Cryptographie

Mathématiques

par **Guy CHASSÉ**
Maître-Assistant de mathématiques
École des Mines de Nantes

*On peut grossièrement définir la **cryptographie** comme un ensemble de techniques visant à assurer la sécurité des communications. Un examen rapide de cette sécurité révèle qu'elle peut se présenter sous deux formes assez distinctes suivant les menaces dont on cherche à se prémunir.*

■ *Si une entité A envoie un message à une entité B et cherche à rendre inutile l'interception du message à quiconque n'est pas B, le service recherché est celui de la **confidentialité** : il s'agit de rendre inopérante une **attaque passive** (écoute téléphonique, ouverture de courrier). La réponse à ce besoin repose sur l'utilisation d'un **algorithme de chiffrement**.*

■ *Reprenons la même configuration. A envoie un message à B, mais on ne se préoccupe plus maintenant de confidentialité ; on veut que B puisse avoir l'assurance de la provenance de l'information qu'il reçoit, de son authenticité. On veut*

*empêcher une **attaque active**, par exemple un ajout d'information pendant que celle-ci transite sur la ligne de communication. Il existe toute une famille de besoins de ce type. On veut être sûr de l'**intégrité** des données transmises, ou bien on veut s'assurer de l'identité de l'expéditeur (de l'authenticité de la carte bancaire et de son possesseur qui retire de l'argent dans un distributeur par exemple. Il s'agit d'un problème d'**authentification** ou d'**identification**. Si l'on veut encore aller plus loin en requérant une « preuve » de l'identité de l'expéditeur, on peut avoir besoin d'une **signature**.*

C'est surtout le premier type de besoin qui a prévalu pendant des siècles entiers (confidentialité). Les utilisateurs de la cryptographie étaient alors exclusivement les militaires et les diplomates. Aujourd'hui, les échanges bancaires ont atteint un volume impressionnant ; l'usage du courrier électronique et le commerce électronique se développent et, d'une manière générale, l'informatique bouleverse les moyens de communication. Si les utilisateurs traditionnels de la cryptographie voient aussi leurs besoins s'accroître, ils perdent néanmoins le monopole (ce qui n'est pas toujours sans difficultés, les moyens de cryptographie relevant de la législation des armements dans le nombreux pays) et d'autres domaines font appel à la cryptographie. Les besoins du second type cité (authentification, signature) sont peut-être les plus cruciaux pour ces applications « civiles ».

*L'article « **Cryptographie** » fait l'objet de deux fascicules :*

AF 172 Mathématiques

AF 173 Algorithmes

Les sujets ne sont pas indépendants les uns des autres.

Le lecteur devra assez souvent se reporter à l'autre fascicule.

1. Évolution de la cryptographie et vocabulaire

Une introduction à la cryptographie, montrant quelques épisodes de son évolution, est certainement très instructive ; c'est pourquoi nous allons commencer par citer quelques méthodes employées au cours des siècles pour préserver le secret des communications.

1.1 Cryptographie avant l'informatique

1.1.1 Algorithme de César

Les historiens de l'Antiquité (Hérodote, Thucydide…) donnent déjà quelques indications sur des formes d'écritures secrètes utilisées à leurs époques. Le premier usage attesté (à des fins politiques) de ce type de technique est rapporté par l'historien romain Suétone affirmant que César communiquait avec ses amis (notamment Cicéron) à l'aide d'un procédé que nous allons décrire et auquel nous donnerons le nom de chiffre (ou algorithme) de César.

Le but est de transmettre, de manière confidentielle, un message écrit dans une langue alphabétique donnée. Nous supposerons qu'il s'agit de l'alphabet « latin » (en faisant une entorse fréquente à l'histoire consistant à ajouter quelques lettres à celui de César) usuel de 26 lettres donné « dans l'ordre alphabétique » : A B C … Y Z.

Le **procédé de César** consiste à opérer sur cet alphabet ordonné une **permutation circulaire** d'un nombre de positions, que nous notons k, compris entre 0 et 25 et à remplacer chaque lettre du message par la lettre qui intervient k positions plus loin dans la suite alphabétique (supposée faire succéder A à Z quand on est arrivé à la fin, d'où le mot circulaire). Par exemple si $k = 3$, la seconde ligne du tableau suivant donne la lettre correspondant à celle de première ligne sur la même colonne.

A	B	C	D	E	F	G	H	I	J	K	L	M
D	E	F	G	H	I	J	K	L	M	N	O	P
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Ainsi au lieu d'expédier le message :

« HELLO »,

César aurait envoyé :

« KHOOR ».

Le destinataire n'a plus qu'à faire l'opération inverse : pour chaque lettre du message reçu, la chercher dans la seconde ligne du tableau, puis la remplacer par la lettre immédiatement au-dessus dans la première ligne.

On pourrait évidemment perfectionner ce système sans en changer le principe en faisant intervenir, en plus de ces 26 lettres, la distinction capitale-minuscule, les caractères accentués, les signes de ponctuation, les caractères « blanc » qui sépare deux mots…

Une façon plus « **numérique** » de décrire les choses consiste à considérer que le message n'est pas composé de lettres, mais de nombres entre 0 et 25 en assimilant la lettre A au nombre 0, la lettre B au nombre 1, …, la lettre Y au nombre 24 et enfin la lettre Z au nombre 25. On peut alors représenter la rotation circulaire de la suite alphabétique de k positions comme l'addition à chacune des lettres de k modulo 26. Le tableau précédent se traduit par le suivant.

0	1	2	3	4	5	6	7	8	9	10	11	12
3	4	5	6	7	8	9	10	11	12	13	14	15
13	14	15	16	17	18	19	20	21	22	23	24	25
16	17	18	19	20	21	22	23	24	25	0	1	2

Rappelons que, lorsque l'on fait des opérations sur des entiers modulo un entier n (au moins égal à deux pour que cela ait vraiment un intérêt), on utilise les tables habituelles (de multiplication, d'addition, celle de division n'ayant pas toujours d'équivalent), mais on ne garde du résultat que son reste dans la division par n, c'est-à-dire un entier qui peut varier entre 0 et $n - 1$.

Du point de vue des mathématiques, l'ensemble des restes dans la division par n, que l'on peut noter :

$$\mathbb{Z}/n\mathbb{Z} = \{0, 1, \ldots, n - 1\},$$

muni de l'addition a une structure de groupe ; si l'on y adjoint la multiplication, on obtient une structure d'anneau.

Voici, à titre d'exemple, la table d'addition du groupe $\mathbb{Z}/26\mathbb{Z}$, c'est-à-dire des entiers modulo 26 (tableau **1**). Les éléments du groupe sont écrits dans le tableau en gras sur la première ligne et la première colonne. A l'intersection de la colonne correspondant à l'élément i de la première ligne et de la ligne correspondant à l'élément j de la première colonne on a placé l'élément $i + j$ de $\mathbb{Z}/26\mathbb{Z}$.

Tableau 1 – Table d'addition du groupe $\mathbb{Z}/26\mathbb{Z}$

+	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**
0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0
2	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1
3	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2
4	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2	3
5	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2	3	4
6	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2	3	4	5
7	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2	3	4	5	6
8	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2	3	4	5	6	7
9	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2	3	4	5	6	7	8
10	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9
11	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10
12	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11
13	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12
14	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13
15	15	16	17	18	19	20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
16	16	17	18	19	20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
17	17	18	19	20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
18	18	19	20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
19	19	20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
20	20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
21	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
22	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
23	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
24	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
25	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24

1.1.2 Substitutions et transpositions

Dans le jargon cryptologique, l'algorithme de César présenté paragraphe 1.1.1 est un exemple d'**algorithme de substitution** : on substitue une lettre à une autre. Dans un langage plus mathématique, on utilise une permutation circulaire de l'ensemble des lettres de l'alphabet.

Un autre procédé classique a reçu le nom de **transposition** en cryptographie (mais qu'il ne faut pas confondre avec la transposition des mathématiciens désignant une permutation échangeant deux lettres et laissant toutes les autres invariantes). Le procédé cryptographique de transposition consiste à décomposer le message en des blocs de longueur fixée d et ensuite à permuter les lettres de ce bloc. Il faut donc choisir un entier d et une permutation opérant sur d lettres.

Par exemple, choisissons $d = 4$ et la permutation (notée à la manière des cryptographes, « inverse » de celle communément utilisée par les mathématiciens) :

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

ce qui signifie que l'on transforme le bloc de quatre lettres en un nouveau bloc de même longueur dont :

— la première lettre sera la quatrième lettre du premier bloc ;
— la seconde lettre sera la troisième lettre du premier bloc ;
— la troisième lettre sera la première lettre du premier bloc ;
— la quatrième lettre sera la seconde lettre du premier bloc.

Précisément, le message

NOUS ARRIVONS

sera d'abord découpé en trois blocs

NOUS ARRI VONS

qui deviennent respectivement

SUNO IRAR SNVO

d'où le message envoyé

SUNO IRARSNVO

si l'on veut respecter les blancs séparant les mots.

1.1.3 De Vigenère à Kasiski. Statistiques des lettres de l'alphabet

Au seizième siècle, un algorithme a été conçu par **Vigenère**. Il porte son nom et est en quelque sorte une généralisation du procédé de substitution ; on dit qu'il s'agit d'un chiffre **polyalphabétique**. Le message est divisé en blocs de longueur d et on a besoin de d nombres entiers (entre 0 et 25) que l'on note $k_1, k_2, \ldots, k_d$. La première lettre du bloc sera remplacée en utilisant le procédé de César avec le décalage k_1, la seconde lettre du bloc sera remplacée en utilisant le procédé de César avec le décalage k_2, etc., jusqu'à la dernière lettre du bloc qui sera transformée en utilisant le procédé de César avec le décalage k_d.

Choisissons $d = 3$, $(k_1, k_2, k_3) = (7, 0, 12)$ et supposons que l'on veuille transmettre le message :

« **TO BE OR NOT TO BE** »

on enverra alors :

« **AO NL OD UOF AO NL** »

Le découpage du message est ici :

TOB EOR NOT TOB E

Chaque bloc se transforme alors (avec la convention citée paragraphe 1.1.1, consistant à identifier A et 0, B et 1, …, Z et 25) en ajoutant modulo 26 le triplet (H, A, M) = (7, 0, 12) ; le dernier bloc, qui ne contient que la lettre E, se verra ajouter 7 qui donnera L.

On a ici, à nouveau, laissé invariants les blancs du message, mais ce n'est évidemment pas une obligation. On pourrait, par exemple, considérer le blanc comme un caractère et utiliser ainsi un alphabet de 27 lettres.

Nous allons maintenant **formaliser les opérations** à mettre en œuvre pour utiliser les quelques algorithmes que nous venons de décrire. Supposons que les deux personnes qui veulent communiquer se nomment (en respectant la tradition de la littérature cryptographique anglo-saxonne) A (Alice) et B (Bob).

Si Alice veut envoyer de manière confidentielle un **message** M à Bob, elle va commencer par le **chiffrer** (on dit aussi lui appliquer un **algorithme de chiffrement**), c'est-à-dire le transformer de telle sorte que seul Bob puisse le comprendre. Le message ainsi transformé s'appelle **message chiffré** ou **cryptogramme** .

Bob recevant le cryptogramme voudra extraire le message **en clair** M à partir du cryptogramme ; cela s'appelle **déchiffrer** le cryptogramme ou lui appliquer un **algorithme de déchiffrement** .

Le procédé de chiffrement étant défini, il faut fixer un paramètre supplémentaire appelé la **clé** (dans le cas de l'algorithme de César, le nombre k). En fait, la donnée de l'algorithme (par exemple celui de Vigenère) définit toute une famille de transformations possibles, les deux correspondants se mettent d'accord sur les paramètres (la clé) qu'ils gardent alors secrets (dans le cas de Vigenère, les nombres $d, k_1, k_2, \ldots, k_d$).

Qui dit préservation d'un secret dit aussi tentative de se l'approprier. Si quelqu'un écoute la communication entre Alice et Bob, il obtiendra le cryptogramme C correspondant au message M. Vouloir retrouver le message M à partir de C sans connaître la clé, c'est tenter de **décrypter** le message chiffré. De même, **cryptanalyser** un algorithme de chiffrement, c'est se donner les moyens de décrypter tout message chiffré passant sur la ligne.

Cryptanalyse des algorithmes de César et Vigenère

Si c'est l'algorithme de César qui a été utilisé, à partir du moment où l'on a capté un cryptogramme, il suffit d'essayer les 26 clés possibles pour trouver celle qui a été utilisée. On sera alors en mesure de comprendre tout ce qui suivra.

Une observation naïve peut laisser croire que l'algorithme de César tient sa faiblesse du fait que la permutation de l'alphabet qu'il utilise respecte l'ordre alphabétique. En effet, il existe 26! (c'est-à-dire approximativement 4 fois 10^{26}) permutations possibles d'un alphabet de vingt-six lettres et les énumérer toutes pour trouver la bonne est autrement difficile que de se limiter aux 26 essais à réaliser lorsque c'est l'algorithme de César qui est utilisé.

En réalité, il suffit d'examiner beaucoup moins de permutations que cela si l'on fait des hypothèses sur le fait que le message clair est écrit dans une langue donnée : effectivement, une langue a des propriétés statistiques ; toutes les lettres ne sont pas employées avec la même fréquence dans les textes écrits en cette langue. Ces fréquences peuvent être déterminées empiriquement et donnent immédiatement la clé d'un algorithme de César généralisé utilisant une permutation quelconque de l'alphabet.

De telles méthodes statistiques introduites par **Kasiski** permirent à cet officier prussien de publier la cryptanalyse de l'algorithme de Vigenère en 1863. Ce type de considérations est à la base de nombreuses méthodes de cryptanalyse. On peut raffiner les remarques précédentes et regarder les statistiques de couples de lettres successives, etc.

1.1.4 Hasard

Une nouveauté importante a été l'apparition de la notion de clé à longueur variable. Par exemple, on assimile, comme précédemment, lettres et nombres entre 0 et 25. Les deux correspondants chiffrent leurs messages en les additionnant lettre à lettre avec le texte d'un livre choisi à l'avance et ainsi que certaines règles (notamment le point de départ dans ce livre de référence). En fait, ce

procédé peut aussi être attaqué par des méthodes basées sur les propriétés statistiques des langues, sous réserve que les cryptogrammes interceptés soient, bien sûr, suffisamment longs.

Ce type de considération a donné naissance à une idée de Vernam (1917) consistant à proposer une clé « aléatoire » aussi longue que le message. Ce nouveau concept nous conduit tout droit à ce que l'on peut appeler la cryptographie contemporaine. Nous reviendrons d'ailleurs sur sa portée au paragraphe 1.2.2.

1.2 Cryptographie moderne

1.2.1 Un peu de formalisme mathématique

Comme nous l'avons dit dans l'introduction, l'informatique a considérablement élargi le domaine d'application de la cryptographie. Nous sommes dans un monde qui échange énormément de données et le besoin de sécurité est à la mesure des enjeux économiques énormes de ces échanges. La cryptographie a cessé d'être un art, une sorte de hobby pour officier en retraite (Kasiski écrivit son livre après la fin de sa carrière militaire), pour devenir partie intégrante de différentes disciplines que recouvre le mot informatique.

En fait, la **cryptographie** est au carrefour de l'informatique théorique (évaluation des performances des algorithmes, théorie de la complexité), de l'algorithmique (programmation délicate de certains procédés faisant appel à des calculs complexes), de l'électronique (réalisation de circuits mettant en œuvre des algorithmes particuliers) et des mathématiques (algèbre et théorie des nombres notamment).

C'est la raison pour laquelle il est nécessaire de développer un certain formalisme mathématique, évité jusque-là, mais qui sera utile pour la suite de l'article. Néanmoins, le vocabulaire précédemment introduit va nous aider à donner des définitions précises.

Pour rester le plus simple possible, nous allons limiter notre formalisation au problème du chiffrement qui consiste, comme nous l'avons expliqué dans l'introduction, à assurer la confidentialité d'une communication. Nous aurons à manipuler trois ensembles :

— un ensemble de messages (que nous notons $\mathcal{M}$) ;
— un ensemble de cryptogrammes (que nous notons $\mathcal{C}$) ;
— un ensemble de clés (que nous notons $\mathcal{K}$).

Le plus souvent $\mathcal{M}$ est égal à $\mathcal{C}$ et ces trois ensembles sont finis.

Soit E une application :

$$\mathcal{M} \times \mathcal{K} \to \mathcal{C}$$
$$(M, K) \mapsto E(M, K).$$

On note souvent $E_K(M)$ l'élément $E(M, K)$ de sorte que, pour chaque clé K fixée, nous ayons une application E_K :

$$\mathcal{M} \to \mathcal{C}$$
$$M \mapsto E_K(M).$$

Nous disons alors que cette application E est un algorithme de chiffrement si, pour toute clé K dans $\mathcal{K}$, l'application E_K est inversible (en fait, pour éviter la perte d'information au cours de la transmission, il suffit d'exiger que E_K soit injective c'est-à-dire que deux éléments distincts de $\mathcal{M}$ aient des images distinctes dans $\mathcal{C}$ par exemple E_K).

L'application inverse de E_K est notée D_K. Ainsi, pour tout message M, on a :

$$D_K \circ E_K(M) = M.$$

Dans les exemples décrits paragraphe 1.1, l'algorithme étant choisi, les deux correspondants se mettaient d'accord sur la clé K qu'ils gardaient secrète. Le processus était alors symétrique ; chacun pouvait envoyer et recevoir des messages confidentiellement. On dit que de tels algorithmes sont **symétriques** ou à **clé secrète** [AF 173].

Les années 1970 ont vu apparaître un nouveau type d'algorithmes dits **à clé publique** ou **asymétriques** [AF 173]. Ils correspondent, dans notre formalisme, à une situation où la donnée de E_K ne suffit pas ***pratiquement*** (en un sens à définir précisément, mais disons à l'aide des moyens de calculs existants) pour retrouver D_K. Dans ce cas, le procédé n'est plus symétrique ; le possesseur de E_K est capable d'envoyer des messages au détenteur de D_K qui sera le seul à pouvoir les lire. Il n'y a alors aucune raison de laisser l'application E_K secrète ; on la publie sous l'appellation de **clé publique**. Chacun peut envoyer de manière confidentielle des messages au possesseur de D_K, cette dernière application ou ce qu'il faut pour la construire prenant le nom de **clé secrète** . Dans la suite de ce texte, nous allons décrire des exemples qui permettront de clarifier cette notion d'algorithme à clé publique.

1.2.2 Sécurité des algorithmes

Pour simplifier, et pour le moment, nous allons parler seulement de chiffrement. Notre introduction des algorithmes à clé publique s'est faite en disant qu'une certaine fonction inversible E_K possédait une application réciproque D_K qui n'était pas calculable pratiquement à partir de E_K seule (§ 1.2.1). Ce type de considération pose le problème de savoir comment évaluer la sécurité d'un algorithme.

Remarquons que l'on peut envisager plusieurs **types d'attaques** sur un algorithme (supposé connu dont il s'agit de calculer la clé) ; nous en énumérons ici quelques-unes par ordre décroissant de difficulté pour le cryptanalyste :

— attaque « message chiffré connu » : le cryptanalyste a réussi à capter un certain nombre de cryptogrammes et doit travailler avec ces données (l'algorithme de César ne résiste pas à ce type d'attaque) ;

— attaque « message clair connu » : le cryptanalyste connaît des couples message et cryptogramme correspondant, mais n'a pas de contrôle sur ces données ;

— attaque « message clair choisi » : le cryptanalyste connaît des couples messages et cryptogramme correspondant en ayant choisi les messages clairs ; cela revient, pour le cryptanalyste, à posséder la machine à chiffrer sous forme de « boîte noire » et à chercher à en déterminer le contenu (la clé).

On peut imaginer des algorithmes qui résistent au premier type d'attaque mais pas aux autres, qui résistent au second mais pas au troisième.

Nous allons distinguer deux **types de sécurité** :

— les algorithmes inconditionnellement sûrs ;
— les algorithmes sûrs d'un point de vue informatique.

● La **sécurité inconditionnelle** ou **secret parfait** signifie que la connaissance d'un cryptogramme ne donne aucune indication sur le message clair correspondant. Cela se définit de manière parfaitement rigoureuse. Il s'agit d'un concept lié à la théorie de l'information qui a été introduit dans les travaux de Claude Shannon [50], dans les années 1940. On connaît un seul exemple de schéma cryptographique inconditionnellement sûr en ce sens. Il s'agit du procédé (connu en anglais sous le nom de « *one time pad* ») dont l'idée remonte à Vernam (§ 1.1.4). Pour simplifier, supposons que le message est une suite binaire de longueur N :

$$m_0\, m_1 \ldots m_N ;$$

la clé secrète doit être une suite binaire aléatoire de longueur N également :

$$k_0\, k_1 \ldots k_N .$$

Cela suppose que les deux correspondants aient pu auparavant échanger de manière secrète cette clé. On sait, par ailleurs, fabriquer ce type de clé à partir de phénomènes physiques aléatoires

(rayonnement d'une diode notamment). Le cryptogramme est de nouveau une suite binaire de longueur N :

$$c_0\, c_1 \ldots c_N$$

obtenue par « ou exclusif » (langage des informaticiens ou électroniciens) des deux suites précédentes :

$$c_i = m_i \oplus k_i$$

c'est-à-dire par addition modulo 2 (langage des mathématiciens) :

$$c_i = m_i + k_i \text{ modulo } 2.$$

Le destinataire qui connaît la clé (la suite aléatoire) n'a plus qu'à la combiner de la même manière au cryptogramme reçu pour obtenir le message clair car :

$$c_i + k_i \equiv m_i + k_i + k_i \equiv m_i \text{ modulo } 2.$$

La clé $k_0\, k_1 \ldots k_N$ est évidemment employée une seule fois et la connaissance du message clair et du message chiffré correspondant ne peut être d'aucune utilité pour décrypter un message futur (qui sera chiffré avec une nouvelle clé aléatoire). Plusieurs auteurs affirment que ce procédé a été (est ?) utilisé en diplomatie. Il est impossible à mettre en œuvre dans les besoins actuels en informatique, car il suppose l'échange préalable d'une quantité d'information aussi grande que celle que l'on veut chiffrer.

● Après avoir évoqué la notion de secret parfait et donné une illustration de ce concept, venons-en à l'autre concept de sécurité. Un **algorithme** est dit « **informatiquement** » (*computationally* en anglais) **sûr** si le temps de calcul nécessaire pour trouver la clé est hors de portée avec les moyens de calculs disponibles. Ce type de considération donne naissance à une hiérarchie dans la sécurité. On peut concevoir des algorithmes qui résisteraient à une capacité de calcul, mais pas à une autre. Des considérations économiques apparaissent aussi ; le cryptanalyste n'a pas intérêt à faire l'acquisition de moyens de calculs d'un coût supérieur au gain escompté.

Comme dans le cas de la sécurité inconditionnelle, on a donné des fondations rigoureuses à ces notions ; il s'agit de la **théorie de la complexité** (cf., par exemple, le livre de Dehornoy [13]). Cette théorie construit des classes de problèmes en établissant des modèles abstraits de machines informatiques (machines de Turing notamment) ; elle fait appel à la logique mathématique.

Il y a également des approches quantitatives aux problèmes de complexité visant, par exemple, à donner des majorations (absolues ou le plus souvent asymptotiques) du temps ou de la place mémoire nécessaires à la mise en œuvre des algorithmes. Le plus souvent, ces méthodes font appel à l'analyse mathématique (théorie analytique des nombres notamment pour beaucoup d'algorithmes liés à la cryptographie, cf., par exemple, l'article [41] et, plus généralement [24]).

En cryptographie, il ne faut pas perdre de vue néanmoins que la notion de sécurité est relative aux moyens informatiques et aux algorithmes disponibles à un moment donné. C'est ainsi que l'on a pu dire, sous forme d'une boutade qui contient sa part de vérité, qu'un algorithme cryptographique n'était sûr que tant qu'il n'avait pas été « cassé » (c'est-à-dire cryptanalysé).

2. Mathématiques élémentaires de la cryptographie

Nous introduisons rapidement les notions d'algèbre (arithmétique et polynômes sur un corps) qui seront utilisés dans la suite. Pour une présentation du langage mathématique et des structures algébriques en général, nous renvoyons à l'article de B. Randé [AF 33] *Langage des ensembles et des structures*.

Une étude plus complète des polynômes est disponible dans l'article de B. Randé [AF 37] *Polynômes. Étude algébrique*.

2.1 Arithmétique

2.1.1 Quelques propriétés de l'anneau des entiers relatifs

Nous allons donner quelques propriétés de l'ensemble $\mathbb{Z}$ des entiers relatifs.

2.1.1.1 Division et nombres premiers

Rappelons la notion de division euclidienne dans $\mathbb{Z}$. Soient m et n deux entiers tels que $n > 0$. Il existe deux entiers q et r, respectivement dénommés le quotient de m par n et le reste dans la division de m par n, tels que :

$$m = qn + r$$

uniquement déterminés par la condition :

$$0 \leqslant r < n\ .$$

Si $r = 0$, on dit que n divise m et on écrit $n|m$.

Il est bien connu que l'addition des entiers confère à $\mathbb{Z}$ une structure de groupe abélien et, si l'on prend en compte la multiplication des entiers, on a une structure d'anneau commutatif sur $\mathbb{Z}$. Les seuls nombres entiers qui possèdent un inverse (c'est-à-dire un élément symétrique pour la multiplication) sont 1 et –1.

Le **groupe multiplicatif** de l'anneau $\mathbb{Z}$, noté $\mathbb{Z}^*$ ou $\mathbb{Z}^\times$, c'est-à-dire l'ensemble des éléments inversibles de l'anneau, qui forme toujours un groupe multiplicatif, est $\{1, -1\}$.

Si l'on s'intéresse à la multiplication, parmi les entiers, certains sont en quelque sorte des briques de base indécomposables : ce sont les nombres premiers.

Définition 1. Un entier positif est dit **premier** s'il est distinct de 0 et 1 et s'il n'admet comme diviseur positif supérieur à 1 que lui-même.

Les inversibles n'interviennent pas dans la théorie des nombres premiers ; ainsi, de ce point de vue, il n'y a pas lieu de faire une différence entre un nombre premier p et son opposée $-p$; si l'on voulait être très précis, il faudrait dire que ce sont deux nombres premiers « associés », ce qui signifie que l'un est le produit de l'autre par un élément inversible. C'est pourquoi nous n'avons considéré comme premiers que des nombres positifs.

Euclide savait déjà démontrer l'existence d'une infinité de nombres premiers. Un autre résultat fondamental est le t**héorème 1 de décomposition unique** .

Théorème 1. Soit n un entier naturel strictement supérieur à 1. Alors n se décompose de manière unique en produit de nombres premiers :

$$n = p_1^{e_1} p_2^{e_2} \ldots p_r^{e_r}$$

où les p_i sont des nombres premiers distincts deux à deux et les e_i ainsi que r sont des entiers strictement positifs.

La décomposition de l'entier négatif $-n$ serait évidemment la même, précédée du facteur inversible –1. Les p_i sont appelés les facteurs premiers de n. Les diviseurs de n sont exactement les nombres :

$$p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}$$

pour tous les a_i vérifiant $0 \leqslant a_i \leqslant e_i$ et les i tels que $1 \leqslant i \leqslant r$.

2.1.1.2 pgcd et ppcm

Soient n et m deux entiers de $\mathbb{Z}$. Considérons l'intersection de leurs ensembles de diviseurs positifs ; c'est un ensemble fini d'entiers. Il a un plus petit élément qui est toujours égal à 1 ; son plus grand élément est, par définition, le ***plus grand commun diviseur*** de m et n, il est noté pgcd (m, n) ou bien (m, n).

L'intersection des ensembles des multiples strictement positifs de m et n est un ensemble infini d'entiers ; il a un plus petit élément que l'on appelle le ***plus petit commun multiple*** de m et n, il est noté **ppcm** (m, n) ou bien $[m, n]$.

On a toujours, par construction de (m, n) et $[m, n]$:

$$1 \leqslant (m, n) \leqslant m \wedge n$$

et

$$m \vee n \leqslant [m, n] \leqslant mn.$$

en notant $x \wedge y$ le plus petit des entiers x et y et $x \vee y$ le plus grand.

Appelons $\mathcal{P}$ l'ensemble des nombres premiers. Pour un entier n non nul et un nombre premier p, on note $v_p(n)$ le plus grand exposant e tel que $p^e | n$. En termes savants, le nombre $v_p(n)$ est la valuation p-adique de n et, n étant fixé, $v_p(n)$ est nul pour presque tout p, c'est-à-dire ici pour tous les p premiers sauf un nombre fini d'entre eux. On a :

$$v_p(-n) = v_p(n)$$

et il est naturel de poser :

$$v_p(0) = +\infty.$$

Il résulte de la définition de la fonction v_p que, pour x et y dans $\mathbb{Z}$ (avec une règle usuelle sur le symbole $+\infty$) :

$$v_p(xy) = v_p(x) + v_p(y).$$

On peut écrire, si n est strictement positif (s'il est strictement négatif, on met un –1 en facteur devant le produit) :

$$n = \prod_{p \in \mathcal{P}} p^{v_p(n)}$$

en convenant, comme toujours, que $p^0 = 1$; le produit infini ci-dessus ne contient en fait qu'un nombre fini de termes distincts de 1.

La proposition **1** suivante est une conséquence immédiate de la décomposition unique d'un entier en produit de facteurs premiers.

Proposition 1.

Soient a et b deux entiers, on a :

$$a | b \Leftrightarrow \forall p \in \mathcal{P},\ v_p(a) \leqslant v_p(b).$$

On apprend (ou l'on apprenait) très tôt dans l'enseignement secondaire les deux résultats suivants :

— le pgcd de m et n est égal au produit de tous les facteurs premiers communs à m et n pris une seule fois avec leur plus petit exposant ;

— le ppcm de m et n est égal au produit de tous les facteurs premiers communs et non communs à m et n pris une seule fois avec leur plus grand exposant.

Cela s'écrit encore :

$$(m, n) = \prod_{p \in \mathcal{P}} p^{v_p(m) \wedge v_p(n)}$$

et

$$(m, n) = \prod_{p \in \mathcal{P}} p^{v_p(m) \vee v_p(n)}.$$

Il est alors immédiat que :

$$(m, n)\,[m, n] = mn$$

puisque pour tout couple d'entiers (x, y) on a :

$$(x \wedge y) + (x \vee y) = x + y.$$

Les deux propositions suivantes sont faciles à justifier avec les considérations que nous venons de faire.

Proposition 2.

Tout diviseur commun à deux entiers divise leur plus grand commun diviseur.

Proposition 3.

Tout multiple commun à deux entiers est un multiple de leur plus petit commun multiple.

Les notions de pgcd et ppcm se généralisent à tout ensemble fini de nombres entiers.

2.1.1.3 Entiers premiers entre eux

Deux nombres m et n sont dits ***premiers entre eux*** ou ***étrangers*** si leur pgcd est égal à un, autrement dit s'ils n'ont aucun diviseur premier commun. On voit facilement, avec la notation sous forme de produit infini introduite paragraphe 2.1.1.2 que m et n étant fixés, pour tout nombre premier p, l'un au moins des entiers $v_p(m/(n, m))$ et $v_p(n/(n, m))$ est nul. Ainsi les nombres $m/(n, m)$ et $n/(n, m)$ sont étrangers.

Proposition 4.

Soient a et b des entiers et p un nombre premier. Si p divise le produit ab alors p\a ou p\b.

Preuve. ◊ Utilisons la valuation p-adique. On a $v_p(ab) \geqslant 1$ car $p | ab$. Or

$$v_p(ab) = v_p(a) + v_p(b).$$

Donc l'un au moins des entiers $v_p(a)$ et $v_p(b)$ est non nul. ◊

Corollaire 1.

Soient a, b et n des entiers. Si n divise le produit ab et est premier à a, alors n divise b.

Preuve. ◊ En effet, soit p un diviseur premier de n alors :

$$v_p(n) \leqslant v_p(ab) = v_p(b).$$ ◊

Proposition 5.

Soient a et b deux entiers étrangers divisant un autre entier n ; alors ab\n.

Preuve. ◊ Soit p un diviseur de ab ; il divise alors a ou b d'après la proposition **4**. Nous allons montrer que $v_p(ab) \leqslant v_p(n)$.

Si p est un diviseur premier de a, il ne divise pas b car $(a, b) = 1$ et

$$v_p(ab) = v_p(a) \leqslant v_p(n)$$

car a divise n.

Un argument analogue montre que si p est un diviseur premier de b :

$$v_p(ab) = v_p(b) \leqslant v_p(n)$$

ce qui achève la preuve. ◊

2.1.1.4 Sous-groupes de $\mathbb{Z}$

Proposition 6.

Soit G un sous-groupe additif de $\mathbb{Z}$. Alors G est l'ensemble des multiples d'un entier n.

Preuve. ◊ D'abord, tout ensemble $n\mathbb{Z}$ des multiples d'un entier fixé n est un sous-groupe de $(\mathbb{Z}, +)$. En effet, il contient 0 et, s'il contient deux autres entiers u et v, ces derniers sont aussi des multiples de n ; il existe des entiers a et b tels que $u = an$ et $v = bn$. Mais alors

$$u - v = an - bn = (a - b)\,n$$

est aussi un multiple de n et appartient à $n\mathbb{Z}$, ce qui montre que ce dernier est un sous-groupe de $\mathbb{Z}$.

Inversement, soit $G \subset \mathbb{Z}$ un sous-groupe additif.

Si $G = \{0\}$, alors c'est l'ensemble des multiples de 0.

Si $G \neq \{0\}$, il contient un plus petit élément strictement positif noté n ; en effet, G contient des nombres positifs, car si $x \in G$ alors $-x \in G$ (existence d'un opposé). Par conséquent, G contient l'ensemble $n\mathbb{Z}$ des multiples de n : il contient $2n = n + n$, $3n = n + n + n$, etc., et leurs opposés. Supposons que G contienne un entier m positif non multiple de n ; effectuons la division euclidienne de m par n ; nous obtenons :

$$m = qn + r$$

où q est le quotient et r le reste qui vérifie $0 < r < n$.

L'entier qn est dans G, donc il en est de même de $m - qn = r$. Ainsi, G possède un élément strictement positif plus petit que n, ce qui contredit l'hypothèse définissant n comme le plus petit entier strictement positif contenu dans G. Nous avons obtenu, par l'absurde, que :

$$G = n\mathbb{Z}. \qquad \Diamond$$

Traduisons la relation de divisibilité en termes d'inclusion de sous-groupes de $\mathbb{Z}$.

Proposition 7.

Soient a et b des entiers. On a :

$$a|b \Leftrightarrow a\mathbb{Z} \supset b\mathbb{Z}\ .$$

Preuve. ◊ Immédiate.◊

Théorème 2. Soient a et b des entiers. On a :

$$a\mathbb{Z} + b\mathbb{Z} = (a, b)\mathbb{Z}$$

$$a\mathbb{Z} \cap b\mathbb{Z} = [a, b]\mathbb{Z}.$$

Preuve. ◊ L'ensemble $a\mathbb{Z} + b\mathbb{Z}$ (défini comme l'ensemble des entiers s'écrivant comme somme d'un multiple de a et d'un multiple de b) est un sous-groupe de $\mathbb{Z}$.

Il contient 0 et, s'il contient deux éléments $au + bv$ et $au' + bv'$, il contient leur différence car :

$$au + bv - (au' + bv') = a(u - u') + b(v - v').$$

Par conséquent, il existe un entier positif d tel que :

$$a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}.$$

Les nombres a et b sont dans $d\mathbb{Z}$, donc d les divise ; par suite $d|(a, b)$.

Inversement, d s'écrit $au + bv$; or a et b sont des multiples de (a, b), donc il en est de même de d ce qui signifie que $(a, b)\ |d$.

La seconde égalité est immédiate. ◊

Corollaire 2 (**théorème de Bézout**).

Deux nombres entiers a et b sont premiers entre eux si, et seulement si, il existe deux entiers u et v tels que :

$$au + bv = 1.$$

2.1.1.5 Algorithme d'Euclide

Contrairement aux apparences, nous n'avons pas donné de procédé permettant de calculer « facilement » le pgcd de deux entiers. Le calcul que nous avons suggéré suppose que l'on connaisse la factorisation des deux entiers avant le calcul de leur pgcd. Or la factorisation des entiers est très difficile (dès que ces entiers deviennent « grands »). Pourtant, un algorithme efficace et beaucoup plus simple que la factorisation existe. Il s'agit de l'« **algorithme d'Euclide** ». Il est basé sur une suite de divisions euclidiennes. Cet algorithme est d'une importance fondamentale dans beaucoup de calculs utilisant des nombres entiers. Il est également important en informatique théorique, puisqu'il sert de prototype pour certaines analyses de complexité.

L'algorithme d'Euclide procède de la manière suivante. Soit à calculer un pgcd de a et b ; on effectue les divisions euclidiennes suivantes jusqu'à obtenir un reste nul :

$$\begin{aligned} a &= bq_0 + r_0 \\ b &= r_0 q_1 + r_1 \\ r_0 &= r_1 q_2 + r_2 \\ r_1 &= r_2 q_3 + r_3 \\ &\vdots \\ r_{n-2} &= r_{n-1} q_n + r_n \\ r_{n-1} &= r_n q_{n+1} + 0 \end{aligned}$$

avec $r_n > 0$.

Puisque $r_0 < b$, $r_1 < r_0$, etc., il faut *au plus b* étapes pour aboutir à un reste nul. En fait, nous allons voir qu'il en faut beaucoup moins, mais assurons-nous d'abord que nous avons bien obtenu ce que nous cherchions.

Nous n'avons rien dit du cas où $r_0 = 0$; il signifie que $b|a$ et l'algorithme peut s'arrêter.

Théorème 3. Dans l'algorithme d'Euclide, le dernier reste non nul r_n est le pgcd de a et b.

Preuve. ◊ Le nombre (a, b) divise r_0, car il divise a et b et que l'on a $r_0 = bq_0 + a$.

Le même type d'argument prouve que $(a, b)\ |r_1$ et ainsi de suite ; par récurrence, on aboutit à $(a, b)\ |r_n$.

Inversement, $r_n|r_{n-1}$ par la dernière ligne de l'algorithme, d'où l'on tire $r_n|r_{n-2}$ par l'avant-dernière ligne et ainsi de suite en remontant ; on aboutit à $r_n|r_1$, puis $r_n|r_0$, $r_n|b$ et, enfin, $r_n|a$; ainsi $r_n|(a, b)$, ce qui achève la preuve. ◊

Le résultat qui suit est très important d'un point de vue « informatique ». Il nous indique que le temps de calcul d'un pgcd est logarithmique (en les données), c'est-à-dire petit, donc à notre portée. Imaginons que le nombre d'opérations nécessaires pour un tel calcul soit de l'ordre de grandeur de l'un des nombres dont on veut calculer pgcd ; si ce nombre est de l'ordre de 2^{120}, c'est hors de portée ; si c'est deux fois son logarithme en base deux (c'est-à-dire grossièrement deux fois son nombre de chiffres binaires), cela devient abordable.

Nous allons noter $\log_2$ le logarithme en base deux.

Théorème 4. Dans l'algorithme d'Euclide calculant le pgcd de a et b, on effectue $n + 2$ divisions euclidiennes et le nombre n vérifie l'inégalité

$$n < 2 \log_2 (a \wedge b) + 2.$$

Preuve. ◊ On suppose sans restriction que $a \geqslant b$. Soit p tel que $2p \leqslant n < 2p + 2$. Puisque $(r_i)_{0 \leqslant i \leqslant n}$ est strictement décroissante, $q_i \geqslant 1$ pour $i \geqslant 1$. Donc :

$$r_i \geqslant r_{i+1} + r_{i+2} \geqslant 2 r_{i+2}$$

et par conséquent :

$$r_0 \geqslant 2^p r_{2p}.$$

Donc :

$$b \geqslant 2^p r_n \geqslant 2^p$$

car $r_n \geqslant 1$ et $p \leqslant \dfrac{\ln b}{\ln 2}$.

Donc :

$$n < 2 \log_2 b + 2. \qquad \Diamond$$

2.1.2 Quotients de $\mathbb{Z}$

Dans l'anneau $\mathbb{Z}$, les idéaux (c'est-à-dire les sous-groupes additifs de $\mathbb{Z}$ stables pour la multiplication par n'importe quel entier) sont exactement les ensembles $n\mathbb{Z}$ de multiples d'un entier donné n ; on exprime cette propriété en disant que $\mathbb{Z}$ est un **anneau principal**. Il est facile de voir que deux entiers n et m ont le même ensemble de multiples si, et seulement si, ils sont opposés, c'est-à-dire :

$$m = -n\ ;$$

ainsi, on peut ne considérer que les idéaux $n\mathbb{Z}$ correspondant aux entiers naturels n.

Les **anneaux quotients** de $\mathbb{Z}$ par ces idéaux jouent un rôle très important, ce sont les anneaux notés $\mathbb{Z}/n\mathbb{Z}$ pour un entier n. On appelle $\mathbb{Z}/n\mathbb{Z}$ l'anneau des entiers modulo n ; si deux entiers x et y ont même reste dans la division par n, on dit qu'ils sont congrus modulo n et on écrit :

$$x \equiv y \text{ modulo } n,$$

ce qui signifie que les (classes des) éléments x et y sont égaux dans l'anneau $\mathbb{Z}/n\mathbb{Z}$.

Les deux cas triviaux :

$n = 0$ correspondant à $\mathbb{Z}/\{0\} \simeq \mathbb{Z}$ (ici $\{0\}$ désigne l'anneau nul qui ne contient que l'élément 0 et le symbole $\simeq$ indique l'existence d'un isomorphisme d'anneaux) ;

$n = 1$ correspondant au quotient $\mathbb{Z}/\mathbb{Z} \simeq \{0\}$

sont de peu d'intérêt.

Si n est un entier au moins égal à deux, l'anneau quotient $\mathbb{Z}/n\mathbb{Z}$ s'identifie à l'ensemble d'entiers :

$$\{0, 1, \ldots, n-1\}$$

où l'entier i représente alors la classe des entiers ayant pour reste i dans la division euclidienne par n. Les deux opérations dans le quotient sont induites par leur opération correspondante dans $\mathbb{Z}$:

— la somme des éléments i et j de $\mathbb{Z}/n\mathbb{Z}$ est égale au reste, dans la division euclidienne, de l'entier naturel $i + j$ par n ;

— de même, le produit des éléments i et j de $\mathbb{Z}/n\mathbb{Z}$ est égal au reste, dans la division euclidienne, de l'entier naturel ij par n.

Les tableaux **2** et **3** donnent, à titre d'exemple, les tables d'addition et de multiplication dans $\mathbb{Z}/6\mathbb{Z}$.

Tableau 2 – Table d'addition dans $\mathbb{Z}/6\mathbb{Z}$

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Tableau 3 – Table de multiplication dans $\mathbb{Z}/6\mathbb{Z}$

x	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Le groupe additif de l'anneau $\mathbb{Z}/n\mathbb{Z}$ est engendré (additivement, ce qui signifie que tous les éléments du groupe s'écrivent comme une somme dont chaque terme est égal à 1) par l'élément 1, ce que nous écrivons :

$$\mathbb{Z}/n\mathbb{Z} = \langle 1 \rangle ;$$

il est donc cyclique (c'est-à-dire engendré par un élément et fini). On sait d'ailleurs que tout groupe cyclique d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$. On peut se demander combien ce groupe a de générateurs, ou combien il y a d'éléments dans le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^*$, c'est-à-dire d'éléments inversibles dans notre anneau. La réponse à ces deux questions est identique comme nous allons le voir.

Proposition 8.

Soit n un entier positif. Alors le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^*$ est constitué de toutes les classes d'entiers m vérifiant :

$$1 \leqslant m \leqslant n-1 \text{ et } (m, n) = 1.$$

Preuve. ◊ Un élément m est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si, et seulement si, il existe u dans cet anneau tel que :

$$um \equiv 1 \text{ modulo } n$$

ce qui signifie qu'il existe deux entiers (relatifs) u et v tels que

$$um + vn = 1,$$

autrement dit si, et seulement si, m et n sont premiers entre eux. ◊

Corollaire 3.

Soit n un entier positif et m un élément du groupe cyclique $\mathbb{Z}/n\mathbb{Z}$. Alors m est un générateur de ce groupe cyclique si, et seulement si :

$$(m, n) = 1.$$

Preuve. ◊ L'élément m engendre $\mathbb{Z}/n\mathbb{Z}$ si, et seulement si, 1 est dans le groupe engendré par m, ce qui revient à dire qu'il existe dans ce groupe un élément u tel que

$$mu \equiv 1 \text{ modulo } n$$

ce qui est équivalent à dire que m est inversible, donc premier à n. ◊

Définition 2. Soit n un entier positif. Le cardinal du groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^*$ est noté $\varphi(n)$ et on appelle φ la **fonction indicatrice d'Euler**.

Nous verrons, à la fin de ce paragraphe, comment on peut calculer $\varphi(n)$ lorsque l'on connaît la factorisation de n en produit de puissances de nombres premiers.

Corollaire 4.

Soit n un entier positif. Alors l'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si, et seulement si, n est premier.

Preuve. ◊ C'est une conséquence immédiate de la preuve du corollaire **3** : n est un nombre premier si tous les entiers m :

$$1 \leqslant m \leqslant n-1$$

sont premiers à n. ◊

Ce dernier résultat a une conséquence sur la fonction φ d'Euler :

$$\varphi(p) = p - 1$$

si, et seulement si, l'entier $p > 1$ est premier.

Exemple 1 : l'anneau $\mathbb{Z}/2\mathbb{Z}$ est un corps que nous noterons $\mathbb{F}_2$; les tableaux **4** et **5** en sont les tables d'addition et de multiplication.

Tableau 4 – Table d'addition dans $\mathbb{F}_2$

+	0	1
0	0	1
1	1	0

Tableau 5 – Table de multiplication dans $\mathbb{F}_2$

x	0	1
0	0	0
1	0	1

Nous allons utiliser les notions de **produit direct** d'anneaux et de groupes.

Si G_1 et G_2 sont deux **groupes**, leur produit direct est le produit cartésien $G_1 \times G_2$ muni de la loi de groupe induite sur ce produit cartésien par la loi de G_1 sur la première composante et par la loi de G_2 sur la seconde.

De même, si A et B sont des **anneaux**, on a un anneau produit direct $A \times B$ en effectuant les 2 opérations composante par composante.

Pour ce qui est des groupes additifs des quotients de $\mathbb{Z}$, il faut connaître le théorème **5**.

Théorème 5. Soient n et m deux entiers positifs, le produit direct de groupes :

$$\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

est cyclique (c'est-à-dire isomorphe à $\mathbb{Z}/mn\mathbb{Z}$) si, et seulement si, m et n sont premiers entre eux.

Un résultat fondamental qui approfondit le précédent est le « **théorème chinois** » (théorème **6**).

Théorème 6. Soient m et n deux entiers premiers entre eux, alors on a un isomorphisme canonique d'anneaux :

$$\mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$
$$a \mapsto (a \text{ modulo } m, a \text{ modulo } n).$$

La forme explicite de l'isomorphisme réciproque est la suivante :

$$\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/mn\mathbb{Z}$$
$$(\alpha, \beta) \mapsto \alpha n\,(n^{-1} \bmod m) + \beta m\,(m^{-1} \bmod n),$$

où $(n^{-1} \bmod m)$ désigne l'inverse multiplicatif de n modulo m et $(m^{-1} \bmod n)$ l'inverse multiplicatif de m modulo n. La justification est une simple vérification.

Un aspect important du théorème chinois (théorème **6**) est qu'il n'affirme pas seulement que les deux anneaux considérés sont isomorphes ; il donne explicitement un isomorphisme dont nous avons déduit l'isomorphisme réciproque. Ce caractère effectif est évidemment crucial pour les applications. Le fait qu'il s'agisse d'un isomorphisme d'anneaux a pour conséquence que sa restriction au groupe multiplicatif $(\mathbb{Z}/mn\mathbb{Z})^*$ donne un isomorphisme de groupes dans le groupe multiplicatif $(\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$; celui-ci est en fait le groupe multiplicatif de l'anneau produit.

On en déduit une nouvelle propriété de la fonction d'Euler à savoir que :

$$\varphi(mn) = \varphi(m)\varphi(n)$$

si m et n sont premiers entre eux.

Le théorème chinois se généralise sans difficulté à un produit de plusieurs entiers. En particulier, soient n est un entier strictement plus grand que 1 et

$$n = p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}$$

sa factorisation sous forme de puissances de nombres premiers distincts deux à deux. Alors, on a l'isomorphisme canonique d'anneaux :

$$\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/p_1^{a_1}\mathbb{Z} \times \mathbb{Z}/p_2^{a_2}\mathbb{Z} \times \ldots \times \mathbb{Z}/p_r^{a_r}\mathbb{Z}$$

$$x \mapsto (x \bmod p_1^{a_1}, x \bmod p_2^{a_2}, \ldots, x \bmod p_r^{a_r})$$

Cette dernière affirmation montre, en particulier, que le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^*$ est isomorphe au produit de groupes multiplicatifs :

$$(\mathbb{Z}/p_1^{a_1}\mathbb{Z})^* \times (\mathbb{Z}/p_2^{a_2}\mathbb{Z})^* \times \ldots \times (\mathbb{Z}/p_r^{a_r}\mathbb{Z})^*.$$

Pour la fonction d'Euler, cela se traduit par :

$$\varphi(n) = \prod_{i=1}^{r} \varphi(p_i^{a_i}).$$

Si l'on veut terminer le calcul de $\varphi(n)$, il faut maintenant calculer $\varphi(p^m)$ pour un nombre premier p et un nombre entier $m \geqslant 1$; en fait, on connaît déjà la réponse pour $m = 1$.

Il s'agit donc de dénombrer les entiers k de

$$[\![0, p^m - 1]\!]$$

qui sont premiers avec p^m. Il est plus commode de dénombrer ceux qui ne sont pas premiers avec p^m, c'est-à-dire ceux qui sont divisibles par p. Ce sont les termes de la progression arithmétique 0, p, $2p$, ..., $(p^{m-1}-1)\,p$. Il y en a donc p^{m-1}. Autrement dit, le complément à p^m est la valeur de $\varphi(p^m)$, soit :

$$\varphi(p^m) = p^m - p^{m-1}.$$

On peut en fait obtenir beaucoup mieux : la structure du groupe multiplicatif $(\mathbb{Z}/p^m\mathbb{Z})^*$ comme produit de groupes cycliques additifs.

Nous distinguons les cas $p = 2$ et p impair et nous ne donnons pas la preuve du résultat (on peut la trouver, par exemple, dans [22], pages 57 et suivantes).

Si $\boldsymbol{p = 2}$ et $m \geqslant 2$ (le cas $m = 1$ étant évident), on a :

$$(\mathbb{Z}/2^m\mathbb{Z})^* \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{m-2}\mathbb{Z}$$

(en particulier, ce groupe n'est pas cyclique si m > 2).

Si ***p* est impair**, on a :

$$(\mathbb{Z}/p^m\mathbb{Z})^* \simeq \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{m-1}\mathbb{Z}$$

(ce groupe est donc nécessairement cyclique).

- Nous pouvons préciser la **forme de cet isomorphisme**.

Si $\boldsymbol{p = 2}$, on peut montrer que l'élément $5 = 1 + 2^2$ est d'ordre multiplicatif 2^{m-2} modulo 2^m et que tout élément u de $(\mathbb{Z}/2^m\mathbb{Z})^*$ peut s'écrire de manière unique sous la forme

$$u = (-1)^v (1 + 2^2)^w :$$

avec v dans $(\mathbb{Z}/2\mathbb{Z})$ et w dans $\mathbb{Z}/2^{m-2}\mathbb{Z}$. L'isomorphisme cherché est alors :

$$(\mathbb{Z}/2^m\mathbb{Z})^* \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{m-2}\mathbb{Z}$$
$$u \mapsto (v, w).$$

Maintenant si ***p* est impair**, nous choisissons un élément g d'ordre multiplicatif $p - 1$ dans $(\mathbb{Z}/p^m\mathbb{Z})^*$ (il en existe mais le choix n'est pas canonique). On peut, en outre, montrer que $1 + p$ est d'ordre multiplicatif p^{m-1} dans $(\mathbb{Z}/p^m\mathbb{Z})^*$.

Tout $u \in (\mathbb{Z}/p^m\mathbb{Z})^*$ peut alors s'écrire de manière unique sous la forme :

$$u = g^v (1 + p)^w$$

avec $v \in \mathbb{Z}/(p-1)\mathbb{Z}$ et $w \in \mathbb{Z}/p^{m-1}\mathbb{Z}$. On obtient l'isomorphisme :

$$(\mathbb{Z}/p^m\mathbb{Z})^* \to \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{m-1}\mathbb{Z}$$
$$u \mapsto (v, w).$$

- Il est important de noter que, contrairement à celui du théorème chinois, cet isomorphisme n'est pas canonique. Par exemple, si p est impair et $m = 1$ (cas du groupe multiplicatif du corps fini $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ un isomorphisme

$$\mathbb{Z}/(p-1)\mathbb{Z} \to (\mathbb{Z}/p\mathbb{Z})^*$$

est défini en envoyant l'élément 1 sur un générateur quelconque de $(\mathbb{Z}/p\mathbb{Z})^*$.

Il y a $\varphi(p-1)$ (φ est la fonction d'Euler) générateurs semblables et il n'y a aucune raison de privilégier l'un d'entre eux, d'où le caractère non canonique de cette correspondance.

Outre le caractère non canonique, nous remarquons également que, contrairement au cas du théorème chinois où l'isomorphisme est explicite et immédiatement calculable, ici nous n'avons pas donné de procédé algorithmique pour trouver l'élément noté w par exemple.

■ Nous pouvons maintenant faire une liste de **propriétés de la fonction φ d'Euler** :

— si n et m sont premiers entre eux :

$$\varphi(mn) = \varphi(m)\,\varphi(n),$$

on dit parfois que la fonction d'Euler est multiplicative ;

— si p est un nombre premier et n un entier positif alors :

$$\varphi(p^n) = (p-1)\,p^{n-1} ;$$

— soient n un entier positif et

$$n = \prod_{i=1}^{r} p_i^{e_i}$$

sa décomposition en produit de nombres premiers distincts, alors, on a :

$$\varphi(n) = \prod_{i=1}^{r} ((p_i - 1)p_i^{e_i - 1}) = n\prod_{i=1}^{r}\left(1 - \frac{1}{p_i}\right).$$

2.2 Polynômes et corps finis

2.2.1 Polynômes en une indéterminée sur un anneau

Le premier exemple d'anneau étudié était $\mathbb{Z}$ (§ 2.1). Nous allons maintenant en introduire un second dont les propriétés sont fort semblables à celles du premier : l'anneau des polynômes en une variable à coefficients dans un corps. Si ce corps est fini, l'analogie avec $\mathbb{Z}$ est encore plus profonde, notamment les quotients sont également finis comme les $\mathbb{Z}/n\mathbb{Z}$. Une étude plus approfondie de $\mathbb{Z}$ serait le passage à la théorie algébrique des nombres et un développement de l'étude des polynômes sur un corps fini mènerait à la théorie des courbes algébriques sur de tels corps ; les analogies se révéleraient alors dans toute leur profondeur.

■ Pour commencer, construisons l'**anneau des polynômes en une variable sur un anneau**.

Soient un A anneau commutatif et $B = A^{(\mathbb{N})}$ l'ensemble des suites à valeurs dans A, nulles, sauf en un nombre fini d'entiers. Nous allons construire sur B une structure d'anneau pour obtenir ce que nous appellerons l'anneau des polynômes à une indéterminée sur A.

L'**addition** se réalise composante par composante, à partir de celle de A. Par exemple si $x = (x_0, x_1, x_2, \ldots x_i, \ldots)$ (tous les x_i sont nuls, sauf un nombre fini d'entre eux) et $y = (y_0, y_1, y_2, \ldots, y_i, \ldots)$ (tous les y_i sont nuls, sauf un nombre fini d'entre eux) sont deux éléments de B, $x + y$ désignera l'élément

$$(x_0 + y_0, x_1 + y_1, x_2 + y_2, \ldots, x_i + y_i, \ldots)$$

(à nouveau toutes les composantes sont nulles sauf un nombre fini d'entre elles).

Passons à la **multiplication** . Nous conviendrons d'appeler produit de x par y l'élément z de B donné par :

$$(x_0y_0, x_1y_0 + y_1x_0, x_2y_0 + x_1y_1 + y_2x_0, \ldots).$$

Autrement dit, la i-ème composante z_i de z est donnée par :

$$z_i = x_0y_i + x_1y_{i-1} + x_2y_{i-2} + \ldots + x_ky_{i-k} + \ldots + x_iy_0 = \sum_{k=0}^{i} x_ky_{i-k}.$$

Nous laissons au lecteur le soin de montrer que nous avons bien défini un anneau commutatif.

■ On pose $T = (0, 1, 0, \ldots, 0, \ldots)$. On note $A[T]$ l'anneau B que nous venons de construire. On dit que $A[T]$ est l'anneau des polynômes en une variable à coefficients dans A. On appelle T « **indéterminée** » ou « **variable** ». Tout élément non nul de $A[T]$ se représente comme une suite

$$(a_0, a_1, \ldots, a_n, 0, \ldots)$$

($a_n \neq 0$ et tous les a_i sont nuls pour i strictement supérieur à n). Un tel élément s'écrit habituellement sous la forme :

$$a_0 + a_1T + a_2T^2 + \ldots + a_nT^n.$$

Les éléments a_i de A, qui interviennent dans cette écriture, sont appelés les **coefficients du polynôme** .

Si tous les a_i sont nuls pour $i > 0$, on dit qu'il s'agit d'un polynôme constant. Le coefficient a_0 est dénommé **coefficient constant** .

On appelle monôme de degré i un polynôme du type a_iT^i, avec $a_i \neq 0$.

Le **degré** d'un polynôme non nul est celui de son monôme de degré le plus élevé. Nous définissons le degré d'un polynôme constant non nul comme égal à 0 et nous convenons que le degré du polynôme nul est égal à $-\infty$.

L'addition pour l'anneau consiste à faire la somme (dans A) des coefficients des monômes de même degré.

La multiplication s'obtient par distributivité et par la règle de produit des monômes :

$$(a_iT^i)(a_jT^j) = a_ia_jT^{i+j}.$$

L'application $A \to A[T]$ qui, à tout élément de A, associe le polynôme constant lui correspondant est un morphisme injectif d'anneaux ; ainsi l'anneau A est un sous-anneau de $A[T]$. Les polynômes constants sont évidemment les éléments de ce sous-anneau ; ce sont ceux qui ne font pas intervenir l'indéterminée.

Deux polynômes sont égaux si, et seulement si, tous leurs coefficients de monômes de même degré sont égaux.

■ Il y a souvent confusion entre les **notions de polynôme et d'application polynomiale** ; c'est pourquoi il est nécessaire de préciser leurs relations.

Nous avons, d'abord, construit l'anneau $A[T]$ en définissant ses éléments comme des expressions formelles et c'est ainsi qu'il faut considérer un polynôme.

Cependant, au polynôme $\sum_{i=0}^{n} a_iT^i$, on peut associer l'application f :

$$A \to A$$

$$\alpha \mapsto \sum_{i=0}^{n} a_i\alpha^i.$$

Une telle application f est appelée application polynomiale.

Rappelons que deux applications f et g de A dans A sont dites égales si

$$f(x) = g(x)$$

pour tout x dans A. Sur certains anneaux, on peut trouver des polynômes distincts qui correspondent à la même fonction. Pour illustrer, donnons un exemple sur le corps $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$. Les polynômes $T + 1$ et $T^2 + 1$ sont distincts ; néanmoins les fonctions correspondantes de $\mathbb{F}_2$ dans lui-même sont égales.

2.2.2 Polynômes en une indéterminée sur un corps

A partir de maintenant, nous allons nous placer non pas sur un anneau A mais sur un corps commutatif K et nous énoncerons certaines propriétés de l'anneau $K[T]$. Comme le lecteur va le constater, cet anneau a des propriétés qui rappellent celles de $\mathbb{Z}$.

Commençons par noter que, dans $K[T]$, le degré du produit de deux polynômes non nuls est égal à la somme des degrés de ces polynômes (avec la convention habituelle pour le degré du polynôme nul : $-\infty + n = -\infty$ pour tout entier naturel n).

Proposition 9.

L'ensemble des polynômes inversibles de $K[T]$ est l'ensemble K^* des constantes non nulles.

Preuve. ◊ La preuve est une conséquence directe du fait que si f et g sont deux polynômes non nuls, le degré du produit fg est égal à la somme des degrés de f et g. ◊

Proposition 10.

L'anneau $K[T]$ est un anneau intègre, c'est-à-dire que, si le produit de deux polynômes est nul, l'un des deux facteurs au moins est nul.

Preuve. ◊ C'est le même argument que la preuve de la proposition **9**. ◊

Définition 3. Soit $f(T)$ un polynôme à coefficients dans K.
On dit qu'un élément a de K est une racine de $f(T)$ si l'application polynomiale associée à $f(T)$ s'annule en a.

Souvent, on a d'autres formulations pour exprimer que a est une racine. Par exemple, on dit que $f(a) = 0$ ou que f s'annule lorsqu'on substitue a à T.

Définition 4. Soit $f(T)$ un polynôme de $K[T]$.
On dit que le polynôme $g(T)$ divise $f(T)$ dans $K[T]$ et l'on écrit

$$g(T) \mid f(T)$$

s'il existe un polynôme $h(T)$ dans $K[T]$ tel que

$$f(T) = g(T)\, h(T).$$

Définition 5. Soit $f(T)$ un polynôme non constant de $K[T]$.
On dit qu'il est **irréductible** si tout polynôme qui le divise est soit de même degré que f, soit constant.

Il découle immédiatement de la définition **5** que tout polynôme de degré 1 est irréductible.

Proposition 11.

Soient f un polynôme non constant en T, à coefficients dans K, et $b \in K$; alors $T - b$ divise le polynôme $f(T) - f(b)$.

Preuve. ◊ Posons $f(T) = \sum_{i=0}^{n} a_i T^i$. On a :

$$\begin{aligned} f(T) - f(b) &= \sum_{i=0}^{n} a_i T^i - \sum_{i=0}^{n} a_i b^i \\ &= \sum_{i=0}^{n} a_i (T^i - b^i) \\ &= \sum_{i=0}^{n} a_i \left[(T-b) \left(\sum_{j=0}^{i-1} T^j b^{i-1-j} \right) \right] \\ &= (T-b) \sum_{i=0}^{n} a_i \left(\sum_{j=0}^{i-1} T^j b^{i-1-j} \right), \end{aligned}$$

ce qui fait apparaître la divisibilité par le facteur $T - b$.◊

Théorème 7. Soient f un polynôme en T, à coefficients dans K, et a une racine de f. Alors $T - a$ divise f.

Preuve. ◊ C'est une application de la proposition **11** : $T - a$ divise

$$f(T) - f(a) = f(T). \qquad ◊$$

Définition 6. Soit m un entier positif.
On dit qu'une racine a d'un polynôme $f(T)$ est de multiplicité m si $(T-a)^m$ est la plus grande puissance du polynôme $T - a$ qui divise $f(T)$.

Corollaire 5.

Soit $f(T)$ un polynôme non constant, de degré n, dans $K[T]$. Alors $f(T)$ a au plus n racines.

Le résultat suivant affirme que l'on peut faire une division polynomiale, à l'image de la division des entiers, avec un reste de degré strictement inférieur au degré du diviseur. On note $\deg f$ ou $\deg(f)$ le degré d'un polynôme f.

Théorème 8. Soient f et g deux polynômes à coefficients dans K. Il existe deux autres polynômes (le quotient et le reste), notés q et r, uniquement déterminés par les propriétés :

$$g = fq + r$$

et

$$\deg r < \deg f.$$

■ A l'image de ce qui se passe dans $\mathbb{Z}$ (§ 2.1.1.2), on a, dans $K[T]$, la **notion de « plus grand commun diviseur »** (pgcd) de deux polynômes. Dans le cas de deux polynômes, le pgcd n'est pas unique, mais deux d'entre eux diffèrent par le produit d'une constante non nulle. Ce qui empêche l'unicité est l'existence d'éléments inversibles dans l'anneau $K[T]$, dont l'ensemble, comme nous l'avons vu (proposition **9**), n'est autre que K^*. Dans $\mathbb{Z}$ où les seuls inversibles étaient 1 et –1, on avait obtenu l'unicité en prenant pour pgcd de deux entiers leur plus grand diviseur **positif**. Nous allons voir à la fin de ce paragraphe comment on peut également assurer une certaine unicité avec les polynômes à condition de se restreindre aux polynômes « unitaires » (qui sont, de ce point de vue, l'équivalent des nombres entiers strictement positifs).

Définition 7. Soient f et g deux polynômes à coefficients dans K.
On dit qu'un polynôme u est pgcd de f et g si $u \mid f$, $u \mid g$ et tout polynôme h vérifiant $h \mid f$ et $h \mid g$ est de degré inférieur ou égal à celui de u.

Définition 8. Soient f et g deux polynômes à coefficients dans K.
On dit que ces deux polynômes sont associés s'il existe une constante non nulle (c'est-à-dire un élément de K^*) α telle que

$$f = \alpha g.$$

Proposition 12.

Soient f et g deux polynômes à coefficients dans K, u et v deux pgcd de f et g. Alors u et v sont deux polynômes associés.

■ Comme dans le cas des entiers (§ 2.1.1.5), il existe un moyen pratique de calculer un pgcd de deux polynômes. Cet algorithme porte également le nom d'**algorithme d'Euclide**. Il procède de manière

identique. Soit à calculer un pgcd de f et g, on effectue la suite de divisions suivantes jusqu'à obtenir un reste nul :

$$g = fq_0 + r_0$$
$$f = r_0q_1 + r_1$$
$$r_0 = r_1q_2 + r_2$$
$$r_1 = r_2q_3 + r_3$$
$$\vdots$$
$$r_{n-2} = r_{n-1}q_n + r_n$$
$$r_{n-1} = r_nq_{n+1} + 0$$

Puisque $\deg(r_0) < \deg(f)$, $\deg(r_1) < \deg(r_0)$, etc., il faut *au plus* $\deg(f)$ étapes pour aboutir à un reste nul.

Le théorème **9** se démontre comme dans le cas des entiers par simple vérification.

Théorème 9. Dans l'algorithme d'Euclide, le dernier reste non nul r_n est un pgcd de f et g.

Nous ne donnons pas, ici, la vérification de l'exemple qui suit.

Exemples 2 :

Dans l'anneau $\mathbb{F}_2[T]$, on a :

$$\text{pgcd}\,(T^2 + 1,\ T^5 + 1) = T + 1$$

Dans l'anneau $\mathbb{F}_3[T]$, on a :

$$\text{pgcd}\,(T^3 - T^2 - 1,\ T^3 + T + 1) = T^2 + T - 1.$$

Théorème 10 (de Bézout). Soit d un pgcd de f et g. Alors d peut être écrit sous la forme

$$d = af + bg$$

où a et b sont deux éléments de $K[T]$.

Définition 9. On dit que deux polynômes sont ***premiers entre eux*** ou ***étrangers*** s'ils admettent pour plus grand commun diviseur une constante non nulle.

La notion de **polynôme unitaire** permettra de simplifier un énoncé fondamental dans la suite (corollaire **6**).

Définition 10. Soit $f(T)$ un polynôme non nul de $K[T]$.

On dit que ce ***polynôme*** est ***unitaire*** si le coefficient de son terme de plus haut degré est égal à 1.

Proposition 13.

Tout polynôme non nul de $K[T]$ est associé à un unique polynôme unitaire.

Preuve. ◊ Soit $f(T) = \sum_{i=0}^{n} a_i T^i$ un polynôme de degré $n \geqslant 1$ à coefficients dans K. Le coefficient a_n n'étant pas nul, il est inversible dans K et on peut le mettre en facteur dans le polynôme :

$$f(T) = a_n \sum_{i=0}^{n} \frac{a_i}{a_n} T^i.$$

Le polynôme $f(T)$ apparaît ainsi comme associé au polynôme unitaire $\sum_{i=0}^{n} \frac{a_i}{a_n} T^i$ et la proposition est établie. ◊

On peut ainsi affirmer que le pgcd de deux polynômes est unique si l'on exige qu'il soit unitaire.

Définition 11. Un anneau A est dit principal s'il est intègre et si tout idéal I de cet anneau est engendré par un élément $a \in A$.

Rappelons que, dans un anneau A, l'idéal, engendré par les éléments a_1, a_2, ..., a_n, est l'ensemble $a_1A + a_2A + \ldots + a_nA$ des éléments de l'anneau qui s'écrivent comme somme d'un multiple de a_1, d'un multiple de a_2, ..., et d'un multiple de a_n. En particulier, l'idéal engendré par un seul élément a est l'ensemble aA des multiples de a.

Théorème 11. Pour tout corps K, l'anneau $K[T]$ des polynômes en une variable sur K est principal.

2.2.3 Factorisation des polynômes de $K[T]$ en produits de polynômes irréductibles

Théorème 12. Soit $f(T)$ un polynôme à coefficients dans le corps K. Alors, ou bien f est irréductible ou bien f se factorise en un produit de polynômes irréductibles.

Théorème 13. Si $f = p_1p_2 \ldots p_s = q_1q_2 \ldots q_t$ sont deux factorisations en produit de polynômes irréductibles d'un polynôme de $K[T]$, alors

$$s = t$$

et on peut réordonner les polynômes q_{i_1} , $0 \leqslant i \leqslant s$, au moyen d'une permutation τ de $\{1, \ldots, s\}$ en

$$q_{\tau(1)}, q_{\tau(2)}, \ldots, q_{\tau(s)}$$

de sorte que p_i et $q_{\tau(i)}$ soient associés (c'est-à-dire on passe de l'un à l'autre en multipliant par une constante non nulle).

Ce dernier résultat peut s'énoncer de manière plus claire en utilisant la notion de polynôme unitaire.

Corollaire 6.

Soit $f(T)$ un polynôme non constant à coefficients dans un corps K.

Alors $f(T)$ a une factorisation unique sous la forme :

$$f(T) = \alpha p_1^{a_1}(T) p_2^{a_2}(T) \ldots p_r^{a_r}(T)$$

où α est un élément de K^* et où les $p_i(T)$, $1 \leqslant i \leqslant r$, sont des polynômes irréductibles et unitaires de $K[T]$ distincts deux à deux.

Exemples 3 :

Le lecteur pourra vérifier les calculs suivants à l'aide de son système de calcul formel préféré.

Dans $\mathbb{Q}[T]$:

$$-1 + T^8 = (-1 + T)(1 + T)(1 + T^2)(1 + T^4).$$

Par contre, dans le même anneau $-1 + T^2 + T^4 + T^6 + T^8$ est irréductible.

Voici un exemple de factorisation du même polynôme sur différents corps, vérifiable à l'aide de tout logiciel de calcul formel. Nous allons observer la factorisation du polynôme $-1 + T^2 + T^4 + T^6 + T^8$, considéré successivement comme polynôme à coefficients dans $\mathbb{Q}$, $\mathbb{F}_2$, $\mathbb{F}_3$, $\mathbb{F}_5$ et $\mathbb{F}_7$.

Sur $\mathbb{Q}$; ce polynôme est irréductible.

Sur $\mathbb{F}_2$:

$$1 + T^2 + T^4 + T^6 + T^8 = (1 + T + T^2 + T^3 + T^4)^2.$$

Sur $\mathbb{F}_3$:

$$-1 + T^2 + T^4 + T^6 + T^8 = (1 + T)(2 + T)(1 + 2T^4 + T^6).$$

Sur $\mathbb{F}_5$:

$$-1 + T^2 + T^4 + T^6 + T^8 = (2 + 2T + 2T^3 + T^4)(2 + 3T + 3T^3 + T^4).$$

Sur $\mathbb{F}_7$:

$$-1 + T^2 + T^4 + T^6 + T^8 = (4 + T^2)(3 + 3T + 4T^2 + T^3)(4 + 3T + 3T^2 + T^3).$$

Comme nous l'avons déjà dit (§ 2.2.2), sur tout corps, les polynômes de degré un sont irréductibles.

Dans $\mathbb{C}[T]$, ce sont les seuls (le corps des nombres complexes est algébriquement clos).

Dans $\mathbb{R}[T]$, les polynômes irréductibles sont les polynômes de degré un et les polynômes de degré deux à discriminant négatif.

Par contre, sur $\mathbb{Q}$, on démontre qu'il existe des polynômes irréductibles de tout degré et le même résultat est vrai sur le corps $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ pour un nombre premier p.

Si K est un sous-corps de L, un polynôme à coefficients dans K irréductible sur L est à fortiori irréductible sur K, mais un polynôme de $K[T]$ irréductible peut se factoriser dans $L[T]$.

On peut citer, par exemple $T^2 + 1$, irréductible sur $\mathbb{R}$, mais qui s'écrit aussi $(T + i)(T - i)$ sur $\mathbb{C}$; $T^4 + 1$, irréductible sur $\mathbb{Q}$, qui se factorise sur $\mathbb{R}$ en $(T^2 + \sqrt{2}\,T + 1)(T^2 - \sqrt{2}\,T + 1)$.

La notion d'irréductibilité d'un polynôme en une variable est donc relative à un corps de référence.

2.2.4 Quotients d'anneaux de polynômes

On a vu, dans le paragraphe (§ 2.2.2) (proposition **11**) que tout idéal I de $K[T]$ était l'ensemble des multiples d'un polynôme donné $f(T)$, ce qui se note

$$I = (f(T)).$$

On peut établir que les autres générateurs de I sont les polynômes associés de f. En effet, si I n'est pas l'idéal nul ni l'anneau tout entier, il possède au moins un polynôme $f(T)$ non constant de degré minimal, disons d.

Soit $g(T) = \alpha f(T)$ avec $\alpha \in K^*$ un polynôme associé de f ; alors, on a

$$I = (g(T)).$$

Réciproquement, si g est un polynôme de degré d qui engendre I, alors g est un multiple $h(T)\,f(T)$ de f, mais, comme les degrés de f et g sont égaux, cela signifie que h est une constante non nulle.

Trivialement, si f est une constante non nulle, $K[T]/(f(T))$ est l'anneau nul et, si $f = 0$, on a l'isomorphisme d'anneaux

$$K[T]/(0) \simeq K[T].$$

Théorème 14. Soit $f(T) \in K[T]$ un polynôme de degré $d \geqslant 1$. Alors, si l'on note t la classe de T dans l'anneau quotient $A = K[T]/(f(T))$, cet anneau est le K espace vectoriel de base $(1, t, t^2, \ldots, t^{d-1})$.

Preuve. ◊ La structure d'espace vectoriel ne pose pas de problème à établir.

Soit g un polynôme à coefficients dans K. Si l'on effectue la division euclidienne de g par f, on obtient un reste $h(T)$ de degré au plus $d - 1$. Ainsi, toute classe modulo l'idéal $(f(T))$ admet un représentant qui est polynôme de degré au plus $d - 1$; ce polynôme est unique, car deux polynômes distincts de degrés inférieurs ou égaux à $d - 1$ ne peuvent être équivalents (cela signifierait que leur différence est un multiple non nul de f, ce qui est impossible pour des raisons de degré). Cela montre que les classes de $1, T, T^2, \ldots, T^{d-1}$ forment une base de A comme K espace vectoriel. ◊

Cette description permet de comprendre comment calculer explicitement dans l'anneau A. On peut toujours choisir le polynôme f unitaire, ce que nous allons supposer :

$$f(T) = \sum_{j=0}^{d-1} a_j T^j + T^d.$$

Chaque élément de A se représente alors de manière unique comme un « polynôme » en t de degré au plus $d - 1$. L'addition est ce qu'on imagine ; quant à la multiplication, on l'obtient par la multiplication des polynômes, puis la règle de simplification

$$t^d = -\sum_{j=0}^{d-1} a_j t^j,$$

car t est une racine dans A du polynôme $f(T)$.

Théorème 15. Soit $f(T) \in K[T]$. Alors l'anneau quotient $A = K[T]/(f(T))$ est un corps si, et seulement si, le polynôme f est irréductible sur K.

Preuve. ◊ C'est une conséquence immédiate de la relation de Bézout (dans théorème **10**) : f est irréductible s'il est premier à tout polynôme non nul de degré strictement inférieur. ◊

Dans le contexte du théorème **15**, ou f est irréductible, on dit que A est une extension de degré d de K ; en particulier, les extensions de degré 2 sont appelées extensions quadratiques.

Prendre le quotient de $K[T]$ par l'idéal engendré par un polynôme $f(T)$ irréductible sur K consiste en fait à grossir le corps K en le surcorps L le plus petit possible contenant K et une racine de f. Si K est un corps fini, L contient nécessairement toutes les autres racines de f (on dit que l'extension est galoisienne), mais cela n'est pas vrai en général.

Pour s'en convaincre, on peut prendre le corps $\mathbb{Q}$ et le polynôme irréductible $T^3 - 2$; le corps $\mathbb{Q}[T]/(T^3 - 2)$ est une extension cubique (c'est-à-dire de degré 3) de $\mathbb{Q}$ qui ne contient qu'une racine de $T^3 - 2$.

Corollaire 7.

Soit $f(T) \in K[T]$. Alors si l'anneau quotient $A = K[T]/(f(T))$ est intègre, c'est un corps.

Preuve. ◊ Dire que A n'est pas intègre signifie qu'il existe deux polynômes g et h de degrés strictement inférieurs à celui de f et tels que le produit gh soit un multiple de f ; cela revient à dire que f n'est pas irréductible donc que f n'est pas un corps. ◊

Le corollaire **7** est une spécificité du type d'anneau que nous étudions ici (quotient d'anneau de polynômes en une variable). En général, si un anneau A est un corps, il est intègre, mais la réciproque est fausse ; ainsi, $\mathbb{Z}$ est un anneau intègre mais n'est pas un corps.

2.2.5 Polynômes à plusieurs indéterminées sur un corps *K*

Nous avons montré (§ 2.2.1) comment construire à partir d'un anneau A l'anneau $A[T]$. Cette construction peut être itérée. Partons d'un corps K, on sait donc construire l'anneau $K[X]$; partant de cet anneau et notant Y une nouvelle indéterminée, on peut construire l'anneau $K[X][Y]$ des polynômes en Y à coefficients dans $K[X]$. La multiplication étant commutative, X et Y jouent un rôle symétrique et

$$K[X][Y] = K[Y][X],$$

ce qui justifie la notation $K[X, Y]$ pour cet anneau. Ses éléments sont appelés polynômes à deux variables sur le corps K et sont des expressions du type

$$\sum_{i,j \in \mathbb{N}} a_{i,j} X^i Y^j$$

avec seulement un nombre fini de coefficients $a_{i,j}$ (qui sont des éléments de K) non nuls.

Un polynôme du type aX^iY^j est appelé **monôme** ; le degré total de ce monôme est le nombre $i + j$, son degré en X est i, son degré en Y est j.

Le **degré total d'un polynôme** est le plus grand des degrés totaux de ses monômes, le degré en X le plus grand degré en X de ses monômes et de même pour le degré en Y.

Il n'y a pas de raison de s'arrêter à deux variables et on peut ainsi construire l'anneau $K[X_1, X_2, ..., X_n]$ en les n variables $X_1, X_2, ..., X_n$ à coefficients sur K.

La notion de **polynôme irréductible** existe encore et on a une décomposition unique à un facteur multiplicatif près (du type indiqué paragraphe 2.2.2 pour le cas à une variable) en produit de polynômes irréductibles.

Comme précédemment (§ 2.2.3), des polynômes irréductibles sur un corps peuvent se **factoriser** sur un corps plus gros, par exemple $X^2 + Y^2$ est irréductible sur $\mathbb{R}$, mais se factorise en $(X + iY)(X - iY)$ sur $\mathbb{C}$. Néanmoins, contrairement à ce que suggère ce dernier exemple, même sur $\mathbb{C}$, tous les polynômes irréductibles à plusieurs variables ne sont pas de degré 1.

Comme nous l'avons fait (§ 2.2.1), il faut considérer un polynôme $f(X_1, X_2, ..., X_n)$ en n variables comme une expression formelle, mais il importe de comprendre également qu'il définit une application (dite polynomiale) notée en général f :

$$K^n \to K$$

$$(a_1, a_2, ..., a_n) \mapsto f(a_1, a_2, ..., a_n).$$

2.2.6 Théorème chinois

Comme dans le cas de $\mathbb{Z}$ (théorème **6**), on a ici un « théorème chinois ».

Théorème 16. Soient K un corps, $f(T)$ et $g(T)$ deux polynômes de $K[T]$ premiers entre eux. Alors on a l'isomorphisme canonique

$$K[T]/(f(T)\,g(T)) \to K[T]/(f(T)) \times K[T]/(g(T))$$

$$h(T) \mapsto (h(T) \text{ modulo } f(T),\ h(T) \text{ modulo } g(T)).$$

Soient $f \in K[T]$ un polynôme et

$$f = f_1^{a_1} f_2^{a_2} \dots f_r^{a_r}$$

sa factorisation sous forme de puissances de polynômes irréductibles distincts de $K[T]$.

Alors on a un isomorphisme canonique d'anneaux :

$$(\mathbb{K}[T]/(f) \to K[T])/(f_1^{a_1}) \times K[T]/(f_2^{a_2}) \times \dots \times K[T]/(f_r^{a_r})$$

$$g(T) \bmod f \mapsto \left(g(T) \bmod f_1^{a_1}(T),\ g(T) \bmod f_2^{a_2}(T),\ \dots,\ g(T) \bmod f_r^{a_r}(T)\right).$$

2.2.7 Corps finis

Nous avons déjà rencontré (§ 2.2.3) des corps finis, les corps $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ pour tout nombre premier p. Il en existe d'autres et nous résumons ici rapidement ce qu'il nous faut connaître de la théorie des corps finis pour nos besoins cryptographiques.

■ Nous énonçons et admettons les **résultats suivants sur les corps finis**.

• Tout corps fini est commutatif (théorème de **Wedderburn**).

• Soit k un corps fini ; alors, son cardinal est une puissance d'un nombre premier p.

• Soient p un nombre premier et $n > 0$ un entier ; il existe un corps fini k, et un seul à isomorphisme près, de cardinal p^n. On dit que c'est le corps fini à p^n éléments, on le note $\mathbb{F}_{p^n}$ (pour le mot anglais « *field* ») ou bien $GF(p^n)$ (pour « *Galois field* », du nom du mathématicien français Évariste Galois, car on appelle aussi les corps finis les **corps de Galois**).

• Soit p un nombre premier. Le corps $\mathbb{F}_p$ n'est autre que $\mathbb{Z}/p\mathbb{Z}$.

• Le corps $\mathbb{F}_{p^m}$ est contenu dans le corps $\mathbb{F}_{p^n}$ si, et seulement si, $m|n$.

• Soit q une puissance d'un nombre premier p et $n > 0$ un entier. Le corps $\mathbb{F}_{q^n}$ est isomorphe au quotient de l'anneau de polynômes $\mathbb{F}_q[T]$ par tout idéal engendré par un polynôme irréductible de dégré n.

• Le groupe multiplicatif d'un corps fini est cyclique, par conséquent on a :

$$\mathbb{F}_q^* \simeq \mathbb{Z}/(q-1)\mathbb{Z},$$

mais cet isomorphisme n'est pas canonique.

■ Si un corps fini a un nombre d'éléments qui est une puissance du nombre premier p, il contient $\mathbb{Z}/p\mathbb{Z}$, comme nous venons de le voir. Ainsi, dans ce corps :

$$p = 1 + 1 + \dots + 1\ (p \text{ fois}) = 0\ ;$$

on dit qu'il est de caractéristique p.

Le lecteur prendra bien garde au fait que si $n > 1$, le corps $\mathbb{F}_{p^n}$ n'est pas l'anneau $\mathbb{Z}/p^n\mathbb{Z}$. Le groupe additif de ce corps est, par contre, isomorphe au produit direct $(\mathbb{Z}/p\mathbb{Z})^n$: c'est immédiat si l'on a compris que $\mathbb{F}_{p^n}$ et un $\mathbb{F}_p$ espace vectoriel de dimension n.

■ Nous allons décrire explicitement, à titre d'exemple, le corps fini à 4 éléments $\mathbb{F}_4$. Le polynôme $T^2 + T + 1$ est irréductible sur $\mathbb{F}_2$ puisqu'il n'a pas de racine. En effet, s'il avait un diviseur de degré un, il aurait une racine dans le corps à deux éléments. Par conséquent, le corps à quatre éléments est l'anneau quotient $\mathbb{F}_2[T]/(T^2 + T + 1)$. Notons dans ce quotient t la classe du polynôme T modulo $T^2 + T + 1$, on a alors :

$$\mathbb{F}_4 = \{0, 1, t, 1 + t\}$$

et les tables d'addition et de multiplication données par les tableaux **6** et **7**.

Tableau 6 – Table d'addition dans $\mathbb{F}_4$

+	0	1	t	$1 + t$
0	0	1	t	$1 + t$
1	1	0	$1 + t$	t
t	t	$1 + t$	0	1
$1 + t$	$1 + t$	t	1	0

Tableau 7 – Table de multiplication dans $\mathbb{F}_4$

x	0	1	t	$1 + t$
0	0	0	0	0
1	0	1	t	$1 + t$
t	0	t	$1 + t$	1
$1 + t$	0	$1 + t$	1	t

2.3 Suites récurrentes linéaires sur un corps fini

2.3.1 Généralités

Ce paragraphe est une simple énumération de propriétés des suites récurrentes linéaires sur un corps fini. Les démonstrations se trouvent, par exemple, dans le mémoire de Selmer [49] ou celui de Ferrand [18]. La référence classique (en particulier peut-être pour les non mathématiciens) est le livre de Golomb [21].

Nous noterons k le corps fini $\mathbb{F}_q$ à q éléments où q est une puissance du nombre premier p. Dans la pratique, on a souvent :

$$p = q = 2.$$

■ Il existe une **opération** de l'anneau **des polynômes** en une variable $k[T]$ sur l'ensemble $k^{\mathbb{N}}$ des suites à valeurs dans k, très utile pour comprendre les calculs que nous aurons à réaliser sur ces suites.

Soit s une telle suite :

$$s = (s_i)_{i \in \mathbb{N}},\ s_i \in k.$$

Nous allons noter $T.s$ la suite obtenue à partir de s en supprimant le terme s_0 (c'est-à-dire la suite obtenue par « décalage à gauche ») :

$$(T.s)_i = s_{i+1} \text{ pour tout } i \in \mathbb{N}$$

On dit que T est l'opérateur de décalage.

Soit f un polynôme de $K[T]$. On peut également le faire agir sur la suite s. Si :

$$f(T) = a_0 + a_1 T + \ldots + a_n T^n,$$

on pose, pour définir cette action d'un élément quelconque de $k[T]$:

$$(f(T).s)_i = a_0 s_i + a_1 s_{i+1} + \ldots + a_n s_{i+n}.$$

Par exemple, soient $k = \mathbb{F}_2$ et la suite

$$s = \overline{10010011}$$

où la barre supérieure signifie que ce motif se répète, c'est-à-dire que la suite est périodique.

En faisant agir successivement les « monômes » puissances de T, on obtient :

$$T.s = \overline{0010111},$$

$$T^2.s = \overline{0101110},$$

$$T^3.s = \overline{1011100},$$

et en allant plus loin :

$$T^7.s = \overline{1001011} = s.$$

Cela prouve que :

$$(T^7 + 1).s = 0.$$

Mais, on vérifie aussi facilement que :

$$(T^3 + T + 1).s = 0.$$

On dit que ces deux polynômes $T^3 + T + 1$ et $T^7 + 1$ annulent la suite s.

■ Voyons les **propriétés** de l'action de $k[T]$ **sur les suites** à valeurs dans k qui vient d'être définie.

Soient f et g des polynômes en T à coefficient dans k, s et t deux suites à valeurs dans k ; on a :

$$0.s = 0,$$

$$(f + g).s = f.s + g.s,$$

$$(fg).s = f.(g.s),$$

$$f.(s + t) = f.s + f.t.$$

On sait, par ailleurs, que l'ensemble des suites à valeurs dans k muni de l'addition est un groupe abélien. L'opération des polynômes, que nous avons définie, fait de $k^{\mathbb{N}}$ un $k[T]$ module.

Soit $s \in k^{\mathbb{N}}$. On appelle ***annulateur*** de s l'ensemble :

$$\text{Ann}(s) = \{f(T) \in k[T] ;\ f(T).s = 0\}.$$

Cet ensemble Ann(s) est un idéal (sous-groupe additif stable par la multiplication de tout élément de l'anneau) de l'anneau $k[T]$.

Pour l'exemple, déjà cité :

$$s = \overline{1001011},$$

on peut montrer que

$$\text{Ann}(s) = (T^3 + T^2 + 1) \subset \mathbb{F}_2[T],$$

c'est-à-dire l'idéal engendré par le polynôme $T^3 + T^2 + 1$.

On dit qu'une suite $s \in k^{\mathbb{N}}$ est ***récurrente linéaire*** si Ann(s) $\neq \{0\}$.

On note $\mathcal{S}(k)$ l'ensemble des suites récurrentes linéaires sur k. Cet ensemble est muni de deux structures dont nous aurons besoin :

— c'est un espace vectoriel sur k ;
— c'est un $k[T]$ module.

Nous utilisons en permanence le fait que l'anneau $k[T]$ est un **anneau principal**, c'est-à-dire que tout idéal de cet anneau est engendré par un élément. On sait que tout anneau principal est factoriel, ce qui signifie que tout élément se factorise de manière unique (à la multiplication près par une unité de l'anneau) comme produit de puissances d'éléments indécomposables ou irréductibles ; ceux-ci sont caractérisés par le fait que si on les écrit sous la forme d'un produit de deux facteurs, l'un des facteurs est une unité.

Soit $s \in \mathcal{S}(k)$. L'idéal Ann(s), qui n'est pas nul, est engendré par un unique polynôme unitaire (c'est-à-dire dont le coefficient du monôme de plus haut degré et égal à 1). Ce polynôme est appelé le ***polynôme minimal*** de la suite s.

Soit r le degré du polynôme minimal d'une suite récurrente linéaire ; on dit que la suite est récurrente d'ordre r.

Les suites récurrentes linéaires (en particulier sur le corps à deux éléments $\mathbb{F}_2$) sont, en fait, les suites produites par les dispositifs appelés, notamment par les électroniciens, (registres à décalage et à rétroaction linéaire *linear feedback shift registers* en anglais). Il est commode de représenter un tel mécanisme par la figure **1** dont les boîtes A_i de la première ligne doivent être considérées comme des cellules contenant chacune un élément du corps $\mathbb{F}_q$.

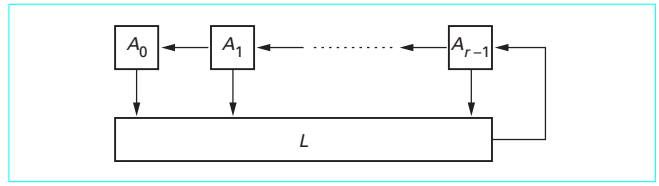

Figure 1 – Registre à décalage et rétroaction linéaire

Pour comprendre cette figure, il faut considérer que, à un instant $t \in \mathbb{N}$, chaque cellule A_i contient un élément du corps $\mathbb{F}_q$ que nous notons $A_i(t)$. A l'instant $t+1$, $A_i(t)$ va dans A_{i-1} pour tout i tel que $1 \leqslant i \leqslant r-1$ et on met dans A_{r-1} l'élément :

$$L(A_0(t), A_1(t), \ldots, A_{r-1}(t)) = \sum_{i=0}^{r-1} a_i A_i(t)$$

où les a_i sont des éléments fixés de $\mathbb{F}_q$.

Regardons la suite $(A_0(t))_{t \in \mathbb{N}}$; c'est une suite dont les r premiers termes sont :

$$A_0(0), A_1(0), \ldots, A_{r-1}(0)$$

c'est-à-dire les contenus initiaux des cellules du registre et qu'annule le polynôme :

$$f(T) = -\sum_{i=0}^{r-1} a_i T^i + T^n \in \mathbb{F}_q[T],$$

parfois appelé **polynôme de rétroaction du registre** .

On peut évidemment considérer des registres à décalage non linéaires, c'est-à-dire dans lesquels la fonction L n'est pas une forme linéaire $\mathbb{F}_q^n \to \mathbb{F}_q$. Cela reviendrait à considérer des suites récurrentes non linéaires sur un corps fini. Ce sujet ne manque certainement pas d'intérêt et il est un peu abordé dans le livre de Golomb [21], mais, à notre connaissance, même aujourd'hui, plus de 30 ans après la publication de ce livre, presque rien n'est connu sur ce sujet si l'on excepte des choses très particulières (liées aux suites de de Bruijn notamment).

2.3.2 Suites récurrentes linéaires sur un corps fini. Suites périodiques

Proposition 14.

Une suite récurrente linéaire sur un corps fini est ultimement périodique (c'est-à-dire périodique à partir d'un certain rang).

Elle est périodique si, et seulement si, son polynôme minimal a un coefficient constant non nul.

Soit $f \in k[T]$ un polynôme de degré d. Nous désignons par $\Omega(f)$ l'ensemble des suites à valeurs dans k annulées par f.

Par exemple, trivialement, $\Omega(0) = k^{\mathbb{N}}$.

Proposition 15.

L'ensemble $\Omega(f)$ est un espace vectoriel sur k de dimension d.

Proposition 16.

Soient f et g deux polynômes à coefficients dans k. Alors, on a :

$$\Omega(f) \subset \Omega(g) \Leftrightarrow f | g.$$

Soit :

$$f = f_1^{\alpha_1} . f_2^{\alpha_2} \ldots f_i^{\alpha_i}$$

la décomposition de f en produit de puissances de polynômes irréductibles distincts deux à deux. A cette décomposition de f correspond une décomposition de $\Omega(f)$.

Proposition 17.

On a un isomorphisme d'espaces vectoriels :

$$\Omega(f) \simeq \bigoplus_{j=1}^{i} \Omega(f_j^{\alpha_j});$$

le terme de droite représente une somme directe d'espaces vectoriels sur k.

Autrement dit, toute suite annulée par f se décompose, de manière unique, en une somme de i suites de $\mathcal{S}(k)$, la première annulée par $f_1^{\alpha_1}$, la seconde par $f_2^{\alpha_2}$, ..., et la i-ième par $f_i^{\alpha_i}$.

Ce dernier résultat suggère la détermination de la structure du k espace vectoriel $\Omega(f^i)$ des suites annulées par la i-ième puissance d'un polynôme f irréductible sur k.

Proposition 18.

Soit f un polynôme de k[T] tel que $f(0) \neq 0$. Il existe alors un entier $e \in \mathbb{N} \setminus \{0\}$ tel que :

$$f(T) \text{ divise } T^e - 1.$$

*Le plus petit e ayant cette propriété est appelé la **période** de f.*

Corollaire 8.

Les racines de f (dans une extension convenable de k) ont pour ordre multiplicatif un diviseur de e.

Rappelons, concernant ce dernier résultat, que, de la théorie des corps, il résulte qu'il existe nécessairement un surcorps commutatif de k (c'est-à-dire un corps contenant k) dans lequel le polynôme se factorise en facteurs de degré un.

Proposition 19.

Soient s une suite récurrente linéaire et f son polynôme minimal. Supposons que $f(0) \neq 0$. Alors la période de s est égale à la période de f.

Corollaire 9.

Soient s une suite récurrente linéaire, f son polynôme minimal et d le degré de ce polynôme. Supposons que $f(0) \neq 0$. La période de f est inférieure ou égale à $q^d - 1$ (on rappelle que $k = \mathbb{F}_q$).

Proposition 20.

Soient s une suite récurrente linéaire, f son polynôme minimal et d le degré de ce polynôme. Supposons que $f(0) \neq 0$ et que, de plus, f est irréductible. La période e de s divise $q^d - 1$ et est égale à l'ordre multiplicatif d'une racine (donc de toutes) de f dans $\mathbb{F}_{q^d}$.

Définition 12. Soit $f \in k[T]$ un polynôme de degré d irréductible. On dit que f est primitif si chacune de ses racines est un générateur du groupe multiplicatif $\mathbb{F}_{q^d}^*$.

Sur $\mathbb{F}_2$, les trois polynômes de degré 4 :

$$T^4 + T^3 + T^3 + T + 1,$$

$$T^4 + T^3 + 1$$

et

$$T^4 + T + 1$$

sont irréductibles ; ce sont d'ailleurs les trois seuls polynômes de degré 4 irréductibles sur ce corps. On peut montrer (par construction explicite de $\mathbb{F}_{16}$ comme quotient de l'anneau des polynômes sur $\mathbb{F}_2$ par l'idéal engendré par le polynôme correspondant et en calculant les puissances successives de la classe de T) que le premier n'est pas primitif (ses racines dans $\mathbb{F}_{16}$ sont d'ordre multiplicatif 5) tandis que les deux derniers le sont.

Parmi tous les polynômes de degré donné, ceux qui sont primitifs permettent de construire des suites récurrentes linéaires de période maximale.

Si le polynôme f est irréductible, de période e, l'espace $\Omega(f)$ contient la suite nulle et des suites de polynôme minimal f, de période $q^e - 1$.

2.3.3 Suite récurrente linéaire et racines du polynôme minimal

Soient $s \in \mathcal{S}(k)$ et $f \in k[T]$, de degré d, son polynôme minimal. On suppose que f n'a pas de racine multiple. Soit K une extension de k contenant les racines de f que nous appellerons $\alpha_1, \alpha_2, \ldots, \alpha_d$.

Théorème 17. Les suites s annulées par f sont exactement celles qui sont définies par des relations du type :

$$s_i = \sum_{j=1}^{d} a_j \alpha_j^i \text{ pour tout } i \in \mathbb{N}$$

pour des constantes a_j, $1 \leqslant j \leqslant d$ dans K.

Si, de plus, f est irréductible, s est à valeurs dans k si, et seulement si, il existe un $a \in K$ tel que :

$$s_i = \sum_{j=1}^{d} a^{q^j} \left(\alpha^{q^j}\right)^i,$$

c'est-à-dire si, et seulement si :

$$s_i = \mathrm{Tr}(a\alpha^i)$$

en notant Tr l'application « trace » $\mathbb{F}_{q^d} \to \mathbb{F}_q$.

2.3.4 Séries formelles et suites récurrentes linéaires

Commençons par quelques notions sur les **séries formelles** en une variable sur le corps k. Une telle série est une expression :

$$U(T) = \sum_{i \in \mathbb{N}} u_i T^i,$$

où T est une indéterminée et les u_i des éléments de k. Le coefficient u_0 est appelé le terme constant de la série U. Ces séries font penser aux séries entières de l'analyse, qui sont des fonctions où l'indéterminée est appelée à être remplacée par un nombre réel ou complexe. Dans ce qui nous préoccupe ici, nous n'aurons à considérer aucune question de convergence, les séries que nous utiliserons ne seront jamais des fonctions ; nous ne nous intéresserons qu'à des opérations formelles sur elles.

L'ensemble $k[[T]]$ de ces séries formelles se construit de manière analogue aux polynômes à coefficients dans k, mais en considérant toutes les suites à coefficients dans k (contrairement à la construction des polynômes exposée paragraphe 2.2.1, où l'on a considéré des suites dont tous les termes étaient nuls sauf un nombre fini d'entre eux).

On définit, sur ces séries formelles, une addition et une multiplication qui prolongent les mêmes opération sur les polynômes. Soient U et V deux éléments de $k[[T]]$:

$$U(T) = \sum_{i \in \mathbb{N}} u_i T^i \text{ et } V(T) = \sum_{i \in \mathbb{N}} v_i T^i.$$

Pour l'addition, on pose :

$$U(T) + V(T) = \sum_{i \in \mathbb{N}} (u_i + v_i) T^i$$

et pour la multiplication :

$$UV(T) = \sum_{i \in \mathbb{N}} \left(\sum_{j=0}^{i} u_j v_{i-j} \right) T^i.$$

Ces deux opérations munissent l'ensemble $k[[T]]$ des séries formelles d'une structure d'anneau. C'est un **anneau principal** (donc factoriel). Il a un seul idéal maximal (c'est-à-dire un idéal contenu dans un seul autre idéal, l'anneau tout entier), celui engendré par T (c'est-à-dire l'ensemble des séries de terme constant nul). C'est ce que l'on appelle un anneau **local** et son groupe multiplicatif est constitué de tous les éléments qui ne sont pas dans l'idéal maximal : ce sont les séries avec terme constant non nul. Ainsi, dans cet anneau, on a :

$$(1-T)^{-1} = \sum_{i \in \mathbb{N}} T^i.$$

L'anneau $k[T]$ des polynômes est un sous-anneau de $k[[T]]$.

L'anneau $k[[T]]$ étant intègre, il possède un corps de fractions que l'on note $k((T))$ et dont on appelle « **séries de Laurent** » les éléments. Une série de Laurent en une variable sur k peu s'écrire sous la forme :

$$U(T) = \sum_{i \geqslant N} u_i T^i$$

pour un $N \in \mathbb{Z}$, le plus petit N tel que $u_N \neq 0$ est appelé l'ordre de la série U et noté $\omega(U)$.

Le corps des fonctions rationnelles en une variable $k(T)$ (corps des fractions de $k[T]$) s'injecte dans $k((T))$.

Considéré comme série de Laurent, une fraction rationnelle $f(T) / g(T)$ écrite sous forme irréductible, avec f et g dans $k[T]$, est dans $k[[T]]$ si, et seulement si, l'ordre de f est supérieur ou égal à celui de g.

Soit $f(T) = a_0 + a_1 T + \ldots + a_d t^d \in k[T]$ de degré d. On appelle polynôme conjugué de f et on note f^* de polynôme :

$$f^*(T) = a_0 T^d + a_1 T^{d-1} + \ldots + a_{d-1} T + a_d.$$

Formellement, on a :

$$f^*(T) = T^d f\left(\frac{1}{T}\right).$$

De plus :

$$\deg(f^*) = d - \omega(f)$$

et :

$$f^{**}(T) = \frac{f(T)}{T^{\omega(f)}}$$

en particulier : $f^{**} = f$ si $f(0) \neq 0$.

A toute suite s à valeurs dans k on peut associer une série formelle $S(s)$ en une variable, à coefficients dans k, appelée la **série génératrice** de s et définie par

$$S = S(s;T) = \sum_{i \in \mathbb{N}} s_i T^i \in k[[T]].$$

Le résultat suivant caractérise la série génératrice d'une suite récurrente linéaire.

Théorème 18. Une suite $s \in k^{\mathbb{N}}$ est récurrente linéaire si, et seulement si, sa série génératrice $S(s;T)$ est une fonction rationnelle. Dans ce cas, on a

$$S(s;T) = \frac{T^{\omega(s)} P(T)}{f^*(T)}$$

où $\omega(s)$ désigne l'ordre de $S(s;T)$, f^* est le polynôme conjugué du polynôme minimal f de s et $P(T)$ est un polynôme de degré strictement inférieur à celui de f qui dépend des d premiers termes de s et des coefficients de f.

2.3.5 Algorithme de Massey-Berlekamp et complexité linéaire d'une suite

Nous reprenons ici le vocabulaire de D. Ferrand [18], dont nous recommandons la lecture pour une étude approfondie de l'algorithme de Massey-Berlekamp.

Définition 13. Soit s une suite à valeurs dans k.

On dit qu'un polynôme unitaire

$$f(T) = a_0 + a_1 T + \ldots + a_{L-1} T^{L-1} + T^L \in k[T]$$

de degré L relie les $N+1$ premiers termes de s ou bien est un N-relateur de s si l'on a :

$$(f.s)_n = a_0 s_n + a_1 s_{n+1} + \ldots + a_{L-1} s_{n+L-1} + s_{n+L} = 0 \; \forall n, \; 0 \leqslant n < N - L.$$

On dit que f est un N-relateur minimal si son degré L est minimal parmi les degrés des polynômes qui relient les N premiers termes de s ; dans ce contexte, le nombre L est appelé la complexité linéaire de la suite finie $(s_n)_{0 \leqslant n \leqslant N}$.

Le terme « ***N*-relateur minimal** » est la traduction du « *minimal length linear feedback shift register* (LFSR) » de Massey [32].

L'algorithme de Massey-Berlekamp, décrit dans [32], fournit, à partir de la suite finie $(s_n)_{0 \leqslant n \leqslant N}$, un N-relateur minimal de cette suite finie.

Par conséquent, si l'on connaît $2L + 1$ éléments consécutifs d'une suite récurrente linéaire d'ordre L (c'est-à-dire dont le polynôme minimal est de degré L), l'algorithme de Massey-Berlekamp produit ce polynôme minimal. Dans ce cas, le nombre L est aussi appelé la **complexité linéaire de la suite** .

Nous précisons bien qu'il ne faut pas confondre la période et complexité linéaire d'une suite : soit $s \in \mathcal{S}(k)$ une suite admettant un polynôme minimal primitif de degré L (c'est-à-dire une suite de complexité linéaire égale à L), sa période (si elle n'est pas la suite nulle) sera $2^L - 1$, ce qui est très différent de L.

2.4 Fonctions booléennes

On appelle souvent **fonctions booléennes** (surtout si $q = 2$) les applications $f : \mathbb{F}_q^n \to \mathbb{F}_q$. Comme $\mathbb{F}_q$ est un anneau, l'ensemble des applications de $\mathbb{F}_q^n$ dans $\mathbb{F}_q$ a aussi une structure d'anneau induite par l'addition et la multiplication dans $\mathbb{F}_q$. Ces applications ont une forme polynomiale que nous allons étudier.

Commençons par le cas de $n = 1$.

Dans ce paragraphe, nous notons, comme c'est l'usage, E^F l'ensemble des applications d'un ensemble F dans un ensemble E.

Théorème 19. Soit f une application $\mathbb{F}_q \to \mathbb{F}_q$. Alors f peut se représenter sous la forme d'un polynôme en une variable, de degré inférieur ou égal à $q - 1$, à coefficients dans $\mathbb{F}_q$. Plus précisément, on a un isomorphisme d'anneaux :

$$\mathbb{F}_q[X]/(X^q - X) \to \mathbb{F}_q^{\mathbb{F}_q}.$$

Preuve. ◊ Tout polynôme peut s'interpréter comme une application de $\mathbb{F}_q$ dans $\mathbb{F}_q$, ce qui nous fournit une application θ :

$$\mathbb{F}_q[X] \to \mathbb{F}_q^{\mathbb{F}_q}.$$

Par cette correspondance θ, le polynôme nul est envoyé sur l'application nulle et le polynôme 1 est envoyé sur l'application constante 1, élément neutre de la multiplication des applications.

De même, une somme de polynômes est envoyée sur la somme correspondante d'applications et un produit de polynômes sur le produit des applications des correspondantes. Nous avons donc affaire à un **morphisme d'anneaux**.

Soit g un élément du noyau de ce morphisme d'anneaux. Alors g admet pour racines tous les éléments de $\mathbb{F}_q$. Il est bien connu que cela entraîne que :

$$X^q - X \mid g$$

(il suffit de vérifier que les racines du polynôme $X^q - X$ sont exactement les éléments de $\mathbb{F}_q$), donc $g \in (X^q - X)$.

Inversement, tout élément de l'idéal $(X^q - X) \subset \mathbb{F}_q[X]$ s'annule sur $\mathbb{F}_q$. Ainsi

$$\ker(\theta) = (X^q - X)$$

et, par passage au quotient, θ induit un morphisme d'anneaux injectif :

$$\mathbb{F}_q[X]/(X^q - X) \to \mathbb{F}_q^{\mathbb{F}_q}.$$

Que ce morphisme soit aussi surjectif résulte du fait que les deux anneaux sont finis et de même cardinal. ◊

Théorème 20. L'anneau des fonctions booléennes $\mathbb{F}_q^{\mathbb{F}_q^n}$ est canoniquement isomorphe à l'anneau quotient :

$$\mathbb{F}_q[Y_1, Y_2, \ldots, Y_n]/(Y_1^q - Y_1, Y_2^q - Y_2, \ldots, Y_n^q - Y_n).$$

Preuve. ◊ Soit ψ une application $\mathbb{F}_q^n \to \mathbb{F}_q$. Choisissons un isomorphisme de $\mathbb{F}_q$ espaces vectoriels $\Theta : \mathbb{F}_q^n \to \mathbb{F}_{q^n}$ (un tel isomorphisme existe, mais il n'en est pas de canonique si $n > 1$). Cela revient à choisir une base $(\xi_1 = 1, \xi_2, \ldots, \xi_n)$ de $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$ et à poser que Θ est l'application :

$$(y_1, y_2, \ldots, y_n) \mapsto \sum_{i=1}^{n} y_i \xi_i.$$

L'application ψ se factorise en :

$$\psi = \phi \circ \Theta$$

où ϕ est l'application $\psi \circ \Theta^{-1} : \mathbb{F}_{q^n} \to \mathbb{F}_q$.

Or, une telle application est polynomiale de degré inférieur ou égal à $q^n - 1$ comme on vient de le voir (théorème **19**), ainsi $\phi\left(\sum_{i=1}^{n} y_i \xi_i\right)$ peut s'écrire sous la forme

$$\sum_{i=1}^{n} P_i(y_1, y_2, \ldots, y_n) \xi_i$$

où les P_i sont des polynômes en $y_1, y_2, \ldots y_n$.

Comme ϕ est à valeurs dans le sous-corps $\mathbb{F}_q$ de $\mathbb{F}_{q^n}$, tous ces polynômes sont nuls sauf (éventuellement) P_1. Comme les y_i sont dans $\mathbb{F}_q$ on a $y_i^q = y_i$; ainsi, on peut voir P_1 comme un élément de l'anneau de polynômes $\mathbb{F}_q[Y_1, Y_2, \ldots, Y_n]$ *quotienté* par l'idéal $Y_1^q - Y_1, Y_2^q - (Y_2, \ldots, Y_n^q - Y_n)$.

Nous avons donc défini une application injective :

$$\mathbb{F}_q^{\mathbb{F}_q^n} \to \mathbb{F}_q[Y_1, Y_2, \ldots, Y_n]/(Y_1^q - Y_1, Y_2^q - Y_2, \ldots, Y_n^q - Y_n)$$
$$\phi \mapsto P_1,$$

dont nous allons établir maintenant qu'elle est surjective.

Dans la suite, on notera y_i la classe de Y_i dans l'anneau :

$$A = \mathbb{F}_q[Y_1, Y_2, \ldots, Y_n]/(Y_1^q - Y_1, Y_2^q - Y_2, \ldots, Y_n^q - Y_n).$$

Pour montrer que la correspondance est surjective, nous allons comparer les cardinaux de $\mathbb{F}_q^{\mathbb{F}_q^n}$ et A. Le premier cardinal est q^{q^n}. Quant à A, c'est le $\mathbb{F}_q$ espace vectoriel de base tous les monômes :

$$\prod_{i=1}^{n} y_i^{a_i}$$

avec $0 \leqslant a_i < q$. Il y a q^n monômes semblables, ainsi

$$\# A = q^{q^n},$$

désignant le cardinal, et le théorème est établi. ◊

À titre d'exemple, le lecteur pourra constater que la fonction g :

$$\mathbb{F}_2^3 \to \mathbb{F}_2$$

est donnée par le polynôme en trois variables

$$g > (x_1, x_2, x_3) = x_1x_2x_3 + x_1x_2 + x_2 + x_3 + 1.$$

Sa « table de vérité » est donnée tableau **8**.

Tableau 8 – Table de vérité de la fonction *g*

x_1	x_2	x_3	$g(x_1, x_2, x_3)$
0	0	0	1
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	1
1	0	1	0
1	1	0	1
1	1	1	1