseur premier $\mathfrak{p}_i$ quand l'ordre de $\frac{P(x)}{Q(x)}$ relatif à $\mathfrak{p}_i$ est au moins égal à σ_i.

On dit que $\frac{P(x)}{Q(x)}$ est divisible par d (sans épithète) quand $\frac{P(x)}{Q(x)}$ est divisible par d relativement à $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_h$, et a, relativement à tout autre diviseur premier[133]), un ordre positif ou nul; d est alors *un* diviseur de $\frac{P(x)}{Q(x)}$.

On dit que

$$d = \mathfrak{p}_1^{\sigma_1}\mathfrak{p}_2^{\sigma_2}\ldots\mathfrak{p}_n^{\sigma_n}$$

est *le* diviseur de $\frac{P(x)}{Q(x)}$, et non plus seulement *un* diviseur de $\frac{P(x)}{Q(x)}$ quand l'ordre de $\frac{P(x)}{Q(x)}$ relativement à $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_h$ est précisément égal à $\sigma_1, \sigma_2, \ldots, \sigma_h$, et que cet ordre est nul relativement à tout autre diviseur premier.

Le diviseur d de $\frac{P(x)}{Q(x)}$ correspond ainsi à l'ensemble complet des infinis et des zéros de $\frac{P(x)}{Q(x)}$. Quand on connaît *le* diviseur de $\frac{P(x)}{Q(x)}$ la fonction $\frac{P(x)}{Q(x)}$ est déterminée à un facteur constant près.

Il s'en faut d'ailleurs que tout symbole

$$d = \mathfrak{p}_1^{\sigma_1}\mathfrak{p}_2^{\sigma_2}\ldots\mathfrak{p}_h^{\sigma_h}$$

soit *le* diviseur d'une fonction rationnelle. Pour qu'il en soit ainsi, il faut et il suffit que la somme

$$\sigma_1 + \sigma_2 + \cdots + \sigma_h,$$

à laquelle on donne le nom d'*ordre de d*, soit nulle.

Ainsi, $\mathfrak{p}$ désignant le diviseur premier correspondant à α, le symbole

$$\mathfrak{p}\mathfrak{p}_\infty^{-1}, \quad \text{ou} \quad \frac{\mathfrak{p}}{\mathfrak{p}_\infty},$$

est *le* diviseur de la fonction $x - \alpha$.

132) *Theorie der algebraischen Funktionen einer Variabel und ihre Anwendung auf algebraische Kurven und Abelsche Integrale, Leipzig 1902, p. 13.*

133) *On peut d'ailleurs dire que tout diviseur non représenté effectivement dans le symbole (1) y figure effectivement avec l'exposant zéro.*

Toute fonction rationnelle de x dont d est *un* diviseur est dite *multiple* de d. Pour obtenir les multiples d'un diviseur d d'ordre négatif $-\tau$ on formera la fonction $\frac{P(x)}{Q(x)}$ dont

$$d' = d\mathfrak{p}_\infty^\tau$$

est *le* diviseur; les multiples cherchés de d sont alors les fonctions obtenues en donnant à $c_0, c_1, \ldots, c_\tau$, dans l'expression

$$\frac{P(x)}{Q(x)}(c_0 + c_1 x + \cdots + c_\tau x^\tau),$$

des valeurs constantes arbitraires. Les diviseurs d'ordre positif n'ont pas de multiple.*

33. Notion de diviseur premier algébrique. *Soit

$$f(x, y) = 0$$

l'équation d'une courbe algébrique irréductible. A chaque valeur α donnée à la variable indépendante x correspondent[134]) n séries de la forme

$$(1) \qquad y = (x-\alpha)^{\frac{\tau}{a}}\left[C_0 + C_1(x-\alpha)^{\frac{1}{a}} + C_2(x-\alpha)^{\frac{2}{a}} + \cdots\right]$$

vérifiant identiquement en x l'équation $f(x, y) = 0$. Le nombre n de ces séries est égal au degré en y de la fonction $f(x, y)$; a est un nombre positif entier, τ est un entier (positif nul ou négatif); $C_0, C_1, C_2, \ldots$ sont des nombres complexes (réels ou imaginaires), C_0 n'est pas nul. Les nombres a, τ peuvent avoir des valeurs distinctes dans les n séries (1) correspondant à la même valeur α de x.

Si dans une des séries (1) le nombre a est plus grand que 1, les $a - 1$ séries que l'on déduit de (1) en y remplaçant successivement les puissances de $(x-\alpha)^{\frac{1}{a}}$ par celles de même exposant de

$$\varepsilon_1(x-\alpha)^{\frac{1}{a}}, \ \varepsilon_2(x-\alpha)^{\frac{1}{a}}, \ \ldots, \ \varepsilon_{a-1}(x-\alpha)^{\frac{1}{a}},$$

où $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{a-1}$ sont les $a - 1$ racines $a^{\text{ièmes}}$ de l'unité autres que 1, vérifient comme la série (1) elle-même, l'équation $f(x, y) = 0$ identiquement en x. Ces a séries vérifient identiquement une équation de la forme $F(x, y) = 0$, où $F(x, y)$ envisagée comme une fonction de y est une fonction rationnelle entière de degré a (en y), dont les coefficients sont des séries entières en $(x - \alpha)$. Cette fonction de y ne peut d'ailleurs être décomposée en facteurs ayant pour coefficients des séries entières en $(x - \alpha)$.

134) *Voir par ex. *E. Picard*, Traité d'Analyse (2e éd.) 2, Paris 1905, p. 392 et suiv.*

On dit de ces a séries qu'elles forment un cycle contenant a termes. Pour uniformiser le langage on dit aussi, quand $a = 1$, que la série correspondante (1) forme un cycle à un seul terme.

On appelle *éléments* de la courbe $f(x, y) = 0$ les cycles que l'on peut ainsi former pour les diverses valeurs de α.

Les diverses séries du même cycle correspondant à une valeur α de la variable indépendante x ont pour $x = \alpha$ la même valeur $y = \beta$; cette valeur $y = \beta$ est égale à C_0, à zéro, ou à l'infini selon que τ est nul, positif ou négatif. Il peut même arriver que les séries de plusieurs éléments correspondant à la même valeur α de x se réduisent pour $x = \alpha$ à la même valeur $y = \beta$. Dans ce cas il convient de *distinguer* plusieurs points (α, β) de la courbe ayant les mêmes coordonnées mais appartenant à des éléments distincts.

Ceci convenu, à chaque point de la courbe faisons correspondre un symbole $\mathfrak{P}$ déterminant non seulement les coordonnées de ce point, mais aussi l'élément auquel il appartient. On dit d'un tel symbole qu'il est un *diviseur algébrique premier* du corps K.

Si l'on fait usage de la représentation géométrique des fonctions algébriques due à *B. Riemann*[135]), on voit qu'à chaque diviseur algébrique premier du corps K correspond un point de la surface de Riemann; *K. Hensel* et *L. Landsberg*[136]) identifient ce point et le diviseur algébrique premier correspondant.

Si $\mathfrak{P}$ correspond à un point P de la courbe algébrique appartenant à un élément de cycles contenant a termes, où $a > 1$, ce point P est dit *point de ramification* et $\mathfrak{P}$ est dit *diviseur premier de ramification d'ordre* $a - 1$.

Aux n séries (1) pour lesquelles α est supposé donné, correspondent n diviseurs du corps K. On les appelle les diviseurs conjugués de ce corps; ils ne sont tous distincts que si aucun d'eux n'est diviseur premier de ramification. Si $\mathfrak{P}$ est un diviseur premier de ramification d'ordre $a - 1$, le nombre des diviseurs conjugués de $\mathfrak{P}$ qui sont égaux à $\mathfrak{P}$ est précisément égal à $a - 1$.

Soit maintenant $\frac{P(x, y)}{Q(x, y)}$ une fonction rationnelle entière quelconque de x et y, donc une fonction quelconque du corps K; envisageons un diviseur premier quelconque $\mathfrak{P}$ de K et remplaçons dans $\frac{P(x, y)}{Q(x, y)}$ successivement y par les a séries du cycle correspondant à $\mathfrak{P}$; nous

135) *Diss. Göttingue 1851, p. 4 (§ 5); Werke[25]), (2e éd.), p. 7; trad. *L. Laugel*, p. 6. Voir aussi *E. Picard*, Traité d'Analyse[134]), (2e éd.) 2, p. 411.*

136) *Alg. Funkt.[132]), p. 145.*

obtenons ainsi a nouvelles séries de la forme

$$(x-\alpha)^{\frac{\varrho}{a}}\left[A_0 + A_1(x-\alpha)^{\frac{1}{a}} + A_2(x-\alpha)^{\frac{2}{a}} + \cdots\cdots\right]$$

qui peuvent ne pas être toutes distinctes les unes des autres; ϱ désigne un nombre entier (positif, nul ou négatif) et A_0 n'est pas nul.

A chaque diviseur $\mathfrak{P}$ correspond ainsi un cycle de séries pour la fonction rationnelle $\frac{P(x, y)}{Q(x, y)}$. On dit que cette fonction est d'ordre ϱ par rapport à $\mathfrak{P}$. L'*ordre* ϱ par rapport à $\mathfrak{P}$ est le numérateur de l'exposant $\frac{\varrho}{a}$ de $(x - \alpha)$ dans le premier terme du développement des a séries du cycle correspondant à $\mathfrak{P}$.

La notion de diviseur algébrique premier $\mathfrak{P}$ d'un corps K déterminé par l'équation $f(x, y) = 0$ joue déjà un rôle dans l'étude des points d'intersection de la courbe $f(x, y) = 0$ et d'une courbe algébrique quelconque $\varphi(x, y) = 0$. Fixons une des séries (1) de l'élément de $f(x, y) = 0$ qui correspond à un diviseur détermine $\mathfrak{P}$ de K. Si l'*ordre* ϱ de la fonction $\varphi(x, y)$, dans laquelle y est envisagé comme une fonction algébrique de x définie par l'équation $f(x, y) = 0$, est *positif* par rapport à $\mathfrak{P}$, on dit qu'au diviseur premier $\mathfrak{P}$ correspond un point d'intersection de *multiplicité* ϱ de $f(x, y) = 0$ et de $\varphi(x, y) = 0$.

Si au point d'intersection $x = \alpha$, $y = \beta$, des deux courbes $f(x, y) = 0$ et $\varphi(x, y) = 0$, on peut faire correspondre plusieurs diviseurs $\mathfrak{P}_1$, $\mathfrak{P}_2$, $\ldots$, $\mathfrak{P}_i$ et si au diviseur $\mathfrak{P}_1$ correspond une intersection de multiplicité ϱ_1, au diviseur $\mathfrak{P}_2$ une intersection de multiplicité ϱ_2, $\ldots$, au diviseur $\mathfrak{P}_i$ une intersection de multiplicité ϱ_i de ces deux courbes, on dit qu'au point $x = \alpha$, $y = \beta$ se trouvent confondus $\varrho_1 + \varrho_2 + \cdots + \varrho_i$ points d'intersection des deux courbes.

Ce qui précède s'applique aussi au cas où $\alpha = \infty$ à condition de remplacer partout $x - \alpha$ par $\frac{1}{x}$.*

34. Notion générale des diviseurs algébriques. Classes de diviseurs. **K. Hensel* et *G. Landsberg*[137]) comprennent sous le nom de diviseurs algébriques d'un corps K attaché à une courbe $f(x, y) = 0$ l'ensemble des symboles

$$D = \mathfrak{P}_1^{\varrho_1}\mathfrak{P}_2^{\varrho_2}\cdots\mathfrak{P}_h^{\varrho_h}, \tag{1}$$

où $\mathfrak{P}_1$, $\mathfrak{P}_2$, $\ldots$, $\mathfrak{P}_h$ sont h quelconques des diviseurs premiers de ce corps K, et où ϱ_1, ϱ_2, $\ldots$, ϱ_h sont des nombres entiers arbitrairement fixés (positifs, nuls ou négatifs).

Un tel diviseur est dit *entier*, si aucun des exposants ϱ n'est

137) *Alg. Funkt.[132]), p. 146.*

négatif, *fractionnaire* dans le cas contraire: l'ensemble des facteurs à exposants positifs et celui des facteurs à exposants négatifs constituent respectivement le *numérateur* et le *dénominateur.* La somme des exposants ϱ est *l'ordre du diviseur.*

Si l'on convient d'entendre par $\mathfrak{P}_i^0$ que le facteur $\mathfrak{P}_i$ ne figure pas dans un symbole (1), on peut évidemment, pour comparer entre eux deux diviseurs quelconques du corps K les mettre sous la forme

$$(2) \qquad D = \mathfrak{P}_1^{\varrho_1} \mathfrak{P}_2^{\varrho_2} \dots \mathfrak{P}_h^{\varrho_h}, \quad D' = \mathfrak{P}_1^{\sigma_1} \mathfrak{P}_2^{\sigma_2} \dots \mathfrak{P}_h^{\sigma_h},$$

où dans D et D' figurent les mêmes facteurs $\mathfrak{P}$. Ceci posé, on appelle *produit* des deux diviseurs D et D' le symbole

$$DD' = \mathfrak{P}_1^{\varrho_1+\sigma_1} \mathfrak{P}_2^{\varrho_2+\sigma_2} \dots \mathfrak{P}_h^{\varrho_h+\sigma_h};$$

on appelle *quotient* des deux diviseurs D et D' le symbole

$$\frac{D}{D'} = \mathfrak{P}_1^{\varrho_1-\sigma_1} \mathfrak{P}_2^{\varrho_2-\sigma_2} \dots \mathfrak{P}_h^{\varrho_h-\sigma_h}.$$

Quand ce quotient est un diviseur *entier* du corps K, on dit que D est divisible par D'.

Si, dans les symboles (2), on désigne, pour chacun des indices i, par τ_i le plus petit des deux nombres ϱ_i et σ_i, le symbole

$$\mathfrak{P}_1^{\tau_1} \mathfrak{P}_2^{\tau_2} \dots \mathfrak{P}_h^{\tau_h}$$

est divisible par les diviseurs communs à D et à D' et par ceux-là seulement; c'est pourquoi on l'appelle *le plus grand commun diviseur* de D et de D'.

Le symbole (1) n'a par lui-même aucun sens; mais l'emploi de ce symbole permet de s'exprimer d'une façon simple et commode dans toute la théorie qui nous occupe. On dit, en particulier, qu'une fonction quelconque $\frac{P(x,y)}{Q(x,y)}$ du corps K est divisible par le diviseur (1) relativement à un diviseur premier donné $\mathfrak{P}$, lorsque l'ordre de cette fonction relativement à $\mathfrak{P}$ est au moins égal à l'exposant ϱ avec lequel $\mathfrak{P}$ figure dans le diviseur (1).

A chaque diviseur *entier* D correspond un groupe de points sur la courbe algébrique $f(x, y) = 0$. La condition nécessaire et suffisante pour que les points de ce groupe soient points d'intersection (avec multiplicité convenable déterminée par D) de la courbe $f(x, y) = 0$ et d'une autre courbe algébrique $P(x, y) = 0$, est que la fonction $P(x, y)$, après qu'on y a remplacé y par la fonction algébrique de x définie par l'équation $f(x, y) = 0$, soit *partout* divisible par D.

On dit que le symbole (1) représente *le* diviseur (et non plus *un* diviseur) d'une fonction attachée à la courbe si, pour $i = 1, 2, \dots, h$,

l'ordre de cette fonction au point

$$\mathfrak{P}_i$$

est *exactement* égal à ϱ_i et que de plus la fonction est d'ordre nul en tout point non représenté dans le symbole (1). Le diviseur d'une fonction fait par conséquent connaître l'ensemble complet des zéros et des infinis de la fonction.

La connaissance du diviseur d'une fonction attachée à la courbe détermine complètement cette fonction à un facteur constant près[138]. Mais il s'en faut que tout symbole (1) soit le diviseur d'une fonction. Il faut d'abord, d'après un théorème connu[139], que l'ordre du symbole soit nul, d'où résulte, en particulier, que le diviseur (si la fonction correspondante ne se réduit pas à une constante) doit être fractionnaire; cette condition n'est d'ailleurs elle-même pas suffisante et entre le numérateur et le dénominateur doivent en outre exister un série de relations (que fait connaître le théorème d'Abel).

Si ces diverses conditions sont remplies et si, par conséquent, il existe une fonction dont le diviseur est D, celui-ci est dit un diviseur *principal.* Il est clair que le produit de deux diviseurs principaux est encore un diviseur principal.

Deux diviseurs appartiennent à une même *classe* si leur quotient est un diviseur principal[140]. Il est clair que tous les diviseurs d'une même classe ont même ordre: on appelle cet ordre *l'ordre de la classe.* Les classes de diviseurs se multiplient évidemment comme les classes d'idéaux. A chaque classe de diviseurs correspond une classe *opposée* ou *réciproque* qui, multipliée par la première, donne la classe principale.*

35. Norme d'un diviseur. Soit $\mathfrak{P}$ un diviseur premier algébrique du corps K attaché à la courbe

$$f(x, y) = 0.$$

Soit

$$y = (x-\alpha)^{\frac{\tau}{\alpha}}\left[C_0 + C_1(x-\alpha)^{\frac{1}{\alpha}} + C_2(x-\alpha)^{\frac{2}{\alpha}} + \cdots\cdots\right]$$

une des séries de l'élément correspondant de la courbe (quand $\alpha = \infty$, il est entendu que $x - \alpha$ doit être remplacé par $\frac{1}{x}$).

138) *En effet, une fonction partout finie sur la courbe est une constante [voir *E. Picard*, Traité d'analyse[134]) (2e éd.) 2, p. 430].*

139) *Cf. *E. Picard*, Traité d'Analyse[134]) (2e éd.) 2, p. 471.*

140) *De même que l'on envisage des *classes de diviseurs*, on peut aussi envisager des *classes d'idéaux* d'un corps de fonctions. Il importe d'observer ici que, contrairement à ce que l'on a trouvé pour les *corps de nombres*, les classes d'idéaux des *corps de fonctions* sont, comme les classes de diviseurs de ces *corps de fonctions*, en nombre infini.*

On appelle *norme de* $\mathfrak{P}$ le diviseur $\mathfrak{p}$ correspondant à α dans le corps des fonctions rationnelles de x. On peut l'identifier au produit de $\mathfrak{P}$ et des $n-1$ diviseurs premiers algébriques (de K) conjugués de $\mathfrak{P}$.

Quand la norme de $\mathfrak{P}$ est $\mathfrak{p}_\infty$ on dit que $\mathfrak{P}$ est un diviseur premier algébrique infini et on le représente par le symbole $\mathfrak{P}_\infty$.

$_*$Si

$$\mathrm{D} = \mathfrak{P}_1^{\sigma_1} \mathfrak{P}_2^{\sigma_2} \dots \mathfrak{P}_h^{\sigma_h}$$

est un diviseur algébrique quelconque du corps K attaché à la courbe $f(x, y) = 0$, on appelle *norme*[141]) de D le diviseur rationnel

$$d = \mathfrak{p}_1^{\sigma_1} \mathfrak{p}_2^{\sigma_2} \dots \mathfrak{p}_h^{\sigma_h}$$

obtenu en remplaçant dans D chacun des facteurs $\mathfrak{P}_i$ par sa norme $\mathfrak{p}_i$.

Dans le cas où l'ordre d'un diviseur est nul (et dans ce cas seulement), la norme de ce diviseur est le diviseur d'une fonction rationnelle de x seul. En particulier, si D est le diviseur d'une fonction algébrique, d est le diviseur de la norme de cette fonction algébrique.*

36. Fonctions admettant un diviseur donné. $_*$L'un des problèmes fondamentaux de la théorie est le suivant: trouver toutes les fonctions admettant un diviseur donné de la forme

$$\mathfrak{P}_1^{\varrho_1} \mathfrak{P}_2^{\varrho_2} \dots \mathfrak{P}_h^{\varrho_h} \tag{1}$$

ou, plus exactement, trouver toutes les fonctions dont le diviseur est divisible par un diviseur donné.

Nous supposerons que $\mathfrak{P}_1, \mathfrak{P}_2, \dots, \mathfrak{P}_h$ sont des diviseurs finis et qu'à tous les diviseurs infinis du corps K envisagé correspondent des cycles à un terme. S'il n'en était pas ainsi il suffirait d'effectuer une substitution

$$x' = \frac{1}{x - \alpha_0}$$

dans l'équation $f(x, y) = 0$ pour retomber sur le cas envisagé.

Avant d'aborder la solution du problème que l'on vient de poser, nous déterminerons toutes les fonctions du corps K qui, par rapport à chaque diviseur *fini* $\mathfrak{P}$, sont divisibles par un diviseur (1), donc aussi celles qui sont d'ordre négatif pour un ou plusieurs diviseurs infinis $\mathfrak{P}_\infty$. Nous désignons par J l'ensemble de ces fonctions et nous dirons de J qu'il est un *idéal entier* ou un *idéal fractionnaire*[142]) suivant que D sera un diviseur entier ou fractionnaire.

141) $_*$*K. Hensel* et *G. Landsberg*, Alg. Funkt.[132]), p. 150.*

142) $_*$Sur la différence entre les notions d'*idéal* et de *diviseur*, voir aussi *G. Landsberg*, Jahresb. deutsch. Math. Ver. 14 (1905), p. 93.*

Les idéaux entiers sont identiques aux idéaux de *R. Dedekind* [n° **26**].

Pour déterminer les fonctions de l'idéal J[143]) envisageons une base $(\xi_1, \xi_2, \dots, \xi_n)$ du corps [n° **7**]. Choisissons cette base, ce qui est toujours possible, de façon que chaque ξ_i soit contenue dans l'idéal J. Soit alors

$$\Delta = \begin{vmatrix} \xi_1 & \xi_1' & \xi_1'' & \dots & \xi_1^{(n-1)} \\ \xi_2 & \xi_2' & \xi_2'' & \dots & \xi_2^{(n-1)} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \xi_n & \xi_n' & \xi_n'' & \dots & \xi_n^{(n-1)} \end{vmatrix}$$

le déterminant des éléments $\xi_1, \xi_2, \dots, \xi_n$ de cette base et de leurs conjugués.

Si α est une valeur finie quelconque de x, si $\mathfrak{p}$ est le diviseur premier rationnel correspondant, et si $\mathfrak{P}$ est un des diviseurs de K ayant pour norme $\mathfrak{p}$, si enfin ϱ est l'exposant avec lequel $\mathfrak{P}$ figure dans le symbole (1), et si $\mathfrak{P}$ correspond à un cycle d'ordre a, le développement de la fonction Δ suivant les puissances de $x - \alpha$ commence par un terme dont l'exposant est au moins égal à

$$t_\alpha = \sum \left(\varrho + \frac{a-1}{2}\right),$$

où la somme est étendue à toutes les valeurs de $\varrho + \frac{a-1}{2}$ qui correspondent aux différents diviseurs $\mathfrak{P}$ ayant pour norme $\mathfrak{p}$.

Il n'y a qu'un nombre fini de telles valeurs α de x pour lesquelles l'exposant en question soit plus grand que t_α. Un nombre *fini* d'opérations permet de passer à des bases telles que le nombre de ces valeurs de α diminue de plus en plus pour enfin devenir nul. Si l'on convient de désigner encore par $(\xi_1, \xi_2, \dots, \xi_n)$ la base pour laquelle le nombre de ces valeurs de α est nul, on a pour cette dernière base

$$\Delta = \prod (x - \alpha)^{\Sigma\left(\varrho + \frac{a-1}{2}\right)}, \tag{2}$$

où le produit est étendu à toutes ces valeurs de α pour lesquelles la valeur de p correspondant à $x - \alpha$ est égale à la norme d'un diviseur $\mathfrak{P}$ pour lequel ϱ ou $a - 1$ est différent de zéro.

Si l'on a fixé cette base $(\xi_1, \xi_2, \dots, \xi_n)$ parmi celles dont les éléments appartiennent à J, toutes les fonctions pouvant être représentées par la formule

$$\xi = u_1 \xi_1 + u_2 \xi_2 + \dots + u_n \xi_n,$$

143) $_*$*K. Hensel* et *G. Landsberg*, Alg. Funkt.[132]), p. 204/21; *K. Hensel*, J. reine angew. Math. 115 (1895), p. 254.*

et celles-là-seulement, sont contenues dans J. Ici $u_1, u_2, \ldots, u_n$ désignent des fonctions rationnelles entières de x.

Nous dirons d'une telle base qu'elle est un *système fondamental* pour J.*

Supposons, en particulier, qu'il s'agisse de l'idéal principal (1), c'est-à-dire de l'ensemble des quantités entières du corps. Alors $(\xi_1, \xi_2, \ldots, \xi_n)$ est la *base* des quantités entières du corps dans le sens de *R. Dedekind* [n° **20**] et le carré du déterminant Δ, c'est-à-dire le *discriminant du corps*, est, à un facteur constant près,

$$D = \Pi(x-\alpha)^{\Sigma(a-1)}. \tag{3}$$

Égalé à zéro, il représente le système des points de ramification ou, plus exactement, l'équation qui fournit les abscisses des points de ramification finis.

*On peut aussi mettre en évidence la signification du discriminant du corps en observant que *à chaque point de ramification correspond un diviseur premier de ramification*, donc aussi, quand on se borne aux points de ramification à abscisses finies, un certain *idéal premier de ramification*. Soient

$$P_1,\ P_2,\ P_3,\ \ldots\ldots$$

les points de ramification et

$$a_1,\ a_2,\ a_3,\ \ldots\ldots$$

les ordres de ramification de ces différents points de ramification; si l'on désigne par

$$\mathfrak{P}_1,\ \mathfrak{P}_2,\ \mathfrak{P}_3,\ \ldots\ldots$$

les diviseurs premiers des points de ramification et par

$$\mathfrak{a}_1,\ \mathfrak{a}_2,\ \mathfrak{a}_3,\ \ldots\ldots$$

les idéaux premiers correspondants, on dira que le symbole

$$\mathfrak{Z} = \mathfrak{P}_1^{a_1-1}\mathfrak{P}_2^{a_2-1}\mathfrak{P}_3^{a_3-1}\ldots\ldots$$

est le *diviseur de ramification*[144]) du corps et que l'idéal correspondant

$$\mathfrak{a}_1^{a_1-1}\mathfrak{a}_2^{a_2-1}\mathfrak{a}_3^{a_3-1}\ldots\ldots$$

est l'*idéal de ramification* ou encore la *différente* du corps. *Le discriminant D du corps est donc la norme de la différente.**

*Pour tout idéal J, autre que l'idéal principal (1), le carré du discriminant Δ des ξ qui constituent le système fondamental de cet idéal,

144) *K. Hensel* et *G. Landsberg*, Alg. Funkt.[132]), p. 219. Il faut observer que s'il existe aussi des points de ramifications pour lesquels $x = \pm\infty$, on devra en tenir compte dans la formation du diviseur de ramification.*

est d'après (2) le produit de D par une quantité qui peut être écrite immédiatement connaissant le diviseur.*

*Le système fondamental $(\xi_1, \xi_2, \ldots, \xi_n)$ de l'idéal J étant ainsi calculé, il s'agit de passer de l'idéal au *diviseur* dont on l'a déduit, c'est-à-dire de tenir compte des conditions à l'infini en multipliant les fonctions obtenues par des puissances convenables des diviseurs correspondant aux points à l'infini, diviseurs qui jouent le rôle d'*unités* dans la théorie constituée jusqu'ici. C'est à quoi l'on parvient aisément en rendant cette base *normale* pour $x = \infty$.

Voici comment on distingue les bases en *normales* et *non normales*[145]).

Soit $(\xi_1, \xi_2, \ldots, \xi_n)$ une base donnée du corps. Développons la fonction ξ_i et ses conjuguées suivant les puissances croissantes de $\frac{1}{x}$; soit alors r_i le plus petit des n exposants (nombres entiers ou fractionnaires) des premiers termes de ces n développements. Ceci fait, pour $i = 1, 2, \ldots, n$, développons aussi, suivant les puissances croissantes de $\frac{1}{x}$, le déterminant Δ correspondant à la base donnée; l'exposant r de $\frac{1}{x}$ dans le premier terme de ce développement sera alors nécessairement égal ou supérieur à la somme $r_1 + r_2 + \cdots + r_n$.

On dit que *la base* $(\xi_1, \xi_2, \ldots, \xi_n)$ *est normale pour* $x = \infty$ *quand*

$$r = r_1 + r_2 + \cdots + r_n$$

et qu'elle est *non normale* pour $x = \infty$ quand

$$r > r_1 + r_2 + \cdots + r_n.$$

La même définition convient pour un point fini quelconque α, à condition de remplacer partout $\frac{1}{x}$ par $x - \alpha$.

Quand le système fondamental de l'idéal J forme une base non normale pour $x = \infty$, on peut toujours le remplacer par un système fondamental $(\xi_1, \xi_2, \ldots, \xi_n)$ formant une base normale pour $x = \infty$. Alors $r_1, r_2, \ldots, r_n$ sont nécessairement entiers. Convenons de ranger ces entiers dans un ordre tel qu'on ait

$$r_1 \geqq r_2 \geqq \cdots \geqq r_n,$$

et soit alors s le plus grand des indices pour lesquels r_s ne soit pas négatif. On démontre[146]) que les fonctions du corps K qui peuvent être mises sous la forme

$$\xi = u_1\xi_1 + u_2\xi_2 + \cdots + u_s\xi_s,$$

145) *K. Hensel* et *G. Landsberg*, Alg. Funkt.[132]), p. 167.*

146) *Id. p. 223.*

où u_i désigne une fonction rationnelle entière de x de degré $\leqq r_i$, et celles-la seulement, sont *partout divisibles* par D.*

37. Combinaisons linéaires de diviseurs d'une même classe. *Il convient d'affecter d'un facteur numérique chacun des diviseurs envisagés; quoique ces facteurs numériques n'interviennent aucunement dans les recherches sur la divisibilité des fonctions par ces diviseurs ou dans la distribution de ces diviseurs en classes, on les utilisera en effet plus tard dans d'autres recherches.

Ces facteurs numériques permettent, en particulier, de s'arranger de façon qu'à chaque diviseur de la classe principale ne correspond qu'*une seule* fonction, et non une infinité. Si dans le corps K nous fixons arbitrairement un diviseur premier $\mathfrak{P}_0$, si d'autre part

$$\mathfrak{P}_1^{\sigma_1}\mathfrak{P}_2^{\sigma_2}\dots\mathfrak{P}_h^{\sigma_h}$$

est *le* diviseur d'une fonction $\frac{P(x,y)}{Q(x,y)}$ du corps K, et si enfin e_α est le coefficient du premier terme du développement en série de $\frac{P(x,y)}{Q(x,y)}$ suivant les puissances de $x-\alpha$, correspondant au diviseur $\mathfrak{P}_0$, nous conviendrons de faire correspondre à la fonction $\frac{P(x,y)}{Q(x,y)}$ le diviseur

$$e_\alpha\mathfrak{P}_1^{\sigma_1}\mathfrak{P}_2^{\sigma_2}\dots\mathfrak{P}_h^{\sigma_h},$$

et nous exprimerons cette correspondance en écrivant

$$\frac{P(x,y)}{Q(x,y)}=e_\alpha\mathfrak{P}_1^{\sigma_1}\mathfrak{P}_2^{\sigma_2}\dots\mathfrak{P}_h^{\sigma_h}.$$

L'introduction des facteurs numériques e_α ainsi définis permet la constitution d'une notion nouvelle, celle de la *combinaison linéaire*[147]) de deux diviseurs D_1 et D_2 pourvu que ceux-ci appartiennent à la même classe. Soit, en effet, E un diviseur appartenant à la classe réciproque; alors ED_1 et ED_2 seront deux diviseurs principaux auxquels correspondent deux fonctions φ_1, φ_2 déterminées. Le diviseur de toute fonction de la forme

$$c_1\varphi_1+c_2\varphi_2,$$

où c_1 et c_2 sont des constantes, contient évidemment E en facteur. Le facteur restant sera celui que l'on envisagera comme étant de la forme

$$c_1D_1+c_2D_2.$$

On peut de même former des combinaisons linéaires de plus de deux diviseurs de la même classe.

Dans une classe déterminée, le nombre des diviseurs linéairement

147) **K. Hensel* et *G. Landsberg*, Alg. Funkt.[132]), p. 253/8.*

indépendants (c'est-à-dire tels qu'on ne puisse pas avec ces diviseurs former de combinaison linéaire qui soit identiquement nulle) est *fini*; on dit que ce nombre fini est la *dimension* de la classe.

Plus généralement, on peut se proposer de trouver tous les diviseurs linéairement indépendants qui appartiennent à une classe donnée $(\mathfrak{A})$ et sont en même temps multiples d'un diviseur donné B d'une classe $(\mathfrak{B})$. Ce problème se réduit au problème du n° **36** lorsque $(\mathfrak{A})$ est la classe principale. Le cas général se ramène à celui-là en multipliant par un diviseur de la classe opposée à $(\mathfrak{A})$. Le nombre des diviseurs cherchés est égal à la dimension de la classe $\frac{(\mathfrak{A})}{(\mathfrak{B})}$ et, par conséquent, ne change pas quand on remplace le diviseur B de la classe $(\mathfrak{B})$ par un autre diviseur de la même classe.*

38. ***Transformations birationnelles. Invariants.** Dans le corps K attaché à la courbe algébrique irréductible $f(x,y)=0$, on peut choisir d'une infinité de manières deux fonctions rationnelles de x et y

$$(1)\qquad \xi=r_1(x,y),\quad \eta=r_2(x,y)$$

de façon que non seulement à chaque point de la courbe corresponde un couple déterminé de valeurs ξ,η, mais qu'inversement les coordonnées x, y de chacun des points de la courbe s'expriment rationnellement au moyen de ξ,η, en sorte que

$$(2)\qquad x=R_1(\xi,\eta),\quad y=R_2(\xi,\eta).$$

L'équation irréductible

$$F(\xi,\eta)=0$$

qui lie ξ et η permet d'envisager η comme une fonction algébrique de ξ.

On dit que les équations (1) et (2) représentent une transformation birationnelle de la courbe $f(x,y)=0$ en la courbe $F(\xi,\eta)=0$. On dit aussi que les équations (1) représentent une transformation du corps K en lui-même; cela revient à ne pas envisager comme distincts les corps attachés aux deux courbes $f(x,y)=0$ et $F(\xi,\eta)=0$. Quand il importe de distinguer ces deux corps l'un de l'autre, nous représenterons par $K(x,y)$ le corps attaché à la première courbe et par $K(\xi,\eta)$ le corps attaché à la seconde courbe.

A un point (x,y) de la courbe $f(x,y)=0$ et au point correspondant (ξ,η) de la courbe $F(\xi,\eta)=0$ nous adjoignons le *même* diviseur $\mathfrak{P}$ du corps K.

Soit

$$\xi=r_1(x,y)$$

une fonction rationnelle quelconque du corps K; on peut toujours déterminer deux constantes a et b telles que les deux relations

(3) $$\xi = r_1(x, y), \quad \eta = a r_1(x, y) + b y$$

représentent une transformation birationnelle de K. Si

$$\eta = r_2(x, y)$$

est une *fonction primitive* du corps K, en d'autres termes si la fonction η et ses conjuguées sont toutes distinctes, les deux relations

(4) $$\xi = x, \quad \eta = r_2(x, y)$$

représentent aussi une transformation birationnelle de K. Toute transformation birationnelle de K peut être représentée par une *combinaison* d'une transformation du type (3) et d'une transformation du type (4).

Plusieurs caractères importants d'une courbe algébrique restent les mêmes quand on remplace cette courbe par une de ses transformées à l'aide de relations du type (4); on dit que ces caractères sont *invariants* pour ces transformations (4).

D'après la définition que l'on a donnée des fonctions primitives, il en est ainsi pour le degré n de l'équation $f(x, y) = 0$ en y. C'est aussi le cas pour le diviseur $\mathfrak{n}_x$ qui figure au dénominateur de l'expression de x (envisagé comme quantité de K) par le quotient

$$x = \frac{\mathfrak{z}_x}{\mathfrak{n}_x}$$

de deux diviseurs entiers $\mathfrak{n}_x$, $\mathfrak{z}_x$ premiers entre eux. Cet invariant $\mathfrak{n}_x$ est le produit des diviseurs premiers de K correspondant à ceux des points de la courbe $f(x, y) = 0$ pour lesquels $x = \infty$ (en n'oubliant pas de compter a fois les diviseurs premiers de ramification d'ordre $a - 1$). D'après le n° **35** on peut identifier à $\mathfrak{p}_\infty$ ce diviseur $\mathfrak{n}_x$.

Le plus important des invariants de cette espèce est le *diviseur de ramification* (n° **36**)

$$\mathfrak{Z}_x = \prod \mathfrak{P}^{a-1},$$

dans lequel figure en facteur chaque diviseur premier de ramification $\mathfrak{P}$ autant de fois que l'indique son ordre $a - 1$ de ramification.

Un cas particulier très simple de transformation birationnelle est celui des *transformations linéaires* de x, y représenté par les relations

(5) $$\xi = \frac{ax + b}{cx + d}, \quad \eta = \frac{\alpha y + \beta}{\gamma y + \delta},$$

où $a, b, c, d, \alpha, \beta, \gamma, \delta$ sont des constantes données. A ces transformations correspond un invariant

$$\mathrm{D}$$

que l'on obtient aisément en formant la dérivée $\frac{\partial f(x, y)}{\partial y}$ et en y remplaçant y en fonction de x; la fonction de x ainsi définie peut se

mettre sous la forme

$$\frac{\mathfrak{Z}_x \mathrm{D}}{\mathfrak{n}_x^m \mathfrak{n}_y^{n-2}},$$

où m est le degré de $f(x, y)$ en x et n le degré de $f(x, y)$ en y, où $\mathfrak{Z}_x$, $\mathfrak{n}_x$ viennent d'être définis et où $\mathfrak{n}_y$ est le produit des diviseurs de K correspondant à ceux des points de la courbe $f(x, y) = 0$ pour lesquels $y = \infty$. Le facteur D est un diviseur *entier*[148]); c'est l'invariant cherché des transformations linéaires envisagées. On a donné à cet invariant D le nom de *diviseur des points doubles* de la courbe $f(x, y) = 0$.

Les fonctions du corps $\mathrm{K}(x, y)$ qui, pour x fini, sont divisibles par D forment un idéal entier auquel on a donné le nom d'*idéal des points doubles* de $f(x, y) = 0$. La norme de cet idéal est le carré d'une fonction rationnelle entière X de x.

Si Δ est le discriminant du corps $\mathrm{K}(x, y)$, le discriminant par rapport à y de l'équation $f(x, y) = 0$ est égal à

$$X^2 \Delta.$$

On dit que X^2 est le diviseur non-essentiel du discriminant par rapport à y de l'équation $f(x, y) = 0$.

On obtient aisément des invariants pour *toutes* les transformations birationnelles de K en observant que pour chaque transformation birationnelle (1) on a

(6) $$\frac{d\xi}{dx} = \frac{\mathfrak{Z}_\xi}{\mathfrak{n}_\xi^2} : \frac{\mathfrak{Z}_x}{\mathfrak{n}_x^2},$$

si l'on convient de désigner par $\mathfrak{n}_\xi$ et $\mathfrak{Z}_\xi$ les expressions qui dans $\mathrm{K}(\xi, \eta)$ jouent le même rôle que $\mathfrak{n}_x$ et $\mathfrak{Z}_x$ dans $\mathrm{K}(x, y)$. Cette relation (6), dans laquelle $\frac{d\xi}{dx}$ doit être envisagée comme une fonction algébrique de x appartenant au corps K, met en évidence que les diviseurs

$$\frac{\mathfrak{Z}_\xi}{\mathfrak{n}_\xi^2} \quad \text{et} \quad \frac{\mathfrak{Z}_x}{\mathfrak{n}_x^2}$$

font partie de la même classe. On voit donc que la classe dont fait partie $\frac{\mathfrak{Z}_x}{\mathfrak{n}_x^2}$ ne sera pas altérée si l'on remplace la courbe $f(x, y) = 0$ par une autre courbe déduite de la première par transformation birationnelle. Cette classe à laquelle on a donné le nom de „classe différentielle“ est donc un *invariant* de toutes ces transformations birationnelles. L'ordre de la classe différentielle est un nombre pair $\geqq -2$; si l'on représente cet ordre par

$$2(p - 1),$$

148) **K. Hensel* et *G. Landsberg*, Alg. Funkt.[132]), p. 383.*

p est donc un nombre naturel. On dit que p est le *genre*[149]) de K ou de la courbe $f(x, y) = 0$.*

39. Applications aux intégrales abéliennes. *Si, $U(x, y)$ désignant une fonction rationnelle quelconque attachée à la courbe $f(x, y) = 0$, on représente par

$$V(\xi, \eta)\, d\xi$$

la transformée, par une transformation birationnelle quelconque, de la différentielle (abélienne)

$$U(x, y)\, dx,$$

on a, en appliquant l'équation (6) du n° **38**, la relation

$$D\frac{\mathfrak{Z}_x}{\mathfrak{n}_x^2} = D_1 \frac{\mathfrak{Z}_\xi}{\mathfrak{n}_\xi^2},$$

dans laquelle D représente le diviseur de $U(x, y)$ et D_1 celui de $V(\xi, \eta)$. On appelle

$$D\frac{\mathfrak{Z}_x}{\mathfrak{n}_x^2}$$

le *diviseur différentiel* de $U(x, y)\, dx$.

Tous les diviseurs de cette espèce appartiennent à une même classe, la *classe différentielle* envisagée au n° **38**. Inversement, à chaque diviseur de cette classe correspond une différentielle abélienne, déterminée à un facteur constant près. On appelle *ordre* de $U(x, y)\, dx$ relativement à $\mathfrak{P}$, l'exposant avec lequel le diviseur premier $\mathfrak{P}$ figure dans l'expression $D\frac{\mathfrak{Z}_x}{\mathfrak{n}_x^2}$.

La recherche des intégrales abéliennes des différentes espèces n'est qu'un cas particulier du problème de la fin du n° **37**.*

Les différentielles abéliennes de première espèce correspondent aux diviseurs entiers de la classe différentielle. Leur recherche s'effectue par l'application pure et simple de la méthode générale et, en particulier, on obtient ainsi très simplement le nombre des différentielles abéliennes linéairement indépendantes; il est égal au genre p de $f(x, y) = 0$[150]).

En cherchant, dans la classe différentielle, non plus les diviseurs entiers, mais ceux qui sont divisibles par $\mathfrak{P}^{-2}$ ou par $(\mathfrak{P} \cdot \mathfrak{P}')^{-1}$ (où

149) *Cet invariant p a d'abord été envisagé par *B. Riemann* [J. reine angew. Math. 54 (1857), p. 132/3; Werke[26]), (2e éd.) p. 118/9; trad. *L. Laugel*, p. 129/30.*

150) *K. Hensel*, J. reine angew. Math. 117 (1897), p. 29; *K. Hensel* et *G. Landsberg*, Alg. Funkt.[132]), p. 298 (9ième leçon, § 4).

$\mathfrak{P}, \mathfrak{P}'$ sont des diviseurs premiers), on aurait les intégrales de deuxième ou de troisième espèce.

On arrive au théorème de Riemann-Roch en cherchant, dans cette même classe différentielle, les diviseurs multiples d'un diviseur donné quelconque[151]).

La réduction des singularités[152]), celle du degré de la courbe par transformation birationnelle, peuvent également se déduire de considérations semblables.

40. Les formes homogènes algébriques. On peut modifier la théorie précédente en introduisant une variable d'homogénéité de façon que les nouvelles variables envisagées soient toujours nécessairement *finies*. Il suffit à cet effet d'envisager x comme le quotient $\frac{x_1}{x_2}$ de deux nouvelles variables x_1 et x_2 auxquelles on impose la double condition de rester toutes deux finies et de n'être jamais nulles simultanément.

*A chaque fonction algébrique $\eta(x)$ du corps $\mathrm{K}(x, y)$ attaché à la courbe $f(x, y) = 0$ correspond alors une infinité de *formes homogènes algébriques* attachées à la courbe $f(x, y) = 0$, ou à la surface de Riemann correspondante. On appelle ainsi les fonctions définies par la relation

$$\eta(x_1, x_2) = \eta\left(\frac{x_1}{x_2}\right) x_2^{\nu}, \tag{1}$$

où ν est un entier quelconque, positif, nul ou négatif.

Le nombre ν qui correspond à une forme homogène algébrique $\eta(x_1, x_2)$ déterminée est le *degré d'homogénéité* de cette forme.

A chaque fonction algébrique *entière* $\eta(x)$ du corps $\mathrm{K}(x, y)$ attaché à la courbe $f(x, y) = 0$ correspond, dès que ν est positif et suffisamment grand, des formes homogènes algébriques $\eta(x_1, x_2)$ qui, pour les valeurs envisagées de x_1 et x_2, ne deviennent jamais infinies. On donne à ces formes $\eta(x_1, x_2)$ le nom de *formes homogènes algébriques entières.*

Toute fonction algébrique entière ou fractionnaire de $x = \frac{x_1}{x_2}$ peut être mise sous la forme d'un quotient de deux formes homogènes algébriques entières de x_1 et x_2.

151) *G. Landsberg*, Math. Ann. 50 (1898), p. 333, 577; *K. Hensel* et *G. Landsberg*, Alg. Funkt.[132]), p. 301.

152) *L. Kronecker*, J. reine angew. Math. 91 (1881), p. 301; Werke 2, Leipzig 1897, p. 195. Voir *F. Klein*, Riemannsche Flächen 1 (cours autographié, Göttingue 1891/2); réimpr. 1, Göttingue 1906, p. 128/229 (sections 4 et 5). Voir aussi *K. Hensel* et *G. Landsberg*, Alg. Funkt.[132]), p. 397.

Les propriétés des formes algébriques entières ont été étudiées par *K. Hensel*[153]). Au théorème concernant l'existence d'un système fondamental pour les fonctions entières du corps $K(x, y)$ [n° **20**] correspond ici le théorème suivant:

Si l'équation $f(x, y) = 0$ d'une courbe algébrique est de degré n en y, il existe n formes homogènes algébriques *entières*

$$\eta_1, \eta_2, \ldots, \eta_n$$

attachées à cette courbe, telles que toute forme homogène algébrique entière attachée à la même courbe s'exprime sous la forme

$$u_1\eta_1 + u_2\eta_2 + \cdots + u_n\eta_n,$$

où $u_1, u_2, \ldots, u_n$ sont des fonctions rationnelles *entières* convenablement choisies de x_1 et x_2.*

41. Propriétés projectives. Diviseurs corésiduels. Classes généralisées. *Les diviseurs jouent également un rôle important dans l'étude des propriétés projectives de la courbe $f(x, y) = 0$ et des courbes obtenues en effectuant sur cette courbe des transformations birationnelles.

Choisissons, dans le corps K attaché à la courbe irréductible $f(x, y) = 0$, trois fonctions x_0, x_1, x_2 qui ne soient liées par aucune relation linéaire et homogène à coefficients constants et pour lesquelles les relations

$$\xi = \frac{x_1}{x_0}, \quad \eta = \frac{x_2}{x_0} \tag{1}$$

représentent une transformation birationnelle[154]).

L'équation $f(x, y) = 0$ se transforme ainsi en une équation $\varphi(\xi, \eta) = 0$. En multipliant φ par une puissance convenable de x_0, nous pouvons mettre l'équation transformée sous la forme

$$F(x_0, x_1, x_2) = 0,$$

où F est une fonction rationnelle entière homogène de x_0, x_1, x_2. On peut envisager x_0, x_1, x_2 comme des coordonnées ponctuelles projectives homogènes; l'équation $F = 0$ est alors l'équation de la courbe irréductible $\varphi = 0$, en coordonnées projectives homogènes.

On peut envisager cette équation $F = 0$ comme une relation entre des diviseurs du corps K. Soit, en effet, $\mathfrak{M}$ le p. g. c. d. des

153) J. reine angew. Math. 109 (1892), p. 1; trad. par *G. Brincard*, Acta math. 18 (1894), p. 247. Voir aussi *F. Klein*, Math. Ann. 36 (1890), p. 21; Vorles. über elliptische Modulfunktionen, publ. par *R. Fricke* 2, Leipzig 1892, p. 486.

154) **K. Hensel* et *G. Landsberg*, Alg. Funkt.[152]), p. 420.*

diviseurs de K correspondant à x_0, x_1, x_2; en posant

$$x_0 = \mathfrak{M}\mathfrak{A}_0, \quad x_1 = \mathfrak{M}\mathfrak{A}_1, \quad x_2 = \mathfrak{M}\mathfrak{A}_2,$$

$\mathfrak{A}_0, \mathfrak{A}_1, \mathfrak{A}_2$ seront premiers entre eux et appartiendront à une même classe $(\mathfrak{A})$ de dimension égale ou supérieure à 3. Si ν est le degré de F (en x_0, x_1, x_2), ν est aussi l'ordre de la classe $(\mathfrak{A})$; chaque terme de la fonction

$$F(\mathfrak{A}_0, \mathfrak{A}_1, \mathfrak{A}_2)$$

est un diviseur de la classe $(\mathfrak{A})^\nu$; l'équation

$$F(\mathfrak{A}_0, \mathfrak{A}_1, \mathfrak{A}_2) = 0$$

peut donc être envisagée comme fournissant une relation linéaire entre les diviseurs de la classe $(\mathfrak{A})^\nu$ dans le sens du n° **37**, relation qui devient une équation entre les quantités de K si l'on multiplie par $\mathfrak{M}^\nu$ ou par un diviseur équivalent à $\mathfrak{M}^\nu$.

A chaque diviseur premier $\mathfrak{P}$ du corps K correspond un point déterminé (ou d'une façon plus précise un élément déterminé) de $f(x, y) = 0$, donc aussi un point de $\varphi(\xi, \eta) = 0$ c'est-à-dire de $F(x_0, x_1, x_2) = 0$.

Pour obtenir les diviseurs qui correspondent aux points d'intersection de $F(x_0, x_1, x_2) = 0$ avec la droite

$$c_0x_0 + c_1x_1 + c_2x_2 = 0,$$

il suffit de décomposer

$$c_0\mathfrak{A}_0 + c_1\mathfrak{A}_1 + c_2\mathfrak{A}_2 \tag{3}$$

en ses diviseurs premiers.

La théorie de la courbe $F(x_0, x_1, x_2) = 0$ est donc intimement liée à celle du réseau de diviseurs que l'on obtient en envisageant dans l'expression (3) c_0, c_1, c_2 comme des paramètres variables. En particulier, la géométrie projective de la courbe $F = 0$ peut être envisagée comme une théorie de ce réseau de diviseurs; à une transformation projective de la courbe correspond le fait de former le réseau (3) non plus au moyen des trois diviseurs $\mathfrak{A}_0, \mathfrak{A}_1, \mathfrak{A}_2$ mais au moyen de trois autres diviseurs du même réseau.

Si l'on désigne par D le diviseur des points doubles [n° **38**] de l'équation $F(x_0, x_1, x_2) = 0$, c'est-à-dire de l'équation $F(1, \xi, \eta) = 0$, le quotient

$$\overline{\mathrm{D}} = \frac{\mathrm{D}}{\mathfrak{A}_0^{\nu-1}}$$

est un diviseur *entier*, et c'est un *invariant* dans toutes les transformations projectives possibles. On appelle souvent $\overline{\mathrm{D}}$ le *diviseur des points doubles* de $F(x_0, x_1, x_2) = 0$ au sens projectif.

Toute courbe $\Phi(x_0, x_1, x_2) = 0$ qui contient les points de

$F(x_0, x_1, x_2)$ correspondant aux diviseurs premiers de K, chacun avec un ordre de multiplicité au moins égal au nombre de fois que le diviseur premier correspondant figure dans $\overline{\mathrm{D}}$, est dite *courbe adjointe* à $F(x_0, x_1, x_2) = 0$ au sens projectif.

Envisageons le système de points qu'une courbe adjointe d'ordre μ a en commun avec la courbe $F(x_0, x_1, x_2) = 0$; après avoir mis à part les points singuliers qui correspondent au diviseur $\overline{\mathrm{D}}$, distribuons d'une façon quelconque les autres points du système envisagé en deux groupes; soient $\mathfrak{R}$ et $\mathfrak{S}$ les diviseurs correspondant à ces deux groupes: on démontre que

$$\mathfrak{G} = \overline{\mathrm{D}}\mathfrak{R}\mathfrak{S}$$

est un diviseur entier de la classe $(\mathfrak{A})^\mu$, divisible par $\overline{\mathrm{D}}$. On dit que $\mathfrak{R}$ et $\mathfrak{S}$ sont *restes* l'un de l'autre. A chaque diviseur $\mathfrak{R}$ on peut faire correspondre un diviseur $\mathfrak{S}$ tel que $\mathfrak{R}$ et $\mathfrak{S}$ soient restes l'un de l'autre, car il suffit de fixer μ suffisamment grand pour pouvoir trouver dans la classe $(\mathfrak{A})^\mu$ des diviseurs $\mathfrak{G}$ entiers et divisibles par $\overline{\mathrm{D}}\mathfrak{R}$, et alors $\frac{\mathfrak{G}}{\overline{\mathrm{D}}\mathfrak{R}} = \mathfrak{S}$ est un reste de $\mathfrak{R}$. On peut même trouver ainsi une infinité de restes $\mathfrak{S}$ de $\mathfrak{R}$, puisque l'ordre μ de la courbe rencontrant $F = 0$ peut être fixé aussi grand que l'on veut.

Deux diviseurs entiers $\mathfrak{R}$ et $\mathfrak{R}'$, et aussi les systèmes de points qui leur correspondent, sont dits *corésiduels* lorsqu'ils sont restes d'un même diviseur $\mathfrak{S}$. La condition nécessaire et suffisante pour qu'il en soit ainsi est que $\frac{\mathfrak{R}'}{\mathfrak{R}}$ appartienne à une classe qui soit une puissance de $(\mathfrak{A})$.

Si $\mathfrak{R}$ et $\mathfrak{R}'$ sont corésiduels à $\mathfrak{R}''$, $\mathfrak{R}$ et $\mathfrak{R}'$ sont aussi corésiduels l'un à l'autre. Tous les diviseurs entiers d'une même classe sont corésiduels.

Deux diviseurs du corps K peuvent être corésiduels ou non suivant le choix que l'on fait de la courbe $F(x_0, x_1, x_2) = 0$ ou, ce qui revient au même, des quantités x_0, x_1, x_2 de K figurant dans les équations (1).

Ce qu'on vient de dire sur les diviseurs corésiduels donne tout naturellement l'idée de grouper les classes de diviseurs en *classes généralisées.*

Convenons à cet effet de dire de deux classes de diviseurs $(\mathfrak{B})$ et $(\mathfrak{C})$ qu'elles sont *équivalentes relativement à une classe de diviseurs* $(\mathfrak{A})$ arbitrairement *fixée*, lorsque leur quotient est une puissance de $(\mathfrak{A})$ et réunissons toutes les classes équivalentes relativement à $(\mathfrak{A})$ en *une même classe généralisée.*

Au lieu d'une classe fondamentale en obtient une classe fondamentale généralisée en réunissant l'ensemble des puissances de $(\mathfrak{A})$.

On voit que la distribution en classes généralisées dépend entièrement du choix que l'on fait de la classe $(\mathfrak{A})$, en d'autres termes de celle des classes généralisées que l'on convient de prendre comme classe fondamentale généralisée. On observera d'ailleurs que le choix de la classe $(\mathfrak{A})$ n'est pas limité par les restrictions faites au cours de ce n° **41**, en sorte que la dimension de $(\mathfrak{A})$ par exemple n'est pas nécessairement égale ou supérieure à 3.*

42. *__Retour aux corps de nombres. Nombres entiers module p.__ Dans la théorie des fonctions, l'emploi des séries de puissances facilite singulièrement l'étude des corps de fonctions algébriques. *K. Hensel*[155]) s'est demandé s'il ne serait pas possible de former des séries à termes numériques rendant le même service dans l'étude des corps de nombres. Avant d'exposer les résultats auxquels il est parvenu nous donnerons quelques définitions et fixerons quelques notations dont nous aurons à faire usage.

Convenons tout d'abord de désigner toujours par p un nombre *premier* rationnel donné.

On dit qu'un nombre rationnel ou algébrique est *entier* (mod. p) lorsqu'il est racine d'une équation

$$a_0x^n + a_1x^{n-1} + \cdots + a_n = 0, \tag{1}$$

où $a_0, a_1, \ldots, a_n$ sont des nombres rationnels entiers et où a_0 n'est pas divisible par p.

Pour qu'un nombre rationnel ou algébrique x soit entier (mod. p) il faut et il suffit que l'équation à coefficients rationnels, de degré le plus petit possible, que vérifie x puisse être mise sous la forme (1) en multipliant tous ses coefficients par un même nombre rationnel.

Tout nombre rationnel entier ou algébrique entier est un nombre rationnel ou algébrique *entier* (mod. p) quel que soit p. Mais un nombre (rationnel ou algébrique) entier (mod. p) n'est pas nécessairement (rationnel ou algébrique) entier au sens ordinaire du mot.

Si un nombre u est rationnel entier (mod. p) ou algébrique entier (mod. p) et qu'il en soit de même de sa valeur réciproque $\frac{1}{u}$, on dit que u et $\frac{1}{u}$ sont des *unités* (mod. p).

155) *Math. Ann. 55 (1902), p. 301/36; J. reine angew. Math. 127 (1904), p. 51/84; 128 (1905), p. 1/32; 129 (1905), p. 68/85; Jahresb. deutsch. Math.-Ver. 14 (1905), p. 545/58; 16 (1907), p. 299/319, 388/93, 470/96. Exposé détaillé dans *K. Hensel*, Theorie der algebraischen Zahlen 1, Leipzig et Berlin 1908. Complément important dans le mémoire de *K. Hensel*, J. reine angew. Math. 136 (1909), p. 183/209. Le texte et les notes des n^os **42** à **50** sont entièrement dus à *J. Kürschák*.*

L'ensemble des nombres algébriques entiers (mod. p) forme un domaine holoïde [n° **15**]. L'ensemble des unités (mod. p) forme un module logarithmique [n° **19**].

Si α et β sont deux nombres algébriques tels que

$$\frac{\alpha - \beta}{p^\varrho}$$

soit un nombre algébrique entier (mod. p), on convient d'écrire

$$\alpha \equiv \beta \ (\mathrm{mod.}\ p^\varrho).$$

Ici ϱ peut être un nombre entier ordinaire (positif, nul ou négatif). En écrivant que l'on a, par exemple,

$$\frac{\sqrt{5}}{12} \equiv \frac{1}{12} \quad (\mathrm{mod.}\ 2^{-1})$$

on veut dire que le quotient

$$\frac{\frac{\sqrt{5}}{12} - \frac{1}{12}}{\frac{1}{2}},$$

c'est-à-dire le nombre $\frac{\sqrt{5}-1}{6}$ défini par l'équation

$$9x^2 + 3x - 1 = 0,$$

est un nombre entier (mod. 2). On voit par contre que $\frac{\sqrt{5}}{12}$ et $\frac{1}{12}$ ne sont pas congrus (mod. 2^0).

Il convient d'ailleurs d'observer que l'on n'est pas en droit de remplacer ici (mod. 2^0) par (mod. 1).

Ceci posé, soient $f(x)$ et $g(x)$ deux *fonctions rationnelles entières* de x ayant pour coefficients des nombres rationnels ou algébriques. Lorsque les coefficients du quotient

$$\frac{f(x) - g(x)}{p^\varrho}$$

sont des nombres entiers (mod. p), on convient d'écrire

$$f(x) \equiv g(x) \qquad (\mathrm{mod.}\ p^\varrho).^*$$

43. $_*$**Les nombres p-adiques.** Un nombre p-adique est un *symbole* représenté par une série

$$(1) \qquad a_\varrho p^\varrho + a_{\varrho+1} p^{\varrho+1} + a_{\varrho+2} p^{\varrho+2} + \cdots\cdots,$$

où ϱ est un nombre rationnel entier (positif, nul ou négatif) et où les coefficients $a_\varrho, a_{\varrho+1}, a_{\varrho+2}, \ldots\ldots$ sont soit des nombres rationnels entiers (mod. p), auquel cas on dit que le nombre p-adique est *rationnel*, soit des nombres algébriques entiers (mod. p) faisant partie d'un corps algébrique donné $(\mathfrak{R}, \xi)$, auquel cas on dit que le nombre p-adique est *algébrique*.

Les nombres

$$\begin{aligned} A_\varrho &= a_\varrho p^\varrho, \\ A_{\varrho+1} &= a_\varrho p^\varrho + a_{\varrho+1} p^{\varrho+1}, \\ A_{\varrho+2} &= a_\varrho p^\varrho + a_{\varrho+1} p^{\varrho+1} + a_{\varrho+2} p^{\varrho+2}, \\ &\cdots\cdots\cdots\cdots\cdots\cdots \end{aligned}$$

sont les *réduites* successives du nombre p-adique

$$a_\varrho p^\varrho + a_{\varrho+1} p^{\varrho+1} + \cdots + a_{\varrho+i} p^{\varrho+i} + \cdots\cdots;$$

A_k est la $k^{\text{ième}}$ réduite.

Ces réduites successives ne tendent pas nécessairement vers une limite représentée par un nombre réel ou imaginaire: les nombres p-adiques ne sont d'ailleurs en rien semblables aux nombres réels ou imaginaires qu'on envisage en Analyse; ce ne sont que des *symboles* que l'on soumet aux règles de calcul suivantes:

1°) Deux nombres p-adiques[156])

$$\begin{aligned} A &= a_\varrho p^\varrho + a_{\varrho+1} p^{\varrho+1} + \cdots + a_{\varrho+i} p^{\varrho+i} + \cdots\cdots, \\ B &= b_\varrho p^\varrho + b_{\varrho+1} p^{\varrho+1} + \cdots + b_{\varrho+i} p^{\varrho+i} + \cdots\cdots \end{aligned}$$

sont *égaux* lorsqu'on a, pour chaque indice i,

$$A_{\varrho+i} = B_{\varrho+i} \qquad (\mathrm{mod.}\ p^{\varrho+i+1}).$$

2°) On a

$$\begin{aligned} A + B &= (a_\varrho + b_\varrho) p^\varrho + (a_{\varrho+1} + b_{\varrho+1}) p^{\varrho+1} + \cdots + (a_{\varrho+i} + b_{\varrho+i}) p^{\varrho+i} + \cdots \\ AB &= a_\varrho b_\varrho p^{2\varrho} + (a_\varrho b_{\varrho+1} + a_{\varrho+1} b_\varrho) p^{2\varrho+1} + \cdots \\ &\quad + (a_\varrho b_{\varrho+i} + a_{\varrho+1} b_{\varrho+i-1} + \cdots + a_{\varrho+i} b_\varrho) p^{2\varrho+i} + \cdots\cdots \end{aligned}$$

Nous dirons souvent que la série (1) est une *série* p-adique. Cette façon de parler est surtout commode dans les recherches où les symboles p-adiques sont envisagés comme représentant des séries numériques ordinaires [cf. n° **49**].

Parmi les séries du type (1) les plus simples sont celles où tous

156) $_*$Si les exposants de p dans le premier terme de chacune des deux séries qui définissent A et B ne sont pas égaux, il suffit, pour appliquer les formules du texte, de supposer que un ou plusieurs des premiers coefficients de l'une des deux séries sont nuls. Rien n'empêche d'ailleurs de supposer que les coefficients de l'une des deux séries fassent partie d'un corps $(\mathfrak{R}, \xi_1)$ et que les coefficients de l'autre série fassent partie d'un corps $(\mathfrak{R}, \xi_2)$ distinct du précédent. Dans ce cas les coefficients de la somme $A + B$ et ceux du produit AB font partie du corps

$$(\mathfrak{R}, \xi_1, \xi_2)$$

obtenu en adjoignant à $\mathfrak{R}$, à la fois ξ_1 et ξ_2.*

les termes

$$a_i p^i \qquad (i = \varrho + 1,\ \varrho + 2,\ \varrho + 3,\ \ldots\ldots)$$

sont nuls et où $a_\varrho p^\varrho$ est un nombre rationnel ou algébrique donné. Lorsque nous envisagerons un nombre rationnel ou algébrique donné α comme un nombre p-adique il sera entendu que nous entendrons par là une série A dont tous les termes, sauf un

$$\alpha = a_\varrho p^\varrho,$$

sont nuls, ou tout au moins une série[157]) p-adique B qui soit égale à la série A au sens fixé par la définition (1°).

On dit qu'un nombre p-adique est *entier* lorsque toutes ses réduites sont entières (mod. p). Tout nombre p-adique qui n'est pas entier est dit *fractionnaire.*

A tout nombre *rationnel* p-adique A correspond une et une seule série p-adique α qui soit égale à A au sens de la définition (1°) et dans laquelle chacun des coefficients est l'un ou l'autre des nombres

$$0,\ 1,\ 2,\ \ldots,\ p-1.$$

On dit de cette série α qu'elle est la *forme réduite* de A. Si dans α la plus petite puissance de p ayant pour coefficient un nombre a_ϱ différent de zéro est p^ϱ on dit que le nombre p-adique rationnel A est d'ordre ϱ[158]).

Quand l'ordre de A est positif ou nul, A est entier; quand l'ordre de A est négatif, A est fractionnaire.

On comprend ici sous le nom d'*unités* tous les nombres p-adiques rationnels d'ordre *nul.*

L'ensemble des nombres p-adiques rationnels forme un domaine orthoïde [n° **9**]; nous représenterons ce domaine par le symbole

$$\mathrm{K}(p).^*$$

44. $_*$**Fonctions rationnelles entières à coefficients p-adiques.** Soit $F(x)$ une fonction rationnelle entière à coefficients p-adiques. Si l'on remplace chacun des coefficients par sa $k^{\text{ième}}$ réduite, on obtient une fonction que nous désignerons par $F^{(k)}(x)$ et à laquelle on donne le nom de $k^{\text{ième}}$ *réduite de* $F(x)$.

Pour que deux fonctions rationnelles entières $F(x)$ et $\Phi(x)$ aient des coefficients p-adiques égaux, il faut et il suffit que pour chaque

157) $_*$Cette série envisagée comme numérique n'est pas nécessairement convergente et, quand elle est convergente, elle peut fort bien avoir une somme différente du nombre rationnel ou algébrique envisagé α [cf. n° **49**].*

158) $_*$*K. Hensel,* Alg. Zahlen[155]), p. 21.*

valeur de k on ait

$$F^{(k)}(x) \equiv \Phi^{(k)}(x) \qquad (\text{mod. } p^{k+1}).$$

Quand il en est ainsi on écrit

$$F(x) = \Phi(x) \qquad (p).$$

Le symbole (p) indique ici que les coefficients des deux fonctions sont des nombres p-adiques et que si ce sont des nombres ordinaires ils doivent être envisagés comme des nombres p-adiques suivant les règles de calcul données au n° **43**.

Bornons-nous tout d'abord au cas où les coefficients des fonctions envisagées sont des nombres p-adiques *rationnels.* Comme le domaine $\mathrm{K}(p)$ est orthoïde, les notions de *diviseur*, d'*irréductibilité*, de *plus grand commun diviseur*, de *résultant* et de *discriminant* s'étendent sans ambiguïté aux fonctions rationnelles entières de x à coefficients faisant partie du domaine orthoïde $\mathrm{K}(p)$.

Le théorème d'après lequel une fonction ne peut être décomposée en facteurs irréductibles que d'une seule façon s'applique aussi, à condition bien entendu de ne pas envisager comme distincts deux diviseurs d'une fonction qui ne diffèrent que par un facteur constant.

On dit qu'une fonction rationnelle entière $F(x)$, à coefficients p-adiques rationnels, est *primitive* quand les coefficients de cette fonction sont des nombres p-adiques rationnels *entiers* et que l'un, au moins, de ces coefficients est une *unité* du domaine orthoïde $\mathrm{K}(p)$.

Quand dans une fonction primitive $F(x)$ le coefficient de la puissance la plus élevée de x est égal à 1 ou à une puissance de p, on dit que cette fonction primitive $F(x)$ est une fonction *primaire*[159]).

A chaque fonction rationnelle $F(x)$ dont les coefficients sont des nombres p-adiques rationnels correspond une et une seule fonction primaire dont elle ne diffère que par un facteur constant. Dans toute recherche concernant la divisibilité nous remplacerons toujours $F(x)$ par la fonction primaire correspondante.

Ceci posé, la théorie de la divisibilité des fonctions rationnelles entières $F(x)$ à coefficients p-adiques rationnels est entièrement élucidée par le théorème que voici[160]):

Si δ est l'ordre du discriminant de $F(x)$ dans le corps $\mathrm{K}(p)$, la condition nécessaire et suffisante pour que la fonction primaire $F(x)$ soit réductible est que la $\delta^{\text{ième}}$ réduite $F^{(\delta)}(x)$ de $F(x)$ se décompose en deux facteurs au moins (mod. $p^{\delta+1}$). A chaque décomposition

$$F^{(\delta)}(x) \equiv f_1(x)\,\varphi_1(x) \qquad (\text{mod. } p^{\delta+1})$$

159) $_*$*K. Hensel,* Alg. Zahlen[155]), p. 64.*

160) $_*$Id. p. 68.*

correspond une décomposition de $F(x)$

$$F(x) = f(x)\,\varphi(x) \qquad (p)$$

telle que $f_1(x)$ soit une réduite de $f(x)$ et $\varphi_1(x)$ une réduite de $\varphi(x)$.*

45. *Théorème fondamental de l'algèbre pour les nombres p-adiques. Supposons qu'un nombre p-adique α vérifie une équation algébrique

$$f(x) = 0 \qquad (p),$$

où $f(x)$ est un polynome de degré n en x dont les coefficients appartiennent au domaine orthoïde $\mathrm{K}(p)$ et qui soit irréductible dans ce domaine.

Les fonctions rationnelles *entières* de α, à coefficients faisant partie de $\mathrm{K}(p)$, forment un domaine orthoïde. On nomme ce domaine un *corps algébrique p-adique de degré n*; nous le désignerons par

$$\mathrm{K}(p, \alpha).$$

Il comprend bien entendu aussi les fonctions rationnelles fractionnaires de α à coefficients faisant partie de $\mathrm{K}(p)$.

Le symbole α peut aussi représenter un nombre algébrique ordinaire vérifiant une équation algébrique

$$f(x) = 0$$

irréductible non seulement dans le domaine $\mathfrak{R}$ mais aussi[161]) dans le domaine $\mathrm{K}(p)$ quand les coefficients numériques de $f(x)$ sont envisagés comme des nombres p-adiques suivant les règles de calcul indiquées au n° **43**.

A chaque équation algébrique

$$F(x) = 0 \qquad (p)$$

à coefficients faisant partie d'un domaine $\mathrm{K}(p)$ on peut, par un choix convenable de α, faire correspondre un corps p-adique $\mathrm{K}(p, \alpha)$ formant un domaine orthoïde dans lequel $F(x) = 0$ admet au moins une racine. On peut même, si l'on veut, choisir toujours α parmi les nombres algébriques ordinaires.

Nous n'examinerons ici que le cas où $F(x)$ est irréductible dans le domaine $\mathrm{K}(p)$ et peut être mis sous la forme

$$F(x) = x^n + A_1 x^{n-1} + \cdots + A^n \qquad (p),$$

dans laquelle $A_1, A_2, \ldots, A_n$ représentent des nombres p-adiques

161) *Si l'équation $f(x) = 0$ à laquelle satisfait α est réductible dans le corps $\mathrm{K}(p)$, les fonctions rationnelles entières de α à coefficients faisant partie de $\mathrm{K}(p)$ forment un domaine hyperorthoïde (n° 9) [cf. *K. Hensel*, J. reine angew. Math. 136 (1909), p. 188].*

rationnels entiers. On peut alors toujours[162]) prendre pour α un nombre algébrique ordinaire, racine de l'équation

$$F^{(k)}(x) = 0 \qquad (p),$$

où $F^{(k)}(x)$ est une réduite de $F(x)$ telle que k soit plus grand que l'ordre δ du discriminant de $F(x)$. Le corps

$$\mathrm{K}(p, \alpha)$$

est alors de degré n, et le degré de tout autre corps

$$\mathrm{K}(p, \alpha'),$$

dans lequel l'équation

$$F(x) = 0 \qquad (p)$$

admet au moins une racine α', est égal ou supérieur à n.

K. Hensel[163]) désigne chacun des corps p-adiques algébriques dans lesquels se trouve contenue au moins une racine de l'équation $F(x) = 0$, irréductible en $\mathrm{K}(p)$, sous le nom de *corps de résolubilité* de cette équation $F(x) = 0$.

Si $\mathrm{K}(p, \alpha)$ est un corps de résolubilité de $F(x) = 0$, chaque corps

$$\mathrm{K}(p, \overline{\alpha}),$$

égal à $\mathrm{K}(p, \alpha)$ *au sens abstrait du mot* (n° **9**) de façon que dans $\mathrm{K}(p, \alpha)$ et $\mathrm{K}(p, \overline{\alpha})$ chaque nombre p-adique rationnel se corresponde à lui-même, est aussi un corps de résolubilité de $F(x) = 0$. Inversement tous les corps de résolubilité de $F(x) = 0$ de degrés les plus petits possibles sont égaux au sens abstrait du mot[164]).

On peut aller plus loin encore et montrer que à chaque équation algébrique $F(x) = 0$ à coefficients faisant partie de $\mathrm{K}(p)$, correspond [que $F(x)$ soit d'ailleurs irréductible ou réductible en $\mathrm{K}(p)$] un nombre algébrique ordinaire γ défini par une équation algébrique irréductible en $\mathrm{K}(p)$ et tel que $F(x)$ se décompose en facteurs du premier degré en x dans le domaine $\mathrm{K}(p, \gamma)$. Si ce corps $\mathrm{K}(p, \gamma)$ est choisi de façon que son degré soit aussi petit que possible on l'appelle un *corps de décomposition* de l'équation[165])

$$F(x) = 0 \qquad (p).$$

Si cette équation a plusieurs corps de décomposition, ces corps de décomposition sont tous égaux au sens abstrait du mot.

162) **K. Hensel*, Alg. Zahlen[155]), p. 160.*

163) *J. reine angew. Math. 136 (1909), p. 183.*

164) *Id. p. 190. Au lieu de „égal au sens abstrait", *K. Hensel* dit ici *isomorphe* ou *équivalent.**

165) *Id p. 199.*

Si le discriminant de $F(x)$ est différent de zéro, le nombre de racines de l'équation

$$F(x) = 0 \qquad (p),$$

dans le corps de décomposition

$$\mathrm{K}(p, \gamma),$$

est égal à n. Chacune de ces racines correspond à l'un des facteurs linéaires de $F(x)$. Et il en est de même si l'on remplace le corps de décomposition $\mathrm{K}(p, \gamma)$ par un corps (domaine orthoïde) quelconque de nombres p-adiques contenant $\mathrm{K}(p, \gamma)$ comme diviseur.*

46. ***Le nombre premier π du corps $\mathrm{K}(p, \alpha)$.** Soit

$$f(x) = 0 \qquad (p) \tag{1}$$

une équation algébrique de degré λ ayant pour coefficients des quantités du domaine orthoïde $\mathrm{K}(p)$. Supposons que cette équation soit irréductible dans $\mathrm{K}(p)$ et désignons par $\mathrm{K}(p, \gamma)$ un corps (domaine orthoïde) de nombres p-adiques algébriques dans lequel $f(x)$ se décompose en facteurs du premier degré en x. Désignons par

$$\alpha, \alpha', \ldots, \alpha^{(\lambda-1)}$$

les λ racines de l'équation (1) dans le corps $\mathrm{K}(p, \gamma)$.

Les fonctions rationnelles de α à coefficients faisant partie de $\mathrm{K}(p)$ forment un corps de degré λ que nous désignerons par $\mathrm{K}(p, \alpha)$.

On dit que les λ corps

$$\mathrm{K}(p, \alpha), \quad \mathrm{K}(p, \alpha'), \quad \ldots, \quad \mathrm{K}(p, \alpha^{(\lambda-1)})$$

sont des *corps conjugués.*

Si $\beta = \psi(\alpha)$ est une quantité quelconque du corps $\mathrm{K}(p, \alpha)$, en d'autres termes si $\psi(\alpha)$ est une fonction rationnelle quelconque de α ayant pour coefficients des quantités du domaine $\mathrm{K}(p)$, on dit que

$$\beta = \psi(\alpha), \quad \beta' = \psi(\alpha'), \quad \ldots, \quad \beta^{(\lambda-1)} = \psi(\alpha^{(\lambda-1)})$$

sont des *quantités conjuguées.* Le produit

$$\beta\beta' \ldots \beta^{(\lambda-1)}$$

est un nombre rationnel p-adique qu'on appelle *la norme* de β et qu'on désigne par

$$N(\beta).$$

Pour qu'un nombre β du corps $\mathrm{K}(p, \alpha)$ soit *entier* il faut et il suffit que $N(\beta)$ soit un nombre p-adique rationnel entier.

Si $N(\beta)$ est une unité, β et $\frac{1}{\beta}$ sont tous deux des entiers du corps $\mathrm{K}(p, \alpha)$, et l'on convient de dire que β est une *unité de ce corps.*

Quand β_1 et β_2 sont deux nombres (entiers ou fractionnaires) du corps $\mathrm{K}(p, \alpha)$ tels que $\frac{\beta_1}{\beta_2}$ soit *entier,* on dit que β_1 est *divisible* par β_2.

On dit que deux nombres β_1 et β_2 sont *équivalents* lorsque chacun d'eux est divisible par l'autre[166]).

Pour que deux nombres soient équivalents il faut et il suffit que $\frac{\beta_1}{\beta_2}$ soit une unité.

Parmi tous les nombres entiers du corps $\mathrm{K}(p, \alpha)$ le nombre p mérite une mention particulière. Ce nombre p n'a pas toujours le caractère d'un nombre premier dans le corps $\mathrm{K}(p, \alpha)$, car quand il existe, dans ce corps, un nombre β tel que

$$N(\beta) = p^c \cdot u,$$

où $0 < c < n$ et où u est une unité du corps, on a

$$p = \beta\bar{\beta},$$

où β et $\bar{\beta} = \frac{p}{\beta}$ sont deux nombres entiers du corps $\mathrm{K}(p, \alpha)$ sans être ni l'un ni l'autre une unité de ce corps. Mais il y a dans *chaque* corps $\mathrm{K}(p, \alpha)$ un nombre π ayant le caractère d'un nombre premier: si, dans $\mathrm{K}(p, \alpha)$ on détermine π de façon que le nombre

$$N(\pi) = p^f \cdot u$$

ait un ordre *positif* aussi petit que possible par rapport à p, on démontre en effet que:

1°) tout nombre entier du corps $\mathrm{K}(p, \alpha)$ qui divise π est équivalent soit à 1 soit à π;

2°) le produit de deux nombres entiers du corps $\mathrm{K}(p, \alpha)$ n'est divisible par π que si l'un, au moins, de ces deux nombres entiers est divisible par π.

Ces deux propriétés résultent immédiatement de ce que chaque nombre entier du corps $\mathrm{K}(p, \alpha)$, autre qu'une unité, est divisible par π[167]).

Seuls les nombres équivalents à π dans $\mathrm{K}(p, \alpha)$ jouissent d'ailleurs de ces propriétés (1°) et (2°) du nombre π.

Dans ce qui suit, nous désignerons par π un quelconque des nombres équivalents jouissant de ces propriétés et nous conviendrons de dire que π est *le nombre premier* de $\mathrm{K}(p, \alpha)$.

L'exposant f de p, qui figure dans le second membre de l'équation

$$N(\pi) = p^f \cdot u,$$

est un diviseur de λ. Dans le cas particulier où l'on a

$$f = \lambda,$$

---

166) **K. Hensel*, Alg. Zahlen[155]), p. 136.*

167) *Id. p. 139.*

chacun des nombres qu'on peut choisir pour le nombre premier π du corps $\mathrm{K}(p, \alpha)$ est ou bien égal à p ou bien équivalent à p. On convient une fois pour toutes de choisir, dans ce cas, $\pi = p$.

Tout nombre β faisant partie de $\mathrm{K}(p, \alpha)$ peut être mis sous la forme

$$\beta = \pi^{\varrho} u,$$

où u est une unité de $\mathrm{K}(p, \alpha)$ et ϱ un nombre rationnel entier. On dit que ϱ est l'*ordre*[168]) de β par rapport à π. Suivant que β est entier ou fractionnaire dans $\mathrm{K}(p, \alpha)$ on a $\varrho \geqq 0$ ou $\varrho < 0$.*

47. ***Les diviseurs premiers dans le domaine** $(\mathfrak{R}, \xi)$. Soit ξ un nombre algébrique ordinaire défini par l'équation

$$F(x) = 0$$

irréductible dans le domaine $\mathfrak{R}$. Si l'on envisage les nombres rationnels comme des nombres p-adiques, comme il a été expliqué au n° **43**, $F(x)$ n'est pas nécessairement irréductible dans le corps $\mathrm{K}(p)$. Supposons que

$$F(x) = f(x)\,\varphi(x) \ldots \qquad (p),$$

où $f(x)$, $\varphi(x)$, ... sont irréductibles dans le corps $\mathrm{K}(p)$, et désignons par λ, μ, ... les degrés respectifs de $f(x)$, $\varphi(x)$, ... Convenons aussi d'affecter $f(x)$ d'un symbole

$$\mathfrak{p},$$

$\varphi(x)$ d'un symbole

$$\mathfrak{q},$$

. . . .

et donnons à ces symboles le nom de *diviseurs premiers*[169]) du corps $(\mathfrak{R}, \xi)$; le symbole $\mathfrak{p}$ par exemple sera le diviseur premier *correspondant à $f(x)$ dans le domaine de p* ou, comme on dit aussi quelquefois, *correspondant à $f(x)$ au point arithmétique p.*

Enfin convenons encore d'affecter chaque nombre faisant partie du corps $(\mathfrak{R}, \xi)$ d'un *ordre* relativement à chacun des diviseurs premiers de ce corps et cela de la façon suivante: envisagons un corps de décomposition [n° **45**] de l'équation

$$F(x) = 0 \qquad (p);$$

dans ce corps de décomposition $\mathrm{K}(p, \gamma)$ le nombre de racines de l'équation

$$f(x) = 0 \qquad (p)$$

est égal à λ; soient

$$\alpha,\ \alpha',\ \ldots,\ \alpha^{(\lambda-1)}$$

168) **K. Hensel*, Alg. Zahlen[155]), p. 140.*

169) *Id. p. 142, 165.*

ces λ racines; on donne à l'ensemble de ces λ racines le nom de *cycle des racines* de l'équation

$$F(x) = 0$$

correspondant au diviseur premier $\mathfrak{p}$. Les racines de l'équation

$$\varphi(x) = 0$$

définissent de même un *cycle de racines* $F(x) = 0$ relatif au diviseur $\mathfrak{q}$, et ainsi de suite.

Plus généralement, si $\eta = \psi(\xi)$ est un nombre quelconque du corps $(\mathfrak{R}, \xi)$, en d'autres termes si ψ est une fonction rationnelle quelconque de ξ à coefficients rationnels ordinaires, on dit que les nombres

$$\psi(\alpha),\ \psi(\alpha'),\ \ldots,\ \psi(\alpha^{(\lambda-1)})$$

forment le *cycle* de

$$\eta = \psi(\xi)$$

correspondant au diviseur premier $\mathfrak{p}$.

Si π est le nombre premier du corps p-adique $\mathrm{K}(p, \alpha)$ et si ϱ est l'ordre de $\psi(\alpha)$ par rapport à π, on dit que

$$\eta = \varphi(\xi)$$

est d'ordre ϱ relativement à $\mathfrak{p}$.

L'ordre de p relativement à $\mathfrak{p}$ est $e = \frac{\lambda}{f}$, où f a le sens défini au n° **46**. On dit que e est l'*ordre* du diviseur premier $\mathfrak{p}$ et que f est le *degré* du diviseur premier $\mathfrak{p}$[170]).

Les nombres e, f, ϱ ne changent pas quand on remplace π par un des nombres de $\mathrm{K}(p, \alpha)$ qui lui sont équivalents. Ils ne changent même pas quand on prend comme point de départ de toutes les recherches dont on vient de parler, au lieu du corps $\mathrm{K}(p, \gamma)$, un autre corps de décomposition.*

48. ***Développement suivant les puissances de** π. Lorsque la différence $\beta_2 - \beta_1$ de deux nombres β_1 et β_2 faisant partie du corps $\mathrm{K}(p, \alpha)$ est divisible par π^k, on écrit

(1) $$\beta_1 \equiv \beta_2 \qquad (\text{mod. } \mathfrak{p}^k).$$

La condition nécessaire et suffisante pour que les deux nombres β_1 et β_2 soient *égaux* est que la congruence (1) ait lieu *quel que soit k*. S'il en est ainsi on écrit

(2) $$\beta_1 = \beta_2 \qquad (\mathfrak{p}).$$

De ce que l'égalité (2) représente l'ensemble des congruences (1)

170) **K. Hensel*, Alg. Zahlen[155]), p. 143.*

obtenu en y faisant varier k, on conclut pour les nombres du corps $K(p, \alpha)$ une représentation analogue à celle des nombres du corps $K(p)$ sous forme de nombres p-adiques réduits (n° **43**).

Parmi les nombres entiers du corps $K(p, \alpha)$ il y en a

$$\sigma = p^f$$

qui sont tels que chaque entier de $K(p, \alpha)$ est congru à un et à un seul d'entre eux

$$(3) \qquad \eta_0, \eta_1, \ldots, \eta_{\sigma-1} \qquad (\text{mod. } \mathfrak{p}).$$

C'est le théorème analogue à celui d'après lequel chaque nombre rationnel entier ordinaire est congru (mod. p) à l'un des nombres

$$0, 1, 2, \ldots, p-1.$$

On dit que le système (3) est un *système complet de restes* (mod. $\mathfrak{p}$).

Si l'on connaît le nombre π et un système (3) de restes complets (mod. $\mathfrak{p}$) on peut former pour chaque nombre β du corps $K(p, \alpha)$ une et une seule série[171]) correspondante

$$(4) \qquad \varepsilon^{(\varrho)}\pi^\varrho + \varepsilon^{(\varrho+1)}\pi^{\varrho+1} + \varepsilon^{(\varrho+2)}\pi^{\varrho+2} + \cdots\cdots$$

telle que, pour chaque valeur déterminée donnée à k, on ait

$$(5) \qquad \beta \equiv \varepsilon^{(\varrho)}\pi^\varrho + \varepsilon^{(\varrho+1)}\pi^{\varrho+1} + \cdots + \varepsilon^{(k)}\pi^k \qquad (\text{mod. } \mathfrak{p}^{k+1}),$$

où $\varepsilon^{(\varrho)}, \varepsilon^{(\varrho+1)}, \varepsilon^{(\varrho+2)}, \ldots\ldots$ sont des nombres pris parmi ceux du système complet de restes (3).

On dit que la série (4) jouissant de cette propriété est le *développement réduit* de β suivant les puissances entières de π.

Inversement, toute série de la forme (4), à coefficients pris parmi les nombres du système complet de restes (3), est le développement réduit d'un nombre déterminé β du corps $K(p, \alpha)$; on obtient ce nombre β en remplaçant par leur somme chaque suite de e termes consécutifs de la série (4) envisagée.

Dans le corps $K(p, \alpha')$ conjugué de $K(p, \alpha)$ désignons par β' le nombre qui correspond au nombre β du corps $K(p, \alpha)$. Si, dans la série (4), on remplace le nombre premier π et les coefficients pris dans le corps $K(p, \alpha)$ par le nombre premier π' et les nombres correspondants pris dans le corps $K(p, \alpha')$, on obtient précisément le développement réduit du nombre β' suivant les puissances entières de π'.

Dans les applications algébriques nous n'avons à envisager que les développements de ceux des nombres des corps $K(p, \alpha)$, $K(p, \alpha')$, ... suivant les puissances entières respectives de $\pi, \pi', \ldots$ qui sont de la forme

$$\beta = \psi(\alpha), \quad \beta' = \psi(\alpha'), \quad \ldots,$$

171) ${}_*$*K. Hensel,* Alg. Zahlen[155]), p. 145.*

où ψ est une fonction rationnelle entière ayant pour coefficients des nombres rationnels ordinaires envisagés comme des nombres p-adiques, comme il a été expliqué au n° **43**.

Les séries (4) jouent dans l'étude des nombres algébriques le rôle que jouent dans la théorie générale des fonctions les développements suivant les puissances entières ou fractionnaires de $x - \alpha$. Le nombre p joue ici le rôle que joue $x - \alpha$ dans la théorie exposée au n° **33**. Les nombres faisant partie du système complet de restes (3) jouent ici le rôle des coefficients constants dans les développements en séries entières.

Les nombres λ et e ont tous deux un sens analogue à celui de l'ordre de ramification a envisagé au n° **33**; mais il importe d'insister sur ce que cette analogie de λ et e avec a n'est au fond qu'apparente. C'est en réalité un autre nombre qui joue ici le rôle de l'ordre de ramification a; ce nombre que nous rencontrerons plus loin, et que nous désignerons par $\bar{e}$, n'est pas toujours égal à e; il est parfois plus grand que e.

Quoique n'étant qu'apparente, l'analogie *simultanée* de

$$\lambda = ef$$

et de e avec le nombre a du n° **33** permet de conclure que pour les diviseurs premiers de la théorie des fonctions il faut envisager f comme égal à 1.

En comparant ainsi la portée des notions de la théorie des nombres à celle des notions correspondantes de la théorie des fonctions d'une variable, on s'aperçoit que non seulement les premières sont plus compliquées que les secondes, mais qu'elles sont aussi plus nombreuses en ce sens qu'à une notion de la théorie des fonctions d'une variable correspondent parfois deux ou plusieurs notions distinctes de la théorie des nombres.*

49. ${}_*$**Représentation, dans le domaine d'un nombre premier p, des nombres algébriques d'après leurs valeurs numériques respectives.** Tandis que les séries entières en $x - \alpha$ du n° **33** convergent pour des valeurs de x suffisamment voisines de α et fournissent les valeurs des fonctions algébriques qu'elles représentent, les nombres p-adiques ne sont que des *symboles* dans l'étude desquels la recherche de la convergence ou de la valeur numérique possible ne sont jusqu'ici intervenues en rien.

Au sujet de ce dernier caractère on rencontre tout d'abord le curieux théorème que voici:[172])

172) ${}_*$*K. Hensel,* Alg. Zahlen[155]), p. 41.*

Soient

$$A = a_\varrho p^\varrho + a_{\varrho+1} p^{\varrho+1} + a_{\varrho+2} p^{\varrho+2} + \cdots\cdots$$

un nombre rationnel p-adique et B un nombre réel *quelconque* donné. On peut toujours déterminer une série p-adique

$$b_\varrho p^\varrho + b_{\varrho+1} p^{\varrho+1} + b_{\varrho+2} p^{\varrho+2} + \cdots\cdots$$

à coefficients rationnels (entiers mod. p) qui, envisagée comme un nombre p-adique, est égale à A et qui, envisagée comme une série numérique ordinaire, a pour somme B.

Lorsqu'on prend pour B un nombre imaginaire le théorème a d'ailleurs encore lieu, à condition bien entendu de prendre pour coefficients dans la série p-adique des nombres complexes rationnels (entiers mod. p).

En prenant pour B un nombre algébrique, on voit que[173]) si,

$$\xi_1, \xi_2, \ldots, \xi_n$$

désignant les n racines d'une équation algébrique

$$F(x) = 0$$

irréductible dans le domaine $\Re$, l'équation

$$F(x) = 0 \qquad (p)$$

a, dans le corps $\mathrm{K}(p)$, au moins une racine α, les n racines $\xi_1, \xi_2, \ldots, \xi_n$ peuvent être développées en n séries p-adiques absolument convergentes, à coefficients complexes rationnels (entiers mod. p) qui, envisagées comme des nombres p-adiques, sont toutes égales à α.

Le théorème suivant est plus général:[174])

Soit ξ un nombre algébrique ordinaire vérifiant l'équation irréductible

$$F(x) = 0.$$

Supposons que dans le corps $\mathrm{K}(p)$ la fonction $F(x)$ décomposée en facteurs irréductibles se présente sous la forme

$$F(x) = f(x)\,\varphi(x)\ldots \qquad (p).$$

Dans le corps de décomposition $\mathrm{K}(p, \gamma)$ de $F(x)$, soit α une racine de l'équation

$$f(x) = 0 \qquad (p).$$

Désignons par $\mathfrak{p}$ le diviseur premier du domaine $(\Re, \xi)$ qui correspond à $f(x)$ dans le domaine de p. On démontre que les nombres

$$\eta, \zeta, \ldots$$

173) **K. Hensel*, Alg. Zahlen[155]), p. 91.*

174) *Id. p. 330.*

du corps $(\Re, \xi)$ peuvent être développés en séries p-adiques absolument convergentes [qui, envisagées comme des nombres p-adiques, appartiennent toutes au domaine $\mathrm{K}(p, \alpha)$] de façon qu'une équation algébrique

$$\varphi(\eta, \zeta, \ldots) = 0,$$

à coefficients rationnels, puisse être envisagée comme exacte *numériquement* et ne puisse l'être que si, dans le domaine de p, l'équation

$$\varphi(\eta, \zeta, \ldots) = 0 \qquad (\mathfrak{p})$$

est vérifiée quand on y remplace $\eta, \zeta, \ldots$ par les séries p-adiques précédentes envisagées comme des nombres p-adiques.

Le théorème que voici est plus général encore[175]):

Soient

$$\xi_1, \xi_2, \ldots, \xi_n$$

les n racines d'une équation algébrique ordinaire

$$F(x) = 0,$$

à coefficients rationnels ordinaires, et soit $\mathrm{K}(p, \gamma)$ le corps de décomposition de l'équation

$$F(x) = 0 \qquad (p).$$

On peut développer $\xi_1, \xi_2, \ldots, \xi_n$ en séries p-adiques absolument convergentes [qui, envisagées comme des nombres p-adiques, appartiennent au domaine $\mathrm{K}(p, \gamma)$] de façon qu'une équation algébrique

$$\varphi(\xi_1, \xi_2, \ldots, \xi_n) = 0,$$

à coefficients rationnels, soit exacte *numériquement* et ne le soit que quand, dans le domaine des nombres p-adiques, l'équation

$$\varphi(\xi_1, \xi_2, \ldots, \xi_n) = 0 \qquad (p)$$

est vérifiée quand on y remplace $\xi_1, \xi_2, \ldots, \xi_n$ par les séries p-adiques précédentes envisagées comme des nombres p-adiques.

Nous n'aurons pas l'occasion dans cet article d'appliquer les théorèmes énoncés dans ce numéro. Nous envisagerons toujours dans ce qui suit les séries p-adiques comme des nombres p-adiques sans jamais les envisager comme des séries numériques.*

50. *Le corps des coefficients. L'équation d'Eisenstein pour π. L'ordre de ramification. Les $\sigma = p^f$ nombres du système complet de restes

$$\eta_0, \eta_1, \ldots, \eta_{\sigma-1}$$

envisagé au n° 48 peuvent être choisis de différentes manières. On

175) **K. Hensel*, Alg. Zahlen[155]), p. 335.*

peut les fixer d'une façon particulièrement simple en s'appuyant sur le théorème suivant:

Dans le corps $K(p, \alpha)$ le premier membre de l'équation

$$x^{p^f} - x = 0 \qquad (\mathfrak{p}) \tag{1}$$

se décompose en facteurs linéaires et les $\sigma = p^f$ racines de l'équation (1) forment un système complet de restes (mod. $\mathfrak{p}$).

Dans tout ce qui suit il sera entendu que quand nous parlerons d'un système complet de restes, il s'agira de ce système-là.

L'une des racines de l'équation (1) est

$$\eta_0 = 0;$$

les $\sigma - 1$ autres racines de l'équation (1) sont racines de l'équation

$$x^{p^f-1} = 1 \qquad (\mathfrak{p}) \tag{2}$$

et sont donc les racines $(p^f-1)^{\text{ièmes}}$ de l'unité dans le corps $K(p, \alpha)$.

Soient d un des diviseurs de $p^f - 1$ et $\varphi(d)$ l'indicateur de d. Parmi les racines de l'équation (2) il y en a $\varphi(d)$ qui appartiennent à l'exposant d; en d'autres termes, $\varphi(d)$ des racines de l'équation (2) élevées à la puissance d sont égales à 1 sans qu'aucune puissance inférieure d'une quelconque de ces $\varphi(d)$ racines soit égale à 1.

Les racines *primitives* $(p^f-1)^{\text{ièmes}}$ de l'unité dans le corps $K(p, \alpha)$ sont celles qui appartiennent à l'exposant $p^f - 1$. Ces racines primitives peuvent être distribuées en groupes contenant chacun f d'entre elles[177]), les racines d'un même groupe vérifiant une équation de degré f

$$G(x) = 0 \qquad (\mathfrak{p})$$

dont les coefficients font partie du domaine orthoïde $K(p)$ et qui, dans ce domaine, est irréductible.

Si, dans le corps $K(p, \alpha)$, η est une racine primitive $(p^f-1)^{\text{ième}}$ de l'unité, les σ racines de l'équation (1) peuvent être représentées par

$$0,\ \eta,\ \eta^2,\ \ldots,\ \eta^{\sigma-1};$$

si, en formant les séries (4) du n° **48** pour le nombre premier π du corps $K(p, \alpha)$, on choisit pour coefficients les nombres de cette suite

$$0,\ \eta,\ \eta^2,\ \ldots,\ \eta^{\sigma-1},$$

ces coefficients représentent des nombres appartenant tous au domaine $K(p, \eta)$. C'est pour cette raison que l'on appelle ce domaine

$$K(p, \eta)$$

le *corps des coefficients correspondant au diviseur* $\mathfrak{p}$.

176) $_*$*K. Hensel*, Alg. Zahlen[155]), p. 185.*

177) $_*$Id. p. 192.*

Le nombre premier π du corps $K(p, \alpha)$ est racine d'une équation de la forme[178])

$$x^e + pc_{e-1}x^{e-1} + pc_{e-2}x^{e-2} + \cdots + pc_0 = 0 \qquad (p), \tag{3}$$

où $c_{e-1}, c_{e-2}, \ldots, c_1$ sont des entiers du corps des coefficients $K(p, \eta)$ et où c_0 est un entier de ce corps non divisible par p.

Cette équation (3) est irréductible dans le corps $K(p, \eta)$ comme on peut s'en convaincre aisément par un raisonnement tout semblable à celui sur lequel repose la démonstration du théorème de *Th. Schönemann* et de *G. Eisenstein* [I 9, **90**]. On a donné à l'équation (3) le nom d'*équation d'Eisenstein.*

Si e n'est pas divisible par p on peut toujours choisir π de façon que l'équation d'Eisenstein se présente sous la forme

$$x^e - p\eta^k = 0 \qquad (p),$$

où k est un nombre rationnel entier.

L'équation d'Eisenstein permet d'étendre aisément à la théorie des nombres la notion si importante d'*ordre de ramification* établie uniquement jusqu'ici dans la théorie des fonctions algébriques.

Si

$$\psi'(x) = ex^{e-1} + (e-1)pc_{e-1}x^{e-2} + (e-2)pc_{e-2}x^{e-3} + \cdots + pc_1$$

est la dérivée, prise par rapport à x, de la fonction

$$\psi(x) = x^e + pc_{e-1}x^{e-1} + pc_{e-2}x^{e-2} + \cdots + pc_0$$

qui figure dans le premier membre de l'équation (3), nous appellerons ordre de ramification de $\mathfrak{p}$ et nous désignerons par

$$\bar{e}$$

l'unité 1 augmentée de l'ordre de $\psi'(\pi)$ par rapport à $\mathfrak{p}$[179]).

Si e n'est pas divisible par p on a

$$\bar{e} = e.$$

Si $e = p^s e_0$, où s désigne un nombre naturel et où e_0 n'est pas divisible par p, on a

$$e + 1 \leqq \bar{e} \leqq (s+1)e.$$

Si l'on se donne un corps $(\mathfrak{R}, \xi)$ et que, pour chaque nombre premier p, on détermine tous les diviseurs premiers

$$\mathfrak{p},\ \mathfrak{q},\ \ldots$$

de ce corps $(\mathfrak{R}, \xi)$ on a, en général,

$$e = \bar{e} = 1;$$

178) $_*$*K. Hensel*, Alg. Zahlen[155]), p. 197.*

179) $_*$Id. p. 219.*

ce n'est que pour un nombre fini de diviseurs premiers du corps $(\mathfrak{R}, \xi)$ que l'on a

$$\bar{e} \geqq e > 1;$$

on a donné à ces diviseurs particuliers le nom de *diviseurs premiers de ramification* et *K. Hensel*[180]) désigne les nombres p correspondants sous le nom de *nombres de ramification.*

Ces nombres de ramification sont identiques aux nombres critiques de *H. Minkowski*[181]).*

51. *La différente d'un corps. L'analogie déjà signalée à plusieurs reprises entre les corps de fonctions et les corps de nombres mérite de fixer notre attention.

Soient

$$(1) \qquad \mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_h$$

h diviseurs premiers du corps $(\mathfrak{R}, \xi)$ et η un nombre quelconque de ce corps.

Comme dans la théorie des fonctions algébriques, on dit encore ici que η est *divisible* par le *diviseur*

$$\mathrm{D} = \mathfrak{p}_1^{\varrho_1} \mathfrak{p}_2^{\varrho_2} \ldots \mathfrak{p}_h^{\varrho_h}$$

lorsque, pour $i = 1, 2, \ldots, h$, l'ordre de η par rapport à $\mathfrak{p}_i$ est plus grand ou égal à ϱ_i et que cet ordre est positif ou nul par rapport à chacun des diviseurs premiers du corps $(\mathfrak{R}, \xi)$ ne figurant pas dans la suite (1) envisagée.

Toutes les définitions et tous les théorèmes énoncés dans les n^{os} **34** et **37** s'étendent avec de légères modifications aux diviseurs de la théorie des nombres que nous venons de définir. L'unique complication résulte de ce que dans la théorie des nombres algébriques il y a des diviseurs $\mathfrak{p}$ de degré $f > 1$.

La distinction entre diviseurs entiers et diviseurs fractionnaires est identique à celle du n° **34**. On peut, ici aussi, déterminer un système de n nombres

$$\xi_1, \xi_2, \ldots, \xi_n$$

tels que la condition nécessaire et suffisante pour qu'un nombre quelconque η du corps envisagé $(\mathfrak{R}, \xi)$ soit divisible par D est que η puisse être mis sous la forme

$$\eta = \xi_1 u_1 + \xi_2 u_2 + \cdots + \xi_n u_n,$$

où $u_1, u_2, \ldots, u_n$ sont des nombres rationnels entiers.

L'ensemble de ceux des nombres du corps envisagé qui sont divisibles par D est ce qu'on appelle *un idéal* de ce corps. L'idéal est

180) *Alg. Zahlen[155]), p. 162.*

181) *Geom. der Zahlen[69]) 1, p. 123.*

dit entier ou fractionnaire suivant que D est un diviseur entier ou fractionnaire. Les idéaux entiers sont des idéaux au sens donné à ce mot au n° **26.**

Si $\mathfrak{p}$ est un diviseur premier de degré f l'idéal correspondant est un idéal premier de degré f; en d'autres termes la norme de cet idéal est égal à p^f.

Le diviseur

$$\mathrm{D} = \mathfrak{p}_1^{\bar{e}_1 - 1} \mathfrak{p}_2^{\bar{e}_2 - 1} \ldots \mathfrak{p}_h^{\bar{e}_h - 1},$$

où $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_h$ sont tous les diviseurs premiers de ramification et $\bar{e}_1, \bar{e}_2, \ldots, \bar{e}_h$ leurs ordres de ramification, doit être signalé à part. On le nomme le *diviseur de ramification* et l'on dit de l'idéal correspondant qu'il est l'*idéal fondamental* ou l'*idéal de ramification* ou encore[182]) la *différente* du corps envisagé.*

52. Les facteurs du discriminant du corps et les facteurs du discriminant d'une équation. De nombreuses analogies entre la théorie des fonctions algébriques et celle des nombres algébriques peuvent évidemment être mises en évidence sans utiliser la théorie des nombres p-adiques et plusieurs de ces analogies ont été découvertes indépendamment de cette théorie.

Parmi ces analogies une des plus remarquables est la suivante:

Comme on l'a vu au n° **36**, le discriminant Δ du corps $\mathrm{K}(x, y)$ attaché à la courbe algébrique $f(x, y) = 0$ est égal à la norme de l'*idéal de ramification.* Pour qu'une fonction linéaire $x - \alpha$ contienne donc un ou plusieurs diviseurs premiers $\mathfrak{P}$ à une puissance supérieure à la première, il faut et il suffit que $x - \alpha$ soit un diviseur de Δ.

R. Dedekind[183]) a montré que, de même, dans la théorie des corps purement numériques envisagés comme des corps absolument algébriques, le discriminant est égal à la norme d'un idéal. Cet idéal que *R. Dedekind* a désigné sous le nom d'*idéal fondamental* est identique à l'idéal introduit à la fin du n° **51** mais il est défini ici par une autre de ses propriétés.

Dans la théorie des corps numériques les facteurs premiers du discriminant sont donc aussi caractérisés[184]) par la condition que chacun d'eux est divisible par le carré d'un idéal premier.

182) **D. Hilbert,* Jahresb. deutsch. Math.-Ver. 4 (1894/5), éd. Berlin 1897, p. 201 (n° 12). *D. Hilbert* définit la *différente* du corps par sa propriété énoncée à la fin du n° **52.***

183) Abh. Ges. Gött. 29 (1882), math. mém. n° 7, p. 38.

184) *R. Dedekind,* Abh. Ges. Gött. 29 (1882), math. mém. n° 7, p. 6; dans *G. Lejeune Dirichlet,* Zahlenth.[9]), (4^e éd.) p. 636 (Suppl. XI, n° 186) spécialement pour le cas des corps quadratiques; *K. Hensel,* J. reine angew. Math. 113 (1894), p. 80.

Le théorème du n° **38** sur la décomposition du discriminant de l'équation $f(x, y) = 0$ peut, lui aussi, être étendu à des corps de nombres.

Avant d'aborder cette question il importe de mettre en évidence les propriétés les plus importantes de l'idéal des points doubles qui a été défini au n° **38**. Il suffit toutefois d'envisager le cas où, dans la fonction $f(x, y)$ envisagée comme une fonction de y seulement, le coefficient de la puissance la plus élevée est égal à 1. Chaque fonction rationnelle entière $E(x, y)$ de x et de y est alors une fonction algébrique *entière* de x. L'ensemble des polynomes entiers $E(x, y)$ en x et y forme un domaine holoïde [n° **15**], c'est-à-dire dans la terminologie de *D. Hilbert* un *anneau* [n° **22**]. En étendant la notion de *conducteur* [n° **31**] sans aucune modification aux anneaux de fonctions, le conducteur de l'anneau qu'on vient de mentionner est l'idéal des points doubles de la courbe $f(x, y) = 0$.

Si l'on entend, comme on l'a fait au n° **12**, par *différente* d'une quantité algébrique quelconque ξ (nombre algébrique, ou fonction algébrique) le produit

$$(\xi - \xi')(\xi - \xi'') \ldots (\xi - \xi^{(n-1)}),$$

où $\xi', \xi'', \ldots, \xi^{(n-1)}$ sont les quantités conjuguées de ξ, la différente de y est, dans le cas actuellement envisagé, égale à $\frac{df}{dy}$ [$f(x, y) = 0$ étant l'équation qui définit y], et sa norme est égale au discriminant de $f(x, y) = 0$. Le théorème sur la décomposition de ce discriminant peut être envisagé comme un corollaire du théorème général que voici:

La différente de y est le produit de l'idéal de ramification et du conducteur de l'anneau des polynomes entiers en x et y.

On peut de même, dans un corps de nombres, considérer l'anneau formé par toutes les fonctions entières à coefficients entiers d'une certaine quantité y, entier algébrique appartenant au corps. On voit alors que, dans un corps de nombres, la différente de y est le produit de l'idéal fondamental par le conducteur de l'anneau ainsi obtenu[185]) et que la norme de ce conducteur est le carré d'un nombre entier, comme dans les corps de fonctions[185]).

Il en résulte (en prenant les normes de ces différents facteurs) que le discriminant de l'équation en y est, même pour des corps de nombres algébriques, le produit de deux facteurs: l'un (dit le *facteur*

185) *R. Dedekind*, Abh. Ges. Gött. 29 (1882), math. mém. n° 7, p. 40; *G. Landsberg*, Jahresb. deutsch. Math.-Ver. 14 (1905), p. 100.

essentiel) est le discriminant même du corps; l'autre (dit le *facteur non essentiel*) est le carré d'un nombre entier[186]).

Pour obtenir aisément l'*idéal fondamental* ou la *différente* d'un corps, qui joue un rôle si important dans les recherches précédentes, on peut procéder comme il suit:

Considérons la *forme fondamentale*, c'est-à-dire l'expression

$$\xi = u_1 \xi_1 + u_2 \xi_2 + \cdots + u_n \xi_n,$$

dans laquelle $(\xi_1, \xi_2, \ldots, \xi_n)$ est une base des quantités entières du corps [n° **20**] et $u_1, u_2, \ldots, u_n$ des indéterminées; prenons la différente de cette expression, autrement dit formons le produit

$$(\xi - \xi')(\xi - \xi'') \ldots (\xi - \xi^{(n-1)})$$

où $\xi', \xi'', \ldots, \xi^{(n-1)}$ sont les expressions conjugées de ξ. C'est une forme de degré $n - 1$ en $u_1, u_2, \ldots, u_n$. Le plus grand commun diviseur des coefficients de cette forme n'est autre que la différente du corps[182]).

53. L'équation fondamentale. Décomposition des quantités premières entières rationnelles en idéaux premiers. La notion de forme fondamentale peut être étendue aux fonctions algébriques de *plusieurs* variables [et aussi à la théorie des fonctions algébriques d'une et de plusieurs variables au point de vue de Kronecker, c'est-à-dire à la théorie des corps dérivés de $R_{\mathfrak{R}}$]. Cette généralisation permet d'obtenir, *par des opérations rationnelles*, la décomposition d'une quantité rationnelle première π (nombre premier ordinaire, binome de la forme $x - x_0$ ou polynome irréductible à plusieurs variables. en idéaux premiers du corps.

Pour définir tout d'abord la forme fondamentale, dans le cas général où nous nous plaçons, envisageons une base

$$(\xi_1, \xi_2, \ldots, \xi_r)$$

dont les éléments soient des quantités entières du corps K envisagé. Si $u_1, u_2, \ldots, u_r$ désignent de nouvelles variables, on entend encore ici par forme fondamentale l'expression

$$(1) \qquad \xi = u_1 \xi_1 + u_2 \xi_2 + \cdots + u_r \xi_r.$$

Toutefois entre cette définition et celle concernant les cas envisagés jusqu'ici, il y a cette différence essentielle que r est ici, en général, *plus grand* que le degré n du corps K.

Ceci posé, et K étant un corps algébrique quelconque (corps de

186) Le théorème était connu sous cette seule forme avant l'introduction de la notion d'idéal fondamental.

nombres algébriques ou corps de fonctions algébriques d'une ou de plusieurs variables), formons l'expression

$$(2)\qquad F(z, u_1, \ldots, u_n) = (z-\xi)(z-\xi')\ldots(z-\xi^{(n-1)}) = 0,$$

équation en z qui a pour racines la forme fondamentale ξ et ses conjuguées $\xi', \ldots, \xi^{(n-1)}$. Cette équation se nomme *l'équation fondamentale* du corps[187]).

Remarquons tout de suite que la forme fondamentale est une *quantité idéale entière* au sens de *Gy. (J.) König* [n° **27**]. Toute autre quantité idéale entière $\mathfrak{A}$ du corps K peut se mettre sous la forme[188])

$$(3)\qquad \mathfrak{A} = v_0 + v_1\xi + v_2\xi^2 + \cdots + v_{n-1}\xi^{n-1},$$

où $v_0, v_1, v_2, \ldots, v_{n-1}$ sont des quantités idéales rationnelles entières, c'est-à-dire des quantités idéales entières dont les coefficients sont des quantités entières du domaine naturel de rationalité ayant servi à former le corps envisagé K.

[Si l'on se place au point de vue de la théorie des fonctions algébriques de *L. Kronecker* on sait seulement que le produit de $\mathfrak{A}$ par un certain nombre d peut être mis sous la forme (3); ce nombre d est rationnel entier et divise $(p-2)!$ ainsi que le discriminant de l'équation fondamentale (2). On n'a pu jusqu'ici reconnaître si d peut être pris égal à 1. Ce n'est aussi que pour le produit de $\mathfrak{A}$ par d que *L. Kronecker*[188]) avait démontré la même proposition dans le cas où l'on envisage des corps de nombres; c'est *K. Hensel*[188]) qui a montré que l'on peut alors prendre $d = 1$].

Nous allons maintenant aborder le problème de la décomposition d'une quantité rationnelle π qui a été posé au début de ce numéro[189]).

Convenons, suivant l'usage, de dire qu'un polynome F entier en z est divisible par la quantité rationnelle première π (nombre ou quantité variable indépendante de z) quand les coefficients des différentes puissances de z sont tous divisibles par π. Ceci posé, si l'on peut trouver des polynomes $P, Q, R, \ldots$ entiers en z, tels que la différence

$$F - PQR\ldots$$

187) *L. Kronecker*, Festschrift[1]) § 25; J. reine angew. Math. 92 (1882), p. 108; Werke 2, p. 370.

188) *L. Kronecker*, Festschrift[1]) § 25; J. reine angew. Math. 92 (1882), p. 108; Werke 2, p. 370; *K. Hensel*, J. reine angew. Math. 113 (1894), p. 74; *Gy. (J.) König*, Alg. Grössen[10]), p. 527.

189) *L. Kronecker*, Festschrift[1]) § 25; J. reine angew. Math. 92 (1882), p. 108; Werke 2, p. 370; *K. Hensel*, J. reine angew. Math. 113 (1894), p. 75; *Gy. (J.) König*, Alg. Grössen[10]), p. 534.

soit divisible par π on dit[190]) que le polynome F, entier en z, est décomposable suivant le module π en facteurs $P, Q, R, \ldots$ et l'on écrit

$$F \equiv PQR\ldots \quad (\text{mod } \pi).$$

Si le polynome F n'admet aucune décomposition de cette espèce, on dit que F est *irréductible suivant le module* π.

Plus généralement encore on dit avec *Gy. (J.) König*[191]) que F est décomposable, suivant le module d'équivalence π, en facteurs $P, Q, R, \ldots$ lorsqu'il existe deux quantités rationnelles entières E_1, E_2 non divisibles par π et telles que l'on ait

$$E_1 F \equiv E_2 PQR \ldots (\text{mod. } \pi).$$

On écrit alors

$$F \equiv PQR \ldots (\text{mod. équiv. } \pi).$$

Cela posé considérons le premier membre F de l'équation fondamentale (2) et décomposons-le en facteurs irréductibles suivant le module d'équivalence π: soit

$$F \equiv P_1^{e_1} P_2^{e_2} \ldots P_r^{e_r} \quad (\text{mod. équiv. } \pi)$$

cette décomposition. Alors la décomposition de π en idéaux premiers est

$$\pi = \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\ldots\mathfrak{P}_r^{e_r},$$

l'idéal premier $\mathfrak{P}_h$ étant le contenu [n° **27**] de la forme ou de la quantité idéale que l'on obtient lorsqu'on substitue à z la forme fondamentale dans l'expression de $\pi + P_h$.

Si K est un corps de nombres ou un corps de fonctions algébriques d'*une seule* variable [le point de vue de Kronecker étant ici exclu], chaque décomposition de F en facteurs premiers suivant le module π fournit aussi une décomposition de F en facteurs premiers suivant le module d'équivalence π. On peut donc pour ces corps K, mais pour ces corps K seulement, se passer de la notion de module d'équivalence[192]).

54. Représentation des diviseurs premiers d'un corps numérique par adjonction de corps plus étendus. Si le domaine K n'est pas complet, et si l'idéal $\mathfrak{a}$ défini par les éléments fondamentaux $\alpha_1, \alpha_2, \ldots, \alpha_r$ est un idéal non principal, le plus grand commun

190) *J. A. Serret*, Alg. sup.[21]) 2, p. 122.

191) Alg. Grössen[10]), p. 505.

192) **L. Kronecker* [Festschrift[1]), § 25; J. reine angew. Math. 92 (1882), p. 108; Werke 2, p. 370] admettait à tort qu'il suffit, quel que soit le corps K envisagé, d'effectuer la décomposition de F suivant le module π. C'est à *Gy. (J.) König* [Alg. Grössen[10]), p. 534] que l'on doit d'avoir éclairci cette question [Note de *J. Kürschák*].*

diviseur des nombres $\alpha_1, \alpha_2, \ldots, \alpha_r$ n'est pas une quantité appartenant à K: elle n'est représentable que par une forme du corps K. On peut cependant, dans certains cas, par un autre mode d'association, représenter les idéaux par des quantités empruntées à un domaine plus étendu que K.

ans le cas des corps numériques, un premier procédé pour arriver à ce but est fourni à *R. Dedekind*[193]) par le théorème [voir n° **30**] d'après lequel, si h est le nombre des classes d'idéaux d'un corps K, la puissance $h^{\text{ième}}$ de tout idéal $\mathfrak{a}$ est un idéal principal (α). L'idéal $\mathfrak{a}$ peut alors être regardé comme correspondant au nombre algébrique $\sqrt[h]{\alpha}$ (en général, extérieur à K): il est, en fait, formé par tous les nombres appartenant à K et divisibles par $\sqrt[h]{\alpha}$.*

*Cette manière d'envisager les choses ne s'est cependant pas jusqu'à présent montrée féconde à elle seule sous sa forme première et directe. Elle subit déjà une transformation dans l'étude de *F. Klein*[194]) sur les corps quadratiques. Les idéaux du corps quadratique $(\mathrm{R}, \sqrt{d})$, où d est le discriminant [n° **20**] du corps, sont liés aux formes quadratiques de déterminant d, de telle sorte qu'aux classes d'idéaux correspondent les classes de formes quadratiques, la *multiplication* des idéaux correspondant à la *composition* des formes [voir I 16, **23** et **24**]. Les idéaux principaux sont liés à la forme principale et aux formes qui lui sont équivalentes. Les idéaux qui ne sont pas idéaux principaux sont liés aux autres classes de formes. Or, à ces idéaux et à ces nouvelles classes de formes quadratiques, *F. Klein* fait correspondre de nouveaux nombres [*nombres adjoints*[194a])] qui se trouvent être égaux à des nombres du corps donné multipliés par certains facteurs très simples.*

*Plaçons-nous d'abord dans le cas où le discriminant d [n° **20**] du corps quadratique K envisagé est divisible par 4. Le nombre $\frac{d}{4}$ est alors soit de la forme $4m+2$, soit de la forme $4m+3$ et il n'est divisible par aucun carré. Pour obtenir tous les entiers de K il suffit de remplacer x et y par tous les entiers rationnels possibles dans

193) *Bull. sc. math. (2) 1 (1877), p. 246.*

194) *Ausgewählte Kapitel der Zahlenlehre 2, rédigé par *A. Sommerfeld* et *Ph. Furtwängler* (autographié) Göttingue 1896, p. 94/221; voir aussi Math. Ann. 48 (1897), p. 562; The Evanston colloquium, Lect. of math., recueillies par *A. Ziwet*, New York 1894, 8ième confé-rence; trad. par *L. Laugel*, Conférences sur les math. faites au congrès de math. tenu à l'occasion de l'exposition de Chicago, éd. Paris 1898, p. 58.*

194a) *C'est ainsi qu'ils ont été désignés dans l'article I 16. Il eût peut-être été préférable de les désigner sous le nom de *nombres secondaires*.*

l'expression

$$(1) \qquad x + \frac{\sqrt{d}}{2} y,$$

en sorte que les normes des entiers de K sont de la forme

$$(2) \qquad x^2 - \frac{d}{4} y^2.$$

Si l'on envisage x et y comme des variables, l'expression (2) est une forme quadratique à laquelle *F. Klein* a donné le nom de *forme principale* (*Hauptform*) de première espèce du corps K. A cette forme principale il adjoint un représentant de chacune des classes (I 16, **14**) de formes

$$(3) \qquad f = ax^2 + bxy + cy^2$$

à coefficients rationnels entiers, ayant pour déterminant $b^2 - 4ac$ [I 16, **22**] le discriminant d du corps K; il obtient ainsi outre la forme (2) un nombre fini $h-1$ de formes f.

En désignant par ϱ un nombre entier, tout d'abord indéterminé, on peut décomposer chacune de ces h formes f en deux facteurs

$$\xi = \varrho\left[\sqrt{a}\,x + \frac{b+\sqrt{d}}{2\sqrt{a}}\,y\right],$$

$$\eta = \frac{1}{\varrho}\left[\sqrt{a}\,x + \frac{b-\sqrt{d}}{2\sqrt{a}}\,y\right];$$

on donne d'après *F. Klein* au nombre ϱ le nom de *facteur azimutal*, et pour chaque paire d'entiers rationnels x, y, on appelle ξ et η les *coordonnées minimales* du point P de coordonnées cartésiennes rectangulaires

$$u = \frac{\xi+\eta}{2}, \qquad v = \frac{\xi-\eta}{2},$$

ou

$$u = \frac{\xi+\eta}{2}, \qquad v = \frac{\xi-\eta}{2i},$$

suivant que d est positif ou négatif.

A chacune des h formes envisagées correspond [cf. I 16, **24**] ainsi dans le plan des (u, v) un réseau (R) de points P que l'on obtient en donnant à x et à y toutes les valeurs rationnelles entières possibles.

On appelle *somme* $P+P'$ de deux points de coordonnées minimales (ξ, η) et (ξ', η') le point de coordonnées minimales $(\xi+\xi', \eta+\eta')$. On appelle *produit* PP' de deux points de coordonnées minimales (ξ, η), (ξ', η') le point de coordonnées minimales $(\xi\xi', \eta\eta')$.

Si l'on multiplie chaque point P d'un réseau (R) par chaque point P' d'un réseau (R') et si l'on ajoute, de toutes les manières possibles, les points ainsi obtenus, on obtient un nouveau réseau qu'on appelle le *réseau composé* (RR') du réseau (R) et du réseau (R').

Si l'on fixe arbitrairement le facteur azimutal ϱ, le réseau composé de deux des h réseaux correspondant aux h formes f envisagées, ne coïncidera pas, en général, avec l'un de ces h réseaux. Mais si l'on prend pour la forme principale (2) un facteur azimutal $\varrho = 1$, on pourra déterminer les facteurs azimutaux des autres formes de façon que le réseau composé de deux quelconques des h réseaux coïncide toujours avec un des h réseaux. L'ensemble des h réseaux correspondant à ce choix des facteurs azimutaux ϱ est ce que *F. Klein* appelle la *figure normale des h réseaux.*

Les points du réseau qui correspond à la forme principale (2) sont dits *points principaux*, les coordonnées minimales des points principaux sont dits *nombres principaux.* Les points des réseaux qui correspondent aux autres formes f envisagées sont dits *points adjoints*, les coordonnées minimales des points adjoints sont dits *nombres adjoints.*

Les nombres principaux sont les nombres *entiers* du corps quadratique K. Les nombres adjoints sont des nombres algébriques entiers ne faisant pas partie du corps quadratique K.

L'ensemble des nombres principaux et adjoints forme un *domaine holoïde complet* dans lequel chaque nombre peut, d'une et d'une seule manière, être décomposé en facteurs premiers, si l'on convient d'envisager comme *équivalents* deux nombres dont le quotient est égal à une unité du domaine holoïde complet.

Quand le déterminant d du corps quadratique envisagé n'est pas divisible par 4, le nombre d est de la forme $4m+1$ et il n'est divisible par aucun carré. Rien n'est changé à ce qui précède si ce n'est que l'expression (1) est remplacée par l'expression

$$x + \frac{\sqrt{d}-1}{2}\, y \tag{1a}$$

et la forme (2) par la forme

$$x^2 + xy + \frac{1-d}{4}\, y^2. \tag{2a}$$

F. Klein a donné à cette forme (2a) le nom de *forme principale de seconde espèce*[194b]).*

Une série de recherches beaucoup plus étendues est celle à laquelle on est conduit en supposant que le corps quadratique considéré $K = (\Re, \sqrt{d})$ soit imaginaire (d étant un entier négatif): il est

194b) *Ce texte est entièrement dû à *J. Kürschák.**

alors lié à un cas de multiplication complexe [voir I 19] de fonctions elliptiques et l'on obtient un nombre algébrique u en substituant $\sqrt{d}$ dans une fonction modulaire elliptique. Le corps $\mathfrak{K} = (K, u)$ est ce que l'on nomme le *corps de classes*[195]) correspondant à K. Il est relativement abélien [nº **14**] par rapport à K et son degré par rapport à K n'est autre que le nombre h des classes idéales de K: son groupe relatif est holoédrique isomorphe au groupe [nº **30**] formé par les dites classes d'idéaux et son discriminant relatif est égal à 1. Pour exprimer cette dernière propriété du corps de classe $\mathfrak{K}$, on dit souvent que $\mathfrak{K}$ est non ramifié par rapport à K. Dans le nouveau corps $\mathfrak{K}$, à chaque idéal $\mathfrak{a}$ de K correspond un nombre α tel que $\mathfrak{a}$ soit formé par ceux des nombres de K qui sont divisibles par α dans le corps $\mathfrak{K}$.

C'est *D. Hilbert*[196]) qui a étendu cette notion à un corps K quelconque de nombres algébriques. Le *corps de classe* $\mathfrak{K}$ est alors défini comme comprenant tous les corps relatifs non ramifiés par rapport à K: il est encore relativement abélien et son degré est encore égal au nombre des classes de K, mais avec une définition plus étroite de l'équivalence [voir la fin du nº **30**]. Il jouit aussi de cette propriété fondamentale de renfermer des nombres correspondant à tous les idéaux de K. Ce corps de classes dont l'existence avait été ainsi établie par *D. Hilbert* a été formé d'une manière effective et étudié par *Ph. Furtwängler*[197]) et par *F. Bernstein*[197]). Dans le cas primitif où K est quadratique, il est bien identique[198]) au corps de classes considéré tout à l'heure.

Bien entendu, les nombres entiers du corps de classes $\mathfrak{K}$ ne forment pas de domaine holoïde complet; au contraire $\mathfrak{K}$ introduit des idéaux qui lui sont propres, et en lesquels les idéaux de K sont décomposables: le nombre des facteurs se trouve être le même pour deux idéaux équivalents (au sens restreint) de K.

55. Représentation des diviseurs des fonctions algébriques par adjonction de fonctions transcendantes. Fonctions premières. Formes premières. Si maintenant K est un corps de *fonctions algébriques* d'une variable, considérées sur une surface de Riemann (R),

195) *L. Kronecker,* Monatsb. Akad. Berlin 1857, p. 455; *H. Weber,* Elliptische Funktionen und algebraische Zahlen, Brunswick 1891, 3ième partie, surtout § 110, p. 438; Math. Ann. 48 (1897), p. 433; 49 (1897), p. 83; 50 (1898), p. 1.

196) Nachr. Ges. Gött. 1898, p. 370.

197) *Ph. Furtwängler,* Nachr. Ges. Gött. 1903, p. 203, 282; id. 1904, p. 173; *F. Bernstein,* Nachr. Ges. Gött. 1903, p. 46, 304.

198) *R. Fueter,* Diss. Göttingue 1903; J. reine angew. Math. 132 (1907), p. 255.

la théorie des intégrales abéliennes fournit le moyen de représenter les diviseurs [n^os **33**, **34**] de K[199].

Désignons par x la variable indépendante. Soit y la fonction algébrique de x qui, adjointe au corps R, a donné naissance au corps K. Si p est le *genre* de la surface de Riemann (R) sur laquelle on considère les fonctions algébriques du corps K, et si

$$(1) \qquad (x', y'),\ (a_1, b_1),\ (a_2, b_2),\ \ldots,\ (a_p, b_p)$$

représentent $p+1$ points de cette surface, on peut toujours déterminer une infinité de fonctions rationnelles de x, y et de x', y' qui, envisagées comme des fonctions du point x, y, admettent, aux $p+1$ points (1), des infinis algébriques d'ordre 1 [elles sont donc elles-mêmes d'ordre -1 [n° **33**] en chacun de ces $p+1$ points] et qui sont finies[200]) en tout autre point de la surface (R).

Si l'on représente par

$$F(x, y;\ x', y')$$

l'une de ces fonctions rationnelles, toutes ces fonctions rationnelles s'obtiendront en remplaçant dans l'expression

$$A \cdot F(x, y;\ x', y') + B$$

A et B par des fonctions rationnelles quelconques de x', y' indépendantes de x, y.

Si l'on choisit A et B de façon à ce que $AF + B$ ait comme résidu 1 pour le pôle $x = x'$, $y = y'$, et comme valeur 0 pour un point donné $x = a_0$, $y = b_0$, on obtient la fonction rationnelle de x, y, x', y' que *K. Weierstrass* désigne par[201])

$$H(x, y;\ x', y').$$

Si le point (x', y') décrit sur (R) une courbe quelconque, indépendante de (x, y), joignant le point (x_ν', y_ν') au point (x_ν, y_ν), la fonction

$$E(x, y;\ x_\nu, y_\nu;\ x_\nu', y_\nu') = e^W, \text{ où } W = \int_{(x_\nu', y_\nu')}^{(x_\nu, y_\nu)} H(x, y;\ x', y')\,dx',$$

est une fonction *univoque* du point (x, y) qui

199) Voir *K. Weierstrass,* Vorles. über die Abel'schen Transcendenten (Leçons sur les transcendantes abéliennes professées en 1875/6 à l'Université de Berlin) chap. 19; Werke 4, Berlin 1902, p. 377/93; *K. Hensel* et *G. Landsberg,* Alg. Funkt.[132]), p. 659/64. Voir aussi *G. Landsberg,* Jahresb. deutsch. Math.-Ver. 14 (1905), p. 97.

200) $_*$*K. Weierstrass,* Abelschen Transc.[199]); Werke 4, p. 64/8.*

201) $_*$Id. p. 73.*

1°) admet en (a_1, b_1), (a_2, b_2), $\ldots$, (a_p, b_p) des singularités essentielles,

2°) admet en (x_ν, y_ν) un zéro du premier ordre,

3°) admet en (x_ν', y_ν') un pôle simple (infini du premier ordre).

K. Weierstrass[202]) a désigné ces fonctions E sous le nom de *fonctions transcendantes premières (Primfunktionen).*

Toute fonction du corps K qui s'annule en r points, et devient donc aussi infinie en r points, peut être représentée par un produit de r fonctions transcendantes premières. Les fonctions E jouent donc dans la théorie des fonctions algébriques le même rôle que jouent les fonctions linéaires (entières et fractionnaires) dans la théorie des fonctions rationnelles. Elles représentent les diviseurs algébriques fractionnaires de la forme $\mathfrak{p}\mathfrak{q}^{-1}$, où $\mathfrak{p}$ et $\mathfrak{q}$ sont des diviseurs premiers[203]).*

A cette représentation due à *K. Weierstrass* du *quotient* de deux diviseurs premiers, *F. Klein* a joint une représentation des diviseurs premiers ou idéaux premiers eux-mêmes. A cet effet, il fait usage d'une *forme première*, homogène par rapport à deux variables x_1, x_2, dont le quotient est égal à la variable indépendante primitive x'.

Soient (x, y), (x', y'), (ξ, η), (ξ', η') des points de la surface (R) et

$$P_{x\,x'}^{\xi\,\xi'} = P_{\xi\,\xi'}^{x\,x'}$$

une intégrale de troisième espèce aux arguments x, x' et aux paramètres ξ, ξ', admettant l'échange du paramètre et de l'argument; supposons que la surface de Riemann soit une surface *canonique* sur laquelle existe une forme homogène algébrique entière $G(x_1, x_2)$ [n° **40**] ne s'annulant qu'aux points de ramification et soit

$$\frac{x_1\,dx_2 - x_2\,dx_1}{G(x_1, x_2)} = d\xi_x.$$

La forme première de *F. Klein* sera alors

$$P(x, x') = \lim \sqrt{-\,d\xi_x d\xi_{x'} e^{-P_{x,\,x'}^{x+dx,\,x'+dx'}}} \qquad (\lim dx = \lim dx' = 0).$$

C'est une quantité (transcendante) homogène et du premier degré en x_1, x_2 ainsi qu'en x_1', x_2' qui a un zéro du premier ordre pour $x = x'$, $y = y'$. Contrairement à celle de *K. Weierstrass,* elle n'a pas de singularité, mais se multiplie, lorsque la variable décrit des contours fermés, par des facteurs exponentiels transcendants. Ceux-ci peuvent être compensés par l'introduction de *formes intermédiaires*[204]).

202) $_*$Abelschen Transc.[199]); Werke 4, p. 377/93, en partic. p. 387.*

203) $_*$*K. Weierstrass,* Werke 2, Berlin 1895, p. 235; *A. Brill* et *M. Nöther,* Jahresb. deutsch. Math.-Ver. 3 (1892/3), éd. Berlin 1894, p. 428 (Texte et notes 200 à 203 de *J. Kürschák*).*

204) *F. Klein,* Math. Ann. 36 (1890), p. 1; Ellipt. Modulfunct.[153]) 2, p. 502/6; *E. Ritter,* Math. Ann. 44 (1894), p. 261.

Systèmes modulaires.

56. Modules. Les considérations précédentes sont, à plusieurs points de vue, en relation avec la notion de *module,* généralisation naturelle de la notion de divisibilité.

*D'une manière générale, soit considérée une catégorie d'entités mathématiques à l'intérieur de laquelle l'addition et la soustraction peuvent être définies. On pourrait dire qu'un ensemble pris dans cette classe constitue un module, si la différence de deux éléments quelconques de cet ensemble appartiennent au même ensemble. Ce n'est toutefois pas cette définition qui a été adoptée dans tous les cas.

Pour un ensemble de *nombres,* on dit, il est vrai, avec *R. Dedekind*[205]) que cet ensemble constitue un *module* si la différence de deux nombres quelconques de l'ensemble appartient au même ensemble. Un élément qui appartient à un module est dit encore *divisible* par ce module.

De cette définition du module, il résulte

1°) que chaque module contient comme élément le nombre 0;

2°) que la somme de deux éléments du module appartient au module

3°) que le produit d'un élément du module par un nombre rationnel entier appartient au module.

On peut donc dire qu'un ensemble de nombres constitue un module lorsque les nombres de cet ensemble se reproduisent par addition, par soustraction et quand on les multiplie par un nombre rationnel entier quelconque.

Un cas particulier important est celui des modules *finis.* On entend par là les modules dont tous les éléments sont des sommes de multiples de n éléments fondamentaux

$$\alpha_1, \alpha_2, \ldots, \alpha_n;$$

205) *R. Dedekind* dans *G. Lejeune Dirichlet,* Zahlenth.[9]), (4ᵉ éd.) p. 493, (Suppl. XI, n° 168); Bull. sc. math. (2) 1 (1877), p. 18.

On peut également former, avec des nombres entiers rationnels, des *modules additifs* à l'intérieur desquels l'addition, mais non la soustraction, est possible et qui ont des propriétés toutes différentes des modules ordinaires. De tels *modules additifs* se présentent, dans la théorie des fonctions algébriques d'une variable, lorsqu'on étudie les fonctions d'un même corps qui n'ont qu'un pôle. Les ordres de cet unique pôle pour ces diverses fonctions forment un *module additif. K. Weierstrass,* Abelschen Transc.[199]); Werke 4, p. 211/25 (chap. 9); *K. Hensel* et *G. Landsberg,* Alg. Funkt.[132]), p. 493; *M. Haure,* Ann. Ec. Norm. (3) 13 (1896), p. 115.

ces n éléments forment la *base* du module. On peut dire aussi que les modules *finis* sont ceux dont tous les éléments peuvent se mettre sous la forme

$$\lambda_1\alpha_1 + \lambda_2\alpha_2 + \cdots + \lambda_n\alpha_n,$$

$\lambda_1, \lambda_2, \ldots, \lambda_n$ étant des nombres entiers rationnels[206]). Un module fini est dit *module à n paramètres* (*n-gliedriger Modul*) lorsque le nombre des éléments de la base de ce module est égal à n.

R. Dedekind et *H. Weber*[207]) disent qu'un ensemble de *fonctions* constitue un *module,* lorsque ces fonctions se reproduisent par addition, par soustraction et quand on les multiplie par une fonction rationnelle entière quelconque.

Ainsi, contrairement à la définition générale qu'on aurait pu donner des modules, l'ensemble des fonctions linéaires d'une variable x n'est pas un module, quoique la somme et la différence de deux fonctions linéaires de x soient manifestement des fonctions linéaires de x.

Un module de fonctions est *fini* lorsqu'il contient n éléments fondamentaux $\alpha_1, \alpha_2, \ldots, \alpha_n$ tels que chacun de ses éléments s'exprime sous la forme

$$\lambda_1\alpha_1 + \lambda_2\alpha_2 + \cdots + \lambda_n\alpha_n,$$

où $\lambda_1, \lambda_2, \ldots, \lambda_n$ sont des fonctions rationnelles entières.

[Dans l'arithmético-algèbre on devra évidemment n'entendre ici par fonctions rationnelles entières que celles dont les coefficients sont des nombres entiers].

Quoique la plupart des résultats de ce numéro et du numéro suivant s'étendent sans peine aux modules de fonctions algébriques, nous nous bornerons dans ces deux numéros au cas des modules de nombres algébriques.

Un module $\mathfrak{a}$ est dit divisible par un module $\mathfrak{b}$ si tous les éléments de $\mathfrak{a}$ appartiennent à $\mathfrak{b}$: on dit aussi que $\mathfrak{b}$ est *contenu* dans $\mathfrak{a}$. Deux modules $\mathfrak{a}$ et $\mathfrak{b}$ ont un *plus grand commun diviseur* $\mathfrak{d}$. Il est défini comme contenant la somme ou la différence d'un élément quelconque de $\mathfrak{a}$ avec un élément quelconque de $\mathfrak{b}$. On désignera[208]), le plus p. g. c. d. $\mathfrak{d}$ de $\mathfrak{a}$ et $\mathfrak{b}$ par le symbole

$$\mathfrak{d} = (\mathfrak{a}, \mathfrak{b})$$

206) *R. Dedekind* dans *G. Lejeune Dirichlet,* Zahlenth.[9]), (4ᵉ éd.) p. 494 (Suppl. XI, n° 168); Bull. sc. math. (2) 1 (1877), p. 23.

R. Dedekind [Nachr. Ges. Gött. 1895, p. 183] a aussi considéré le cas où $\lambda_1, \lambda_2, \ldots, \lambda_n$ pourraient être choisis parmi tous les entiers d'un corps.

207) *J. reine angew. Math. 92 (1882), p. 195.*

208) *C'est la notation adoptée par *E. Steinitz,* Math. Ann. 52 (1899), p. 8.*

ou encore, avec *R. Dedekind,* par le symbole

$$\mathfrak{d} = \mathfrak{a} + \mathfrak{b}.$$

Deux modules $\mathfrak{a}$ et $\mathfrak{b}$ ont un plus petit commun multiple $\mathfrak{m}$. Il est défini comme formé par les éléments communs à $\mathfrak{a}$ et à $\mathfrak{b}$. On désignera le plus petit commun multiple $\mathfrak{m}$ de $\mathfrak{a}$ et $\mathfrak{b}$, avec *E. Steinitz*[208]), par le symbole

$$\mathfrak{m} = [\mathfrak{a}, \mathfrak{b}]$$

ou, avec *R. Dedekind,* par le symbole

$$\mathfrak{m} = \mathfrak{a} - \mathfrak{b}.$$

En multipliant chaque élément de $\mathfrak{a}$ par chaque élément de $\mathfrak{b}$ et additionnant entre eux les produits ainsi obtenus on obtient les éléments d'un module auquel on a donné le nom de *produit* des deux modules $\mathfrak{a}$ et $\mathfrak{b}$. On étend immédiatement cette définition au produit d'un nombre quelconque de modules. La multiplication des modules est associative et commutative. Un produit de modules égaux à $\mathfrak{a}$ est désigné sous le nom de *puissance* de $\mathfrak{a}$.

Si $\mathfrak{b}$ est un module à un terme, de base p, on convient d'écrire au lieu de $\mathfrak{a}\mathfrak{b}$, soit $\mathfrak{a}p$, soit $p\mathfrak{a}$. On obtient les éléments de $p\mathfrak{a}$ en multipliant par p chaque élément de $\mathfrak{a}$.

On peut aussi parler du *quotient* de $\mathfrak{a}$ par $\mathfrak{b}$: c'est le module $\mathfrak{c}$ formé par tous les éléments p tels que $p\mathfrak{a}$ soit divisible par $\mathfrak{b}$. On voit que $\mathfrak{c}\mathfrak{b}$ est un multiple de $\mathfrak{a}$: il peut d'ailleurs être égal à $\mathfrak{a}$ ou différent de $\mathfrak{a}$.

R. Dedekind[209]) considère en particulier le quotient

$$\mathfrak{a}^0 = \frac{\mathfrak{a}}{\mathfrak{a}},$$

qu'il appelle l'*ordre du module* $\mathfrak{a}$. Si deux nombres α, β appartiennent à $\mathfrak{a}^0$, il en est de même du produit $\alpha\beta$. Le module $\mathfrak{a}^0$ est donc [n° **15**] un domaine holoïde (de König). Si $\mathfrak{a}$ est fini, son ordre $\mathfrak{a}^0$ est un module fini composé de nombres tous entiers. Dans la terminologie de *L. Kronecker* $\mathfrak{a}^0$ est donc une espèce, dans celle de *D. Hilbert* un anneau [n° **22**].

On a d'ailleurs

$$\mathfrak{a}\mathfrak{a}^0 = \mathfrak{a},$$

mais si l'on désigne par $\mathfrak{a}^{-m}$ le quotient

$$\mathfrak{a}^{-m} = \frac{\mathfrak{a}^0}{\mathfrak{a}^m},$$

209) *R. Dedekind* dans *G. Lejeune Dirichlet,* Zahlenth.[9]), (4e éd.) p. 505 (Suppl. XI, n° 170).

on n'a pas nécessairement

$$\mathfrak{a}\mathfrak{a}^{-1} = \mathfrak{a}^0.$$

Si cette égalité est vérifiée, le module $\mathfrak{a}$ est dit un *module propre* (*eigentlicher Modul*). C'est dans le cas des modules propres ayant le même ordre que les lois de la division sont entièrement analogues à ce qu'elles sont pour les nombres ordinaires. Ainsi pour tout entier rationnel m ou n on a

$$\frac{\mathfrak{a}^m}{\mathfrak{a}^n} = \mathfrak{a}^{m-n}, \quad \frac{\mathfrak{a}^m}{\mathfrak{b}^m} = \left(\frac{\mathfrak{a}}{\mathfrak{b}}\right)^m.$$

Les définitions du p. g. c. d. et du p. p. c. m. s'étendent aisément au cas où l'on envisage plus de deux modules. Les opérations $(\mathfrak{a}, \mathfrak{b})$ et $[\mathfrak{a}, \mathfrak{b}]$ sont alors non seulement commutatives, mais aussi associatives.

57. Classes suivant un module. Applications. Deux nombres sont *congrus*[210]) suivant un module si leur différence est divisible par ce module. Tous les éléments d'un module $\mathfrak{a}$ qui sont congrus entre eux relativement à un module $\mathfrak{b}$ sont dits constituer une *classe* suivant le module $\mathfrak{b}$. Un cas important est celui de deux modules $\mathfrak{a}$, $\mathfrak{b}$ liés de telle sorte que $\mathfrak{a}$ est séparable en un nombre fini s de classes suivant le module $\mathfrak{b}$. *R. Dedekind* représente le nombre s par le symbole $(\mathfrak{a}, \mathfrak{b})$ qu'il importe de ne pas confondre avec le symbole $(\mathfrak{a}, \mathfrak{b})$ de *E. Steinitz* représentant le p. g. c. d. de $\mathfrak{a}$ et $\mathfrak{b}$ dont on a parlé au n° **56**.

Si, dans chacune des s classes, on choisit un élément comme le *représentant* de la classe, on obtient s éléments dont l'ensemble équivaut, suivant le module $\mathfrak{b}$, à l'ensemble de tous les éléments possibles. L'ensemble de ces s éléments est ce qu'on appelle un *système complet de restes* suivant le module $\mathfrak{b}$. Si, par exemple, $\mathfrak{a}$ est l'ensemble de tous les nombres rationnels entiers et $\mathfrak{b}$ l'ensemble des multiples de n, on a $s = n$ et les nombres $0, 1, 2, \ldots, n-1$ forment un système complet de restes.

On a vu [n° **26**] qu'un idéal est nécessairement un module et un module fini (dont le nombre de paramètres est le degré n du corps): c'est sur cette base que repose, principalement sous la dernière forme[211]), la théorie des idéaux de *R. Dedekind.*

De ce qu'un entier η d'un corps numérique K est défini, à l'aide de la base

$$(\xi_1, \xi_2, \ldots, \xi_n)$$

des nombres entiers du corps et de n entiers rationnels ordinaires

210) *R. Dedekind* dans *G. Lejeune Dirichlet,* Zahlenth.[9]), (4e éd.) p. 508 (Suppl. XI, n° 171); Bull. sc. math. (2) 1 (1877), p. 20.

211) *R. Dedekind*[210]), p. 550/4 (Suppl. XI, n° 177).

$u_1, u_2, \ldots, u_n$, par l'expression

$$(1) \qquad \eta = u_1 \xi_1 + u_2 \xi_2 + \cdots + u_n \xi_n,$$

on conclut que chaque module $\mathfrak{a}$ formé à l'aide de nombres entiers de K est nécessairement *fini*, et que le nombre r de ses paramètres est au plus égal à n.

Si $(\alpha_1, \alpha_2, \ldots, \alpha_r)$ constitue la base d'un tel module $\mathfrak{a}$ et si

$$\alpha_i = a_{i1}\xi_1 + a_{i2}\xi_2 + \cdots + a_{in}\xi_n \qquad (i = 1, 2, \ldots, r),$$

la matrice

$$A = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ . & . & . & . \\ a_{r1} & a_{r2} & \ldots & a_{rn} \end{pmatrix}$$

jouit de la propriété que la condition nécessaire et suffisante pour qu'un nombre η appartienne au module $\mathfrak{a}$ est que l'on puisse déterminer r nombres rationnels entiers $\nu_1, \nu_2, \ldots, \nu_r$ tels que les $u_1, u_2, \ldots u_r$ qui figurent dans l'expression (1) de η s'expriment sous la forme

$$u_j = a_{1j}\nu_1 + a_{2j}\nu_2 + \cdots + a_{rj}\nu_r \qquad (j = 1, 2, \ldots, n).$$

D'autre part, si $\mathfrak{b}$ est un second module de la même catégorie, correspondant à une matrice B à r' lignes, et si $\mathfrak{a}$ est divisible par $\mathfrak{b}$, les matrices A et B ont aussi entre elles une relation de divisibilité. Il faut, en particulier, qu'il existe une matrice C à r lignes et r' colonnes telle que l'on ait

$$a_{ij} = c_{i1}b_{1j} + c_{i2}b_{2j} + \cdots + c_{ir'}b_{r'j} \qquad (i = 1, 2, \ldots, r;\ j = 1, 2, \ldots, n),$$

les a, b, c étant respectivement des éléments de A, B, C. La théorie des modules est donc liée à celle des formes linéaires à coefficients entiers développée par *G. Frobenius* [I 15]; les résultats concernant la théorie des modules que l'on peut déduire de ceux de *G. Frobenius* ont été établis par *E. Steinitz*[212]).

Si le nombre r des paramètres du module envisagé $\mathfrak{a}$ est égal à n et si $\mathfrak{o}$ est l'ordre principal (ou l'espèce principale) [n° **22**] formé par tous les entiers du corps K, le nombre des classes de $\mathfrak{o}$ suivant ce module $\mathfrak{a}$ est fini et $(\mathfrak{o}, \mathfrak{a})$ est égal au déterminant de la matrice A: c'est à cette proposition que l'on a donné le nom de *theorème sur la norme d'un idéal* [n° **29**].

La proposition fondamentale d'après laquelle *tout idéal* $\mathfrak{a}$ *divisible par un idéal* $\mathfrak{b}$ est le produit de l'idéal $\mathfrak{b}$ par un troisième idéal $\mathfrak{C}$

212) *G. Frobenius,* J. reine angew. Math. 86 (1879), p. 146; 88 (1880), p. 96; *E. Steinitz,* Math. Ann. 52 (1899), p. 1.

a été ramenée par *R. Dedekind*[213]) à ce fait qu'un idéal est un module *propre,* dont l'ordre est $\mathfrak{o}$.

58. Systèmes modulaires. Laissant de côté les modules de nombres ou de fonctions algébriques, nous allons, à partir d'à présent, considérer des modules finis dont les éléments sont des polynomes entiers à n variables indépendantes $x_1, x_2, \ldots, x_n$.

Soient donc

$$M_1, M_2, \ldots, M_k$$

des polynomes donnés en nombre *fini*. Envisageons l'ensemble des polynomes M qui peuvent se mettre sous la forme

$$(1) \qquad M = X_1 M_1 + X_2 M_2 + \cdots + X_k M_k$$

(les X étant des polynomes entiers). On dit, avec *L. Kronecker*[214]), que chaque polynome M *contient* le *système de polynomes*

$$(M_1, M_2, \ldots, M_k)$$

ou est *divisible* par ce système. Et l'on donne à ce système le nom de *système modulaire* ou de *système de diviseurs.*

Gy. (J.) König[215]) désigne sous le nom *d'équation linéaire de Diophante,* toute équation (1) dans laquelle $M, M_1, M_2, \ldots, M_k$ sont des polynomes donnés et $X_1, X_2, \ldots, X_k$ des polynomes inconnus, à déterminer de façon que l'équation (1) soit vérifiée.

[Au point de vue de l'algèbre pure, quand on étudie les conditions de divisibilité d'un polynome M par un système de modules $(M_1, M_2, \ldots, M_k)$ donné, aucune condition n'est imposée aux coefficients des polynomes X: c'est ce qu'on peut appeler *divisibilité de première espèce.* Au contraire, au point de vue de *L. Kronecker,* il y a lieu d'imposer à ces coefficients la condition (que l'on suppose vérifiée par les coefficients des M) d'être rationnels entiers (ou encore celle d'appartenir à un domaine holoïde déterminé): c'est ce qu'on peut appeler la *divisibilité de seconde espèce.*

Gy. (J.) König[215]) qui a étudié d'une façon approfondie les systèmes modulaires en se plaçant soit au point de vue de l'algèbre

213) *R. Dedekind* dans *G. Lejeune Dirichlet,* Zahlenth.[9]), (4e éd.) p. 553 (Suppl. XI, n° 177).

214) *L. Kronecker,* Festschrift[1]), § 20; J. reine angew. Math. 92 (1882), p. 70; Werke 2, p. 326; *J. Molk,* Thèse, Paris 1884; Acta math. 6 (1885), en partic. p. 52/3.

215) Alg. Grössen[10]), p. 347/460 (chap. 7 et 8).

Pour les systèmes modulaires dans lesquels les coefficients sont des entiers empruntés à un corps algébrique donné, voir *H. Hancock,* Thèse, Paris 1901 (2ième partie), p. 55 et suiv.

pure, soit au point de vue de *L. Kronecker*, donne à la théorie de la divisibilité de première espèce le nom de théorie *algébrique*, à celle de la divisibilité de seconde espèce (quand les coefficients sont rationnels entiers) le nom de théorie *arithmétique* des problèmes linéaires de Diophante. Les difficultés que l'on rencontre dans la théorie arithmétique sont bien plus grandes que celles que l'on rencontre dans la théorie algébrique. Dans le cas limite où $n = 0$, la théorie arithmétique se confond avec la théorie ordinaire des équations linéaires indéterminées].

Le système modulaire $(M_1, M_2, \ldots, M_k)$ *contient* le système $(N_1, N_2, \ldots, N_l)$ ou est *divisible* par le système $(N_1, N_2, \ldots, N_l)$ quand chacun des polynomes $M_1, M_2, \ldots, M_k$ contient le système $(N_1, N_2, \ldots, N_l)$. Deux systèmes modulaires dont chacun est divisible par l'autre ne sont pas regardés comme différents et sont dits *équivalents*. Pour représenter l'équivalence, *L. Kronecker* fait usage du symbole

$$\sim$$

Gy. (J.) König emploie le symbole

$$\simeq$$

et réserve le symbole $\sim$ pour indiquer que les polynomes du système $(M_1, M_2, \ldots, M_k)$ ont le même p. g. c. d. que les polynomes du système $(N_1, N_2, \ldots, N_l)$, ce qui n'implique pas nécessairement l'équivalence de ces deux systèmes. Nous indiquerons simplement ici l'équivalence de deux systèmes de modules par le signe d'égalité $=$.

Tous les systèmes de modules qui divisent $M = 1$ sont équivalents entre eux; nous représenterons chacun d'entre eux par le symbole 1. Conformément à cette convention on aura, par exemple,

$$(x + 1,\ x^2 + x + 1) = 1$$

puisque pour $X = -x$, $Y = 1$, on a

$$1 = (x + 1) X + (x^2 + x + 1) Y.$$

Conformément à la théorie générale des modules le p. g. c. d. des systèmes modulaires

$$\mathfrak{M} = (M_1, M_2, \ldots, M_k),$$
$$\mathfrak{N} = (N_1, \ldots, N_h)$$

est

$$(\mathfrak{M}, \mathfrak{N}) = (M_1, M_2, \ldots, M_k, N_1, N_2, \ldots, N_h)$$

et leur produit est

$$\mathfrak{M}\mathfrak{N} = (M_1 N_1,\ M_1 N_2,\ \ldots,\ M_1 N_h,\ M_2 N_1,\ \ldots,\ M_k N_h).$$

Le produit de deux systèmes modulaires est divisible par chacun d'eux; mais comme précédemment, du fait que $\mathfrak{P}$ est divisible par $\mathfrak{M}$, il ne

résulte pas nécessairement l'existence d'un module $\mathfrak{N}$ tel que

$$\mathfrak{P} = \mathfrak{M}\mathfrak{N}\ ^{216}).$$

Ainsi (x^2, y^2) contient le système de diviseurs (x, y) et cependant il n'y a pas de système de diviseurs $(M_1, M_2, \ldots, M_k)$ tel que l'on ait

$$(x^2, y^2) = (x, y) \cdot (M_1, M_2, \ldots, M_k).$$

59. Cas des fonctions transcendantes. La notion de divisibilité et, par suite, la théorie des modules s'étendent aux fonctions analytiques de plusieurs variables. Une série entière

$$\mathfrak{P}_1(x_1, x_2, \ldots, x_n)$$

est dite, d'après *K. Weierstrass*[217]), divisible par une autre série entière

$$\mathfrak{P}_0(x_1, x_2, \ldots, x_n)$$

lorsqu'elle peut être représentée par le produit de cette dernière et d'une série entière

$$\mathfrak{P}_2(x_1, x_2, \ldots, x_n).$$

Une condition nécessaire et suffisante pour qu'il en soit ainsi est que le quotient $\frac{\mathfrak{P}_1}{\mathfrak{P}_0}$ reste inférieur en valeur absolue à un nombre fixe, dans le voisinage du point $(0, 0, \ldots, 0)$.

Les *unités* sont, à ce point de vue, les séries entières dont le terme constant est différent de zéro. Toute série entière est, en ce même sens, *associée* [nº **18**] à une autre série qui est de degré fini par rapport à l'une des variables (autrement dit qui, par rapport à cette variable seule, est un polynome): c'est le célèbre lemme de *K. Weierstrass*[218]), qui en a fait la base de sa théorie des fonctions algébriques.

Ces considérations permettent[219]) d'étendre aux fonctions analytiques

$$\mathfrak{P}(x_1, x_2, \ldots, x_n)$$

les notions d'irréductibilité, de systèmes modulaires et les théorèmes qui s'y rapportent dus à *D. Hilbert* et à *M. Nöther*.

60. Notion de rang. Systèmes modulaires premiers. Une notion essentielle dans la théorie des systèmes modulaires est celle de

216) *L. Kronecker*, Festschrift ¹), § 20, 21; J. reine angew. Math. 92 (1882) p. 70/83; Werke 2, p. 326/42.

217) Abh. aus der Funktionenlehre, Berlin 1886, p. 107/28; Werke 2, Berlin 1895, p. 135/54.

218) Voir aussi *E. Picard*, Traité d'analyse, (1re éd.) 2, Paris 1893, p. 241/5; (2e éd.) 2, Paris 1905, p. 261/5; *E. Goursat*, Bull. Soc. math. France 36 (1908), p. 209.

219) *E. Lasker*, Math. Ann. 60 (1905), p. 85/105.

rang (*Stufe*). Tout système modulaire

$$\mathfrak{M} = (M_1, M_2, \ldots, M_k)$$

fournit un système d'*équations*, savoir

$$(1) \qquad M_1 = 0,\ M_2 = 0,\ \ldots,\ M_k = 0,$$

qui définit une *variété* ou une *multiplicité* algébrique contenue dans l'espace lieu du point $(x_1, x_2, \ldots, x_n)$.

Si les polynomes M_i sont *linéaires et homogènes*, le rang du système d'équations n'est autre que le rang de la matrice

$$\begin{pmatrix} \frac{\partial M_1}{\partial x_1}, & \frac{\partial M_1}{\partial x_2}, & \ldots, & \frac{\partial M_1}{\partial x_n} \\ \cdot & \cdot & \cdot & \cdot \\ \frac{\partial M_k}{\partial x_1}, & \frac{\partial M_k}{\partial x_2}, & \ldots, & \frac{\partial M_k}{\partial x_n} \end{pmatrix}$$

des coefficients, tel que l'introduit la théorie des déterminants (donc le plus haut degré des sous-déterminants normaux: voir I 2, **26**; I 9, **11**).

Nous nous placerons, dans ce qui va suivre, au seul point de vue de la divisibilité de première espèce. Dans ces conditions le rang d'un système modulaire sera par définition celui du système d'équations correspondant.

Ce rang peut être égal au nombre (minimé) k des polynomes fondamentaux et, par conséquent, des équations correspondantes; mais il est souvent moindre. C'est, par exemple, ce qui arrive d'une manière générale lorsque le système d'équations s'obtient en annulant tous les déterminants d'ordre r contenus dans une matrice dont le nombre de lignes et le nombre de colonnes sont donnés et dont les éléments sont des fonctions rationnelles et entières de n indéterminées: systèmes dont la théorie a été établie par *A. Cayley*, *G. Salmon*, *S. Roberts*, *A. Brill*[220]), tant au point de vue du rang ν qu'à celui de l'*ordre*, c'est-à-dire du nombre des points communs de la variété algébrique avec une variété linéaire arbitraire de $(n-\nu)^{\text{ième}}$ rang.

L'évaluation de cet ordre est aussi le but que s'est proposé *H. Schubert*[221]) dans son calcul énumératif; les résultats qu'il a obtenus demanderaient toutefois à être examinés à nouveau[222]).

220) *A. Cayley*, Cambr. Dublin math. J. 4 (1849), p. 132; Papers 1, Cambridge 1889, p. 457; *G. Salmon*, Lessons introductory to the modern higher algebra, (2ᵉ éd.) Dublin 1866; p. 228; (4ᵉ éd.) Dublin 1885; trad. par *O. Chemin*, Paris 1890; *S. Roberts*, J. reine angew. Math. 67 (1867), p. 266; *A. Brill*, Math. Ann. 5 (1872), p. 378; 36 (1890), p. 321. Voir encore *W. F. Meyer*, Verh. Ges. deutsch. Naturf. Ärzte 63, Brême 1890, éd. Leipzig 1891, p. 9.

221) Kalkül der abzählenden Geometrie, Leipzig 1879.

222) *Pour ce qui concerne les objections faites contre le *principe de la conservation du nombre* qui constitue la base des évaluations de *H. Schubert*, voir *G. Kohn*, Archiv Math. Phys. (3) 4 (1903), p. 312/6; *E. Study*, Verhandl. des 3ten internat. Math.-Kongresses Heidelberg 1904, publ. par *A. Krazer*, éd. Leipzig 1905, p. 388/95.*

La détermination effective du rang se fait par la théorie générale de l'élimination[223]) [I 9, nᵒˢ **69**, **70**] en formant les résolvants partiels complets du système d'équations

$$M_1 = 0,\ M_2 = 0,\ \ldots,\ M_k = 0$$

correspondant au système modulaire

$$(M_1, M_2, \ldots, M_k)$$

envisagé.

Soient

$$D_1, D_2, \ldots, D_\nu, \ldots, D_n$$

les résolvants partiels complets que l'on obtient ainsi successivement, comme il a été expliqué [I 9, **69**, **70**]. Lorsque parmi eux D_ν est

223) La théorie générale de l'élimination a été établie par *L. Kronecker* [Festschrift[1]), § 10; J. reine angew. Math. 92 (1882), p. 27; Werke 2, p. 275].

Quelques-uns des procédés dont il fait usage sont cependant d'origine plus ancienne. Ainsi l'introduction, dans cette théorie, de la quantité auxiliaire

$$x = u_1 x_1 + \cdots + u_n x_n,$$

où $u_1, u_2, \ldots, u_n$ désignent des indéterminées, remonte au moins à *S. D. Poisson* [J. Éc. polyt. (1) cah. 11 (an. X), p. 199] et *J. Liouville* [J. math. pures appl. (1) 12 (1847), p. 68]; *J. A. Serret* [Alg. sup.[38]) 1, p. 160] en a fait également usage. La quantité

$$x = u_1 x_1 + \cdots + u_n x_n$$

n'est d'ailleurs autre que le premier membre de l'équation

$$u_1 x_1 + \cdots + u_n x_n = 1$$

du point $(x_1, x_2, \ldots, x_n)$ en géométrie analytique.

La représentation d'une courbe algébrique à double courbure par *une seule* équation a, d'autre part, été donnée par *A. Cayley* [Quart. J. pure appl. math. 3 (1860), p. 225; Papers 4, Cambridge 1891, p. 446] qui s'est par là même singulièrement approché du point de vue auquel s'est plus tard placé *L. Kronecker*.

Mais, malgré ces essais partiels, c'est à *L. Kronecker* qu'est incontestablement dû le principe de la décomposition de variétés algébriques quelconques en *variétés simples* et celui de la décomposition des variétés simples en *variétés irréductibles*.

Au sujet de la théorie de l'élimination avant *L. Kronecker*, voir *J. A. Serret* [Alg. sup.[38]) 1, p. 143/220] et *F. Faà di Bruno* [Théorie générale de l'élimination, Paris 1859]. Les méthodes de *L. Kronecker* sont développées systématiquement par *J. Molk*, Thèse, Paris 1884; Acta math. 6 (1885), p. 1; *E. Netto* [Vorlesungen über Algebra 2, Leipzig 1900, p. 127/35; *E. Borel* et *J. Drach*, Introd. à l'étude de la théorie des nombres et de l'algèbre supérieure d'après des conférences de *J. Tannery*, Paris 1895, p. 218/25 et, avec des compléments sur la multiplicité des solutions, par *Gy.* (*J.*) *König*, Alg. Grössen[10]), p. 199/259.

le seul qui ne se réduise pas à une constante, on dit que

$$\mathfrak{M} = (M_1,\ M_2,\ \ldots,\ M_k)$$

est un système modulaire *simple* de rang ν.

Lorsque tous les résolvants partiels se réduisent à des constantes, le rang du système modulaire est égal à $n+1$.

Lorsque parmi les résolvants partiels, il y en a plusieurs

$$D_\nu,\ D_{\nu_1},\ \ldots$$

qui ne se réduisent pas à des constantes, on dit que le système de modules

$$\mathfrak{M} = (M_1,\ M_2,\ \ldots,\ M_k)$$

est un système *mixte* de rangs $\nu, \nu_1, \ldots$; parfois aussi on dit que ce système mixte est de rang ν, si ν est le plus petit des nombres $\nu, \nu_1, \ldots$ [cf. I 9, n° **69**].

La notion de rang une fois acquise, on peut, avec *L. Kronecker*, définir les systèmes modulaires premiers.

Un système modulaire est, suivant *L. Kronecker*, dit *premier* si tous les systèmes qu'il contient lui sont équivalents ou sont de rang supérieur (un tel système est, par conséquent, forcément simple).

Pour qu'un système modulaire soit premier il faut qu'il soit *irréductible* c'est-à-dire qu'il faut qu'il ne puisse être décomposé en deux systèmes modulaires chacun non équivalent à 1. Cette condition nécessaire n'est toutefois pas suffisante pour que le système modulaire soit premier[224]). Ainsi le système modulaire de rang 2

$$(x^2,\ y^2)$$

est irréductible sans être premier, car il contient le système de rang 2

$$(x,\ y).$$

La résolvante (unique) d'un système premier est irréductible, et la réciproque est vraie.

Un produit de facteurs ne peut être divisible par un système modulaire premier sans qu'un au moins des facteurs le soit. La propriété contraire est caractéristique des systèmes non premiers[225]). C'est pour cette raison que *Gy. (J.) König*[226]) a défini les systèmes

224) *L. Kronecker* lui-même avait [Festschrift[1]), § 21; J. reine angew. Math. 92 (1882), p. 78; Werke 2, Leipzig 1897, p. 336] primitivement confondu les notions de module premier et de module irréductible. Mais [J. reine angew. Math. 99 (1886), p. 337; Werke 3[1], Leipzig 1899, p. 158] il a été ensuite amené à les distinguer nettement comme nous l'avons fait dans le texte.

225) *L. Kronecker,* Sitzgsb. Akad. Berlin 1888, p. 453/8 (§ XII—XV).

226) Alg. Grössen[10]), p. 359/61.

de modules premiers, sans faire usage de la notion de rang, comme l'avait fait *L. Kronecker.*

D'après *Gy. (J.) König* un système de modules S est dit *premier* lorsqu'un produit $\mathfrak{A}\mathfrak{B}$ de deux systèmes de modules n'est divisible par S que quand un des deux systèmes $\mathfrak{A}$ ou $\mathfrak{B}$ au moins est divisible par S.

Dans l'exemple précédent, on voit immédiatement que (x^2, y^2) n'est pas premier, puisque $(x^2, y)\ (x, y^2)$ est divisible par (x^2, y^2) alors que ni (x^2, y), ni (x, y^2) ne sont divisibles par (x^2, y^2).

Soit S un système modulaire premier, de rang ν et T un système modulaire dont le (plus petit) rang est $\geqq \nu$, et qui soit tel que, si A désigne un polynome non divisible par S, le produit AF ne soit divisible par T que quand le polynome F est divisible par T. *E. Lasker*[227]) dit alors que T est un système modulaire *primaire* et que S est le système modulaire premier correspondant. Il démontre, pour les systèmes modulaires formés à l'aide de polynomes homogènes, que tout système modulaire peut être envisagé comme le p. p. c. m. des systèmes modulaires

$$T_1,\ T_2,\ \ldots,\ T_k,\ R,$$

où

$$T_1,\ T_2,\ \ldots,\ T_k$$

représentent des systèmes modulaires primaires, et où R est un système modulaire dont les polynomes n'ont aucun zéro commun.

61. Décomposition en systèmes premiers. Discriminant d'un système modulaire. Il y a lieu de se demander si un système modulaire donné est décomposable en un produit de facteurs premiers. Ceci n'est pas possible d'une manière entièrement générale, mais le devient moyennant certaines conditions, dont la plus importante est la suivante: supposons le système donné

$$\mathfrak{M} = (M_1,\ M_2,\ \ldots,\ M_k)$$

simple et de rang ν, et formons-en la résolvante

$$F(x;\ x_1,\ x_2,\ \ldots,\ x_{n-\nu}).$$

Le discriminant, par rapport à x, de cette résolvante est une fonction de $x_1, x_2, \ldots, x_{n-\nu}$ qui est dite le *discriminant du système modulaire*[228]) et dont l'évanouissement identique exprime la condition pour que les points multiples de la multiplicité (1) du n° **60** forment une multiplicité du même rang[229]).

227) Math. Ann. 60 (1905), p. 51.

228) *J. Molk,* Thèse, Paris 1884, (chap. 4); Acta math. 6 (1885), p. 79.

229) Le discriminant d'un système modulaire simple peut aussi être défini

Si le discriminant est différent de zéro, le système est décomposable en systèmes premiers et cette décomposition est entièrement parallèle à celle de la résolvante en facteurs premiers.

Quand le rang est égal à n, *E. H. Moore* a montré[230]) qu'on peut toujours (que le discriminant soit ou non différent de zéro) décomposer le système en produit de *systèmes simples*; un système simple est, dans sa terminologie, un système tel que les équations correspondantes n'ont qu'une seule solution commune.

Si le discriminant d'un système modulaire $\mathfrak{M}$ est nul, il y a toujours un polynome X dont une puissance est divisible par $\mathfrak{M}$ sans que X lui-même le soit.

Si au contraire, le discriminant n'est pas identiquement nul, il fournit, lorsqu'on l'égale à zéro, l'ensemble des valeurs de $x_1, x_2, \ldots, x_{n-\nu}$ auxquelles correspondent des points multiples de la variété (1). Cette *multiplicité* (ou *surface*) *discriminante*, ainsi formée par les points multiples, est située sur (1), mais de rang supérieur.

Dans le cas d'une équation du $n^{\text{ième}}$ degré à une inconnue et à $n+1$ coefficients indéterminés (les n racines étant regardées comme des fonctions de ces coefficients), *D. Hilbert*[231]) a étudié la multiplicité discriminante au point de vue de son ordre et de la nature de ses singularités; la signification de cette multiplicité au point de vue de la réalité des racines a été considérée par *L. Kronecker*[232]).

62. Applications. Nombres complexes à plusieurs unités. Si deux systèmes modulaires

$$\mathfrak{M} = (M_1, M_2, \ldots, M_k)$$

et

$$\mathfrak{M}' = (M_1', M_2', \ldots, M_k')$$

sont équivalents, les systèmes d'équations qu'ils fournissent sont équivalents, c'est-à-dire que toute solution de l'un (quelconque) d'entre eux est aussi solution de l'autre.

---

comme discriminant [I 9, **66**] de certains systèmes d'équations [cf. *L. Kronecker*, Sitzgsb. Akad. Berlin 1888, p. 451].

La notion de discriminant actuellement définie ne coïncide pas avec ce que l'on nomme en géométrie analytique le discriminant d'une courbe plane ou d'une surface; ce dernier est la fonction irréductible des coefficients dont l'évanouissement exprime l'existence de points multiples formant en général une multiplicité de rang *supérieur*.

230) Bull. Amer. math. Soc. 3 (1896/7), p. 372.

231) Math. Ann. 30 (1887), p. 437.

232) Monatsb. Akad. Berlin 1878, p. 95; Werke 2, Leipzig 1897, p. 39. Cf. *H. Weber*, Alg.[14]) 1, p. 299; trad. par *J. Griess* 1, p. 292.

La réciproque n'est pas exacte [cf. n° **64**]. Cependant, dans un certain nombre de cas intéressants où l'équivalence des systèmes d'équations est connue a priori, celle des systèmes modulaires a pu être établie. C'est ainsi que la condition pour que deux tableaux carrés de n^2 éléments soient réciproques s'exprime par l'un ou l'autre de deux systèmes de n^2 équations, et que l'on démontre[233]) l'équivalence des deux systèmes modulaires formés respectivement par les premiers membres de ces équations. Il en est de même[234]) pour les premiers membres des deux systèmes d'équations, au nombre de $\frac{n(n+1)}{2}$ chacun, qui expriment qu'un tableau de n^2 éléments est orthogonal.

Les conditions pour que deux polynomes du $n^{\text{ième}}$ degré en x, $P(x)$ et $Q(x)$, aient un p. g. c. d. $R(x)$ de degré m, et l'expression de ce p. g. c. d. $R(x)$, peuvent se mettre sous une forme telle que, lorsque les polynomes P et Q sont quelconques, R représente le p. g. c. d. de P et de Q suivant un certain système modulaire $\mathfrak{M}$, dont les éléments sont des fonctions entières des coefficients de P et de Q et, égalés à zéro, donnent les conditions d'existence du p. g. c. d. absolu[235]). L'avantage de cette manière d'opérer est que les propriétés ainsi établies du p. g. c. d. s'étendent d'elles-mêmes aux congruences suivant un système premier quelconque et donnent, par exemple, immédiatement la condition pour que deux polynomes en x à coefficients entiers aient un p. g. c. d. de degré m suivant un module premier p.

Un autre application des systèmes modulaires est l'obtention de tous les systèmes de nombres complexes à plusieurs unités principales [I 5] pour lesquels la multiplication est commutative.

Tout système modulaire simple $\mathfrak{M}$ à n variables, et qui est de rang n, admet un système de restes fini, c'est-à-dire qu'il existe ν polynomes $f_1, f_2, \ldots, f_\nu$ tels que tout autre polynome f aux variables données satisfasse, d'une manière et d'une seule, à la congruence

$$f \equiv c_0 + c_1 f_1 + \cdots + c_\nu f_\nu \pmod{\mathfrak{M}},$$

$c_0, c_1, \ldots, c_\nu$ étant des constantes.

---

233) *L. Kronecker*, J. reine angew. Math. 107 (1891), p. 254; *E. Netto*, id. 108 (1891), p. 144.

234) *L. Kronecker*, J. reine angew. Math. 107 (1891), p. 259.

235) *L. Kronecker*, J. reine angew. Math. 99 (1886), p. 329 (méthodes des séries récurrentes); Werke 3[1], Leipzig 1899, p. 147; *E. Netto*, J. reine angew. Math. 104 (1889), p. 321; id. 106 (1890), p. 81; Mitteil. math. Ges. Hamburg 2 (1890) [Festschrift], p. 36 pour la méthode d'élimination de *L. Euler*.

Comme, d'après cela, chacun des produits

$$f_g f_h \qquad (g, h = 1, 2, \ldots, \nu)$$

est aussi congru à une fonction linéaire de $f_1, f_2, \ldots, f_\nu$, on a ainsi, en remplaçant celles-ci par ν unités complexes $e_1, e_2, \ldots, e_\nu$ et les congruences par des égalités, un système de nombres complexes à $\nu + 1$ unités principales

$$1, e_1, e_2, \ldots, e_\nu$$

avec multiplication commutative.

Inversement, *L. Kronecker* a montré[236]) qu'un tel système de nombres complexes correspond toujours à un système modulaire de rang ν, à ν variables.

Les cas considérés antérieurement par *K. Weierstrass*[237]), *R. Dedekind*[238]), *J. Petersen*[239]) se rapportent à des systèmes modulaires de cette nature, dont le discriminant est différent de zéro.

63. Théorèmes de Hilbert. Un progrès important dans la théorie des systèmes modulaires a été obtenu par une série de théorèmes de *D. Hilbert*, qui résolvent la question de savoir si un ensemble donné d'un nombre infini de polynomes peut être ramené à un système modulaire. Établis en vue d'applications à la théorie des invariants, les théorèmes de *D. Hilbert* ne se rapportent, au moins sous leur forme primitive, qu'à des polynomes *homogènes*, et, dans ce qui va suivre, le mot *forme* désignera à nouveau, conformément à la terminologie habituelle, de tels polynomes. Cela posé, on a les trois théorèmes fondamentaux suivants:

I. Un système quelconque de formes (en général en nombre infini) étant donné, il existe un nombre fini *m d'entre elles,*

$$F_1, F_2, \ldots F_m,$$

telles que toute autre forme F du système puisse s'exprimer par une combinaison linéaire des précédentes

$$F = A_1 F_1 + A_2 F_2 + \cdots + A_m F_m,$$

où $A_1, A_2, \ldots, A_m$ sont des formes entières.

[Si les formes données sont à coefficients entiers, le théorème subsiste lorsqu'on assujettit $A_1, A_2, \ldots, A_m$ à vérifier cette même condition][240]).

Si, en modifiant la définition de *R. Dedekind*, on appelle *module* un ensemble de polynomes homogènes tel que le produit de l'un quelconque d'entre eux par un polynome homogène arbitraire et les sommes de pareils produits (pourvu qu'elles soient homogènes) soient aussi des polynomes appartenant à l'ensemble, on voit que tout «module» se ramène à un système modulaire, au sens précédent.

Une seconde conséquence du même théorème est la suivante:

Le système d'équations linéaires

$$(1) \qquad F_{i1} X_1 + F_{i2} X_2 + \cdots + F_{il} X_l = 0 \qquad (i = 1, 2, \ldots, m)$$

étant donné, système dans lequel les F_{ij} sont des formes données de $x_1, x_2, \ldots, x_n$ et $X_1, X_2, \ldots, X_l$ des formes inconnues, toutes les solutions de ce système (1) se déduisent d'un nombre fini d'entre elles

$$(2) \qquad X_1 = X_{1s}, \ X_2 = X_{2s}, \ldots, X_l = X_{ls} \qquad (s = 1, 2, \ldots, q)$$

par des combinaisons linéaires

$$(3) \qquad X_j = A_1 X_{j1} + A_2 X_{j2} + \cdots + A_q X_{jq} \qquad (j = 1, 2, \ldots, l).$$

On suppose naturellement que aucun des q systèmes (2) n'est une combinaison linéaire des $q - 1$ autres systèmes (2). Il peut cependant arriver qu'une même solution puisse se mettre de plusieurs façons différentes sous la forme (3): les conditions pour qu'il en soit ainsi font l'objet du théorème suivant:

II. Dans un système d'équations tel que (1), les conditions moyennant lesquelles une solution est susceptible de plusieurs représentations de la forme (3) conduisent à un second système de même nature

$$X_{j1} V_1 + \cdots + X_{jq} V_q = 0 \qquad (j = 1, 2, \ldots, l)$$

que l'on appelle *système dérivé* ou *syzygie* des solutions de (1); de ce système dérivé, on dérive de même un troisième système auquel on donne le nom de *second système dérivé* ou de *seconde syzygie* des solutions de (1); et ainsi de suite.

Cette suite d'opérations *est toujours limitée* et se termine au plus

236) Sitzgsb. Akad. Berlin 1888, p. 429, 447, 557, 595, 983.

237) Nachr. Ges. Gött. 1884, p. 395/414; Werke 2, Berlin 1895, p. 311/39. C'est un extrait de lettres adressées à *H. A. Schwarz*, datées des 19/27 juin 1883.

238) Nachr. Ges. Gött. 1885, p. 141/59; id. 1887, p. 1/7.

239) Id. 1887, p. 489/502.

240) *D. Hilbert*, Math. Ann. 36 (1890), p. 473. Démonstration simple (pour les formes homogènes ou non) par *Gy. (J.) König*, Alg. Grössen [10]) p. 366. Compléments par *P. Gordan*, Math. Ann. 42 (1893), p. 132; Nachr. Ges. Gött. 1899, p. 240. Voir aussi *E. Delassus*, Bull. sc. math. (2) 21 (1897), p. 59. Extension aux séries entières par *A. Capelli*, Rendic. Accad. Napoli (3) 2 (1896), p. 198/231 et par *E. Lasker*, Math. Ann. 60 (1905), p. 88.

tard au $n^{\text{ième}}$ système dérivé, lequel n'admet plus aucune solution. Autrement dit:

La suite des syzygies d'un système d'équations linéaires (1) est finie[241]).

D'après ce théorème on peut, parmi les formes d'un système modulaire $(F_1, F_2, \ldots, F_m)$, discerner celles qui sont représentables de plusieurs façons comme combinaisons linéaires de $F_1, F_2, \ldots, F_m$.

Grâce à cette circonstance, on peut calculer le nombre de conditions *indépendantes* auxquelles doivent satisfaire les coefficients d'une forme d'ordre R pour appartenir au système modulaire. Pour des valeurs suffisamment grandes de R, ce nombre est un polynome en R à coefficients numériques rationnels, que l'on nomme la *fonction caractéristique* du module, et que l'on désigne par $\chi(R)$.

Si n est le nombre des variables homogènes, ν le rang du système, enfin

$$d = n - \nu - 1$$

la dimension du domaine algébrique défini en égalant à zéro les fonctions du système, on a

$$\chi(R) = \chi_0 + \chi_1 \binom{R}{1} + \chi_2 \binom{R}{2} + \cdots + \chi_d \binom{R}{d}.$$

Dans cette formule $\binom{R}{s}$ est le coefficient binomial

$$\frac{R(R-1)\ldots(R-s+1)}{s!}$$

et $\chi_0, \chi_1, \chi_2, \ldots, \chi_d$ sont des entiers caractéristiques du système modulaire: χ_d, en particulier, est l'ordre de ce système, c'est-à-dire le nombre de ses intersections avec une multiplicité linéaire $n-1-d$ fois étendue; quant à $\chi_0, \chi_1, \chi_2, \ldots, \chi_{d-1}$, ils sont liés aux genres du domaine algébrique.

La fonction caractéristique est en relation avec les évaluations numériques essentielles de la géométrie analytique: par exemple, pour une courbe gauche algébrique C, sans point double, d'ordre m et de genre p, le nombre des conditions que doit remplir une surface d'ordre R pour contenir la courbe est

$$\chi(R) = -p + 1 + mR.$$

Si $\mathfrak{D}$ est le p. g. c. d. de deux modules $\mathfrak{A}, \mathfrak{B}$, et si $\mathfrak{M}$ est leur p. p. c. m., on a

$$\chi_{\mathfrak{A}}(X) + \chi_{\mathfrak{B}}(R) = \chi_{\mathfrak{D}}(R) + \chi_{\mathfrak{M}}(R).$$

241) *D. Hilbert*, Math. Ann. 36 (1890), p. 473.

Si $\mathfrak{A}$ et $\mathfrak{B}$ correspondent à deux courbes gauches sans points doubles C_m^p, $C_{m'}^{p'}$ qui, par leur ensemble forment l'intersection complète de deux surfaces F_μ, $F'_{\mu'}$, le module $\mathfrak{D}$ est le système de toutes les surfaces qui passent par C, C'; $\mathfrak{M}$ est le système des surfaces qui passent par les points communs aux deux courbes et la relation précédente donne le nombre de ces points d'intersection, exprimé en fonction des deux ordres μ, μ' et des deux genres p, p'.

Si le domaine algébrique correspondant à un système modulaire

$$(F_1, F_2, \ldots, F_m)$$

est coupé par un autre, défini par les formes *générales*

$$\Phi_1, \Phi_2, \ldots, \Phi_q$$

des ordres respectifs $n_1, n_2, \ldots, n_q$, la fonction caractéristique $\chi_q(R)$ du domaine d'intersection s'exprime à l'aide de la fonction caractéristique $\chi(R)$ de module $(F_1, F_2, \ldots, F_m)$, savoir[242])

$$\chi_q(R) = \chi(R) - \sum_{i=1}^{i=q} \chi(R - n_i) + \sum_{\substack{i,k \\ (i<k)}} \chi(R - n_i - n_k)$$
$$- \sum_{\substack{i,k,l \\ (i<k<l)}} \chi(R - n_i - n_k - n_l) + \cdots.$$

III. Enfin une troisième proposition permet de décider en général des relations qui peuvent être établies entre deux systèmes modulaires lorsque les systèmes d'équations correspondants sont équivalents. Cette proposition est la suivante:

Soient

$$G, G', G'' \ldots$$

des polynomes homogènes quelconques en $x_1, x_2, \ldots, x_n$, nuls pour tout système de valeurs des variables qui annulent les fonctions de système modulaire

$$(F_1, F_2, \ldots, F_m);$$

il est possible de trouver un entier ϱ tel que tout produit $\Pi^{(\varrho)}$ de ϱ fonctions quelconques de la suite

$$G, G', G'', \ldots$$

242) *W. Wirtinger*, Untersuchungen über Thetafunctionen, Leipzig 1895, p. 19; *W. Wirtinger* détermine la fonction caractéristique $\chi(R)$ du domaine algébrique (généralisation de la *surface de Kummer*) que l'on obtient en considérant comme coordonnées homogènes dans l'espace à $2^p - 1$ dimensions 2^p fonctions Thêta linéairement indépendantes du second ordre de $v_1, v_2, \ldots, v_p$ ayant la caractéristique $\begin{Bmatrix} 0 \\ 0 \end{Bmatrix}$. On a

$$\chi(R) = 2^{p-1}(R^p + 1).$$

soit divisible par le système modulaire[243])

$$(F_1, F_2, \ldots, F_m).$$

Sur ces trois théorèmes fondamentaux, *D. Hilbert* fonde la démonstration de la limitation du nombre des invariants distincts d'un système de formes, celle de la limitation du nombre des syzygies irréductibles entre ces invariants, et les propriétés du corps des invariants.

64. Généralisation des notions de divisibilité et d'équivalence. Le troisième théorème de *D. Hilbert* montre que l'équivalence de deux systèmes d'équations n'entraîne pas sans restriction celle des deux systèmes modulaires formés par leurs premiers membres. C'est ce que *L. Kronecker* avait déjà constaté sur l'exemple suivant:

Soient

$$A_0, A_1, \ldots, A_r, B_0, B_1, \ldots, B_s$$

des polynomes quelconques (homogènes on non, cette fois) à plusieurs variables $x_1, x_2 \ldots, x_n$ et posons, en introduisant une indéterminée X,

$$(1)\qquad \begin{aligned}(A_0X^r + A_1X^{r-1} + \cdots + A_r)(B_0X^s + B_1X^{s-1} + \cdots + B_s)\\ = C_0X^{r+s} + C_1X^{r+s-1} + \cdots + C_{r+s};\end{aligned}$$

les $(r+1)(s+1)$ équations

$$A_0B_0 = A_0B_1 = \cdots = A_0B_{s-1} = A_1B_0 = \cdots = A_iB_k = \cdots = A_rB_s = 0$$

imposent aux variables $x_1, \ldots, x_n$ les mêmes conditions que les $r+s+1$ équations

$$C_0 = C_1 = \cdots = C_{r+s} = 0.$$

Si cependant on considère les systèmes modulaires correspondants

$$\mathfrak{A}\mathfrak{B} = (A_0, A_1, \ldots, A_r)(B_0, B_1, \ldots, B_s) = (A_iB_k)\begin{pmatrix} i = 0, 1, 2, \ldots, r \\ k = 0, 1, 2, \ldots, s\end{pmatrix}$$

et

$$\mathfrak{C} = (C_0, C_1, \ldots, C_{r+s}),$$

on peut seulement affirmer que $\mathfrak{C}$ est divisible par $\mathfrak{A}\mathfrak{B}$. Mais *L. Kronecker*[244]) complète cette proposition par la suivante:

243) *D. Hilbert,* Math. Ann. 42 (1893), p. 313.

Un cas particulier ($n = 3$) avait déjà été démontré par *E. Netto* [Acta math. 7 (1885/6), p. 101]. *E. Netto* détermine, dans ce cas, le nombre r comme étant la plus grande multiplicité des points d'intersection des courbes. Voir aussi *E. Netto,* Alg.[223]) 2, p. 121/6.

Démonstration simple dans *Gy. (J.) König,* Alg. Grössen[10]), p. 398; autre démonstration par *E. Lasker* [Math. Ann. 60 (1905), p. 56] avec extension aux séries [id. p. 95].

244) Sitzgsb. Akad. Berlin 1883, p. 957; Werke 2, Leipzig 1897, p. 417. Voir aussi *J. Molk,* Thèse, Paris 1884; Acta math. 6 (1885), p. 71 et suiv.

Moyennant l'équation (1), tout élément A_iB_k du système modulaire $\mathfrak{A}\mathfrak{B}$ est racine d'une équation

$$(2)\qquad V^m + G_1V^{m-1} + G_2V^{m-2} + \cdots + G_m = 0,$$

dont les coefficients $G_1, G_2, \ldots, G_m$ sont respectivement divisibles par les puissances successives

$$\mathfrak{C}, \mathfrak{C}^2, \ldots, \mathfrak{C}^m.$$

R. Dedekind avait, de son côté, obtenu, sous une forme un peu différente[245]), ce théorème qui permet d'établir d'une manière simple la théorie des idéaux[246]).

Gy. (J.) König[247]) a énoncé ce même théorème sous la forme que voici:

Il existe toujours un nombre fini de formes homogènes

$$H_1, H_2, \ldots, H_t, \ldots, H_\nu$$

de

$$A_0, A_1, \ldots, A_r;\ B_0, B_1, \ldots, B_s$$

et un nombre fini de formes homogènes linéaires

$$L^{(t)}_{ik\sigma}$$

de

$$C_0, C_1, \ldots, C_{r+s}$$

telles que l'on ait

$$H_tA_iB_k = L^{(t)}_{ik1}H_1 + L^{(t)}_{ik2}H_2 + \cdots + L^{(t)}_{ik\nu}H_\nu$$
$$(i = 0, 1, \ldots, r;\ k = 0, 1, \ldots, s;\ t = 1, 2, \ldots, \nu).$$

Si dans ces relations, i et k étant supposés fixes, on remplace t successivement par $1, 2, \ldots, \nu$, et qu'entre les ν équations ainsi obtenues on élimine les ν formes $H_1, H_2, \ldots, H_\nu$, on obtient effectivement le théorème de *L. Kronecker* sous sa forme primitive.

On peut étendre la notion de divisibilité en convenant de dire qu'une quantité V qui est racine d'une équation de la forme (2) est encore divisible par $\mathfrak{C}$, et moyennant cette extension, qui respecte d'ailleurs les propriétés fondamentales précédemment énoncées, le théorème de *L. Kronecker* rétablit l'équivalence des deux modules

$$\mathfrak{C},\quad \mathfrak{A}\mathfrak{B}.$$

Du théorème de *L. Kronecker*, *A. Hurwitz*[248]) a déduit la conséquence suivante:

245) Mitteilungen der Deutschen math. Gesellschaft in Prag 1892, éd. Vienne 1892, p. 1; Nachr. Ges. Gött. 1895, p. 106.

246) *Gy. (J.) König,* Alg. Grössen[10]), p. 474.

247) Alg. Grössen[10]), p. 74 et suiv.

248) Nachr. Ges. Gött. 1894, p. 291.

Si les A et les B sont des entiers algébriques et que

$$C_0, \ldots, C_{r+s}$$

soit divisibles par un entier ω, il en est de même de tous les produits

$$A_i B_k.$$

65. Théorème fondamental de Nöther. Le troisième théorème de *D. Hilbert* s'applique naturellement encore à des polynomes non homogènes. Si donc un polynome f s'annule pour chacune des solutions du système non homogène d'équations algébriques

$$\varphi_1 = 0,\ \varphi_2 = 0,\ \ldots,\ \varphi_m = 0,$$

les puissances de f, à partir d'un certain exposant ϱ, s'expriment linéairement en fonction de $\varphi_1, \varphi_2, \ldots, \varphi_m$. En général ϱ est toutefois ici > 1.

Prenons l'hypothèse où le rang ν du système est égal au nombre m des fonctions et aussi au nombre n des inconnues. Dans le cas plus spécial encore de deux variables x, y, cas où $n = \nu = 2$, l'énoncé des conditions nécessaires et suffisantes pour qu'un polynome qui s'annule pour toutes les solutions communes aux deux équations

$$\varphi = 0,\ \psi = 0$$

appartienne au module (φ, ψ), c'est-à-dire puisse se mettre sous la forme

$$f = A\varphi + B\psi, \tag{1}$$

constitue le célèbre théorème de *M. Nöther*[249]), généralisé depuis, au cas où la valeur commune de m, n, ν est supérieure à 2, par *Gy. (J.) König* et *F. Severi*[250]), puis étendu par *E. Lasker*[251]) aux séries entières [voir n° **59**].

M. Nöther montre [cf. I 9, **9**] que la conclusion est toujours légitime lorsque tous les points communs aux deux courbes

$$\varphi = 0,\ \psi = 0$$

sont simples. Si, d'autre part, (a, b) étant un quelconque de ces points

249) Math. Ann. 2 (1870), p. 314; plus rigoureusement Math. Ann. 6 (1873), p. 351. Voir aussi *E. Picard* et *G. Simart*, Théorie des fonctions algébriques de deux variables indépendantes 2, Paris 1906, p. 1/17 (tout le chapitre 1 est consacré à l'exposé du théorème de *M. Nöther*).

250) *Gy. (J.) König,* Alg. Grössen[10]), p. 385 et suiv.; *F. Severi,* Atti R. Accad. Lincei *Rendic.* mat. (5) 11 I (1902), p. 105.

251) *E. Lasker,* Math. Ann. 60 (1905), p. 85 et suiv.

communs (en général multiple), on écrit les conditions pour que l'équation (1) soit possible *au voisinage de ce point,* c'est-à-dire pour qu'elle puisse être vérifiée en posant pour A, B des développements ordonnés suivant les puissances de $x - a$, $y - b$ (conditions qui se réduisent à $f(a, b) = 0$ si la solution commune en question est simple), l'ensemble de ces conditions pour tous les points (a, b) donne les conditions nécessaires et suffisantes cherchées.

En particulier, $x = a$, $y = b$ étant pour la fonction φ un point i^{uple}, pour la fonction ψ un point k^{uple} à tangentes séparées, les conditions en ce point sont vérifiées d'elles-même si la fonction $f(x, y)$ y possède un point multiple d'ordre $i + k - 1$ au moins[252]).

Ce théorème est désigné sous le nom de *théorème fondamental* et est en effet tel pour la théorie des fonctions algébriques de *A. Brill* et *M. Nöther.*

Des travaux ultérieurs ont été consacrés à la simplification de la démonstration[253]) et à la recherche de la plus petite dimension jusqu'à laquelle en un point (a, b), il faille opérer la comparaison des coefficients. *E. Bertini*[254]) trouve pour ce nombre la valeur

$$\alpha' = (i + k - 2) + (\alpha - ik),$$

où α est le nombre, égal ou supérieur à ik, des intersections confondues en (a, b). Si donc φ et ψ n'ont aucune tangente commune en ce point, α' a la valeur

$$(i - 1) + (k - 1),$$

résultat qui a été étendu au cas de plus de deux variables[255]).

66. Divisibilité de seconde espèce. Systèmes modulaires de rang deux; leurs formes normales. Dans les recherches concernant la divisibilité de seconde espèce, on se borne généralement à envisager des systèmes de modules de la forme

$$(M_1(x),\ M_2(x),\ \ldots,\ M_n(x)),$$

où chaque élément $M_i(x)$ ne dépend que de la variable x. Le cas le plus important est celui où le p. g. c. d. des éléments $M_i(x)$ est

252) Voir *A. Clebsch,* Vorles. über Geometrie publ. par *F. Lindemann* 1, Leipzig 1876, p. 341; trad. *Ad. Benoist* 2, Paris 1880, p. 45.

253) *A. Voss,* Math. Ann. 27 (1886), p. 527; *M. Nöther,* Math. Ann. 30 (1887), p. 410; *L. Stickelberger,* Math. Ann. 30 (1887), p. 401; *A. Brill,* Math. Ann. 39 (1891), p. 129.

254) *E. Bertini,* Math Ann. 34 (1889), p. 447; Reale Ist. Lombardo *Rendic.* (2) 24 (1891), p. 1095; *M. Nöther,* Math. Ann. 40 (1892), p. 140

255) *Gy. (J.) König,* Alg. Grössen[10]), p. 394.

équivalent à 1; dans ce cas on dit que le système de modules envisagé est *simple*, de *rang* 2.

Lorsque le p. g. c. d. F des éléments $M_i(x)$ est un nombre différent de 0, 1 ou -1, et aussi lorsque ce p. g. c. d. F est une fonction rationnelle $F(x)$ d'une seule variable x, deux cas peuvent se présenter:

Ou bien F est divisible par le système de modules envisagé; ce système de modules est alors équivalent au module F et on lui donne le nom de système de modules *simple de rang* 1.

Ou bien F n'est pas divisible par le système de modules envisagé. Si alors on pose, pour chaque indice i,

$$M_i(x) = F \cdot A_i(x),$$

chaque $A_i(x)$ est encore une fonction rationnelle entière, à coefficients rationnels entiers, et le système de modules envisagé est équivalent au produit du module simple de rang 1

$$F$$

par le système de modules simple de rang 2

$$(A_1(x),\ A_2(x),\ \ldots,\ A_m(x)).$$

A chaque système de modules simple de rang 2 on peut d'ailleurs adjoindre un nombre p, convenablement choisi, sans modifier en rien, par cette adjonction, l'équivalence du système. On peut donc toujours supposer que chaque système de modules simple de rang 2 est donné sous la forme

$$\mathfrak{M} = (A_1(x),\ A_2(x),\ \ldots,\ A_m(x),\ p).$$

Le cas le plus simple est celui de p premier. Les fonctions $A_1(x), A_2(x), \ldots, A_m(x)$ peuvent alors être remplacées par une seule fonction, leur p. g. c. d. $M(x)$ suivant le module p, et l'on peut, dans ce cas, généraliser les lois ordinaires de la théorie des nombres, comme cela est fait à des points de vue divers, dans les travaux de *C. F. Gauss, J. A. Serret, Th. Schönemann, R. Dedekind*[256]). Un cas particulier important est celui où M est une fonction P irréductible suivant le module p; dans ce cas (et dans ce cas seulement) le système modulaire $(P,\ p)$ est *un système modulaire premier* [n° **58**].

Si p n'est pas premier, il s'agit, en premier lieu, de mettre le système modulaire $\mathfrak{M}$ sous une forme normale permettant de reconnaître, par de simples divisions, si une fonction entière donnée X à coefficients entiers est divisible par $\mathfrak{M}$ ou non. D'après *K. Hensel*

256) *C. F. Gauss*, Œuvre posth.; Werke 2, Göttingen 1876, p. 199. Voir aussi *J. A. Serret*, Alg. sup.[21]) 2, p. 122; *Th. Schönemann*, J. reine angew. Math. 31 (1846), p. 269; 32 (1846), p. 93; *R. Dedekind*, id. 54 (1857), p. 1.

et *G. Landsberg*[257]) on peut toujours obtenir la forme normale

$$\mathfrak{N} = (F_1,\ e_1F_2,\ e_2F_3,\ \ldots,\ e_{r-1}F_r,\ e_r)$$

dont les éléments sont caractérisés par les quatre propriétés suivantes:

1° Les premiers coefficients des F sont tous égaux à 1.

2° Leurs degrés $\gamma_1, \gamma_2, \ldots, \gamma_r$ forment une suite décroissante.

3° Chacun des nombres entiers e_ϱ divise le suivant $e_{\varrho+1}$ et lui est inférieur.

4° Pour chacun des indices $\varrho = 1, 2, \ldots, r-1$, où $r > 1$, la fonction F_ϱ est divisible par le système modulaire

$$\mathfrak{N}_\varrho = \left(F_{\varrho+1},\quad \frac{e_{\varrho+1}}{e_\varrho} F_{\varrho+2}, \ldots, \frac{e_{r-1}}{e_\varrho} F_r,\quad \frac{e_r}{e_\varrho}\right)$$

qui a également la forme normale.

Dans ces conditions, pour que le polynome X soit divisible par $\mathfrak{N}$, il doit, lorsqu'on le divise par F_1, donner un reste contenant e_1 en facteur, et la fonction X_1 obtenue par suppression de ce facteur doit être divisible par $\mathfrak{N}_1$; cette dernière divisibilité est de même ramenée à celle d'une certaine fonction X_2 par le système modulaire $\mathfrak{N}_1$, etc.

Toutes les questions simples relatives au système modulaire $\mathfrak{M}$ (systèmes contenus ou non dans $\mathfrak{M}$, nombre des fonctions distinctes suivant $\mathfrak{M}$) trouvent leur réponse grâce à la forme normale.

Le système $\mathfrak{M}$ peut être décomposé, d'une manière et d'une seule, en systèmes modulaires qu'on pourrait appeler *simples* (einfach) ou *primaires* (prim) si ces mots n'avaient pas déjà une autre signification. Un *système simple*, au nouveau sens du mot, serait alors caractérisé par ce fait qu'il n'est divisible que par un seul système modulaire premier, au sens précédemment indiqué. Toute fonction X divisible par chacun des *facteurs simples* de $\mathfrak{M}$, au nouveau sens du mot, serait divisible par $\mathfrak{M}$.

Ces résultats peuvent se transporter immédiatement au cas de systèmes modulaires de rang deux, composés de fonctions de deux variables, et où la divisibilité est de première espèce (de sorte qu'aucune

257) *K. Hensel*, J. reine angew. Math. 118 (1897), p. 234; 119 (1898), p. 114, 175; *G. Landsberg*, Nachr. Ges. Gött. 1897, p. 277; *L. Kronecker*, Zahlenth.[96]) p. 185/241 (leçons 16 à 20). Voir aussi *H. Hancock*, J. reine angew. Math. 119 (1898), p. 148; 122 (1900), p. 265; Thèse, Paris 1901, p. 36. Les recherches de *H. Hancock* se rattachent à la marche suivie par *L. Kronecker* qui avait cherché à obtenir le plus grand degré de généralité possible, mais n'a pas atteint le but qu'il s'était proposé.

restriction n'est imposée aux coefficients): il suffit de remplacer les mots *nombre entier* par *fonction entière de la deuxième variable* y et *nombre premier* par *facteur linéaire* $y - \beta$.

En transportant ainsi ces résultats aux systèmes de modules de rang 2, le dernier théorème que nous avons établi sur ces systèmes de modules de rang 2 nous fournit précisément le théorème de *M. Nöther.*

La divisibilité de seconde espèce des systèmes de modules dont les éléments dépendent de plus d'une variable a été, au moins dans le cas de deux, trois ou quatre variables, étudiée par *Gy. (J.) König*[258]) à qui l'on doit une méthode permettant de reconnaître si deux systèmes de modules quelconques, sont équivalents ou non.

**H. Hancock*[259]) discute les systèmes modulaires dans lesquels les coefficients sont des entiers d'un corps algébrique donné et étend, dans ce cas, aux systèmes modulaires premiers les théorèmes de *P. de Fermat* et de *J. Wilson.*

E. Lasker[260]) a étendu à la divisibilité de seconde espèce, non seulement son théorème fondamental [n° **60**] mais aussi la plupart de ses recherches sur les systèmes de modules.

Corps en général.

67. Corps premiers et domaines d'intégrité premiers. Extensions équivalentes. *La description de tous les types de corps possibles et de leurs relations réciproques que *E. Steinitz*[261]) a récemment formulée, contribue beaucoup à uniformiser nos connaissances sur la théorie des corps.

E. Steinitz envisage les corps au point de vue abstrait et général de *H. Weber* [n° **9**] en faisant complètement abstraction de la signification donnée à leurs éléments et en envisageant simultanément les domaines *orthoïdes* et les domaines *pseudo-orthoïdes.* Il est ainsi amené non seulement à généraliser les notions données au n° **7**, mais même parfois à les modifier.

Deux corps K et K′ sont de même type lorsqu'ils sont *identiques abstraitement parlant* [n° **9**]. *E. Steinitz* dit que les corps de même

258) Alg. Grössen[10]), p. 401/60.

259) **H. Hancock,* Thèse, Paris 1901, en partic. p. 104, 106.*

260) Math. Ann. 60 (1905), p. 59/84.

261) *J. reine angew. Math. 137 (1910), p. 167. Les numéros **67** à **81** sont entièrement dus à *J. Kürschák.**

type sont *isomorphes* et il appelle *isomorphisme* la correspondance qui a lieu entre leurs éléments.

Lorsqu'un corps L contient tous les éléments d'un corps K et que ces éléments s'ajoutent et se multiplient dans L comme dans K, on dit que K est un *sous-corps* de L et que L est un *corps supérieur* à K ou une *extension* de K. On convient de faire en général usage de ces mêmes expressions dans le cas limite où K et L sont identiques et de dire que K est un sous-corps *proprement dit* de L, que L est une *véritable* extension de K quand ce cas limite est exclu.

Quand un corps est à la fois un sous-corps de L et une extension de K, on dit qu'il est situé *entre* K et L.

Soit $\mathfrak{S}$ un système de sous-corps de K, en nombre fini ou infini. Les éléments, tels que *zéro* ou l'*unité absolue* par ex., qui figurent dans tous les corps du système $\mathfrak{S}$, forment un corps que l'on appelle l'*intersection* des corps de $\mathfrak{S}$.

Tout corps P qui n'a aucun sous-corps est dit *corps premier.* Un corps premier est ou bien du type de $\mathfrak{R}$ ou bien du type d'un des domaines pseudo-orthoïdes $\mathfrak{R}_p$ envisagés au n° **9**. Chaque corps K contient comme sous-corps un et un seul corps premier P, à savoir l'intersection de tous les sous-corps de K. Si ce corps premier P est du type de $\mathfrak{R}$, on dit que K et tous ses sous-corps ont comme *caractéristique zéro*; si le corps premier P est du type de $\mathfrak{R}_p$, on dit que K et tous ses sous-corps ont comme *caractéristique p.* Dans le cas des domaines orthoïdes la caractéristique est toujours *zéro,* dans le cas des domaines pseudo-orthoïdes elle n'est jamais *zéro.*

Envisageons un système U de corps, en nombre fini ou infini, tel que à deux corps quelconques K_1 et K_2 de ce système U corresponde au moins un corps K_3 qui les contienne tous deux (et fasse partie de U). On peut déterminer un corps K contenant tous les corps de U comme sous-corps et qui ne contienne pas d'autre élément que ceux qui figurent dans les corps de U. On dit que ce corps K, qui ne fait pas nécessairement partie de U, est le *plus petit multiple* des corps du système U.

Si par ex. U est le système de tous les genres [n° **7**] qui dérivent du corps $\mathfrak{R}$, le plus petit multiple K des corps du système U est formé par l'ensemble de tous les nombres algébriques.

Soit $\mathfrak{S}$ un système quelconque d'éléments faisant partie d'un corps L. Si K est un des corps contenus dans L, on désignera par

$$K(\mathfrak{S})$$

l'intersection de tous les corps situés entre K et L et contenant tous les éléments de $\mathfrak{S}$. On dit que $K(\mathfrak{S})$ est engendré par l'*adjonction* à K du système $\mathfrak{S}$. Les adjonctions envisagées au n° **7** correspondent au cas où $\mathfrak{S}$ est formé d'un nombre *fini* d'éléments.

Quand la correspondance isomorphe de deux extensions L et L′ d'un corps K est telle que chaque élément de K se corresponde à lui-même, on dit que les deux extensions L et L′ sont *équivalentes.* L'isomorphisme n'entraîne d'ailleurs pas toujours l'équivalence.

Lorsque toutes les extensions d'un corps qui satisfont aux conditions d'un problème déterminé sont équivalentes, on convient de dire que le problème n'admet qu'*une* solution.

A la notion générale de corps correspond une notion générale de *domaine d'intégrité.* On entend par domaine d'intégrité tout ensemble d'éléments jouissant des propriétés d'un corps (donc d'un domaine orthoïde ou pseudoorthoïde) à l'exception de celle qui concerne la possibilité de la division, en sorte qu'il peut y avoir, dans le domaine, des éléments A et B autres que zéro pour lesquels l'équation

$$AX = B$$

n'admette pas de solution dans le domaine.

Les notions de sous-domaine d'intégrité, d'intersection des domaines d'intégrité d'un système, ou d'adjonction d'un système d'éléments à un domaine d'intégrité s'entendent maintenant d'elles-mêmes.

On désignera par

$$J[\mathfrak{S}]$$

le domaine d'intégrité obtenu en adjoignant à un domaine d'intégrité J le système $\mathfrak{S}$ d'éléments faisant partie d'un nouveau domaine d'intégrité.

Si donc x est une indéterminée,

$$\mathfrak{R}[x]$$

représentera l'ensemble des fonctions rationnelles entières de x à coefficients rationnels, tandis que

$$\mathfrak{R}(x)$$

représente l'ensemble des fonctions rationnelles (entières ou non) de x à coefficients rationnels.

Un *domaine d'intégrité premier* est un domaine d'intégrité sans véritable sous-domaine d'intégrité. Un tel domaine est ou bien du type de l'ensemble des nombres rationnels entiers ou bien du type de l'un des domaines $\mathfrak{R}_p$.

Chaque domaine d'intégrité J contient un et un seul domaine d'intégrité premier. Suivant que ce dernier est du type de l'ensemble des nombres (rationnels) entiers, ou du type $\mathfrak{R}_p$, on dit que J a comme *caractéristique zéro* ou p[262]).

On peut compléter tout domaine d'intégrité de façon à constituer un corps [cf. n° **15**].*

68. Extensions finies. *Si K′ est une extension d'un corps K on dit qu'un élément x de K′ est *algébrique* ou *transcendant* relativement à K suivant que x vérifie ou non une équation algébrique à coefficients faisant partie de K. Lorsque x est algébrique relativement au corps premier de K on dit que x est *absolument algébrique.*

Le *degré* d'un élément algébrique x par rapport à K est le degré de l'équation algébrique du plus petit degré (à coefficients faisant partie de K) que vérifie x.

On dit que n éléments

$$\alpha_1, \alpha_2, \ldots, \alpha_n$$

du corps K′ sont linéairement indépendants lorsqu'ils ne sont liés par aucune équation linéaire homogène à coefficients faisant partie de K (le cas où tous ces coefficients seraient nuls simultanément étant naturellement exclu).

Une extension K′ du corps K est *finie* et *de degré n relativement à* K lorsqu'on peut déterminer n éléments de K′, linéairement indépendants, mais que $n+1$ éléments quelconques de K′ ne sont pas linéairement indépendants. On écrit alors

$$[K' : K] = n.$$

Chaque élément d'un tel corps K′ est algébrique relativement à K.

Soit L un corps quelconque situé entre K et M. Une condition nécessaire et suffisante pour que M soit fini relativement à K est que L soit fini relativement à K et que M soit fini relativement à L. On a alors

$$[M:K] = [L:K] \cdot [M:L].$$

Si L et M sont des extensions finies de même degré de K et si L est contenu dans M, L est nécessairement identique à M.

Une condition nécessaire et suffisante pour qu'une extension K′ de K soit finie relativement à K est que l'on puisse déduire K′ de K par adjonction d'un *nombre fini* d'éléments (relativement) algébriques.

Lorsqu'entre un corps K et une extension L de ce corps il n'y a qu'un nombre *fini* de corps, L est fini relativement à K.

262) *Les domaines d'intégrité de caractéristique zéro sont les domaines holoïdes (propres et impropres) de *Gy.* (*J.*) *König* [n° **15**]. Les domaines d'intégrité de caractéristique p sont ceux que *Gy.* (*J.*) *König* [Alg. Grössen [10]), p. 409] nomme *pseudoholoïdes.**

La définition précédente des corps finis relativement à K est identique à celle donnée au n° 7 dans le cas plus restreint où les corps K sont soit *numériques*, soit *fonctionnels.* La généralisation consiste en ce que K peut maintenaut être un corps abstrait quelconque ou un corps à caractéristique p.*

69. Extensions algébriques et transcendentes. *Puisqu'on ne se borne plus comme au n° 7 aux extensions d'un corps K obtenues par adjonction d'un système *fini* $\mathfrak{S}$, il importe de distinguer avec soin les *corps finis relativement à* K des *corps algébriques relativement à* K.

Toute extension K' du corps K sera dite *extension algébrique* de K lorsque chacun des éléments de K' est algébrique relativement à K; toute autre extension K' du corps K sera dite *extension transcendante de* K. On dit aussi, dans le premier cas, que K' est un *corps algébrique relativement à* K et, dans le second cas, que K' est *un corps transcendant relativement à* K.

Lorsque l'on obtient K($\mathfrak{S}$) par adjonction à K d'un système (fini ou infini) $\mathfrak{S}$ dont chacun des éléments est algébrique relativement à K, les éléments de K($\mathfrak{S}$) non contenus dans K et $\mathfrak{S}$ sont cependant algébriques relativement à K; le corps K($\mathfrak{S}$) est donc dans ce cas *algébrique* relativement à K. Ainsi le corps K' obtenu en adjoignant au corps $\mathfrak{R}$ des nombres rationnels les racines carrées de tous les nombres rationnels est *algébrique* relativement à K; mais il n'est pas *fini.*

Ceux des éléments d'un corps quelconque L qui sont algébriques relativement à un sous-corps K de L forment un corps K' qui ne peut évidemment être qu'algébrique relativement à K.*

70. Corps absolument algébriques. Corps finis. *Un corps dont tous les éléments sont absolument algébriques [n° **68**] est dit *absolument algébrique.* Si ce corps est fini et de degré n relativement à son corps premier, n est ce qu'on appelle le *degré absolu de* K.

Un corps qui ne contient qu'un nombre fini d'éléments est dit *fini.*

Ces définitions sont essentiellement distinctes de celles données au n° 7 pour les *corps finis ou algébriques au sens absolu du mot.*

Le nombre des éléments d'un corps fini est toujours égal à une puissance entière d'un nombre premier. Et à chaque puissance p^n d'un nombre premier p correspond un et un seul type de corps fini ayant précisément p^n éléments; p est la caractéristique et n le degré absolu de ce corps[263]).*

---

263) Ce théorème est dû à *E. H. Moore* [Math. papers Chicago[34]), p. 210].

71. Extensions simples. Corps algébriquement fermés. Les plus simples des extensions d'un corps K sont celles que l'on peut obtenir par adjonction d'un seul élément; aussi les appelle-t-on des *extensions simples* de K.

On entend par *élément primitif* (relativement à K) d'une extension simple K' de K, tout élément x de K' qui, adjoint à K, donne K'. Si par exemple, K est formé par l'ensemble des nombres complexes et si K est le corps formé par adjonction à K de $\sin z$ et de $\cos z$,

$$x = \operatorname{tg}\frac{z}{2} = \frac{\sin z}{1+\cos z}$$

est un élément primitif de l'extension K' de K. Tout élément de la forme

$$\frac{\alpha\cos\frac{z}{2}+\beta\sin\frac{z}{2}}{\gamma\cos\frac{z}{2}+\delta\sin\frac{z}{2}},$$

où $\alpha, \beta, \gamma, \delta$ sont des nombres quelconques tels que $\alpha\delta-\beta\gamma$ soit différent de zéro, est d'ailleurs un élément primitif de K'.

Si L est une extension simple d'un corps K, tout corps situé entre K et L est une extension simple de K.

Une extension simple K(x) d'un corps K est *transcendante* ou *algébrique* suivant que l'élément adjoint x est lui-même transcendant ou algébrique relativement à K.

Le problème de l'extension d'un corps K par adjonction d'un élément transcendant x est toujours possible et n'admet qu'une solution. L'élément transcendant adjoint x est généralement désigné sous le nom d'*indéterminée.* L'extension K(x) comprend l'ensemble des fonctions rationnelles de x à coefficients faisant partie de K. Tous les éléments du corps K(x) sauf ceux de K sont transcendants relativement à K. Les éléments primitifs de K(x) sont les fonctions rationnelles de x de degré 1, c'est-à-dire les fonctions

$$\frac{\alpha+\beta x}{\gamma+\delta x},$$

où $\alpha, \beta, \gamma, \delta$ sont des éléments quelconques de K tels que $\alpha\delta-\beta\gamma$ soit différent de zéro.

Parmi les fonctions rationnelles de x, les fonctions rationnelles entières forment un domaine d'intégrité

$$\mathrm{K}[x].$$

Les notions de diviseur, de plus grand commun diviseur, de diviseur irréductible s'appliquent à ces fonctions. Pour obtenir le plus grand commun diviseur on peut appliquer le procédé indiqué [I 9, n° **4**] et la décomposition en facteurs irréductibles est univoque à condition d'envisager comme identiques deux diviseurs ne différant que par un facteur indépendant de x.

En ce qui concerne les extensions algébriques simples, il faut observer tout d'abord qu'il y a des corps ne permettant aucune extension algébrique. *E. Steinitz* les appelle *corps algébriquement fermés*; ceux de ces corps qui ont pour caractéristique zéro, sont identiques aux *domaines clos* du n° **7**.

Si K est un corps permettant une extension algébrique, il y a toujours, parmi ses extensions algébriques, des extensions *simples.* Si K n'est pas algébriquement fermé et a la caractéristique nulle, toute extension finie de K est une extension algébrique simple. Mais pour un corps quelconque K on peut dire seulement que si L est une extension du corps K finie relativement à K et de degré n, le degré de chaque élément de L (relativement à K) est nécessairement un diviseur de n; pour que l'extension L soit simple il faut et il suffit que des éléments de degré n figurent effectivement dans L: ces éléments sont alors primitifs et ce sont les seuls qui soient primitifs, tous les autres sont imprimitifs.

Pour discerner si un corps K est algébriquement fermé ou non on forme le corps $K(x)$ par adjonction à K de l'indéterminée x. Si alors chaque élément du domaine d'intégrité $K[x]$ peut être décomposé en fonctions linéaires à coefficients faisant partie de K, le corps K est algébriquement fermé. De ce qu'une seule fonction rationnelle entière non linéaire $\varphi(x)$, à coefficients faisant partie de K, est irréductible en K on peut par contre conclure que K admet une et, au sens du n° **67**, une seule extension algébrique simple K′ dans laquelle figure un élément *primitif* j vérifiant l'équation $\varphi(x) = 0$. Cette extension K′ du corps K est d'ailleurs équivalente au corps envisagé au n° **9** sous le nom de *corps congruentiel du corps* K *relativement au module* $\varphi(x)$; on peut aussi dire que c'est *le corps obtenu par adjonction à* K *du zéro* j *de* $\varphi(x)$.*

72. Corps normaux et fonctions normales. *Pour plus de netteté nous n'envisagerons d'abord que des extensions finies. Nous nous occuperons ensuite des extensions algébriques infinies et ne traiterons qu'en dernier lieu des corps transcendants.

Le théorème, d'après lequel une fonction rationnelle entière donnée $\varphi(x)$ de l'indéterminée x, dont les coefficients font partie d'un corps quelconque donné K, a ou bien un zéro au moins dans K ou bien un zéro au moins dans une certaine extension finie de K, peut être

généralisé. On démontre, en effet, que ou bien $\varphi(x)$ se décompose dans K en facteurs linéaires, ou bien $\varphi(x)$ se décompose dans une certaine extension algébrique K′ de K en facteurs linéaires sans se décomposer en facteurs linéaires dans aucun des corps situés entre K et K′; dans ce dernier cas le problème de la détermination de K′ n'admet qu'une solution: on dit de cette solution K′ qu'elle *suffit à la décomposition complète de* $\varphi(x)$.

Cette solution unique K′ est comprise parmi les extensions que l'on appelle *extensions normales.* On dit d'une extension $\mathfrak{N}$ de K qu'elle est *normale* relativement à K lorsqu'elle est une extension algébrique de K et qu'en outre chaque fonction entière $\varphi(x)$, à coefficients faisant partie de K, et qui est irréductible dans K tout en ayant un zéro dans $\mathfrak{N}$, se décompose dans $\mathfrak{N}$ en facteurs linéaires. Toute extension équivalente à une extension normale est manifestement elle aussi normale.

Lorsqu'un corps $\mathfrak{N}$ est normal relativement à l'un de ses sous-corps K_0 il est aussi normal relativement à chacun des corps compris entre K_0 et $\mathfrak{N}$.

On appelle *fonction normale* en un corps K toute fonction $\varphi(x)$, à coefficients faisant partie de K, qui est d'une part irréductible en K et qui, d'autre part, est telle que le corps $K(j)$, obtenu en adjoignant à K une racine j de l'équation $\varphi(x) = 0$, soit normal.

Pour discerner si une fonction entière $\varphi(x)$, irréductible en K, est normale ou non, c'est-à-dire si l'adjonction à K d'une racine j de l'équation $\varphi(x) = 0$ engendre, ou non, un corps normal, il suffit de voir si la fonction $\varphi(x)$ se décompose, ou non, en facteurs linéaires dans le corps $K(j)$.

Si $\varphi(x)$ représente une fonction normale du corps K, et si L désigne une extension de K, tout facteur de $\varphi(x)$ irréductible en L est normal dans L.

Les théorèmes énoncés dans le présent numéro ont lieu quelle que soit la caractéristique du corps K envisagé. Il n'en sera pas de même dans les numéros suivants où les propositions même les plus usuelles qui ont lieu pour les corps de caractéristique zéro ne seront applicables aux corps de caractéristique p qu'après avoir subi de profondes modifications.*

73. Multiplicité des zéros d'une fonction entière. *Comme toutes les extensions d'un corps K suffisantes à la décomposition d'une fonction donnée $\varphi(x)$ (à coefficients faisant partie de K) en facteurs linéaires sont équivalentes, on prévoit que la façon dont on effectue l'extension de K pour décomposer $\varphi(x)$ ne saurait avoir aucune importance dans l'étude des questions que nous envisageons ici. En effet, si

$$\varphi(x) = (x - w_1)(x - w_2) \dots (x - w_n)$$

représente la décomposition de $\varphi(x)$ dans une extension L de K,

$$\mathfrak{N} = \mathrm{K}(w_1, w_2, \dots, w_n)$$

est le seul corps situé entre K et L qui suffise à la décomposition envisagée de $\varphi(x)$; pour une décomposition de $\varphi(x)$ dans une autre extension L' de K, on obtient de même un corps

$$\overline{\mathfrak{N}} = \mathrm{K}(\overline{w}_1, \overline{w}_2, \dots, \overline{w}_n)$$

en adjoignant à K les zéros de $\varphi(x)$ contenus dans L'. En fixant convenablement l'ordre dans lequel on prend $\overline{w}_1, \overline{w}_2, \dots, \overline{w}_n$, les deux corps $\mathfrak{N}$ et $\overline{\mathfrak{N}}$ sont isomorphes en ce sens que si l'on envisage un élément quelconque de $\mathfrak{N}$, c'est-à-dire une combinaison quelconque de $w_1, w_2, \dots, w_n$ à coefficients faisant partie de K, il suffit d'y remplacer

$$w_1 \text{ par } \overline{w}_1,\ w_2 \text{ par } \overline{w}_2, \dots,\ w_n \text{ par } \overline{w}_n$$

pour obtenir l'élément correspondant de $\overline{\mathfrak{N}}$. Nous ne nous occuperons d'ailleurs que de celles des propriétés des éléments des corps qui ont lieu simultanément pour certains éléments de $\mathfrak{N}$ et pour les éléments correspondants de $\overline{\mathfrak{N}}$.

En particulier si quelques-unes des racines w_i sont égales entre elles, les racines correspondantes $\overline{w}_i$ sont aussi égales. On peut donc parler du nombre des racines simples, doubles, triples, ... d'une équation $\varphi(x) = 0$ sans spécifier celle des extensions du corps K à laquelle apartient la racine envisagée.

Pour évaluer le nombre des zéros de $\varphi(x)$ qui sont d'un ordre de multiplicité donné, nous formerons les dérivées de $\varphi(x)$ en appliquant les règles du calcul différentiel même lorsque les coefficients de $\varphi(x)$ ne sont ni des nombres ni des fonctions de paramètres au sens ordinaire du mot. Nous représenterons donc dans tous les cas par $f'(x)$ et $g'(x)$ les fonctions

$$f'(x) = \frac{df(x)}{dx} = a_1 + 2a_2x + \dots + ma_mx^{m-1},$$

$$g'(x) = \frac{dg(x)}{dx} = b_1 + 2b_2x + \dots + nb_nx^{n-1}$$

si

$$f(x) = a_0 + a_1x + a_2x^2 + \dots + a_mx^m,$$
$$g(x) = b_0 + b_1x + b_2x^2 + \dots + b_nx^n$$

et nous poserons

$$\frac{d}{dx}\left(\frac{f(x)}{g(x)}\right) = \frac{g(x)f'(x) - f(x)g'(x)}{[g(x)]^2}.$$

Si la caractéristique du corps K est zéro, la condition nécessaire et suffisante pour que la dérivée d'une expression que l'on sait être fonction rationnelle $R(x)$ de x, à coefficients faisant partie de K, s'annule est que $R(x)$ ne dépende pas effectivement de x, en d'autres termes que l'expression envisagée soit un élément de K.

Si la caractéristique du corps K est p, la condition nécessaire et suffisante pour que la dérivée de $R(x)$ s'annule est que $R(x)$ soit une fonction rationnelle de x^p.

Si la caractéristique du corps K est p et si $f(x)$ est une fonction rationnelle entière de x^p, la fonction $f(x)$ est égale à la $p^{\text{ième}}$ puissance d'une fonction entière de x. Et inversement.

Plus généralement si la caractéristique du corps K est p et si $f(x)$ est une fonction rationnelle entière de x^{p^f}, la fonction $f(x)$ est égale à une puissance d'une fonction entière x et l'exposant de cette puissance est p^f. Et inversement.

Cela posé, envisageons les racines de

$$f(x) = 0$$

dans une extension de K dans laquelle $f(x)$ se décompose en facteurs *linéaires*. Si $f(x)$ admet un facteur linéaire d'ordre de multiplicité r (où $r \geqq 1$), la dérivée $f'(x)$ de $f(x)$ admet ce même facteur au moins avec l'ordre de multiplicité $r - 1$; lorsque la caractéristique de K est p et que r est divisible par le nombre premier p, l'ordre de multiplicité du facteur envisagé est au moins r dans la dérivée $f'(x)$; dans tout autre cas il est précisément égal à $r - 1$.

Quand $f(x)$ n'a que des facteurs simples, le plus grand commun diviseur de $f(x)$ et de $f'(x)$ est l'unité absolue; dans tout autre cas ce plus grand commun diviseur est du premier degré au moins.

Envisageons maintenant une fonction $F(x)$ rationnelle entière de x, à coefficients faisant partie de K, ayant l'unité absolue comme coefficient de la puissance la plus élevée de x. Dans une extension convenable de K elle se décompose en

$$F(x) = (x - \alpha_1)^{r_1}(x - \alpha_2)^{r_2} \dots (x - \alpha_\nu)^{r_\nu}.$$

Désignons par $f_m(x)$ le produit de ceux des facteurs de $F(x)$, chacun pris une fois seulement, qui figurent précisément m fois dans $F(x)$, en sorte que

$$F(x) = f_1(x)[f_2(x)]^2[f_3(x)]^3 \dots$$

et que deux quelconques des fonctions $f_1(x), f_2(x), f_3(x), \dots$ soient sans diviseur commun.

Lorsque la caractéristique de K est zéro ou qu'elle est p sans que p divise m, les coefficients de $f_m(x)$ appartiennent à K et l'on peut déterminer $f_m(x)$ par des opérations rationnelles.

Lorsque la caractéristique de K est p et que p^f divise m (sans que p^{f+1} divise m), les coefficients de la puissance de $f_m(x)$ à exposant p^f appartiennent à K et peuvent être déterminés par des opérations rationnelles.

Dans le premier de ces deux cas on forme le quotient $\varphi(x)$ de $F(x)$ par le p. g. c. d. des deux fonctions $F(x)$ et $F'(x)$ et l'on forme ensuite le quotient $\chi_m(x)$ du p. g. c. d. de $(\varphi(x))^m$ et $F(x)$ par le p. g. c. d. de $(\varphi(x))^{m-1}$ et $F(x)$. Après avoir formé de même $\chi_{m+1}(x)$, on a

$$f_m(x) = \frac{\chi_m(x)}{\chi_{m+1}(x)}.$$

Dans le second cas, si $\pi = p^f$ et si $m = \pi\mu$ (où μ n'est pas divisible par p), on commence par former

$$(f_k(x))^k$$

pour chaque nombre naturel k non divisible par π. Soit alors

$$\Phi(x)$$

le produit des facteurs de $F(x)$ autres que ceux que l'on vient de former; $\Phi(x)$ est la puissance à exposant π d'une fonction rationnelle entière de x, donc une fonction rationnelle de x^π. Si l'on pose

$$y = x^\pi, \quad \Phi(x) = G(y),$$

on peut déterminer le produit $g_\mu(y)$ des facteurs linéaires de $G(y)$ [chacun pris une fois seulement] qui figurent précisément μ fois dans $G(y)$. On a alors, en remplaçant y par x^π,

$$(f_m(x))^\pi = g_\mu(x^\pi).$$

On voit donc que $(f_m(x))^m$ est, dans tous les cas, une fonction de x dont les coefficients font partie du corps K et peuvent être déterminés par des opérations rationnelles. En divisant par m le degré de cette fonction, on obtient le nombre des zéros de $F(x)$ dont l'ordre de multiplicité est m.*

74. Corps parfaits et imparfaits. Théorème des éléments primitifs. Théorème des corps intermédiaires. *Lorsque K est un corps à caractéristique zéro, chaque fonction rationnelle entière $f(x)$ de x, dont les coefficients font partie de K, et qui est irréductible en K, n'a que des zéros simples dans chacune des extensions de K. Lorsque K est un corps à caractéristique p on ne peut énoncer ce même théorème que dans le cas où l'extraction des racines $p^{\text{ièmes}}$ est

possible dans K (cette extraction de racine est alors une opération univoque).

Un corps K est dit *parfait* quand il n'existe aucune fonction rationnelle entière $f(x)$, à coefficients faisant partie de K, qui soit irréductible en K et admette cependant des zéros *multiples* dans une extension convenablement choisie de K.

Tout corps absolument algébrique [n° **70**] est parfait. Toute extension algébrique d'un corps parfait est un corps parfait.

Un grand nombre de théorèmes concernant les corps à caractéristique zéro s'étendent aux corps parfaits sans s'étendre aux corps non parfaits.

Ainsi *toute extension finie d'un corps parfait est simple.* C'est à ce théorème que *E. Steinitz* donne le nom de *théorème des éléments primitifs.*

On voit aussi qu'*entre un corps parfait* K *et une extension finie quelconque* L *de* K *il n'y a qu'un nombre fini de corps. E. Steinitz* donne à ce théorème le nom de *théorème des corps intermédiaires.*

Ces deux théorèmes concernant les corps parfaits peuvent se déduire d'une proposition plus générale qui s'applique à tous les corps, parfaits ou non:

Si L est engendré par adjonction à K d'un nombre fini d'éléments

$$\alpha, \beta, \gamma, \ldots$$

satisfaisant respectivement aux équations

$$f(x) = 0, \quad g(x) = 0, \quad h(x) = 0, \quad \ldots,$$

supposées à racines simples seulement et dont les coefficients font partie de K, l'extension L est simple relativement à K. On peut alors déduire L de K par adjonction d'un seul élément satisfaisant à une équation n'ayant que des racines simples et dont les coefficients font partie de K.

Parmi les corps de caractéristique p il y en a pour lesquels aucun des deux théorèmes des éléments primitifs ou des corps intermédiaires ne s'applique. Cela résulte immédiatement du théorème suivant:

Soit L une extension d'un corps K à caractéristique p. Si la $p^{\text{ième}}$ puissance de chaque élément de L fait partie de K et si le degré [n° **68**] de L relativement à K est plus grand que p (à supposer naturellement que L est fini relativement à K), l'extension L de K n'est pas simple et un nombre infini de corps sont situés entre K et L.

Pour construire, en s'appuyant sur ce théorème, un corps pour lequel aucun des théorèmes des éléments primitifs ou des éléments intermédiaires ne s'applique, adjoignons à un corps quelconque M à caractéristique p deux indéterminées indépendantes l'une de l'autre t et u et envisageons simultanément les corps

$$L = M(t, u), \qquad K = M(t^p, u^p), \qquad K' = M'(t, u^p).$$

Comme t ne figure pas dans K, ni u dans K', la fonction $x^p - t^p$ est irréductible dans K et la fonction $x^p - u^p$ est irréductible dans K'; on a donc

$$[L:K] = [K':K] \cdot [L:K'] = p^2.$$

Un élément quelconque v de

$$L = M(t, u)$$

peut être mis sous la forme

$$v = \frac{v_1}{v_2},$$

où v_1 et v_2 font partie du domaine d'intégrité

$$M[t, u],$$

et peuvent par suite être représentés par une somme de termes de la forme

$$et^m u^n,$$

où e est un élément de M. En vertu de l'identité (1) du nº **75**, chacune des deux expressions $v_1{}^p$ et $v_2{}^p$ est alors représentée par une somme de termes de la forme

$$e^p t^{mp} u^{np}$$

et appartient par conséquent au domaine d'intégrité

$$M[t^p, u^p];$$

la puissance

$$v^p = \frac{v_1{}^p}{v_2{}^p}$$

est donc un élément du corps

$$K = M(t^p, u^p)$$

et par conséquent L est une extension de K qui est finie mais n'est pas simple, en sorte qu'il y a une infinité de corps entre K et L.*

75. Condition nécessaire et suffisante pour que les théorèmes des éléments primitifs et des corps intermédiaires aient lieu. *Deux éléments quelconques a et b d'un corps K de caractéristique p satisfont

aux relations identiques

(1) $$a^p + b^p = (a+b)^p,$$

(2) $$a^p - b^p = (a-b)^p,$$

(3) $$a^p \cdot b^p = (a \cdot b)^p,$$

(4) $$a^p : b^p = (a : b)^p.$$

Il en résulte que les puissances $p^{\text{ièmes}}$ de tous les éléments de K forment un corps: on le désigne par K^p.

Les deux corps K et K^p sont équivalents; leur isomorphisme s'obtient en faisant correspondre à chaque élément a de K l'élément a^p de K^p.

Quand K est parfait, on a $K^p = K$; dans tout autre cas K^p est un sous-corps de K.

Le théorème des éléments primitifs et celui des corps intermédiaires ont lieu pour chaque corps parfait K et pour tout corps non parfait K de caractéristique p qui est fini et de degré p relativement à K^p. Pour tout autre corps non parfait ni l'un ni l'autre de ces deux théorèmes n'ont lieu.*

76. La plus petite extension parfaite et le plus grand sous-corps d'un corps non parfait. *Quel que soit le corps K de caractéristique p que l'on envisage, on peut toujours former une extension L de ce corps telle que K ait pour éléments les puissances $p^{\text{ièmes}}$ des éléments de L et ces puissances $p^{\text{ièmes}}$ seulement. Pour tout corps parfait K, le corps L est identique à K; mais pour tout corps non parfait K, le corps L contient des éléments qui ne figurent pas dans K. On désignera le corps L par le symbole

$$K^{p^{-1}}.$$

Cela posé, formons à l'aide d'un corps non parfait arbitrairement fixé K la suite de corps infinie (dans les deux sens)

(1) $$\ldots, K^{p^{-2}}, K^{p^{-1}}, K, K^p, K^{p^2}, \ldots$$

dont chacun a pour éléments les puissances $p^{\text{ièmes}}$ des éléments du précédent.

Soient C le plus petit multiple commun des corps de la suite (1) et D l'intersection des corps de cette suite (1). Le corps C est alors la *plus petite* extension de K, en ce sens que toute autre extension de K formant un corps parfait ou bien est équivalente à C, ou bien contient un sous-corps équivalent à C. De même D est le *plus grand* sous-corps de K.*

77. Extension algébrique de première espèce. Corps radicaux. *On dit qu'une fonction rationnelle entière d'une indéterminée x, à coefficients faisant partie de K, et qui est irréductible en K, est de *première espèce* lorsque, dans tout corps dans lequel elle a des racines, ces racines sont simples. On dit qu'un élément algébrique γ relativement à K est de *première espèce* lorsque la fonction irréductible en K qui s'annule pour $x = \gamma$ est de première espèce.

Une extension algébrique de K est de *première espèce* lorsque tous les éléments de cette extension algébrique sont de première espèce relativement à K.

Toute extension finie de première espèce est simple.

Les extensions d'un corps parfait K, donc en particulier de tout corps de caractéristique zéro, ne peuvent engendrer que des fonctions rationnelles entières, des éléments algébriques et des extensions algébriques de première espèce.

Soit $g(x)$ une fonction rationnelle entière de x dont les coefficients font partie d'un corps K de caractéristique p et qui est irréductible en K. On peut toujours déterminer un nombre entier positif ou nul f de façon que $g(x)$ soit une fonction rationnelle entière de x^{p^f} sans être fonction rationnelle entière de $x^{p^{f+1}}$. La fonction $g(x)$ peut alors être mise sous la forme

$$g(x) = x^{np^f} + a_1 x^{(n-1)p^f} + \cdots + a_{n-1} x^{p^f} + a_n,$$

où figure au moins un terme où l'exposant de x n'est pas divisible par p^{f+1}. On dit que n est le *degré réduit* et que f est l'*exposant* de $g(x)$. On étend d'ailleurs ces deux dénominations aux zéros de $g(x)$.

La condition nécessaire et suffisante pour que $g(x)$ [et chaque zéro de $g(x)$] soit de première espèce est que f prenne la plus petite valeur possible, c'est-à-dire que l'on ait $f = 0$.

La plus petite valeur que puisse prendre n est $n = 1$. Dans ce cas $g(x)$ est de la forme

$$x^{p^f} - a$$

et tous ses zéros sont égaux entre eux. Les éléments algébriques de degré réduit $n = 1$ relativement à K sont ce qu'on appelle les *éléments radicaux.*

On appelle *corps radical* relativement à K toute extension de K dans laquelle chaque élément est un élément radical relativement à K.

Entre un corps non parfait K et une extension algébrique quelconque L de ce corps se trouve nécessairement un corps L_0 de première espèce relativement à K et tel que L soit un *corps radical* relativement à L_0. Ce corps L_0 a pour éléments ceux des éléments de L qui sont de première espèce relativement à K.

Nous avons ainsi une vue complète sur les extensions finies d'un corps quelconque K. Si ce corps a pour caractéristique zéro, ses extensions algébriques simples fournissent toutes ses extensions finies. S'il est parfait et à caractéristique p, ses extensions finies sont toutes de première espèce; s'il n'est pas parfait, ses extensions finies ne comprennent, outre celles qui sont de première espèce, que celles que l'on obtient en adjoignant de toutes les manières possibles au corps K et à ses extensions algébriques de première espèce un nombre fini d'éléments radicaux.

A toute extension finie L d'un corps non parfait K correspond un nombre entier positif ou nul f tel que le corps L contienne des éléments à exposant f mais n'en contienne pas à exposant plus grand que f. Ce nombre f est l'*exposant du corps* L *relativement à* K.

Si l'on désigne par L_1 le sous-corps de L qui a pour élément tous les éléments de première espèce de L et si

$$[L_1 : L] = n,$$

on dit que n est le *degré réduit de* L relativement à K.*

78. Extensions algébriques infinies. Les corps absolument algébriques ayant pour caractéristique un nombre premier. *L'étude des extensions algébriques *infinies* est basée sur certains principes de la théorie des ensembles de certitude fort précaire, en particulier sur le postulat de *E. Zermelo*, d'après lequel un ensemble E qui se décompose en ensembles partiels séparés $E_1, E_2, E_3, \ldots$, comprenant chacun au moins un élément, possède au moins *un* ensemble partiel E′ ayant en commun un et un seul élément avec chacun des ensembles $E_1, E_2, E_3, \ldots$, postulat dont on a besoin pour démontrer[264]) que chaque ensemble peut être bien ordonné. Si l'on refusait d'admettre ce postulat, les propositions dont nous allons parler ne reposeraient plus sur aucun fondement certain.

Supposons d'abord que le corps K envisagé soit un *corps premier* à caractéristique p [n° **67**]. Ses extensions algébriques infinies ne sont alors que les corps infinis absolument algébriques ayant pour caractéristique le nombre premier p. Pour l'étude de ces corps il suffit de supposer le postulat que l'on vient de citer sans avoir besoin de s'appuyer sur ce que chaque ensemble peut être bien ordonné.

Pour les corps *finis* ayant pour caractéristique un nombre premier p, on a déjà vu [n° **70**] qu'à chaque nombre entier n positif ou nul

264) *E. Zermelo*, Math. Ann. 59 (1904), p. 514; 65 (1908), p. 107.*

correspond un et un seul type de corps à caractéristique p, ayant un degré absolu égal à n. Il s'agit d'étendre ce théorème aux corps infinis absolument algébriques à caractéristique p.

Désignons, à cet effet, par

$$q_1 = 2,\quad q_2 = 3,\quad q_3 = 5,\quad q_4 = 7,\quad q_5 = 11,\quad \ldots.$$

les nombres premiers ordinaires successifs et envisageons tous les produits symboliques de la forme

$$q_1^{k_1} q_2^{k_2} \ldots q_i^{k_i} \ldots\ldots,$$

où chaque exposant k_i est supposé remplacé soit par 0, soit par un nombre naturel, soit encore par le symbole ∞. Nous dirons de chacun de ces produits symboliques qu'il est un *nombre de type J.* Les nombres naturels sont compris parmi ceux de type J.

Nous postulerons que *deux nombres de type J,*

$$\mathfrak{m} = q_1^{\varkappa_1} q_2^{\varkappa_2} \ldots q_i^{\varkappa_i} \ldots\ldots,$$
$$\mathfrak{n} = q_1^{\lambda_1} q_2^{\lambda_2} \ldots q_i^{\lambda_i} \ldots\ldots,$$

sont égaux et ne sont égaux que si

$$\varkappa_1 = \lambda_1,\ \varkappa_2 = \lambda_2,\ \ldots,\ \varkappa_i = \lambda_i,\ \ldots\ldots$$

et que $\mathfrak{m}$ est *divisible* par $\mathfrak{n}$ quand on a simultanément

$$\varkappa_1 \geqq \lambda_1,\ \varkappa_2 \geqq \lambda_2,\ \ldots,\ \varkappa_i \geqq \lambda_i,\ \ldots\ldots$$

La notion de plus grand commun diviseur s'étend alors sans peine aux nombres de type J.

Les degrés absolus des sous-corps finis d'un corps infini absolument algébrique K à caractéristique p ont pour p. g. c. d. un nombre $\mathfrak{m}$ de type J. On dit de ce nombre $\mathfrak{m}$ qu'il est le *degré total* de K.

A tout nombre $\mathfrak{m}$ de type J correspond un et un seul corps (fini ou infini) absolument algébrique, à caractéristique p, ayant un degré absolu égal à $\mathfrak{m}$.

C'est là la généralisation annoncée du théorème du n° **70** sur les corps finis.*

79. Théorème fondamental des extensions algébriques. *Soit K un corps quelconque choisi parmi ceux qui ne sont pas algébriques fermés [n° **71**]. On démontre que, par adjonction à K d'éléments algébriques relativement à K, on peut obtenir un et un seul corps algébrique fermé (quand on n'envisage pas comme distinctes deux extensions équivalentes). Ce corps algébrique fermé est parfois une extension finie de K; il en est ainsi, par exemple, quand le corps K est formé par l'ensemble des nombres réels. Mais, en général, le corps algébrique fermé que l'on obtient ainsi est un corps infini.

Ce théorème fondamental repose sur ce que chaque ensemble peut être bien ordonné.*

80. Extensions purement transcendantes. *On dit qu'un élément a d'une extension L d'un corps K dépend *algébriquement* (relativement à K) d'un système $\mathfrak{S}$ d'éléments de L quand a est algébrique relativement au corps

$$\mathrm{K}(\mathfrak{S})$$

obtenu en adjoignant $\mathfrak{S}$ à K.

On dit qu'un système $\mathfrak{S}'$ d'éléments dépend algébriquement de $\mathfrak{S}$ quand chaque élément de $\mathfrak{S}'$ dépend algébriquement de $\mathfrak{S}$.

Quand l'élément a dépend algébriquement du système $\mathfrak{S}$ on peut déterminer un système partiel fini $\mathfrak{S}'$ contenu dans $\mathfrak{S}$ et dont a dépend algébriquement.

Si $\mathfrak{S}_3$ dépend algébriquement de $\mathfrak{S}_2$ et si $\mathfrak{S}_2$ dépend algébriquement de $\mathfrak{S}_1$, $\mathfrak{S}_3$ dépendra algébriquement de $\mathfrak{S}_1$.

Deux systèmes $\mathfrak{S}_1$ et $\mathfrak{S}_2$ sont *algébriquement équivalents relativement à* K quand chacun de ces deux systèmes dépend algébriquement de l'autre. Deux systèmes algébriquement équivalents à un troisième relativement à K sont équivalents entre eux relativement à K.

On dit qu'un système $\mathfrak{S}$ d'éléments d'une extension L de K est *algébriquement réductible* relativement à K lorsque ce système $\mathfrak{S}$ est algébriquement équivalent à une de ses parties ou encore lorsque $\mathfrak{S}$ est formé d'un seul élément algébrique relativement à K. Dans tout autre cas on dit que $\mathfrak{S}$ est *algébriquement irréductible relativement à* K.

Tout système partiel d'un système algébriquement irréductible relativement à K est algébriquement irréductible relativement à K.

Tout système algébriquement réductible relativement à K contient un système partiel fini algébriquement réductible relativement à K.

On appelle *extension transcendante pure* de K toute extension transcendante $\mathrm{K}(\mathfrak{S})$ de K obtenue en adjoignant à K un système $\mathfrak{S}$ algébriquement irréductible relativement à K.

Si les éléments (indéterminés)

$$x_1,\ x_2,\ \ldots,\ x_n$$

de ce système $\mathfrak{S}$ sont en nombre *fini*, le corps $\mathrm{K}(\mathfrak{S})$ est formé par les fonctions rationnelles de ces indéterminées

$$x_1,\ x_2,\ \ldots,\ x_n$$

à coefficients faisant partie de K.

Si, au contraire, les éléments de $\mathfrak{S}$ sont en nombre infini, le corps $\mathrm{K}(\mathfrak{S})$ est formé par les éléments des corps $\mathrm{K}(\mathfrak{S}')$ obtenus en prenant pour $\mathfrak{S}'$ successivement tous les sytèmes partiels finis contenus dans $\mathfrak{S}$.

Si les systèmes $\mathfrak{S}_1$ et $\mathfrak{S}_2$ sont tous deux algébriquement irréductibles relativement à K et ont même nombre cardinal (c'est-à-dire même nombre fini ou infini d'éléments), les corps

$$\mathrm{K}(\mathfrak{S}_1) \text{ et } \mathrm{K}(\mathfrak{S}_2)$$

sont des extensions de K algébriquement équivalentes relativement à K.*

81. Extensions transcendantes quelconques. Le degré de transcendance. Distribution des corps en classes. *Soit

$$\mathrm{L} = \mathrm{K}(\mathfrak{S})$$

une extension transcendante quelconque de K. On peut toujours déterminer un système algébriquement irréductible $\mathfrak{S}'$, algébriquement équivalent à $\mathfrak{S}$; les éléments de $\mathfrak{S}$ sont alors algébriques relativement à $\mathrm{K}(\mathfrak{S}')$. Il en résulte que $\mathrm{K}(\mathfrak{S})$ est une extension algébrique de $\mathrm{K}(\mathfrak{S}')$ et que $\mathrm{K}(\mathfrak{S}')$ est une extension transcendante pure de K.

On voit ainsi que chaque extension transcendante d'un corps peut être obtenue en faisant suivre une extension transcendante pure de ce corps d'une extension algébrique de cette extension transcendante pure.

La *décomposition* d'une extension transcendante quelconque donnée d'un corps en une extension transcendante pure et une extension algébrique peut être réalisée d'une infinité de manières mais le nombre des éléments du système $\mathfrak{S}'$ est toujours le même. On donne à ce nombre cardinal le nom de *degré de transcendance de* L *relativement* à K.

Si le degré de transcendance d'une extension quelconque L de K est s relativement à K et si le degré de transcendance d'une extension quelconque L′ de L est t relativement à L, le degré de transcendance de L′ par rapport à K est $s + t$.

On appelle *degré absolu de transcendance* d'un corps quelconque le degré de transcendance de ce corps relativement à son corps premier.

L'ensemble de tous les corps (ou types de corps) ayant même caractéristique c et même degré de transcendance absolu t constitue une *classe*

$$K_{c,t}$$

de corps (ou types de corps).

Chaque classe $K_{c,t}$ contient deux types qui ont un caractère extrême. L'un de ces types s'obtient quand on envisage une extension transcendante pure, de degré de transcendance t, d'un corps premier à caractéristique c; c'est un type déterminé appartenant à la classe $K_{c,t}$ que nous désignerons par

$$\mathfrak{R}_{c,t}.$$

L'autre type de caractère extrême s'obtient de la façon que voici:

Tout corps

$$\mathfrak{R}'_{c,t}$$

de type $\mathfrak{R}_{c,t}$ admet parmi ses extensions algébriques une et, au sens du nº **67**, une seule extension

$$\mathfrak{A}'_{c,t}$$

qui soit algébrique *fermee.* Le type

$$\mathfrak{A}_{c,t}$$

de cette extension algébrique fermée ne dépend que du type $\mathfrak{R}_{c,t}$ sans dépendre en rien des corps $\mathfrak{R}'_{c,t}$ que l'on a envisagés.

Tous les corps situés entre $\mathfrak{R}'_{c,t}$ et $\mathfrak{A}'_{c,t}$ appartiennent à la classe $K_{c,t}$. Inversement tout type de la classe $K_{c,t}$ peut être représenté par un corps, au moins, compris entre $\mathfrak{R}'_{c,t}$ et $\mathfrak{A}'_{c,t}$ ou identique à l'un de ces deux corps.*

I 11. THEORIE DES FORMES ET DES INVARIANTS.

Exposé, d'après l'article allemand de **W. F. MEYER** (Königsberg), par **J. DRACH** (Toulouse).

Théorie algébrique des formes quadratiques et des formes bilinéaires.

Éléments de la théorie[1]).

1. Formes quadratiques. *La forme quadratique générale à n variables $x_1, x_2, \ldots, x_n$ se représente par:

$$f(x) = \sum_{(i,k)} a_{ik} x_i x_k \qquad (i, k = 1, 2, \ldots, n),$$

où l'on a

$$a_{ik} = a_{ki};$$

elle renferme $\frac{1}{2} n(n+1)$ coefficients arbitraires.

Une transformation linéaire (S)

$$x_i = s_{i1} y_1 + s_{i2} y_2 + \cdots + s_{in} y_n \qquad (i = 1, 2, \ldots, n)$$

la change en une nouvelle forme

$$f(S(y)) \equiv g(y) \equiv \sum_{(i,k)} b_{ik} y_i y_k \qquad (i, k = 1, 2, \ldots, n),$$

aux variables $y_1, y_2, \ldots, y_n$, dont les coefficients se déduisent des a_{ik} par les formules

$$b_{ik} = \sum_{(l,m)} a_{lm} s_{li} s_{mk} \qquad (l, m = 1, 2, \ldots, n)$$

quadratiques par rapport aux n^2 coefficients de la transformation.

Si le déterminant $|s_{ik}|$ n'est pas nul, on passe de la forme $g(y)$ à la forme $f(x)$ par la transformation *inverse* (S^{-1}), obtenue en résolvant par rapport aux y les équations qui définissent (S).

1) *Voir, en général, pour toute cette théorie, *P. Muth*, Theorie und Anwendungen der Elementarteiler, Leipzig 1899.*

La complication des formules de transformation des coefficients laisse difficilement apparaître les propriétés communes à $f(x)$ et à l'ensemble de toutes ses transformées $g(y)$ par des transformations *ordinaires* (à déterminant non nul). La *réduction* à une *forme canonique* les manifeste immédiatement.

J. L. Lagrange[2]) observe que, si a_{11} n'est pas nul, l'expression

$$F = f(x) - \frac{1}{a_{11}}(a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n)^2 = f(x) - \frac{1}{a_{11}}\left(\frac{1}{2}\frac{\partial f}{\partial x_1}\right)^2$$

est une forme quadratique qui ne renferme plus x_1. En opérant sur F comme sur f, dans le cas où il y reste des *carrés*, on fait disparaître les variables de proche en proche.

Si l'on arrive ainsi à une forme qui ne renferme que des *rectangles*, par exemple $2a_{ik}x_ix_k$, on n'a qu'à introduire les nouvelles variables

$$x'_i = x_i + x_k, \qquad x'_k = x_i - x_k$$

pour faire réapparaître des carrés; la méthode s'applique donc encore.

Toute forme quadratique à n variables s'écrit ainsi par des opérations rationnelles

$$f = \lambda_1 P_1^2 + \lambda_2 P_2^2 + \cdots + \lambda_r P_r^2,$$

où $P_1, P_2, \ldots, P_r$ sont des *formes linéaires distinctes* des n variables $x_1, x_2, \ldots, x_n$. Chacune d'elles renferme une variable x ou x' qui ne figure pas dans les suivantes.

La transformation ordinaire

$$y_1 = P_1(x), \quad y_2 = P_2(x), \quad \ldots, \quad y_r = P_r(x),$$

exécutée seulement sur les r variables x, x' qui figurent dans $P_1, P_2, \ldots, P_r$ comme *variables initiales*, change la forme en

$$\lambda_1 y_1^2 + \lambda_2 y_2^2 + \cdots + \lambda_r y_r^2.$$

Le nombre r est le *rang* de la forme. En observant que

$$\frac{1}{2}\frac{\partial f}{\partial x_i} = \lambda_1 P_1 \frac{\partial P_1}{\partial x_i} + \lambda_2 P_2 \frac{\partial P_2}{\partial x_i} + \cdots + \lambda_r P_r \frac{\partial P_r}{\partial x_i},$$

on voit que les dérivées de f sont des combinaisons linéaires des r formes $P_1, P_2, \ldots, P_r$ qui sont indépendantes. Comme les dérivées

$$\frac{\partial f}{\partial y_1}, \frac{\partial f}{\partial y_2}, \ldots, \frac{\partial f}{\partial y_r}$$

sont indépendantes, le rang r est le *rang de la matrice formée par les*

2) Misc. Taurinensia 1 (1759), math. p. 18/23; Œuvres 1, Paris 1867, p. 3/9; *C. F. Gauss*, Disquisitiones arithmeticae, Leipzig 1801, n° 271; trad. *A. Ch. M. Poullet Delisle*, Recherches arithmétiques, Paris 1807; Werke 1, Göttingue 1870, p. 305; Commentat. Soc. Gott. recent. 5 (1819/22), éd. Göttingue 1823, § 31; Werke 4, Göttingue 1880, p. 29, 37.

coefficients a_{ik}. Il ne dépend pas de la manière dont on a obtenu la forme réduite; c'est aussi *le nombre minimé de variables qui peuvent figurer dans une transformée de f.*

Une transformation linéaire *ordinaire* ne change pas le rang d'une forme.

Une forme *décomposable en deux facteurs linéaires distincts*

$$f = PQ$$

est *de rang deux,* et réciproquement. Une forme carré parfait est de rang un et réciproquement.*

2. Cas où les coefficients sont réels. *Si les coefficients de la forme quadratique, de rang r

$$f = \sum_{(i,k)} a_{ik} z_i z_k \qquad (i, k = 1, 2, \ldots, n)$$

sont réels, nous avons vu que par des transformations rationnelles (réelles) on la ramène à la forme

$$f = \lambda_1 y_1^2 + \lambda_2 y_2^2 + \cdots + \lambda_r y_r^2.$$

Le nombre des coefficients λ_i qui sont positifs (et par suite aussi le nombre de ceux qui sont négatifs) *est le même pour toutes les formes réduites.*

C'est la *loi d'inertie* de *J. J. Sylvester*[3]), donnée en 1852, mais que *C. G. J. Jacobi*[4]) possédait dès 1847.

En introduisant les nouvelles variables réelles définies par

$$|\lambda_i|\, y_i^2 = Y_i^2 \qquad (i = 1, 2, \ldots, r)$$

la forme réduite s'écrit, par exemple

$$f = Y_1^2 + Y_2^2 + \cdots + Y_i^2 - Y_{i+1}^2 - \cdots - Y_r^2,$$

et si l'on avait de même

$$f = Z_1^2 + Z_2^2 + \cdots + Z_k^2 - Z_{k+1}^2 - \cdots - Z_r^2,$$

avec $i < k$ par exemple, les Z seraient des formes linéaires de $Y_1, Y_2, \ldots, Y_r$.

Les équations

$$Y_1 = Y_2 = \cdots = Y_i = 0, \qquad Z_{k+1} = Z_{k+2} = \cdots = Z_r = 0,$$

regardées comme équations en $Y_1, Y_2, \ldots, Y_r$, sont en nombre

$$(r + i - k)$$

3) London Edinb. Dublin philos. mag. (4) 4 (1852), p. 140; Philos. Trans. London 143 (1853), p. 481; Papers 1, Cambridge 1904, p. 376/7, 511.

4) *C. W. Borchardt,* J. reine angew. Math. 53 (1857), p. 281; Werke, Berlin 1888, p. 469; cf. *C. G. J. Jacobi,* Œuvres posth. publ. par *C. W. Borchardt,* J. reine angew. Math. 53 (1857), p. 275; Werke 3, Berlin 1884, p. 593.

et admettent une solution au moins pour laquelle

$$Y_{i+1}, Y_{i+2}, \ldots, Y_r$$

ne sont pas tous nuls.

Or elles entraînent

$$Y_{i+1}^2 + Y_{i+2}^2 + \cdots + Y_r^2 + Z_1^2 + Z_2^2 + \cdots + Z_k^2 = 0,$$

c'est-à-dire, en particulier,

$$Y_{i+1} = Y_{i+2} = \cdots = Y_r = 0.$$

On a donc nécessairement $i = k$.

Ch. Hermite[5]) a donné une démonstration de la loi d'inertie, basée sur le calcul de la transformation qui permettrait d'écrire

$$Y_1^2 + \cdots + Y_i^2 - Y_{i+1}^2 - \cdots - Y_r^2 = Z_1^2 + \cdots + Z_k^2 - Z_{k+1}^2 - \cdots - Z_r^2 \quad (i<k).$$

En posant

$$\begin{aligned} Y_1 &= p_1 Z_1 + q_1 Z_2 + \cdots + s_1 Z_r, \\ Y_2 &= p_2 Z_1 + q_2 Z_2 + \cdots + s_2 Z_r, \\ &\ldots\ldots\ldots\ldots\ldots, \\ Y_r &= p_r Z_1 + q_r Z_2 + \cdots + s_r Z_r, \end{aligned}$$

parmi les conditions auxquelles doivent satisfaire les coefficients figure

$$p_1^2 + p_2^2 + \cdots + p_i^2 - p_{i+1}^2 - p_{i+2}^2 - \cdots - p_r^2 = 1.$$

Cette condition est impossible si

$$p_1 = p_2 = \cdots = p_i = 0.$$

Ch. Hermite déduit de la transformation précédente une transformation analogue dans laquelle

$$p_1 = p_2 = \cdots = p_i = 0.$$

En remplaçant Z_1 par

$$Z_1 \sin\varphi + Z_2 \cos\varphi$$

et Z_2 par

$$Z_1 \cos\varphi - Z_2 \sin\varphi$$

on peut choisir φ de manière à faire disparaître Z_1 de Y_1. On fait de même disparaître Z_2, puis Z_3 et ainsi de suite jusqu'à Z_{k-1}.

La même méthode peut faire disparaître $Z_1, Z_2, \ldots, Z_{k-2}$ de l'expression de Y_2 et ainsi de suite.

On obtient de cette manière une transformation où Z_1 ne figure dans aucune des expressions $Y_1, Y_2, \ldots, Y_{k-1}$, et ne figure donc pas *a fortiori* dans $Y_1, Y_2, \ldots, Y_i$.

On appelle quelquefois *signature* d'une forme quadratique de rang r la différence

$$s = P - N$$

5) J. reine angew. Math. 53 (1857), p. 271/4 [1856]; Œuvres, publ. par *E. Picard* 1, Paris 1905, p. 429/33.

entre le nombre des carrés positifs et celui des carrés négatifs de la forme réduite.

Deux formes de même *rang* r et de même *signature* sont transformées l'une de l'autre par une transformation réelle.

Si les lettres $x_1, x_2, \ldots, x_r$ de la forme réelle

$$f(x_1, x_2, \ldots, x_n)$$

de *rang* r sont choisies de telle sorte que la suite

$$A_0 = 1,\ A_1 = a_{11},\ A_2 = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}, \ldots, A_r = \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1r} \\ a_{21} & a_{22} & \cdots & a_{2r} \\ \cdot & \cdot & \cdot & \cdot \\ a_{n1} & a_{n2} & \cdots & a_{nr} \end{vmatrix}$$

ne renferme pas deux termes consécutifs nuls et que d'autre part A_r soit différent de zéro, un terme nul est toujours compris entre deux termes de signes contraires.

La *signature* de la forme est la différence entre le nombre des permanences et le nombre des variations de la suite précédente [les zéros étant comptés ou non, avec un signe quelconque].

3. Réduction simultanée de deux formes quadratiques. La réduction simultanée de deux formes quadratiques à une forme canonique (en l'espèce à une somme de carrés) a donné lieu à de nombreux travaux, à partir des recherches de *A. L. Cauchy*[6]) et de *C. G. J. Jacobi*[7]) sur la détermination des axes principaux d'une surface du second degré.

Si l'on considère la forme

$$F = \varphi - \lambda\psi = \sum_{(i,j)} (a_{ij} - \lambda b_{ij}) x_i x_j \qquad (i, j = 1, 2, \ldots, n)$$

construite avec les deux formes données φ et ψ, le *discriminant* ou *déterminant* [cf. I 16, **42**]

$$F(\lambda) \equiv |a_{ij} - \lambda b_{ij}|$$

est un polynome en λ de degré inférieur ou égal à n. Les racines de l'équation

$$F(\lambda) = 0$$

(équation caractéristique de Cauchy) et par suite les rapports des coefficients de $F(\lambda)$ à l'un d'entre eux, demeurent inaltérés quand on remplace φ et ψ par les formes φ_1, ψ_1 en $y_1, y_2, \ldots, y_n$ qui s'en déduisent par une transformation linéaire (S)

$$x_i = \sum_{l=1}^{l=n} s_{il} y_l \qquad (i = 1, 2, \ldots, n).$$

6) Exercices math. 4, Paris 1829, p. 152; Œuvres (2) 9, Paris 1891, p. 187.
7) J. reine angew. Math. 12 (1834), p. 1; Werke 3, Berlin 1884, p. 193.

Ce sont des *invariants* du système des deux formes, vis à vis des transformations linéaires exécutées sur les variables.

Si λ_1 est une racine *simple* de l'équation $F(\lambda) = 0$, une transformation ordinaire réelle des variables permet de remplacer φ et ψ par

$$\lambda_1 c_1 y_1^2 + \varphi_1(y_2, y_3, \ldots, y_n),$$
$$c_1 y_1^2 + \psi_1(y_2, y_3, \ldots, y_n),$$

où c_1 est différent de zéro; en répétant cette opération on donne, *dans le cas où l'équation*

$$F(\lambda) = 0$$

a n racines distinctes, aux deux formes φ, ψ l'expression

$$\lambda_1 c_1 z_1^2 + \lambda_2 c_2 z_2^2 + \cdots + \lambda_n c_n z_n^2,$$
$$c_1 z_1^2 + c_2 z_2^2 + \cdots + c_n z_n^2,$$

dans l'hypothèse où le déterminant de ψ n'est pas nul.

Une transformation qui n'est plus nécessairement réelle (sauf si tous les c sont de même signe) donne enfin les deux formes canoniques

$$\lambda_1 z_1^2 + \lambda_2 z_2^2 + \cdots + \lambda_n z_n^2, \qquad z_1^2 + z_2^2 + \cdots + z_n^2.$$

Dans le cas où l'une des formes est déjà réduite à la forme canonique

$$z_1^2 + z_2^2 + \cdots + z_n^2,$$

des transformations *orthogonales*, c'est-à-dire satisfaisant à la condition

$$z_1^2 + z_2^2 + \cdots + z_n^2 = y_1^2 + y_2^2 + \cdots + y_n^2,$$

permettent de ramener une forme ordinaire quelconque en $z_1, z_2, \ldots, z_n$ à la même réduite canonique

$$\lambda_1 y_1^2 + \lambda_2 y_2^2 + \cdots + \lambda_n y_n^2.$$

Les coefficients $\lambda_1, \lambda_2, \ldots, \lambda_n$, racines de l'équation $F(\lambda) = 0$, dite parfois *équation en λ*, sont *réels*.

La démonstration de cette réalité a été d'abord une réduction à l'absurde. *A. L. Cauchy*[8]) l'a établie directement. *Ch. Hermite*[9]) y parvient par induction complète en la démontrant d'abord pour $n = 3$.

Si les racines de l'équation caractéristique ne sont plus distinctes les formes réduites doivent être modifiées. L'expression définitive de la réduction est due à *K. Weierstrass*; elle sera développée plus loin [cf. n° **5**]. Déjà en 1858, *K. Weierstrass* avait abordé la question pour des formes réelles.*

8) Exercices math. 3, Paris 1828, p. 1/22; Œuvres (2) 8, Paris 1890, p. 9/35.
9) J. reine angew. Math. 53 (1857), p. 271/4; Œuvres[5]) 1, p. 429/33.

4. Formes bilinéaires. *La forme bilinéaire générale à n variables

$$f = \sum_{(i,k)} a_{ik} x_i y_k \quad (i, k = 1, 2, \ldots, n)$$

s'écrit aussi

$$f = \sum_{k=1}^{k=n} f_k y_k,$$

en posant

$$f_k = \sum_{i=1}^{i=n} a_{ik} x_i.$$

Si son déterminant $|a_{ik}|$ n'est pas nul, $f_1, f_2, \ldots, f_n$ sont des formes indépendantes et la transformation définie par

$$x_i = f_i \qquad (i = 1, 2, \ldots, n)$$

ramène à la forme réduite

$$y_1 x_1 + y_2 x_2 + \cdots + y_n x_n.$$

Si $f_1, f_2, \ldots, f_r$ sont indépendantes et $f_{r+1}, f_{r+2}, \ldots, f_n$ fonctions linéaires des précédentes:

$$f_{r+i} = \sum_{j=1}^{j=n} b_{kj} f_j \qquad (i = 1, 2, \ldots, n-r)$$

c'est-à-dire si $|a_{ik}|$ est de *rang r*, la forme s'écrit

$$f_1(y_1 + \sum_{i=1}^{i=n} b_{i1} y_{k+i}) + \cdots + f_r(y_r + \sum_{i=1}^{i=n} b_{ir} y_{r+i})$$

ou encore, en posant

$$X_i = f_i, \qquad Y_j = y_j + \sum_{i=1}^{i=n} b_{ij} y_{n+i},$$

$$f = X_1 Y_1 + X_2 Y_2 + \cdots + X_r Y_r.$$

On a dû pour obtenir cette forme réduite transformer à la fois les x_i et les y_k et par des transformations indépendantes.*

Équivalence des faisceaux ordinaires d'après Weierstrass[10]).

5. Diviseurs élémentaires. *Envisageons deux formes bilinéaires[11])

$$A = \sum_{(i,k)} a_{ik} x_i y_k, \qquad B = \sum_{(i,k)} b_{ik} x_i y_k \qquad (i, k = 1, \ldots, n)$$

10) *K. Weierstrass*, Monatsb. Akad. Berlin 1868, p. 310; Werke 2, Berlin 1895, p. 19. Dix ans avant, *K. Weierstrass* s'était déjà occupé de la question [Monatsb. Akad. Berlin 1858, p. 207; Werke 1, Berlin 1894, p. 233].

11) *Dans l'hypothèse $a_{ik} = a_{ki}$, $b_{ik} = b_{ki}$, en faisant $x_i = y_i$ on obtient *un faisceau de formes quadratiques* auquel la notion des diviseurs élémentaires s'étend immédiatement.*

des $2n$ variables x_i, y_k. L'ensemble des formes

$$\lambda_1 A + \lambda_2 B,$$

où λ_1 et λ_2 sont deux paramètres quelconques, constitue un *faisceau* dont le *déterminant* Δ est, par définition, celui de la forme générale

$$|\lambda_1 A + \lambda_2 B|.$$

Si Δ n'est pas nul identiquement, le faisceau est *ordinaire*; Δ est alors décomposable en un produit de facteurs du premier degré en λ_1, λ_2; il en est de même de tous ses mineurs.

Si

$$p = a\lambda_1 + b\lambda_2$$

désigne un diviseur de Δ, il peut arriver que p divise tous les mineurs de Δ d'un certain degré; soit alors l_ϱ la plus haute puissance de p qui divise tous les mineurs de Δ de *degré* ϱ: il est clair que p figure avec l'exposant l_ϱ dans le plus grand commun diviseur de tous ces mineurs.

On a toujours

$$l_{\varrho+1} > l_\varrho, \quad \text{si } l_\varrho > 0.$$

Car si D est un mineur de Δ de degré $(\varrho + 1)$, il est, ainsi que les dérivées partielles $\frac{\partial D}{\partial \lambda_1}, \frac{\partial D}{\partial \lambda_2}$, une combinaison linéaire de mineurs de degré ϱ. Si $l_\varrho = 0$, on n'a plus nécessairement que $l_{\varrho+1} \geqq l_\varrho$.

Si l'on définit n nombres non négatifs $e_1, e_2, \ldots, e_n$ par les égalités

$$e_n = l_n - l_{n-1},\ e_{n-1} = l_{n-1} - l_{n-2}, \ldots,\ e_2 = l_2 - l_1,\ e_1 = l_1,$$

d'où l'on conclut

$$l_n = e_1 + e_2 + \cdots + e_n$$

et

$$(a\lambda_1 + b\lambda_2)^{l_n} = (a\lambda_1 + b\lambda_2)^{e_1} (a\lambda_1 + b\lambda_2)^{e_2} \ldots (a\lambda_1 + b\lambda_2)^{e_n},$$

chacun des facteurs $(a\lambda_1 + b\lambda_2)^{e_i}$ est dit *diviseur élémentaire* de Δ, quand e_i est différent de zéro.

Une décomposition analogue étant faite pour chaque diviseur de Δ, on voit que Δ *est le produit de ses diviseurs élémentaires.*

Il est clair qui si p figure dans Δ avec l'exposant l et divise encore tous les mineurs de degré $(n - l + 1)$, il ne divise ces derniers qu'une seule fois: tous les diviseurs élémentaires correspondants sont égaux à p.

La notion de diviseur élémentaire est susceptible d'extensions variées[12]). *Il suffit évidemment que les a_{ik} appartiennent à un domaine*

12) Le cas où les éléments a_{ik} sont des fonctions entières ou rationnelles d'un corps algébrique a été étudié par *K. Hensel*, J. reine angew. Math. 115 (1895), p. 254/94.

dans lequel Δ et tous ses mineurs peuvent d'une seule manière être décomposés en produits de facteurs irréductibles. Ces derniers joueront le rôle des diviseurs du premier degré p; nous les désignerons de la même manière.

Par exemple les a_{ik} peuvent être des nombres entiers[12a]) ou encore des fonctions rationnelles entières d'une ou de plusieurs variables dont les coefficients appartiennent à un domaine de rationalité déterminé $[R]$.

Il est clair que si tous les mineurs de Δ de degré $(r+1)$ sont nuls, sans qu'il en soit de même pour les mineurs de degré r, c'est-à-dire si Δ est de *rang r, au sens de Frobenius*, on devra arrêter la suite des diviseurs élémentaires à $\varrho = r$. Si Δ n'est pas nul, r est égal à n; si tous les a_{ik} sont nuls, r est égal à zéro. Cette définition du rang et des diviseurs élémentaires s'étend aux matrices rectangulaires qu'on transforme en matrices carrées par l'adjonction de lignes ou de colonnes formées d'éléments nuls.

Soit D_σ le plus grand commun diviseur de tous les mineurs de Δ de degré σ et posons, pour $\sigma > r$,

$$D_\sigma = 0;$$

D_r sera le produit de tous les diviseurs élémentaires du système a_{ik}

Les quotients

$$E_r = \frac{D_r}{D_{r-1}},\ E_{r-1} = \frac{D_{r-1}}{D_{r-2}},\ \cdots,\ E_1 = D_1$$

sont, d'après ce qu'on a vu sur les exposants l_ϱ, des fonctions rationnelles entières des variables $\lambda, \mu, \ldots$ comme les a_{ik}. On pose

$$E_{r+1} = E_{r+2} = \cdots = E_n = 0$$

et l'on appelle E_j le $j^{\text{ième}}$ *diviseur élémentaire*[13]) du système a_{ik}, ou mieux le $j^{\text{ième}}$ *produit élémentaire.*

Il convient d'observer tout de suite que *les produits élémentaires* $E_1, E_2, \ldots, E_r$ s'obtiennent, de même que les D_ϱ, par des opérations rationnelles, en partant des a_{ik}.

Pour avoir les diviseurs élémentaires il faut ensuite décomposer chaque produit E_ϱ en ses diviseurs irréductibles

$$E_\varrho = \prod p^{e_\varrho};$$

12a) La théorie correspondante a été développée par *H. J. S. Smith,* Philos. Trans. London 151 (1861), p. 318; Papers 1, Oxford 1894, p. 397.

13) *Le choix du même terme *diviseur élémentaire (Elementarteiler)* pour désigner deux choses distinctes p^{e_ϱ} et E_ϱ peut prêter à équivoque. *J. Drach* propose de désigner E_ϱ qui est le *produit* de tous les p^{e_ϱ} sous le nom de *$\varrho^{\text{ième}}$ produit élémentaire* ou *produit élémentaire d'indice ϱ.**

la théorie de la divisibilité enseigne à le faire de la façon la plus simple. On préciserait aisément les opérations irrationnelles nécessaires pour obtenir les p.*

6. Suite des exposants des diviseurs élémentaires. *La suite des exposants des diviseurs élémentaires

$$e_1,\ e_2,\ \ldots,\ e_n$$

qui correspondent à un même diviseur irréductible p n'est pas quelconque. On a toujours

$$e_n \geqq e_{n-1} \geqq e_{n-2} \geqq \cdots \geqq e_2 \geqq e_1;$$

en d'autres termes les *différences secondes de la suite*

$$l_n,\ l_{n-1},\ \ldots,\ l_2,\ l_1,\ 0$$

sont positives ou nulles. Ce fait a été remarqué par *A. Cayley*[14]).

Il entraîne cette conséquence que *le $(\varrho+1)^{\text{ième}}$ produit élémentaire $E_{\varrho+1}$ est divisible par le $\varrho^{\text{ième}}$* produit élémentaire E_ϱ. *La réciproque est vraie.*

L'établissement de cette proposition, et d'autres qui s'y rattachent étroitement et qui sont indispensables à l'exposé rigoureux de la méthode de *K. Weierstrass,* a donné lieu à de nombreuses recherches:

L. Stickelberger[15]) emploie un procédé indirect pour établir la généralité de la forme réduite de *K. Weierstrass*; il donne plus tard une nouvelle exposition rigoureuse mais où les diviseurs élémentaires ne prennent leur signification que de la forme réduite alors que *K. Weierstrass* les introduit dès le début.

L. Kronecker[16]) cherche à réaliser la condition nécessaire au raisonnement de *K. Weierstrass* en faisant subir au faisceau une transformation linéaire à coefficients indéterminés, sans établir toutefois que ce procédé convient aux formes quadratiques.

G. Frobenius[17]) étendant la méthode employée par *H. S. Smith* pour les systèmes à coefficients entiers montre qu'elle peut s'appliquer aux systèmes dont les éléments sont des fonctions entières d'un paramètre. Sa démonstration a été, depuis la publication de la *réduction d'un système*

14) J. reine angew. Math. 50 (1855), p. 314; Papers 2, Cambridge 1889, p. 217. Dans le cas des a_{ik} entiers *H. J. S. Smith* l'a établi [Philos. Trans. London 151 (1861), p. 318; Papers 1, Oxford 1894, p. 397.

15) Diss. Berlin 1874; J. reine angew. Math. 86 (1879), p. 20.

Voir aussi *L. O. Hesse*, Vorlesungen über analytische Geometrie des Raumes, (3e éd.) publ. par *S. Gundelfinger,* Leipzig 1876, p. 498/525.

16) Monatsb. Akad. Berlin 1874, p. 215; Werke 1, Leipzig 1895, p. 391.

17) J. reine angew. Math. 88 (1880), p. 96.

à coefficients entiers de *L. Kronecker*[18]), simplifiée par *K. Hensel*[19]). Nous la donnerons plus loin.

Enfin *G. Frobenius*[20]), au moyen d'une identité de la théorie des déterminants due à *L. Kronecker*, en a donné une démonstration algébrique. *K. Weierstrass*[20a]) a renvoyé pour ce point aux publications de *G. Frobenius*.*

7. Théorèmes de Frobenius. *Soit l_ϱ l'exposant de la plus haute puissance de p qui figure dans D_ϱ; tout mineur de degré ϱ qui contient exactement p à la puissance l_ϱ est *régulier* pour p.

Il y a au moins un mineur régulier pour chaque indice ϱ; nous allons établir, avec *G. Frobenius*, les trois propositions suivantes:

a) *On a toujours*

$$e_\varrho \geqq e_{\varrho-1} \qquad (\varrho = 2, 3, \ldots, r)$$

c'est-à-dire

$$l_\varrho - 2l_{\varrho-1} + l_{\varrho-2} \geqq 0.$$

b) *Tout mineur régulier de degré ϱ du déterminant $|a_{ik}|$ contient au moins un mineur régulier de degré $(\varrho-1)$.*

c) *Tout mineur régulier de degré $(\varrho-1)$ est contenu dans au moins un mineur régulier de degré ϱ.*

Tout mineur du second degré de $|a_{ik}|$ contient p à un exposant au moins égal à $2l_1$, donc $l_2 \geqq 2l_1$, $l_2 - l_1 \geqq l_1$ c'est-à-dire $e_2 \geqq e_1$.

Supposons démontré, *pour une certaine valeur de ϱ et dans tout système a_{ik}*,

$$e_1 \leqq e_2 \leqq e_3 \leqq \cdots \leqq e_{\varrho-1},$$

nous allons prouver que

$$e_{\varrho-1} \leqq e_\varrho$$

et démontrer en même temps les deux autres propositions.

Soit

$$M = |a_{\mu\nu}|$$

un mineur de degré ϱ de $|a_{ik}|$ correspondant à

$$\mu = \mu_1, \mu_2, \ldots, \mu_\varrho$$
$$\nu = \nu_1, \nu_2, \ldots, \nu_\varrho:$$

admettons que p figure dans le plus grand commun diviseur des mineurs de degré σ de M à l'ordre $l'_\sigma (\sigma = 1, \ldots, \varrho)$.

Il y aura dans M au moins un mineur T de degré $(\varrho - 2)$ qui

18) J. reine angew. Math. 107 (1891), p. 135.
19) J. reine angew. Math. 114 (1895), p. 25/30.
20) Sitzgsb. Akad. Berlin 1894, p. 33.
20a) Monatsb. Akad. Berlin 1868, p. 324 (§ 4); Werke 2, Berlin 1895, p. 31.

contiendra p à la puissance $l'_{\varrho-2}$; mais on a identiquement

$$MT = PS - QR,$$

où P, Q, R, S sont des mineurs de M de degré $(\varrho - 1)$.

Le second membre renferme p à une puissance *au moins égale* à $2l'_{\varrho-1}$; donc

$$l'_\varrho + l'_{\varrho-2} \geqq 2l'_{\varrho-1}$$

ou bien

$$l'_{\varrho-1} - l'_{\varrho-2} \leqq l'_\varrho - l'_{\varrho-1}.$$

Nous avons supposé établi pour chaque système (donc pour celui de M) la suite d'inégalités

$$l'_1 - l'_0 \leqq l'_2 - l'_1 \leqq \cdots \leqq l'_{\varrho-1} - l'_{\varrho-2},$$

on peut donc ajouter à la suite l'inégalité précédente, c'est-à-dire remplacer dans cette suite $(\varrho - 1)$ par ϱ.

Soit maintenant

$$L = |a_{\varkappa\lambda}| \qquad \begin{pmatrix} \varkappa = \varkappa_1, \varkappa_2, \ldots, \varkappa_{\varrho-1} \\ \lambda = \lambda_1, \lambda_2, \ldots, \lambda_{\varrho-1} \end{pmatrix}$$

un mineur *quelconque* de $|a_{ik}|$ de degré $(\varrho - 1)$. Déduisons de L, en le bordant des éléments de M qui forment la ligne et la colonne se coupant en $a_{\mu\nu}$, un déterminant $L_{\mu\nu}$. Si $a_{\mu\nu}$ appartient à L, on aura $L_{\mu\nu} = 0$.

L. Kronecker[21]) a démontré l'identité

$$|La_{\mu\nu} - L_{\mu\nu}| = 0 \qquad \begin{pmatrix} \mu = \mu_1, \mu_2, \ldots, \mu_\varrho \\ \nu = \nu_1, \nu_2, \ldots, \nu_\varrho \end{pmatrix}$$

qui s'écrit si l'on développe le déterminant suivant les puissances de L

$$L^\varrho M = L^{\varrho-1} M_1 + L^{\varrho-2} M_2 + \cdots + M_\varrho,$$

où M_ϱ est une fonction homogène de degré σ des quantités $L_{\mu\nu}$ dont les coefficients sont des mineurs[22]) de M de degré $\varrho - \sigma$.

Si le diviseur p figure dans L à la puissance l et dans le plus grand commun diviseur des $L_{\mu\nu}$ à la puissance l', le terme $L^{\varrho-\sigma} M_\sigma$ renfermera p à une puissance *au moins* égale à

$$(\varrho - \sigma) l + \sigma l' + l'_{\varrho-\sigma} = m_\sigma.$$

Le premier membre $L^\varrho M$ contient exactement p à la puissance

$$m_0 = \varrho l + l'_\varrho.$$

21) J. reine angew. Math. 72 (1870), p. 153; Werke 1, Leipzig 1895, p. 237.
22) *G. Frobenius* [Sitzgsb. Akad. Berlin 1894, p. 34] montre que ce théorème de *L. Kronecker* est compris dans une proposition de *J. J. Sylvester*, London Edinb. Dublin philos. mag. (4) 1 (1851), p. 297; Papers 1, Cambridge 1904, p. 243; *G. Frobenius*, J. reine angew. Math. 86 (1879), p. 54; cf. I 2, 23.

De la définition de m_σ on déduit

$$m_{\sigma+1} - m_\sigma = l' - l - (l'_{\varrho-\sigma-1})$$

et comme nous avons établi

$$l'_{\varrho-\sigma} - l'_{\varrho-\sigma-1} \leqq l'_\varrho - l'_{\varrho-1} \qquad (\sigma = 0, 1, \ldots, (\varrho-1))$$

il en résulte

$$m_{\sigma+1} - m_\sigma \geqq l' - l - (l'_\varrho - l'_{\varrho-1}) \qquad (\sigma = 0, 1, \ldots, (\varrho-1))$$

Le second membre est négatif ou nul; si l'on avait en effet

$$l' - l > l'_\varrho - l'_{\varrho-1}$$

on en déduirait

$$m_\varrho > m_{\varrho-1} > \cdots > m_0$$

et dans l'identité de Kronecker le second membre serait divisible par p^{m_1} alors que le premier ne l'est que par p^{m_0}.

L'inégalité ainsi établie s'écrit[23])

$$l'_\varrho + l \geqq l'_{\varrho-1} + l'.$$

Si l'on prend maintenant pour L et M des mineurs *réguliers* du déterminant $|a_{ik}|$ on aura

$$l = l_{\varrho-1}, \; l'_\varrho = l_\varrho,$$

donc

$$l_{\varrho-1} + l_\varrho \geqq l' + l'_{\varrho-1}.$$

Mais, d'autre part, on a

$$l' \geqq l_\varrho, \; l'_{\varrho-1} \geqq l_{\varrho-1}$$

d'après la définition des l_ϱ; on a donc nécessairement

$$l'_{\varrho-1} = l_{\varrho-1}, \qquad l' = l_\varrho;$$

d'où l'on déduit:

1°) qu'il y a dans M un mineur du premier ordre *régulier*,
2°) qu'un des $L_{\mu\nu}$, dont L est un mineur, est *régulier*,
3°) en se reportant à l'inégalité

$$l'_{\varrho-1} - l'_{\varrho-2} \leqq l'_\varrho - l'_\varrho - l'_{\varrho-1}$$

et observant que la régularité de M et l'hypothèse que tout mineur régulier de degré $(\varrho-1)$ renferme un mineur régulier de degré $(\varrho-2)$

23) *On en peut conclure en passant une proposition intéressante. Supposons que le plus grand commun diviseur *de tous les déterminants de degré ϱ dont L est un mineur* renferme p à la puissance λ'; on a évidemment $l' \geqq \lambda' \geqq l_\varrho$ donc *a fortiori*

$$l'_\varrho + l \geqq l'_{\varrho-1} + \lambda'$$

c'est-à-dire:

*Le produit de deux déterminants M et L des degrés ϱ et $(\varrho-1)$ est divisible par le produit du plus grand commun diviseur des mineurs du premier ordre de M par le plus grand commun diviseur de tous les déterminants de degré ϱ dont L est un mineur.**

donnent

$$l'_{\varrho-2} = l_{\varrho-2},$$

on voit aussi que l'on a

$$l_{\varrho-1} - l_{\varrho-2} \leqq l_\varrho - l_{\varrho-1},$$

c'est-à-dire

$$e_{\varrho-1} \leqq e_\varrho.$$

Les trois propositions annoncées sont donc établies.

Remarque: Parmi les conséquences de la première nous signalerons seulement la suivante:

Si l'on a

$$l_\varrho > 0, \; l_{\varrho-1} = 0 \qquad (\text{d'où } l_{\varrho-2} = l_{\varrho-3} = \cdots = l_1 = 0),$$

c'est-à-dire

$$e_\varrho = l_\varrho - l_{\varrho-1} > 0,$$

on a aussi $l_\varrho < l_{\varrho+1} < l_{\varrho+2}, \ldots$ et $e_{\varrho+1}, e_{\varrho+2}, \ldots$ ne sont pas nuls[24]). On a donc alors

$$e_r \geqq e_{r-1} \geqq \cdots \geqq e_\varrho > 0.$$

Si le $r^{\text{ième}}$ produit élémentaire E_r contient p à la première puissance, c'est-à-dire si $l_r = 1$, tous les diviseurs élémentaires sont égaux à p. Ceci arrive lorsque p qui figure dans D_r avec l'exposant l_r figure dans D_{r-1} avec l'exposant $(l_r - 1)$ et n'arrive que dans ce cas.*

8. Réduction d'un faisceau ordinaire. *Soit

$$\lambda_1 A + \lambda_2 B$$

où

$$A = \sum_{(i,k)} a_{ik} x_i y_k, \quad B = \sum_{(i,k)} b_{ik} x_i y_k \qquad (i, k = 1, 2, \ldots, n),$$

un faisceau de formes bilinéaires *ordinaire*, c'est-à-dire dont le déterminant

$$|\lambda_1 A + \lambda_2 B|$$

n'est pas identiquement nul.

Supposons d'abord que le déterminant $|A|$ soit différent de zéro et considérons la forme

$$C = \lambda A - B = \sum_{(i,k)} c_{ik} x_i y_k \qquad (i, k = 1, 2, \ldots, n),$$

où λ est un paramètre arbitraire et dont le déterminant

$$|\lambda A - B| = S$$

est un polynome en λ d'ordre égal à n.

24) *Ceci résulte aussi de la remarque évidente du début $l_{\varrho+1} > l_\varrho$ si l_ϱ est différent de zéro, *dans le cas où p est linéaire en λ_1, λ_2.**

Soient $c_1, c_2, \ldots, c_m$ $(m \leqq n)$ les racines de l'équation

$$S = 0;$$

choisissons l'une d'elles que nous nommons c et désignons par $l_\varkappa$ l'exposant de la puissance de $(\lambda - c)$ commune à tous les mineurs de S d'ordre $\varkappa$ (sous-déterminants de degré $n - \varkappa$); les différences

$$e_1 = l_1,\ e_2 = l_2 - l_1,\ e_3 = l_3 - l_2,\ \ldots,\ e_n = l_n - l_{n-1}$$

donnent les *diviseurs élémentaires*

$$(\lambda - c)^{e_1},\ (\lambda - c)^{e_2},\ \ldots,\ (\lambda - c)^{e_n}$$

correspondant à la racine c.

Soient S_{ik} le coefficient de c_{ik} dans le développement de S suivant les éléments de la ligne i ou de la colonne k, $S^{(\varkappa)}$ le déterminant déduit de S par suppression des $\varkappa$ premières lignes et des $\varkappa$ premières colonnes, enfin $(-1)^{i+k}\, S^{(\varkappa)}_{ik}$ le déterminant déduit de $S^{(\varkappa)}$ par suppression de la ligne de rang $i - \varkappa$ et de la colonne de rang $k - \varkappa$. Si l'un des nombres $i - \varkappa$, $k - \varkappa$ est nul ou négatif on posera

$$S^{(\varkappa)}_{ik} = 0;$$

on a d'ailleurs

$$S^{(\varkappa - 1)}_{\varkappa\varkappa} = S^{(\varkappa)}.$$

La théorie des déterminants donne les identités (où l'on a écrit S' pour $S^{(1)}$, S'' pour $S^{(2)}$, S''' pour $S^{(3)}$)

$$\begin{gathered} S_{11} S_{ik} - S_{i1} S_{1k} = S S'_{ik} \\ S'_{22} S'_{ik} - S'_{i2} S'_{2k} = S' S''_{ik} \\ S''_{33} S''_{ik} - S''_{i3} S''_{3k} = S'' S'''_{ik} \\ \cdots\cdots\cdots \\ S^{(n-1)}_{nn} S^{(n-1)}_{ik} - S^{(n-1)}_{in} S^{(n-1)}_{nk} = S^{(n-1)} S^{(n)}_{ik} \end{gathered}$$

où l'on doit poser

$$S^{(n-1)}_{nn} = S^{(n)} = 1.$$

Les déterminants $S, S', S'', \ldots, S^{(n-1)}$ peuvent être supposés réguliers[25]) *par rapport au diviseur* $(\lambda - c)$.

Car S possède un mineur régulier de degré $(n-1)$: la ligne et la colonne supprimées pour l'obtenir peuvent être amenées par permutation avec les autres à être la première ligne et la première colonne, de sorte que S' sera un mineur régulier. Le raisonnement peut se répéter pour S'' et ainsi de suite.

Or l'échange de deux lignes (ou de deux colonnes) équivaut à une permutation des variables y (ou x).

25) *Ce point avait été admis implicitement par *K. Weierstrass* et n'a été établi qu'avec beaucoup de peine. Voir à ce sujet le n° **5** de cet article I 11.*

On peut donc, si c'est nécessaire, exécuter sur les x et les y deux substitutions unimodulaires telles que les mineurs S', S'', ... soient tous réguliers pour $\lambda = c$.

On pourra par suite écrire les égalités précédentes

$$\begin{gathered} \frac{S_{ik}}{S} = \frac{S'_{ik}}{S'} + \frac{S_{i1} S_{1k}}{S S'}, \\ \frac{S'_{ik}}{S'} = \frac{S''_{ik}}{S''} + \frac{S'_{i2} S'_{2k}}{S' S''}, \\ \cdots\cdots\cdots \end{gathered}$$

puisque $S_{11} = S'$, $S'_{11} = S''$, ...; d'où en les ajoutant membre à membre

$$\frac{S_{ik}}{S} = \frac{S_{i1} S_{1k}}{S S'} + \frac{S'_{i2} S'_{2k}}{S' S''} + \cdots + \frac{S^{(n-1)}_{in} S^{(n-1)}_{nk}}{S^{(n-1)} S^{(n)}}.$$

K. Weierstrass multiplie les deux membres de cette égalité par $u_k v_i$ et fait la somme de tous les termes analogues. Ce qui donne

$$\Omega = \sum_{(i,k)} \frac{S_{ik}}{S} u_k v_i = \frac{X' Y'}{S S'} + \frac{X'' Y''}{S' S''} + \cdots + \frac{X^{(n)} Y^{(n)}}{S^{(n-1)} S^{(n)}}$$

$$(i, k = 1, 2, \ldots, n),$$

où l'on reconnaît, *au signe près*, au premier membre la forme *réciproque* de

$$C = \sum_{(i,k)} c_{ik} x_i y_k$$

(obtenue en divisant par S ce déterminant *bordé* d'une colonne v et d'une ligne u) et où l'on a

$$\begin{aligned} X' &= S_{11} u_1 + S_{12} u_2 + \cdots + S_{1n} u_n \\ X'' &= S'_{22} u_2 \qquad\quad + \cdots + S'_{2n} u_n \\ &\cdots\cdots\cdots \\ X^{(n)} &= \qquad\qquad\qquad\quad S^{(n-1)}_{nn} u_n \end{aligned}$$

et

$$\begin{aligned} Y' &= S_{11} v_1 + S_{21} v_2 + \cdots + S_{n1} v_n \\ Y'' &= \qquad\quad S'_{22} v_2 + \cdots + S'_{n2} v_n \\ &\cdots\cdots\cdots \\ Y^{(n)} &= \qquad\qquad\qquad\quad S^{(n-1)}_{nn} v_n. \end{aligned}$$

K. Weierstrass transforme Ω en posant[26])

$$u_i = \frac{\partial A}{\partial y_i},\ v_j = \frac{\partial A}{\partial x_j} \qquad (i, j = 1, 2, \ldots, n),$$

26) Pour cette transformation voir *C. G. J. Jacobi*, J. reine angew. Math. 53 (1857), p. 265; Werke 3, Berlin 1884, p. 585.

ce qui donne, en désignant par $\frac{\Phi(x, y)}{S}$ le résultat

$$\Phi(x, y) = - \begin{vmatrix} c_{11} & c_{12} & \cdots & c_{1n} & \frac{\partial A}{\partial x_1} \\ c_{21} & c_{22} & \cdots & c_{2n} & \frac{\partial A}{\partial x_2} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ c_{n1} & c_{n2} & \cdots & c_{nn} & \frac{\partial A}{\partial x_n} \\ \frac{\partial A}{\partial y_1} & \frac{\partial A}{\partial y_2} & \cdots & \frac{\partial A}{\partial y_n} & 0 \end{vmatrix}$$

Eu égard aux expressions

$$c_{ik} = \lambda a_{ik} - b_{ik},$$

on déduit de là par des combinaisons faciles des lignes et des colonnes

$$-\lambda^2 \Phi(x, y) = \begin{vmatrix} c_{11} & c_{12} & \cdots & c_{1n} & \frac{\partial B}{\partial x_1} \\ c_{21} & c_{22} & \cdots & c_{2n} & \frac{\partial B}{\partial x_2} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ c_{n1} & c_{n2} & \cdots & c_{nn} & \frac{\partial B}{\partial x_n} \\ \frac{\partial B}{\partial y_1} & \frac{\partial B}{\partial y_2} & \cdots & \frac{\partial B}{\partial y_n} & (-\lambda A - B) \end{vmatrix}$$

c'est-à-dire

$$\frac{\lambda^2 \Phi(x, y)}{S} = \lambda A + B + \frac{\Psi}{S},$$

où Ψ est de degré $n-1$ au plus par rapport à λ, ce qui donne pour λ suffisamment grand

$$\frac{\lambda^2 \Phi(x, y)}{S} = \lambda A + B + \frac{\Delta}{\lambda} + \frac{\Delta'}{\lambda^2} + \cdots\cdots$$

Les deux premiers termes du développement de $\frac{\Phi(x, y)}{S}$ *suivant les puissances décroissantes de* λ *sont donc*

$$\frac{A}{\lambda} \text{ et } \frac{B}{\lambda^2}.$$

Toute la méthode revient à former d'une autre manière, pour cette fonction $\frac{\Phi(x, y)}{S}$, les coefficients des termes en $\frac{1}{\lambda}$ et $\frac{1}{\lambda^2}$.*

9. Décomposition de la forme Ω. *Revenons à la forme Ω qui est rationnelle en λ et cherchons à la décomposer en fractions simples.

Considérons d'abord les termes qui renferment au dénominateur une puissance de $(\lambda - c)$.

Les déterminants $S^{(\varkappa)}$ et $S^{(\varkappa-1)}$ renferment $(\lambda - c)$ aux puissances $l_\varkappa$ et $l_{\varkappa-1}$ puisqu'ils sont réguliers; donc le quotient

$$Q = \sqrt{\frac{S^{(\varkappa-1)} S^{(\varkappa)}}{(c-\lambda)^{l_\varkappa + l_{\varkappa-1}}}}$$

ne s'annule pas pour $\lambda = c$ et comme $X^{(\varkappa)}$ et $Y^{(\varkappa)}$ sont, quand les u et les v sont arbitraires, divisibles justement par $(\lambda - c)^{e_\varkappa}$, on peut écrire

$$\frac{X^{(\varkappa)}}{Q} = (\lambda - c)^{e_\varkappa}[X_{\varkappa 0} + (\lambda - c) X_{\varkappa 1} + \cdots\cdots],$$

$$\frac{Y^{(\varkappa)}}{Q} = (\lambda - c)^{e_\varkappa}[Y_{\varkappa 0} + (\lambda - c) Y_{\varkappa 1} + \cdots\cdots],$$

avec

$$X_{\varkappa\mu} = \frac{1}{\sqrt{C_\varkappa}}(C_{\varkappa\varkappa\mu} u_\varkappa + \cdots + C_{n\varkappa\mu} u_n),$$

$$Y_{\varkappa\nu} = \frac{1}{\sqrt{C_\varkappa}}(D_{\varkappa\varkappa\nu} v_\varkappa + \cdots + D_{n\varkappa\nu} v_n),$$

où $C_\varkappa$ *et les coefficients des* u *et des* v *désignent des fonctions entières de* c *et des coefficients de* A *et* B.

On conclut de là

$$\frac{X^{(\varkappa)} Y^{(\varkappa)}}{S^{(\varkappa-1)} S^{(\varkappa)}} = \frac{1}{(\lambda - c)^{e_\varkappa}}[Z_0 + Z_1(\lambda - c) + \cdots].$$

Pour obtenir les termes en $\frac{1}{\lambda}$ et $\frac{1}{\lambda^2}$, les coefficients de $\frac{1}{\lambda - c}$ et $\frac{1}{(\lambda - c)^2}$ nous sont seuls nécessaires; ils sont évidemment ici

$$F_\varkappa = Z_{e_\varkappa - 1} = X_{\varkappa 0} Y_{\varkappa, e_\varkappa - 1} + X_{\varkappa 1} Y_{\varkappa, e_\varkappa - 2} + \cdots + X_{\varkappa, e_\varkappa - 1} Y_{\varkappa 0},$$

$$G_\varkappa = Z_{e_\varkappa - 2} = X_{\varkappa 0} Y_{\varkappa, e_\varkappa - 2} + X_{\varkappa 1} Y_{\varkappa, e_\varkappa - 3} + \cdots + X_{\varkappa, e_\varkappa - 2} Y_{\varkappa 0}.$$

K. Weierstrass les représente par les notations abrégées

$$(X_\varkappa Y_\varkappa)_{e_\varkappa} \text{ et } (X_\varkappa Y_\varkappa)_{e_\varkappa - 1}.$$

On a donc, avec ces notations, pour coefficients de $\frac{1}{\lambda - c}$ et de $\frac{1}{(\lambda - c)^2}$ dans Ω, les expressions

$$F = F_1 + F_2 + \cdots + F_n = \sum_{\varkappa=1}^{\varkappa=n} (X_\varkappa Y_\varkappa)_{e_\varkappa},$$

$$G = G_1 + G_2 + \cdots + G_n = \sum_{\varkappa=1}^{\varkappa=n} (X_\varkappa Y_\varkappa)_{e_\varkappa - 1}.$$

Si l'on suppose

$$e_k > 0 \text{ et } e_{k+1} = 0,$$

on a vu que l'on a

$$e_1 \geqq e_2 \geqq \cdots \geqq e_k$$

$$e_{k+1} = e_{k+2} = \cdots = e_n = 0;$$

on peut alors écrire simplement, en se bornant aux termes qui existent réellement

$$F = \sum_{\varkappa=1}^{\varkappa=k} (X_\varkappa Y_\varkappa)_{e_\varkappa},$$

$$G = \sum_{\varkappa=1}^{\varkappa=k} (X_\varkappa Y_\varkappa)_{e_\varkappa - 1},$$

où les formes

$$X_{\varkappa, j} \text{ et } Y_{\varkappa, j} \qquad (\varkappa = 1, 2, \ldots, k; j = 0, 1, 2, \ldots, e_\varkappa - 1)$$

sont en même nombre, égal à la somme

$$e_1 + e_2 + \cdots + e_k.$$

Remarque: On a fait observer plus haut qu'une certaine permutation des (x, y) pouvait être nécessaire pour obtenir des déterminants $S, S', S'', \ldots$ *réguliers par rapport au diviseur* $(\lambda - c)$. Cette permutation des x entraîne une permutation correspondante (adjointe) des u_i, v_i, mais il est clair que la forme

$$\Omega = \sum_{(i,k)} \frac{S_{ik}}{S} u_k v_i \qquad (i, k = 1, 2, \ldots, n)$$

donne ainsi la réciproque de la transformée de C.

Les coefficients F et G de $\frac{1}{\lambda - c}$ et $\frac{1}{(\lambda - c)^2}$ dans la transformée de Ω étant ainsi obtenus, la permutation inverse exécutée sur u, v donnera ceux des mêmes éléments dans Ω. Pour simplifier l'écriture nous continuerons à les désigner de même.

Pour chaque diviseur $(\lambda - c_i)$ de S il pourra être nécessaire de ranger les variables $x_1, x_2, \ldots; x_r, y_1, y_2, \ldots, y_s$ dans un ordre déterminé afin de pouvoir appliquer la décomposition précédente; il faudra toujours ensuite revenir à l'ordre initial des indices croissants.

Les coefficients de $\frac{1}{\lambda - c}$ et de $\frac{1}{(\lambda - c)^2}$ dans Ω donnent immédiatement ceux de $\frac{1}{\lambda}$ et $\frac{1}{\lambda^2}$, puisque

$$\frac{F}{\lambda - c} = \frac{F}{\lambda} + c\frac{F}{\lambda^2} + \cdots\cdots,$$

$$\frac{G}{(\lambda - c)^2} = \frac{G}{\lambda^2} + \cdots\cdots$$

En rétablissant les indices qui correspondent aux diverses racines

et désignant par

$$\frac{F^{(\varrho)}}{\lambda} + \frac{G^{(\varrho)} + c_\varrho F^{(\varrho)}}{\lambda^2}$$

la partie qui provient du diviseur $(\lambda - c_\varrho)$, on aura donc

$$\Omega = \frac{\Sigma F^{(\varrho)}}{\lambda} + \frac{\Sigma(G^{(\varrho)} + c_\varrho F^{(\varrho)})}{\lambda^2} + \cdots\cdots,$$

les sommes étant étendues à toutes les racines c_ϱ distinctes.

Comme

$$F^{(\varrho)} = F_1^{(\varrho)} + F_2^{(\varrho)} + \cdots + F_{k_\varrho}^{(\varrho)} = \sum_{\varkappa=1}^{\varkappa=n} (X_\varkappa^{(\varrho)} Y_\varkappa^{(\varrho)})_{e_\varkappa^{(\varrho)}}$$

ces sommes sont en réalité des sommes doubles, mais leur composition linéaire va nous permettre de les remplacer par des sommes simples et justifier à nouveau l'introduction des diviseurs élémentaires.*

10. Formes réduites. *Soient

$$(\lambda - c_1)^{e_1}, (\lambda - c_2)^{e_2}, \ldots, (\lambda - c_m)^{e_m}$$

les diviseurs élémentaires de S écrits dans un ordre quelconque, les quantités c_i, c_k n'étant plus nécessairement distinctes; on a

$$e_1 + e_2 + \cdots + e_m = n$$

et la somme double

$$\sum_{(\varkappa, \varrho)} (X_\varkappa^{(\varrho)} Y_\varkappa^{(\varrho)})_{e_\varkappa^{(\varrho)}}$$

s'écrira simplement

$$(X_1 Y_1)_{e_1} + (X_2 Y_2)_{e_2} + \cdots + (X_m Y_m)_{e_m}.$$

Avec ces notations nous aurons

$$\Omega = \frac{\Sigma(X_\sigma Y_\sigma)_{e_\sigma}}{\lambda} + \frac{\Sigma c_\sigma (X_\sigma Y_\sigma)_{e_\sigma} + \Sigma(X_\sigma Y_\sigma)_{e_\sigma - 1}}{\lambda^2} + \cdots\cdots,$$

où, dans chacune des sommes, $\sigma = 1, 2, \ldots, m$, et il suffira de poser

$$u_i = \frac{\partial A}{\partial y_i}, \quad v_j = \frac{\partial A}{\partial x_j}$$

pour obtenir les expressions des X, Y:

$$X_{\sigma\mu} = \frac{1}{\sqrt{C_\sigma}} (C'_{1\sigma\mu} x_1 + C'_{2\sigma\mu} x_2 + \cdots + C'_{n\sigma\mu} x_n),$$

$$Y_{\sigma\nu} = \frac{1}{\sqrt{C_\sigma}} (D'_{1\sigma\nu} y_1 + D'_{2\sigma\nu} y_2 + \cdots + D'_{n\sigma\nu} y_n),$$

où les C_σ, $C'_{i\sigma\mu}$, $D'_{i\sigma\nu}$ $(i = 1, 2, \ldots, n)$ sont des fonctions de c_σ et des coefficients a_{ik}, b_{ik}.

Nous parvenons donc ainsi à la nouvelle forme de développement

$$\frac{\Phi(x,y)}{S}=\frac{\Sigma(X_\sigma Y_\sigma)_{e_\sigma}}{\lambda}+\frac{\Sigma c_\sigma(X_\sigma Y_\sigma)_{e_\sigma}+\Sigma(X_\sigma Y_\sigma)_{e_\sigma-1}}{\lambda^2}+\cdots\cdots,$$

d'où l'on conclut *les expressions réduites* de A et B

$$A=\sum_{\sigma=1}^{\sigma=m}(X_\sigma Y_\sigma)_{e_\sigma},$$

$$B=\sum_{\sigma=1}^{\sigma=m}c_\sigma(X_\sigma Y_\sigma)_{e_\sigma}+\sum(X_\sigma Y_\sigma)_{e_\sigma-1}.$$

Les formes $X_{\sigma\mu}$, $Y_{\sigma\nu}$ sont au nombre de n puisque σ variant de 1 à m, μ varie de 0 à $e_\sigma-1$; *ces formes sont indépendantes.*

Car si l'on désigne par A la forme A regardée comme dépendant des variables $X_{\sigma\mu}$, $Y_{\sigma\nu}$, on aura pour $\mu+\nu=e_\sigma-1$

$$\frac{d\mathsf{A}}{dX_{\sigma\mu}}=Y_{\sigma\nu},\qquad \frac{d\mathsf{A}}{dY_{\sigma\nu}}=X_{\sigma\mu},\qquad \frac{d^2\mathsf{A}}{dX_{\sigma\mu}\,dY_{\sigma\nu}}=1;$$

les autres dérivées de A sont nulles, d'où

$$|\mathsf{A}|=1.$$

En égard à la transformation qui conduit de A à A, on a donc

$$|A|=D_x(X_{\sigma\mu})\,.\,1\,.\,D_y(Y_{\sigma\nu})$$

en désignant, par exemple, par

$$D_x(X_{\sigma\mu})$$

le déterminant des n formes $X_{\mu\sigma}$ par rapport à $x_1, x_2, \ldots, x_n$. Comme $|A|$ est différent de zéro,

$$D_x(X_{\sigma\mu}),\qquad D_y(Y_{\sigma\nu})$$

sont tous deux différents de zéro et *l'on peut exprimer* $x_1, x_2, \ldots, x_n$ *au moyen des* $X_{\sigma\mu}$ *et aussi* $y_1, y_2, \ldots, y_n$ *au moyen des* $Y_{\sigma\nu}$.

En résumé, *si A et B sont deux formes bilinéaires de* $2n$ *variables, telles que* $|A|$ soit différent de zéro, *et si*

$$(\lambda-c_1)^{e_1},\ (\lambda-c_2)^{e_2},\ \ldots,\ (\lambda-c_m)^{e_m}$$

sont les diviseurs élémentaires de

$$|\lambda A-B|,$$

on peut les transformer simultanément par des substitutions linéaires à déterminant non nul, en les deux formes

$$A_1=\sum_{\sigma=1}^{\sigma=m}(X_\sigma Y_\sigma)_{e_\sigma},$$

$$B_1=\sum_{\sigma=1}^{\sigma=m}c_\sigma(X_\sigma Y_\sigma)_{e_\sigma}+\sum_{\sigma=1}^{\sigma=m}(X_\sigma Y_\sigma)_{e_\sigma-1},$$

où

$$(X_\sigma Y_\sigma)_{e_\sigma}=\sum X_{\sigma\mu}Y_{\sigma\nu}\qquad\begin{pmatrix}\mu=0,1,2,\ldots,e_\sigma-1\\ \mu+\nu=e_\sigma-1\end{pmatrix}$$

et où $(X_\sigma Y_\sigma)_{e_\sigma-1}$ *doit être annulé pour* $e_\sigma=1$.*

11. Cas général. *Supposons maintenant que $|A|$ et $|B|$ soient nuls tous deux mais toujours

$$|\lambda_1 A+\lambda_2 B|\gtrless 0;$$

soient

$$(a_1\lambda_1+b_1\lambda_2)^{e_1},\ (a_2\lambda_1+b_2\lambda_2)^{e_2},\ \ldots,\ (a_m\lambda_1+b_m\lambda_2)^{e_m}$$

les diviseurs élémentaires de ce dernier déterminant, écrits dans un ordre quelconque.

K. Weierstrass pose

$$\lambda_1=g\lambda-g',\quad \lambda_2=h\lambda-h',\ \text{où}\ gh'-hg'=1,$$

ce qui donne

$$\lambda_1A+\lambda_2B=(gA+hB)\lambda-(g'A+h'B)=\lambda A'-B'.$$

On peut choisir $\frac{g}{h}$ de façon que le déterminant $|A'|$ soit différent de zéro; à chaque diviseur élémentaire de

$$|\lambda_1A+\lambda_2B|$$

correspond un diviseur élémentaire de

$$|\lambda A'-B|$$

et l'on peut disposer des constantes a_σ, b_σ de façon que

$$a_\sigma g+b_\sigma h=1\qquad(\sigma=1,2,\ldots,m)$$

puisque leur rapport seul est connu. On aura alors

$$a_\sigma\lambda_1+b_\sigma\lambda_2=\lambda-(a_\sigma g'+b_\sigma h')=\lambda-c_\sigma.$$

La théorie précédente s'applique à

$$\lambda A'-B'$$

puisque le déterminant $|A'|$ est différent de zéro; les formules

$$A=h'A'-hB'$$
$$B=-g'A'+gB'$$

donnent ainsi pour A et B les expressions réduites

$$A=\sum_{\sigma=1}^{\sigma=m}a_\sigma(X_\sigma Y_\sigma)_{e_\sigma}-h\sum_{\sigma=1}^{\sigma=m}(X_\sigma Y_\sigma)_{e_\sigma-1}$$

$$B=\sum_{\sigma=1}^{\sigma=m}b_\sigma(X_\sigma Y_\sigma)_{e_\sigma}+g\sum_{\sigma=1}^{\sigma=m}(X_\sigma Y_\sigma)_{e_\sigma-1}$$

en tenant compte des égalités évidentes

$$a_\sigma = h' - c_\sigma h, \qquad b_\sigma = c_\sigma g - g'.$$

Ces formes réduites ne dépendent que des diviseurs élémentaires de

$$|\lambda_1 A + \lambda_2 B|;$$

il en résulte que *deux faisceaux ordinaires (non singuliers) de formes bilinéaires, avec le même nombre de variables, dont les déterminants ont les mêmes diviseurs élémentaires sont susceptibles d'être ramenés par des transformations linéaires à déterminant non nul à une même forme réduite. Ils sont donc équivalents.**

12. Problème inverse. *Les diviseurs élémentaires déterminent la forme réduite. L'inverse a-t-il lieu?

Supposons que l'on choisisse m nombres entiers $e_1, e_2, \ldots, e_m$ satisfaisant à la condition

$$e_1 + e_2 + \cdots + e_m = n$$

et des constantes a_σ, b_σ, g, h satisfaisant aux conditions

$$a_\sigma g + b_\sigma h = 1 \qquad (\sigma = 1, 2, \ldots, m).$$

Les formes A et B construites au moyen des formules précédentes,

$$A = \sum_{\sigma=1}^{\sigma=m} [a_\sigma (X_\sigma Y_\sigma)_{e_\sigma} - h (X_\sigma Y_\sigma)_{e_\sigma - 1}],$$

$$B = \sum_{\sigma=1}^{\sigma=m} [b_\sigma (X_\sigma Y_\sigma)_{e_\sigma} + g (X_\sigma Y_\sigma)_{e_\sigma - 1}],$$

où l'on regarde les $X_{\sigma\mu}$, ainsi que les $Y_{\sigma\nu}$, comme n variables indépendantes, sont-elles telles que les diviseurs élémentaires de

$$|\lambda_2 A + \lambda_2 B|$$

soient précisément

$$(a_\sigma \lambda_1 + b_\sigma \lambda_2)^{e_\sigma} \qquad (\sigma = 1, 2, \ldots, m).$$

K. Weierstrass a montré qu'il en est bien ainsi.

Si l'on pose

$$A_\sigma = a_\sigma (X_\sigma Y_\sigma)_{e_\sigma} - h (X_\sigma Y_\sigma)_{e_\sigma - 1}$$
$$B_\sigma = b_\sigma (X_\sigma Y_\sigma)_{e_\sigma} + g (X_\sigma Y_\sigma)_{e_\sigma - 1},$$

le déterminant

$$\Delta = |\lambda_1 A + \lambda_2 B|$$

est le produit des déterminants

$$\Delta_\sigma = |\lambda_1 A_\sigma + \lambda_2 B_\sigma|$$

En écrivant

$$a_\sigma \lambda_1 + b_\sigma \lambda_2 = u_\sigma, \qquad g \lambda_2 - h \lambda_1 = v,$$

on a d'ailleurs:

$$\Delta_\sigma = \begin{vmatrix} 0 & 0 & 0 \ldots 0 & v & u_\sigma \\ 0 & 0 & 0 \ldots v & u_\sigma & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ v & u_\sigma & 0 \ldots 0 & 0 & 0 \\ u_\sigma & 0 & 0 \ldots 0 & 0 & 0 \end{vmatrix} = \pm (u_\sigma)^{e_\sigma}$$

et l'on observe *qu'en supprimant la dernière ligne et la dernière colonne de Δ_σ, on a un mineur non divisible par u_σ.*

Les diviseurs élémentaires de Δ ne peuvent être que des puissances des u_σ.

Les seuls mineurs de Δ, de degré $(n - \varkappa)$, qui ne sont pas identiquement nuls sont de la forme

$$\Pi_\sigma \Delta_{\sigma, m_\sigma},$$

avec

$$m_1 + m_2 + \cdots + m_\sigma = \varkappa,$$

en désignant par

$$\Delta_{\sigma, m_\sigma}$$

un mineur de degré $e_\sigma - m_\sigma$.

Soit

$$a \lambda_1 + b \lambda_2$$

un diviseur linéaire de Δ; cherchons combien de fois il entre en facteur dans chaque produit de l'ensemble précédent. Désignons par

$$\sigma_1, \sigma_2, \ldots, \sigma_r$$

les valeurs de σ pour lesquelles

$$a_\sigma = a, \quad b_\sigma = b;$$

on peut supposer les exposants correspondants

$$e_{\sigma_1}, e_{\sigma_2} \ldots, e_{\sigma_r}$$

rangés en une suite décroissante.

Si l'on a $\varkappa \geqq r$, comme on peut former par des produits de mineurs d'ordre un des Δ_{σ_i} un mineur de degré $(n - r)$ de Δ qui n'admette pas le diviseur $a\lambda_1 + b\lambda_2$, les mineurs de Δ de degré $(n - \varkappa)$ ne l'admettent pas non plus. Si l'on a $\varkappa < r$, parmi les entiers $m_{\sigma_1}, m_{\sigma_2}, \ldots, m_{\sigma_r}$, dont la somme est $\varkappa$, il y en a au moins $(r - \varkappa)$ qui sont nuls. Donc tout mineur de degré $(n - \varkappa)$ de Δ est au moins divisible par une puissance de $(a\lambda_1 + b\lambda_2)$ dont l'exposant est la somme de $(r - \varkappa)$ des nombres $e_{\sigma_1}, e_{\sigma_2}, \ldots, e_{\sigma_r}$. Le plus petit de ces exposants est la somme des $(r - \varkappa)$ derniers.

Or si l'on pose

$$l = e_{\sigma_1} + \cdots + e_{\sigma_r},\ l^{(1)} = l - e_{\sigma_1}, \ldots, l^{(\varkappa)} = l^{(\varkappa-1)} - e_{\sigma_\varkappa}$$

cette somme des $(r - \varkappa)$ derniers exposants est $l^{(\varkappa)}$. On forme d'ailleurs un *mineur* de degré $(n - \varkappa)$ qui n'admet pas $(a\lambda_1 + b\lambda_2)$ à une puissance plus élevée en prenant

$$m_{\sigma_1} = \cdots = m_{\sigma_\varkappa} = 1, \qquad m_{\sigma+1} = \cdots = m_{\sigma_r} = 0.$$

Ainsi les diviseurs élémentaires de Δ relatifs au diviseur linéaire $a\lambda_1 + b\lambda_2$ ont pour exposants $e_{\sigma_1}, e_{\sigma_2}, \ldots, e_{\sigma_r}$ *ce qui établit la proposition.**

13. Types de faisceaux ordinaires. *La théorie de *K. Weierstrass* donne une classification naturelle des faisceaux ordinaires: deux faisceaux sont de même *classe* quand ils sont équivalents; ils seront de même *type* quand le nombre des racines distinctes du déterminant $|\lambda A' - B'|$, où le déterminant $|A'|$ est différent de zéro, et les exposants des diviseurs élémentaires correspondant à ces diverses racines sont identiques. En d'autres termes si les diviseurs élémentaires de $|\lambda A' - B'|$ sont

$$\begin{array}{l}(\lambda - c_1)^{e'_1} (\lambda - c_1)^{e'_2} \ldots (\lambda - c_1)^{e'_{k'}},\\ (\lambda - c_2)^{e''_1} (\lambda - c_2)^{e''_2} \ldots (\lambda - c_2)^{e''_{k''}},\\ \cdot\ \ \cdot\ \ \cdot\ \ \cdot\ \ \cdot\ \ \cdot\ \ \cdot\ \ \cdot\ \ \cdot\ \ \cdot\ \ \cdot\ ,\\ (\lambda - c_m)^{e_1^{(m)}} (\lambda - c_m)^{e_2^{(m)}} \ldots (\lambda - c_m)^{e_{k^{(m)}}^{(m)}},\end{array}$$

où deux quelconques des nombres $c_1, c_2, \ldots, c_m$ sont inégaux, le type à $2n$ variables correspondant sera déterminé par sa *caractéristique*

$$[(e'_1 \ldots e'_{k'})\ (e''_1 \ldots e''_{k''}) \ldots (e_1^{(m)} \ldots e_{k^{(m)}}^{(m)})],$$

les entiers e_j^i étant uniquement assujettis à la condition

$$e'_1 + \cdots + e'_{k'} + e''_1 + \cdots + e''_{k''} + \cdots + e_1^{(m)} + \cdots + e_{k^{(m)}}^{(m)} = n.$$

Le nombre des solutions entières et non négatives de cette équation est limité; le nombre des types l'est donc aussi. Nous savons d'ailleurs construire pour chaque type un faisceau représentatif $\lambda A' - B'$ pour lequel le déterminant $|A'|$ est différent de zéro.

Par exemple, pour $n = 1$ on a un seul type

$$e_1 = 1$$

de caractéristique [1]; il donne, avec les notations de *K. Weierstrass*,

$$A' = (X_1 Y_1)_1 = X_{10} Y_{10}, \qquad B' = c_1 (X_1 Y_1)_1 = c_1 X_{10} Y_{10}.$$

Pour $n = 2$ on a les trois types [1, 1], [(11)], [2] qui donnent:

[1, 1]: $A' = X_{10} Y_{10} + X_{20} Y_{20}$, $\quad B' = c_1 X_{10} Y_{10} + c_2 X_{20} Y_{20}$;

([11)]: $A' = X_{10} Y_{10} + X_{20} Y_{20}$, $\quad B' = c_1 (X_{10} Y_{10} + X_{20} Y_{20})$;

[2]: $A' = X_{10} Y_{11} + X_{11} Y_{10}$, $\quad B' = c_1 (X_{10} Y_{11} + X_{11} Y_{10}) + X_{10} Y_{10}$.

Pour $n = 3$ on a six types, caractérisés par

[111], [(11), 1], [(111)], [2, 1], [(21)], [3]

que l'on peut représenter avec des variables à un seul indice, sous la forme suivante:

[111]: $A' = x_1 y_1 + x_2 y_2 + x_3 y_3$, $\quad B' = c_1 x_1 y_1 + c_2 x_2 y_2 + c_3 x_3 y_3$;

[(11) 1]: même forme $c_1 = c_2$; [(111)]: même forme $c_1 = c_2 = c_3$;

[21]: $A' = x_1 y_2 + x_2 y_1 + x_3 y_3$, $\quad B' = c_1 (x_1 y_2 + x_2 y_1) + c_3 x_3 y_3 + x_1 y_1$;

[(21)]: se déduit de la forme précédente en faisant $c_1 = c_3$;

[3]: $A' = x_1 y_3 + x_2 y_2 + x_3 y_1$, $\quad B' = c_1 (x_1 y_3 + x_2 y_2 + x_3 y_1) + x_1 y_2 + x_2 y_1$.

Le nombre des types à considérer croît rapidement avec n; pour $n = 4$ il y en a déjà 14, pour $n = 5$ il y en a 27, etc. . . .

A. Cayley[27]) a indiqué le moyen de trouver d'une façon générale le nombre des types.

Si l'on considère d'abord un seul diviseur p et ses ordres de multiplicité $l_n, l_{n-1}, \ldots$ dans $\Delta, D_{n-1}, \ldots$ on a, pour chaque valeur de l_n, toutes les solutions de l'équation

$$l_n = f + 2f' + 3f'' + 4f''' + \cdots,$$

où $f, f', f'', \ldots$ sont des entiers positifs. Les valeurs de $l_{n-1}, l_{n-2}, \ldots$ sont données par

$$l_{n-1} = f' + 2f'' + 3f''' + \cdots; \quad l_{n-2} = f'' + 2f''' + 3f^{(\mathrm{IV})} + \cdots; \text{ etc.}$$

d'où les diviseurs élémentaires

$$e_n = f + f' + f'' + \cdots; \quad e_{n-1} = f' + f'' + \cdots; \quad e_{n-2} = f'' + \cdots$$

Les nombres de types pour $l_n = 1, 2, 3, 4, 5, 6, 7, 8, \ldots$, sont respectivement 1, 2, 3, 5, 7, 11, 15, 22, . .; ce sont les coefficients de $x, x^2, x^3, x^4, x^5, \ldots$ dans le développement de

$$(1 - x)^{-1} (1 - x^2)^{-2} (1 - x^3)^{-3} \ldots$$

qui se présentent dans la *partition des nombres.*

Si l'on considère tous les diviseurs p de Δ, on aura deux problèmes de partition superposés.

On forme aisément de proche en proche les tableaux des types. *A. Cayley* donne pour $n = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11$ les nombres 1, 3, 6, 14, 27, 58, 111, 223, 424, 817, 1527.

Signalons, en terminant, le cas intéressant où *la caractéristique ne renferme que des unités.*

27) J. reine angew. Math. 50 (1855), p. 313/7; Papers 2, Cambridge 1889, p. 216/20.

Les formes réduites sont alors

$$A' = x_1 y_1 + x_2 y_2 + \cdots + x_n y_n,$$
$$B' = c_1 x_1 y_1 + c_2 x_2 y_2 + \cdots + c_n x_n y_n,$$

où $c_1, c_2, \ldots, c_n$ peuvent être différents ou non.

On a vu que ce cas est caractérisé par le fait que *tout diviseur linéaire p qui figure dans* $\Delta = |\lambda_1 A + \lambda_2 B|$ *à la puissance l figure à la puissance* $(l-1)$ *dans le plus grand commun diviseur des mineurs du premier ordre de* Δ.*

Équivalence des faisceaux singuliers d'après Kronecker[28]).

14. Relations linéaires entre les dérivées de $\lambda\varphi - \psi$. *Soient φ, ψ deux formes bilinéaires dont *chacune*[29]) dépend des variables $x_1, x_2, \ldots, x_r$ et $y_1, y_2, \ldots, y_s$; *supposons le déterminant* $|\lambda_1\varphi + \lambda_2\psi|$ *identiquement nul* (ce qui a lieu pour r différent de s) et posons, pour abréger l'écriture,

$$\varphi_i = \frac{\partial\varphi}{\partial x_i}, \ \psi_i = \frac{\partial\psi}{\partial x_i}, \ \lambda\varphi - \psi = f, \ \lambda\varphi_i - \psi_i = f_i.$$

Puisque $|\lambda\varphi - \psi| \equiv 0$, il y a entre $f_1, f_2, \ldots, f_r$ au moins une relation linéaire et homogène

$$\sum_{i=1}^{i=r} A_i f_i = 0,$$

où les A_i peuvent dépendre de λ. S'ils sont de degré g par rapport à λ, une transformation linéaire des x, à coefficients indépendants de λ, ne peut que conserver ou abaisser ce degré; une transformation linéaire des y ne modifie par les A.

Parmi toutes les relations linéaires qui peuvent lier les f_i prenons celle dont le degré en λ est *le plus petit*; soit m ce degré et

$$\sum_{\alpha=0}^{\alpha=m} \sum_{\beta=1}^{\beta=r} c_{\alpha\beta}\lambda^\alpha f_\beta = C_0 + C_1\lambda + \cdots + C_m\lambda^m = 0$$

cette relation. *Le nombre m* est au plus égal *au plus petit des entiers* s et r (on le démontrera tout à l'heure).

On a nécessairement $m > 0$, car, pour $m = 0$, la condition

$$c_{01}f_1 + c_{02}f_2 + \cdots + c_{0r}f_r = 0$$

donne

$$\sum_{i=1}^{i=r} c_{0i}\varphi_i = \sum_{i=1}^{i=r} c_{0i}\psi_i = 0$$

28) *L. Kronecker,* Sitzgsb. Akad. Berlin 1890, p. 1225.

29) *Il suffit d'ajouter des termes à coefficients nuls pour réaliser cette condition.*

et, si l'on suppose par exemple $c_{0\gamma}$ différent de zéro, en posant

$$x_\beta = x'_\beta + c_{0\gamma}x'_\gamma \qquad [\beta = 1, 2, \ldots, \gamma-1, \gamma+1, \ldots, r]$$
$$x_\gamma = x'_\gamma,$$

on aura

$$\varphi = x_1\varphi_1 + \cdots + x_r\varphi_r = x'_1\varphi_1 + \cdots + x'_{\gamma-1}\varphi_{\gamma-1} + x'_{\gamma+1}\varphi_{\gamma+1} + \cdots + x'_r\varphi_r + x'_\gamma[c_{01}\varphi_1 + \cdots + c_{0r}\varphi_r];$$

x'_γ disparaît de φ et aussi de ψ.

Une substitution linéaire indépendante de λ abaisse donc d'une unité le nombre des variables x.

Nous supposerons, qu'ayant de cette manière tenu compte s'il y a lieu des relations pour lesquelles $m = 0$, *le faisceau*

$$\lambda_1\varphi + \lambda_2\psi$$

n'est équivalent à aucun autre où le nombre des x soit moindre que r et le nombre des y moindre que s.

Dans la relation de degré le plus petit m,

$$C_0 + C_1\lambda + \cdots + C_m\lambda^m = 0,$$

les coefficients $C_0, C_1, \ldots, C_m$ *sont linéairement indépendants,* c'est-à-dire qu'il n'existe aucune relation

$$a_0C_0 + a_1C_1 + \cdots + a_mC_m = 0$$

où les a soient indépendants de λ. On déduirait en effet d'une telle relation l'identité en λ

$$(a_0\lambda^m + a_1\lambda^{m-1} + \cdots + a_m)(C_0 + C_1\lambda + \cdots + C_m\lambda^m) = 0$$

qui s'écrit, puisque le terme en λ^m manque dans le produit,

$$f_1g_1(\lambda) + \cdots + f_rg_r(\lambda) + \lambda^{m+1}[f_1h_1(\lambda) + \cdots + f_rh_r(\lambda)] = 0,$$

où les g et les h sont d'ordre au plus $(m-1)$ en λ.

En remplaçant les f_i par leurs expressions $\lambda\varphi_i - \psi_i$, on a une première partie de degré $\leqq m$ et une seconde de degré au moins $(m+1)$. On en déduira donc

$$f_1h_1(\lambda) + f_2h_2(\lambda) + \cdots + f_rh_r(\lambda) = 0$$

c'est-à-dire une relation linéaire entre les f_i d'ordre $(m-1)$ au plus, ce qui est contraire à l'hypothèse faite sur m.

Il suit de là que $(m+1)$, nombre des formes C_i, est au plus égal à s, nombre des variables y, et aussi au plus égal à r, nombre des formes $f_1, f_2, \ldots, f_r$.

Le tableau

$$c_{\alpha\beta} \qquad (\alpha = 0, 1, \ldots, m;\ \beta = 1, 2, \ldots, r)$$

a donc un déterminant *principal,* de degré $(m+1)$, différent de zéro;

on peut ajouter des éléments $c_{p\beta}$ de façon à obtenir un tableau carré dont le déterminant $|c_{\alpha\beta}|$ soit différent de zéro.*

15. Réduction du faisceau. *Faisons la substitution

$$x_k = \sum_{(i,k)} c_{ik} x'_i \qquad (i=0,1,\ldots,r-1;\ k=1,\ldots,r);$$

soient φ', ψ', f' les transformées de φ, ψ, f; on aura

$$f'_i = \sum_{j=1}^{j=r} c_{ij} f_j$$

et la relation de degré le plus petit en λ s'écrira

$$C_0 + C_1\lambda + \cdots + C_m\lambda^m = f'_0 + f'_1\lambda + \cdots + f'_m\lambda^m = 0$$

ou encore

$$\sum_{i=0}^{i=m} (\lambda\varphi'_i - \psi'_i)\lambda^i = 0.$$

Envisagée comme identité en λ, elle donne donc

$$\psi'_0 = \varphi'_m = 0, \quad \psi'_1 = \varphi'_0, \quad \psi'_2 = \varphi'_1, \quad \ldots, \quad \psi'_m = \varphi'_{m-1}$$

et aussi

$$f'_0 = \lambda\psi'_1, \quad f'_1 = \lambda\psi'_2 - \psi'_1, \quad \ldots, \quad f'_m = -\psi'_m.$$

Il n'existe aucune relation linéaire entre $\psi'_1, \psi'_2, \ldots, \psi'_m$ car on en déduirait entre $f'_0, f'_1, \ldots, f'_m$ une relation, de degré $(m-1)$ au plus en λ, qui donnerait en $f_1, f_2, \ldots, f_r$ une relation de même degré au plus.

On transforme alors les y par la substitution

$$Y_\alpha = \psi'_\alpha = \varphi'_{\alpha-1} \qquad (\alpha = 1, \ldots, m),$$
$$Y_{m+1} = y_{m+1}, \quad \ldots, \quad Y_s = y_s$$

ce qui donne

$$\lambda_1\varphi' + \lambda_2\psi' = \sum_{i=0}^{i=m} (\lambda_1\varphi'_i + \lambda_2\psi'_i)x'_i$$
$$= \sum_{\alpha=1}^{\alpha=m} (\lambda_1 x'_{\alpha-1} + \lambda_2 x'_\alpha)\, Y_\alpha + \sum_{k=1}^{k=s}\sum_{p=m+1}^{p=r-1} (\lambda_1 a_{pk} + \lambda_2 b_{pk}) x'_p Y_k.$$

En posant

$$X_0 = x'_0 + \sum_{p=m+1}^{p=r-1} a_{p1} x'_p,$$

et, pour $\alpha = 1, 2, \ldots, m$,

$$X_\alpha = x'_\alpha + \sum_{p=m+1}^{p=r-1} b_{p\alpha} x'_p,$$

on aura enfin

$$S = \sum_{\alpha=1}^{\alpha=m} (\lambda_1 X_{\alpha-1} + \lambda_2 X_\alpha) Y_\alpha + \lambda_1 \sum_{\alpha=2}^{\alpha=m} u_\alpha Y_\alpha + \lambda_1 \Phi + \lambda_2 \Psi,$$

où $u_1, u_2, \ldots, u_m$ sont des fonctions linéaires de $X_{m+1}, X_{m+2}, \ldots, X_{r-1}$ et où Φ et Ψ sont des formes bilinéaires des variables

$$X_{m+1}, X_{m+2}, \ldots, X_{r-1} \quad \text{et} \quad Y_{m+1}, Y_{m+2}, \ldots, Y_s.$$

Remarque. Soit R le rang du déterminant

$$|\lambda_1\varphi + \lambda_2\psi|;$$

admettons que φ et ψ soient choisis de telle sorte que le plus grand commun diviseur de tous les mineurs de degré R de ce déterminant ne soit pas divisible par λ_2, en d'autres termes que $|\varphi|$ soit de rang R. Nous allons montrer qu'en donnant au faisceau la forme précédente, où

$$\lambda_1\Phi + \lambda_2\Psi$$

est un faisceau à $(r-m-1)$ variables X et $(s-m)$ variables Y, le déterminant

$$|\lambda_1\Phi + \lambda_2\Psi|$$

est de même rang que le déterminant $|\Phi|$.

Il suffit de former le déterminant $|S|$ du faisceau $\lambda_1\varphi + \lambda_2\psi = S$:

$$|S| = \begin{vmatrix} S_{X_0Y_1} & S_{X_1Y_1} & \ldots & S_{X_{r-1}Y_1} \\ \cdot & \cdot & \cdot & \cdot \\ S_{X_0Y_s} & S_{X_1Y_s} & \ldots & S_{X_{r-1}Y_s} \\ 0 & 0 & \ldots & 0 \\ \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \ldots & 0 \end{vmatrix}$$

en posant

$$S_{X_iY_k} = \frac{\partial^2 S}{\partial X_i \partial Y_k}$$

(les lignes nulles disparaissent si $s = r$). Le rang du système S_1 des m premières lignes est m; soit m' celui du système S_2 des $(r-m)$ dernières.

Tous les mineurs de $|S|$ de degré supérieur à $(m+m')$ sont nuls puisqu'ils renferment plus de m' des $(r-m)$ dernières lignes, donc

$$R = m + m'.$$

Tout mineur de degré $(m+m')$ de S qui n'est pas nul, contient m' lignes de S_2, c'est donc une combinaison linéaire de certains mineurs de degré m' de $|\lambda_1\Phi + \lambda_2\Psi|$.

Si tous ces derniers s'annulaient pour $\lambda_2 = 0$, il en serait de même des premiers et R ne serait pas le rang de $|S|$.

Cette remarque faite, revenons à la forme obtenue pour le faisceau $\lambda_1\varphi + \lambda_2\psi$.

La première partie

$$\sum_{\alpha=1}^{\alpha=m} (\lambda_1 X_{\alpha-1} + \lambda_2 X_\alpha)\, Y_\alpha$$

se déduit aisément de la forme réduite de *K. Weierstrass*

$$(\lambda_1 + c_\varrho \lambda_2)\, \Phi_\varkappa^{(\varrho)} + \lambda_2\, \Psi_\varkappa^{(\varrho)};$$

il suffit d'y poser

$$c_\varrho = 0, \quad Y^{(\varrho)}_{\varkappa, e_\varkappa^{(\varrho)}-1} = 0, \quad e_\varkappa^{(\varrho)} - 1 = m, \quad X^{(\varrho)}_{\varkappa, m} = X_0,$$
$$X^{(\varrho)}_{\varkappa, m-\alpha} = X_\alpha, \; Y^{(\varrho)}_{\varkappa, \alpha-1} = Y_\alpha \qquad (\alpha = 1, 2, \ldots, m).$$

Si le déterminant

$$|\lambda_1 \Phi + \lambda_2 \Psi|$$

ne s'annule pas identiquement, le faisceau ordinaire $\lambda_1 \Phi + \lambda_2 \Psi$ peut être réduit par la méthode de *K. Weierstrass* à la forme

$$\sum_{\varkappa=1}^{\varkappa=n} (\lambda_1 + c_\varrho \lambda_2)\, \Phi_\varkappa^{(\varrho)} + \lambda_2\, \Psi_\varkappa^{(\varrho)}$$

puisque $|\Phi|$ est différent de 0. Les transformations de variables

$$X_p \text{ (où } p > m), \qquad Y_q \text{ (où } q > m),$$

qui conduisent à cette forme réduite, n'altèrent pas la première partie et conservent la forme de la seconde partie

$$\sum_{\alpha=1}^{\alpha=m} u_\alpha Y_\alpha,$$

où les u_α ne dépendent que de $X_{m+1}, X_{m+2}, \ldots, X_{r-1}$.

Si le déterminant

$$|\lambda_1 \Phi + \lambda_2 \Psi| \equiv 0$$

est de rang R', on a vu que $|\Phi|$ est aussi de même rang. On peut alors appliquer au faisceau singulier

$$\lambda_1 \Phi + \lambda_2 \Psi$$

la méthode de réduction précédente.

Au bout d'un nombre limité d'essais on aura donc effectué la réduction à trois espèces de groupements:

1°) des groupements de la forme réduite de *K. Weierstrass*;

2°) des groupements qui se déduisent de cette forme par une modification des indices des variables (indiquée plus haut), l'hypothèse $c_\varrho = 0$ et l'annulation de l'une des variables (celle dont le second indice est le plus élevé);

3°) des groupements analogues à

$$u_1 Y_1 + u_2 Y_2 + \cdots + u_m Y_m,$$

où u_α dépend uniquement de $X_{m+1}, X_{m+2}, \ldots, X_{r-1}$.

Nous supposerons que l'on a pu réduire le faisceau

$$\lambda_1 \Phi + \lambda_2 \Psi$$

à une somme de groupements des deux premières espèces (le dernier faisceau est évidemment réduit de cette manière) et nous allons montrer que la même chose est possible pour

$$\lambda_1 \varphi + \lambda_2 \psi,$$

c'est-à-dire qu'on peut faire disparaître

$$u_1 Y_1 + u_2 Y_2 + \cdots + u_m Y_m.$$

La réduction de

$$\lambda_1 \Phi + \lambda_2 \Psi$$

à des groupements des deux premières espèces conduit à introduire certaines combinaisons des

$$X_{m+1}, X_{m+2}, \ldots, X_{r-1}$$

comme nouvelles variables $X^{(\varrho)}_{\varkappa\mu}$. Montrons que $u_1, u_2, \ldots, u_m$ *s'expriment uniquement avec les* $X^{(\varrho)}_{\varkappa\mu}$.

S'il subsistait en effet une variable X_p, après l'introduction des $X^{(\varrho)}_{\varkappa\mu}$ dans les u, en formant les $(m+1)$ dérivées de

$$\lambda_1 \varphi + \lambda_2 \psi$$

par rapport à $X_1, X_2, \ldots, X_m, X_p$ on obtiendrait $(m+1)$ formes linéaires en $Y_1, Y_2, \ldots, Y_m$ qui seraient par suite liées par une relation linéaire d'ordre au plus égal à $(m-1)$ en $\lambda = \frac{\lambda_1}{\lambda_2}$.

On peut donc écrire à nouveau le faisceau singulier sous la forme suivante (où l'on a supprimé dans la première partie les indices $\varkappa$ et ϱ):

$$\lambda_1 \varphi + \lambda_2 \psi = \lambda_1 \Phi^0 + \lambda_2 \Psi^0 + \lambda_1 \sum_{\alpha=1}^{\alpha=e-2} F_\alpha Y_\alpha + \sum_{(\varkappa, \varrho)} [(\lambda_1 + \lambda_2 c_\varrho)\, \Phi_\varkappa^{(\varrho)} + \lambda_2\, \Psi_\varkappa^{(\varrho)}]$$

avec

$$\Phi^0 = X_1 Y_{e-2} + X_2 Y_{e-3} + \cdots + X_{e-1} Y_0,$$
$$\Psi^0 = X_0 Y_{e-2} + X_1 Y_{e-3} + \cdots + X_{e-2} Y_0;$$

les F sont des formes linéaires en $X^{(\varrho)}_{\varkappa\mu}$ et la troisième partie peut comprendre des groupements de la forme réduite de *K. Weierstrass*, de la forme modifiée qui constitue la première partie, enfin de cette même forme où X et Y sont échangés.

Considérons maintenant la seconde partie

$$F_1 Y_1 + F_2 Y_2 + \cdots + F_{e-2} Y_{e-2}$$

et supposons que F_α renferme la variable $X^{(\varrho)}_{\varkappa\mu}$ avec le coefficient D_α. Si cette variable figure dans le coefficient de λ_1, c'est-à-dire dans un terme $\Phi^{(\varrho)}_{\varkappa\mu}$, les deux variables

$$X_{e-\alpha-2} \text{ et } Y^{(\varrho)}_{\varkappa\nu} \qquad (\nu = e^{(\varrho)}_\varkappa - \mu - 1)$$

coefficients de $Y_{\alpha+1}$ et $X^{(\varrho)}_{\varkappa\mu}$ figurent uniquement dans l'ensemble (auquel on ajoute le terme $\lambda_1 D_\alpha X^{(\varrho)}_{\varkappa\mu} Y_\alpha$ qu'on veut faire disparaître)

$$(\lambda_1 Y_{\alpha+1} + \lambda_2 Y_\alpha) X_{e-\alpha-2} + \lambda_1 D_\alpha X^{(\varrho)}_{\varkappa\mu} Y_\alpha$$
$$+ [\lambda_1 + c_\varrho \lambda_2) X^{(\varrho)}_{\varkappa\mu} + \lambda_2 X^{(\varrho)}_{\varkappa,\mu-1}] Y^{(\varrho)}_{\varkappa\nu}.$$

Il suffit de poser

$$X_{e-\alpha-2} = \xi_{e-\alpha-2} + D_\alpha(c_\varrho X^{(\varrho)}_{\varkappa\mu} + X^{(\varrho)}_{\varkappa,\mu-1}),$$
$$Y^{(\varrho)}_{\varkappa\nu} = \eta^{(\varrho)}_{\varkappa\nu} - D_\alpha Y_\alpha$$

pour transformer cet ensemble en

$$(\lambda_1 Y_{\alpha+1} + \lambda_2 Y_\alpha)\xi_{e-\alpha-2} + \lambda_1 D_\alpha(c_\varrho X^{(\varrho)}_{\varkappa\mu} + X^{(\varrho)}_{\varkappa,\mu-1}) Y_{\alpha+1}$$
$$+ [(\lambda_1 + c_\varrho \lambda_2) X^{(\varrho)}_{\varkappa\mu} + \lambda_2 X^{(\varrho)}_{\varkappa,\mu-1}] \eta^{(\varrho)}_{\varkappa\nu};$$

on voit que la première et la troisième partie gardent leur forme, le terme $D_\alpha X^{(\varrho)}_{\varkappa\mu}$ disparaît de F_α et $F_{\alpha+1}$ est remplacé par

$$F_{\alpha+1} + D_\alpha(c_\varrho X^{(\varrho)}_{\varkappa\mu} + X^{(\varrho)}_{\varkappa,\mu-1}).$$

Pour faire disparaître tous les termes des F_α, on fera donc d'abord disparaître $X^{(\varrho)}_{\varkappa,e^{(\varrho)}_\varkappa-1}$ de F_2, puis de F_3 et ainsi de suite; on répétera l'opération pour $X^{(\varrho)}_{\varkappa,e^{(\varrho)}_\varkappa-2}$, puis pour $X^{(\varrho)}_{\varkappa,e^{(\varrho)}_\varkappa-3}$ et ainsi de suite et ceci pour chacune des valeurs de $\varkappa$.

On élimine ainsi des F_α tous les termes qui figurent dans une fonction $\Phi^{(\varrho)}_{\varkappa\mu}$; ce sont tous les

$$X^{(\varrho)}_{\varkappa\mu} \qquad (\mu = 0, 1, \ldots, e^{(\varrho)}_\varkappa - 1)$$

si le groupement correspondant a la forme de *K. Weierstrass* ou la forme dans laquelle

$$c_\varrho = 0, \ X^{(\varrho)}_{\varkappa,e^{(\varrho)}_\varkappa-1} = 0.$$

Il ne subsiste donc que les $X^{(\varrho)}_{\varkappa 0}$ qui proviennent de groupements où

$$c_\varrho = 0, \ X^{(\varrho)}_{\varkappa,e^{(\varrho)}_\varkappa-1} = 0.$$

On fait disparaître ces termes très facilement.

Supposons que F_α renferme le terme $D_\alpha X^{(\varrho)}_{\varkappa 0} Y_\alpha$ et, pour simplifier les notations, représentons le groupement qui renferme cette variable

$X^{(\varrho)}_{\varkappa 0}$, écrite simplement X'_0, par $\lambda_1 \Phi'_0 + \lambda_2 \Psi'_0$ ou explicitement par

$$\lambda_1(X'_1 Y'_{e'-2} + X'_2 Y'_{e'-3} + \cdots + X'_{e'-1} Y'_0)$$
$$+ \lambda_2(X'_0 Y'_{e'-2} + X'_1 Y'_{e'-3} + \cdots + X'_{e'-2} Y'_0).$$

Considérons l'ensemble des termes obtenus en ajoutant à ceux-là la première partie

$$\lambda_1(X_1 Y_{e-2} + X_2 Y_{e-3} + \cdots + X_{e-1} Y_0)$$
$$+ \lambda_2(X_0 Y_{e-2} + X_1 Y_{e-3} + \cdots + X_{e-2} Y_0)$$

et le terme $D_\alpha X'_0 Y_\alpha$ à faire disparaître. Nous poserons

$$Y'_\nu = \eta_\nu + D_\alpha Y_{\alpha-\mu} \quad (\mu = 1, 2, \ldots, \alpha; \mu + \nu = e' - 1)$$

et l'ensemble étudié deviendra

$$(\lambda_1 X'_1 + \lambda_2 X'_0)\eta_{e'-2} + (\lambda_1 X'_2 + \lambda_2 X'_1)\eta_{e'-3} + \cdots + (\lambda_1 X'_\alpha + \lambda_2 X'_{\alpha-1})\eta'_{e-1-1}$$
$$+ (\lambda_1 X'_{\alpha+1} + \lambda_2 X'_\alpha) Y'_{e-\alpha} + \cdots + (\lambda_1 X'_{e'-2} + \lambda_2 X'_{e'-2})$$
$$+ Y_0[\lambda_1(X_{e-1} + D_\alpha X'_\alpha) + \lambda_2(X_{e-2} + D_\alpha X'_{\alpha-1})]$$
$$+ Y_1[\lambda_1(X_{e-2} + D_\alpha X'_{\alpha-1}) + \lambda_2(X_{e-3} + D_\alpha X'_{\alpha-2})]$$
$$+ Y_{\alpha-1}[\lambda_1(X_{e-\alpha} + D_\alpha X'_1) + \lambda_2(X_{e-\alpha-1} + D_\alpha X'_0)]$$
$$+ \cdots + Y_\alpha[\lambda_1(Y_{e-\alpha-1} + D_\alpha X'_0) + \lambda_2 X_{e-\alpha-2}]$$
$$+ Y_{\alpha+1}(\lambda_1 X_{e-\alpha-2} + \lambda_2 X_{e-\alpha-3}) + \cdots$$

On voit qu'il suffit d'y poser:

$$X_{e-1} + D_\alpha X'_\alpha = \xi_{e-1}, \ X_{e-2} + D_\alpha X'_{\alpha-1} = \xi_{e-2}, \ldots, \ X_{e-\alpha-1} + D_\alpha X'_0 = \xi_{e-\alpha-1}$$

pour retrouver la forme initiale (sauf le terme $D_\alpha X'_0 Y_\alpha$, où certains X et Y sont remplacés par les ξ et η de même indice.

Remarque: Pour que le raisonnement puisse se répéter pour chaque valeur de α, il faut que l'indice ν soit au moins égal à zéro et comme α peut atteindre $e - 2$, il faut $e' - 1 - (e - 2) > 0$.

On démontre aisément que $(e' - e)$ *est toujours positif.* Considérons le faisceau

$$\lambda_1 \varphi + \lambda_2 \psi = S$$

comme fonction des variables

$$X_1, \ X_2, \ldots, X_{e-1}, X'_0, \ldots, \ X'_{e'-1}$$

qui sont en nombres $e + e' - 1$; les dérivées de S relatives à ces variables ne dépendent que de

$$Y_0, \ Y_1, \ldots, \ Y_{e-2}, \ Y'_0, Y'_1, \ldots, \ Y'_{e'-2}$$

qui sont en nombre $e + e' - 2$. Il existe donc entre ces dérivées une relation linéaire qu'on déduit de l'expression

$$S = \lambda_1 \Phi_0 + \lambda_2 \Psi_0 + \lambda_1 \sum_{\alpha=1}^{\alpha=e-2} F_\alpha Y_\alpha + \lambda_1 \Phi'_0 + \lambda_2 \Psi'_0 + \cdots,$$

où F_α renferme un seul terme $D_\alpha X'_0$ à considérer.

Les formules

$$\frac{\partial S}{\partial X_{e-1}} = \lambda_1 Y_0, \quad \frac{\partial S}{\partial X_{e-i}} + \lambda_1 Y_i + \lambda_2 Y_{i-1} \ (i=2,\ldots,e-1)$$

$$\frac{\partial S}{\partial X'_{e'-1}} = \lambda_1 Y'_0, \quad \frac{\partial S}{\partial X'_{e'-i}} = \lambda_1 Y'_{i-1} + \lambda_2 Y'_{i-2} \ (i=2,\ldots,e'-1)$$

$$\frac{\partial S}{\partial X'_0} = \lambda_2 Y'_{e-2} + \lambda_1 \sum_{\alpha=1}^{\alpha=e-2} D_\alpha Y_\alpha$$

donnent aisément pour cette relation

$$\lambda_1^{e'}\left[\frac{\partial S}{\partial X_1} A_1 + \ldots + \frac{\partial S}{\partial X_m} A_m\right] + \lambda_1^m \left[\frac{\partial S}{\partial X'_0} \lambda_1^{e'-1} - \frac{\partial S}{\partial X'_1} \lambda_1^{e'-2} \lambda_2 + \cdots\right] = 0,$$

où le coefficient de $\lambda_1^{e'}$ est de degré $(m-1)$ en λ_1, λ_2. Si $e' \leqq m$ c'est-à-dire $e' \leqq e-1$ on aurait, en divisant par $\lambda_1^{e'}$, une relation entière d'ordre $(m-1)$ au plus en $\frac{\lambda_1}{\lambda_2}$ entre les dérivées relatives aux X et aux X', ce qui est contraire à l'hypothèse faite sur m.

Tout faisceau singulier de formes bilinéaires

$$\lambda_1 \varphi + \lambda_2 \psi$$

dans lequel le rang de $|\varphi|$ *est égal à celui de* $|\lambda_1 \varphi + \lambda_2 \psi|$ se laisse donc mettre sous la forme d'une *somme de groupements de la forme de Weierstrass*

$$\text{(W)} \quad \begin{aligned} &(\lambda_1 + c_1 \lambda_2)(X_0 Y_{e-1} + X_1 Y_{e-2} + \cdots + X_{e-1} Y_0) \\ &\qquad + \lambda_2 X_0 Y_{e-2} + \cdots + X_{e-2} Y_0) \end{aligned}$$

et de groupements de l'une et l'autre des deux formes

$$(\mathrm{K}_y) \quad \lambda_1(X_1 Y_{e-2} + \cdots + X_{e-1} Y_0) + \lambda_2(X_0 Y_{e-2} + \cdots + X_{e-2} Y_0)$$

et

$$(\mathrm{K}_x) \quad \lambda_1(X_0 Y_{e-1} + \cdots + X_{e-2} Y_1) + \lambda_2(X_0 Y_{e-2} + \cdots + X_{e-2} Y_0),$$

qui se déduisent de la première en faisant

$$c_1 = 0, \ Y_{e-1} = 0 \ \textit{ou} \ X_{e-1} = 0.$$

Deux quelconques de ces groupements n'ont aucune variable commune.

Un groupement (W) dépend de e variables X et de e variables Y; le déterminant de la forme W est au signe près $(\lambda_1 + c\lambda_2)^e$, il n'a qu'un diviseur élémentaire qui est lui-même.

Un groupement (K_y) dépend de e variables X et $(e-1)$ variables Y; son déterminant est nul. Les dérivées de ce groupement K_y relatives aux X sont liées par une relation linéaire de degré $(e-1)$ en $\frac{\lambda_1}{\lambda_2}$. On a $(e-1) > 0$.

Des observations analogues s'appliquent à (K_x).

Les formes (K_x) et (K_y) n'ont pas de diviseurs élémentaires; elles sont entièrement déterminées par le nombre entier e.*

16. Signification des parties du faisceau réduit. *Il est facile de donner la signification, rapportée au faisceau initial

$$\lambda_1 \varphi + \lambda_2 \psi,$$

des diverses parties du faisceau réduit et des constantes correspondantes.

Si nous écrivons les groupements (W) sous leur forme générale

$$\lambda_1[a_\sigma (X_\sigma Y_\sigma)_{e_\sigma} - h\,(X_\sigma Y_\sigma)_{e_\sigma - 1}] + \lambda_2[b_\sigma (X_\sigma Y_\sigma)_{e_\sigma} + g(X_\sigma Y_\sigma)_{e_\sigma - 1}]$$

où $g a_\sigma + h b_\sigma = 1$, chacun d'eux donne un diviseur élémentaire $(a_\sigma \lambda_1 + b_\sigma \lambda_2)^{e_\sigma}$.

Leur ensemble est donc la somme des faisceaux de Weierstrass qui correspondent aux divers diviseurs élémentaires de $\lambda_1 \varphi + \lambda_2 \psi$.

Soit un faisceau singulier

$$\lambda_1 \varphi + \lambda_2 \psi$$

dépendant de $2n$ variables (x_i, y_k) et soit τ le *rang* du système des coefficients de la forme générale

$$\lambda_1 \varphi + \lambda_2 \psi = \omega.$$

Il existera entre les dérivées $\frac{\partial \omega}{\partial x_i}$ (et aussi entre les dérivées $\frac{\partial \omega}{\partial y_k}$) exactement $(n-\tau)$ relations linéaires et homogènes indépendantes.

On peut classer ces relations d'après leurs degrés en $\frac{\lambda_1}{\lambda_2}$; soient donc, pris dans l'ordre croissant,

$$P_1, P_2, \ldots, P_{n-\tau},$$

les degrés respectifs des relations entre les $\frac{\partial \omega}{\partial x_i}$ et de même

$$Q_1, Q_2, \ldots, Q_{n-\tau}$$

les degrés correspondants pour les relations qui lient les $\frac{\partial \omega}{\partial y_k}$.

Les nombres P, Q sont, d'après une remarque antérieure, des *invariants numériques* du faisceau.

Si les ϱ premiers P sont nuls ainsi que les σ premiers Q on a vu que le faisceau peut être remplacé par un autre qui ne renferme que $n - \varrho = r$ variables de la première série, $n - \sigma = s$ variables de la seconde série; c'est ce dernier faisceau que nous avons réduit.

Dans le faisceau réduit l'existence de ces ϱ relations d'ordre zéro entre les $\frac{\partial \omega}{\partial x_i}$ et des σ relations d'ordre zéro entre les $\frac{\partial \omega}{\partial y_k}$ se traduit par ce fait qu'en écrivant la forme réduite de manière à ce qu'elle renferme autant de variables X que de variables Y on est obligé d'ajouter au moins ϱ variables X et σ variables Y.

Soit maintenant (K_y) un faisceau avec e variables X et $(e-1)$ variables Y; si l'on considère la forme obtenue en ajoutant à K_y un des groupements (W) avec $2e'$ variables X, Y, *le rang de cette forme* $(\mathrm{W}+\mathrm{K}_y)$ est $e-1+e'$, comme le nombre des variables X est $e'+e$ il n'existe qu'*une* relation entre les dérivées

$$\frac{\partial(\mathrm{W}+\mathrm{K}_y)}{\partial \mathrm{X}_i} \qquad (i=1,2,\ldots,e+e');$$

c'est, par suite, la relation qui lie les dérivées

$$\frac{\partial \mathrm{K}_y}{\partial \mathrm{X}_i} \qquad (i=1,2,\ldots,e).$$

Si de même on considère la forme

$$\mathrm{K}_y+\mathrm{K}_x,$$

obtenue en ajoutant à K_y un groupement avec $e'-1$ variables X et e' variables Y, le rang du système des coefficients est encore $e+e'-1$ et la seule relation linéaire qui lie les dérivées

$$\frac{\partial(\mathrm{K}_y+\mathrm{K}_x)}{\partial \mathrm{X}}$$

est celle qui lie les dérivées

$$\frac{\partial \mathrm{K}_y}{\partial \mathrm{X}_i} \qquad (i=1,2,\ldots,e).$$

Enfin, en considérant la forme

$$\mathrm{K}_x+\mathrm{K}_x',$$

où K_x' est à e' variables X et à $(e'-1)$ variables Y, son rang est $e+e'-2$ et les deux relations qui lient les dérivées

$$\frac{\partial(\mathrm{K}_x+\mathrm{K}_x')}{\partial \mathrm{X}}$$

sont celles qui lient séparément les dérivées

$$\frac{\partial \mathrm{K}_x}{\partial \mathrm{X}_i} \quad (i=1,2,\ldots,e), \qquad \frac{\partial \mathrm{K}_x'}{\partial \mathrm{X}_i'} \quad (i=1,2,\ldots,e');$$

ces relations sont indépendantes car elles sont relatives à des variables différentes sur la forme réduite.

On conclut de là que *la forme réduite de Kronecker contient autant de groupements* (K_y) *qu'il y a de nombres* $P_1, P_2, \ldots, P_{n-\tau}$ *différents de zéro; chacun de ces nombres augmenté de l'unité donne le nombre des variables* X *du groupement.* On peut formuler une conclusion analogue pour les groupements (K_x).

Ainsi *les entiers* e (nombre de variables X d'un groupement K_y), *diminués d'une unité, donnent les degrés différents de zéro* $P_1, P_2, \ldots, P_{n-\tau}$

en $\frac{\lambda_1}{\lambda_2}$, *des relations independantes entre les dérivées* $\frac{\partial \omega}{\partial x}$ *de la forme générale*

$$\omega=\lambda_1\varphi+\lambda_2\psi.^*$$

17. Conditions d'équivalence. *La forme réduite obtenue par *L. Kronecker* est entièrement déterminée par les diviseurs élémentaires du faisceau singulier

$$\omega=\lambda_1\varphi+\lambda_2\psi$$

à r variables x et s variables y et par les entiers

$$P_1, P_2, \ldots, P_{r-\tau}, \; Q_1, Q_2, \ldots, Q_{s-\tau}$$

supposés différents de zéro, qui sont les degrés des relations entre les dérivées $\frac{\partial \omega}{\partial x_i}$ et ceux des relations entre les dérivées $\frac{\partial \omega}{\partial y_k}$; il suit de là que *si ces éléments sont les mêmes pour deux faisceaux singuliers, ces deux faisceaux sont équivalents et réciproquement.*

Nous savons qu'on peut déterminer rationnellement les *produits élémentaires*

$$E_1, E_2, \ldots, E_\tau,$$

τ désignant le rang du système des coefficients de ω; il en est évidemment de même pour les nombres

$$P_1, \ldots, P_{r-\tau}, \; Q_1, \ldots, Q_{s-\tau}.$$

On ramène donc rationnellement un faisceau singulier à sa forme réduite et on le transforme rationnellement en tout faisceau équivalent.

L. Kronecker introduit, au lieu des éléments P_i, Q_k et e_σ [ce dernier est l'exposant du diviseur élémentaire d'un groupement (W)], les entiers

$$n_\sigma=2e_\sigma, \quad n_i^0=2P_i+1, \quad \overline{n}_k^0=2Q_k+1$$

qui représentent respectivement *les nombres de variables des groupements*

$$\mathrm{W}, \; \mathrm{K}_y, \; \mathrm{K}_x.$$

Si l'on considère un faisceau singulier

$$\lambda_1\varphi+\lambda_2\psi$$

à $2n$ *variables*

$$x_i, \; y_k \qquad (i,k=1,2,\ldots,n),$$

sa réduction donnera lieu à une égalité:

$$2n=\sum_{(\alpha)} n_\alpha^0+\sum_{(\beta)}\overline{n}_\beta^0+\sum_{(\gamma)} n_\gamma$$

dans laquelle les n_γ seront pairs et pourront manquer, les n_α^0 et $\overline{n}_\beta^0$ seront impairs. Si ϱ des nombres n_α^0 et σ des nombres $\overline{n}_\beta^0$ sont égaux à 1 le faisceau peut être amené à ne renfermer que $n-\varrho$ variables x et $n-\sigma$

variables y; le nombre des éléments n_α^0 est égal à celui des éléments $\bar{n}_\beta^0$: leur valeur commune est

$$n - \tau = t,$$

τ désignant le *rang* du système des coefficients du faisceau.

Considérons inversement une décomposition de $2n$ en entiers impairs de même nombre n_α^0, $\bar{n}_\alpha^0$ et en entiers pairs n_γ satisfaisant à ces conditions. On lui fera correspondre un faisceau singulier en posant:

$$n_\sigma = 2e_\sigma, \quad n_i^0 = 2P_i + 1, \quad \bar{n}_k^0 = 2Q_k + 1;$$

ce faisceau sera la somme d'autant de groupements (K_y) qu'il y a de nombres P_i différents de zéro, de groupements (K_x) qu'il y a d'entiers Q_i différents de zéro et enfin de groupements (W) à diviseurs élémentaires

$$(a_\sigma \lambda_1 + b_\sigma \lambda_2)^{e_\sigma},$$

où a_σ, b_σ, g, h sont arbitraires sous la condition

$$g a_\sigma + h b_\sigma$$

soit différent de 0. Ajoutons en terminant que *les invariants de Kronecker* (c'est-à-dire les nombres n_i^0, $\bar{n}_k^0$) *et les invariants de Weierstrass* (c'est-à-dire les nombres e_σ et les quotients $\frac{b_\sigma}{a_\sigma}$) *du faisceau*

$$\lambda_1 \varphi + \lambda_2 \psi$$

*sont identiques à ceux des diverses parties du faisceau.**

18. Types de faisceaux singuliers. *Si un faisceau singulier de formes bilinéaires, à n variables x et n variables y, conduit à l'égalité

$$2n = \sum_{\alpha=1}^{\alpha=t} n_\alpha^0 + \sum_{\beta=1}^{\beta=t} \bar{n}_\beta^0 + \sum_{\gamma=1}^{\gamma=p} n_\gamma,$$

on dit qu'il possède la *caractéristique*

$$[\{n_1^0 n_2^0 \ldots n_t^0\}\{\bar{n}_1^0 \bar{n}_2^0 \ldots \bar{n}_t^0\}(n_1 \ldots) \ldots (n_\sigma \ldots) \ldots (\ldots n_p)]$$

où l'on a groupé sous la forme $(n_\sigma \ldots)$ les nombres pour lesquels les exposants $e_\sigma = \frac{n_\sigma}{2}$ correspondent à un même diviseur élémentaire irréductible.

Le nombre des caractéristiques distinctes est fini pour toute valeur de n. Il convient d'observer qu'en permutant les n_α^0 et les $\bar{n}_\alpha^0$ on n'a pas deux caractéristiques distinctes, pas plus qu'en permutant les éléments de même rang de deux groupes

$$(n_\sigma \ldots) \qquad (n_{\sigma'} \ldots)$$

qui en renferment le même nombre.

Le nombre des types de faisceaux singuliers à $2n$ variables qui peuvent (par suite de la présence de n_α^0, $\bar{n}_\alpha^0$ égaux à 1) être ramenés à dépendre de $2(n-i)$ variables est égal à celui des types *ordinaires et singuliers* à $2(n-1)$ variables.

Car, en supprimant les nombres n_1^0 et $\bar{n}_1^0$ qui sont égaux à 1, on obtient la caractéristique d'un faisceau à $2(n-1)$ variables (qui peut être ordinaire si tous les autres n_α^0, $\bar{n}_\alpha^0$ sont nuls), et réciproquement. Les formes réduites correspondantes à $2(n-1)$ variables sont d'ailleurs les mêmes que celles à $2n$ variables.

Il est facile de former *de proche en proche* les divers types de faisceaux singuliers pour $n = 1, 2, 3, \ldots$

Pour $n = 1$, l'équation

$$2 = n_1^0 + \cdots + \bar{n}_1^0 + \cdots + n_1 + \cdots$$

n'admet que la solution

$$n_1^0 = \bar{n}_1^0 = 1,$$

caractéristique $\{1, \bar{1}\}$, qui donne les formes à 2 variables identiquement nulles.

Pour $n = 2$, on peut prendre l'une des trois solutions

$$n_1^0 = 3, \qquad \bar{n}_1^0 = 1$$
$$n_1^0 = 1, \qquad \bar{n}_1^0 = 1, \qquad n_1 = 2$$
$$n_1^0 = n_2^0 = \bar{n}_1^0 = \bar{n}_2^0 = 1.$$

La première donne la forme normale qui correspond à

$$P_1 = 1 \qquad Q_1 = 0;$$

elle comprend deux variables x et une variable y et s'écrit

$$\lambda_1 x_1 y_0 + \lambda_2 x_0 y_0;$$

les deux autres

$$[\{1, \bar{1}\} 2] \quad \text{et} \quad \{11, \overline{11}\}$$

sont les formes normales de types [1] et $\{1, \bar{1}\}$ pour les faisceaux ordinaires à une variable x et une variable y.

Nous donnons ici le tableau des formes types pour $n = 1, 2, 3, 4$ en observant que les variables des groupes n_α^0 sont numérotées à la suite; celles des groupes $\bar{n}_\alpha^0$ sont numérotées de même mais surmontées d'un trait horizontal, enfin celles des groupes (W) correspondant aux nombres n_γ sont accentuées:

$n = 1$; $\quad \{1, \bar{1}\}: \lambda_1 \cdot 0 + \lambda_2 \cdot 0$

$n = 2$; $\quad \{3, \bar{1}\}: \lambda_1 x_1 y_0 + \lambda_2 x_0 y_0$

$[\{1, \bar{1}\} 2]$ et $\{11, \overline{11}\}$ correspondent aux types [1], $\{1, \bar{1}\}$ à 2 variables x, y.

$n=3;$ $\quad \{5, \bar{1}\}: \lambda_1(x_1y_1+x_2y_0)+\lambda_2(x_0y_1+x_1y_0)$

$$\{3, \bar{3}\}: \lambda_1(x_1y_0+\bar{x}_0\bar{y}_1)+\lambda_2(x_0y_0+\bar{x}_0\bar{y}_0)$$

$$[\{3, \bar{1}\}2]: \lambda_1(x_1y_0+a_1x'_0y'_0)+\lambda_2(x_0y_0+b_1x'_0y'_0)$$

Les formes normales pour les types

$\{31, \overline{11}\}$, $[\{1, \bar{1}\}22]$, $[\{1, \bar{1}\}(22)]$, $[\{1, \bar{1}\}4]$, $[\{11, \overline{11}\}2]$, $\{111, \overline{111}\}$ sont celles qui correspondent aux formes ordinaires ou singulières dépendant de 2 séries de 2 variables

$$\{3, \bar{1}\},\ [11],\ [(11)],\ [\{1, \bar{1}\}2],\ \{11, \overline{11}\}.$$

Le cas $n=4$ ne donnera *de même* comme formes types nouvelles que

$$\{7, \bar{1}\}: \lambda_1(x_1y_2+x_2y_1+x_3y_0)+\lambda_2(x_0y_2+x_1y_1+x_2y_0)$$

$$\{5, \bar{3}\}: \lambda_1(x_1y_1+x_2y_0+\bar{x}_0\bar{y}_1)+\lambda_2(x_1y_0+\bar{x}_0\bar{y}_0)$$

$$\{33, \overline{11}\}: \lambda_1(x_1y_0+x_3y_1)+\lambda_2(x_0y_0+x_2y_1)$$

$$[\{5, \bar{1}\}2]: \lambda_1(x_1y_1+x_2y_0+a_1x'_0y'_0)+\lambda_2(x_1y_0+b_1x'_0y'_0)$$

$$[\{3, \bar{3}\}2]: \lambda_1(x_1y_0+\bar{x}_0\bar{y}_1+a_1x'_0y'_0)+\lambda_2(x_0y_0+\bar{x}_0\bar{y}_0+b_1x'_0y'_0)$$

$$[\{3, \bar{1}\}22]: \lambda_1(x_1y_0+a_1x'_0y'_0+a_2x'_1y'_1)+\lambda_2(x_0y_0+b_1x'_0y'_0+b_2x'_1y'_1)$$

$[\{3, \bar{1}\}(22)]$: se déduit du précédent en faisant $a_1=a_2$, $b_1=b_2$.

$$[\{3, \bar{1}\}4]: \lambda_1(x_1y_0+a_1(x'_0y'_1+x'_1y'_0)-hx'_0y'_0)$$
$$+\lambda_2(x_0y_0+b_1(x'_0y'_1+x'_1y'_0)+gx'_0y'_0).$$

Les quinze autres types donnent les mêmes formes normales que les faisceaux ordinaires et singuliers à 6 variables x, y.*

Méthode de Darboux.

19. Décomposition en carrés. *G. Darboux*[30]) est parvenu aux résultats de *K. Weierstrass* et de *L. Kronecker* par une méthode qui lui est propre; elle repose sur l'étude de formes nouvelles (*adjointes de Darboux*) associées à une forme quadratique (ou bilinéaire). Il s'est borné à considérer les formes quadratiques; *L. Sauvage*[31]) a appliqué depuis cette méthode aux formes bilinéaires. Soit

$$f=\sum a_{ij}x_ix_j, \quad \text{où} \quad a_{ij}=a_{ji} \qquad (i, j=1, 2, \dots, n)$$

30) J. math. pures appl. (2) 19 (1874), p. 347. Il convient d'observer qu'à cette époque la théorie de *K. Weierstrass* n'était pas établie pour les formes quadratiques. On verra plus loin les difficultés correspondant à ce cas. Pour $n=3$ voir l'exposé simple de *H. Vogt* [Nouv. Ann. math. (3) 15 (1896), p. 441].

31) Ann. Éc. Norm. (3) 8 (1891), p. 255/340; cf. pour les faisceaux singuliers Ann. Éc. Norm. (3) 10 (1893), p. 9/42.

une forme quadratique à déterminant

$$\Delta=|a_{ik}|;$$

G. Darboux s'est proposé tout d'abord de donner pour f *une décomposition en carrés sous la forme la plus générale.*

Soit

$$\Phi_p=\left|\begin{array}{ccc|cccc} & & & X_1^1 & X_1^2 & \dots & X_1^p \\ & \Delta & & \vdots & \vdots & & \vdots \\ & & & X_n^1 & X_n^2 & \dots & X_n^p \\ \hline X_1^1 & \dots & X_n^1 & 0 & 0 & \dots & 0 \\ X_1^2 & \dots & X_n^2 & 0 & 0 & \dots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ X_1^p & \dots & X_n^p & 0 & 0 & \dots & 0 \end{array}\right|;$$

cette forme Φ_p contient p séries de variables

$$X_1^i,\ X_2^i,\ \dots,\ X_n^i \quad (i=1, 2, \dots, p);$$

elle est quadratique par rapport à chacune de ces séries et, si on la regarde comme dépendant des a_{ik}, elle est linéaire par rapport aux mineurs d'ordre p de Δ.

On a

$$\Phi_0=\Delta,$$

$$\Phi_1=-\sum\frac{\partial\Phi_0}{\partial a_{ij}}X_i^1X_j^1$$

(Φ_1 est donc, au signe près, l'*adjointe de Gauss* de f), et d'une manière générale

$$-\Phi_{p+1}=\sum\frac{\partial\Phi_p}{\partial a_{ij}}X_i^{p+1}X_j^{p+1}.$$

La suite s'arrête à

$$\Phi_n=(-1)^n\left|\begin{array}{ccc} X_1^1 & \dots & X_n^1 \\ \vdots & & \vdots \\ X_1^n & \dots & X_n^n \end{array}\right|^2.$$

Pour représenter les polaires des Φ_p, *G. Darboux* emploie la notation suivante:

$$\left\{\begin{matrix} X^1X^2\dots X^p \\ Y^1Y^2\dots Y^p \end{matrix}\right\}=\left|\begin{array}{ccc|ccc} & & & X_1^1 & \dots & X_1^p \\ & \Delta & & \vdots & & \vdots \\ & & & X_n^1 & \dots & X_n^p \\ \hline Y_1^1 & \dots & Y_n^1 & 0 & \dots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ Y_1^p & \dots & Y_n^p & 0 & \dots & 0 \end{array}\right|;$$

la forme Φ_p elle même s'écrira par suite

$$\begin{Bmatrix} X^1 X^2 \dots X^p \\ X^1 X^2 \dots X^p \end{Bmatrix}.$$

Une propriété connue des déterminants permet d'écrire

$$(\alpha)\qquad \begin{aligned} &\begin{Bmatrix} X^1 \dots X^{p-1} X^p \\ Y^1 \dots Y^{p-1} Y^p \end{Bmatrix} \cdot \begin{Bmatrix} X^1 \dots X^{p-1} X^{p+1} \\ Y^1 \dots Y^{p-1} Y^{p+1} \end{Bmatrix} \\ &- \begin{Bmatrix} X^1 \dots X^{p-1} X^{p+1} \\ Y^1 \dots Y^{p-1} Y^p \end{Bmatrix} \cdot \begin{Bmatrix} X_1 \dots X^{p-1} X^p \\ Y_1 \dots Y^{p-1} Y^{p+1} \end{Bmatrix} \\ &= \begin{Bmatrix} X^1 \dots X^{p-1} \\ Y^1 \dots Y^{p-1} \end{Bmatrix} \cdot \begin{Bmatrix} X^1 \dots X^p X^{p+1} \\ Y^1 \dots Y^p Y^{p+1} \end{Bmatrix}; \end{aligned}$$

cette relation sera essentielle dans la suite.

Si l'on suppose que, lorsque $x_1, x_2, \dots, x_n$ subissent une transformation linéaire quelconque, l'expression

$$X_1^i x_1 + X_2^i x_2 + \cdots + X_n^i x_n$$

demeure invariable (ce qui exige que $X_1^i, X_2^i, \dots, X_n^i$ subissent la transformation adjointe), chacune des formes Φ_p sera simplement multipliée par δ^2, δ désignant le déterminant de la transformation.

La forme Φ_p peut être regardée comme le déterminant (invariant) de la forme

$$f(x_1, \dots, x_n) + 2t_1(X_1^1 x_1 + \cdots + X_n^1 x_n) + \cdots + 2t_p(X_1^p x_1 + \cdots + X_n^p x_n),$$

où les t ne sont pas transformés.

En prenant pour $(p+1)^{\text{ième}}$ système

$$X_i = \frac{1}{2}\frac{\partial f}{\partial x_i},$$

ce qui donne

$$\Phi_0 f = -\begin{vmatrix} a_{11} \dots a_{1n} & X_1 \\ \vdots & \vdots \\ a_{n1} \dots a_{nn} & X_n \\ X_1 \dots X_n & 0 \end{vmatrix};$$

et partant de l'identité

$$\begin{Bmatrix} X^1 \dots X^n X \\ X^1 \dots X^n X \end{Bmatrix} = 0,$$

G. Darboux obtient, par application successive de la relation (α), en posant

$$R_p = \begin{Bmatrix} X^1 \dots X^{n-p} X \\ X^1 \dots X^{n-p} X \end{Bmatrix}, \qquad A_p = \begin{Bmatrix} X^1 \dots X^{n-p} X \\ X^1 \dots X^{n-p} X^{n-p+1} \end{Bmatrix},$$

l'expression générale

$$\frac{R_p}{\Phi_{n-p}} = \frac{A_1{}^2}{\Phi_n \Phi_{n-1}} + \frac{A_2{}^2}{\Phi_{n-1}\Phi_{n-2}} + \cdots + \frac{A_p^2}{\Phi_{n-p+1}\Phi_{n-p}}$$

qui donne

$$\frac{R_n}{\Phi_0} = -f = \frac{A_1{}^2}{\Phi_n \Phi_{n-1}} + \frac{A_2{}^2}{\Phi_{n-1}\Phi_{n-2}} + \cdots + \frac{A_n^2}{\Phi_1 \Phi_0},$$

c'est-à-dire, pour la forme quadratique f, une somme de carrés de formes linéaires indépendantes

$$A_1, A_2, \dots, A_n;$$

le nombre des carrés positifs est égal à celui des variations de signe de la suite

$$\Phi_0, \Phi_1, \dots, \Phi_n,$$

quelles que soient les valeurs des X_j^i.

La forme Φ_p ne change pas si l'on ajoute aux variable X_j^i d'une série une même combinaison linéaire des variables des autres séries; ce n'est donc pour aucune des séries X_j^i une forme *générale*: elle ne dépend que de $(n-p+1)$ formes linéaires de $X_1^p, X_2^p, \dots, X_n^p$. On le voit d'ailleurs par l'expression de R_p qui se déduit de Φ_p en remplaçant les variables de la dernière série par $X_1, X_2, \dots, X_n$.

Cette forme Φ_p ne peut être identiquement nulle que si tous les mineurs d'ordre p de Φ_0 sont nuls; alors

$$\Phi_{p-i} \equiv 0.$$

Si Φ_p est différent de zéro, on peut toujours disposer des X_j^{p+1} de façon que Φ_{p+1} soit aussi différent de zéro, et ainsi de suite.

Or *si tous les mineurs d'ordre* $(p-1)$ *de* Φ_0 *sont nuls et si un mineur d'ordre* p *est* différent de zéro, on aura

$$R_{n-p} = -\Phi_p f(x_1, \dots, x_n);$$

d'où l'on conclut *la décomposition en carrés indépendants:*

$$-f = \frac{A_1{}^2}{\Phi_n \Phi_{n-1}} + \cdots + \frac{A_{n-p}^2}{\Phi_{p+1}\Phi_p}.$$

G. Darboux montre aussi en particulier que l'expression précédente donne, pour une forme *générale*

$$f(x_1, x_2, \dots, x_n)$$

dont les variables sont liées par p relations

$$X_j^i x_1 + \cdots + X_n^i x_n = 0 \qquad (i = 1, 2, \dots, p),$$

une décomposition en $(n-p)$ carrés obtenue sans avoir éliminé les p variables dépendantes.*

20. Réduction d'un faisceau ordinaire. „Si l'on considère un faisceau de formes

$$F = f + \lambda\varphi,$$

où
$$f=\sum_{(i,k)} a_{ik}x_ix_k,\quad \varphi=\sum_{(i,k)} b_{ik}x_ix_k \qquad (i,k=1,2,\dots,n),$$
et si l'on pose
$$X_i=\frac{1}{2}\frac{\partial F}{\partial x_i},$$
on aura l'identité
$$F=f+\lambda\varphi=\frac{-1}{\Delta(\lambda)}\begin{vmatrix} a_{11}+\lambda b_{11} & \dots & a_{1n}+\lambda b_{1n} & X_1\\ \vdots & & \vdots & \vdots\\ a_{n1}+\lambda b_{n1} & \dots & a_{nn}+\lambda b_{nn} & X_n\\ X_1 & \dots & X_n & 0\end{vmatrix}$$
en désignant par $\Delta(\lambda)$ le déterminant de F.

Regardons un instant les X comme des arbitraires; on pourra décomposer F en fractions simples et, *si l'on suppose les racines de* $\Delta(\lambda)=0$ *distinctes*, on aura
$$f+\lambda\varphi=-\sum\frac{1}{(\lambda-\lambda_i)\Delta'(\lambda_i)}\begin{vmatrix} a_{11}+\lambda_i b_{11} & \dots & a_{1n}+\lambda_i b_{1n} & X_1\\ a_{21}+\lambda_i b_{21} & \dots & a_{2n}+\lambda_i b_{2n} & X_2\\ \cdot & \cdot & \cdot & \cdot\\ a_{n1}+\lambda_i b_{n1} & \dots & a_{nn}+\lambda_i b_{nn} & X_n\\ X_1 & \dots & X_n & 0\end{vmatrix}.$$

Tous les déterminants qui figurent au second membre sont des *carrés parfaits* (ce sont les formes adjointes des $f+\lambda_i\varphi$ dont le déterminant est nul); on a donc:
$$f+\lambda\varphi=\sum\frac{U_i^2}{(\lambda-\lambda_i)\Delta'(\lambda_i)}$$
avec
$$U_i=A_{i1}X_1+A_{i2}X_2+\dots+A_{in}X_n.$$

Sans changer ces déterminants on peut ajouter aux éléments de la dernière colonne (et de la dernière ligne) les expressions
$$-\left(\frac{\partial f}{\partial x_j}+\lambda_i\frac{\partial\varphi}{\partial x_j}\right),$$
c'est-à-dire remplacer X_j par
$$(\lambda-\lambda_i)\cdot\frac{1}{2}\frac{\partial\varphi}{\partial x_j};$$
on aura donc
$$U_i=\frac{\lambda-\lambda_i}{2}\sum_{(j)}A_{ij}\frac{\partial\varphi}{\partial x_j}=\frac{\lambda-\lambda_i}{2}V_i$$
où V_i est indépendant de λ. On trouve alors
$$f+\lambda\varphi=\sum_{i=1}^{i=n}\frac{\lambda_i V_i^2}{\Delta'(\lambda_i)}-\lambda\sum_{i=1}^{i=n}\frac{V_i^2}{\Delta'(\lambda_i)};$$
c'est *la réduction simultanée de f et de φ à une somme de carrés.*

La méthode est en défaut si le déterminant de φ est nul; le coefficient de λ^n dans $\Delta(\lambda)$ est nul, mais on peut alors, *si $\Delta(\lambda)$ n'est pas identiquement nul*, remplacer φ par une autre forme du faisceau.

Il reste donc deux cas à étudier, celui où $\Delta(\lambda)$ *a des racines multiples* et celui où $\Delta(\lambda)$ *est identiquement nul.*

Plaçons-nous d'abord dans le cas des *racines multiples de* $\Delta(\lambda)=0$. Soit toujours
$$F(X_1,\dots,X_n|\lambda)=f+\lambda\varphi$$
et $\lambda=\lambda_i$ une racine multiple de
$$\Delta(\lambda)=0.$$
L'ensemble des fractions simples correspondant à λ_i sera le coefficient de $\frac{1}{h}$ dans le développement de
$$\frac{F(X_1,\dots,X_n|\lambda_i+h)}{\lambda-\lambda_i-h}$$
et comme
$$-F(X_1,\dots,X_n|\lambda_i+h)=\frac{A_1^2}{\Phi_n\Phi_{n-1}}+\frac{A_2^2}{\Phi_{n-1}\Phi_{n-2}}+\dots+\frac{A_n^2}{\Phi_1\Phi_0},$$
où $A_1, A_2,\dots, A_n$ sont des fonctions linéaires de $X_1, X_2,\dots, X_n$, on est conduit à chercher le coefficient de $\frac{1}{h}$ dans le développement de
$$\frac{A_{n-p+1}^2}{\Phi_{p-1}\Phi_p}\cdot\frac{1}{\lambda-\lambda_i-h}.$$

Supposons que $\lambda-\lambda_i$ entre au degré α_0 dans Φ_0 (c'est-à-dire dans $\Delta(\lambda)$), au degré α_1 dans Φ_1 (quelles que soient les arbitraires de Φ_1), au degré α_2 dans Φ_2, etc. il est clair qu'on a:
$$\alpha_0>\alpha_1>\alpha_2>\cdots$$
car si $(\lambda-\lambda_i)^{\alpha_1}$ divise Φ_1, il annule α_1 fois tous les mineurs du premier ordre de Φ_0, *donc aussi la dérivée de Φ_0 par rapport à λ*; donc Φ_0 contiendra $(\lambda-\lambda_i)$ au moins au degré α_1+1, etc. Les diviseurs élémentaires sont les expressions $(\lambda-\lambda_i)^{\alpha_0-\alpha_1}$, $(\lambda-\lambda_i)^{\alpha_1-\alpha_2}$, ...

Si l'on pose $\lambda=\lambda_i+h$ dans Φ_p on aura
$$\Phi_p=h^{\alpha_p}\Delta_p,$$
Δ_p ne renfermant plus h en facteur; d'autre part
$$A_{n-p+1}=\begin{vmatrix} a_{11}+(\lambda_i+h)b_{11} & \dots & a_{1n}+(\lambda_i+h)b_{1n} & X_1^1 & \dots & X_1^p\\ \vdots & & \vdots & \vdots & & \vdots\\ a_{n1}+(\lambda_i+h)b_{n1} & \dots & a_{nn}+(\lambda_i+h)b_{nn} & X_n^1 & \dots & X_n^p\\ X_1^1 & \dots & X_n^1 & 0 & \dots & 0\\ \vdots & & \vdots & \vdots & & \vdots\\ X_1^{p-1} & \dots & X_n^{p-1} & 0 & \dots & 0\\ X_1 & \dots & X_n & 0 & \dots & 0\end{vmatrix}$$

donne, en transformant convenablement la dernière ligne,

$$A_{n-p+1} = B_{n-p+1}(\lambda - \lambda_i - h) + C_{n-p+1},$$

où l'on a

$$B_{n-p+1} = h^{\alpha_p} B_{n,p}, \qquad C_{n-p+1} = h^{\alpha_p - 1} C_{n,p},$$

$B_{n,p}$ désignant une combinaison linéaire de $\frac{\partial \varphi}{\partial x_1}, \frac{\partial \varphi}{\partial x_2}, \ldots, \frac{\partial \varphi}{\partial x_n}$ dont les coefficients dépendent de λ_i et de h.

Soit

$$\frac{B_{n,p}}{\sqrt{\Delta_p \Delta_{p-1}}} = \xi_1 + \xi_2 h + \xi_3 h^2 + \cdots;$$

les ξ_i seront des fonctions linéaires de $x_1, x_2, \ldots, x_n$; *G. Darboux* montre que le terme en $\frac{1}{h}$ dans

$$\frac{A_{n-p+1}}{\Phi_p \Phi_{p-1}}$$

provient uniquement du développement de

$$\frac{B_{n,p}^2}{\Delta_p \Delta_{p-1}} \frac{(\lambda - \lambda_i - h)}{h^{e_p}},$$

où l'on a posé avec *K. Weierstrass*

$$e_p = \alpha_{p-1} - \alpha_p.$$

On aura donc pour ce terme

$$(\lambda - \lambda_i)(\xi_1 \xi_{e_p} + \xi_2 \xi_{e_p - 1} + \cdots + \xi_{e_p} \xi_1) - (\xi_1 \xi_{e_p - 1} + \xi_2 \xi_{e_p - 2} + \cdots + \xi_{e_p - 1} \xi_1)$$

et l'on en conclut

$$f = \sum \{ \lambda_i [\xi_1 \xi_{e_p} + \xi_2 \xi_{e_p - 1} + \cdots + \xi_{e_p} \xi_1] + \xi_1 \xi_{e_p - 1} + \cdots + \xi_{e_p - 1} \xi_1 \},$$

$$\varphi = -\sum (\xi_1 \xi_{e_p} + \cdots + \xi_{e_p} \xi_1).$$

C'est la forme de Weierstrass. Le nombre des fonctions linéaires ξ est $\sum e_p = n$; comme en général $f + \lambda \varphi$ dépend de n variables, aucun des ξ n'est nul et les formes sont linéairement distinctes.

G. Darboux indique également comment l'existence de racines infinies pour $\Delta(\lambda) = 0$ modifie la forme réduite de φ.*

21. Réduction d'un faisceau singulier. *Plaçons-nous maintenant dans le cas où $\Delta(\lambda)$ *est identiquement nul.* Si

$$\Phi_0 = \Delta(\lambda) \equiv 0$$

le faisceau

$$f + \lambda \varphi$$

est *singulier*; nous supposons que $\Phi_1, \Phi_2, \ldots, \Phi_{p-1}$ sont aussi *nuls quelles que soient les arbitraires qui y figurent,* c'est-à-dire que tous les mineurs d'ordre $(p-1)$ de $\Delta(\lambda)$ sont nuls, et nous supposons de plus que Φ_p ne soit pas nul. Alors

$$F = f + \lambda \varphi$$

ne dépend que de $(n-p)$ fonctions linéaires des x; il existe p relations distinctes entre les dérivées.

Si l'on pose

$$u_i = \frac{\partial F}{\partial x_i} = \frac{\partial f}{\partial x_i} + \lambda \frac{\partial \varphi}{\partial x_i},$$

les relations linéaires entre les x_i (qui peuvent dépendre de λ) s'écriront, si on les ordonne par rapport à λ,

$$A_i = \lambda^{q_i} V_i^0 - \lambda^{q_i - 1} V_i^1 + \cdots \pm V_i^{q_i} = 0 \qquad (i = 1, 2, \ldots, p).$$

On peut admettre que les V_i^j, qui sont linéaires en $u_1, u_2, \ldots, u_n$, sont linéairement distincts, sans quoi on pourrait abaisser l'ordre des A_i par rapport à λ. Leur nombre est alors inférieur ou égal à n:

$$q_1 + 1 + \cdots + q_p + 1 \leqq n.$$

Une substitution linéaire exécutée sur les x permet de réduire chacune de ces fonctions V_i^j à un seul terme, par exemple V_1^0 à u_1, V_1^1 à u_2, etc.; les relations

$$A_i = 0$$

sont, après cette substitution, du type

$$\lambda^q \frac{\partial F}{\partial x_1} - \lambda^{q-1} \frac{\partial F}{\partial x_2} + \cdots \pm \frac{\partial F}{\partial x_{q+1}} = 0$$

qui exprime que F ne dépend des variables $x_1, x_2, \ldots, x_{q+1}$ que par les combinaisons

$$z_1 = x_1 + \lambda x_2, \quad z_2 = x_2 + \lambda x_3, \quad \ldots, \quad z_q = x_q + \lambda x_{q+1}.$$

Il existe donc $(p+1)$ groupes de variables, dont les p premiers sont:

$$z_1^i = x_1^i + \lambda x_2^i, \quad \ldots, \quad z_j^i = x_j^i + \lambda x_{j+1}^i, \quad \ldots, \quad z_{q_i}^i = x_{q_i}^i + \lambda x_{q_i+1}^i,$$

$$(i = 1, 2, \ldots, p)$$

et le dernier est formé de h variables $\xi_1, \xi_2, \ldots, \xi_h$, où

$$h + p + q_1 + \cdots + q_p = n,$$

groupes tels que F soit une fonction entière de λ et des variables

$$z_j^i (j = 1, 2, \ldots, q_i \mid i = 1, 2, \ldots, p), \quad \xi_1, \xi_2, \ldots, \xi_h$$

qui sont en nombre $(n-p)$.

Comme F ne contient λ qu'au premier degré, on a nécessairement

$$F = \sum_{i=1}^{i=p} (y_1^i z_1^i + y_2^i z_2^i + \cdots + y_{q_i}^i z_{q_i}^i) + \varpi(\xi_1, \ldots, \xi_h) + \lambda \varpi'(\xi_1, \ldots, \xi_h),$$

où les y sont des fonctions linéaires quelconques de $\xi_1, \xi_2, \ldots, \xi_h$.

Ces y sont linéairement distincts: une relation linéaire et homogène identique entre les y permettrait en effet de faire disparaître une variable z et la forme ne dépendrait plus de n variables.

Si l'on suppose une seule série de variables ($i = 1$), ce qui ne change rien au raisonnement, on aura

$$f = x_1 y_1 + x_2 y_2 + \cdots + x_k y_k + \varpi,$$
$$\varphi = x_2 y_1 + x_3 y_2 + \cdots + x_{k+1} y_k + \varpi',$$

où quelques-uns des ξ pourront s'exprimer peut-être avec les y. Des transformations simples des ξ et des x feront disparaître ces ξ qui dépendent des y et conduiront aux formes

$$f = x_1 y_1 + x_2 y_2 + \cdots + x_k y_k + \psi(\xi_1, \xi_2, \ldots, \xi_\alpha),$$
$$\varphi = x_2 y_1 + x_3 y_2 + \cdots + x_{k+1} y_k + \psi'(\xi_1, \xi_2, \ldots, \xi_\alpha),$$

où le faisceau

$$\psi + \lambda\psi'$$

est ordinaire. Dans le cas de plusieurs séries de variables z on a simplement plusieurs groupements analogues et *dans tous les cas*

$$f + \lambda\varphi$$

est la somme de groupements des trois types

$$y_1(x_1 + \lambda x_2) + y_2(x_2 + \lambda x_3) + \cdots + y_k(x_k + \lambda x_{k+1}),$$
$$(\lambda_i - \lambda)(x_1 x_n + x_2 x_{n-1} + \cdots + x_n x_1) + x_1 x_{n-1} + \cdots + x_{n-1} x_n$$

et

$$x_1 x_n + \cdots + x_n x_1 + \lambda(x_1 x_{n-1} + \cdots + x_{n-1} x_1).$$

Ce sont les résultats de *K. Weierstrass* et de *L. Kronecker*[32]) d'où l'on déduit les conditions nécessaires et suffisantes de l'équivalence de deux faisceaux singuliers.*

22. Formes bilinéaires. *La méthode de *G. Darboux* s'étend aisément aux formes bilinéaires. *L. Sauvage*[31]) qui a développé cette extension a également traité depuis le cas des faisceaux singuliers.

A une forme bilinéaire

$$F = \sum_{(\alpha, \beta)} a_{\alpha\beta} x_\alpha y_\beta \qquad (\alpha, \beta = 1, 2, \ldots, n)$$

on associe les *adjointes de Darboux* obtenues en *bordant* son déterminant de θ lignes et de θ colonnes formées de séries de n variables nouvelles. En mettant, par exemple, en évidence les variables et désignant par $u_1^{(i)}, u_2^{(i)}, \ldots, u_n^{(i)}$ la $(n+i)^{\text{ième}}$ ligne horizontale, par $v_1^{(i)}, v_2^{(i)}, \ldots, v_n^{(i)}$ la $(n+i)^{\text{ième}}$ colonne on peut représenter *l'adjointe* correspondante par l'une ou l'autre des notations

$$B(u^1, \ldots, u^\theta;\ v^1, \ldots, v^\theta),\ B(u^\theta, v^\theta),$$

32) *L. Kronecker,* Monatsb. Akad. Berlin 1868, p. 339/46; Werke 1, Leipzig 1895, p. 167/74; *L. Kronecker* [Sitzgsb. Akad. Berlin 1890, p. 1375; 1891, p. 9, 33] est revenu sur ce sujet.

suivant qu'on y considère toutes les lignes et colonnes ajoutées ou seulement les dernières. On a toujours l'identité

$$B(u^{\theta-1}, u^\theta;\ v^{\theta-1}, v^\theta) \cdot B(u^{\theta-1}, u^{\theta+1};\ v^{\theta-1}, v^{\theta+1})$$
$$- B(u^{\theta-1}, u^{\theta+1};\ v^{\theta-1}, v^\theta)\ B(u^{\theta-1}, u^\theta;\ v^{\theta-1}, v^{\theta+1})$$
$$= B(u^{\theta+1};\ v^{\theta+1})\ B(u^{\theta-1}, v^{\theta-1}).$$

L. Sauvage pose, avec *G. Darboux,*

$$R_\theta = B(u^{n-\theta}, X;\ v^{n-\theta}, Y) \qquad (R_0 = 0)$$

et ensuite

$$B(u^{n-\theta-1}, X;\ v^{n-\theta}) = U_{\theta+1},$$
$$B(u^{n-\theta};\ v^{n-\theta-1}, Y) = V_{\theta+1},$$

ce qui donne

$$R_{\theta+1} B_{n-\theta} - U_{\theta+1} V_{\theta+1} = B_{n-\theta-1} R_\theta,$$

et l'on déduit de cette identité, en faisant $\theta = 0, 1, 2, \ldots, n$, la *réduction la plus générale de la forme bilinéaire à sa forme canonique*:

$$F = -\frac{U_1 V_1}{B_n B_{n-1}} - \frac{U_2 V_2}{B_{n-1} B_{n-2}} \cdots - \frac{U_n V_n}{B_1 B_0}.$$

Si l'on choisit les arbitraires u, v de manière que, $B_0, B_1, \ldots, B_{\theta-1}$ *étant identiquement nuls,* B_θ ne s'annule pas (ce qui est toujours possible), $B_{\theta+1}, \ldots$ pourront être supposés différents de zéro. La forme F renfermera au moins 2θ variables U, V et sera réduite.

En posant

$$B_0(s) = |a_{ij} s + b_{ij}|,$$

un faisceau $F = fs + \varphi$ traité par la même méthode pourra s'écrire

$$F = fs + \varphi = -\frac{B_1(X, Y)}{B_0(s)} = F(X, Y, s);$$

il n'y aura plus qu'à décomposer en fractions simples la réduite

$$F = -\frac{U_1 V_1}{B_n B_{n-1}} - \frac{U_2 V_2}{B_{n-1} B_{n-2}} - \cdots - \frac{U_n V_n}{B_1 B_0}$$

et à suivre pas à pas la méthode de *K. Weierstrass.**

Formes bilinéaires symétriques ou alternées.

23. Équivalence des faisceaux symétriques. *Soit

$$A = \sum_{(i, k)} a_{ik} x_i x_k,$$

où

$$a_{ik} = a_{ki} \qquad (i, k = 1, 2, \ldots, n),$$

une *forme quadratique* à n variables; si $|a_{ik}|$ n'est pas nul, on la dira *ordinaire*; si $|a_{ik}|$ est nul, on la dira *singulière.*

Un faisceau

$$S = \lambda_1 A + \lambda_2 B$$

de formes quadratiques sera *ordinaire* si le déterminant $|\lambda_1 A + \lambda_2 B|$ est différent de zéro, *singulier* si ce déterminant est nul. Dans ce dernier cas les dérivées de S relatives à $x_1, x_2, \ldots, x_n$ sont liées par $n - r$ relations linéaires indépendantes, si r désigne le *rang* du déterminant $|S|$. Si l'on choisit parmi ces relations celle qui a le plus petit degré m_1 en $\frac{\lambda_1}{\lambda_2}$, puis celle qui a le plus petit degré m_2 supérieur à m_1, et ainsi de suite, les nombres $m_1, m_2, \ldots, m_{n-r}$ se conservent évidemment par une transformation linéaire quelconque des x.

Considérons à côté des formes quadratiques A et B les *polaires*

$$P_a = \frac{1}{2}\left(\frac{\partial A}{\partial x_1} y_1 + \frac{\partial A}{\partial x_2} y_2 + \cdots + \frac{\partial A}{\partial x_n} y_n\right),$$

$$P_b = \frac{1}{2}\left(\frac{\partial B}{\partial x_1} y_1 + \frac{\partial B}{\partial x_2} y_2 + \cdots + \frac{\partial B}{\partial x_n} y_n\right);$$

ce sont des formes bilinéaires *symétriques*. Il est clair que l'on a

$$|\lambda_1 A + \lambda_2 B| = |\lambda_1 P_a + \lambda_2 P_b|.$$

D'autre part, si la substitution (T)

$$x_i = \sum_{k=1}^{k=n} t_{ik} x_k'$$

donne lieu à l'identité

$$\lambda_1 A + \lambda_2 B = \lambda_1 A' + \lambda_2 B',$$

les substitutions cogrédientes

$$x_i = \sum_{k=1}^{k=n} t_{ik} x_k', \qquad y_i = \sum_{k=1}^{k=n} t_{ik} y_k'$$

donnent lieu à l'identité analogue

$$\lambda_1 P_a + \lambda_2 P_b = \lambda_1 P'_{a'} + \lambda_2 P'_{b'},$$

et réciproquement.

L'équivalence des faisceaux

$$\lambda_1 A + \lambda_2 B \quad \text{et} \quad \lambda_1 A' + \lambda_2 B'$$

de formes quadratiques entraîne donc la *congruence* des faisceaux de formes bilinéaires symétriques

$$\lambda_1 P_a + \lambda_2 P_b \quad \text{et} \quad \lambda_1 P_{a'} + \lambda_2 P_{b'},$$

et réciproquement. Il suit de là qu'*une condition nécessaire de l'équivalence des faisceaux quadratiques est l'identité des diviseurs élémentaires de leurs déterminants*

$$|\lambda_1 A + \lambda_2 B| \qquad |\lambda_1 A' + \lambda_2 B'|$$

*et aussi des nombres $m_1, m_2, \ldots, m_{n-r}$ attachés à un faisceau singulier de rang r.**

24. Congruence des faisceaux symétriques. *C'est un fait digne de remarque que ces conditions nécessaires pour l'*équivalence* des faisceaux de formes bilinéaires symétriques soient suffisantes pour leur *congruence*.

Pour l'établir, il est nécessaire de compléter sur un point la théorie donnée par *K. Weierstrass* dans le cas des formes quelconques. Nous avons vu que dans ce dernier cas, de simples permutations des lignes et des colonnes entre elles [ou des permutations des x et des y entre eux] amènent tous les mineurs formés en supprimant les ϱ premières lignes et ϱ premières colonnes de $|S|$ à être *réguliers* pour un diviseur premier p donné. Le raisonnement ne peut plus s'appliquer ici puisque $|S|$ est symétrique et que cette symétrie ne se conserve pas par des permutations *indépendantes* faites sur les lignes et sur les colonnes.

Soit

$$a_{ik} = a_{ki} \qquad (i, k = 1, 2, \ldots, n)$$

un système symétrique; nous appellerons *mineur symétrique* du déterminant $|a_{ik}|$ un mineur dont la diagonale principale est formée d'éléments de la diagonale principale de $|a_{ik}|$. Un tel mineur est évidemment symétrique et réciproquement.

Soit a_{ik} un élément *régulier* par rapport au diviseur premier p, c'est-à-dire qui le renferme à la puissance l_1; le mineur symétrique du second degré

$$a_{ii} a_{kk} - (a_{ik})^2$$

contient exactement p à la puissance $2l_1$; s'il n'était pas régulier c'est que

$$l_2 < 2l_1,$$

mais on a toujours

$$l_2 \geqq 2l_1,$$

donc le mineur symétrique considéré est régulier et

$$l_2 = 2l_1.$$

Admettons que le mineur symétrique $A_{\varrho-1}$ de degré $(\varrho - 1)$, formé avec les $(\varrho - 1)$ premières colonnes, soit *régulier*

$$A_{\varrho-1} = \sum \pm a_{11} a_{22} \ldots a_{\varrho-1, \varrho-1},$$

et qu'*aucun mineur symétrique de degré ϱ contenant $A_{\varrho-1}$ ne soit régulier.*

Il existe toujours un mineur régulier de degré ϱ contenant $A_{\varrho-1}$, soit A_{ik} ce mineur

$$A_{ik} = \sum \pm a_{11} a_{22} \ldots a_{\varrho-1, \varrho-1} a_{ik};$$

supposons $\varrho + 1 \leqq r$, r désignant le *rang* de $|a_{ik}|$ et considérons le mineur symétrique de degré $(\varrho + 1)$

$$A_{\varrho+1} = \sum \pm a_{11} a_{22} \ldots a_{\varrho-1,\,\varrho-1} a_{ii} a_{kk};$$

on aura, en posant

$$A_{ii} = \sum \pm a_{11} a_{22} \ldots a_{\varrho-1,\,\varrho-1} a_{ii} \qquad (i = \varrho,\ \varrho + 1, \ldots),$$

l'identité

$$A_{\varrho-1} A_{\varrho+1} = A_{ii} A_{kk} - (A_{ik})^2$$

dans laquelle A_{ik} est divisible par p^{l_ϱ}, A_{ii}, A_{kk} par une puissance supérieure. L'exposant de p dans $A_{\varrho+1}$, qui est $l'_{\varrho+1}$, satisfait donc à l'égalité

$$l_{\varrho-1} + l'_{\varrho+1} = 2 l_\varrho;$$

or on a toujours

$$l_{\varrho+1} - 2 l_\varrho + l_{\varrho-1} \geqq 0,$$

d'où

$$l'_{\varrho+1} \leqq l_{\varrho+1},$$

et comme l'inégalité n'est pas possible, d'après la définition même de $l_{\varrho+1}$, on a

$$l'_{\varrho+1} = l_{\varrho+1}.$$

Le mineur symétrique $A_{\varrho+1}$ est donc régulier; de plus l'égalité:

$$l_{\varrho+1} - 2 l_\varrho + l_{\varrho-1} = 0$$

donne

$$e_{\varrho+1} = e_\varrho.$$

On peut donc transformer un système symétrique par une permutation convenable des lignes et *la même permutation des colonnes,* de façon que[33])

si le déterminant symétrique

$$A_\varrho = \sum \pm a_{11} a_{22} \ldots a_{\varrho\varrho}$$

n'est pas régulier pour le diviseur p, les mineurs symétriques

$$A_{\varrho-1} \quad \text{et} \quad A_{\varrho+1}$$

sont réguliers ainsi que les mineurs

$$B_\varrho = \sum \pm a_{11} \ldots a_{\varrho-1,\,\varrho-1} a_{\varrho,\,\varrho+1},$$
$$C_\varrho = \sum \pm a_{11} \ldots a_{\varrho-1,\,\varrho-1} a_{\varrho+1,\,\varrho+1}.$$

Si le déterminant A_{r-1} était régulier, on aurait dans l'identité

$$A_{r-1} A_{r+1} = A_{ii} A_{kk} - (A_{ik})^2$$

$A_{r+1} = 0$ et il serait impossible, si A_{ik} est régulier, que A_{ii} et A_{kk} qui comprennent A_{r-1} ne le fussent pas tous deux.

Nous avons donc établi que *s'il existe un mineur symétrique régulier*

33) *G. Frobenius,* Sitzgsb. Akad. Berlin 1894, p. 36.

de degré $(\varrho - 1)$ qui n'est contenu dans aucun mineur symétrique régulier de degré ϱ, on a pour $\varrho + 1 \leqq r$

$$e_{\varrho+1} = e_\varrho.$$

Admettons que la forme

$$A = \sum_{(i,\,k)} a_{ik} x_i y_k \qquad (i, k = 1, 2, \ldots, n)$$

ait été amenée par permutation convenable des x (et la même permutation des y) à satisfaire aux conditions précédentes.

Supposons que les mineurs symétriques $A_1, A_2, \ldots, A_{\varrho-1}$ soient réguliers, que A_ϱ ne le soit pas; nous avons démontré que $A_{\varrho+1}$ l'était et qu'en outre

$$e_{\varrho+1} = e_\varrho.$$

Remplaçons, dans la forme A, les variables $x_{\varrho+1}$, $y_{\varrho+1}$ par

$$x_{\varrho+1} - x_\varrho, \quad y_{\varrho+1} - y_\varrho$$

sans modifier les autres; nous obtiendrons par cette transformation unimodulaire une forme symétrique

$$A' = \sum a'_{ik} x_i y_k$$

dont le déterminant $|A'|$ se déduit de $|A|$ en remplaçant les éléments de la $\varrho^{\text{ième}}$ ligne par ces éléments diminués de ceux de la $(\varrho + 1)^{\text{ième}}$ et les éléments de la $\varrho^{\text{ième}}$ colonne par ces éléments diminués de ceux de la $(\varrho + 1)^{\text{ième}}$. En désignant par un accent les éléments de A' correspondant à ceux de A, on a

$$A_1' = A_1, \quad A_2' = A_2, \quad \ldots, \quad A'_{\varrho-1} = A_{\varrho-1}, \quad A'_{\varrho+1} = A_{\varrho+1}, \quad \ldots$$

et

$$A_\varrho' = A_\varrho - 2 B_\varrho + C_\varrho$$

car le terme diagonal, modifié dans A_ϱ, est

$$a_{\varrho\varrho} - a_{\varrho,\varrho+1} - a_{\varrho+1,\varrho} + a_{\varrho+1,\varrho+1}.$$

Comme B_ϱ est régulier et que, par hypothèse, A_ϱ et C_ϱ ne le sont pas, A_ϱ' *l'est certainement.*

L'application de cette méthode conduira donc à une forme A pour laquelle $A_1, A_2, \ldots, A_r$ seront réguliers pour le diviseur p.

Si l'on choisit comme point de départ le système des coefficients du faisceau symétrique

$$S_1 = \lambda A_1 - B_1$$

on voit qu'avec des permutations des x, les mêmes permutations des y et des transformations élémentaires, *indépendantes de λ,* unimodulaires et congruentes des x et des y, on transformera ce système en un système symétrique S_1', tel que *tous les mineurs symétriques du* *déterminant* $|S_1'|$ *formés avec les i premières lignes et les i premières colonnes* ($i = 1, 2, \ldots, r$) *soient réguliers pour le diviseur premier p.*

Il suffira de faire une dernière permutation des x (et la même permutation des y) qui échange la première ligne et la $n^{\text{ième}}$, la deuxième ligne et la $(n-1)^{\text{ième}}$, etc. (et les colonnes de même) pour obtenir *le déterminant symétrique* $|S|$ *qui correspond au faisceau symétrique*

$$S = \lambda A - B$$

satisfaisant cette fois aux conditions qui permettent l'application de la méthode de Weierstrass.

En se reportant à l'exposé de cette méthode on reconnaît immédiatement que dans la suite des calculs les x et les y jouent le même rôle et que les formules définitives qui déterminent les $X_{\sigma\mu}$ au moyen des x sont *identiques* à celles qui déterminent les $Y_{\sigma\mu}$ au moyen des y.

En d'autres termes *un faisceau symétrique ordinaire de formes bilinéaires*

$$S = \lambda A - B$$

peut être amené par des transformations congruentes des x et des y à la forme réduite de Weierstrass, où n'interviennent que les diviseurs élémentaires du déterminant $|\lambda A - B|$.

L'identité des diviseurs élémentaires, qui est une condition *nécessaire* d'*équivalence*, est donc aussi une condition *suffisante* de *congruence* pour un faisceau symétrique ordinaire.*

Calcul symbolique des formes bilinéaires d'après Frobenius.

25. Opérations symboliques. *L'idée d'étendre le calcul ordinaire des nombres à des tableaux carrés ou rectangulaires

$$|a_{ik}| \qquad (i = 1, 2, \ldots, m;\ k = 1, 2, \ldots, n),$$

en définissant pour ces tableaux une addition et une multiplication symboliques, paraît due à *A. Cayley*[34]).

A. Cayley et *J. J. Sylvester* l'ont développée à diverses occasions sous le nom de *théorie des matrices*.

E. N. Laguerre[35]) l'a reprise dans son „Calcul des systèmes linéaires" en indiquant, parmi les nombreuses applications qu'elle comporte, l'étude des formes quadratiques et bilinéaires, en particulier la recherche des transformations de ces formes en elles-mêmes. Sans avoir élucidé définitivement cette question, il est parvenu à des résultats intéressants qui gagneraient à être mis en lumière. Le „calcul des systèmes

34) Cambr. math. J. 4 (1843/5), p. 119; Papers 1, Cambridge 1889, p. 55.

35) J. Éc. polyt. (1) cah. 42 (1867), p. 215/64; Œuvres 1, Paris 1898, p. 221/67.

linéaires" de *E. N. Laguerre* semble d'ailleurs susceptible d'applications plus étendues que le symbolisme de *G. Frobenius.*

C'est à *G. Frobenius*[36]) qu'on doit le développement systématique de la théorie des formes bilinéaires basée sur un calcul symbolique du tableau des coefficients a_{ik}. Comme on parvient ainsi de façon simple à la plupart des propositions essentielles de cette théorie, il nous a paru nécessaire d'indiquer en quoi il consiste, d'autant plus qu'*une partie de ces résultats s'applique à des formes bilinéaires dont les coefficients sont plus généraux que ceux considérés par K. Weierstrass et L. Kronecker.*

a. *Multiplication symbolique.* Une forme bilinéaire

$$A = \sum_{(i,k)} a_{ik} x_i y_k \qquad (i, k = 1, 2, \ldots, n)$$

est regardée comme l'*image* du système d'éléments homologues a_{ik}.

Soit

$$B = \sum_{(i,k)} b_{ik} x_i y_k \qquad (i, k = 1, 2, \ldots, n)$$

une seconde forme *aux mêmes variables*; *G. Frobenius* déduit de ces deux formes[37])

$$P = \sum_{(i,k)} \frac{\partial A}{\partial y_i} \frac{\partial B}{\partial x_i} \qquad (i, k = 1, 2, \ldots, n)$$

qu'il appelle *produit de A par B* et représente par la notation

$$P = AB.$$

Cette *multiplication* des formes est *symbolique* alors que leur *addition* est réelle.

D'après la définition du produit AB

$$P = \sum_{(i,k)} a_{ik} x_i \frac{\partial B}{\partial x_k} = \sum_{(i,k)} b_{ik} \frac{\partial A}{\partial y_i} y_k = \sum_{(i,k,l)} a_{il} b_{lk} x_i y_k,$$

où $i, k, l = 1, 2, \ldots, n$; on obtient donc le produit AB en faisant dans A la transformation $\left(y_k \mid \frac{\partial B}{\partial x_k}\right)$ ou dans B la transformation $\left(x_i \mid \frac{\partial A}{\partial y_i}\right)$. Il résulte de là, ou de l'expression de P,

$$|AB| = |A| \cdot |B|.$$

Tout mineur de degré ϱ de $|AB|$ est donc combinaison linéaire des mineurs de degré ϱ de $|A|$ et $|B|$.

La multiplication symbolique des formes bilinéaires est

36) J. reine angew. Math. 84 (1878), p. 1.

37) Si les formes A et B ne dépendent pas des mêmes variables on les ramène au cas étudié en ajoutant des termes $x_i y_k$ à coefficients nuls.

1°) *associative*:

$$(AB)C = A(BC) = ABC = \sum_{(i,\,k)} b_{ik} \frac{\partial A}{\partial y_i} \frac{\partial C}{\partial x_k} \qquad (i, k = 1, 2, \ldots, n);$$

2°) *non commutative*:

$$AB = \sum a_{il} b_{lk} x_i y_k,$$

$$BA = \sum b_{il} a_{lk} x_i y_k.$$

Lorsque

$$AB = BA$$

on dit que A et B sont *permutables*. On a, dans le cas où B et C sont permutables avec A,

$$A(BC) = (AB)C = (BA)C = B(AC) = B(CA) = (BC)A$$

c'est-à-dire que le produit (BC) est permutable avec A.

3°) *distributive* par rapport à l'addition, à droite et à gauche:

Si

$$C = \sum_{(i,\,k)} C_{ik} x_i y_k \qquad (i, k = 1, 2, \ldots, n)$$

on a

$$A(B + C) = \sum_{i=1}^{i=n} \frac{\partial A}{\partial x_i} \cdot \frac{\partial (B + C)}{\partial x_i} = AB + AC,$$

$$(B + C)A = \sum_{i=1}^{i=n} \frac{\partial (B + C)}{\partial y_i} \cdot \frac{\partial A}{\partial x_i} = BA + CA.$$

Les rapports de la multiplication symbolique de *G. Frobenius* avec la théorie des substitutions linéaires sont immédiats.

Si

$$B = SAT$$

on obtient B en faisant dans A les deux substitutions

$$\left(x_i \mid \frac{\partial S}{\partial y_i}\right), \qquad \left(y_i \mid \frac{\partial T}{\partial x_i}\right),$$

c'est-à-dire *en remplaçant les x par les dérivées du facteur de gauche relatives aux y de même indice et les y par les dérivées du facteur de droite relatives aux x de même indice.*

Le produit UV de deux substitutions des x

$$\left(x_i \mid \frac{\partial V}{\partial y_i}\right), \qquad \left(x_i \mid \frac{\partial U}{\partial y_i}\right)$$

s'obtient en remplaçant dans $\frac{\partial V}{\partial y_i}$ les variables x_i par $\frac{\partial U}{\partial y_i}$ car on obtient $\frac{\partial (UV)}{\partial y_i}$ en formant d'abord UV, c'est-à-dire remplaçant dans V les

x_i par $\frac{\partial U}{\partial y_i}$, puis dérivant par rapport à y_i. En d'autres termes

$$(UV)A = U(VA)$$

définit l'effet de (UV) sur A.

Si l'on considère au contraire une substitution des y

$$T = UV$$

on l'exécutera dans A en formant

$$A(UV) = (AU)V.$$

Formes conjuguées. Deux formes A et A' sont conjuguées quand on passe de l'une à l'autre en permutant x_i et y_i:

$$A' = \sum_{(i,\,k)} a_{ik} y_i x_k \qquad (i, k = 1, 2, \ldots, n),$$

On a

$$(A')' = A$$

$$(A + B)' = A' + B', \quad (AB)' = \sum_{i=1}^{i=n} \frac{\partial A'}{\partial x_i} \cdot \frac{\partial B'}{\partial y_i} = B'A'$$

et par suite aussi

$$(ABC)' = C'B'A', \text{ etc.}$$

Si A et B sont permutables on a

$$A'B' = B'A'.$$

Une forme identique à sa conjuguée est *symétrique*; elle est *alternée* si elle est opposée à sa conjuguée:

AA' est symétrique, $A - A'$ est alternée.

b. *Division symbolique.* Soit

$$X = \sum_{(i,\,k)} x_{ik} x_i y_k, \qquad (i, k = 1, 2, \ldots, n);$$

l'identité

$$AX \equiv 0$$

exige les n^2 équations

$$\sum_{j=1}^{j=n} a_{ij} x_{jk} = 0 \qquad (i, k = 1, 2, \ldots, n);$$

pour qu'elles aient d'autres solutions que $x_{jk} = 0$ il faut donc que l'on ait

$$|A| = 0.$$

Soit α_{ik} le coefficient de a_{ik} dans $|A|$, c'est-à-dire l'*adjoint* de a_{ik}; la forme

$$\text{adj.}\, A = \sum_{(i,\,k)} \alpha_{ik} x_k y_i \qquad (i, k = 1, 2, \ldots, n)$$

est l'*adjointe* de A.

Posons
$$x_1 y_1 + x_2 y_2 + \cdots + x_n y_n = E;$$
on aura
$$A \text{ adj.} A = \text{adj.} A \cdot A = E \cdot |A|.$$

Si le déterminant $|A|$ est nul, il n'existe aucune forme X satisfaisant à
$$AX = E \quad \text{ou à} \quad XA = E;$$
si le déterminant $|A|$ est différent de zéro, on peut prendre
$$X = \frac{\text{adj} A}{|A|}$$
et il n'y a pas d'autre solution. Elle satisfait aux deux équations.

La forme
$$\frac{\text{adj} A}{|A|},$$
quotient de l'adjointe par le déterminant $|A|$, est appelée *réciproque* de A. On la représente par A^{-1}; donc
$$AA^{-1} = A^{-1}A = E,$$
et la réciproque de A^{-1} est A.

Comme d'autre part, si $|A| \cdot |B|$ est différent de zéro,
$$(AB)(B^{-1}A^{-1}) = A(BB^{-1})A^{-1} = AEA^{-1} = AA^{-1} = E,$$
la réciproque du produit AB est $B^{-1}A^{-1}$.

On a aussi
$$(A')^{-1} = (A^{-1})'.$$

Enfin de l'équation symbolique
$$B = SAT,$$
où $|S| \cdot |T|$ est différent de zéro, on déduit
$$A = S^{-1}BT^{-1};$$
les formes S^{-1}, T^{-1} sont donc les images des substitutions *inverses* de S et T.

Dans l'hypothèse
$$S = T',$$
c'est-à-dire
$$B = T'AT,$$
on aura
$$A = (T')^{-1}BT^{-1} = (T^{-1})'BT^{-1};$$
on dit que les formes A et B sont *congruentes*; comme *on passe de A à B par la même substitution T exécutée à la fois sur les x et sur les y* ces deux séries de variables sont *cogrédientes.*

Si l'on suppose
$$S = T^{-1},$$
c'est-à-dire
$$B = T^{-1}AT$$
ce qui donne
$$A = TBT^{-1},$$
les formes A et B sont dites *semblables*, les variables x, y sont *contragrédientes.*

Les dénominations „cogrédientes", „contragrédientes" sont transportées des variables aux substitutions qu'elles subissent.

On a évidemment
$$T^{-1}ET = T^{-1}T = E;$$
inversement l'équation
$$SET = E$$
donne
$$S = T^{-1},$$
c'est-à-dire que *des substitutions semblables sont caractérisées par ce fait qu'elles transforment E en elle-même.*

Admettons enfin
$$T' = T^{-1},$$
T est dite *forme orthogonale*: on a, en posant
$$T = \sum t_{ik} x_i y_k,$$
$$t_{ik} = \frac{\tau_{ik}}{|T|}$$
et par suite
$$\sum (t_{ik})^2 = 1, \quad \sum t_{ik} t_{il} = 0.$$

Si T est orthogonale, il en est de même de T^{-1}; si T et U sont orthogonales, il en est de même de TU.*

26. Équation caractéristique. *La forme AA se représente naturellement par A^2; on définit de même
$$A^n = A^{n-1}A = AA^{n-1}$$
et les lois ordinaires du calcul des exposants sont valables à condition de poser
$$A^0 = E.$$

Si $|A|$ est différent de zéro, comme $AA^{-1} = E$, on peut aussi définir
$$A^{-n} = (A^{-1})^n$$
et le calcul des exposants négatifs s'applique.

Soit
$$g(\lambda) = a_0 + a_1\lambda + \cdots + a_n\lambda^n$$

une fonction entière de λ; la forme

$$a_0 A^0 + a_1 A + a_2 A^2 + \cdots + a_n A^n$$

est dite fonction entière de degré n de A et se représente par $g(A)$.

Comme

$$(A^\alpha)' = (A')^\alpha,$$

la conjuguée de $g(A)$ est $g(A')$.

Deux fonctions entières $g(A)$, $h(A)$ sont toujours permutables (cela légitime la notation précédente).

Si $|h(A)|$ est différent de zéro, le quotient $\frac{g(A)}{h(A)}$ est une fonction rationnelle de A; si $f(\lambda) = \frac{g(\lambda)}{h(\lambda)}$, nous poserons

$$f(A) = \frac{g(A)}{h(A)}.$$

Le déterminant $|\lambda E - A|$ est, d'après *A. L. Cauchy*[38]), le *déterminant ou la fonction caractéristique* de la forme A:

$$|\lambda E - A| = \varphi(\lambda) = c\,(\lambda - \lambda_1)(\lambda - \lambda_2) \cdots (\lambda - \lambda_n),$$

où c désigne une constante.

Soit $g(\lambda)$ une fonction quelconque de degré m en λ

$$g(\lambda) = a_0 \lambda^m + a_1 \lambda^{m-1} + \cdots + a_m = a_\mu(\mu_1 - \lambda)(\mu_2 - \lambda) \cdots (\mu_m - \lambda);$$

on aura

$$g(A) = a_0 A^m + a_1 A^{m-1} + \cdots + a_m = a(\mu_1 E - A)(\mu_2 E - A) \cdots (\mu_m E - A)$$

et par suite

$$|g(A)| = a^n \varphi(\mu_1)\varphi(\mu_2) \cdots \varphi(\mu_m) = g(\lambda_1) g(\lambda_2) \cdots g(\lambda_n).$$

Si $|h(A)|$ est différent de zéro, avec

$$f(\lambda) = \frac{g(\lambda)}{h(\lambda)},$$

on aura donc

$$|f(A)| = \frac{g(\lambda_1) g(\lambda_2) \ldots g(\lambda_n)}{h(\lambda_1) h(\lambda_2) \ldots h(\lambda_n)} = f(\lambda_1) f(\lambda_2) \cdots f(\lambda_n).$$

En considérant la fonction rationnelle

$$\frac{\lambda h(A) - g(A)}{h(A)} = \lambda E - f(A)$$

on aura donc aussi

$$|\lambda E - f(A)| = (\lambda - f(\lambda_1))(\lambda - f(\lambda_2)) \cdots (\lambda - f(\lambda_n)).$$

38) Exercices d'Analyse et de phys. math. 1, Paris 1840, p. 53.

Les racines de l'équation caractéristique de $f(A)$ sont donc

$$f(\lambda_1),\ f(\lambda_2),\ \ldots,\ f(\lambda_n),$$

si $\lambda_1, \lambda_2, \ldots, \lambda_n$ sont les racines de l'équation caractéristique de A[39]).

Comme il n'y a que n^2 formes bilinéaires *indépendantes* (linéairement distinctes) de $2n$ variables, la suite des puissances $A^0, A, A^2, \ldots$ conduit à une forme qui est combinaison linéaire (à coefficients constants) des précédentes; soit A^p la première qui possède cette propriété:

$$\psi(A) = a_0 A^0 + a_1 A + \cdots + a_p A^p = 0,$$

où a_p est différent de zéro, *est l'équation de moindre degré vérifiée par A*; on a évidemment aussi

$$a_0 A^\varrho + a_1 A^{\varrho+1} + \cdots + a_p A^{\varrho+p} = 0.$$

Si l'on considère la série

$$S = \frac{A^0}{\lambda} + \frac{A}{\lambda^2} + \frac{A^2}{\lambda^3} + \cdots,$$

convergente pour chaque système de valeurs des a_{ik}, x_i, y_k pour $|\lambda|$ assez grand, le produit $S\psi(\lambda)$ ne renferme pas de puissances négatives de λ; c'est donc une forme dont les coefficients sont de degré $(p-1)$ en λ. Posons

$$S\psi(\lambda) = G(\lambda);$$

la fraction $\frac{G(\lambda)}{\psi(\lambda)}$ est *irréductible*, car d'une relation $S\psi_1(\lambda) = G_1(\lambda)$ où $\psi_1(\lambda)$ serait de degré $p_1 < p$, on conclurait l'existence de l'équation $\psi_1(A) = 0$. On a d'ailleurs

$$S(\lambda E - A) = A^0 = E,$$

c'est-à-dire que *S est la réciproque de $(\lambda E - A)$*.

Nous avons donc établi les égalités

$$S = \frac{G(\lambda)}{\psi(\lambda)} = \frac{F(\lambda)}{\varphi(\lambda)},$$

où

$$(-1)^n F(\lambda) = \begin{vmatrix} a_{11} - \lambda & a_{12} & \ldots & a_{1n} & y_1 \\ a_{21} & a_{22} - \lambda & \ldots & a_{2n} & y_2 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ a_{n1} & a_{n2} & \ldots & a_{nn} - \lambda & y_n \\ x_1 & x_2 & \ldots & x_n & 0 \end{vmatrix}$$

et

$$(-1)^n \varphi(\lambda) = |A - \lambda E|$$

39) *C. W. Borchardt,* J. reine angew. Math. 30 (1846), p. 41; Werke, Berlin 1888, p. 8.

Comme $\frac{G}{\psi}$ est irréductible, si $\theta(\lambda)$ désigne le plus grand commun diviseur de F et de φ, on a

$$\varphi(\lambda) = \theta(\lambda)\psi(\lambda).$$

Donc $\psi(\lambda) = \frac{\varphi(\lambda)}{\theta(\lambda)}$ est le quotient du déterminant $|A - \lambda E|$ par le plus grand commun diviseur *de tous les mineurs du premier ordre de* $\varphi(\lambda)$ (de degré $(n-1)$), c'est-à-dire le $n^{\text{ième}}$ *produit élémentaire du déterminant* $|A - \lambda E|$.

Ainsi *l'équation de moindre degré vérifiée par la forme* A,

$$\psi(A) = 0$$

s'obtient en égalant à zéro le $n^{\text{ième}}$ *produit élémentaire* (n^{ter} Elementar Theiler) *du déterminant* $|A - \lambda E|$[40]).

Toute racine de l'équation $\psi(\lambda) = 0$ annule $\varphi(\lambda)$ et comme $\psi(\lambda)$ est le $n^{\text{ième}}$ produit élémentaire de $|A - \lambda E|$ la réciproque est vraie.

Comme d'autre part $\varphi(\lambda) = \psi(\lambda)\theta(\lambda)$, on a aussi

$$\varphi(A) = \psi(A)\theta(A) = 0$$

c'est-à-dire qu'*on a toujours* $\varphi(A) = 0$[41]).

Si l'on a $f(A) = 0$ et si $h(\lambda)$ désigne le plus grand commun diviseur de $f(\lambda)$ et de $\psi(\lambda)$, on aura

$$f(\lambda)G(\lambda) - \psi(\lambda)F(\lambda) = h(\lambda);$$

d'où l'on conclut $h(A) = 0$ et, comme $h(A)$ ne peut être de degré supérieur à $\psi(A)$, il faut nécessairement que

$$h(\lambda) = c\psi(\lambda),$$

où c est une constante.

Ainsi $f(\lambda)$ *est divisible par* $\psi(\lambda)$ *lorsque* $f(A) = 0$.

En particulier si l'on suppose $f(A) = 0$ et $f(\lambda)$ *sans facteurs multiples* il ne pourra y en avoir dans $\psi(\lambda)$; par suite *tous les diviseurs élémentaires de* $|A - \lambda E|$ *sont simples.**

27. Racine carrée d'une forme. *Soient

$$\psi(\lambda) = (\lambda - a)^\alpha(\lambda - b)^\beta(\lambda - c)^\gamma \dots$$

une fonction rationnelle entière de degré p, $F(\lambda)$, $G(\lambda)$, ... des fonctions rationnelles entières quelconques.

On a, en décomposant en fractions simples,

$$\frac{F(\lambda)}{\psi(\lambda)} = \frac{A_0}{(\lambda - a)^\alpha} + \dots + \frac{A_{\alpha-1}}{\lambda - a} + R(\lambda),$$

40) *G. Frobenius*, J. reine angew. Math. 84 (1878), p. 12; Sitzgsb. Akad. Berlin 1896, p. 601; *Edouard Weyr*, Monatsh. Math. Phys. 1 (1890), p. 187.

41) *A. Cayley*, Philos. Trans. London 148 (1858), p. 415/55; Papers 2, Cambridge 1889, p. 513/57.

où $R(\lambda)$ demeure fini pour $\lambda = a$, ce que nous écrirons plus simplement

$$\frac{F(\lambda)}{\psi(\lambda)} = \frac{A(\lambda)}{(\lambda - a)^\alpha} + R(\lambda).$$

Soient de même $\frac{B(\lambda)}{(\lambda - b)^\beta}$ la partie du développement en fractions simples de $\frac{G(\lambda)}{\psi(\lambda)}$ qui devient infinie pour $\lambda = b$, et ainsi de suite.

La fonction

$$\chi(\lambda) = A(\lambda)\frac{\psi(\lambda)}{(\lambda - a)^\alpha} + B(\lambda)\frac{\psi(\lambda)}{(\lambda - b)^\beta} + \cdots$$

est un polynome de degré $(p-1)$ en λ, dont le développement: 1°) suivant les puissances croissantes de $\lambda - a$ coïncide avec celui de $F(\lambda)$ jusqu'au terme $(\lambda - a)^{\alpha-1}$; 2°) suivant les puissances croissantes de $(\lambda - b)$ coïncide avec celui de $G(\lambda)$ jusqu'au terme $(\lambda - b)^{b-1}$; etc.

On a, en d'autres termes,

$$\chi(a) = F(a),\ \chi'(a) = F'(a),\ \dots,\ \chi^{(\alpha-1)}(a) = F^{(\alpha-1)}(a)$$
$$\chi(b) = G(b)),\ \chi'(b) = G'(b),\ \dots,\ \chi^{(\beta-1)}(b) = G^{(\beta-1)}(b)$$

. . . .

Ces conditions caractérisent $\chi(\lambda)$: car si $\chi_1(\lambda)$ y satisfaisait, la différence

$$\chi(\lambda) - \chi_1(\lambda)$$

qui est de degré $(p-1)$ s'annulerait à l'ordre α pour $\lambda = a$, à l'ordre β pour $\lambda = b$, etc., c'est-à-dire aurait p racines.

Supposons $abc\dots$ différent de zéro; formons le développement de $\sqrt{\lambda}$ suivant les puissances croissantes de $(\lambda - a)$:

$$\sqrt{\lambda} = \sqrt{a}\sqrt{1 + \frac{\lambda - a}{a}} = \sqrt{a}\left(1 + \frac{1}{2}\frac{\lambda - a}{a} - \frac{1}{2 \cdot 4}\frac{(\lambda - a)^2}{a^2} + \cdots\right)$$

et soit $F(\lambda)$ l'ensemble des α premiers termes; soit de même $G(\lambda)$ l'ensemble des β premiers termes du développement de $\sqrt{\lambda}$ suivant les puissances de $\lambda - b$, etc.

Formons d'autre part le polynome $\chi(\lambda)$ de degré $(p-1)$

$$p = \alpha + \beta + \cdots$$

qui satisfait aux conditions indiquées plus haut avec ces fonctions particulières $F(\lambda)$, $G(\lambda)$, ..., il est clair que la différence

$$\chi(\lambda) - \sqrt{\lambda}$$

développée suivant les puissances croissantes de $(\lambda - a)$ commence à la puissance α, etc.

On en conclut que

$$\chi(\lambda)^2 - \lambda \text{ est divisible par } (\lambda - a)^\alpha(\lambda - b)^\beta \dots,$$

c'est-à-dire que

$$\chi(\lambda)^2 - \lambda = \psi(\lambda) \cdot \varpi(\lambda).$$

Supposons maintenant que A soit une forme bilinéaire pour laquelle le déterminant $|A|$ ne soit pas nul; alors, l'équation

$$|\lambda E - A| = 0$$

n'admet pas la racine $\lambda = 0$; il en est de même de l'équation

$$\psi(\lambda) = 0,$$

si $\psi(A) = 0$ désigne l'équation de plus petit degré vérifiée par A.

On aura donc, dans l'hypothèse

$$\psi(\lambda) = (\lambda - a)^\alpha (\lambda - b)^\beta \dots,$$

la relation

$$\chi^2(A) - A = 0.$$

Les formes $\chi(A)$ et $-\chi(A)$ sont dites *racines carrees* de A et l'on écrit symboliquement

$$\chi(A) = A^{\frac{1}{2}} = \sqrt{A}.$$

On a d'ailleurs

$$|\chi(A)| = \sqrt{|A|}.*$$

28. Formes décomposables. *Une forme

$$A = \sum_{(i,k)} a_{ik} x_i y_k$$

est *décomposable* si elle est somme de formes $A_1, A_2, \dots$ dont deux quelconques n'ont aucune variable commune. On ajoutera toujours si c'est nécessaire à chacune des *parties* $A_1, A_2, \dots$ des termes à coefficients nuls de façon que le nombre des variables x qui y figurent soit égal à celui des variables y.

Exemple:

$$x_1 y_1 + x_2 y_1 + x_3 y_2 + x_3 y_3$$

est décomposable en deux parties

$$A_1 = x_1 y_1 + x_2 y_1 + 0 \cdot x_1 y'_2 + 0 \cdot x_2 y'_2,$$
$$A_2 = 0 \cdot x'_2 y_2 + 0 \cdot x'_2 y_3 + x_3 y_2 + x_3 y_3.$$

Si l'on a deux décompositions

$$A = A_1 + A_2 + \cdots$$
$$B = B_1 + B_2 + \cdots$$

de telle sorte que B_i renferme les mêmes variables que A_i, on dit que A et B sont *décomposables de même.*

Supposons

$$A = A_1 + A_2,$$

A dépendant de $2n$, A_1 de $2m_1$ et A_2 de $2m_2$ variables

$$(2n = 2m_1 + 2m_2);$$

on a évidemment

$$|A| = |A_1| \cdot |A_2|,$$

les déterminants du second membre étant relatifs aux $2m_1$ ou $2m_2$ variables qui figurent dans A_1 et A_2.

Tout mineur ϱ de $|A|$ qui n'appartient ni à $|A_1|$ ni à $|A_2|$ est le produit d'un mineur de degré $(\varrho - \sigma)$ de $|A_1|$ par un mineur de degré σ de $|A_2|$: *le rang r de $|A|$ est donc la somme des rangs r_1 et r_2 de $|A_1|$* et *$|A_2|$*.

Si A est décomposable, $\lambda E - A$ est *décomposable de même*; la fonction caractéristique de A est donc le produit des fonctions caractéristiques de ses parties.

Soient A une forme, dont les coefficients sont des fonctions rationnelles entières de un ou plusieurs paramètres $\lambda, \mu, \dots$, décomposable en deux parties A_1 et A_2; ϱ un entier au plus égal au rang r de $|A|$; D_ϱ, D'_ϱ, D''_ϱ les plus grands diviseurs communs à tous les mineurs de degré r de $|A|, |A_1|, |A_2|$. Dans le cas où ϱ dépasse le rang (r_1 ou r_2) de l'une des parties ($|A_1|$ ou $|A_2|$), on fera D'_ϱ ou D''_ϱ égal à zéro.

Cela posé, on démontre que D_ϱ *est le plus grand commun diviseur des* $(\varrho + 1)$ *fonctions*

$$D'_\varrho,\ D'_{\varrho-1} D''_1,\ D'_{\varrho-2} D''_2,\ \dots,\ D'_1 D''_{\varrho-1},\ D''_1.$$

Car tout mineur de degré ϱ de $|A|$, non compris dans $|A_1|$ ou $|A_2|$, est le produit d'un mineur de degré $(\varrho - \sigma)$ de $|A_1|$ par un mineur de degré σ de $|A_2|$ et tout produit de cette espèce est un mineur de degré ϱ de $|A|$.

Si $\varrho = r$, on a plus simplement

$$D_r = D'_{r_1} \cdot D''_{r_2},$$

puisque ϱ est supérieur à r_1 et r_2.*

29. Équivalence des systèmes. *Supposons que les éléments du système a_{ik} soient des fonctions rationnelles entières de paramètres $\lambda, \mu, \dots$[42]); toute forme

$$B = \sum_{(i,k)} b_{ik} x'_i y'_k \qquad (i, k = 1, 2, \dots, n)$$

---

42) *Les coefficients de ces polynomes en $\lambda, \mu, \dots$ peuvent être assujettis à diverses conditions: on peut les regarder comme des constantes arbitraires, comme des nombres algébriques quelconques, comme des nombres algébriques d'un domaine de rationalité fixé $[R]$ ou comme des *entiers algébriques* d'un tel domaine. Les coefficients des polynomes en $\lambda, \mu, \dots$ qui interviennent dans les

déduite de

$$A = \sum_{(i,k)} a_{ik} x_i' y_k' \qquad (i, k = 1, 2, \ldots, n)$$

par des substitutions

$$(S)\ x_i = \sum_{k=1}^{k=n} s_{ik} x_k', \qquad (T)\ y_i = \sum_{k=1}^{k=n} t_{ki} y_k',$$

où les s_{ik}, t_{ik} sont des fonctions entières de $\lambda, \mu, \ldots$, c'est-à-dire *toute forme B qui donne lieu à l'identité symbolique*

$$B = SAT,$$

est dite contenue dans A. Le système des coefficients b_{ik} est dit *multiple* du système a_{ik}.

Cette dernière définition s'étend aux systèmes b_{ik} qu'on obtient par *composition* de plusieurs autres, a_{ik} étant l'un de ceux-là. Dans tous les cas on peut toujours trouver S et T de telle sorte que

$$B = SAT.$$

Tout déterminant de degré ϱ formé avec les b_{ik} est une combinaison linéaire et homogène des déterminants de degré ϱ du système a_{ik}. Donc si D_ϱ' est le plus grand commun diviseur des premiers et D_ϱ le plus grand commun diviseur des derniers, *D_ϱ' est multiple de D_ϱ*.

Le rang r' du système b_{ik} est au plus égal au rang r du système a_{ik}.

Si un système c_{ik} est multiple d'un système b_{ik}, le $\varrho^{\text{ième}}$ produit élémentaire du premier système est multiple du $\varrho^{\text{ième}}$ produit élémentaire du second système.

Supposons, par exemple

$$c_{ik} = a_{i1} b_{1k} + a_{i2} b_{2k} + \cdots + a_{in} b_{nk} \qquad (i, k = 1, \ldots, n)$$

et désignons respectivement par $\beta_\varrho, \gamma_\varrho$ les puissances auxquelles figure un *diviseur irréductible p* dans les plus grands communs diviseurs des mineurs de $|b_{ik}|$ et de $|c_{ik}|$, qui sont de degré ϱ. Nous allons montrer qu'on a toujours

$$\beta_\varrho - \beta_{\varrho-1} \leqq \gamma_\varrho - \gamma_{\varrho-1}.$$

Il résulte de la formation des c_{ik} que le rang du système composé, r_c, est au plus égal au plus petit des rangs r_a, r_b des composants: on devra donc supposer ϱ inférieur ou égal au plus petit de ces nombres.

Soient

$$L = |b_{\varkappa\lambda}| \qquad \begin{pmatrix} \varkappa = \varkappa_1, \ldots, \varkappa_{\varrho-1} \\ \lambda = \lambda_1, \ldots, \lambda_{\varrho-1} \end{pmatrix}$$

substitutions (ou transformations) que subissent les formes considérées doivent naturellement satisfaire aux mêmes conditions.*

un mineur régulier, de degré $(\varrho - 1)$, du système b_{ik} et

$$M = |c_{\mu\nu}| \qquad \begin{pmatrix} \mu = \mu_1, \ldots, \mu_\varrho \\ \nu = \nu_1, \ldots, \nu_\varrho \end{pmatrix}$$

un mineur *régulier* de degré ϱ du système c_{ik}; considérons le système à $(2\varrho - 1)$ lignes et colonnes obtenu en complétant le tableau carré

$$\left|\frac{L}{\quad}\right|\frac{\quad}{M}\right|$$

par des éléments de b_{ik} et de c_{ik}, de la manière suivante:

$$\begin{matrix} b_{\varkappa,\lambda_1} & \ldots b_{\varkappa_1,\lambda_{\varrho-1}} & b_{\varkappa_1,\nu_1} & \ldots b_{\varkappa_1,\nu_\varrho} \\ \cdot & \cdot & \cdot & \cdot \\ b_{\varkappa_{\varrho-1},\lambda_1} & \ldots b_{\varkappa_{\varrho-1},\lambda_{\varrho-1}} & b_{\varkappa_{\varrho-1},\nu_1} & \ldots b_{\varkappa_{\varrho-1},\nu_\varrho} \\ c_{\mu_1,\lambda_1} & \ldots c_{\mu_1,\lambda_{\varrho-1}} & c_{\mu_1,\nu_1} & \ldots c_{\mu_1,\nu_\varrho} \\ \cdot & \cdot & \cdot & \cdot \\ c_{\mu_\varrho,\lambda_1} & \ldots c_{\mu_\varrho,\lambda_{\varrho-1}} & c_{\mu_\varrho,\nu_1} & \ldots c_{\mu_\varrho,\nu_\varrho}. \end{matrix}$$

Ce système donne lieu à une identité due à *L. Kronecker*

$$|L c_{\mu\nu} - L_{\mu\nu}| = 0,$$

où les $L_{\mu\nu}$ sont obtenus en bordant L par les éléments des lignes et colonnes du tableau qui se coupent en $c_{\mu\nu}$.

On en déduira donc, comme on l'a fait plus haut [nº 7], l'inégalité

$$l' - l \leqq l_\varrho' - l_{\varrho-1}',$$

dans laquelle l est l'exposant de p dans le plus grand commun diviseur des $L_{\mu\nu}$, l l'exposant de p dans L, l_ϱ' l'exposant de p dans le plus grand commun diviseur des mineurs du premier ordre de M.

Or on a ici

$$l = \beta_{\varrho-1}, \qquad l_\varrho' = \gamma_\varrho,$$

puisque L et M sont réguliers, $l_{\varrho-1}' = \gamma_{\varrho-1}$ puisqu'un mineur du premier ordre de M est régulier et enfin

$$l' \geqq \beta_\varrho,$$

puisque les $L_{\mu\nu}$ sont, *en égard à la forme des c*, des combinaisons linéaires des mineurs *d'ordre* ϱ du système b_{ik}.

On a donc *a fortiori*

$$\beta_\varrho - \beta_{\varrho-1} \leqq \gamma_\varrho - \gamma_{\varrho-1};$$

c'est ce qu'on voulait démontrer.

Ainsi quand un système b_{ik} est multiple du système a_{ik}, non seulement D_ϱ' est multiple de D_ϱ, mais le quotient $E_\varrho' = \dfrac{D_\varrho'}{D_{\varrho-1}'}$ est aussi multiple de $E_\varrho = \dfrac{D_\varrho}{D_{\varrho-1}}$.

Si, la forme B étant contenue dans A, A est contenue dans B, A et B sont dites *équivalentes.*

Une forme est dite *élémentaire* ou *irréductible,* si elle n'est ni décomposable ni équivalente à une forme décomposable. Toute forme est donc équivalente à une forme décomposable en formes élémentaires. Ceci se transporte des formes aux systèmes des coefficients. D'après cela, *deux formes équivalentes* A *et* B *ont même rang* r, *et l'on a*

$$D'_\varrho = D_\varrho \qquad (\varrho \leqq r),$$
$$E'_\varrho = E_\varrho \qquad (\varrho \leqq n),$$

c'est-à-dire que *les plus grands communs diviseurs des déterminants de degré* ϱ *des systèmes* b_{ik} et a_{ik} *(et par suite les produits élémentaires) sont identiques*[43]*).*

Si le déterminant non nul d'une substitution S est indépendant des paramètres $\lambda, \mu, \ldots$ on la dit *unitaire*; l'inverse S^{-1} sera aussi unitaire. Le produit de deux substitutions unitaires est encore unitaire.

Si l'on a

$$B = SAT,$$

S *et* T *étant unitaires,* on en conclura

$$A = S^{-1}BT^{-1},$$

les coefficients de S^{-1}, T^{-1} étant entiers; *les deux formes* A *et* B *sont donc équivalentes.**

30. Réduction des systèmes[44]). *On emploie pour *réduire* un système par des transformations linéaires, exécutées sur les variables de la forme associée, les *transformations élémentaires* suivantes sur les x (et des transformations analogues sur les y):

a) Changement de x_i en $-x_i$, tous les autres x étant conservés. Les coefficients a_{ik} $(k = 1, 2, \ldots, n)$ changent de signe.

b) Permutation de x_i et x_k seuls. Les coefficients a_{ij} $(j = 1, 2, \ldots, n)$ sont permutés avec les coefficients a_{kj} $(j = 1, 2, \ldots, n)$ de même indice j. (Échange de deux lignes du système).

c) Remplacement de x_i par $x_i + mx_k$, m étant une fonction rationnelle entière de $\lambda, \mu, \ldots$, c'est-à-dire une fonction de même nature que les a_{ik}. On ajoute aux éléments $a_{k1}, a_{k2}, \ldots, a_{kn}$ ceux de la $i^{\text{ième}}$ ligne multipliés par m.

43) *Cette conclusion résulte simplement de la remarque faite plus haut (D'_ϱ multiple de D_ϱ et $r' \leqq r$) et n'exige pas l'intervention de la proposition d'après laquelle E'_ϱ est multiple de E_ϱ.*

44) Cette théorie a été donnée par *H. J. S. Smith* [Philos. Trans. London 151 (1861), p. 314; Papers 1, Oxford 1894, p. 391] pour les systèmes de nombres entiers, étendue par *G. Frobenius* [J. reine angew. Math. 86 (1879), p. 158]; cf. *L. Kronecker*, [J. reine angew. Math. 107 (1891), p. 135]. L'exposition actuelle est celle de *L. Kronecker.*

L'application des transformations (a) et (b) permet d'amener le système à avoir pour élément a_{11} une fonction entière α de degré inférieur en $\lambda, \mu, \ldots$ à celui de tous les éléments de la première ligne et de la première colonne.

S'il se trouve dans la première ligne ou la première colonne un élément β non divisible par α, en faisant la division

$$\beta = h\alpha + \gamma,$$

la transformation (c) qui remplace β par $\beta - h\alpha$ donnera dans la ligne ou colonne correspondante un élément γ de degré inférieur à α. Une transformation (b) amènera cet élément à être le premier élément diagonal.

Si γ ne divise pas α, on répète le raisonnement jusqu'au moment où le premier élément diagonal est le plus grand commun diviseur α_1 de β et de α.

Si tous les éléments de la première ligne ou de la première colonne ne sont pas divibles par α_1, on pourra recommencer.

Comme on laisse toujours subsister les lignes ou les colonnes dont les premiers éléments sont multiples du premier élément diagonal, qui est lui-même remplacé par un de ses diviseurs, *au bout d'un nombre limité d'opérations* tous les éléments de la première ligne et de la première colonne seront des multiples du premier élément diagonal t_1.

Des transformations (c) amènent enfin tous ces éléments à être nuls.

S'il existe, dans les autres lignes ou colonnes, des éléments non divisibles par t_1, on peut ajouter la ligne ou la colonne correspondant à la première et reprendre le raisonnement.

On parvient ainsi à un système T_1 dans lequel *tous les éléments de la première ligne et de la première colonne sont nuls, sauf le premier* t_1 *qui est le plus grand commun diviseur des éléments* a_{ik}.

Le mineur de t_1 dans T_1 est un système T_2 qu'on réduit de même à avoir pour premier élément diagonal t_2, le plus grand commun diviseur de ses éléments, les autres éléments de la première ligne et de la première colonne étant nuls, et ainsi de suite.

On obtient donc enfin un *système diagonal* pour lequel les plus grands communs diviseurs des mineurs du 1^{er}, $2^{\text{ième}}$, ... degré sont

$$D_1 = t_1,\ D_2 = t_1 t_2, \ldots, D_r = t_1 t_2 \ldots t_r,$$

c'est-à-dire que les *produits élémentaires* sont

$$E_1 = t_1,\ E_2 = t_2, \ldots, E_r = t_r,$$

si le système est de rang r. Il en résulte que *la réduction à un système diagonal est unique.*

La forme

$$\sum_{(i,k)} a_{ik} x_i y_k \qquad (i, k = 1, 2, \ldots, n),$$

de déterminant $|a_{ik}|$ différent de zéro, *se laisse transformer par des substitutions élémentaires* (*a*), (*b*), (*c*) *en une forme*

$$E_1 x_1' y_1' + E_2 x_2' y_2' + \cdots + E_n x_n' y_n'.$$

Cette forme est *décomposable* en parties $E_i x_i' y_i'$ qui sont *irréductibles.*

Elle est donc *réduite.**

31. Conditions suffisantes d'équivalence. *On peut maintenant établir que *si les produits élémentaires relatifs à une forme B sont des multiples des produits élémentaires de même indice relatifs à la forme A, B est contenue dans A* (le système des b_{ik} est multiple du système des a_{ik}).

Il existe des substitutions unitaires S, T, U, V satisfaisant aux identités

$$SAT = E_1 x_1 y_1 + E_2 x_2 y_2 + \cdots + E_n x_n y_n = \boldsymbol{A},$$
$$UBV = E_1' x_1 y_1 + E_2' x_2 y_2 + \cdots + E_n' x_n y_n = \boldsymbol{B}.$$

Dans l'hypothèse où l'on a

$$E'_\varrho = \gamma_\varrho E_\varrho \qquad (\varrho = 1, 2, \ldots, n),$$

les γ_i désignant des fonctions entières en $\lambda, \mu, \ldots$, posons

$$C = \gamma_1 x_1 y_1 + \cdots + \gamma_n x_n y_n;$$

d'après une remarque faite sur les formes décomposables on aura

$$\boldsymbol{B} = \boldsymbol{A} C = C \boldsymbol{A}.$$

La forme

$$B = U^{-1} \boldsymbol{B} V^{-1}$$

peut donc s'écrire

$$B = U^{-1} C \boldsymbol{A} V^{-1} = U^{-1} \boldsymbol{A} C V^{-1},$$

ou encore en tenant compte de l'expression de $\boldsymbol{A}$

$$B = (U^{-1} C S) A (T V^{-1}) = (U^{-1} S) A (T C V^{-1});$$

B est donc contenue dans A, et si l'on écrit, pour abréger, les identités précédentes

$$B = PAQ = XAY,$$

les deux substitutions

$$Q = TV^{-1}, \qquad X = U^{-1} S$$

sont unitaires.

Si l'on suppose, en particulier, que les deux formes A et B ont mêmes produits élémentaires, la forme C sera identique à

$$E = x_1 y_1 + x_2 y_2 + \cdots + x_n y_n$$

et les deux substitutions

$$P = U^{-1} E S = U^{-1} S = X,$$
$$Q = T V^{-1} = T E V^{-1} = Y$$

seront unitaires. *Les formes A et B seront donc équivalentes.*

Ainsi *la condition nécessaire et suffisante pour l'équivalence de deux formes* (au sens adopté plus haut) *est l'identité des produits élémentaires.* Ces produits s'obtiennent par *des opérations rationnelles* (recherche de diviseurs communs à deux fonctions entières de $\lambda, \mu, \ldots$); *la réduite commune* et un système de substitutions unitaires transformant les formes données en cette réduite s'en déduisent aussi rationnellement.

On peut conclure de là une importante propriété des *formes décomposables.*

Observons d'abord qu'une forme à $2n$ variables

$$C = \gamma_1 x_1 y_1 + \gamma_2 x_2 y_2 + \cdots + \gamma_r x_r y_r,$$

où les γ_i sont des fonctions entières de $\lambda, \mu, \ldots$ non nulles, étant donnée *a priori*, on trouve aisément les produits élémentaires du système de ses coefficients.

Soit

$$D_r = \gamma_1 \gamma_2 \cdots \gamma_r$$

et supposons qu'un diviseur irréductible p de D_r figure dans γ_i avec l'exposant g_i; désignons par

$$e_1, e_2, \ldots, e_r$$

ces exposants g_i rangés en une suite croissante

$$e_1 \leqq e_2 \leqq \cdots \leqq e_r.$$

Le plus grand commun diviseur des déterminants de degré $(r-1)$ du système des coefficients de C renfermera p à la puissance

$$e_1 + e_2 + \cdots + e_{r-1};$$

l'exposant de p dans $E_r = \frac{D_r}{D_{r-1}}$ sera précisément e_r.

Les diviseurs élémentaires relatifs à p sont donc

$$p^{e_r}, p^{e_{r-1}}, \ldots, p^{e_1}$$

et les produits élémentaires s'obtiendront par la règle suivante: chacun des γ_i étant décomposé en produit de puissances de facteurs irréductibles distincts, le produit des plus hautes puissances de tous les facteurs différents donnera E_r (c'est le p. p. c. m. de $\gamma_1, \gamma_2, \ldots, \gamma_r$); si l'on supprime ces plus hautes puissances, le produit des plus hautes puissances restantes donnera E_{r-1}, et ainsi de suite[45]).

45) *On sait d'ailleurs que E_r, E_{r-1} s'obtiendraient par des opérations rationnelles.*

Considérons maintenant une forme décomposable

$$C = A + B;$$

soient r, p, q les rangs des trois formes C, A, B $(r = p + q)$; désignons par $\gamma_1, \gamma_2, \ldots, \gamma_p$ les produits élémentaires du système des coefficients de A et par $\gamma_{p+1}, \ldots, \gamma_r$ ceux du système des coefficients de B.

Nous savons qu'il existe des substitutions unitaires S, T, U, V telles que

$$SAT = \gamma_1 x_1 y_1 + \gamma_2 x_2 y_2 + \cdots + \gamma_p x_p y_p,$$
$$UBV = \gamma_{p+1} x_{p+1} y_{p+1} + \gamma_{p+2} x_{p+2} y_{p+2} + \cdots + \gamma_r x_r y_r.$$

On en conclut

$$(S + U)(A + B)(T + V) = \gamma_1 x_1 y_1 + \cdots + \gamma_p x_p y_p + \cdots + \gamma_r x_r y_r$$

car on a

$$SAV = SBT = SBV = UAT = UAV = UBT = 0,$$

puisque les variables qui figurent dans S, A, T manquent dans U, B, V et inversement.

Si l'on pose

$$P = S + U, \qquad Q = T + V,$$

on aura donc

$$PCQ = \gamma_1 x_1 y_1 + \cdots + \gamma_r x_r y_r$$

et, comme P et Q sont décomposables,

$$|P| = |S| \cdot |V|, \qquad |Q| = |T| \cdot |V|,$$

c'est-à-dire que P et Q sont unitaires.

Les diviseurs élémentaires de $C = A + B$ sont ceux de la forme

$$\gamma_1 x_1 y_1 + \gamma_2 x_2 y_2 + \cdots + \gamma_r x_r y_r;$$

d'après ce qu'on a vu on les obtient en décomposant $\gamma_1, \gamma_2, \ldots, \gamma_r$ en produits de puissances de facteurs irréductibles distincts: ce sont donc les diviseurs élémentaires des deux parties A, B pris ensemble.

*Les diviseurs élémentaires d'une forme décomposable s'obtiennent en réunissant les diviseurs élémentaires de ses parties.**

32. Équivalence des faisceaux de formes bilinéaires. *Supposons que les coefficients d'une forme A soient des fonctions entières de λ de degré α; on dit qu'elle est *de degré α* et l'on peut écrire

$$A = A_0 \lambda^\alpha + A_1 \lambda^{\alpha-1} + \cdots + A_\alpha$$

où A_0 n'est pas nul. Si l'on a de même, pour une forme de degré β,

$$B = B_0 \lambda^\beta + B_1 \lambda^{\beta-1} + \cdots + B_\beta$$

le produit AB s'écrira, si $|B_0|$ n'est pas nul,

$$AB = A_0 B_0 \lambda^{\alpha+\beta} + (A_0 B_1 + A_1 B_0) \lambda^{\alpha+\beta-1} + \cdots;$$

il sera de degré $(\alpha + \beta)$ car $A_0 B_0$ ne peut s'annuler que si A_0 est nul.

Si $\beta \leqq \alpha$ et si $|B_0|$ est différent de zéro, *on peut toujours trouver une forme Q de degré $\alpha - \beta$ et une forme C de degré $< \beta$, telles que l'on ait*

$$A = QB + C$$

(et de même des formes Q_1, C_1 telles que $A = Q_1 B + C_1$).

Si l'on veut en effet que, en posant

$$Q = Q_0 \lambda^\gamma + Q_1 \lambda^{\gamma-1} + \cdots \qquad (\gamma = \alpha - \beta),$$

la différence $A - QB$ soit de degré inférieur à β, il suffit qu'on ait

$$A_0 = Q_0 B_0,$$
$$A_1 = Q_0 B_1 + Q_1 B_0,$$
$$\cdots\cdots\cdots$$
$$A_\gamma = Q_0 B_\gamma + Q_1 B_{\gamma-1} + \cdots + Q_\gamma B_0,$$

et comme $|B_0|$ n'est pas nul, ces équations donnent

$$Q_0 = A_0 B_0^{-1}, \quad Q_1 = (A_1 - Q_0 B_1) B_0^{-1}, \quad \ldots\ldots$$

Considérons maintenant deux formes A et B dont les coefficients dépendent d'un paramètre λ *au premier degré* (c'est-à-dire *deux faisceaux*)

$$A = \lambda A_0 + A_1, \qquad B = \lambda B_0 + B_1.$$

Il est clair, par exemple, que si $|A_0|$ est différent de zéro

$$|A| = |\lambda A_0 + A_1| = \lambda^n |A_0| + \cdots + |A_1|$$

n'est pas nul quel que soit λ.

Nous avons vu que l'identité des produits élémentaires des systèmes de coefficients de A et de B est la condition nécessaire et suffisante de l'*équivalence* de ces formes, *c'est-à-dire ici d'une identite*

$$B = PAQ$$

dans laquelle les substitutions unitaires P, Q dépendent en général de λ et se déterminent d'ailleurs rationnellement. On peut montrer qu'il existe toujours, dans ce cas, deux substitutions P_2, Q_2 *indépendantes de λ* satisfaisant à l'identité

$$B = P_2 A Q_2,$$

où $|P_2| \cdot |Q_2|$ n'est pas nul, c'est-à-dire que *le faisceau $\lambda B_0 + B_1$ est transformé de $\lambda A_0 + A_1$ par deux substitutions à coefficients constants appliquées aux variables x et aux variables y.*

Posons, pour simplifier l'écriture,

$$P^{-1} = R, \qquad Q^{-1} = S;$$

les substitutions R, S sont unitaires et l'on a

$$PA = BS, \qquad AQ = RB.$$

Si l'on divise respectivement P et Q par B, R et S par A, on sera conduit aux identités

$$P = BP_1 + P_2, \qquad Q = Q_1 B + Q_2,$$
$$R = AR_1 + R_2, \qquad S = S_1 A + S_2,$$

dans lesquelles on peut supposer P_2, Q_2, R_2, S_2 *indépendantes de* λ puisque A et B sont du premier degré.

On déduit de là deux expressions de PA:

$$PA = BS = B(S_1 A + S_2) = BS_1 A + BS_2,$$
$$PA = (BP_1 + P_2)A = BP_1 A + P_2 A;$$

d'où l'identité

$$BS_1 A + BS_2 = BP_1 A + P_2 A$$

qui s'écrit aussi

$$B(S_1 - P_1)A = P_2 A - BS_2.$$

Or le premier membre renferme un terme en λ^2 si $|B_0|\cdot|A_0|$ est différent de zéro; le second membre est du premier degré en λ: il en résulte

$$S_1 - P_1 = 0$$

et ensuite

$$P_2 A = BS_2.$$

Pour établir que $|P_2|\cdot|S_2|$ n'est pas nul, si l'on pose, suivant l'usage,

$$E = x_1 y_1 + x_2 y_2 + \cdots + x_n y_n,$$

on aura

$$E = QS$$

et par suite, en tenant compte des expressions de Q et S,

$$E = Q(S_1 A + S_2) = QS_1 A + QS_2 = QS_1 A + Q_1 BS_2 + Q_2 S_2.$$

Cette expression de E donne donc aussi

$$E - Q_2 S_2 = QS_1 A + Q_1 P_2 A = (QS_1 + Q_1 P_2)A;$$

or le premier membre est indépendant de λ et le second renferme λ si l'on n'a pas

$$QS_1 + Q_1 P_2 = 0.$$

Avec cette identité, on a par suite

$$E = Q_2 S_2;$$

d'où l'on peut conclure que $|Q_2|$ et $|S_2|$ ne sont pas nuls.

L'identité

$$P_2 A Q_2 = BS_2 Q_2 = BE = B$$

prouve alors que $|P_2|$ est différent de zéro, puisque $|B|$ est différent de zéro.

Nous avons donc établi, dans l'hypothèse $|A_0|\cdot|B_0|$ différent de zéro, que *si les produits élementaires relatifs aux coefficients des formes*

$$A = \lambda A_0 + A_1, \quad B = \lambda B_0 + B_1$$

sont identiques il existe deux substitutions à coefficients indépendants de λ *et à déterminant non nul* (substitutions qu'on peut obtenir rationnellement) *qui satisfont à l'identité*

$$B = P_2 A Q_2,$$

c'est-à-dire transforment le faisceau A *en le faisceau* B. C'est le résultat de *K. Weierstrass*.

Des considérations entièrement analogues à celles de *K. Weierstrass* permettent d'étendre ce résultat au cas où $|A_0| = 0$, $|B_0| = 0$ mais où les déterminants $|A|$ et $|B|$ ne sont pas identiquement nuls, c'est-à-dire donnent *les conditions nécessaires et suffisantes de l'équivalence de deux faisceaux ordinaires.**

Applications du calcul symbolique aux formes symétriques ou alternées.

I. Équivalence large des formes symétriques ou alternées.

33. Congruence des formes symétriques. *Supposons que les deux formes *symétriques* A et B donnent lieu à l'identité

$$B = PAQ;$$

en passant aux conjuguées on aura

$$B = Q'AP',$$

d'où, en égalant les valeurs de B

$$Q'^{-1}PA = AP'Q^{-1}.$$

Il suffit de poser

$$U = (Q')^{-1}P, \text{ ce qui donne } U' = PQ^{-1},$$

pour obtenir

$$UA = AU', \; U^2 A = AU'^2, \ldots, \; U^k A = AU'^k, \ldots;$$

d'où l'on conclut, *quelle que soit la fonction rationnelle entière* $X(U)$,

$$X(U)A = AX(U')$$

ou, si $|X(U)|$ est différent de zéro,

$$B = PX(U)^{-1}AX(U')Q.$$

Peut-on choisir $X(U)$ *de manière que les transformations*

$$PX(U)^{-1} \text{ et } X(U')Q$$

soient conjuguées?

On devra écrire:

$$PX(U)^{-1} = [X(U')Q]' = Q'X(U)$$

d'où

$$P = Q'X(U)^2, \quad (Q')^{-1}P = X(U)^2 = U.$$

La fonction $X(U)$ est donc celle que nous avons représentée par $\sqrt{U}$.

Inversement soit V l'une des racines carrées de U, désignons par $\sqrt{U'}$ la conjuguée V'; on aura, en posant

$$R = V'Q,$$
$$R'AR = Q'VAV'Q.$$

Or pour toute fonction rationnelle entière $\varphi(U)$

$$\varphi(U)A = A\varphi(U'),$$

donc aussi

$$VA = AV'$$

et

$$R'AR = Q'AV'^2Q = Q'AU'Q,$$

c'est-à-dire enfin

$$R'AR = Q'AP = B \text{ puisque } U'Q = P'.$$

D'ailleurs

$$|R| = |V'|\,|Q| = \pm\sqrt{|U'|}\cdot|Q| = \pm\sqrt{|P|\,|Q|}$$

est différent de zéro.

Ainsi *deux formes symétriques A et B qui satisfont à une identité*

$$B = PAQ, \text{ où } |P|\,|Q| \text{ n'est pas nul,}$$

satisfont également à une identité

$$B = R'AR, \text{ où } |R| \text{ n'est pas nul,}$$

dans laquelle R ne dépend que des substitutions P et Q,

$$R = \sqrt{P'Q^{-1}}\cdot Q,$$

c'est-à-dire sont transformables l'une dans l'autre par des substitutions congruentes des deux séries de variables.

On conclut du fait que R dépend seulement de P et Q que si l'on a

$$B_i = PA_iQ \qquad (i = 1, 2, 3, \ldots),$$

où les A_i et B_i sont symétriques, on a aussi

$$\Sigma\lambda_iB_i = P(\Sigma\lambda_iA_i)Q.$$

Pour $i = 2$ on a la proposition de *K. Weierstrass*: *si deux faisceaux de formes bilinéaires symétriques sont équivalents, il sont congruents.*

On observera ici qu'on sait trouver *par des opérations rationnelles* les substitutions P et Q qui transforment un faisceau symétrique $\lambda_1A_1 + \lambda_2A_2$ en un faisceau équivalent $\lambda_1B_1 + \lambda_2B_2$. Il suffira pour déterminer la transformation R qui, exécutée à la fois sur les x et sur les y, change le faisceau

$$\lambda_1A_1 + \lambda_2A_2$$

en

$$\lambda_1B_1 + \lambda_2B_2$$

d'extraire la racine carrée de

$$(Q')^{-1}P = U,$$

ce qui exige la formation *et la résolution de l'équation de degré le plus petit vérifiée par U.*

La proposition précédente s'étend au cas où les formes A_1 et A_2 sont toutes deux alternées ainsi que B_1 et B_2, et aussi au cas où A_1 et B_1 sont symétriques, A_2 et B_2 alternées.

Cela résulte immédiatement du fait qu'avec

$$B = PAQ$$

on a aussi, si B et A sont *alternées*, en passant aux conjuguées

$$(-B) = Q'(-A)P' \text{ ou bien } B = Q'AP'.\text{"}$$

II. Étude du faisceau $\lambda_1S + \lambda_2T$ où S est symétrique et T alterné.

34. Lemme de Stickelberger. „Cette étude, due essentiellement à *L. Kronecker*[46]), conduit à des résultats très importants pour la recherche des transformations congruentes des formes bilinéaires en elles-mêmes.

Nous en donnerons les résultats au moyen de la méthode de *G. Frobenius* qui est fondée sur l'établissement préalable du lemme suivant, dû à *L. Stickelberger*[47]).

Soient A et B deux formes bilinéaires de $2n$ variables; si le faisceau

$$\lambda A - B$$

est ordinaire et si

$$(\lambda - c)^{e_1}, (\lambda - c)^{e_2}, \ldots$$

sont les diviseurs élémentaires de $|\lambda A - B|$ correspondant à la base $\lambda - c$ et rangés d'après l'ordre décroissant de leurs exposants, on sait qu'en développant $(\lambda A - B)^{-1}$ suivant les puissances croissantes de $(\lambda - c)$ on aura

$$(\lambda A - B)^{-1} = H(\lambda - c)^{-e_1} + \cdots$$

où H est une forme bilinéaire convenable.

L. Stickelberger établit que *le rang de $|H|$ est r si l'on a*

$$e_1 = e_2 = \cdots = e_r > e_{r+1};$$

la réciproque en résulte.

---

46) Monatsb. Akad. Berlin 1874, p. 441; Werke 1, Leipzig 1895, p. 476; Sitzgsb. Akad. Berlin 1890, p. 1225/37, 1379/88; id. 1891, p. 9/17, 34/44.

47) J. reine angew. Math. 86 (1879), p. 20. La démonstration donnée ici est de *G. Frobenius* (d'après une lettre adressée à *L. Stickelberger* en 1878).

a) *G. Frobenius* démontre d'abord la proposition dans un cas particulier.

Si l'on pose

$$C = x_1 y_2 + \cdots + x_{n-1} y_n$$

on aura symboliquement

$$C^2 = x_1 y_3 + \cdots + x_{n-2} y_n$$
$$\cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot$$
$$C^{n-1} = x_1 y_n$$
$$C^n = 0$$

et le rang de $|C^{n-1}|$ est un.

Soient alors $a, b, \ldots, s$ des entiers positifs décroissants tels que

$$a + b + \cdots + s \leqq n$$

et

$$C_1 = x_1 y_2 + \cdots + x_{a-1} y_a$$
$$C_2 = x_{a+1} y_{a+2} + \cdots + x_{a+b-1} y_{a+b}$$
$$\cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot$$
$$E_1 = x_1 y_1 + \ldots + x_a y_a$$
$$E_2 = x_{a+1} y_{a+1} + \cdots + x_{a+b} y_{a+b}$$
$$\cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot$$

Posons en outre

$$E_0 = x_{s+1} y_{s+1} + \cdots + x_n y_n$$

et désignons par C_0 une forme *ordinaire* de ces $2(n-s)$ variables.

On a

$$E = E_1 + E_2 + \cdots + E_0,$$

et si l'on pose

$$B = C_1 + C_2 + \cdots + C_0$$

le faisceau

$$\lambda E - B$$

est *décomposable* en faisceaux

$$\lambda E_1 - C_1, \quad \lambda E_2 - C_2, \quad \ldots, \quad \lambda E_0 - C_0.$$

Les diviseurs élémentaires correspondant à ces faisceaux sont

$$\lambda^a, \ \lambda^b, \ldots;$$

comme le déterminant $|\lambda E_0 - C_0|$ n'a pas la racine $\lambda = 0$, ces diviseurs élémentaires sont aussi les diviseurs élémentaires de $|\lambda E - B|$ pour la base λ.

Mais on a symboliquement, d'après l'expression de B,

$$B^2 = C_1{}^2 + C_2{}^2 + \cdots + C_0{}^2$$
$$B^3 = C_1{}^3 + C_2{}^3 + \cdots + C_0{}^3$$
$$\cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot$$

et si l'on suppose $a \geqq b \geqq \cdots \geqq s$, on aura par suite

$$C_i^a = 0 \text{ (pour } i \text{ différent de zéro) et } B^{a+k} = C_0^{a+k}.$$

D'autre part, on a les développements

$$(\lambda E_1 - C_1)^{-1} = \frac{E_1}{\lambda} + \frac{C_1}{\lambda^2} + \frac{C_1{}^2}{\lambda^3} + \cdots + \frac{C_1^{a-1}}{\lambda^a}$$
$$\cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot$$
$$(\lambda E_0 - C_0)^{-1} = \frac{E_0}{\lambda} + \frac{C_0}{\lambda^2} + \cdots + \frac{C_0^{a-1}}{\lambda^a} + \frac{C_0^a}{\lambda^{a+1}} + \cdots,$$

d'où l'on déduit, en ajoutant membre à membre,

$$\Sigma(\lambda E_i - C_i)^{-1} = \frac{E}{\lambda} + \frac{B}{\lambda^2} + \frac{B^2}{\lambda^3} + \cdots$$

Le second membre est le développement de $(\lambda E - B)^{-1}$; on a donc

$$(\lambda E_1 - C_1)^{-1} + \cdots + (\lambda E_0 - C_0)^{-1} = (\lambda E - B)^{-1}.$$

Dans l'hypothèse actuelle, ce développement de $(\lambda E - B)^{-1}$ commence à la puissance $(-a)$ et l'on peut écrire

$$(\lambda E - B)^{-1} = \frac{H}{\lambda^a} + \frac{J}{\lambda^{a+1}} + \cdots$$

Supposons que les r premiers nombres $a, b, \ldots$ soient égaux et supérieurs au $(r+1)^{\text{ième}}$, on aura

$$H = C_1^{a-1} + C_2^{a-1} + \cdots + C_r^{a-1};$$

la forme H est *décomposable* en r formes de *rang un*. Elle est donc de rang r. La réciproque est évidente. Le lemme est donc établi pour le faisceau

$$(\lambda E - B),$$

où B a la signification indiquée plus haut.

b) Supposons un faisceau

$$\lambda A - B$$

pour lequel le déterminant $|A|$ est différent de zéro tandis que le déterminant $|B|$ est nul, et soient

$$\lambda^a, \ \lambda^b, \ldots$$

les diviseurs élémentaires relatifs à la base λ, rangés dans l'ordre des exposants décroissants.

Choisissons C_0 de manière que les diviseurs élémentaires de $|\lambda E_0 - C_0|$ coïncident avec ceux de $|\lambda A - B|$ qui n'ont pas la base λ (ce qui est possible d'après les résultats obtenus par *K. Weierstrass*); en posant alors

$$\overline{B} = C_1 + C_2 + \cdots + C_0$$

le déterminant $|\lambda E - \overline{B}|$ a mêmes diviseurs élémentaires que $|\lambda A - B|$.

Il existe donc deux substitutions ordinaires P, Q à coefficients indépendants de λ, telles que

$$\lambda E - \overline{B} = P(\lambda A - B)Q.$$

On en déduit

$$(\lambda E - \overline{B})^{-1} = Q^{-1}(\lambda A - B)^{-1}P^{-1},$$

et si l'on pose

$$(\lambda E - \overline{B})^{-1} = \frac{\overline{H}}{\lambda^{\alpha}} + \cdots, \qquad (\lambda A - B)^{-1} = \frac{H}{\lambda^{\alpha}} + \cdots,$$

on en peut conclure

$$\overline{H} = Q^{-1}HP^{-1}.$$

Comme $|P|$ et $|Q|$ sont différents de zéro, $\overline{H}$ et H sont de même rang r. Ainsi $(\lambda A - B)$ possède exactement r fois le diviseur élémentaire λ^{α}.

Le lemme est donc établi si $|A|$ n'est pas nul lorsque $|B|$ est nul, pour la base λ.

c) Dans le cas général où

$$(\lambda - c)^{e_1},\ (\lambda - c)^{e_2}, \ldots$$

sont les diviseurs élémentaires du faisceau ordinaire $\lambda A - B$, relatifs à la base $\lambda - c$, et où l'on a

$$e_1 \geqq e_2 \geqq \cdots$$

et

$$(\lambda A - B)^{-1} = \frac{H}{(\lambda - c)^{e_1}} + \frac{J}{(\lambda - c)^{e_1 + 1}} + \cdots,$$

on pose, dans l'hypothèse où $|gA - B|$ est différent de 0,

$$\lambda - c = \frac{(c-g)\mu}{1-\mu}, \quad \text{où} \quad \mu = \frac{\lambda - c}{\lambda - g},$$

ce qui donne

$$\lambda A - B = \frac{1}{\mu - 1}[\mu(gA - B) - (cA - B)] = \frac{1}{\mu - 1}(\mu\bar{A} - \overline{B}).$$

Le nouveau faisceau $\mu\bar{A} - \overline{B}$ est tel que $|\bar{A}|$ soit différent de zéro et que $|\overline{B}|$ soit nul; les diviseurs élémentaires relatifs à la base μ sont

$$\mu^{e_1},\ \mu^{e_2}, \ldots$$

et l'on a

$$(\mu - 1)(\mu\bar{A} - \overline{B})^{-1} = (\lambda A - B)^{-1} = \frac{H}{(c-g)^{e_1}} \cdot \frac{(1-\mu)^{e_1}}{\mu^{e_1}} + \cdots,$$

d'où l'on conclut

$$(\mu\bar{A} - \overline{B})^{-1} = \frac{-H}{(c-g)^{e_1}} \frac{(1-\mu)^{e_1 - 1}}{\mu^{e_1}} + \cdots = \frac{-H}{(c-g)^{e_1}} \frac{1}{\mu^{e_1}} + \cdots$$

Il suit de là que, si $|H|$ est de rang r, on a

$$e_1 = e_2 = \cdots = e_r > e_{r+1}.$$

Le lemme est donc établi dans le cas général.*

35. Théorème de Kronecker. *„Si S est une forme symetrique, T une forme alternée de $2n$ variables, les diviseurs élémentaires $\lambda_1^{2\varkappa}$ et $\lambda_2^{2\varkappa+1}$ du faisceau ordinaire*

$$\lambda_1 S + \lambda_2 T$$

s'associent toujours par couples[48]).

Supposons $|T| = 0$; soient $\lambda_1^{e_1}, \lambda_1^{e_2}, \ldots$ les diviseurs élémentaires relatifs à la base λ_1, rangés d'après l'ordre décroissant des exposants. On aura

$$(\lambda S - T)^{-1} = \frac{H}{\lambda^{e_1}} + \cdots$$

et, si l'on passe aux formes conjuguées

$$(\lambda S + T)^{-1} = \frac{H'}{\lambda^{e_1}} + \cdots$$

En changeant dans la dernière identité λ en $-\lambda$, il vient

$$-(\lambda S - T)^{-1} = (-1)^{e_1}\frac{H'}{\lambda^{e_1}} + \cdots,$$

d'où l'on conclut

$$H = (-1)^{e_1 + 1}H'.$$

Si e_1 est pair, H est une forme alternée; son rang r est un nombre pair.

Les diviseurs élémentaires *égaux*

$$\lambda_1^{e_1},\ \ldots,\ \lambda_1^{e_r}$$

sont donc en nombre pair.

Supposons $|S| = 0$ et soient

$$\lambda_2^{e_1},\ \lambda_2^{e_2}, \ldots$$

les diviseurs élémentaires relatifs à la base λ_2, avec $e_1 \geqq e_2 \geqq \cdots$

On aura alors

$$(\lambda T - S)^{-1} = \frac{H}{\lambda^{e_1}} + \cdots$$

et, en passant aux conjuguées,

$$(-\lambda T - S)^{-1} = \frac{H'}{\lambda^{e_1}} + \cdots,$$

d'où comme plus haut

$$H = (-1)^{e_1}H'.$$

Si e_1 est impair, H est une forme alternée; son rang r est pair. Les diviseurs élémentaires *égaux*

$$\lambda_2^{e_1},\ \lambda_2^{e_2},\ \ldots,\ \lambda_2^{e_r}$$

sont donc en nombre pair.

48) *L. Kronecker,* Monatsb. Akad. Berlin 1874, p. 397/447; Werke 1, Leipzig 1895, p. 423/83.

Il nous reste à établir que cette propriété appartient aussi aux diviseurs élémentaires $\lambda_1^{2\varkappa}$ (ou $\lambda_2^{2\varkappa+1}$) *quand leurs exposants ne sont pas les plus elevés relatifs aux bases* λ_1 (ou λ_2). *G. Frobenius* le démontre, *même pour un faisceau singulier* $\lambda_1 S + \lambda_2 T$, comme suit:

Soit r le rang du déterminant $|\lambda_1 S + \lambda_2 T|$ supposé identiquement nul; admettons que λ_1 figure à la puissance l_ϱ dans le plus grand commun diviseur de ses mineurs de degré ϱ. Si l'on pose

$$e_\varrho = l_\varrho - l_{\varrho-1}$$

on aura

$$e_r \geqq e_{r-1} \geqq \cdots$$

Faisons l'hypothèse que pour un certain $\varrho \leqq r-1$ on ait

$$e_{\varrho+1} > e_\varrho$$

et montrons qu'il existe, relativement à λ_1, un mineur principal *régulier* de degré ϱ.

Soient a_{ik} les éléments de $|\lambda_1 S + \lambda_2 T|$; si l'on pose

$$Q = |a_{\varkappa\nu}| \qquad (\varkappa = \varkappa_1, \varkappa_2, \ldots, \varkappa_\varrho;\ \nu = \nu_1, \nu_2, \ldots, \nu_\varrho)$$

$$R = |a_{\mu\lambda}| \qquad (\mu = \nu_1, \nu_2, \ldots \nu_\varrho;\ \lambda = \varkappa_1, \varkappa_2, \ldots, \varkappa_\varrho)$$

et de même

$$P = |a_{\varkappa\lambda}|, \qquad S = |a_{\mu\nu}|,$$

ces derniers sont des mineurs principaux de degré ϱ.

Supposons Q régulier relativement à λ_1, il en sera de même de R qui s'en déduit en changeant λ_2 en $-\lambda_2$; le produit QR est donc divisible *exactement* par la puissance $2l_\varrho$ de λ_1.

On sait d'autre part que

$$QR - PS$$

contient λ_1 à une puissance *au moins égale à* $l_{\varrho-1} + l_{\varrho+1}$, et supérieure à $2l_\varrho$ puisque $e_{\varrho+1} > e_\varrho$. On en conclut que *$P$ et S sont réguliers* (leur produit contient exactement λ_1 à la puissance $2l_\varrho$).

Il existe en outre toujours un mineur principal *de degré r*, régulier relativement à λ_1. Car dans l'hypothèse $\varrho = r$, on a simplement

$$PS - QR = 0$$

et si Q est régulier, il en sera de même de R, puis de P et S.

Soit maintenant P un mineur principal *de degré r*, régulier par rapport à λ_1, du déterminant $|\lambda_1 S + \lambda_2 T|$; si l'on écrit la forme bilinéaire qui a P pour déterminant

$$\lambda_1 S_0 + \lambda_2 T_0$$

S_0 est symétrique et T_0 alternée. Les diviseurs élémentaires de P relatifs à la base λ_1 sont aussi ceux de $|\lambda_1 S + \lambda_2 T|$ pour la même base,

$$\lambda_1^{e_r}, \lambda_1^{e_{r-1}}, \ldots$$

Si e_r est un nombre pair, on aura donc

$$e_r = e_{r-1} = \cdots = e_{\varrho+1} > e_\varrho$$

la différence $r - \varrho$ étant paire, d'après la démonstration donnée plus haut.

Puisque $e_{\varrho+1} > e_\varrho$, il existe un mineur principal de degré ϱ régulier par rapport à λ_1, et le même raisonnement montre que *si e_ϱ est pair, le nombre des diviseurs élémentaires égaux à $\lambda_1^{e_\varrho}$ est également pair.*

Et ainsi de suite . . .

On démontre d'une manière analogue la proposition relative aux diviseurs élémentaires $\lambda_2^{2\varkappa+1}$.

Faisceau singulier. Supposons qu'il existe entre les dérivées

$$U_i = \frac{\partial(\lambda_1 S + \lambda_2 T)}{\partial y_i}$$

une relation linéaire

$$a_1 U_1 + a_2 U_2 + \cdots + a_n U_n = 0,$$

où les coefficients a_i sont de degré g par rapport à $\frac{\lambda_1}{\lambda_2}$; on en déduit, en permutant les x et les y de même indice et changeant λ_2 en $-\lambda_2$, une relation

$$a_1' V_1 + a_2' V_2 + \cdots + a_n' V_n = 0$$

entre les

$$V_i = \frac{\partial(\lambda_1 S + \lambda_2 T)}{\partial x_i},$$

où les a_i' sont de degré g en $\frac{\lambda_1}{\lambda_2}$.

L'ensemble des mineurs de $|\lambda_1 S + \lambda_2 T|$ de degré ϱ, demeure inaltéré par le changement de λ_2 en $-\lambda_2$; il en résulte que si le diviseur linéaire $(a\lambda_1 + b\lambda_2)$, où ab n'est pas nul, figure dans le plus grand commun diviseur de ces mineurs avec l'exposant l, le diviseur linéaire $(a\lambda_1 - b\lambda_2)$ y figure avec le même exposant.

A tout diviseur élémentaire

$$(a\lambda_1 + b\lambda_2)^e$$

correspond ainsi un diviseur élémentaire

$$(a\lambda_1 - b\lambda_2)^e.$$

On peut d'ailleurs construire un faisceau

$$\lambda_1 S + \lambda_2 T$$

à $2n$ variables de type donné à l'avance au sens de *L. Kronecker* et *K. Weierstrass,* pourvu que les diviseurs élémentaires satisfassent aux conditions précédentes.*

III. Équivalence étroite des formes bilinéaires.

36. Formes congruentes. *Si la même transformation R exécutée sur les x et sur les y change une forme A en une forme B, on dit que les deux formes sont *congruentes* et l'on a symboliquement

$$B = R'AR.$$

On déduit de là en permutant les x et les y de même indice

$$B' = R'A'R,$$

d'où

$$\lambda_1 B + \lambda_2 B' = R'(\lambda_1 A + \lambda_2 A')R.$$

L'équivalence des faisceaux

$$\lambda_1 A + \lambda_2 A' \quad \text{et} \quad \lambda_1 B + \lambda_2 B'$$

est donc une condition nécessaire pour que les formes A et B soient congruentes.

Cette condition est suffisante[48]).

Admettons en effet que

$$\lambda_1 B + \lambda_2 B' = P(\lambda_1 A + \lambda_2 A')Q, \qquad |P||Q| \neq 0$$

On en déduira, en introduisant les formes symétriques

$$A_1 = A + A', \qquad B_1 = B + B'$$

et les formes alternées

$$A_2 = A - A', \qquad B_2 = B - B',$$

$$B_1 = PA_1Q, \qquad B_2 = PA_2Q,$$

puis ensuite

$$\lambda_1 B_1 + \lambda_2 B_2 = P(\lambda_1 A_1 + \lambda_2 A_2)Q.$$

Sous cette nouvelle forme, nous savons qu'il existe pour le faisceau une transformation R qui change la forme symétrique A_1 en B_1 et la forme alternée A_2 en B_2:

$$B_1 = R'A_1R, \qquad B_2 = R'A_2R;$$

nous avons donc aussi

$$\lambda_1 B + \lambda_2 B' = R'(\lambda_1 A + \lambda_1 B')R$$

et en particulier

$$B = R'AR.$$

La condition nécessaire et suffisante pour qu'une même transformation exécutée sur les x et sur les y change une forme A en une forme B est que les faisceaux $\lambda_1 A + \lambda_2 A'$ et $\lambda_1 B + \lambda_2 B'$ (où A', B' sont les conjuguées de A et B) soient équivalents.

Étudions d'un peu plus près le faisceau $\lambda_1 A + \lambda_2 A' = S$.

Une permutation de x_i et y_i accompagnée de celle de λ_1 et λ_2 ne l'altère pas. Les nombres m_i sont donc respectivement égaux aux $\overline{m}_i$, de telle sorte que, pour un faisceau singulier, il n'existe qu'une série de ces nombres.

Supposons $|\lambda_1 A + \lambda_2 A'|$ de rang r; soit $\varrho \leqq r$ et D_ϱ le plus grand commun diviseur des mineurs de degré ϱ du déterminant $|\lambda_1 A + \lambda_2 A'|$, D_ϱ est symétrique ou alterné en λ_1, λ_2. Les quotients

$$E_\varrho = \frac{D_\varrho}{D_{\varrho-1}}, \quad (\varrho = 1, 2, \ldots, n)$$

sont donc aussi symétriques ou alternés en λ_1, λ_2.

Si l'on décompose ces *produits élémentaires* en diviseurs élémentaires, à tout diviseur $(a_\sigma \lambda_1 + b_\sigma \lambda_2)^{e_\sigma}$ correspondra

$$(a_\sigma \lambda_2 + b_\sigma \lambda_1)^{e_\sigma} \quad \text{si} \quad a_\sigma \text{ est différent de } \pm b_\sigma.$$

Écrivons

$$\lambda_1 A + \lambda_2 A' = \frac{\lambda_1 + \lambda_2}{2}(A + A') + \frac{\lambda_1 - \lambda_2}{2}(A - A');$$

en posant

$$\frac{\lambda_1 + \lambda_2}{2} = \lambda'_1, \qquad \frac{\lambda_1 - \lambda_2}{2} = \lambda'_2$$

et remarquant que $A + A'$ est symétrique, $A - A'$ alternée, on peut conclure d'une étude antérieure[49]) que les diviseurs élémentaires $\lambda_1'^{2\varkappa}$ ou $\lambda_2'^{2\varkappa+1}$ sont doubles, tandis que ceux qui sont de la forme $\lambda_1'^{2\varkappa+1}$ ou $\lambda_2'^{2\varkappa}$ peuvent figurer en nombre quelconque.

Ainsi, *pour un faisceau singulier $\lambda_1 A + \lambda_2 A'$ les diviseurs élémentaires de $|\lambda_1 A + \lambda_2 A'|$ sont deux à deux de même degré et de la forme $(a_\sigma \lambda_1 + b_\sigma \lambda_2)^{e_\sigma}$, $(a_\sigma \lambda_2 + b_\sigma \lambda_1)^{e_\sigma}$, sauf ceux de la forme $(\lambda_1 + \lambda_2)^{2\varkappa+1}$ ou $(\lambda_1 - \lambda_2)^{2\varkappa}$ qui peuvent être en nombre pair ou impair.**

37. Types de formes congruentes. *Posons

$$n_i^0 = 2m_i + 1$$

et désignons par

$$\overset{+}{e}_\sigma$$

l'exposant d'un diviseur élémentaire $(\lambda_1 + \lambda_2)^{e_\sigma}$, par

$$\overset{-}{e}_\sigma$$

celui d'un diviseur élémentaire $(\lambda_1 - \lambda_2)^{e_\sigma}$; on aura, puisque $m_i = \overline{m}_i$,

$$n = \sum n_i^0 + \sum \overset{+}{e}_\sigma + \sum \overset{-}{e}_\sigma + \sum e_\sigma.$$

Les n_i^0 manquent si $|\lambda A + \lambda_2 A'|$ est différent de zéro; les nombres pairs $\overset{+}{e}_\sigma$ et les nombres impairs $\overset{-}{e}_\sigma$ figurent par couples.

49) *L. Kronecker*, Monatsb. Akad. Berlin 1874, p. 441; Werke 1, Leipzig 1895, p. 477.

Pour tout système de valeurs des entiers

$$n_i^0,\ \overset{+}{e}_\sigma,\ \ldots$$

satisfaisant à ces conditions, on peut construire un faisceau

$$\lambda_1 A + \lambda_2 A'$$

qui possède ces invariants. On l'obtiendra comme somme de faisceaux des six types suivants:

$$(\alpha_1) \qquad T_i^0 = x_0 y_1 + x_1 y_2 + \cdots + x_{2m_i-1} y_{2m_i},$$

où

$$n_i^0 = 2m_i + 1 > 1.$$

Cette forme est à $2m_i + 1$ couples de variables; le déterminant $|\lambda_1 T_i^0 + \lambda_2 T_i^0|$ est de rang $2m_i$; il n'existe donc qu'une seule relation entre les dérivées $\frac{\partial}{\partial x_i}$ $\left(\text{et entre les dérivées } \frac{\partial}{\partial y_i}\right)$.

Le faisceau correspondant n'a pas de diviseurs élémentaires.

$$(\alpha_2)\ T_\sigma = (x_0 y_1 + c x_1 y_0) + (x_1 y_2 + c x_2 y_1) + \cdots + (x_{2e_\sigma-2} y_{2e_\sigma-1} + c x_{2e_\sigma-1} y_{2e_\sigma-2}),$$

où c^2 est différent de 1.

Cette forme dépend de $2e_\sigma$ couples de variables; le faisceau $(\lambda_1 T_\sigma + \lambda_2 T_\sigma')$ a les diviseurs élémentaires

$$(\lambda_1 + c\lambda_2)^{e_\sigma},\ (c\lambda_1 + \lambda_2)^{e_\sigma}.$$

$$(\alpha_3)\ \overset{+}{F}_\sigma = (x_0 y_1 + x_1 y_0) + (x_1 y_2 - x_2 y_1) + \cdots + (x_E y_{E+1} + (-1)^E x_{E+1} y_E),$$

où

$$E = 2\overset{+}{e}_\sigma - 2 \quad \text{et} \quad \overset{+}{e}_\sigma = 2\varkappa.$$

Le faisceau

$$(\lambda_1 \overset{+}{F}_\sigma + \lambda_2 \overset{+}{F}_\sigma{}')$$

dépend de $2\overset{+}{e}_\sigma$ couples de variables; il a les diviseurs élémentaires

$$(\lambda_1 + \lambda_2)^{\overset{+}{e}_\sigma},\ (\lambda_1 + \lambda_2)^{\overset{+}{e}_\sigma}.$$

$$(\alpha_4)\ \overset{+}{G}_\sigma = x_0 y_0 + (x_1 y_0 - x_0 y_1) + (x_2 y_1 + x_1 y_2) + \cdots + (x_E y_{E-1} + (-1)^E x_{E-1} y_E),$$

où

$$E = \overset{+}{e}_\sigma - 1 \quad \text{et} \quad \overset{+}{e}_\sigma = 2\varkappa + 1.$$

Le déterminant du faisceau à $\overset{+}{e}_\sigma$ couples de variables n'a qu'un seul diviseur élémentaire

$$(\lambda_1 + \lambda_2)^{\overset{+}{e}_\sigma}.$$

A ces deux formes $\overset{+}{F}_\sigma$ et $\overset{+}{G}_\sigma$ en correspondent deux autres

$$(\alpha_5)\ \overline{F}_\sigma = x_0 y_0 + (x_1 y_0 - x_0 y_1) + (x_2 y_1 + x_1 y_2) + \cdots + (x_E y_{E-1} + (-1)^E x_{E-1} y_E)$$

où

$$E = \overline{e}_\sigma - 1 \quad \text{et où} \quad \overline{e}_\sigma = 2\varkappa,$$

et

$$(\alpha_6) \qquad \overline{G}_\sigma = \sum_{(k)} (x_k y_{k+1} - (-1)^k x_{k+1} y_k)$$

où

$$k = 0, 1, \ldots, 2\overline{e}_\sigma - 2; \quad \text{et} \quad \overline{e}_\sigma = 2\varkappa + 1$$

et les faisceaux correspondants ont respectivement les diviseurs élémentaires

$$(\lambda_1 - \lambda_2)^{\overline{e}_\sigma} \text{ et } (\lambda_1 - \lambda_2)^{\overline{e}_\sigma},\ (\lambda_1 - \lambda_2)^{\overline{e}_\sigma}.$$

L. Kronecker réunit $\overset{+}{F}_\sigma$ et $\overline{G}_\sigma$ dans une même expression, en introduisant dans chaque parenthèse le facteur $(-1)^{e_\sigma}$ devant le premier terme; et de même $\overset{+}{G}_\sigma$ et $\overline{F}_\sigma$ qui ne diffèrent de $\overset{+}{F}_\sigma$ et $\overline{G}_\sigma$ que par la parité de e_σ.

Si l'on dit qu'une forme bilinéaire à *variables cogrédientes* est *irréductible* ou *élémentaire* quand elle n'est ni décomposable ni congruente à une forme décomposable, on peut reconnaître que *les formes* $(\alpha_1), \ldots, (\alpha_6)$ *sont irréductibles.*

C'est évident pour (α_1), (α_4), (α_5) qui n'ont qu'un invariant; pour les autres cela résulte de ce qu'un faisceau congruent décomposable en deux autres possède au moins quatre diviseurs élémentaires.

Étant donnée une forme bilinéaire quelconque A à $2n$ variables, nous pouvons construire, comme somme de formes irréductibles $(\alpha_1), \ldots, (\alpha_6)$, une forme R qui dépende de $2n$ variables et possède les mêmes invariants (c'est-à-dire que les faisceaux $\lambda_1 A + \lambda_2 A'$ et $\lambda_1 R + \lambda_2 R'$ ont mêmes invariants). Cette forme R est dite *réduite*; comme elle est congruente à A, nous avons effectué la *réduction d'une forme quelconque par des transformations congruentes des deux séries de variables.*

Lorsque le faisceau

$$\lambda_1 A + \lambda_2 A'$$

possède les invariants

$$n_1^0, n_2^0, \ldots, (\lambda_1 + c_1\lambda_2)^{e_1}, (c_1\lambda_1 + \lambda_2)^{e_1}, \ldots, (\lambda_1 + \lambda_2)^{\overset{+}{e}_\varrho}, \ldots, (\lambda_1 + \lambda_2)^{\overline{e}_\sigma}, \ldots,$$

on dit que la forme possède la *caractéristique*

$$[\{n_1^0\, n_2^0 \ldots\}\ e_1\, e_2 \ldots \overset{+}{e}_\varrho \ldots \overline{e}_\sigma \ldots].$$

On peut aisément former le tableau de tous les *types de réduites* pour des transformations congruentes des deux séries de variables.

H. Rosenow[50]) a montré comment on calcule systématiquement le

50) *H. Rosenow*, Programm der vierten höheren Bürgerschule Berlin 1891

nombre de ces types en fonction de n et indiqué ces types pour $n = 1, 2, 3, 4, 5, 6, 7, 8, 9$ et 10.

Voici le tableau relatif à $n = 1, 2, 3$:

$n = 1)$ $\quad [\overset{+}{1}]\, x_0 y_0;\ \{1\}\ 0$

$n = 2)$ $\quad [11]\, x_0 y_1 + c_1 x_1 y_0;\ [\overset{-}{2}]\, x_0 y_0 + x_1 y_0 - x_0 y_1;\ [\overset{-}{1}\overset{-}{1}]\, x_0 y_1 - x_2 y_0$

$[\overset{+}{1}\overset{+}{1}]\, x_0 y_0 + x_1 y_1;\ [\{1\}\overset{+}{1}]$ et $\{11\}$ identiques aux types $n = 1$.

$n = 3)$ $\quad [\overset{+}{1}11]\, x_0 y_0 + (x_1 y_2 + c_1 x_2 y_1);\ [\overset{+}{1}\overset{-}{2}]\, x_0 y_0 + (x_1 y_1 + x_2 y_1 - x_1 y_2)$

$[\overset{+}{1}\overset{-}{1}\overset{-}{1}]\, x_0 y_0 + x_1 y_2 - x_2 y_1;\ [\overset{+}{1}\overset{+}{1}\overset{+}{1}]\, x_0 y_0 + x_1 y_0 - x_0 y_1 + x_2 y_1 + x_1 y_2$

$[\overset{+}{3}]\, x_0 y_1 + x_1 y_0 - x_0 y_1 + x_2 y_1 + x_1 y_2;\ \{3\}\ x_0 y_1 + x_1 y_2$

Les formes normales des six autres types sont identiques aux types relatifs à $n = 2$.

Pour $n = 4$ on a 16 types nouveaux et les douze types qui sont types relatifs à $n = 3$.*

38. ***Formes symétriques ou alternées congruentes.**

1°) Pour une forme *symétrique* générale A,

$$\lambda_1 \frac{\partial A}{\partial y_i} + \lambda_2 \frac{\partial A'}{\partial y_i} = (\lambda_1 + \lambda_2) \frac{\partial A}{\partial y_i};$$

donc si $|\lambda_1 A + \lambda_2 A'| \equiv 0$ tous les m_i sont nuls et tous les n_i^0 sont l'unité.

Comme $\lambda_1 a_{ik} + \lambda_2 a_{ki} = (\lambda_1 + \lambda_2) a_{ik}$, le déterminant $|\lambda_1 A + \lambda_2 A'|$ ne possède que des diviseurs élémentaires $(\lambda_1 + \lambda_1)$ avec l'exposant *un*, en nombre r si $|A|$ est de rang r.

La caractéristique de la forme symétrique A à $2n$ variables est donc

$$[\{11\ldots\}\overset{+}{1}\overset{+}{1}\ldots\overset{+}{1}]$$

le premier groupe renfermant $(n - r)$ éléments, le second r. *La réduite correspondante est*

$$x_1 y_1 + \cdots + x_r y_r.$$

2°) De même pour une forme alternée dont le déterminant est de rang $r = 2r'$, la caractéristique est

$$[\{11\ldots\}\overset{-}{1}\overset{-}{1}\ldots\overset{-}{1}]$$

où le premier groupe renferme toujours $(n - r)$ éléments. *La réduite correspondante est*

$$x_1 y_2 - x_2 y_1 + x_3 y_4 - x_4 y_3 + \cdots + x_{r-1} y_r - x_r y_{r-1}.$$

Deux *formes symétriques* (*ou alternées*) *de* $2n$ *variables de même rang sont donc toujours congruentes.*

pour $n = 5$; J. reine angew. Math. 108 (1891), p. 15 pour $n = 1, 2, 3, 4$; Programm der vierten höheren Bürgerschule Berlin 1892, p. 8/21 pour $n = 6, 7, 8, 9, 10$.

Deux formes quadratiques A et B dépendant du même nombre de variables peuvent toujours être transformées l'une dans l'autre par une transformation ordinaire si les déterminants $|A|$ et $|B|$ sont de même rang et réciproquement.*

39. Formes semblables. *Deux formes A et B sont *semblables* si l'on a

$$B = T^{-1} A T$$

avec $|T|$ différent de zéro.

On a toujours, en posant

$$E = x_1 y_1 + x_2 y_2 + \cdots + x_n y_n,$$

d'après la définition de T^{-1},

$$E = T^{-1} E T;$$

on en conclut

$$\lambda_1 E + \lambda_2 B = T^{-1}(\lambda_1 E + \lambda_2 A) T,$$

et les faisceaux équivalents

$$\lambda_1 E + \lambda_2 A,\ \lambda_2 E + \lambda_2 B$$

ont alors mêmes diviseurs élémentaires.

Réciproquement si ces faisceaux ont mêmes diviseurs élémentaires ils sont équivalents d'après Weierstrass, c'est-à-dire que

$$\lambda_1 E + \lambda_2 B = S(\lambda_1 E + \lambda_2 A) T;$$

on en conclut, pour $\lambda_2 = 0$,

$$E = SET,$$

c'est-à-dire

$$S = T^{-1}.$$

La condition nécessaire et suffisante pour la similitude des formes A et B est donc l'identité des diviseurs élémentaires de leurs déterminants caractéristiques $|\lambda_1 E + \lambda_2 A|$, $|\lambda_1 E + \lambda_2 B|$.*

40. Types de formes semblables. *On a vu que, si $|A|$ n'est pas nul, le faisceau

$$\lambda A - B = \lambda \sum_{\sigma=1}^{\sigma=m} (X_\sigma Y_\sigma)_{e_\sigma} - \sum_{\sigma=1}^{\sigma=m} \{c_\sigma (X_\sigma Y_\sigma)_{e_\sigma} + (X_\sigma Y_\sigma)_{e_\sigma - 1}\}$$

a pour diviseurs élémentaires

$$(\lambda - c_1)^{e_1},\ (\lambda - c_2)^{e_2},\ \ldots,\ (\lambda - c_m)^{e_m} \quad \text{où} \quad e_1 + e_2 + \cdots + e_m = n.$$

Il suffira de remplacer respectivement les variables

$$X_{10}, X_{11}, \ldots, X_{1,e_1-1};\ X_{20}, X_{21}, \ldots, X_{2,e_2-1};\ \ldots$$

par

$$x_1, x_2, \ldots, x_{e_1};\ x_{e_1+1}, x_{e_1+2}, \ldots, x_{e_1+e_2};\ \ldots$$

et de faire de même avec les Y, pour obtenir

$$\begin{aligned}A &= x_1y_1 + x_2y_2 + \cdots + x_ny_n = E\\ B &= c_1(x_1y_1 + \cdots + x_{e_1}y_{e_1}) + c_2(x_{e_1+1}y_{e_1+1} + \cdots x_{e_1+e_2}y_{e_1+e_2}) + \cdots\\ &\quad + (x_1y_2 + \cdots + x_{e_1-1}y_{e_1}) + (x_{e_1+1}y_{e_1+2} + \cdots + x_{e_1+e_2-1}y_{e_1+e_2}) + \cdots\end{aligned}$$

On reconnaît sur cette forme que les diviseurs élémentaires du déterminant caractéristique de B sont précisément les $(\lambda - c_i)^{e_i}$.

Nous avons donc construit une forme B à $2n$ variables dont la fonction caractéristique $|\lambda E - B|$ possède des diviseurs élémentaires arbitraires.

Si l'on dit qu'une forme bilinéaire, *à variables contragrédientes,* est *irréductible* (ou *élémentaire*) quand elle n'est ni décomposable ni semblable à une forme décomposable, on voit immédiatement que *la condition nécessaire et suffisante pour qu'une forme A (x, y contragrédients) soit irréductible est que $|\lambda E - A|$ ne possède qu'un seul diviseur élémentaire.*

La transformation d'une forme A en la forme type de Weierstrass est ainsi une *réduction à une somme de formes* irréductibles.

Il est possible de classer les formes A à variables contragrédientes d'après la nature des *réduites* qui leur sont semblables: appelons *caractéristique* de la forme A celle du faisceau $(\lambda_1 E + \lambda_2 A)$; nous aurons pour $n = 1, 2, 3$ les *types* suivants:

$$\begin{array}{lll} n=1: & [1] & c_1x_1y_1\\ n=2: \left\{\begin{array}{l}\\ \\ \\ \end{array}\right. & [11] & c_1x_1y_1 + c_2x_2y_2\\ & [(11)] & c_1(x_1y_1 + x_2y_2)\\ & [2] & c_1(x_1y_1 + x_2y_2) + x_1y_2\\ n=3: \left\{\begin{array}{l}\\ \\ \\ \\ \\ \\ \end{array}\right. & [111] & c_1x_1y_1 + c_2x_2y_2 + c_3x_3y_3\\ & [(11)1] & c_1(x_1y_1 + x_2y_2) + c_3x_3y_3\\ & [(111)] & c_1(x_1y_1 + x_2y_2 + x_3y_3)\\ & [21] & c_1(x_1y_1 + x_2y_2) + c_2x_3y_3 + x_1y_2\\ & [(21)] & c_1(x_1y_1 + x_2y_2 + x_3y_3) + x_1y_2\\ & [3] & c_1(x_1y_1 + x_2y_2 + x_3y_3) + x_1y_2 + x_2y_3.\end{array}$$

$n = 4$ donne de même 14 types correspondant à ceux signalés à propos de la réduction des faisceaux ordinaires de formes bilinéaires.*

41. Substitutions linéaires. *A la classification précédente des formes bilinéaires à variables contragrédientes correspond une *classification des substitutions linéaires.*

Soit $\boldsymbol{A}$ la substitution

$$\xi_i = a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{in}x_n \qquad (i = 1, 2, \ldots, n);$$

si l'on exécute sur les x et les ξ les transformations congruentes $\boldsymbol{B}$ à déterminant différent de zéro,

$$\begin{aligned}x_i &= b_{i1}x_1' + b_{i2}x_2' + \cdots + b_{in}x_n',\\ \xi_i &= b_{i1}\xi_1' + b_{i2}\xi_2' + \cdots + b_{in}\xi_n',\\ &(i = 1, 2, \ldots, n),\end{aligned}$$

on obtient une nouvelle substitution $\boldsymbol{C}$

$$\xi_i' = c_{i1}x_1' + c_{i2}x_2' + \cdots + c_{in}x_n' \qquad (i = 1, 2, \ldots, n),$$

qui est dite *équivalente* à $\boldsymbol{A}$.

En posant

$$y_i' = b_{i1}y_1 + b_{i2}y_2 + \cdots + b_{in}y_n \qquad (i = 1, 2, \ldots, n),$$

c'est-à-dire en désignant par $y_1, y_2, \ldots, y_n$ des variables *contragrédientes* des x et des ξ, on aura immédiatement

$$\sum_{i=1}^{i=n}\sum_{k=1}^{k=n} a_{ik}x_ky_i = \sum_{i=1}^{i=n}\xi_iy_i = \sum_{i=1}^{i=n}\xi_i'y_i' = \sum_{i=1}^{i=n}\sum_{k=1}^{k=n} c_{ik}x_k'y_i'.$$

Les deux formes

$$A = \sum_{(i,k)} a_{ik}x_ky_i, \qquad C = \sum_{(i,k)} c_{ik}x_k'y_i' \qquad (i, k = 1, 2, \ldots, n)$$

sont donc semblables. La réciproque est évidente.

Ainsi deux substitutions $\boldsymbol{A}$ et $\boldsymbol{C}$ sont équivalentes (ou semblables) quand les diviseurs élémentaires de leurs déterminants caractéristiques $|\lambda E - A|$ et $|\lambda E - C|$ coïncident, et réciproquement.

Si les diviseurs élémentaires de $|\lambda E - A|$ sont $(\lambda - c_\sigma)^{e_\sigma}$ $(\sigma = 1, \ldots, m)$, on dira que la substitution $\boldsymbol{A}$ a la *caractéristique*

$$[(e_1, \ldots) \ldots (e_\sigma, \ldots)];$$

les *formes normales* se déduisent immédiatement du tableau précédent.

D'une manière générale, la substitution $\boldsymbol{A}$ qui donne pour $|\lambda E - A|$ les diviseurs élémentaires

$$(\lambda - c_\sigma)^{e_\sigma} \qquad (\sigma = 1, 2, \ldots, m)$$

s'écrira[51])

$$\begin{gathered}\xi_1 = c_1x_1,\ \xi_2 = x_1 + c_1x_2, \ldots, \xi_{e_1} = x_{e_1-1} + c_1x_{e_1},\\ \xi_{e_1+1} = c_2x_{e_1+1},\ \xi_{e_1+2} = x_{e_1+1} + c_2x_{e_1+2}, \ldots, \xi_{e_1+e_2} = x_{e_1+e_2-1} + c_2x_{e_1+e_2},\\ \cdots\cdots\cdots\cdots\cdots\cdots,\\ \xi_{n-e_m+1} = c_mx_{n-e_m+1}, \ldots, \xi_n = x_{n-1} + c_mx_n.\end{gathered}$$

La détermination de la *forme normale* d'une substitution linéaire

51) *E. Netto*, Acta math. 17 (1893), p. 45.

remonte aux travaux de *A. L. Cauchy* sur les équations différentielles linéaires à coefficients constants.

C. Jordan[52]) a également obtenu cette forme normale et l'a appliquée dans son Traité des substitutions.

Remarque. Ceci nous amène à remarquer que *C. Jordan* s'est occupé à diverses reprises depuis 1873 de la réduction des formes bilinéaires et quadratiques au moyen de substitutions linéaires générales ou particulières. Quelques-uns de ses travaux ont donné lieu à des observations de *L. Kronecker*. Comme *C. Jordan* a également étudié les transformations linéaires qui n'altèrent pas une forme bilinéaire ou quadratique (transformations *automorphes*) ce n'est qu'après l'étude de ces transformations automorphes faites par la méthode de *G. Frobenius* que nous donnerons un exposé d'ensemble des recherches de ce géomètre.*

Transformations automorphes d'une forme quadratique ou bilinéaire.

42. Transformations automorphes. *Une transformation *automorphe*[53]) de la forme

$$A = \sum a_{ik} x_i y_k$$

est définie par deux substitutions

$$(P) \qquad x_i = \frac{\partial P}{\partial y_i'} = \sum p_{li} x_l',$$

$$(Q) \qquad y_k = \frac{\partial Q}{\partial x_k'} = \sum q_{km} y_m'$$

en vertu desquelles A se transforme identiquement en

$$\sum_{(i,k)} a_{ik} x_i' y_k' \qquad (i, k = 1, 2, \ldots, n).$$

On aura donc entre les coefficients p, q les relations bilinéaires

$$a_{ik} = \sum_{\alpha,\beta} a_{\alpha\beta} p_{i\alpha} q_{\beta k} \qquad (i, k = 1, 2, \ldots, n)$$

qui se transforment, lorsque $x_i = y_i$, c'est-à-dire pour les formes quadratiques, en relations *quadratiques*. La détermination effective des coefficients p, q de la transformation la plus générale a d'abord occupé les géomètres; elle est due essentiellement à *Ch. Hermite* et à *A. Cayley*; l'étude des propriétés caractéristiques des transformations P, Q a été faite ensuite par *L. Kronecker, G. Frobenius* et *A. Voss*. Le fait que

52) Traité des substitutions et des équations algébriques, Paris 1870.

53) *A. Cayley*, Philos. Trans. 148 (1858), p. 39; Papers, 2, Cambridge 1889, p. 497.

les transformations automorphes d'une forme engendrent, au sens de *S. Lie*, un *groupe fini et continu* et la théorie des groupes de transformations n'ont joué aucun rôle dans ces recherches; nous indiquerons, pour terminer, les questions que soulève, à ce point de vue, l'étude des formes quadratiques et bilinéaires et les résultats obtenus.*

I. Détermination des transformations automorphes (Cayley, Hermite).

43. Historique. **A. Cayley*[54]) a donné l'expression rationnelle, au moyen de $\frac{n(n-1)}{2}$ paramètres indépendants, des coefficients de la transformation la plus générale qui change en elle même une somme de n carrés

$$x_1^2 + x_1^2 + \cdots + x_n^2.$$

Soient λ_{rs} les éléments d'un *déterminant gauche*, c'est-à-dire des quantités quelconques satisfaisant aux relations

$$\lambda_{rs} + \lambda_{sr} = 0,$$

quand r et s sont inégaux et aux relations

$$\lambda_{rr} = 1 \qquad (r = 1, 2, \ldots, n).$$

Si l'on pose

$$\sum_{r=1}^{r=n} \lambda_{rs} x_r = P_s, \qquad \sum_{s=1}^{s=n} \lambda_{rs} x_s = Q_r$$

et si l'on désigne par K le déterminant

$$|\lambda_{rs}| \qquad (r, s = 1, 2, \ldots, n),$$

en sorte que

$$K x_r = \sum_{s=1}^{s=n} A_{rs} P_s, \qquad K x_s = \sum_{r=1}^{r=n} A_{rs} Q_r,$$

il suffit de poser

$$K\alpha_{rs} = 2A_{rs} \qquad (r, s = 1, 2, \ldots, n)$$

pour r et s inégaux et

$$K\alpha_{rr} = 2A_{rr} - K \qquad (r = 1, 2, \ldots, n)$$

pour obtenir les deux systèmes équivalents

$$Q_r = \sum_{s=1}^{s=n} \alpha_{rs} P_s, \qquad P_s = \sum_{r=1}^{r=n} \alpha_{rs} Q_r$$

d'où l'on déduit

$$\sum_{r=1}^{r=n} \alpha_{rs} \alpha_{rs'} = 0 \qquad (s, s' = 1, 2, \ldots, n),$$

54) J. reine angew. Math. 32 (1846), p. 119, Papers 1, Cambridge 1889, p. 332.

pour s et s' inégaux, et

$$\sum_{r=1}^{r=a} \alpha_{rs}\alpha_{rs} = 1 \qquad (s = 1, 2, \ldots, n),$$

c'est-à-dire les conditions que doivent remplir les coefficients d'une transformation orthogonale. Ces coefficients sont donc des fonctions rationnelles des λ_{rs} qui sont arbitraires; il y en a $\frac{n(n-1)}{2}$.

Si $n = 3$ on retrouve des formules données par *O. Rodrigues*[55]) pour le changement de coordonnées rectangulaires. Ces formules sont déjà dans *L. Euler*[56]).

Ch. Hermite[57]), dans un mémoire sur la théorie des formes ternaires indéfinies, a déterminé toutes les transformations linéaires qui conservent une forme quadratique ternaire.

Si l'on a

$$f(X, Y, Z) = f(x, y, z),$$

en posant

$$x + X = 2\xi, \qquad y + Y = 2\eta, \qquad z + Z = 2\zeta$$

on en déduira

$$2f(\xi, \eta, \zeta) = X\frac{\partial f}{\partial \xi} + Y\frac{\partial f}{\partial \eta} + Z\frac{\partial f}{\partial \zeta},$$

d'où l'on conclut

$$(1) \qquad X = \xi + \nu\frac{\partial f}{\partial \eta} - \mu\frac{\partial f}{\partial \xi}$$
$$\cdots\cdots\cdots$$

où interviennent les trois paramètres λ, μ, ν, et aussi

$$x = 2\xi - X, \qquad y = 2\eta - Y, \qquad z = 2\zeta - Z.$$

Si l'on désigne par $F(\lambda, \mu, \nu)$ la forme adjointe à $f(\lambda, \mu, \nu)$ on a entre les x et les X les relations explicites

$$x(1 + F(\lambda, \mu, \nu)) = X(1 - F(\lambda, \mu, \nu)) + 2(\nu f_Y' - \mu f_Z') + \varpi F_\lambda'$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

où ϖ désigne l'expression $\lambda X + \mu Y + \nu Z$, qui satisfait à l'identité

$$\lambda x + \mu y + \nu z = \lambda X + \mu Y + \nu Z.$$

Ch. Hermite[58]) a montré[59]) que les formules précédentes (1)

55) J. math. pures appl. (1) 5 (1840), p. 380, 409.

56) Novi Comm. Acad. Petrop. 15 (1770), éd. 1771, p. 75/106; Commentat. Arith. 1, St Pétersbourg 1849, p. 427/43.

57) J. reine angew. Math. 47 (1854), p. 307; Œinvres[5]) 1, p. 193.

58) J. reine angew. Math. 78 (1874), p. 325.

59) C'est à la suite d'un article de *P. Bachmann* [J. reine angew. Math. 76 (1873), p. 331] que *Ch. Hermite* a été amené à établir ce résultat.

donnent bien toutes les transformations d'une forme ternaire en elle-même. Il est parfois nécessaire d'y faire croître indéfiniment certains des paramètres λ, μ, ν.

J. Tannery[60]) a démontré de façon élémentaire les résultats simplement énoncés par *Ch. Hermite* et a donné des formules simples pour la composition des transformations précédentes.

Ch. Hermite[61]) a depuis étendu sa méthode à une forme quadratique générale à n variables. Si l'on veut avoir

$$f(x_1, x_2, \ldots, x_n) = f(X_1, X_2, \ldots, X_n)$$

il suffit de poser

$$x_r = \xi_r + \frac{1}{2}\sum_{s=1}^{s=n} \lambda_{r,s}\frac{\partial f(\xi_1, \ldots, \xi_n)}{\partial \xi_s},$$

avec $X_r = 2\xi_r - x_r$, les λ_{rs} étant assujettis aux conditions

$$\lambda_{rs} + \lambda_{sr} = 0.$$

Il convient de signaler encore le théorème suivant dont Hermite a fait ultérieurement usage: si l'on désigne par S une transformation de la forme f en elle-même, on peut toujours ramener f à une somme de carrés

$$A^2 + B^2 + C^2 + \cdots$$

choisis de telle sorte qu'en désignant par $\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C}, \ldots$ leurs transformés par S (qui en sont des fonctions linéaires) l'expression

$$A\boldsymbol{A} + B\boldsymbol{B} + C\boldsymbol{C} + \cdots$$

ne renferme aucun rectangle

$$AB, \; AC, \; BC, \ldots$$

A. Cayley[62]) a donné au moyen de sa théorie des matrices une nouvelle expression du résultat de *Ch. Hermite*:

Si l'on désigne par A la matrice des a_{ik}, coefficients de la forme $f(x_1, \ldots, x_n)$, et par X une matrice *symétrique gauche* arbitraire, les transformations S qui conservent f sont représentées par

$$S = A^{-1}(A - X)(A + X)^{-1}A.$$

Les transformations ainsi représentées ont toutes un déterminant égal à $+1$ (transformations *propres*); *A. Cayley* a montré également comment on obtient les transformations *impropres* en introduisant une variable de plus dont on annule les coefficients.

60) Bull. sc. math. (1) 11 (1876), p. 221.

61) Cambr. Dublin math. J. 9 (1854), p. 63; Œuvres[5]) 1, p. 296.

62) J. reine angew. Math. 50 (1855), p. 288, 299; Papers 2, Cambridge 1889, p. 192, 202.

Plus tard *A. Cayley*[63]) a étendu ce résultat à des formes bilinéaires

$$F(x_1, x_2, \ldots, x_n;\ y_1, y_2, \ldots, y_n | a_{ik})$$

pour des substitutions *indépendantes* des deux séries de variables (x) et (y) et caractérisé le rôle des formes symétriques $(a_{ik} = a_{ki})$ ou alternées $(a_{ik} = -a_{ki})$.

Soit A la matrice formée par les coefficients a_{ik} de la forme

$$\sum_{(i,k)} a_{ik} x_i y_k \qquad (i, k = 1, 2, \ldots, n),$$

où i désigne le rang des colonnes et k celui des lignes. Si l'on veut que les deux substitutions

$$(P) \qquad x_i = \sum_{l=1}^{l=n} p_{il} \xi_l$$

et

$$(Q) \qquad y_k = \sum_{m=1}^{m=n} q_{km} \eta_m$$

donnent lieu à l'identité

$$\sum_{(i,k)} a_{ik} x_i y_k = \sum_{(i,k)} a_{ik} \xi_i \eta_k \qquad (i, k = 1, 2, \ldots, n)$$

il faut et il suffit que les matrices A, P, Q satisfassent à la relation

$$Q' A P = A,$$

où Q' désigne la *conjuguée* de Q, déduite de Q par échange des lignes et des colonnes (*A. Cayley* nomme Q' la *transverse* de Q). On peut se donner arbitrairement P ou Q et calculer l'autre par les formules

$$Q' = A P^{-1} A^{-1} \quad \text{ou} \quad P = A^{-1} Q'^{-1} A.$$

En prenant pour M une matrice arbitraire, *à déterminant non nul,* on peut donner de P et de Q' les expressions équivalentes suivantes:

$$\begin{array}{ll} P = 2(A+M)^{-1}A - 1 & Q' = 2A(A-M)^{-1} - 1 \\ P = 1 - 2(A+M)^{-1}M & Q' = 1 + 2M(A-M)^{-1} \\ P = (A+M)^{-1}(A-M) & Q' = (A+M)(A-M)^{-1} \\ P = (2(A-M)^{-1}A - 1)^{-1} & Q' = (2A(A+M)^{-1} - 1)^{-1}. \end{array}$$

L'avantage de ces formes d'apparence compliquée est de se prêter facilement à la particularisation. Par exemple, si A est symétrique et $P = Q$, on déduit de la première expression

$$M = -M',$$

63) Philos. Trans. London 148 (1858), p. 39; Papers 2, Cambridge 1889, p. 497; plus simplement chez *T. Muir*, Amer. J. math. 20 (1898), p. 215.

c'est-à-dire que M est symétrique gauche, les éléments diagonaux étant nuls.

La transformation des fonctions Thêta conduit à réduire une forme bilinéaire à une certaine somme de produits (forme normale). Si le déterminant $|a_{ik}|$ n'est pas nul, *L. Kronecker*[64]) montre au moyen des formes *associées* (beigeordnete) que la résolution d'une certaine équation d'ordre n suffit pour faire cette réduction; il détermine par cela même les transformations automorphes d'une forme bilinéaire pour des substitutions identiques (*congrues*) des deux séries de variables.

E. B. Christoffel[65]) confirme ces résultats par la méthode symbolique de *S. H. Aronhold* et montre que le nombre des paramètres dont dépend la transformation automorphe S est celui des invariants absolus de la forme.

Il convient de rappeler que *E. N. Laguerre*[66]), dans un mémoire sur le calcul des systèmes linéaires, a appliqué la théorie de ces systèmes (c'est-à-dire celle des *matrices*) à la détermination des transformations automorphes d'une forme quadratique à un nombre quelconque de variables.*

II. Transformations générales des formes bilinéaires quelconques (Frobenius, Kronecker).

44. Forme ordinaire. *Supposons la forme bilinéaire

$$A = \sum_{(i,k)} a_{ik} x_i y_k, \qquad (i, k = 1, 2, \ldots, n),$$

où $|A|$ est différent de zéro, transformée en elle-même par les deux substitutions P et Q, à déterminant non nul

$$A = PAQ.$$

Si U et V sont deux formes ordinaires quelconques, l'identité

$$(UPU^{-1})(UAV)(V^{-1}QV) = UAV$$

prouve que la forme UAV se conserve par les deux transformations UPU^{-1}, $V^{-1}QV$. En supposant, par exemple,

$$UPU^{-1} = P \quad \text{et} \quad V = E$$

on voit que toutes les formes UA admettent la transformation P.

64) Monatsb. Akad. Berlin 1866, p. 597; J. reine angew. Math. 68 (1868), p. 273; Werke 1, Leipzig 1895, p. 143.

65) J. reine angew. Math. 68 (1868), p. 253; cf. *A. Clebsch* et *P. Gordan*, Theorie der Abel'schen Functionen, Leipzig 1866, p. 44/7; les invariants absolus d'une forme bilinéaire $F_{11}(x|u)$ paraissent déjà dans *C. W. Borchardt*, J. reine angew. Math. 30 (1846), p. 38; Werke, Berlin 1888, p. 3.

66) J. Éc. polyt. (1) cah. 42 (1867), p. 237; Œuvres 1, Paris 1898, p. 241.

Considérons d'autre part la forme *unitaire*

$$E = x_1 y_1 + x_2 y_2 + \cdots + x_n y_n;$$

on a

$$(\lambda_1 E + \lambda_2 P) A Q = \lambda_1 A Q + \lambda_2 P A Q = A(\lambda_1 Q + \lambda_2 E),$$

d'où l'on conclut, si le déterminant $|A|$ est différent de zéro,

$$\lambda_1 Q + \lambda_2 E = A^{-1}(\lambda_1 E + \lambda_2 P) A Q,$$

c'est-à-dire que *les faisceaux $\lambda_1 E + \lambda_2 P$ et $\lambda_1 Q + \lambda_2 E$ sont équivalents.*

Inversement, si ces deux faisceaux sont équivalents, c'est-à-dire s'il existe une identité

$$\lambda_1 E + \lambda_2 P = A(\lambda_1 Q + \lambda_2 E) B$$

où le produit $|A||B|$ est différent de zéro et où A et B ne dépendent pas de $\frac{\lambda_1}{\lambda_2}$, on en déduira

$$E = AQB, \qquad P = AEB = AB,$$

d'où

$$(PAQ)B = P(AQB) = P = AB$$

c'est-à-dire

$$PAQ = A.$$

La *condition précédente est donc suffisante pour qu'il existe une forme A conservée par P et Q.*

Si $|\lambda E - P|$ décomposé en ses diviseurs élémentaires donne

$$|\lambda E - P| = (\lambda - c_1)^{e_1} (\lambda - c_2)^{e_2} \dots (\lambda - c_m)^{e_m},$$

on aura

$$|\lambda Q - E| = |Q| (\lambda - c_1)^{e_1} (\lambda - c_2)^{e_2} \dots (\lambda - c_m)^{e_m},$$

d'où l'on conclut

$$|Q| c_1^{e_1} c_2^{e_2} \dots c_m^{e_m} = 1$$

et

$$|\lambda E - Q| = \left(\lambda - \frac{1}{c_1}\right)^{e_1} \left(\lambda - \frac{1}{c_2}\right)^{e_2} \cdots \left(\lambda - \frac{1}{c_m}\right)^{e_m}.$$

La condition nécessaire et suffisante d'une identité

$$A = PAQ,$$

où A est à déterminer, est qu'à tout diviseur élémentaire $(\lambda - c)^e$, de la fonction caractéristique $|\lambda E - P|$, corresponde un diviseur élémentaire $\left(\lambda - \frac{1}{c}\right)^e$ de la fonction caractéristique $|\lambda E - Q|$ et réciproquement[67]).*

45. Forme singulière. *Supposons toujours

$$A = PAQ,$$

mais cette fois $|A| = 0$ et de rang r.

67) *G. Frobenius*, J. reine angew. Math. 84 (1878), p. 31.

Posons

$$E_1 = x_1 y_1 + x_2 y_2 + \cdots + x_r y_r,$$

$$E_2 = x_{r+1} y_{r+1} + x_{r+2} y_{r+2} + \cdots + x_n y_n,$$

ce qui donne

$$E = E_1 + E_1,$$

$$E_1^2 = E_1, \qquad E_2^2 = E_2, \qquad E_1 E_2 = E_2 E_1 = 0.$$

La forme A peut se transformer en une forme *A ordinaire à $2r$ variables* qu'on peut par suite ramener à la forme E_1.

L'identité correspondante

$$E_1 = UAV$$

donne

$$P_0 E_1 Q_0 = E_1$$

en posant

$$P_0 = UPU^{-1}, \qquad Q_0 = VQV^{-1}.$$

On déduit de là, en multipliant par E_1 ou E_2 et tenant compte de

$$E_i^2 = E_i, \qquad E_1 E_2 = E_2 E_1 = 0,$$

$$(E_1 P_0 E_1)(E_1 Q_0 E_1) = E_1,$$

$$(E_\varrho P_0 E_1)(E_1 Q_0 E_\sigma) = 0, \qquad [(\varrho, \sigma) = (1, 2), (2, 1,) (2, 2)].$$

Si l'on pose

$$P_{\varrho\sigma} = E_\varrho P_0 E_\sigma, \qquad Q_{\varrho\sigma} = E_\varrho Q_0 E_\sigma,$$

P_{11} sera la partie de P_0 qui renferme les variables

$$x_1, x_2, \dots, x_r, \ y_1, y_2, \dots, y_r,$$

P_{12} celle qui renferme les variables

$$x_1, x_2, \dots, x_r, \ y_{r+1}, y_{r+2}, \dots, y_n,$$

P_{21} celle qui renferme les variables

$$x_{r+1}, x_{r+2}, \dots, x_n, \ y_1, y_2, \dots, y_r.$$

Les deux égalités précédentes donneront

$$|P_{11} Q_{11}| = |P_{11}||Q_{11}| = 1$$

et en particulier

$$P_{11} Q_{12} = P_{21} Q_{11} = 0.$$

Eu égard à ce que $|P_{11}|$ et $|Q_{11}|$ ne sont pas nuls, on en conclut que *Q_{12} et Q_{21} sont identiquement nuls.*

On aura donc

$$|\lambda E - P| = |\lambda E_1 - P_{11}||\lambda E_2 - P_{22}|,$$

$$|\lambda E - Q| = |\lambda E_1 - Q_{11}||\lambda E_2 - Q_{21}|.$$

D'autre part la relation $P_{11} Q_{11} = E_1$ (qui s'écrit aussi $Q_{11} = P_{11}^{-1}$)

montre que, si $c_1, c_2, \ldots, c_r$ sont les racines de l'équation

$$|\lambda E_1 - P_{11}| = 0,$$

celles de l'équation $|\lambda E_1 - Q_{11}| = 0$ sont $c_1^{-1}, c_2^{-1}, \ldots, c_r^{-1}$.

Si $|A|$ est de rang r et si l'on a

$$A = PAQ,$$

l'équation caractéristique de P possède au moins r racines dont les inverses sont racines de l'équation caractéristique de Q.

Il en résulte que si l'équation caractéristique de P possède exactement r racines dont les inverses satisfont à l'équation caractéristique de Q, le rang de la forme A qui satisfait à

$$A = PAQ$$

ne peut dépasser r. Ce rang est donc nul (ainsi que la forme) quand les inverses des racines de $|\lambda E - P| = 0$ ne sont pas racines de

$$|\lambda E - Q| = 0.$$

Supposons que l'on connaisse une forme A donnant lieu à l'identité

$$A = PAQ;$$

si l'on désigne par SA une autre forme quelconque telle que

$$SA = PSAQ,$$

on en déduira, en remplaçant au premier membre A par PAQ

$$SPAQ = PSAQ$$

d'où

$$SP = PS.$$

La réciproque est évidente. *Toutes les formes transformées en elles-mêmes par P et Q s'obtiennent donc sous la forme SA*, où A désigne *l'une d'elles et où*

$$SP = PS.$$

G. Frobenius[68]) a étudié la détermination de S et fixé le nombre des formes S linéairement distinctes (parmi lesquelles figure toujours E) et qu'on peut supposer *ordinaires*. On observe que *la détermination de S est indépendante de Q*.*

46. Remarques sur les transformations congruentes des formes quelconques. *Supposons qu'en transformant de même les deux séries de variables x, y, la forme A se conserve; on aura

$$A = P'AP.$$

---

68) J. reine angew. Math. 84 (1878), p. 29; *L. Maurer,* Diss. Strasbourg 1887; *A. Voss*, Sitzgsb. Akad. München 19 (1889), p. 329.

Si G désigne une forme *ordinaire* quelconque, l'identité

$$(G'P'G'^{-1})(G'AG)(G^{-1}PG) = G'AG$$

exprime que *la substitution GPG^{-1} semblable à P conserve la forme $G'AG$.*

Si le déterminant $|A|$ est différent de zéro, le déterminant $|G'AG|$ est aussi différent de zéro; si A est symétrique ou alternée, il en est de même de $G'AG$.

On aura évidemment

$$(\lambda_1 E + \lambda_2 P')AP = A(\lambda_1 P + \lambda_2 E);$$

les deux faisceaux $\lambda_1 E + \lambda_2 P'$ et $\lambda_1 P + \lambda_2 E$ sont donc équivalents; comme $\lambda_1 E + \lambda_2 P'$ est équivalent à $\lambda_1 E + \lambda_2 P$ (il suffit de permuter x_i et y_i pour passer de l'un à l'autre), il en résulte que $\lambda_1 E + \lambda_2 P$ *et $\lambda_1 P + \lambda_2 E$ sont équivalents.*

Les racines de l'équation caractéristique $|\lambda E - P| = 0$ sont donc deux à deux réciproques à l'exception de celles qui sont égales à ± 1 et les diviseurs élémentaires correspondants ont les mêmes exposants[69]).

Si l'on pose

$$|P| = \varepsilon$$

on aura $\varepsilon^2 = 1$; la substitution P est *propre* si $\varepsilon = +1$, *impropre* si $\varepsilon = -1$.

Il convient d'observer ici qu'en posant

$$P = A^{-1}A',$$

ce qui donne

$$P' = AA'^{-1},$$

on aura

$$P'AP = AA'^{-1} \cdot A \cdot A^{-1}A' = A.$$

La substitution antisymétrique $A^{-1}A'$ conserve toujours la forme ordinaire A.

Supposons maintenant $|A| = 0$ et de rang r. Il suffit de se reporter au cas général relatif aux transformations pour lesquelles

$$A = PAQ \quad \text{et de faire} \quad Q = P'$$

pour reconnaître que le premier membre de l'*équation caractéristique $|\lambda E - P| = 0$ est divisible par un polynome réciproque en λ de degré r.*

Inversement si les deux faisceaux $\lambda_1 E + \lambda_2 P$ et $\lambda_1 P + \lambda_2 E$ sont équivalents, c'est-à-dire si

$$A(\lambda_1 E + \lambda_2 P)B = \lambda_1 P + \lambda_2 E,$$

---

69) *L. Kronecker*, J. reine angew. Math. 68 (1868), p. 273; Werke 1, Leipzig 1895, p. 143; *E. B. Christoffel*, J. reine angew. Math. 68 (1868), p. 253. Pour le cas des formes orthogonales cf. *F. Brioschi*, Ann. sc. mat. fis. 5 (1854), p. 201; *L. Schläfli*, J. reine angew. Math. 65 (1866), p. 185.

ce qui donne

$$AB = P, \qquad APB = E,$$

en observant qu'il existe toujours une forme C pour laquelle

$$CPC^{-1} = P',$$

on en déduira

$$CABC^{-1} = P'$$

ou encore

$$A = C^{-1}P'CB^{-1} = B^{-1}P^{-1}$$

et enfin

$$P'CB^{-1}P = CB^{-1}.$$

Ainsi CB^{-1} *est une forme ordinaire transformée en elle-même par* P. Toutes les formes analogues S s'en déduiront par la formule

$$S = QCB^{-1}$$

pourvu que l'on ait

$$QP' = P'Q.$$

Leur détermination revient donc à celle des *formes permutables avec* P'.*

47. Formes et substitutions décomposables. *Soit toujours

$$A = P'AP;$$

supposons P *décomposable en deux parties,* P_1 dépendant des variables x_μ, y_μ $(\mu = 1, 2, \ldots, m)$, P_2 des variables x_ν, y_ν $(\nu = m+1, \ldots, n)$.

En posant

$$E_1 = x_1y_1 + x_2y_2 + \cdots + x_my_m,$$
$$E_2 = x_{m+1}y_{m+1} + \cdots + x_ny_n,$$

on aura

$$P_\varrho = E_\varrho P = PE_\varrho = E_\varrho PE_\varrho = E_\varrho P_\varrho = P_\varrho E_\varrho \qquad (\varrho = 1, 2).$$

D'autre part P' est décomposable comme P, donc

$$E_\varrho AE_\sigma = E_\varrho P'APE_\sigma = (E_\varrho P')A(PE_\sigma) = (P'_\varrho E_\varrho)A(P_\sigma E_\sigma);$$

d'où, si l'on pose

$$E_\varrho AE_\sigma = A_{\varrho\sigma},$$

l'égalité

$$A_{\varrho\sigma} = P_\varrho' A_{\varrho\sigma} P_\sigma \qquad (\varrho, \sigma = 1, 2).$$

Faisons maintenant l'hypothèse qu'*aucune racine de l'équation caractéristique de* P_1 *ne soit réciproque d'une racine de l'équation caractéristique de* P. Puisque l'équation caractéristique de P_ϱ' est la même que celle de P_ϱ, aucune racine de l'équation relative à P_ϱ' n'est réciproque d'une racine de l'équation relative à P_σ, lorsque σ est différent de ϱ; on a donc nécessairement

$$A_{12} = 0, \qquad A_{21} = 0,$$

d'où l'on conclut

$$A = A_{11} + A_{22}.$$

Si la substitution décomposable P *transforme en elle-même la forme* A *et si les équations caractéristiques de* P_1 *et* P_2 *n'ont pas de racines réciproques, la forme* A *est décomposable de même que* P.

La réciproque est vraie: si la forme ordinaire A est décomposable en deux formes A_1 et A_2 et si les déterminants

$$|A_1 + \lambda A'_1|, \qquad |A_2 + \lambda A'_2|$$

sont sans diviseur commun, toute substitution P qui conserve A est décomposable de même.*

III. Formes symétriques ou alternées.

48. Substitutions d'Hermite. **A. Cayley*[70]) avait remarqué que l'équation caractéristique (envisagée par *A. L. Cauchy*) de la substitution qui transforme en elle-même une forme quadratique (substitution d'Hermite) est réciproque.

En cherchant à caractériser ces substitutions d'Hermite, indépendamment de la forme quadratique, *J. Rosanes*[71]) démontre la réciproque: à toute équation réciproque on peut faire correspondre une substitution S de type *antisymétrique* $(A^{-1}A')$, dont les coefficients s_{ik} s'obtiennent par la résolution des équations

$$\sum_{i=1}^{i=n} a_{ik}x_i' = \varepsilon \sum_{k=1}^{k=n} a_{ki}x_k \qquad (\text{où } \varepsilon^2 = 1),$$

c'est-à-dire sont exprimés au moyen des paramètres *surabondants* a_{ik}; cette substitution transforme en elle-même une forme quadratique

$$A = \sum_{(i,k)} a_{ik}x_ix_k, \quad \text{où} \quad a_{ik} = a_{ki} \qquad (i, k = 1, 2, \ldots, n),$$

ou la forme bilinéaire A dans le cas général (transformations congruentes).

L'algorithme employé par *G. Frobenius*[72]), à la suite de *A. Cayley*, *J. J. Sylvester* et *E. N. Laguerre*, lui a permis de caractériser les transformations automorphes des formes bilinéaires symétriques ou alternées même exceptionnelles. Il a obtenu, pour les représenter, des formules analogues à celles de *Ch. Hermite* et de *A. Cayley*, qu'un passage à la limite a permis d'appliquer à tous les cas singuliers.

70) Philos. Trans. London 148 (1858), p. 39; Papers 2, Cambridge 1889, p. 497.
71) J. reine angew Math. 80 (1875), p. 52.
72) J. reine angew. Math. 84 (1878), p. 1.

Toute substitution U qui transforme en elle-même une forme symétrique ordinaire S, et pour laquelle le déterminant $|E+U|$ est différent de zéro, *peut être mise d'une seule manière sous la forme*

$$U=(S+T)^{-1}(S-T),$$

où

$$T=S\frac{E-U}{E+U}$$

est une forme alternée[73]).

Soient S et T deux formes *quelconques* et $|S+T|$ différent de zéro; si l'on a

$$U=(S+T)^{-1}(S-T)$$

on en déduit

$$(S+T)(E+U)=S+T+(S+T)U=S+T+S-T=2S$$

et de même

$$(S+T)(E-U)=2T,$$

d'où, si $|S|$ est différent de zéro

$$(S+T)U=S-T,$$
$$T(E+U)=S(E-U)$$

et enfin

$$T=S\frac{E-U}{E+U}$$

(car $E+U$, $E-U$ sont permutables).

Soit maintenant, S désignant une forme symétrique ordinaire,

$$S=U'SU$$

avec $|E+U|$ différent de zéro.

Considérons la forme

$$T_0=(E+U')T(E+U)$$

congrue à T; on a d'après la définition de T

$$T_0=(E+U')S(E-U)=U'S-SU,$$

d'où l'on conclut

$$T_0'=-T_0;$$

par suite la forme T congrue à T_0 est aussi alternée.

Ce théorème s'applique également, *mutatis mutandis,* aux formes alternées:

Toute substitution U qui transforme en elle-même une forme alternée ordinaire T et pour laquelle le déterminant $|E-U|$ est différent de zéro peut être mise d'une seule manière sous la forme

$$U=(S+T)^{-1}(S-T),$$

73) Ce théorème est dû à *Ch. Hermite*, J. reine angew. Math. 47 (1854), p. 309; Œuvres[5]) 1, p. 195.

où

$$S=T\frac{E+U}{E-U}$$

est une forme symétrique[74]).

La démonstration est la même.*

49. Caractères des substitutions qui conservent une forme symétrique (ou alternée) ordinaire. Lorsque la substitution P satisfait aux conditions pour que

$$A=P'AP,$$

A désignant une forme quelconque, on a aussi

$$A'=P'A'P$$

et par conséquent

$$(A+A')=P'(A+A')P,\qquad (A-A')=P'(A-A')P,$$

c'est-à-dire que *P transforme toujours en elle-même une forme symétrique et une forme alternée.*

Mais il peut se faire que l'un des déterminants $|A+A'|$, $|A-A'|$ (ou tous deux) s'annule. A quel caractère[75]) reconnaîtra-t-on, par exemple, que pour la forme symétrique le déterminant $|A+A'|$ n'est pas nul?

1°) Supposons *d'abord que le déterminant caractéristique*

$$|\lambda E-P|$$

de P ne s'annule que pour l'une des deux racines ε de $\varepsilon^2=1$, par ex. que $|\varepsilon E+P|$ soit différent de zéro.

Si P transforme en elle-même la forme symétrique ordinaire S, il en sera de même de $U=\varepsilon P$.

Comme, d'après l'hypothèse, $|E+U|$ n'est pas nul, on peut écrire

$$U=(S+T)^{-1}(S-T),$$

où T est une forme alternée; on aura alors en posant

$$S+T=B,$$

ce qui donne

$$S-T=B',$$
$$\varepsilon P=B^{-1}B'$$

et ensuite

$$B(\lambda E-P)=\lambda B-\varepsilon B'.$$

Mais nous savons que $|\lambda B-\varepsilon B'|$ a, en particulier, tous ses diviseurs élémentaires $(\lambda-\varepsilon)^{2\varkappa}$ doubles; il en résulte donc que *les diviseurs élémentaires $(\lambda-\varepsilon)^{2\varkappa}$ de la fonction caractéristique de P, $|\lambda E-P|$, sont toujours doubles.*

74) *L. Kronecker*, J. reine angew. Math. 68 (1868), p. 282; Werke 1, Leipzig 1895, p. 158.

75) *G. Frobenius*, J. reine angew. Math. 84 (1878), p. 39.

2°) Soit maintenant P une substitution *quelconque* pour laquelle

$$S = P'SP,$$

où le déterminant $|S|$ est différent de zéro.

La fonction caractéristique de P peut s'écrire

$$|\lambda E - P| = \varphi(\lambda) = \varphi_1(\lambda)\varphi_2(\lambda),$$

où $\varphi_2(\varepsilon)$ est différent de zéro; $\varphi_1(\lambda)$ représente ici le produit des facteurs $(\lambda - \varepsilon)$ où $\varepsilon^2 = 1$. On a donc $\varphi_2(-\varepsilon)$ différent de 0, mais $\varphi_1(-\varepsilon)$ peut s'annuler. Désignons par m le degré de $\varphi_1(\lambda)$; soit P_1 une forme des $2m$ variables

$$x_1, y_1, x_2, y_2, \ldots, x_m, y_m$$

telle qu'en posant

$$E_1 = x_1 y_1 + x_2 y_2 + \cdots + x_m y_m$$

la fonction caractéristique de P_1 décomposée en ses diviseurs élémentaires soit précisément $\varphi_1(\lambda)$

$$|\lambda E_1 - P_1| = \varphi_1(\lambda);$$

soit de même P_2 une fonction des variables restantes telle que l'on ait

$$|\lambda E_2 - P_2| = \varphi_2(\lambda).$$

Il est clair que l'on aura, avec $P_0 = P_1 + P_2$,

$$|\lambda E - P_0| = \varphi_1(\lambda)\varphi_2(\lambda) = |\lambda E - P|;$$

d'où l'on conclut que P_0 et P sont semblables.

Il existe donc une forme S_0 congrue à S, c'est-à-dire symétrique transformée en elle-même par P_0. Mais P_0 est décomposable en deux parties P_1, P_2 telles que la fonction caractéristique de P_1 s'annule pour $\lambda = \varepsilon$ valeur à laquelle ne correspond aucune racine réciproque de la fonction caractéristique de P_2.

Il en résulte que S_0 *est décomposable comme* P_0; si l'on pose

$$S_0 = S_1 + S_2,$$

en désignant par S_1, S_2 les parties correspondantes à P_1, P_2, ces parties sont symétriques et ordinaires; on a

$$|S_1| \cdot |S_2| = |S_0|$$

en sorte que $|S_1|$ et $|S_2|$ sont différents de zéro; S_1, S_2 satisfont aux conditions

$$\begin{aligned} P_0' S_0 P_0 &= (P_1' + P_2')(S_1 + S_2)(P_1 + P_2) = P_1' S_1 P_1 + P_2' S_2 P_2 \\ &= S_0 = S_1 + S_2; \end{aligned}$$

d'où l'on conclut, puisque S_1 et S_2 n'ont pas de variables communes,

$$P_1' S_1 P_1 = S_1, \qquad P_2' S_2 P_2 = S_2.$$

La fonction symétrique ordinaire S_1 est conservée par la trans-

formation P_1 pour laquelle $|\lambda E_1 - P_1|$ ne s'annule que pour $\lambda = \varepsilon$ ($\varepsilon^2 = 1$); les diviseurs élémentaires de ce déterminant qui sont de la forme $(\lambda - \varepsilon)^{2\varkappa}$ sont donc doubles. Ainsi *les diviseurs élémentaires de* $|\lambda E - P|$ *qui sont de la forme* $(\lambda - 1)^{2\varkappa}$ *ou* $(\lambda + 1)^{2\varkappa}$ *figurent tous deux fois dans la suite des diviseurs élémentaires.*

On démontre de même pour une forme *alternée* T que *si*

$$T = P'TP \qquad |T| \neq 0$$

le déterminant caractéristique $|\lambda E - P|$ *de* P *possède deux fois chaque diviseur élémentaire* $(\lambda - \varepsilon)^{2\varkappa+1}$ *pour lequel* $\varepsilon^2 = 1$.*

50. Propositions réciproques. *Ces conditions sont suffisantes pour caractériser les transformations P qui conservent une forme symétrique ordinaire S ou une forme alternée ordinaire T.

En d'autres termes: *Pour qu'une transformation* P *conserve une forme ordinaire symetrique* (*ou alternée*) *il est nécessaire et suffisant que les diviseurs élémentaires de la fonction caractéristique*

$$|\lambda E - P| = 0$$

soient deux à deux des formes $(\lambda - c)^e$, $\left(\lambda - \frac{1}{c}\right)^e$ *sauf ceux de la forme* $(\lambda - \varepsilon)^{2\varkappa+1}$ [ou $(\lambda - \varepsilon)^{2\varkappa}$] avec $\varepsilon = \pm 1$[76]).

Considérons le cas des formes symétriques.

Supposons $|\lambda E - P| = \varphi(\lambda) = \varphi_1(\lambda)\varphi_2(\lambda)$, où $\varphi_1(\lambda)$ désigne le produit des diviseurs élémentaires s'annulant pour $\lambda = -1$; soit m le degré de $\varphi(\lambda)$. Il existera une forme $\lambda A_1 + A_1'$ des variables $x_1, y_1, \ldots, x_m, y_m$ pour laquelle les diviseurs élémentaires de $|\lambda A_1 + A_1'|$ seront ceux de $\varphi_1(\lambda)$ et une forme $\lambda A_2 - A_2'$ des variables x_{m+1}, $y_{m+1}, \ldots, x_n, y_n$ telle que la décomposition de $|\lambda A_2 - A_2'|$ en diviseurs élémentaires donne $\varphi_2(\lambda)$.

Car si l'on pose $\lambda_2^{n-m}\varphi_2\left(-\frac{\lambda_1}{\lambda_2}\right) = \Phi(\lambda_1, \lambda_2)$ les facteurs de Φ sont deux par deux des formes $(\lambda_1 - c\lambda_2)^e \left(\lambda_1 - \frac{1}{c}\lambda_2\right)^e$ (où c peut être $+1$), les seuls facteurs $(\lambda_1 + \lambda_2)^{2\varkappa+1}$ peuvent être en nombre quelconque; il existe alors une forme A_2 telle que les diviseurs élémentaires du faisceau $|\lambda_1 A_2 + \lambda_2 A_2'|$ soient ceux de $\Phi(\lambda_1, \lambda_2)$; $|A_2|$ est différent de zéro puisque $\varphi(0)$ est différent de zéro.

D'après les hypothèses faites sur φ_1, φ_2, le produit

$$|A_1 + A_1'| \; |A_2 + A_2'|$$

n'est pas nul.

Si l'on pose

$$S_1 = A_1 + A_1', \qquad S_2 = A_2 + A_2'$$

76) *G. Frobenius*, J. reine angew. Math. 84 (1878), p. 41.

et
$$S_0 = S_1 + S_2,$$
puis
$$P_1 = -A_1^{-1}A_1', \qquad P_2 = A_2^{-1}A_2', \qquad P_0 = P_1 + P_2,$$
et selon l'usage
$$E_1 = x_1y_1 + x_2y_2 + \cdots + x_my_m, \qquad E_2 = x_{m+1}y_{m+1} + \cdots + x_ny_n,$$
on aura
$$A_1(\lambda E_1 - P_1) = \lambda A_1 + A_1', \qquad A_2(\lambda E_2 - P_2) = \lambda A_2 - A_2';$$
d'où l'on conclut que $|\lambda E_1 - P_1|$ et $|\lambda E_2 - P_2|$ décomposés en diviseurs élémentaires sont précisément $\varphi_1(\lambda)$ et $\varphi_2(\lambda)$, et par suite on a pour diviseurs élémentaires de $|\lambda E - P_0|$ ceux de $|\lambda E - P|$,
$$|\lambda E - P_0| = \varphi_1(\lambda)\varphi_2(\lambda).$$

Les formes P_0, P sont donc semblables, d'où $|P_0|$ différent de zéro. Mais d'autre part
$$P_1'A_1P_1 = A_1,$$
ce qui donne
$$P_1'A_1'P_1 = A_1'$$
et ensuite
$$P_1'S_1P_1 = S_1;$$
on aurait de même
$$P_2'S_2P_2 = S_2,$$
d'où enfin
$$(P_1' + P_2)(S_1 + S_2)(P_1 + P_2) = S_1 + S_2$$
ou
$$P_0'S_0P_0 = S_0.$$

Il existe ainsi une forme symétrique *ordinaire* S_0 que la transformation P_0 conserve: la transformation P semblable à P_0 conserve donc aussi une forme S semblable à S_0 c'est-à-dire ordinaire et symétrique.

Un raisonnement analogue s'appliquerait à la forme alternée.

Remarque: A. Voss[77]) a déduit de là, entre autres, la proposition suivante: si P et Q sont deux transformations automorphes propres (ou impropres) d'une forme symétrique ordinaire, lorsque le déterminant $|P + Q|$ est nul son rang $r = n - q$, où q est toujours pair.

Cette proposition est l'extension d'un théorème de *T. J. Stieltjes*[78]) qui a occupé divers géomètres.*

51. Types de substitutions qui conservent une forme symétrique (ou alternée) ordinaire. *Il résulte des propositions précédentes que, si $\varphi(\lambda)$ est un produit de diviseurs élémentaires qui contient

77) *A. Voss,* Abh. Akad. München 17 (1892), Abt. II (1890/1), p. 261.

78) *T. J. Stieltjes,* Acta math. 6 (1885), p. 319; *E. Netto,* Acta math. 9 (1886/7), p. 291; *A. Voss,* Nachr. Ges. Gött. 1887, p. 424/33.

toujours avec le diviseur $(\lambda - c)^e$ le diviseur $\left(\lambda - \frac{1}{c}\right)^e$ quand c^2 est différent de 1 [et aussi quand $c^2 = 1$ et que e est *pair*], on peut trouver si n est le degré de $\varphi(\lambda)$ une substitution linéaire P, avec $|P$ différent de zéro,
$$x_i = \sum_{(i,k)} p_{ik}x'_k \qquad (i, k = 1, 2, .., n)$$
dont la fonction caractéristique $|\lambda E - P|$ possède les diviseurs élémentaires considérés et ensuite une forme symétrique ordinaire de $2n$ variables S, satisfaisant à l'identité
$$P'SP = S.$$

On a vu que toute autre forme symétrique ordinaire à $2n$ variables est congruente à S; *il existe donc des substitutions semblables à P qui la conservent.*

Une proposition analogue s'applique aux formes alternées.

En posant
$$x_i = y_i.$$
on transforme une forme bilinéaire symétrique en une forme quadratique. *Les résultats précédents s'appliquent donc aux formes quadratiques.*

On déduit de ces résultats une *classification des substitutions qui conservent une forme symétrique (ou alternée) ordinaire à $2n$ variables, ou une forme quadratique à n variables.*

On aura par exemple, en se reportant aux types de substitutions indiqués plus haut pour $n = 3$, les types suivants de substitutions qui conservent une forme quadratique ternaire:

$$\left[1\,1\,\overset{+}{1}\right] \qquad x_1 = c_1x'_1, \qquad x_2 = \frac{1}{c_1}x'_2, \qquad x_3 = x'_3,$$
$$\left[\overset{+}{1}\,\overset{+}{1}\,\overset{+}{1}\right] \qquad x_1 = x'_1, \qquad x_2 = x_2', \qquad x_3 = x_3',$$
$$\left[\overset{+}{1}\,\overset{+}{1}\,\overset{-}{1}\right] \qquad x_1 = x_1', \qquad x_2 = x_2', \qquad x_3 = -x_3',$$
$$\left[\overset{+}{3}\right] \qquad x_1 = x_1', \qquad x_2 = x_1' + x_2', \; x_3 = x_2' + x'_3;$$
le signe + se rapporte à un diviseur élémentaire relatif à la base $(\lambda + 1)$, le signe — à un diviseur élémentaire relatif à $(\lambda - 1)$. On indique aisément des formes ordinaires inaltérées par ces substitutions:
$$x_1x_2 + x_3^2$$
pour les premières par exemple,
$$x_1^2 + 2x_2^2 - 2x_1x_2 - 4x_1x_3$$
pour la dernière.*

52. Cas limites. *On a vu que les équations quadratiques qui déterminent les coefficients a_{ik} de manière que l'on ait
$$U'SU = S,$$

avec $|S|$ différent de zéro, sont résolues par

$$U = (S + T)^{-1}(S - T),$$

où T est une forme alternée quelconque pour laquelle le déterminant $|S + T|$ est différent de zéro. Les paramètres t_{ik} en nombre $\frac{n(n-1)}{2}$ doivent être finis et pour que les u_{ik} le soient il suffit que le déterminant $|S + T|$ soit différent de zéro.

L'identité

$$(S + T)(E + U) = 2S$$

montre alors que nécessairement le déterminant

$$|E + U|$$

est différent de zéro.

Lorsque les t_{ik} tendent vers un système de valeurs pour lesquelles

$$|S + T| = 0,$$

le déterminant $|E + U|$ augmente indéfiniment; un ou plusieurs des u_{ik} augmentent donc indéfiniment. Inversement si les u_{ik} tendent vers un système de valeurs qui annule $|E + U|$, un ou plusieurs des t_{ik} augmentent indéfiniment.

G. Frobenius[79]) a établi que *toute substitution U, propre, qui transforme la forme ordinaire symétrique S en elle-même et pour laquelle le déterminant $|E + U|$ est nul, s'obtient par la formule*

$$U = \lim (S + T_h)^{-1}(S - T_h),$$

où T_h est une forme alternée dont les coefficients t_{ik} sont des fonctions rationnelles du paramètre h.

Ainsi l'adjonction de la condition $|U| = 1$ transforme le système des équations quadratiques en u_{ik} en un système algébriquement irréductible au sens de *L. Kronecker*. La variété unicursale à $\frac{n(n-1)}{2}$ dimensions de l'espace des u_{ik} représentée par ces équations est *indécomposable.*

Pour les formes ternaires ($n = 3$) et pour celles-là seulement toutes les substitutions *propres* sont comprises dans la formule

$$U = (\lambda S + T)^{-1}(\lambda S - T),$$

où λ et les coefficients de la forme alternée T sont finis[80]).

De même *toute substitution automorphe U d'une forme alternée ordinaire T, pour laquelle le déterminant $|E - U|$ est nul, peut s'obtenir par la formule*

$$U = \lim (S_h + T)^{-1}(S_h - T),$$

79) J. reine angew. Math. 84 (1878), p. 43.

80) *P. Bachmann*, id. 76 (1873), p. 338; *Ch. Hermite*, id. 78 (1874), p. 328.

où les coefficients de la forme symétrique quelconque S_h sont des fonctions rationnelles de h.

Une forme alternée ordinaire T n'admet que des transformations U propres.*

53. Formes orthogonales. *Une substitution R est orthogonale si $R' = R^{-1}$; on a dans ce cas

$$R'R = RR' = E, \qquad R'ER = E$$

et réciproquement.

La substitution R transformant en elle-même la forme symétrique ordinaire E, les diviseurs élémentaires de son déterminant caractéristique sont deux à deux $(\lambda - c)^e$, $\left(\lambda - \frac{1}{c}\right)^e$ sauf ceux $(\lambda - \varepsilon)^{2\varkappa+1}$ où $\varepsilon = \pm 1$, qui peuvent être en nombre impair. Il existe d'ailleurs toujours d'après le paragraphe précédent une substitution orthogonale à $2n$ variables dont le déterminant caractéristique possède des diviseurs donnés satisfaisant à ces conditions. On peut donc classer les substitutions orthogonales d'après leurs *caractéristiques.*

Le produit R_1R_2 de deux formes orthogonales R_1, R_2 est une forme orthogonale.

Si A est une forme ordinaire permutable avec sa conjuguée, $A^{-1}A'$ est une forme orthogonale *propre* (à déterminant $+1$).

Si la forme symétrique S est permutable avec la forme alternée T et si la forme $S + T$ est ordinaire, le produit

$$(S + T)^{-1}(S - T)$$

est une forme orthogonale propre.

Si T est alternée et la fonction rationnelle $f(T)$ ordinaire, le produit

$$f(T)^{-1}f(-T)$$

est une forme orthogonale propre.

Si T est une forme alternée pour laquelle le déterminant $|E + T|$ est différent de zéro, la forme

$$R = \frac{E - T}{E + T}$$

est orthogonale et propre; de plus le déterminant $|E + R|$ est différent de zéro. Réciproquement toute forme orthogonale R pour laquelle le déterminant $|E + R|$ n'est pas nul peut s'exprimer d'une seule manière par la formule

$$R = \frac{E - T}{E + T},$$

où $T = \frac{E - R}{E + R}$ est alternée.

Si la forme T est réelle, il en est de même de R et réciproquement.

A toute forme orthogonale réelle R pour laquelle le déterminant $|R + iE|$ est différent de zéro correspond une forme orthogonale

$$\frac{E + iR}{R + iE}$$

dont les coefficients conjugués ont des valeurs complexes conjuguées.

Deux formes orthogonales semblables sont aussi congruentes et transformables l'une dans l'autre par une substitution orthogonale.

Les formes orthogonales *réelles* ont donné lieu à un grand nombre de recherches.

Si R est une forme orthogonale réelle à $2n$ variables, l'équation caractéristique $|\lambda E - R| = 0$ n'a que des racines dont le module est l'unité[81]).

Ses diviseurs élémentaires sont tous simples[82]).

Si deux formes réelles orthogonales ont par suite le même déterminant caractéristique, elles ont mêmes diviseurs élémentaires: elles sont donc semblables. *L. Stickelberger* montre qu'elles sont aussi congruentes par une transformation réelle orthogonale.

On peut construire une forme réelle orthogonale ayant des diviseurs élémentaires donnés

$$\left(\lambda - e^{\pm i\theta_k}\right), \quad (\lambda - 1) \text{ pris } \sigma \text{ fois}, \quad (\lambda + 1) \text{ pris } \tau \text{ fois},$$

c'est-à-dire pour laquelle le déterminant

$$|\lambda E - R| = (\lambda - e^{i\theta_1})(\lambda - e^{-i\theta_1}) \dots (\lambda - e^{i\theta_\varrho})(\lambda - e^{-i\theta_\varrho})(\lambda - 1)^\sigma(\lambda + 1)^\tau,$$

pourvu que

$$2\varrho + \sigma + \tau = n.$$

La substitution orthogonale réelle

$$x_1 = \cos\theta_1 x_1' - \sin\theta_1 x_2', \dots, x_{2\varrho-1} = \cos\theta_\varrho x'_{2\varrho-1} - \sin\theta_\varrho x'_{2\varrho},$$
$$x_2 = \sin\theta_1 x_1' + \cos\theta_1 x_2', \dots, x_{2\varrho} = \sin\theta_\varrho x'_{2\varrho-1} + \cos\theta_\varrho x'_{2\varrho},$$
$$x_{2\varrho+1} = x'_{2\varrho+1}, \dots, x_{2\varrho+\sigma} = x'_{2\varrho+\sigma},$$
$$x_{2\varrho+\sigma+1} = -x'_{2\varrho+\sigma+1}, \dots, x_n = -x'_n$$

satisfait à ces conditions; c'est une forme *normale* de toute substitution orthogonale réelle.*

81) *F. Brioschi*, J. math. pures appl. (1) 19 (1854), p. 253/6; Opere 5, Milan 1909, p. 161/4; *L. Schläfli*, J. reine angew. Math. 65 (1866), p. 186; *G. Frobenius*, J. reine angew. Math. 84 (1878), p. 52; *L. Stickelberger*, Progr. polyt. Schule Zürich 1877, p. 3.

82) *G. Frobenius*, J. reine angew. Math. 84 (1878), p. 53; *L. Stickelberger*, Programm[81]) p. VII.

Transformations congruentes des formes bilinéaires quelconques, d'après Voss.

54. Solution analytique. *Les recherches de *G. Frobenius* sur les transformations congruentes des formes symétriques ou alternées ont été étendues par *A. Voss*[83]) aux formes quelconques.

Il a également retrouvé, par une méthode qui lui est propre et qui se rattache à un travail antérieur sur les formes orthogonales[84]), les résultats de *G. Frobenius* pour les formes symétriques ou alternées.

D'autres résultats particuliers seront signalés brièvement, mais nous donnerons en détail la méthode qui permet de déterminer *par des opérations rationnelles* toutes les transformations automorphes *non singulières* d'une forme quelconque (non symétrique ou alternée) et les conséquences générales que *A. Voss* en a déduit.

Supposons

$$P'AP = A,$$

ce qui s'écrit aussi

$$P'A = AP^{-1},$$

et considérons la forme

$$Q = P(A')^{-1}$$

dont la conjuguée est

$$Q' = A^{-1}P'.$$

On aura immédiatement

$$Q'AQ = A^{-1}P'AP(A')^{-1} = A^{-1}AP^{-1}P(A')^{-1} = (A')^{-1}.$$

La transformation Q change donc A en $(A')^{-1}$ (conjuguée de sa réciproque) que *A. Voss* nomme l'*associée* (beigeordnete) de A.

On déduit de l'équation précédente, en passant aux conjuguées,

$$Q'A'Q = A^{-1}$$

puis aux réciproques

$$Q^{-1}(A')^{-1}(Q')^{-1} = A,$$

ou encore

$$(A')^{-1} = QAQ'.$$

On a donc enfin

$$Q'AQ = QAQ' = (A')^{-1};$$

nous en concluons d'abord

$$A'QA = (Q')^{-1},$$

c'est-à-dire que *la transformation A change aussi Q en son associée*[85]).

Si l'on pose

$$A = \sum_{(i,k)} a_{ik} x_i y_k \qquad (i, k = 1, 2, \dots, n)$$

83) *A. Voss*, Nachr. Ges. Gött. 1887, p. 429; Abh. Akad. München 17 (1892), Abt. II (1890/1), p. 237; Sitzgsb. Akad. München 19 (1889), p. 175/211.

84) *A. Voss*, Math. Ann. 13 (1878), p. 320.

85) *A. Voss*, Abh. Akad. München 17 (1892), Abt. II (1890/1), p. 255.

et si l'on désigne par P une transformation automorphe de A, définie par

$$x_i = \sum_{(m)} p_{im} u_m,$$

$$y_k = \sum_{(l)} p_{kl} v_l,$$

l'égalité

$$P' A P = A$$

donne les n^2 équations *quadratiques*

$$\sum_{(i,k)} a_{ik} p_{im} p_{kl} = a_{ml} \qquad (m, l = 1, 2, \ldots, n)$$

pour déterminer les n^2 coefficients p_{ik}.

Une identité où interviennent les adjointes de *G. Darboux* relatives à la forme $\lambda E - P$ permet à *A. Voss* de remplacer ces relations quadratiques par des relations *linéaires* entre les mineurs du premier ordre ϖ_{ik} du déterminant

$$\Delta(\lambda) = |\lambda E + P|,$$

les mineurs analogues ϖ'_{ik} du déterminant

$$\Delta\left(\frac{1}{\lambda}\right) = \left|\frac{1}{\lambda} E + P\right|$$

et ce dernier déterminant. Si l'on y fait $\lambda = \pm 1$, ce qui donne

$$\varpi_{ik} = \varpi'_{ik},$$

on peut donc calculer les ϖ_{ik}: Δ dans l'hypothèse où $\Delta(\pm 1)$ n'est pas nul et en déduire les p_{ik} par les relations classiques

$$(1) \qquad \begin{cases} \displaystyle\sum_{i=1}^{i=n} p_{ik} \varpi_{il} = 0 \qquad (k \gtrless l) \\ \displaystyle\sum_{i=1}^{i=n} p_{ik} \varpi_{ik} = \Delta. \end{cases}$$

A. Voss tire aussi parti de la réciprocité signalée entre Q et A pour obtenir deux systèmes linéaires analogues déterminant les mineurs des déterminants

$$|Q + A^{-1}|, \qquad |Q + A'^{-1}|$$

dans le cas où l'un ou l'autre de ces déterminants ne s'annule pas.

Les coefficients de Q s'en déduisent par la résolution du système analogue à (1).

On obtient donc les q_{ik} et les p_{ik} par des opérations rationnelles.*

55. Transformations automorphes des formes singulières.

*Supposons $|S| = 0$; *A. Voss* observe que, si l'on a

$$U'(S + \lambda S') U = S + \lambda S',$$

on en conclut

$$U' S U = S$$

pour λ^2 différant de 1.

On peut donc se borner à donner à λ une valeur autre que ± 1 et chercher les transformations automorphes de $S + \lambda S'$.

Ceci n'est plus permis si le faisceau

$$S + \lambda S'$$

est singulier. Supposons qu'une transformation congruente V ramène S à une forme Σ qui ne contient que les variables

$$x_1, y_1, \ldots, x_r, y_r \quad (r < n);$$

si l'on pose, avec

$$V' S V = \Sigma, \qquad V^{-1} U V = W,$$

on aura

$$W' \Sigma W = \Sigma.$$

Si le faisceau

$$\Sigma + \lambda \Sigma'$$

n'est pas singulier, on pourra supposer que le déterminant $|\Sigma|$ n'est pas nul. Dans ce cas, en posant

$$E_1 = x_1 y_1 + x_2 y_2 + \cdots + x_r y_r,$$

on aura

$$E_1 W' E_1 \Sigma E_1 W E_1 = \Sigma,$$

c'est-à-dire que

$$U = E_1 W E_1$$

est une transformation automorphe ordinaire à $2r$ variables de Σ.

Comme on a, pour

$$E_1 + E_2 = E,$$

$$E_2 \Sigma = E_2 W' \Sigma W = 0$$

et que le produit $|W| |\Sigma|$ n'est pas nul, en écrivant

$$E_2 W' E_1 \Sigma W = 0$$

on en peut conclure

$$E_2 W' E_1 = 0$$

ou aussi

$$E_1 W E_2 = 0.$$

Si l'on pose donc

$$W = \Sigma w_{ik} x_i y_k + \Sigma w_{i'k} x_{i'} y_k + \Sigma w_{ik'} x_i y_{k'} + \Sigma w_{i'k'} x_{i'} y_{k'},$$

où les indices non accentués sont pris dans la suite $1, 2, \ldots, r$, et les accentués dans la suite $r+1, \ldots, n$, on en déduira

$$w_{ik'} = 0 \qquad (i = 1, 2, \ldots, r;\ k' = r+1, r+2, \ldots, n).$$

La transformation W est alors entièrement déterminée, car les coefficients w_{ik} sont donnés par

$$W' \Sigma W = \Sigma$$

et les autres $w_{i'k}$, $w_{i'k'}$ disparaissant de cette équation peuvent être choisis arbitrairement.

Lorsque le faisceau

$$\Sigma + \lambda \Sigma'$$

est singulier, comme le nombre des variables de Σ ne peut être réduit, on a

$$\Sigma = S_\alpha + S_\beta,$$

où

$$S_\alpha = x_1 y_2 + x_2 y_3 + \cdots + x_{2p} y_{2p+1} \qquad (2p+1 < r)$$

et S_β désigne une forme ordinaire en

$$x_{2p+2}, y_{2p+2}, \ldots, x_r, y_r.$$

On trouve pour déterminer W les équations

$$(E_1 W' E_1) \Sigma (E_1 W E_1) = \Sigma$$

$$\begin{cases} E_2 W' E_1 \Sigma = 0 \\ \Sigma E_1 W E_2 = 0 \end{cases}$$

dont les premières sont quadratiques et les autres linéaires.

A. Voss détermine en particulier *explicitement* les transformations automorphes W de la forme

$$\Sigma = S_\alpha;$$

chacune d'elles contient en général $(p+1)$ paramètres et si $|W| = \alpha$, l'équation caractéristique de W a $(p+1)$ diviseurs élémentaires simples $(\lambda - \alpha)$ et p diviseurs simples $\left(\lambda - \frac{1}{\alpha}\right)\cdot$

La détermination explicite de W dans le cas

$$\Sigma = S_\alpha + S_\beta$$

est également donnée.

La fonction caractéristique de toute substitution automorphe de $S_\alpha + S_\beta$ est

$$(\alpha - \lambda)^{p+1} \left(\frac{1}{\alpha} - \lambda\right)^p M,$$

où M est la fonction caractéristique relative aux coefficients w_{ik} dont les deux indices dépassent $2p+1$.*

56. Transformations automorphes symétriques ou alternées d'une forme bilinéaire. *Supposons

$$U' S U = S$$

avec

$$U = \pm U';$$

on en déduira

$$U S U = \pm S,$$

puis

$$US^2 = US \cdot S = \pm S U^{-1} S = S^2 U.$$

La substitution U est donc permutable avec S^2; elle l'est même *en général* avec S, car si l'on pose

$$US - SU = X$$

on a

$$SX = SUS - S^2 U, \qquad XS = US^2 - SUS,$$

c'est-à-dire

$$SX + XS = 0.$$

Pour que cette équation admette d'autres solutions que $X = 0$ *il est nécessaire et suffisant que l'équation caractéristique de* S *ait ses racines deux à deux opposées.*

En dehors de ces formes spéciales, $X = 0$.

Transformations symétriques. Une transformation symétrique

$$US = SU$$

donne, avec

$$USU = S,$$

la relation

$$U^2 = E;$$

la réciproque est vraie.

Une forme qui satisfait à

$$U^2 = E$$

n'a pour diviseurs élémentaires que $\lambda + 1$ et $\lambda - 1$; U est donc semblable à $E_1 - E_2$. En posant

$$U = V(E_1 - E_2) V^{-1}$$

on trouve pour que U soit symétrique

$$V' V (E_1 - E_2) = (E_1 - E_2) V' V,$$

où

$$V' V = W$$

est symétrique. Les équations qui s'en déduisent

$$E_2 W E_1 = - E_2 W E_1 = 0,$$

$$E_1 W E_2 = - E_1 W E_2 = 0$$

montrent alors que W est décomposable en deux formes W_1, W_2 qui sont symétriques et formées des variables de E_1 et E_2. Soient T_1, T_2 les deux transformations congruentes qui changent respectivement W_1 en E_1 et W_2 en E_2; en posant

$$T = T_1 + T_2$$

on aura

$$T' V' V T = E$$

ou encore avec

$$Z = VT,$$

on aura

$$Z Z' = E.$$

La transformation Z est donc *orthogonale*.

Réciproquement si Z est orthogonale, $V = ZT^{-1}$ donne
$$U = ZT^{-1}(E_1 - E_2)TZ^{-1} = Z(E_1 - E_2)Z^{-1} = Z(E_1 - E_2)Z'.$$
En exprimant que l'on a
$$US = SU$$
il vient
$$(E_1 - E_2)Z'SZ = Z'SZ(E_1 - E_2),$$
d'où l'on peut conclure que $Z'SZ$ est décomposable en deux formes S_1 et S_2.

Ainsi *pour qu'il existe des solutions U symétriques de l'équation $US = SU$, il faut qu'il existe des transformations orthogonales Z qui changent S en une forme décomposable $S_1 + S_2$.* Cette condition est suffisante.

Transformations alternées. Si l'on veut avoir, pour U alternée,
$$USU = -S \quad \text{avec} \quad US = SU$$
on en déduira
$$U^2 = -E,$$
d'où
$$U = iV(E_1 - E_2)V^{-1}.$$
Si l'on pose
$$V'V = W,$$
la condition pour que U soit alternée donne
$$W(E_1 - E_2) + (E_1 - E_2)W = 0$$
et la forme symétrique W doit vérifier
$$E_1 W E_1 = E_2 W E_2 = 0.$$
Ces conditions sont suffisantes.

Puisque $|W|$ n'est pas nul, il faut que n soit pair ($n = 2p$), le nombre des variables de E_1 et E_2 étant le même. La permutabilité de S et U donne en outre par un calcul facile
$$V'SV(E_1 - E_2) + (E_1 - E_2)V'SV = 0,$$
d'où aussi
$$E_1 V'SV E_1 = E_2 V'SV E_2 = 0.$$

Pour que la forme S de $2p$ couples de variables admette une transformation automorphe U alternée, permutable avec elle, cette forme S doit pouvoir se transformer par une transformation congruente V en une forme décomposable $S_1 + S_2$, S_1 dépendant des variables $x_1, x_2, \ldots, x_p$, $y_{p+1}, \ldots, y_{2p}$ et S_2 des autres. Cette condition est suffisante.

Ces transformations U ne peuvent se déterminer rationnellement. *A. Voss* examine également la détermination de U quand
$$US - SU = X$$

est différent de zéro, mais seulement dans l'hypothèse où l'un des déterminants $|U + E|$, $|U - E|$ est différent de zéro. La transformation U est dite *non singulière* et les méthodes générales développées dans le paragraphe suivant s'appliquent.*

57. Détermination rationnelle des transformations automorphes non singulières d'une forme bilinéaire quelconque. *Si la transformation U conserve la forme S, où $|S|$ n'est pas nul, on a
$$U'SU = S$$
et aussi
$$U'S'U = S'.$$
En posant
$$R_\lambda = S(E\lambda - U)(E\lambda + U)^{-1},$$
ce qui donne
$$R_\lambda' = (E\lambda + U')^{-1}(E\lambda - U')S',$$
et si l'on tient compte des équations
$$U'S' = S'U^{-1}, \qquad (S')^{-1}U' = U^{-1}(S')^{-1}$$
qui permettent d'écrire
$$(E\lambda - U')S' = S'(E\lambda - U^{-1}),$$
$$(S')^{-1}(E\lambda + U') = (E\lambda + U^{-1})(S')^{-1},$$
on aura la nouvelle expression
$$R_\lambda' = S'(E\lambda + U^{-1})^{-1}(E\lambda - U^{-1}) = S'\left(U + \frac{E}{\lambda}\right)^{-1}\left(U - \frac{E}{\lambda}\right).$$
Donc, si $\lambda\mu = 1$,
$$-S^{-1}R_\mu = (S')^{-1}R_\lambda'.$$

A. Voss applique ceci en prenant pour λ une racine η de l'équation $\eta^2 = 1$; on a alors
$$R_\eta = S(E\eta - U)(E\eta + U)^{-1},$$
ce qui donne
$$R_\eta' = -S'S^{-1}R_\eta,$$
et enfin, en prenant
$$T_\eta = S^{-1}R_\eta S^{-1} = (E\eta - U)(E\eta + U)^{-1}S^{-1},$$
on a la relation simple
$$T_\eta'S' = -T_\eta S \quad \text{ou bien} \quad S'T_\eta' = -ST_\eta,$$
dans l'hypothèse où le déterminant de $E\eta + U$ n'est pas nul.

La transformation U se déduit aisément de T_η; en effet
$$U(T_\eta S + E) = (E - T_\eta S)\eta,$$
d'où
$$U = \eta(E - T_\eta S)(E + T_\eta S)^{-1} = \eta(S^{-1} - T_\eta)S(S')^{-1}((S')^{-1} - T_\eta')^{-1}.$$

Cette dernière expression montre que le déterminant $|U|$ est égal à η^n.

Comme pour n impair et une transformation *propre* (de déterminant $+1$) le déterminant $|U-E|$ s'annule, il faudra prendre $\eta = +1$ pour obtenir une transformation propre. Le déterminant $|E+T_\eta S|$, voisin de 1 quand les coefficients homogènes de T_η sont très petits, ne peut s'annuler.

Si n est pair, aucune transformation *impropre* ne peut être donnée par la formule, car $|U+E\eta|$ s'annule; pour n impair, il suffira de prendre $\eta = -1$.

Toute transformation automorphe congruente U de la forme ordinaire S, pour laquelle le déterminant $|U+E\eta|$ n'est pas nul, peut donc se mettre d'une seule manière sous la forme

$$U = \eta(E-TS)(E+TS)^{-1},$$

où T satisfait à l'équation

$$TS + T'S' = 0.$$

On peut remarquer que l'introduction de la forme R qui satisfait à

$$(S')^{-1}R' + S^{-1}R = 0$$

donnerait pour U l'expression

$$U = \eta(S+R)^{-1}(S-R).$$

La réciproque est vraie et se démontre aisément. Elle est valable, même si le déterminant $|S|$ s'annule, pourvu que le déterminant $|TS+E|$ ne soit pas nul.

La recherche des transformations non singulières U est ainsi ramenée à la résolution de l'équation symbolique

$$TS + T'S' = 0,$$

c'est-à-dire à celle du système d'équations *linéaires* à n^2 inconnues

$$\sum_{k=1}^{k=n} t_{ik}s_{kl} + \sum_{k=1}^{k=n} t_{kl}s_{ik} = 0 \qquad (i, l = 1, 2, \ldots, n).$$

Ces transformations se déterminent donc par des opérations rationnelles.

On peut obtenir aussi les transformations *non essentiellement singulières*, qui multipliées par une transformation non singulière donnent une transformation non singulière. Car si l'on a

$$W = UV,$$

où U et W sont non singulières et V singulière, on en déduit

$$V = U^{-1}W,$$

U et W étant données par la méthode précédente.

Il restera donc à trouver les transformations congruentes de S en elle-même, *essentiellement singulières*, c'est-à-dire telles que leur produit par une transformation non singulière donne toujours une transformation singulière.*

58. Remarques sur l'équation $TS + T'S' = 0$. *Le système des n^2 équations linéaires qui déterminent les t_{ik} admet, quand les s_{ik} sont arbitraires, des solutions qui dépendent au moins de N arbitraires, N désignant la partie entière de $\frac{n}{2}$; en d'autres termes le déterminant des coefficients des inconnues et ses mineurs jusqu'à et y compris ceux de l'ordre $(N-1)$ s'annulent identiquement[86]).

L'équation

$$TS + T'S' = 0$$

donne immédiatemant

$$T(S-\lambda S') + (T'+\lambda T)S' = 0;$$

d'où l'on conclut, si le déterminant $|T|$ n'est pas nul, que les diviseurs élémentaires de $|S-\lambda S'|$ sont identiques à ceux de $|T'+\lambda T|$.

Si n est impair, la relation

$$|T| = (-1)^n |T|$$

montre que $|T|$ est nécessairement nul. Il en est alors de même du déterminant $|T'+\lambda T|$ du faisceau $T'+\lambda T$, et d'une manière générale du déterminant

$$\begin{vmatrix} t_{11}+\lambda_1 t_{11}, & t_{12}+\lambda_2 t_{21}, & \ldots, & t_{1n}+\lambda_n t_{n1} \\ t_{21}+\lambda_1 t_{12}, & t_{22}+\lambda_2 t_{22}, & \ldots, & t_{2n}+\lambda_n t_{n2} \\ \cdot & \cdot & \cdot & \cdot \\ t_{n1}+\lambda_1 t_{1n}, & t_{n2}+\lambda_2 t_{2n}, & \ldots, & t_{nn}+\lambda_n t_{nn} \end{vmatrix}$$

quels que soient les paramètres $\lambda_1, \lambda_2, \ldots, \lambda_n$.

Lorsque le déterminant $|T|$ est nul, on peut toujours obtenir une forme X congruente à T qui contienne moins de $2n$ variables et dont le déterminant ne s'annule plus.

L'équation

$$T(S+S') = -(T'-T)S'$$

montre que, si le déterminant $|S+S'|$ n'est pas nul, on a

$$TS = -(T'-T)S'(S+S')^{-1}S;$$

la forme TS, produit d'une forme alternée par une forme symétrique ordinaire, est semblable à une forme alternée.

On observe d'ailleurs que T ne peut être symétrique (ou alterné) que si S est alterné (ou symétrique).

86) *A. Voss*, Abh. Akad. München 17 (1892), Abt. II (1890/1), p. 309.

Si T est symétrique et si le déterminant $|T|$ est nul, on a
$$|S + S'| = 0;$$
cette condition est suffisante.

De même si T est alterné et si le déterminant $|T|$ est nul, on a
$$|S - S'| = 0.$$

Lorsque le déterminant $|S + S'|$ est différent de zéro, le déterminant $|T|$ quand il ne s'annule pas est le carré d'une fonction rationnelle de ses éléments. Car $|T|$ ne peut s'annuler que par un facteur du déterminant gauche $|T' - T|$.

On voit de même que, si le déterminant $|T|$ est nul, ses mineurs sont nuls jusqu'à un ordre k de parité différente de n.*

59. Résolution de l'équation $TS + T'S' = 0$. *Parmi les nombreuses propositions particulières établies par *A. Voss* nous signalerons encore la suivante: soient Θ, T deux solutions de l'équation
$$TS + T'S' = 0,$$
dont l'une au moins T est ordinaire ($|T|$ différent de zéro); les deux équations
$$(\Theta + \lambda\Theta')S + \Theta'(S' - \lambda S) = 0,$$
$$(T + \lambda T')S + T'(S' - \lambda S) = 0$$
donnent
$$\Theta + \lambda\Theta' = \Theta'(T')^{-1}(T + \lambda T'),$$
d'où l'on conclut que les faisceaux
$$\Theta + \lambda\Theta', \qquad T + \lambda T'$$
sont équivalents dès que $|\Theta|$ est différent de zéro.

Si $|\Theta| = 0$, on peut remplacer Θ par $\Theta + hT$ et prendre h de telle sorte que $\Theta - hT$ soit ordinaire.

Toute solution Θ s'exprime donc au moyen de T sous la forme
$$\Theta = hT + V'TV,$$
et la forme V doit satisfaire à la relation
$$V'TVS + V'T'VS' = 0$$
qui donne aisément, en observant que $T^{-1}T' = -S(S')^{-1}$,
$$VS(S')^{-1} = S(S')^{-1}V.$$

Toutes les solutions du problème s'obtiennent donc au moyen d'une seule, ordinaire, et des formes V permutables avec la forme antisymétrique $S(S')^{-1}$.

A. Voss a d'ailleurs ramené complètement la résolution de l'équation symbolique

(a) $$TS + T'S' = 0$$

au *problème des formes permutables.*

Écrivons l'équation
$$ST + S'T' = 0$$
et éliminons T' entre cette équation et la précédente, nous aurons
$$TS(S')^{-1} = (S')^{-1}ST;$$
la forme T admet donc en elle-même la transformation *antisymétrique*
$$X = S(S')^{-1}.$$

En posant
$$T = S^{-1}Y$$
on aura
$$S(S)^{-1}Y = YS(S')^{-1},$$
c'est-à-dire que *Y est permutable avec X.*

Inversement toute forme Y permutable avec X donnera une forme satisfaisant à la relation (a).

Eu égard à l'identité
$$Y'S^{-1} + S^{-1}Y = 0$$
on peut encore donner de T l'expression élégante
$$2T = S^{-1}Y - Y'S^{-1}.*$$

60. Détermination des formes T linéairement distinctes. *Une autre manière de ramener cette même question à celle des formes permutables a l'avantage de conduire à la *détermination du nombre des formes T linéairement indépendantes.*

L'identité
$$(T + T')(S + S') + (T' - T)(S' - S) = 0$$
permet, si $|S - S'|$ n'est pas nul, de déterminer les formes symétriques $T + T'$ et les formes alternées $T - T'$.

Si l'on pose
$$V = S^{-1}(S + S')(S' - S)^{-1} = (S' - S)^{-1}(S + S')S^{-1}$$
la forme V vérifie
$$SV + S'V' = 0$$
et le déterminant de
$$SV + E = 2S'(S' - S)^{-1}$$
est différent de zéro.

On trouve alors aisément
$$[(T + T')S]\,VS = VS[(T' + T)S],$$
et de toute solution X de l'équation
$$X \cdot VS = VS \cdot X$$
on peut déduire l'expression d'une forme symétrique
$$T + T' = XS^{-1} + (S')^{-1}X'$$

et celle de T

$$2T = [XS^{-1} + (S')^{-1}X'](SV + E) = P(SV + E).$$

[Dans l'hypothèse où $|S + S'|$ n'est pas nul, on aurait pu orienter le calcul de façon à trouver d'abord $T' - T$].

Le nombre des formes linéairement indépendantes T ou P s'obtiendra alors comme suit:

Si $X_1, X_2, \ldots, X_k$ sont toutes les formes linéairement indépendantes qui satisfont à

$$X \cdot VS = VS \cdot X,$$

on aura aussi, pour tout indice h,

$$X_h' SV = SVX_h',$$

d'où l'on conclut

$$[(S')^{-1}X_h'S]\,VS = VS[(S')^{-1}X_h'S]$$

et par suite

$$(S')^{-1}X_h'S = \sum_{i=1}^{i=k} \alpha_{hi} X_i.$$

Écrivons les identités

$$X_h = \sum_{i=1}^{i=k} (hi) X_i,$$

$$(hi) = 0 \ (i \gtrless h), \qquad (hh) = 1,$$

et considérons

$$P_h = X_h S^{-1} + (S')^{-1} X_h' = \sum_{i=1}^{i=k} (\alpha_{hi} + (hi)) X_i S^{-1};$$

les formes P_h sont liées par autant de relations linéaires qu'il en existe entre les éléments des colonnes du tableau

$$\alpha_{hi} + (hi) \qquad (i = 1, 2, \ldots, k).$$

On a d'autre part

$$S' X_h S^{-1} = \sum_{i=1}^{i=k} \alpha_{hi} X_i',$$

d'où l'on déduit

$$X_h = \sum_{i=1}^{i=k} \alpha_{hi} (S')^{-1} X_i' S = \sum_{i=1}^{i=k} \alpha_{hi} \alpha_{il} X_l;$$

les coefficients α_{hi} satisfont donc aux conditions

$$\sum_{i=1}^{i=k} \alpha_{hi} \alpha_{il} = (hl)$$

qui expriment que *la forme*

$$A = \sum_{i=1}^{i=k} \alpha_{hi} x_h y_i$$

vérifie l'équation

$$A^2 = E.$$

La fonction caractéristique de A a par suite *un certain nombre p de diviseurs élémentaires simples* $(\lambda - 1)$ et $(k - p)$ diviseurs élémentaires simples $(\lambda + 1)$.

Il existe donc $(k - p)$ systèmes

$$\beta_1^s, \beta_2^s, \ldots, \beta_k^s \qquad (s = 1, 2, \ldots, k - p)$$

linéairement distincts satisfaisant aux équations

$$\sum_{h=1}^{h=k} [\alpha_{hi} + (hi)] \beta_h^s = 0 \qquad (i = 1, 2, \ldots, k);$$

chacun d'eux donnera une relation linéaire et homogène entre les P. *Le nombre des formes T linéairement indépendantes est donc p.*

Nous avons supposé $|S - S'|$ différent de zéro; des considérations analogues conduiraient au résultat lorsque $|S + S'|$ n'est pas nul.

A. Voss[87]) montre que le même raisonnement permettrait d'établir que *le nombre des formes symétriques et alternées linéairement distinctes qui demeurent inaltérées par une substitution U, qui conserve une forme ordinaire S, est exactement égal au nombre des formes indépendantes P permutables avec U.**

61. Cas singulier. *Si l'on a à la fois

$$|S - S'| = 0, \quad |S + S'| = 0,$$

A. Voss part encore de l'identité

$$(T + T')(S + S') + (T' - T)(S' - S) = 0$$

qu'il écrit en multipliant à gauche par V^{-1}, à droite par V:

$$V^{-1}(T + T')(V')^{-1}V'(S + S')V + V^{-1}(T' - T)(V')^{-1}V'(S' - S)V = 0;$$

on y peut choisir V de façon que la forme symétrique $S + S'$, de rang r, soit transformée en

$$x_1 y_1 + x_2 y_2 + \cdots + x_r y_r = E_1,$$

$$V'(S + S')V = E_1.$$

Si l'on pose alors

$$V^{-1}T(V')^{-1} = t,$$

$$V'SV = s,$$

87) *A. Voss*, Abh. Akad. München 17 II. Teil (1890/1), p. 336.

on aura

$$(t+t')E_1+(t'-t)(s'-s)=0;$$

en observant que le second terme peut s'écrire

$$(t'-t)(s'-s)(E_1+E_2),$$

on aura, eu égard à la séparation des variables $x_1, y_1, \ldots, x_r, y_r$,

$$(t'-t)(s'-s)E_2=0, \qquad [(t+t')+(t'-t)(s'-s)]E_1=0.$$

La première égalité donne $n(n-r)$ équations linéaires pour la détermination des $\frac{n(n-1)}{2}$ coefficients de la forme alternée $(t'-t)$; la deuxième donne nr équations linéaires par rapport aux $\frac{n(n+1)}{2}$ coefficients de la forme symétrique $(t+t')$.*

62. Détermination des transformations automorphes de S quand le déterminant $|S+S'|$ n'est pas nul. *La méthode précédente conduit à une détermination élégante des transformations automorphes de S lorsque $E_1=E$ c'est-à-dire quand $|S+S'|$ n'est pas nul.

En posant

$$s'-s=\sigma,$$

on a l'équation

$$(t+t')+(t'-t)\sigma=0,$$

d'où l'on déduit pour $(t'-t)$

$$(t'-t)\sigma=\sigma(t'-t).$$

Toute forme X permutable avec σ donne inversement

$$t'-t=X'-X, \qquad t'+t=-(X'-X)\sigma,$$

d'où l'on déduira t.

Faisons l'hypothèse qu'*aucune racine de l'équation caractéristique de* σ,

$$|\sigma-\lambda E|=|V'|\,|S'-S-\lambda(S+S')|\,|V|=0,$$

n'annule tous ses mineurs du premier ordre. Si l'on a

$$|\sigma-\lambda E|=a_0+a_1\lambda+\cdots+a_n\lambda^n,$$

l'équation de moindre degré vérifiée par σ est

$$a_0\sigma^0+a_1\sigma+\cdots+a_n\sigma^n=0$$

et $\sigma^0, \sigma, \ldots, \sigma^{n-1}$ sont linéairement distinctes.

Comme σ est alternée, on a, si $n=2p$,

$$|\sigma-\lambda E|=a_0+a_2\lambda^2+\cdots+a_{2p}\lambda^{2p}$$

et l'équation en σ s'écrit

$$a_0\sigma+a_2\sigma^3+\cdots+a_{2p}\sigma^{2p+1}=0;$$

les formes alternées $\sigma, \sigma^3, \ldots, \sigma^{2p-1}$ sont en nombre $\frac{n}{2}$ et indépendantes.

Si $n=2p+1$, l'équation en λ s'écrit

$$|\sigma-\lambda E|=a_1\lambda+a_3\lambda^3+\cdots+a_{2p+1}\lambda^{2p+1}=0$$

et les seules formes alternées distinctes sont encore

$$\sigma, \sigma^3, \ldots, \sigma^{2p-1};$$

leur nombre est $p=\frac{n-1}{2}$.

Toutes les formes permutables avec σ et alternées sont ici [cf. nº **64**] comprises dans l'expression

$$b_1\sigma+b_3\sigma^3+\cdots+b_{2p-1}\sigma^{2p-1}$$

et *la solution générale de l'équation*

$$TS+T'S'=0$$

est donnée par les formules

$$V'(S+S')V=E,$$
$$T=VtV',$$
$$V'(S'-S)V=\sigma,$$
$$-2t=(b_1\sigma+b_3\sigma^3+\cdots+b_{2p-1}\sigma^{2p-1})(\sigma+E) \qquad (n=2p,\ 2p+1).$$

Des simplifications se présentent également dans la résolution de

$$TS+T'S'=0$$

quand S est décomposable. *A. Voss* a montré en particulier que, si

$$S=S_1+S_2$$

et si les équations

$$|S'_1-\lambda S_1|=0, \qquad |S_2'-\lambda S_2|=0$$

n'ont pas de racine commune, T est décomposable comme S.

On a vu plus haut que *L. Kronecker* a réduit par des transformations congruentes des deux séries de variables toute forme bilinéaire à une somme de formes irréductibles de divers types $(\alpha_1), \ldots, (\alpha_6)$. *A. Voss* indique le nombre de paramètres indépendants dont dépendent les transformations automorphes ordinaires pour chacune de ces formes irréductibles.

Pour la forme

α_2) $\qquad S=x_0y_1+\cdots+x_{2n-2}y_{2n-1}+c(x_1y_0+\cdots+x_{2n-1}y_{2n-2}),$

où c^2 est supposé différent de 1, si N est le nombre des couples de variables dans S, le nombre des paramètres homogènes indépendants dans la transformation automorphe est $\frac{N}{2}$ ou $\frac{N+1}{2}$ suivant que N est pair ou non; ce nombre est donc égal à n comme dans le cas général.

Pour les formes comprises dans l'expression

α_3) $\qquad S=(x_0y_1+x_1y_0)+(x_1y_2-x_2y_1)+(x_2y_3+x_3y_2)+\cdots$

à N couples de variables, la transformation automorphe renferme pour $N=4p$, $2(2p+1)$, $2p+1$ un nombre de paramètres égal à $4p$, $4p+1$, $p+1$.

De même si

$$\alpha_6)\qquad S = x_0y_1 - x_1y_0 + (x_1y_2 + x_2y_1) + x_2y_3 - x_3y_2 + \cdots,$$

le nombre des paramètres est

$$4p, \qquad 4p+3, \qquad p+1$$

suivant que

$$N=4p, \qquad 2(2p+1), \qquad 2p+1.$$

Enfin si l'on a $[\alpha_4, \alpha_5]$

$$S = x_0y_0 + (x_1y_0 - x_0y_1) + (x_2y_1 + x_1y_2) + (x_3y_2 - x_2y_3) + \cdots$$

le nombre des paramètres est exactement

$$\frac{N}{2} \text{ ou } \frac{N-1}{2}$$

suivant que N est pair ou non.

Il n'y a pas de difficulté à trouver pour une forme réduite à une somme de formes élémentaires le nombre des paramètres dont dépend sa transformation automorphe la plus générale. Si la forme n'est pas réduite, on ne sait pas actuellement la réduire par des opérations rationnelles[88]).*

63. Nombre des paramètres de la transformation automorphe la plus générale. $_*$*A. Voss* a indiqué une autre *détermination du nombre des paramètres qui figurent dans une transformation automorphe ordinaire de la forme quelconque S.*

Il existe toujours, P étant donné, une transformation S pour laquelle

$$SP'S^{-1} = P$$

puisque P' est semblable à P.

Si l'on connaît, S étant donné, une transformation P on peut admettre qu'elle est ordinaire puisque $P - \lambda E$ vérifie la même équation.

Supposons donc $|P|$ différent de zéro; l'équation

$$SP' = PS$$

permet d'écrire

$$PS' + \lambda SP' = P(S' + \lambda S),$$

et puisque les deux faisceaux équivalents sont ici formés de formes conjuguées, ils sont congruents. Il existe donc une substitution V pour laquelle

$$PS' + \lambda SP' = V'(S' + \lambda S)V$$

88) Cf. *C. Jordan*, J. math. pures appl. (4) 4 (1888), p. 349.

ou encore

$$PS' = V'S'V, \qquad SP' = V'SV.$$

L'équation initiale devient ainsi

$$VS^{-1}S' = S^{-1}S'V;$$

elle exprime que V *est permutable avec la forme antisymétrique* $S^{-1}S'$; on a d'ailleurs

$$P = V'S'V(S')^{-1}.$$

Toutes les solutions ordinaires de $SP' = PS$ sont données par la formule précédente.

Soient $P_1, P_2, \ldots, P_\mu$ les solutions indépendantes de

$$SP' = PS$$

dont le nombre est donné par la discussion d'un système d'équations linéaires; soient de même $V_1, V_2, \ldots, V_m$ les solutions indépendantes de

$$VS^{-1}S' = S^{-1}S'V$$

de telle sorte que

$$V = \beta_1V_1 + \cdots + \beta_mV_m.$$

On aura à chercher le nombre des formes distinctes $V'S'V$:

$$V'S'V = \sum_{(i,k)} \beta_i\beta_k(V_i'S'V_k + V_k'S'V_i).$$

En posant

$$Q_{ik} = V_i'S'V_k(S')^{-1},$$

ce qui donne

$$Q_{ik}S = SQ'_{ki},$$

on reconnaît aisément que la forme

$$R_{ik} = Q_{ik} + Q_{ki}$$

satisfait à l'équation

$$R_{ik}S = SR'_{ik}.$$

On peut donc poser

$$R_{ik} = \sum_{s=1}^{s=\mu} r_{iks}P_s$$

($r_{iks} = r_{kis}$ étant des coefficients numériques), d'où l'on conclut

$$P = \sum_{s=1}^{s=\mu} \alpha_sP_s = \sum_{(i,k)} \beta_i\beta_kr_{iks}P_s \qquad (i, k = 1, 2, \ldots, m),$$

puis, à cause de l'indépendance des P,

$$\alpha_s = \sum_{(i,k)} \beta_i\beta_kr_{iks} \qquad (s = 1, 2, \ldots, \mu).$$

Ces équations renferment effectivement toutes les inconnues β; par exemple $V'S'V$ renferme en β_i^2 le seul terme $\beta_i^2 V_i' S' V_i$.

Comme on peut choisir arbitrairement les α, sans cesser d'avoir pour les β un système compatible, *on a bien μ relations distinctes entre les β quand les α sont fixés.* Le nombre des arbitraires qui figurent dans V, après fixation de P, est donc $(m-\mu)$.

Ce nombre est aussi celui des paramètres que renferme la transformation automorphe la plus générale de S.

Si l'on a en effet

$$U'SU = S \quad \text{d'où} \quad U'S'U = S',$$

on en déduit, en éliminant U'

$$S^{-1}S'U = US^{-1}S'$$

et l'on peut poser

$$U = \beta_1 V_1 + \beta_2 V_2 + \cdots + \beta_m V_m.$$

Pour déterminer les β, on doit avoir, par exemple,

$$U'S'U = S'.$$

Donc si l'on pose

$$U'S'U = PS',$$

P est déterminé et égal à E; mais cette fonction P satisfait d'après ce qu'on a vu à

$$SP' = PS.$$

Les β en nombre m sont donc assujettis à μ conditions distinctes; il reste $(m-\mu)$ paramètres homogènes indépendants.

Exemples: Si S est symétrique, $S^{-1}S' = E$, donc $m = n^2$. Le nombre des formes distinctes P pour lesquelles

$$SP' = PS$$

est $\frac{n(n+1)}{2}$, puisqu'il faut et suffit pour cela que PS soit symétrique. Donc

$$m - \mu = \frac{n(n-1)}{2}.$$

Si S est alternée on a de même $m = n^2$, $\mu = \frac{n(n-1)}{2}$ puisqu'il faut et suffit que PS soit alterné; donc

$$m - \mu = \frac{n(n+1)}{2}.$$

A. Voss établit en outre que ce nombre $(m-\mu)$ est encore celui des paramètres indépendants qui figurent dans les transformations automorphes non singulières qu'on peut obtenir par résolution de

$$TS + T'S' = 0.$$

64. Formes semblables et formes permutables. La détermination des transformations automorphes non singulières d'une forme ordinaire S se ramène à celle des formes permutables avec $S^{-1}S'$. Avant d'étudier la résolution de l'équation plus générale

$$AX = XB,$$

où A et B sont donnés, c'est-à-dire la *détermination des transformations qui changent une forme B à variables contragrédientes en une forme semblable A,* nous ferons quelques remarques sur les formes semblables.

Les identités évidentes

$$P^{-1}ABP = P^{-1}AP \cdot P^{-1}BP,$$
$$P^{-1}(aA + bB) = P^{-1}aAP + P^{-1}bBP$$

montrent que, pour toute fonction entière $f(A, B)$,

$$P^{-1}f(A, B)P = f(P^{-1}AP, P^{-1}BP).$$

En particulier, si $B = P^{-1}AP$, on aura

$$\psi(B) = P^{-1}\psi(A)P = 0;$$

toutes les formes semblables à A vérifient la même équation de moindre degré

$$\psi(B) = 0.$$

Nous savons d'ailleurs que la condition nécessaire et suffisante d'une identité $B = X^{-1}AX$ est que les faisceaux $\lambda E - A$, $\lambda E - B$ possèdent les mêmes diviseurs élémentaires ou encore les mêmes produits élémentaires. Si A est *irréductible,* c'est-à-dire n'est ni décomposable ni semblable à une forme décomposable, le faisceau $\lambda E - A$ n'a qu'un diviseur élémentaire; donc

$$|\lambda E - A| = (\lambda - a)^n,$$

les mineurs du premier ordre de $|\lambda E - A|$ n'admettant pas le diviseur commun $(\lambda - a)$. L'équation de moindre degré vérifiée par A est

$$(aE - A)^n = 0.$$

La forme $(aE - A)^k$ est réductible, si $k > 1$.

Pour que la forme $f(A)$, où f est rationnel, soit irréductible il faut et il suffit ou que $n = 1$, ou que, pour $n > 1$, $f'(a)$ ne s'annule pas; alors

$$|\lambda E - f(A)| = (\lambda - f(a))^n.$$

Toute forme A peut être réduite par une transformation convenable à une somme de formes irréductibles

$$P^{-1}AP = A_1 + A_2 + \cdots;$$

on a donc aussi

$$P^{-1}f(A)P = f(A_1) + f(A_2) + \cdots,$$

où la forme du second membre est réduite lorsque $f'(\lambda)$ ne s'annule pour aucune racine multiple de $|\lambda E - A| = 0$ et ne l'est que dans ce cas.

Soit maintenant à résoudre de la manière la plus générale l'équation

$$AX = XB;$$

si l'on en connaît une solution particulière P, il suffira de poser $X = PY$ pour avoir

$$APY = PYB = PBY$$

c'est-à-dire

$$YB = BY;$$

on est donc ramené à chercher les formes permutables avec B.

Mais si $|R|$ est différent de zéro, on peut remplacer $YB = BY$ par

$$R^{-1}YR \cdot R^{-1}BR = R^{-1}BR \cdot R^{-1}YR$$

et réciproquement: on profitera de l'indétermination de R pour ramener B à une somme de formes irréductibles (forme de Weierstrass)

$$R^{-1}BR = \mathsf{B}_1,$$

et si l'on pose

$$R^{-1}YR = \Upsilon_1, \quad \text{d'où} \quad Y = R\Upsilon_1 R^{-1},$$

on n'a plus qu'à *déterminer les formes* Υ_1 *permutables avec une forme réduite* B_1.

Les équations *linéaires* qui définissent les coefficients de Υ_1 peuvent être étudiées sans difficulté. La solution précédente fait appel à la réduction de B à une somme de formes irréductibles, c'est-à-dire à des opérations irrationnelles. On peut cependant déterminer les solutions de $AX = XB$ par des opérations rationnelles, puisque les équations qui déterminent les coefficients de X sont linéaires.

Voici un moyen élégant d'y parvenir.

On a vu [n° **30**] que la méthode de réduction due à *L. Kronecker* permet de déterminer par des opérations rationnelles deux formes S et U entières en λ et dont le déterminant *indépendant de* λ peut être supposé égal à 1, de manière à avoir

$$S\mathsf{A}U = D,$$

où l'on a posé $\mathsf{A} = \lambda E - A$ et où D désigne la forme attachée à un tableau diagonal, qu'on peut écrire

$$D = \Delta_1 x_1 y_1 + \cdots + \Delta_\nu x_\nu y_\nu + x_{\nu+1} y_{\nu+1} + \cdots + x_n y_n$$

dans l'hypothèse où les produits élémentaires du déterminant

$$|\lambda E - A| = \varphi(\lambda)$$

sont respectivement

$$\frac{\varphi(\lambda)}{D_{n-1}} = E_n = \Delta_1, \quad \frac{D_{n-1}}{D_{n-2}} = E_{n-1} = \Delta_2, \ldots, \quad \frac{D_{n-\nu+1}}{D_{n-\nu}} = E_{n-\nu+1} = \Delta_\nu,$$

$$D_{n-\nu} = E_{n-\nu} = 1, \ldots, D_1 = E_1 = 1,$$

c'est-à-dire où les mineurs d'ordre ν de $|\lambda E - A|$ ont pour plus grand commun diviseur l'unité.

On peut de même déterminer T et V de façon que

$$T\mathsf{B}V = D \quad \text{où} \quad \mathsf{B} = \lambda E - B$$

et l'on a par suite

$$\mathsf{A}UV^{-1} = S^{-1}T\mathsf{B},$$

où V^{-1} et S^{-1} sont, d'après $|V| = |S| = 1$, des fonctions entières de λ. En faisant les divisions

$$UV^{-1} = X_1\mathsf{B} + X,$$

$$ST^{-1} = \mathsf{B}Y_1 + Y,$$

on trouve les deux formes X et Y, à coefficients indépendants de λ, qui satisfont à l'identité en λ

$$\mathsf{A}X = Y\mathsf{B},$$

d'où l'on conclut $Y = X$. Toutes les solutions X s'obtiennent en prenant une solution V déterminée et une solution U arbitraire.

Ces formes X à coefficients indépendants de λ peuvent être construites directement[89]).

Soit U une solution de

$$\mathsf{A}U = S^{-1}D$$

définie par

$$U = \sum_{(i,k)} u_{ik} x_i y_k, \quad S^{-1} = \sum_{(i,k)} \sigma_{ik} x_i y_k;$$

on aura pour déterminer les u_{ik} le système

$$\sum_{k=1}^{k=n} (\lambda\varepsilon_{ik} - a_{ik}) u_{kl} = \sigma_{il}\Delta_l \qquad \begin{array}{l}(i = 1, 2, \ldots, n)\\(l = 1, 2, \ldots, \nu)\end{array}$$

$$\sum_{k=1}^{k=n} (\lambda\varepsilon_{ik} - a_{ik}) u_{kl} = \sigma_{il} \qquad \begin{array}{l}(i = 1, 2, \ldots, n)\\(l = \nu+1, \ldots, n)\end{array}$$

et l'on voit que les u_{kl}, où l dépasse ν, peuvent être pris arbitrairement.

Si $W = U\Omega$ désigne une autre solution, conduisant à

$$\mathsf{A}U\Omega = R^{-1}D,$$

89) *Cf. *G. Landsberg*, J. reine angew. Math. 116 (1896), p. 331.*

on aura

$$D\Omega = SR^{-1}D$$

et en posant

$$\Omega = \sum_{(i,\,k)} \omega_{ik} x_i y_k, \quad SR^{-1} = \sum_{(i,\,k)} f_{ik} x_i y_k$$

les équations qui déterminent les ω_i sont simplement:

$$\begin{aligned} \omega_{ik}\Delta_i &= f_{ik}\Delta_k \qquad (i < \nu,\ k < \nu),\\ \omega_{ik} &= f_{ik}\Delta_k \qquad (i > \nu,\ k < \nu),\\ \omega_{ik}\Delta_i &= f_{ik} \qquad (i < \nu,\ k > \nu),\\ \omega_{ik} &= f_{ik} \qquad (i > \nu,\ k > \nu). \end{aligned}$$

On en conclut, si $k \leqq \nu$, que les $\omega_{1k}, \omega_{2k}, \ldots, \omega_{kk}$ sont arbitraires, les $\omega_{(k+1)k}, \ldots, \omega_{\nu k}$ sont respectivement divisibles par $\frac{\Delta_k}{\Delta_{k+1}}, \ldots, \frac{\Delta_k}{\Delta_\nu}$, enfin les $\omega_{(\nu+1)k}, \ldots, \omega_{nk}$ sont tous divisibles par Δ_k. Pour $k > \nu$, les ω_{ik} sont toujours arbitraires.

Mais le système des équations qui déterminent les coefficients u_{ik} de U dans

$$\mathsf{A}U = S^{-1}D$$

possède toujours des solutions telles que les u_{kl} soient de degré inférieur à celui de Δ_l pour $l \leqq \nu$ et des constantes nulles pour $l > \nu$. Pour ces solutions les σ_{il} sont tous constants, donc S^{-1} *et par suite* S *ont leurs coefficients indépendants* de λ.

Si l'on suppose V choisi de même, de façon à vérifier

$$T\mathsf{B}V = D,$$

T aura aussi ses coefficients indépendants de λ et cela sera encore vrai de $S^{-1}T = X$.

L'équation $\mathsf{A}UV^{-1} = X\mathsf{B}$ prouve alors que UV^{-1} est indépendant de λ et par suite égal à X. Toutes les solutions X peuvent évidemment être obtenues ainsi.

Si nous considérons l'expression la plus générale de U, désignée par

$$W = U\Omega = \sum_{(i,\,k)} w_{ik} x_i y_k, \quad w_{ik} = \sum_{l=1}^{l=n} u_{il}\,\omega_{ik} \qquad (i, k = 1, \ldots, n)$$

il faudra réduire pour $k \leqq \nu$, w_{ik} au degré $(\delta_k - 1)$, δ_k désignant le degré de Δ_k, et prendre pour les autres w_{ik}, où $k > \nu$, des constantes nulles. L'expression de w_{ik}, où $k \leqq \nu$, renfermera donc, eu égard au calcul des ω_{ik},

$$k\delta_k + \delta_{k+1} + \delta_{k+2} + \cdots + \delta_\nu$$

La fin de l'article n'a pas été publiée en raison de la guerre.

Paul DU BOIS-REYMOND
• ▭ *Théorie générale des fonctions*

Jean-Baptiste DUMAS
• ▭ *Leçons sur la philosophie chimique*

Ernest DUPORCQ
• ▭ *Premiers principes de géométrie moderne*

Paul DUPUY
• *La vie d'Évariste Galois*

ENCYCLOPÉDIE DES SCIENCES MATHÉMATIQUES PURES ET APPLIQUÉES
Tout ce qui a paru de l'édition française rédigée et publiée d'après l'édition allemande sous la direction de Jules MOLK.
• ▭ *Arithmétique et Algèbre*
• ▭ *Analyse*
• ▭ *Géométrie*
• ▭ *Mécanique*
• ▭ *Physique*
• ▭ *Géodésie et Géophysique*
• ▭ *Astronomie*
• ▭ *Compléments*

F. G.-M. (Frère GABRIEL-MARIE)
• ▭ *Exercices de géométrie*
comprenant l'exposé des méthodes géométriques et 2.000 questions résolues
• ▭ *Exercices de géométrie descriptive*

Pierre FERMAT
• *Précis des Œuvres mathématiques et de l'Arithmétique de Diophante*, par Émile BRASSINNE

J. FITZ-PATRICK
• ▭ *Exercices d'arithmétiques*

Joseph FOURIER
• *Théorie analytique de la chaleur*

Maurice FRÉCHET
• *Les espaces abstraits*

Augustin FRESNEL
• *Mémoire sur la diffraction de la lumière*

Évariste GALOIS
• *Œuvres mathématiques*
suivies de
— *Influence de Galois sur le développement des mathématiques*, par Sophus LIE

Félix R. GANTMACHER
• *Théorie des matrices*

Carl Friedrich GAUSS
• *Recherches arithmétiques*

Francisco GOMES TEIXEIRA
• *Traité des courbes spéciales planes et gauches (3 tomes)*

Édouard GOURSAT
• ▭ *Cours d'Analyse mathématique (3 tomes)*

Édouard GRIMAUX
• ▭ *Lavoisier, 1743-1794*
d'après sa correspondance, ses manuscrits, ses papiers de famille et d'autres documents inédits

Jacques HADAMARD
• *Leçons de géométrie élémentaire (2 tomes)*
• *Essai sur la psychologie de l'invention dans le domaine mathématique*
suivi de
— *L'Invention mathématique*, par Henri POINCARÉ

Paul R. HALMOS
• *Introduction à la théorie des ensembles*

G. H. HARDY
• *Divergent Series* (en anglais)

Werner HEISENBERG
• *Les principes physiques de la théorie des quanta*

Hermann von HELMHOLTZ
• *Optique physiologique (2 tomes)*
• *Théorie physiologique de la musique*

David HILBERT
• *Sur les problèmes futurs des mathématiques (Les 23 Problèmes)*
• *Théorie des corps de nombres algébriques*

Camille JORDAN
• *Traité des substitutions et des équations algébriques*
• ▭ *Cours d'Analyse de l'École Polytechnique (3 tomes)*

Erich KAMKE
• *Théorie des ensembles*

Stephen C. KLEENE
• *Logique mathématique*

Félix KLEIN
• *Le programme d'Erlangen*

Casimir KURATOWSKI
• ▭ *Topologie I et II*

Jean LADRIÈRE
• ▭ *Les limitations internes des formalismes*
Étude sur la signification du théorème de Gödel et des théorèmes apparentés dans la théorie des fondements des mathématiques

Joseph-Louis LAGRANGE
• *Mécanique analytique*

Trajan LALESCO
• *La géométrie du triangle*

Pierre-Simon LAPLACE
• *Théorie analytique des probabilités (2 tomes)*
Le premier tome contient le célèbre *Essai philosophique sur les probabilités*

Pierre LAROUSSE
• ▭ *Jardin des racines grecques* (Livre du Maître)
suivi de
— *Jardin des racines latines* (Livre du Maître)

Antoine-Laurent LAVOISIER
• ▭ *Traité élémentaire de chimie*

Henri LEBESGUE
• *Leçons sur l'intégration et la recherche des fonctions primitives*
• *Les coniques*
• *Leçons sur les constructions géométriques*

C. LEBOSSÉ & C. HÉMERY
• *Géométrie (classe de Mathématiques)*

Julien LEMAIRE
• ▭ *Étude élémentaire de l'hyperbole équilatère et de quelques courbes dérivées*
suivie de
— *Hypocycloïdes et épicycloïdes*

Tullio LEVI-CIVITA
• *Caractéristiques des systèmes différentiels et propagation des ondes*

Paul LÉVY
• ▭ *Calcul des probabilités*
• ▭ *Processus stochastiques et mouvement brownien*
• ▭ *Théorie de l'addition des variables aléatoires*
• ▭ *Problèmes concrets d'analyse fonctionnelle*

Alexandre LIAPOUNOFF
• *Problème général de la stabilité du mouvement*

André LICHNEROWICZ
• *Éléments de calcul tensoriel*

Ernst LINDELÖF
• *Le calcul des résidus et ses applications à la théorie des fonctions*

Gérard de LONGCHAMPS
• ▭ *Cours de problèmes de géométrie analytique (3 tomes)*

Hendrik-Antoon LORENTZ
• ▭ *The Theory of Electrons and its Applications to the Phenomena of Light and Radiant Heat* (en anglais)

Édouard LUCAS
• ▭ *Théorie des nombres*

Nicolas LUSIN
• ▭ *Leçons sur les ensembles analytiques et leurs applications*
suivies du Mémoire
— *Sur les fonctions représentables analytiquement,*
par Henri LEBESGUE

Ernst MACH
• *La Mécanique*
Exposé historique et critique de son développement

James Clerk MAXWELL
• *Traité d'Électricité et de Magnétisme (2 tomes)*

Émile MEYERSON
• ▭ *La déduction relativiste*

Charles MICHEL
• ▭ *Compléments de géométrie moderne*
suivis du recueil des solutions des questions proposées
— *Exercices de géométrie moderne,* par Julien LEMAIRE

Abraham de MOIVRE
• *The Doctrine of Chances* (en anglais)

Gaspard MONGE
• *Géométrie descriptive.*
• *Feuilles d'analyse appliquée à la géométrie*

Pierre Rémond de MONTMORT
• *Essai d'analyse sur les jeux de hasard*

John von NEUMANN
• *Les fondements mathématiques de la Mécanique quantique*

Isaac NEWTON
• *Principes mathématiques de la philosophie naturelle (2 tomes)*

R. NOGUÈS
• ▭ *Théorème de Fermat. Son histoire*

Georges PAPELIER
• ▭ *Exercices de géométrie moderne précédés de l'exposé élémentaire des principales théories*
l'ouvrage comprend
I. Géométrie dirigée
II. Transversales
III. Division et faisceau harmonique
IV. Pôles, polaires, plans polaires, dans le cercle et la sphère
V. Rapport anharmonique
VI. Inversion
VII. Homographie
VIII. Involution
IX. Géométrie projective. Application aux coniques
• ▭ *Éléments de Trigonométrie sphérique*

Julius PETERSEN
• *Méthodes et théories pour la résolution des problèmes de constructions géométriques*

Émile PICARD
• ▭ *Traité d'Analyse (3 tomes)*
• ▭ *Leçons sur quelques types simples d'équations aux dérivées partielles*
suivies de
— *Leçons sur quelques équations fonctionnelles*
— *Leçons sur quelques problèmes aux limites de la théorie des équations différentielles*
— *Quelques applications analytiques de la théorie des courbes et des surfaces algébriques*

Johann Christian POGGENDORFF
• ▭ *Histoire de la physique*

Henri POINCARÉ
• *Calcul des probabilités*
• *La Mécanique nouvelle (Théorie de la Relativité)*
• *Théorie du potentiel newtonien*
• *Théorie des tourbillons*
• *Figures d'équilibre d'une masse fluide*
• *Électricité et Optique*
• ▭ *Théorie mathématique de la lumière*

Siméon-Denis POISSON
• *Recherches sur la probabilité des jugements en matière criminelle et en matière civile*

George POLYA
• *Comment poser et résoudre un problème*

Alfred RÉNYI
• ▭ *Calcul des probabilités*
avec un appendice sur la théorie de l'information

Bernhard RIEMANN
• *Œuvres mathématiques*

F. RIESZ & B. SZ.-NAGY
• *Leçons d'analyse fonctionnelle*

Erwin SCHRÖDINGER
• *Mémoires sur la Mécanique ondulatoire*

Joseph-Alfred SERRET
• ▭ *Cours d'Algèbre supérieure (2 tomes)*
• ▭ *Traité de Trigonométrie rectiligne et sphérique*

Waclaw SIERPINSKI
• *250 problèmes de théorie élémentaire des nombres*
• ▭ *Leçons sur les nombres transfinis*

G. SINGIER
• ▭ *Les correspondances algébriques (1,1), (2,1), (2,2)*
Applications aux courbes et aux surfaces du deuxième et du troisième degré

Jean-Marie SOURIAU
• ▭ *Calcul linéaire*
La solution détaillée des exercices termine l'ouvrage

Paul TANNERY
• *Pour l'histoire de la science hellène*
• *La géométrie grecque*

François-Félix TISSERAND
• *Traité de Mécanique céleste (4 tomes)*
suivi de
— *Leçons sur la détermination des orbites*

Georges VALIRON
• *Équations fonctionnelles – Applications*

Vito VOLTERRA
• *Leçons sur la théorie mathématique de la lutte pour la vie*

ÉDITIONS JACQUES GABAY

RÉIMPRESSIONS

Niels Henrik ABEL
• *Œuvres complètes (2 tomes)*
suivies de
— *Niels Henrik Abel – Sa vie et son action scientifique,* par C.-A. BJERKNES

Jean D'ALEMBERT
• *Traité de dynamique*

André-Marie AMPÈRE
• *Théorie mathématique des phénomènes électro-dynamiques*
• *Considérations sur la théorie mathématique du jeu*

Paul APPELL
• ▭ *Traité de Mécanique rationnelle (5 tomes en 3 vol.)*

Louis BACHELIER
• *Calcul des probabilités*
• *Les lois des grands nombres du calcul des probabilités*
suivies de
— *La spéculation et le calcul des probabilités*
— *Les nouvelles méthodes du calcul des probabilités*
• ▭ *Le Jeu, la Chance et le Hasard*
• *Collection de Mémoires*
titres inclus
— *Théorie de la spéculation*
— *Théorie mathématique des jeux*
— *Théorie des probabilités continues*
— *Les probabilités à plusieurs variables*
— *Mouvement d'un point ou d'un système soumis à l'action des forces dépendant du hasard*
— *Les probabilités cinématiques et dynamiques*

René BAIRE
• *Théorie des nombres irrationnels, des limites et de la continuité*

W. W. Rouse BALL
• ▭ *Récréations mathématiques*
• ▭ *Histoire des mathématiques*

Stefan BANACH
• ▭ *Théorie des opérations linéaires*

Paul BARBARIN
• *La Géométrie non euclidienne*

Edmond BAUER
• *Introduction à la théorie des groupes et à ses applications à la physique quantique*

Jacques BERNOULLI
• *L'art de conjecturer*
Cette première partie de l'*Ars Conjectandi* (la traduction française des parties 2, 3 et 4 n'a jamais paru) contient le célèbre *Traité de la manière de raisonner dans les jeux de hasard,* par Christiaan HUYGENS

Joseph BERTRAND
• ▭ *Calcul des probabilités*

Marcel BOLL
• ▭ *La chance et les jeux de hasard*
• ▭ *Le mystère des nombres et des formes*

Ludwig BOLTZMANN
• *Leçons sur la théorie des gaz*

Émile BOREL
• *Leçons sur les séries divergentes*

Émile BOREL & André CHÉRON
• ▭ *Théorie mathématique du bridge à la portée de tous*
suivie de
— *Applications de la théorie des probabilités aux jeux de hasard,* par Émile BOREL & Jean VILLE
— *Valeur pratique et philosophie des probabilités,* par Émile BOREL

Pierre BOUTROUX
• ▭ *L'idéal scientifique des mathématiciens*

Léon BRILLOUIN
• *Les tenseurs en mécanique et en élasticité*
• *La science et la théorie de l'information*

Louis de BROGLIE
• *Ondes et mouvements*

Georg CANTOR
• *Sur les fondements de la théorie des ensembles transfinis*

Sadi CARNOT
• *Réflexions sur la puissance motrice du feu*

Élie CARTAN
• *Leçons sur la géométrie des espaces de Riemann*
• ▭ *Leçons sur la géométrie projective complexe*
suivies de
— *La théorie des groupes finis et continus et la géométrie différentielle traitées par la méthode du repère mobile*
— *Leçons sur la théorie des espaces à connexion projective*

Augustin-Louis CAUCHY
• *Analyse algébrique*

Michel CHASLES
• *Aperçu historique sur l'origine et le développement des méthodes en géométrie*
• *La dualité et l'homographie*
• *Rapport sur les progrès de la géométrie*

Rudolph CLAUSIUS
• ▭ *Théorie mécanique de la chaleur*

H. COMMISSAIRE & G. CAGNAC
• *Cours de Mathématiques spéciales (3 tomes)*

Antoine-Nicolas de CONDORCET
• *Essai sur l'application de l'analyse à la probabilité des décisions rendues à la pluralité des voix*

Gaspard-Gustave CORIOLIS
• *Théorie mathématique des effets du jeu de billard*
suivie des deux célèbres Mémoires
— *Sur le principe des forces vives dans les mouvements relatifs des machines*
— *Sur les équations du mouvement relatif des systèmes de corps*

Gaston DARBOUX
• ▭ *Leçons sur la théorie générale des surfaces et les applications géométriques du calcul infinitésimal (4 tomes)*
• ▭ *Leçons sur les systèmes orthogonaux et les coordonnées curvilignes*
• ▭ *Principes de géométrie analytique*

R. DELTHEIL & D. CAIRE
• *Géométrie*
suivie de
— *Compléments de géométrie*

G. DEMARTRES
• ▭ *Cours de géométrie infinitésimale*

René DESCARTES
• *La Géométrie*

Paul A.M. DIRAC
• *Les principes de la Mécanique quantique*

▭ = ▭blong®

(Suite à l'intérieur)

Diffusion-Distribution : JACQUES GABAY

ISBN 2-87647-101-9
ISSN 0989-0602