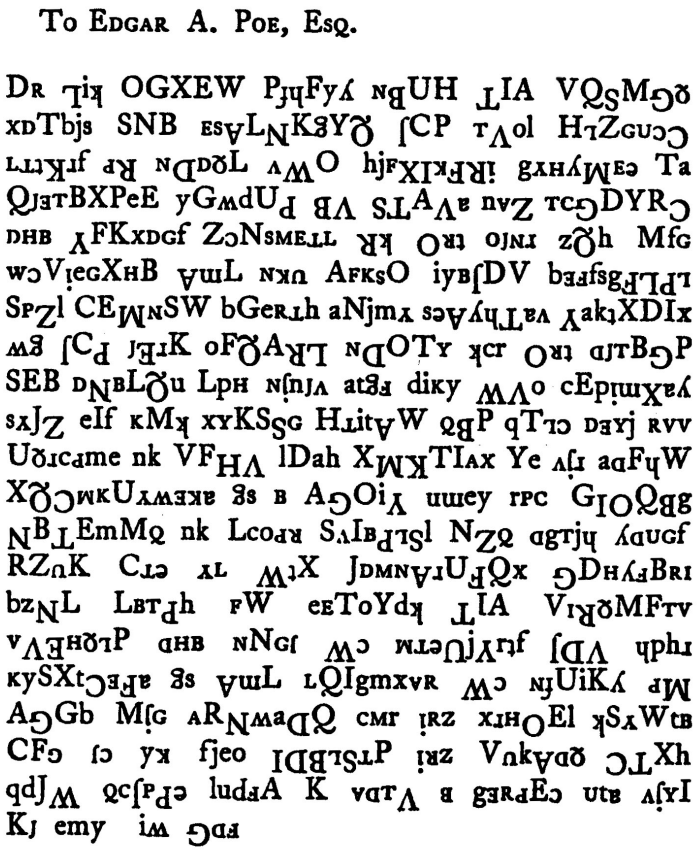
Sorbonne Université

Cryptologie Algébrique



En couverture : une scytale, ou bâton de Plutarque. C'était un bâton de bois utilisé par les Spartiates pour lire ou écrire une dépêche chiffrée.

Ci-dessus : un des deux célèbres cryptogrammes envoyés par W.B. Tyler à Edgar Allan Poe. Ce dernier, fasciné par la cryptographie, n'est jamais parvenu à déchiffrer le message.

Sorbonne Université

Cryptologie algébrique

4MA235

Leonardo Zapponi

TABLE DES MATIÈRES

CHAPITRE 1

ARITHMÉTIQUE DES ENTIERS ET COMPLEXITÉ

D'un point de vue effectif, tous les protocoles cryptographiques que nous étudierons se réduisent en dernière analyse à la manipulation d'entiers (ou de familles d'entiers) et à la détermination explicite d'opérations arithmétiques entre eux. La conception de nombreux cryptosystèmes se base le plus souvent sur la relative simplicité de certaines de ces opérations (effectuées en phase de cryptage, qui se doit d'être rapide) ou, au contraire, de leur difficulté (ce qui rend difficile le déchiffrement lors de la transmission du message chiffré). Nous allons commencer par un rapide rappel des porpriétés algébriques et arithmétique des entiers. Ces constructions et résultats, essentiellement contenus dans les ***Éléments*** d'Euclide, sont présentés dans le langage des anneaux, ce qui permet, entre autre, de se familiariser avec ce formalisme et de passer en revue quelques notions de base d'algèbre commutative. Nous étudierons ensuite l'aspect effectif des opérations, en introduisant la notion de complexité.

1.1. Rappels sur l'arithmétique des entiers

1.1.1. Structure d'anneau euclidien — La plupart des propriétés arithmétiques et algébriques des entiers, ainsi que l'effectivité de nombreux algorithmes découlent de l'existence d'une ***division euclidienne***, ce qui munit $\mathbb{Z}$ d'une structure d'***anneau euclidien***, une classe d'anneaux particulièrement adaptés à des constructions effectives. Le résultat ci-dessous nous accompagne depuis les bancs du collège (voire plus loin).

Théorème 1.1.1 — *Étant donnés deux entiers a et b, avec b non nul, il existe un unique couple d'entiers q et r, appelés respectivement* ***quotient*** *et* ***reste*** *de la division euclidienne de a par b, tels que*

$$a = bq + r,$$

avec $0 \leq r < |b|$.

Démonstration — L'ensemble

$$A = \{a - bq \mid q \in \mathbb{Z}\} \cap \mathbb{N}$$

est non vide (car il contient l'élément $a + |ba| \geq 0$) et possède donc un plus petit élément r. Par construction, on a l'identité $a = bq + r$, avec $q \in \mathbb{Z}$. Si l'on avait $r \geq |b|$, on obtiendrait les relations

$$r' = r - |b| = a - b(q \pm 1) \in A$$

et $r' < r$, ce qui est exclu. On a donc les inégalités $0 \leq r < |b|$. Finalement, si $qb + r = q'b + r'$, avec $0 \leq r, r' < |b|$, on obtient l'identité $b(q - q') = r' - r$. Pour $q \neq q'$, on en déduit les relations

$$|b| \leq |b(q' - q)| = |r - r'| < |b|,$$

ce qui est une fois encore exclu. On a donc $q = q'$ et, par suite $r = r'$, d'où l'unicité du quotient et du reste. □

D'un point de vue pratique, lorsque b est positif, en considérant la division euclidienne $a = bq + r$, on a l'identité $q = \lfloor a/b \rfloor$, où $\lfloor x \rfloor$ désigne la ***partie entière*** d'un réel x, i.e. le plus grand entier n tel que $n \leq x$.

Remarque 1.1.2 — En procédant comme dans la démonstration ci-dessus, on montre l'existence et l'unicité d'un couple d'entiers q et r tels que $a = bq + r$, avec cette fois $-|b|/2 \leq r < |b|/2$. Dans ce cas, on parle de ***division euclidienne modifiée***.

1.1.2. Idéaux — On rappelle qu'un idéal $\mathfrak{a}$ d'un anneau A est ***monogène*** s'il existe un élément $a \in A$, appelé ***générateur*** de $\mathfrak{a}$, tel que

$$\mathfrak{a} = aA = \{ab \mid b \in A\},$$

Le générateur d'un idéal monogène n'est généralement pas unique. Deux éléments a et b de A sont ***associés*** s'ils engendrent le même idéal, i.e. si $aA = bA$.

Lemme 1.1.3 — *Deux éléments $a, b \in A$ d'un anneau intègre A sont associés si et seulement s'il existe un élément $u \in A^\times$ tel que $a = ub$.*

Démonstration — L'assertion étant immédiate lorsque $ab = 0$, supposons a et b non nuls. Si $aA = bA$, on a en particulier $b \in aA$ et $a \in bA$, ou encore $b = ua$ et $a = vb$, avec $u, v \in A$, d'où les identités $a = bv = auv$ et, par suite, $a(1 - uv) = 0$. L'anneau A étant intègre et a étant non nul, on a alors $1 - uv = 0$, ce qui implique que u est inversible, d'inverse v. Réciproquement, si $b = ua$, avec $u \in A^\times$, on a $b \in aA$ et $a = u^{-1}b \in bA$, d'où les inclusions $bA \subset aA$ et $aA \subset bA$, qui sont alors des égalités. □

Un anneau A est ***principal*** s'il est intègre et si tous ses idéaux sont monogènes.

Théorème 1.1.4 — *L'anneau $\mathbb{Z}$ est principal.*

Démonstration — L'anneau $\mathbb{Z}$ étant intègre, il suffit de vérifier que tout idéal $\mathfrak{a}$ de $\mathbb{Z}$ est monogène. L'assertion étant immédiate pour $\mathfrak{a} = 0$, on supose $\mathfrak{a}$ non nul. L'ensemble

$$\mathfrak{a}^+ = \{a \in \mathfrak{a} \mid a > 0\} \subset \mathbb{N}$$

est non vide (car $\mathfrak{a}$ possède un élément non nul a, auquel cas $|a| = \pm a \in \mathfrak{a}^+$) et possède donc un élément minimal $n > 0$. On a on alors l'inclusion $n\mathbb{Z} \subset \mathfrak{a}$. Réciproquement étant donné $m \in \mathfrak{a}$, en considérant la division euclidienne $m = nq + r$, avec $0 \leq r < n$, on obtient les relations $r = m - nq \in \mathfrak{a}$. Pour $r > 0$, on obtiendrait $r \in \mathfrak{a}^+$, contredisant la minimalité de n. On a donc $r = 0$, d'où $m = nq \in n\mathbb{Z}$ et, par suite, l'inclusion $\mathfrak{a} \subset n\mathbb{Z}$, qui est alors une égalité. □

Proposition 1.1.5 — *Un idéal de $\mathbb{Z}$ possède un unique générateur positif. En particulier, l'application qui associe à un entier naturel n l'idéal $n\mathbb{Z}$ définit une bijection entre $\mathbb{N}$ et l'ensemble des idéaux de $\mathbb{Z}$.*

Démonstration — L'identité $\mathbb{Z} = \{\pm 1\}$ combinée avec le lemme 1.1.3 affirme qu'un idéal de $\mathbb{Z}$, qui est monogène (cf. le théorème 1.1.4), possède au plus deux générateurs, opposés l'un de l'autre (qui coïncident si et seulement si l'idéal est nul), un seul d'entre eux étant positif. □

Remarque 1.1.6 — Par définition, un idéal d'un anneau A est un sous-groupe (additif) de A mais la réciproque n'est généralement pas vraie. En effet, étant donné $h \in H$ et $a \in A$, rien ne permet d'affirmer que l'élément ah appartient à H. Par contre, pour $A = \mathbb{Z}$, le sous-groupe H est automatiquement un idéal. En effet, en se réduisant au cas $a \geq 0$, on a les relations

$$ah = h + \cdots (a) \cdots + h \in H.$$

En d'autres termes, pour $\mathbb{Z}$, la notion d'idéal et de sous-groupe coïncident. Dans la proposition ci-dessus, il est par conséquent possible de remplacer le terme idéal par sous-groupe.

1.1.3. Divisibilité, plus grand diviseur commun, identité de Bézout — De manière générale, si a et b sont deux éléments d'un anneau A, on dit que b ***divise*** a, ou que a est un ***multiple*** de b s'il existe $c \in A$ tel que $a = bc$. On utilise la notation $b|a$ pour indiquer que b divise a. Les idéaux sont l'outil le plus adapté dans toute question liée à la divisibilité. Le résultat élémentaire suivant en est une première illustration.

Lemme 1.1.7 — *Étant donnés deux éléments a et b d'un anneau A, on a $b|a$ si et seulement si $aA \subset bA$.*

Démonstration — Si $b|a$, on a $a = bc$, avec $c \in A$, d'où $a \in bA$ et, par suite, l'inclusion $aA \subset bA$. Réciproquement, pour $aA \subset bA$, on a $a \in aA \subset bA$, d'où $a = bc$, avec $c \in A$. □

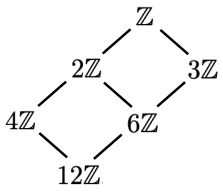
Revenant aux entiers, le résultat ci-dessous complète la proposition 1.1.5.

Proposition 1.1.8 — *Il existe une bijection naturelle entre l'ensemble des diviseurs positifs d'un entier n et l'ensemble des idéaux de $\mathbb{Z}$ contenant $n\mathbb{Z}$.*

Démonstration — Il suffit de combiner la proposition 1.1.5 et le lemme 1.1.7 □

Remarque 1.1.9 — La divisibilité définit une relation d'ordre sur $\mathbb{N}$ (mais pas sur $\mathbb{Z}$). Par ailleurs, l'ensemble des idéaux de $\mathbb{Z}$ est naturellement ordonné par l'inclusion (on pose ici $\mathfrak{a} \leq \mathfrak{b}$ si et seulement si $\mathfrak{b} \subset \mathfrak{a}$). Le résultat ci-dessus affirme que l'application qui associe à un entier naturel n l'idéal $n\mathbb{Z}$ est un isomorphisme d'ensembles ordonnés, i.e. une bijection qui est compatible avec les relations d'ordre.

Exemple 1.1.10 — Les six idéaux de $\mathbb{Z}$ contenant $12\mathbb{Z}$ sont $\mathbb{Z}, 2\mathbb{Z}, 3\mathbb{Z}, 4\mathbb{Z}, 6\mathbb{Z}$ et $12\mathbb{Z}$. La relation d'inclusion entre eux, qui correspond au treillis des diviseurs de 12 est décrite schématiquement dans la figure ci-dessous.



On rappelle que si $\mathfrak{a}$ et $\mathfrak{b}$ sont deux idéaux d'un anneau A, leur ***somme***

$$\mathfrak{a} + \mathfrak{b} = \{a + b \mid a \in \mathfrak{a}, b \in \mathfrak{b}\},$$

est également un idéal de A, c'est d'ailleurs le plus petit idéal contenant $\mathfrak{a} \cup \mathfrak{b}$. En ce qui concerne les entiers, étant donnés $a, b \in \mathbb{Z}$, la somme

$$a\mathbb{Z} + b\mathbb{Z} = \{ax + by \mid x, y \in \mathbb{Z}\}$$

des idéaux $a\mathbb{Z}$ et $b\mathbb{Z}$ est monogène (cf. le théorème 1.1.4), engendré par un unique entier naturel (cf. la proposition 1.1.5), appelé ***plus grand diviseur commun***, ou simplement ***pgcd*** de a et b. On le note généralement $a \wedge b$. Par constructon, il existe un couple d'entiers x et y vérifiant la relation

$$a \wedge b = ax + by,$$

appelée ***identité de Bézout***.

Exercice 1.1.11 — Soient a et b deux entiers. Montrer qu'étant donné un entier naturel d, les conditions suivantes sont équivalentes :

1. On a $d = a \wedge b$.
2. L'entier d divise a et b et si $c \in \mathbb{Z}$ est un diviseur commun à a et b alors c divise d (cette propriété justifie le nom de plus grand diviseur commun).

Deux entiers a et b sont ***premiers entre eux*** si $a \wedge b = 1$, ce qui revient à affirmer qu'il existe une identité de Bézout $ax + by = 1$.

Exercice 1.1.12 — Soient a, b et c des entiers, avec $a \wedge b = 1$. Montrer le ***lemme de Gauss*** : si a divise bc alors a divise c. En déduir que si $a|c$ et $b|c$ alors $ab|c$.

Le ***plus petit commun multiple***, ou ***ppcm*** de a et b, noté $a \vee b$ est l'unique générateur positif de l'idéal $a\mathbb{Z} \cap b\mathbb{Z}$.

Exercice 1.1.13 — Soient a et b deux entiers. Montrer qu'étant donné un entier naturel m, les conditions suivantes sont équivalentes :

1. On a $m = a \vee b$.
2. L'entier m est un multiple de a et b et si $c \in \mathbb{Z}$ est multiple commun à a et b alors c est un multiple de m (cette propriété justifie le nom de plus petit commun multiple).

De manière générale, étant donnés des entiers $a_1, \ldots, a_n$, leur pgcd, noté $a_1 \wedge \cdots \wedge a_n$ est l'unique générateur positif de l'idéal $a_1\mathbb{Z} + \cdots + a_n\mathbb{Z}$. De même, leur ppcm $a_1 \vee \cdots \vee a_n$ est l'unique générateur positif de l'idéal $a_1\mathbb{Z} \cap \cdots \cap a_n\mathbb{Z}$.

Remarque 1.1.14 — Les définitions de pgcd et de ppcm proposées dans ce paragraphe ainsi que leurs propriétés s'appliquent en fait à tout anneau principal, si ce n'est que dans le cas général, on ne dispose pas nécessairement d'un générateur privilégié d'un idéal (on parle alors d'un pgcd plutôt que du pgcd de a et b).

Exercice 1.1.15 — Montrer qu'étant donnés des entiers a, b et c, on a les propriétés suivantes :

1. $a \wedge (b + ac) = a \wedge b$.
2. $(ab) \wedge (ac) = |a|(b \wedge c)$.
3. $(a \wedge b)(a \vee b) = |ab|$.

1.1.4. Factorisation unique — Un ***nombre premier*** est un entier $n > 1$ tel que ses seuls diviseurs (positifs) sont 1 et n lui-même.

Proposition 1.1.16 — *Un entier naturel $n > 1$ est un nombre premier si et seulement si l'idéal $n\mathbb{Z}$ est maximal. En particulier, on en déduit le* ***lemme d'Euclide****, qui affirme que si un nombre premier divise le produit d'entiers alors il divise l'un des facteurs.*

Démonstration — La première assertion est une conséquence directe de la proposition 1.1.8. La seconde découle du fait que tout idéal maximal d'un anneau est premier (cf. l'appendice). □

Théorème 1.1.17 — *Un entier non nul n s'écrit de manière unique comme produit*

$$n = \pm \prod_p p^{e_p},$$

où p parcourt l'ensemble des nombres premiers, les entiers naturels e_p étant presque tous nuls (i.e. tous sauf un nombre fini d'entre eux).

Démonstration — On commence par montrer que tout nombre entier n possède une telle écriture. On procède par récurrence sur $|n|$: l'assertion étant claire pour $n = 1$ (auquel cas il suffit de poser $e_p = 0$ pour tout p), supposons $|n| > 1$ et la propriété vraie pour tout entier m tel que $|m| < |n|$. Si $|n|$ est premier, l'assertion est clairement remplie. Si n est composé, on a $n = ab$, avec $1 < a, b < n$ et il suffit d'appliquer l'hypothèse de récurrence. Concernant l'unicité, considérons deux écritures $n = \pm \prod_p p^{e_p} = \pm \prod_p p^{f_p}$ et supposons qu'il existe un nombre premier q tel que $e_q \neq f_q$. On peut se réduire au cas $e_q < f_q$, ce qui amène à l'identité

$$\prod_{p \neq q} p^{e_p} = \pm q^{f_q - e_q} \prod_{p \neq q} p^{f_p}.$$

En particulier, le nombre premier q divise $\prod_{p \neq q} p^{e_p}$ et coïncide donc avec l'un des facteurs, ce qui est exclu. On a donc $e_p = f_p$ pour tout nombre premier p et le signe dans les deux expressions est clairement le même, d'où l'unicité. □

Remarque 1.1.18 — L'écriture (unique) décrite dans le résultat ci-dessus est en fait valable pour tout rationnel non nul x, si ce n'est que les exposants e_p peuvent être négatifs. Dans le langage des groupes, le théorème fondamental de l'arithmétique établit un isomorphisme entre $\mathbb{Q}^\times$ et $\mu_2 \times \bigoplus_p \mathbb{Z}$, où l'on a posé $\mu_2 = \mathbb{Z}^\times = \{\pm 1\}$.

Exercice 1.1.19 — Étant donnés deux entiers non nuls a et b, considérons leurs factorisations $a = \pm \prod_p p^{e_p}$ et $b = \pm \prod_p p^{f_p}$. Montrer que l'on a $a|b$ si et seulement si $e_p \leq f_p$ pour tout nombre premier p. En déduire les identités

$$\begin{cases} a \wedge b = \prod_p p^{\min\{e_p, f_p\}}, \\ \\ a \vee b = \prod_p p^{\max\{e_p, f_p\}}. \end{cases}$$

1.1.5. L'algorithme d'Euclide étendu — Le calcul de pgcd est omniprésent en cryptographie algébrique. Il est par conséquent nécessaire de fournir un algorithme efficace permettant de le déterminer explicitement. Soient donc a et b deux entiers, que l'on suppose non nuls (dans le cas contraire, la calcul de leur pgcd est trivial). Le pgcd ne dépendant pas du signe des entiers considérés, on peut se réduire au cas $0 < b < a$ (pour $a = b$, on a clairement $a \wedge b = a$). Tout d'abord, on serait tenté de considérer les factorisations de a et b en produit de nombres premiers, utilisant ensuite l'expression du pgcd de l'exercice 1.1.19. Ne disposant à ce jour d'aucun algorithme de factorisation réellement performant, cette démarche est à ecarter. Nous allons décrire

une seconde méthode, le célèbre ***algorithme d'Euclide (étendu)***, qui s'avère bien plus efficace. On construit une suite finie d'entiers naturels $(r_i)_{i\geq 0}$, appelée ***suite des restes*** (associée à a et b) par le procédé suivant :

- On pose $r_0 = a$ et $r_1 = b$.
- Pour $i \geq 1$, si $r_i = 0$ le procédé s'arrête, sinon r_{i+1} est le reste d'une division euclidienne de r_{i-1} par r_i.

Il existe alors un unique entier $n \geq 1$ tel que $v(r_0) \geq v(r_1) > \cdots > v(r_n)$ et $r_{n+1} = 0$. Pour tout $i \in \{1, \ldots, n\}$, en posant

$$r_{i-i} = q_i r_i + r_{i+1},$$

on obtient la ***suite des quotients*** $(q_i)_{1\leq i\leq n}$. Finalement, on considère deux autres suites $(u_i)_{0\leq i\leq n}$ et $(v_i)_{0\leq i\leq n}$ définies par

$$\begin{cases} u_0 = 1, \\ u_1 = 0, \\ u_{i+1} = u_{i-1} - u_i q_i \text{ pour } i > 0, \end{cases} \quad \text{et} \quad \begin{cases} v_0 = 0, \\ v_1 = 1, \\ v_{i+1} = v_{i-1} - v_i q_i \text{ pour } i > 0. \end{cases}$$

Il peut être commode de présenter les étapes de calculs sous la forme du tableau suivant

	q_1	q_2	$\cdots$	q_{n-1}	q_n	
a	b	r_2	$\cdots$	r_{n-1}	r_n	0
1	0	u_2	$\cdots$	u_{n-1}	u_n	
0	1	v_2	$\cdots$	v_{n-1}	v_n	

Proposition 1.1.20 — *Avec les notations et hypothèses ci-dessus, on a les identités*

$$a \wedge b = r_n = au_n + bv_n.$$

Démonstration — Les relations $a \wedge b = r_0 \wedge r_1$ et $r_n = r_n \wedge r_{n+1}$ sont immédiatement vérifiées. Pour tout $i \in \{1, \ldots, n\}$, le point 1 de l'exercice 1.1.15 amène alors aux identités

$$r_{i-1} \wedge r_i = (r_{i-1} - q_i r_i) \wedge r_i = r_{i+1} \wedge r_i,$$

d'où la première égalité. Concernant la seconde, montrons par récurrence que pour tout $i \in \{0, \ldots, n\}$, on a la relation $r_i = au_i + bv_i$. L'assertion étant trivialement vérifiée pour $i = 0$ et $i = 1$, supposons qu'elle est vraie pour un entier $i \geq 1$. On a alors les relations

$$\begin{aligned} r_{i+1} = r_{i-1} - q_i r_i &= au_{i-1} + bv_{i-1} - q_i(au_i + bv_i) = \\ &= a(u_{i-1} - q_i u_i) + b(v_{i-1} - q_i v_i) = au_{i+1} + bv_{i+1}, \end{aligned}$$

ce qui conclut la démonstration. □

Remarque 1.1.21 — Dans ce procédé, on peut librement remplacer la division euclidienne usuelle par sa version modifiée (cf. la remarque 1.1.2). Dans ce cas, les

termes de la suite des restes (r_i) n'étant pas n'écessairement positifs, on obtient l'identité $|r_n| = a \wedge b$) (le nombre d'itérations n n'étant généralement pas le même qu'avec la division euclidienne usuelle). Par contre, l'expression $r_n = au_n + bv_n$ reste valable. La suite $(|r_i|)$ est strictement décroissante, car pour $i > 0$, on a $|r_{i+1}| \leq |r_i|/2$, d'où la relation $|r_i| \leq |b|/2^{i-1}$. En particulier, on obtient $n \leq \log_2(|b|) + 1$, ce qui permet de quantifier le nombre d'itération nécessaires pour que l'algorithme d'Euclide étendu aboutisse (dans sa version modifiée). Une analyse similaire, faisant intervenir la ***suite de Fibonacci***, amène à une majoration semblable du nombre d'itérations nécessaires avec l'agorithme usuel (non modifié).

Exemple 1.1.22 — Déterminons explicitement le pgcd des entiers 1071 et 2023. On a le tableau

	1	1	8	
2023	1071	952	119	0
1	0	1	-1	
0	1	-1	2	

On en déduit la relation $1071 \wedge 2023 = 119$ et l'identité de Bézout

$$2 \cdot 1071 - 1 \cdot 2023 = 119.$$

La division euclidienne modifiée amène au second tableau

	2	-9	
2023	1071	-119	0
1	0	1	
0	1	-2	

L'algorithme est donc plus rapide dans sa version modifiée.

1.2. Quelques notions de complexité

Ayant passé en revue les propriétés essentielles des entiers qui seront utilisés dans la suite du cours, on s'interesse à présent à l'aspect effectif des opérations et constructions présentées (somme, produit, division euclildienne, algorithme d'Euclide étendu,...).

1.2.1. Écriture d'un entier en base b — Nous allons brièvement rappeler une notion qui remonte à nos souvenirs de jeunesse : la numération en base b.

Théorème 1.2.1 — *Soit $b > 1$ un entier. Tout entier naturel n s'écrit de manière unique sous la forme*

$$n = a_0 + a_1 b + \cdots + a_k b^k + \cdots,$$

où les entiers $a_0, a_2, \cdots \in \{0, \ldots, b-1\}$ sont presque tous nuls (i.e. nuls à partir d'un certain rang). Une telle expression est appelée ***écriture en base b de n***.

Démonstration — Concernant l'existence, on procède par récurrence sur l'entier n : pour $n < b$, c'est immédiat. Soit donc $n \geq b$ un entier et supposons que tout entier $m < n$ possède une telle écriture. En particulier, en considérant la division euclidienne $n = bm + a_0$, avec $0 \leq a_0 < b$, on a $m < n$ d'où l'écriture $m = a_1 + a_2 b + a_3 b^2 + \cdots$, ce qui donne

$$n = a_0 + b(a_1 + a_2 b + \cdots) = a_0 + a_1 b + a_2 b^2 + \ldots.$$

Concernant l'unicité, il suffit de remarquer que a_0 est le reste de la division euclidienne de $n_0 = n$ par b ; il est donc unique. Dans ce cas a_1 est le reste de la division euclidienne de $n_1 = (n_0 - a_0)/b$ par b, qui est également unique. En itérant ce procédé, on en déduit qu'il en est de même pour a_i, qui est le reste de la division euclidienne de $n_i = (n_{i-1} - a_{i-1})/b$ par b. □

En suivant la notation et les hypothèses du théorème 1.2.1, notons $\ell = \ell_b(n)$ le plus grand entier naturel tel que $a_\ell \neq 0$. On écrit alors $n = (a_\ell \cdots a_0)_b$ pour indiquer l'écriture en base b de n. Si aucune confusion n'est possible, on utilise également la notation $n = a_\ell \cdots a_0$.

Exercice 1.2.2 — Montrer que $\ell_b(a)$ est le plus petit entier ℓ tel que $b^{\ell+1} > a$, ce qui se traduit par l'identité

$$\ell_b(a) = \lfloor \log_b(a) \rfloor,$$

où $\lfloor x \rfloor$ désigne la partie entière d'un réel x.

Exemple 1.2.3 — Le tableau ci-dessous contient les écritures de l'entier 2024 en base $b < 10$.

2	3	4	5	6	7	8	9
11111101010	2210001	133222	31101	13214	5623	3752	2701

Exercice 1.2.4 — Soit $b > 1$ un entier. Montrer qu'un entier relatif n s'écrit de manière unique sous la forme

$$n = a_0 - a_1 b + a_2 b^2 + \cdots + a_k (-b)^k + \cdots,$$

où les entiers $a_0, \ldots, a_k \in \{0, \ldots, b-1\}$ sont presque tous nuls. Déterminer une telle expression pour $b = 2$ et $n = 2026$.

Exercice 1.2.5 — Considérons un polynôme $f \in \mathbb{Z}[X]$ et supposons que tous ses coefficients sont des entiers naturels. Montrer que la donnée des entiers $n = f(1)$ et $m = f(n+1)$ permet de déterminer f.

1.2.2. La taille d'un entier en informatique — Ayant commencé à compter en utilisant les dix doigts de nos mains, c'est l'écriture en base 10 qui s'est imposée au fil des siècles. Cependant, d'un point de vue pratique, et particulièrement en ce qui concerne les application en informatique, on utilise le plus souvent l'écriture en base 2. Dans ce contexte, un ***bit*** est une variable qui ne peut prendre que les valeurs 0 et 1. En considérant son écriture en base 2, un entier naturel peut être assimilé à une suite de bits. De manière plus précise, étant donnée l'écriture $n = (a_\ell \dots a_0)_2$, l'entier naturel $k = \ell_2(n) + 1$ est la ***taille*** de n, i.e. le nombre de bits nécéssaires pour le mémoriser. On dit alotrs que n est un ***entier de k bits***. On rappelle que l'on a l'identité $k = \lfloor \log_2(n) \rfloor + 1$ (cf. l'exercice 1.2.2). En particulier, n est un entier à ℓ bits si et seulement si l'on a l'encadrement $2^{k-1} \leq n < 2^k$. Le bit a_ℓ est le ***plus significatif*** et a_0 est le ***moins significatif***.

Exemple 1.2.6 — L'entier $2024 = (11111101000)_2$ est de taille 11. À ce jour, dans les applications cryptographiques tels que le cryptosystème RSA (que nous verrons dans le deuxième chapitre), on utilise des entiers de 1024 bits, ce qui correspond à 309 chiffres décimales.

Dans la pratique, on fixe la taille (maximale) k des entiers naturels considérés i.e. la capacité de l'ordinateur avec sur lequel on envisage d'implémenter un algorithme. Si $n = (a_\ell \cdots a_0)_2$ est l'écriture en base 2 d'un tel entier, on a alors $\ell \leq k - 1$ et $(0, \dots, 0, a_\ell, \dots, a_0)$ est le k-plet de bits correspondant à n (on complète par des 0). Lors de l'implémentation de tout algorithme, il faut impérativement tenir compte de la possibilité de dépassement de cette capacité, amenant à une erreur (***overflow*** en anglais).

Remarque 1.2.7 — Voulant encoder un entier relatif quelconque, on peut considérer un bit supplémentaire correspondant à son signe. Il est important de signaler que dans la pratique, on utilise plutôt la technique du ***complément à deux***, qui permet d'effectuer des soustractions de manière plus naturelle. Voulant éviter de s'éloigner des objectifs du cours, nous ne détaillerons pas cette méthode.

1.2.3. Opérations élémentaires sur les bits et opérations arithmétiques sur les entiers — Il existe quatre ***opérations élémentaires*** sur les bits : NOT, OR, AND et XOR. Leur résultat est présenté dans les tableaux ci-dessous.

a	NOT a
0	1
1	0

a	b	a OR b	a AND b	a XOR b
0	0	0	0	0
0	1	1	0	1
1	0	1	0	1
1	1	1	1	0

Étant donné un k-plet $n = (a_k, \cdots, a_1)$ de bits ou, ce qui revient au même, un entier $n < 2^k$, on introduit alors également l'opération élémentaire de ***décalage à droite***, définie par

$$\mathrm{RS}(n) = (0, a_k \cdots, a_2).$$

On remarquera que l'entier correspondant à $\mathrm{RS}(n)$ est le quotient de la division euclidienne de n par 2 et a_1 est son reste. On définit de manière analogue le ***décalage à gauche*** en posant

$$\mathrm{LS}(n) = (a_{k-1}, \ldots a_1, 0).$$

On vérifie facilement que l'entier associé à $\mathrm{LS}(n)$ n'est autre que le reste de la division euclidienne de $2n$ par 2^k. En particulier, pour $a_k = 0$, ce qui se traduit par l'inégalité $n < 2^{k-1}$, on a l'identité $\mathrm{LS}(n) = 2n$.

Toutes les opérations usuelles entre entiers (comparaison, addition, soustraction, multiplication et division euclidienne) peuvent être effectuées par une suite d'opérations élémentaires sur leurs bits. Décrivons par exemple un algorithme permettant d'effectuer la somme de deux entiers naturels a et b à k bits correspondant respectivement aux k-plets $(a_k, \ldots, a_1)$, et $(b_k, \ldots, b_1)$:

$r \leftarrow 0$ (bit de retenue)
Pour i de 1 à k
    $c_i \leftarrow (a_i \,\mathrm{XOR}\, b_i) \,\mathrm{XOR}\, r$
    $r \leftarrow (a_i \,\mathrm{AND}\, b_i) \,\mathrm{OR} (a_i \,\mathrm{AND}\, r) \,\mathrm{OR} (b_i \,\mathrm{AND}\, r)$
$c_k \leftarrow r$

Cet algorithme nécessite $7k$ opérations élémentaires. Le résultat est le $(k+1)$-plet de bits $(c_{k+1}, \ldots, c_1)$ et l'entier qui lui est associé coïncide avec la somme de a et b. Le tableau ci-dessous indique le nombre (pas nécessairement minimal et arrondi par excès) d'opérations élémentaires nécessaires pour effectuer les opérations usuelles entre deux entiers naturels à k bits.

Comparaison	$2k$
Addition	$7k$
Soustraction	$8k$
Multiplication	$8k^2$
Division euclidienne	$13k^2$

1.2.4. Complexité d'un algorithme arithmétique sur les entiers — Comme il a été souligné précédemment, tous les algorithmes considérés dans ce cours se réduisent à une suite d'opérations arithmétique sur des entiers (comparaison, somme, produit, division euclidienne). On peut associer à un tel algorithme deux types de

complexités : la ***complexité en espace***, qui mesure la mémoire (de l'ordinateur) nécessaire à son execution, et la ***complexité en temps***, qui est une évaluation de sa durée d'exécution. C'est cette deuxième notion qui nous intéresse principalement. Nous partirons du principe que toutes les opérations élémentaires sur les bits ont la même durée d'exécution et qu'elles seules contribuent de manière significative au temps d'exécution de l'algorithme (c'est clairement une simplification du problème, mais les résultats présentés restent néanmoins valables). En ce qui nous concerne, il est par conséquent naturel de définir la ***complexité*** de l'algorithme comme le nombre d'opérations élémentaires nécessaires pour qu'il aboutisse, ce nombre dépendant clairement des entiers sur lesquels on applique l'algorithme. Avec cette convention, le temps d'exécution est donc proportionnel à sa complexité. Cette constante de proportionnalité dépend de l'ordinateur utilisé et n'est pas d'un réel intérêt (tant que l'on ne s'intéresse pas à l'implémentation effective de l'algorithme). Afin d'obtenir une expression qui ne tienne pas compte de ce facteur, il est utile d'introduire quelques notions de comparaison asymptotique. Considérons deux applications $f, g : \mathbb{N}_{>0} \to \mathbb{R}$. On dit que g est ***dominée*** par f, et on écrit $g = O(f)$, s'il existe une constante $c \in \mathbb{R}$ telle que

$$|g(n)| \leq c|f(n)|$$

pour tout n. D'après le paragraphe précédent, la complexité des opérations arithmétiques sur les entiers naturels peu être majorée par une fonction ne dépendant que de leur taille. Par exemple, nous avons vu que la complexité de l'algorithme d'addition de deux entiers de k bits est inférieure ou égale à $7k$. Avec la notation asymptotique introduite ci-dessus, la somme de deux entiers de k bits est donc de complexité $O(k)$. Le tableau suivant donne une expression de la complexité de quelques algorithmes de base sur deux entiers de k bits.

Algorithme	Complexité
Comparaison	$O(k)$
Addition/soustraction	$O(k)$
Multiplication/division euclidienne	$O(k^2)$

Remarque 1.2.8 — L'algorithme d'addition utilisé dans la pratique est très proche de celui décrit dans le paragraphe précédent. Concernant la multiplication (ou la division euclidienne), on a utilisé ici un algorithme qui n'est autre que l'adaptation en base 2 de la technique multiplication (ou de division) à la main, telle que l'on apprend à l'école. Ce dernier n'est pas nécessairement optimal d'un point de vue effectif, mais il l'est d'un point de vue asymptotique.

Il est souvent plus pratique d'estimer la complexité d'un algorithme en faisant intervenir les entiers considérés plutôt que leur taille. Tenant compte des relations $\ell_2(n) = \lfloor \log_2(n) \rfloor = O(\log(n))$, la somme de deux entiers naturels a et b est alors de complexité $O(\max\{\log(a), \log(b)\})$.

Dans le tableau ci-dessous, nous avons reporté l'estimation de la complexité en fonction des entiers naturels $b \leq a$ considérés.

Algorithme	Complexité
Comparaison	$O(\log(a))$
Comparaison, addition, soustraction	$O(\log(a))$
Multiplication, division euclidienne	$O(\log^2(a))$
Algorithme d'Euclide étendu	$O(\log^2(a))$

Remarque 1.2.9 — Concernant l'algorithme d'Euclide étendu, à chaque étape, on effectue une division euclidienne (afin de déterminer la suite des restes), deux multiplications et deux soustractions (pour le calcul des suites auxilières (u_n) et (v_n)). On vérifie facilement que les entiers intervenant dans l'emsemble de l'algorithme sont inférieurs ou égaux à a, ce qui implique que chaque étape est de complexité $O(\log^2(a))$. Comme il a été noté précédemment (cf. la remarque 1.1.21), en utilisant la division euclidienne modifiée (qui est elle aussi de complexité $O(\log^2(a))$, l'algorithme aboutit après $\ell_2(a) = \lfloor \log_2(a) \rfloor + 1 = O(\log(a))$ étapes au plus (une estimation semblable est valable si l'on utilise la division euclidienne ordinaire). On en déduit que l'algorithme d'Euclide es de complexité $O(\log^3(a))$. Une étude plus fine (tenant compte du fait que la suite des restes est strictement décroissante) permet de montrer qu'il est en fait de complexité $O(\log^2(a))$.

Un algorithme sur des entiers naturels $a_1, \ldots, a_n$ est ***polynomial*** s'il existe des entiers naturels $d_1, \ldots, d_n$ tels que sa complexité soit égale à $O(\log^{d_1}(a_1) \cdots \log^{d_n}(a_n))$. On dit également que la complexité de l'algorithme est polynomiale. Tel est le cas par exemple pour les algorithmes d'addition, de soustraction, de multiplication, de division euclidienne ou de calcul de pgcd. Ce type d'algorithme est particulièrement adapté à des applications effectives, tout particulièrement en cryptographie, car en augmentant la taille des entiers considérés, la croissance de sa complexité reste modérée (polynomiale par rapport à leur taille, ce qui justifie d'ailleurs le nom).

1.2.5. Le problème de la factorisation — S'il est important en cryptographie de disposer d'algorithmes performants (i.e. de complexité polynomiale), de nombreux cryptosystèmes se basent par contre sur l'absence de tels algorithmes dans des problèmes particuliers, réputés difficiles d'un point de vue effectif. Tel est par exemple le cas pour la factorisation d'un entier : on ne dispose pas à ce jour d'algorithme rapide permettant de déterminer une factorisation non triviale d'un entier composé (i.e. non premier). Un chapitre de ce cours est dédié à cette question. Pour l'heure, remarquons qu'afin de factoriser un entier composé n, une première méthode naturelle (et incontournable) consiste à tester récursivement la divisibilité de n par tous les entiers inférieurs ou égaux à $\sqrt{n}$ (en effet, si n est composé, il possède un diviseur $1 < d \leq \sqrt{n}$), et ce, en effectuant à chaque étape une division euclidienne. On obtient

alors un algorithme de complexité $O(\sqrt{n}\log^2(n))$. En d'autres termes, la croissance de sa complexité est bien plus que polynomiale par rapport à la taille de n (cette dernière étant égale à $\ell_2(n) = O(\log(n))$). Dans ce cas, elle est même ***exponentielle***. Nous verrons que même l'utilisation de techniques plus sophistiquées n'amène pas à une amélioration significative par rapport à la méthode décrite ici (la complexité reste essentiellement exponentielle).

1.3. Deux algorithmes performants

1.3.1. Exponentiation rapide — En cryptographie, il est souvent nécessaire de calculer des (grandes) puissances g^n d'un éléments g d'un groupe G (ou, plus généralement, d'un monoïde). Il existe une méthode naïve de calcul de g^n qui consiste à effectuer $n-1$ multiplications, ce qui, dans la pratique, peut souvent se révéler prohibitif. Un procédé plus astucieux consiste à considérer l'écriture de n en base 2,

$$n = (a_\ell a_{\ell-1} \cdots a_0)_2 = a_0 + 2a_1 + \cdots + a_\ell 2^\ell,$$

où $\ell + 1 = \lfloor \log_2(n) \rfloor + 1$ est la taille de n. En posant $g_i = g^{2^i}$, on a alors l'identité

$$g^n = g_0^{a_0} \cdots g_\ell^{a_\ell}.$$

On remarquera que l'on a la relation $g_{i+1} = g_i^2$. On en déduit que ℓ multiplications (en fait, des élévations au carré) dans G suffisent pour déterminer les éléments $g_0, \ldots, g_\ell$. Les entiers a_i étant égaux à 0 ou 1, l'élément g^n est déterminé en effectuant au plus ℓ multiplication supplémentaires. En tout, on obtient un nombre de multiplications inférieur ou égal à 2ℓ. Cette méthode, appelée ***exponentiation rapide***, est donc performante et couramment utilisée dans la pratique. De nombreux cryptosystèmes (RSA, El-Gamal, Rabin,...) ou algorithmes (critères de primalité, méthodes de factorisation,...) seraient en effet absolument ineffectifs sans l'utilisation cette technique.

Exemple 1.3.1 — En utilisant la méthode d'exponentiation rapide, l'entier $3^{1000000}$ est déterminé en effectuant 27 multiplications dans $\mathbb{N}$. D'un point de vue pratique, sur un Macbook Pro, ce calcul nécessite environ $0,02$ secondes, contre 18 avec la méthode naïve (comportant 999999 multiplications).

1.3.2. Extraction de la racine carrée d'un entier — Nous terminons ce chapitre en décrivant un algorithme rapide pour déterminer la (partie entière de la) racine carrée d'un entier $n > 0$. En notant r le plus grand entier tel que $4^r \leq n$, ce qui se traduit par l'identité $r = \lfloor \log_2(n)/2 \rfloor$, considérons la suite (x_i) définie par $x_0 = 0$ et

$$x_{i+1} = \begin{cases} x_i + 2^{r-i} \text{ si } (x_i + 2^{r-i})^2 \leq n, \\ \\ x_i \text{ sinon.} \end{cases}$$

Proposition 1.3.2 — *L'élément x_{r+1} est la partie entière de $\sqrt{n}$.*

Démonstration — Montrons par récurrence que pour tout $i \in \{1, \ldots, r+1\}$, x_i est un entier naturel vérifiant les inégalités

$$x_i^2 \leq n < (x_i + 2^{r-i+1})^2.$$

Pour $i = 1$, on a l'identité $x_1 = 2^r$, d'où les relations

$$x_1^2 = 4^r \leq n < 4^{r+1} = (x_1 + 2^r)^2.$$

Soit donc $i \in \{1, \ldots, n\}$ et supposons que x_i est un entier naturel vérifiant les inégalités ci-dessus. Pour $(x_i + 2^{r-i})^2 \leq n$, on obtient $x_{i+1} = x_i + 2^{r-i} \in \mathbb{N}$, d'où les relations

$$x_{i+1}^2 \leq n < (x_i + 2^{r-i+1})^2 = (x_{i+1} + 2^{r-i})^2$$

Pour $(x_n + 2^{r-i})^2 > n$, on obtient $x_{i+1} = x_i \in \mathbb{N}$ et les relations

$$x_{i+1}^2 = x_i^2 \leq n < (x_i + 2^{r-i})^2 = (x_{i+1} + 2^{r-i})^2.$$

Finalement, pour $i = r + 1$, on obtient les inégalités

$$x_{r+1}^2 \leq n < (x_{r+1} + 1)^2,$$

d'où le résultat. □

Corollaire 1.3.3 — *L'algorithme d'extraction de la racine carrée d'un entier naturel n est de complexité $O(\log^3(n))$.*

Démonstration — La détermination de l'entier r nécessitant $2r$ décalages vers la gauche et r comparaisons d'entiers inférieurs ou égaux à n, elle est de complexité $O(r \log(n) + 2r) = O(\log^2(n))$. À chaque pas de l'algorithme, on effectue au plus une élévation au carré, une comparaison, un décalage à droite et une somme, le tout avec des entiers inférieurs ou égaux à n^2, ce qui amène à une complexité globale de $O((r+1)(\log^2(n)) = O(\log^3(n))$. □

CHAPITRE 2

PROTOCOLES REPOSANT SUR LE PROBLÈME DE LA FACTORISATION

Ce chapitre est consacré à la description de quelques cryptosystèmes dont la sécurité se base sur la difficulté de factoriser un entier naturel qui est le produit de deux (grands) nombres premiers. L'***artihmétique modulaire***, c'est à dire l'étude des quotients de $\mathbb{Z}$ est au coeur de toutes les constructions, l'interprète théorique principal étant le ***théorème des restes chinois***. Le cryptosystème ***RSA*** est l'un des plus célèbres protocoles cryptographiques reposant sur le problème de la factorisation ; une section entière lui est dédiée. Des questions de factorisation effective se prêtant à des application cryptographiques apparaissent également lorsque l'on s'intéresse aux carrés dans les anneaux $\mathbb{Z}/n\mathbb{Z}$. Les cryptosystèmes de ***Rabin*** et de ***Goldwasser-Micali***, faisant intervenir le ***symbole de Legendre***, en sont des illustrations.

2.1. Arithmétique modulaire

2.1.1. Le groupe $\mathbb{Z}/n\mathbb{Z}$ — On commence à s'interesser à la structure des quotients du groupe $\mathbb{Z}$. D'après la remarque 1.1.6, si H est un sous-groupe de $\mathbb{Z}$, alors $H = n\mathbb{Z}$, où l'entier n est univoquement déterminé. Deux entiers a et b sont ***congrus modulo n*** s'ils défiissent le même élément de $\mathbb{Z}/n\mathbb{Z}$, ce qui se traduit par la relation $n|a-b$, ou encore $a - b \in n\mathbb{Z}$. On écrit alors

$$a \equiv b \pmod{n}.$$

L'élément

$$\bar{a} = a + n\mathbb{Z} = \{a + nm \mid m \in \mathbb{Z}\} \in \mathbb{Z}/n\mathbb{Z}$$

associé à a, i.e. l'ensemble des entiers qui sont congrus à a modulo n, est la ***classe (de congruence) de a modulo n***.

Proposition 2.1.1 — *Soit $n > 0$ un entier. Le groupe $\mathbb{Z}/n\mathbb{Z}$ est cyclique, d'ordre n et il existe une bijection entre l'ensemble de ses sous-groupes et l'ensemble des diviseurs (positifs) de n.*

Démonstration — D'après le théorème 1.1.1, un entier est congru modulo n à un unique élément de l'ensemble $\{0, \dots, n-1\}$ et deux éléments distincts de ce dernier ne sont jamais congrus modulo n, ce qui implique que $\mathbb{Z}/n\mathbb{Z}$ est d'ordre n. Il est cyclique, engendré par l'élément $\bar{1}$ (en effet, pour tout $x = \bar{a} \in \mathbb{Z}/n\mathbb{Z}$, on a l'identité $x = a \cdot \bar{1}$). On a un homomorphisme surjectif canonique de groupes $f : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ défini par $f(a) = \bar{a}$ et la proposition A.2.9 affirme que f définit une bijection entre les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ et les sous-groupes de $\mathbb{Z}$ contenant $n\mathbb{Z}$. Il suffit alors d'appliquer la proposition 1.1.8. □

2.1.2. Groupes cycliques — Le groupe $\mathbb{Z}$ des entiers relatifs vérifie la propriété universelle suivante : étant donné un groupe G (pas nécessairement abélien) et un élément $g \in G$, il existe un unique homomorphisme de groupes $\exp_g : \mathbb{Z} \to G$ tel que $\exp_g(1) = g$. D'un point de vue explicite, on a l'identité

$$\exp_g(n) = g^n$$

pour tout $n \in \mathbb{Z}$. On rappelle que tel qu'il a été défini dans l'appendice, l'ordre de g est le cardinal du sous-groupe $\langle g \rangle$ de G qu'il engendre.

Proposition 2.1.2 — *Soient G un groupe et $g \in G$ un élément d'ordre fini n. Le groupe $\langle g \rangle$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$. En particulier, on a $g^m = 1$ si et seulement si n divise m.*

Démonstration — L'image de l'homomorphisme $\exp_g$ coïncide avec le sous-groupe $\langle g \rangle$ et le thórème d'isomorphisme pour les groupes affirme que ce dernier est isomorphe à $\mathbb{Z}/\ker(\exp_g)$. On a donc $\ker(\exp_g) = d\mathbb{Z}$, avec $d > 0$ univoquement déterminé (on ne peut avoir $d = 0$, sinon le groupe $\mathbb{Z}/\ker(\exp_g)$ serait d'ordre infini). En comparant les ordres, on obtient alors $d = n$. Finalement, on a l'identité $g^m = 1$ si et seulement si $m \in \ker(\exp_g) = n\mathbb{Z}$, ce qui se traduit par la relation $n|m$. □

Corollaire 2.1.3 — *Un groupe cyclique d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.*

Démonstration — C'est un cas particulier du résultat précédent. □

2.1.3. L'anneau $\mathbb{Z}/n\mathbb{Z}$ — Dans ce chapitre, on s'intéresse au quotient de $\mathbb{Z}$ par rapport à un idéal $\mathfrak{a}$. L'anneau $\mathbb{Z}/0$ s'identifiant canoniquement avec $\mathbb{Z}$, on suppose $\mathfrak{a}$ non nul. D'après la proposition 1.1.5, on a alors $\mathfrak{a} = n\mathbb{Z}$, où l'entier $n > 0$ est univoquement déterminé.

Proposition 2.1.4 — *Soit $n > 0$ un entier. L'anneau $\mathbb{Z}/n\mathbb{Z}$ est fini, de cardinal n et il existe une bijection entre l'ensemble de ses idéaux et l'ensemble des diviseurs (positifs) de n.*

Démonstration — D'après le théorème 1.1.1, un entier est congru modulo n à un unique élément de l'ensemble $\{0, \dots, n-1\}$, d'où la première assertion. On a un homomorphisme surjectif canonique d'anneaux $f : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ défini par $f(a) = \bar{a}$ et

la proposition A.3.4 affirme que f définit une bijection entre les idéaux de $\mathbb{Z}/n\mathbb{Z}$ et les idéaux de $\mathbb{Z}$ contenant $n\mathbb{Z}$. Il suffit alors d'appliquer la proposition 1.1.8. □

Dans la pratique, étant donné un élément de $\mathbb{Z}/n\mathbb{Z}$, on considère toujours son unique représentant dans l'ensemble $\{0, \ldots, n-1\}$. Les opérations algébriques dans $\mathbb{Z}/n\mathbb{Z}$ (somme et produit) sont alors effectuées sur des entiers naturels inférieurs ou égaux à n. Au vu des résultats du chapitre précédent, la proposition ci-dessous est immédiate (l'élévation à la puissance m étant effectuée par exponentiation rapide, cf. le praragraphe 1.3.1).

Proposition 2.1.5 — *Les opérations de somme, de produit et d'élévation à la puissance $m > 0$ dans $\mathbb{Z}/n\mathbb{Z}$ sont de complexités respectives $O(\log(n)), O(\log^2(n))$ et $O(\log(m)\log^2(n))$.*

2.1.4. Le théorème des restes chinois — Le célèbre ***théorème des restes chinois*** est à la base de la conception pratique des cryptosystèmes présentés dans ce chapitre. Nous en présentons ici une version très générale. Étant donnés trois anneaux X, Y et S ainsi que deux homomorphismes d'anneaux $f : X \to S$ et $g : Y \to S$, l'ensemble

$$X \times_S Y = \{(x, y) \in X \times Y \mid f(x) = g(y)\}$$

est un sous-anneau de $X \times Y$ appelé ***produit fibré*** de X et Y au dessus de S.

Proposition 2.1.6 — *Étant donnés deux idéaux $\mathfrak{a}$ et $\mathfrak{b}$ d'un anneau A, posons $\mathfrak{c} = \mathfrak{a} + \mathfrak{b}$ et considérons les anneaux $X = A/\mathfrak{a}$, $Y = A/\mathfrak{b}$ et $S = A/\mathfrak{c}$. On a alors des homomorphismes canoniques d'anneaux $f : X \to S$ et $g : Y \to S$. Avec ces hypothèses, l'anneau $X \times_S Y$ est isomorphe à $A/\mathfrak{a} \cap \mathfrak{b}$.*

Démonstration — On a un homomorphisme naturel d'anneaux $h : A \to X \times Y$ défini par $h(a) = (a + \mathfrak{a}, a + \mathfrak{b})$. Son image est contenue dans $X \times_S Y$. Étant donné $(x, y) \in X \times_S Y$, on a $x = a + \mathfrak{a}$ et $y = b + \mathfrak{b}$, avec $a, b \in A$. Par hypothèse, on a $a + \mathfrak{c} = b + \mathfrak{c}$, d'où l'existence de $a' \in \mathfrak{a}$ et $b' \in \mathfrak{b}$ tels que $a - b = a' - b'$. En posant $x = a - a' = b - b'$, on a alors les identités

$$h(x) = (x + \mathfrak{a}, x + \mathfrak{b}) = (a - a' + \mathfrak{a}, b - b' + \mathfrak{b}) = (a + \mathfrak{a}, b + \mathfrak{b}) = (x, y),$$

d'où l'inclusion $X \times_S Y \subset \mathrm{Im}(h)$, qui est alors une égalité. Le noyau de h coïncidant avec $\mathfrak{a} \cap \mathfrak{b}$, le théorème d'isomorphisme pour les anneaux permet de conclure. □

En généralisant la notion définie précédemment, nous dirons que deux éléments x et y de A sont ***congrus modulo*** un ideal $\mathfrak{a}$ s'ils définissent le même élément de $A/\mathfrak{a}$, ce qui se traduit per la relation $x - y \in \mathfrak{a}$. On écrit alors

$$x \equiv y \pmod{\mathfrak{a}}.$$

De manière pratique, la démonstration du résultat ci dessus affirme qu'étant donnés deux éléments $a, b \in A$, le système de congruences

$$\begin{cases} x \equiv a \pmod{\mathfrak{a}}, \\ x \equiv b \pmod{\mathfrak{b}}, \end{cases}$$

admet une solution si et seulement si $a \equiv b \pmod{c}$, auquel cas elle est unique modulo $\mathfrak{a} \cap \mathfrak{c}$.

Deux idéaux $\mathfrak{a}$ et $\mathfrak{b}$ de A sont ***étrangers*** si $\mathfrak{a} + \mathfrak{b} = A$, ce qui se traduit l'existence de deux éléments $a \in \mathfrak{a}$ et $b \in \mathfrak{b}$ tels que $a + b = 1$. On généralise ici la notion de coprimalité introduite dans le chapitre précédent pour $\mathbb{Z}$ et l'identité ci-dessus est l'analogue de l'identité de Bézout.

Lemme 2.1.7 — *Si $\mathfrak{a}$ et $\mathfrak{b}$ sont deux idéaux étranger d'un anneau A alors on a l'identité $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{ab}$.*

Démonstration — L'inclusion $\mathfrak{ab} \subset \mathfrak{a} \cap \mathfrak{b}$ étant immédiate, soit c un élément de $\mathfrak{a} \cap \mathfrak{b}$. Ayant fixé deux éléments $a \in \mathfrak{a}$ et $b \in \mathfrak{b}$ tels que $a + b = 1$, on obtient alors l'identité $c = ac + bc$. Les éléments ac et bc appartenant à l'idéal $\mathfrak{ab}$, il en est alors de même pour c, d'où l'inclusion $\mathfrak{a} \cap \mathfrak{b} \subset \mathfrak{ab}$, qui est donc une egálité. □

Théorème 2.1.8 **(Théorème des restes chinois)** — *Étant donnés deux idéaux étrangers $\mathfrak{a}$ et $\mathfrak{b}$ d'un anneau A, les anneaux $A/\mathfrak{ab}$ et $A/\mathfrak{a} \times A/\mathfrak{b}$ sont isomorphes.*

Démonstration — On reprend les notations de la proposition ci-dessus. Les idéaux $\mathfrak{a}$ et $\mathfrak{b}$ étant étrangers, l'anneau S est nul, ce qui implique que $X \times_S Y$ coïncide avec $X \times Y$, d'où un isomorphisme d'anneaux entre $A/\mathfrak{a} \cap \mathfrak{b}$ et $X \times Y$. Le dernier lemme permet de conclure. □

Ce dernier résultat affirme que le système de congruences présenté précédemment admet toujours une solution, qui est unique modulo $\mathfrak{ab}$. Cette dernière peut être explicitée de la manière suivante : étant donnés $a' \in \mathfrak{a}$ et $b' \in \mathfrak{b}$ tels que $a' + b' = 1$, il suffit de poser $x = ab' + a'b$.

Corollaire 2.1.9 — *Si n et m sont deux entiers premiers entre eux alors les anneaux $\mathbb{Z}/nm\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ sont isomorphes.*

Démonstration — C'est un cas particulier du dernier résultat, en remrquant que les idéaux $n\mathbb{Z}$ et $m\mathbb{Z}$ sont étrangers si et seulement si les entiers n et m sont premiers entre eux □

2.1.5. Le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ et la fonction indicatrice d'Euler — Commençons ce paragraphe en remarquant que le pgcd de deux entiers a et n ne dépend que de la classe de congruence de a modulo n. En particulier, nous pouvons écrire sans ambiguïté $x \wedge n$ pour tout $x \in \mathbb{Z}/n\mathbb{Z}$.

Proposition 2.1.10 — *Étant donné un élément $x \in \mathbb{Z}/n\mathbb{Z}$, les conditions suivantes sont équivalente :*

1. *On a $x \in (\mathbb{Z}/n\mathbb{Z})^\times$.*
2. *L'élément x est un générateur du groupe (additif) $\mathbb{Z}/n\mathbb{Z}$.*
3. *On a l'identité $x \wedge n = 1$.*

Démonstration — Montrons les implications (1)⇒(2)⇒(3)⇒(1).
(1)⇒(2) Tout d'abord, le groupe $\mathbb{Z}/n\mathbb{Z}$ est engendré par la classe $\bar{1}$. Par hypothèse, il existe $y \in \mathbb{Z}/n\mathbb{Z}$ tel que $xy = \bar{1}$. En posant $y = \bar{u}$, avec $u \in \mathbb{N}$, on obtient les identités

$$ux = x + \cdots (u) \cdots + x = \bar{1}.$$

En particulier, l'élément $\bar{1}$ appartient au sous-groupe $\langle x \rangle$ de $\mathbb{Z}/n\mathbb{Z}$ engendré par x, d'où $\langle x \rangle = \mathbb{Z}/n\mathbb{Z}$.
(2)⇒(3) Le groupe $\mathbb{Z}/n\mathbb{Z}$ étant engendré par x, il existe un entier (naturel) u tel que $ux = \bar{1}$. En posant $x = \bar{a}$, avec $a \in \mathbb{Z}$, on obtient la congruence $ua \equiv 1 \pmod{n}$, ce qui se traduit par l'existence d'un entier v tel que $ua + vn = 1$, d'où les identités $(x, n) = (a, n) = 1$.
(3)⇒(1) En posant $x = \bar{a}$, avec $a \in \mathbb{Z}$, il existe un couple d'entiers u et v tels que $au + nv = 1$, d'où l'identité $xy = 1$, avec $y = \bar{u}$ et, par suite, la relation $x \in (\mathbb{Z}/n\mathbb{Z})^\times$. □

Proposition 2.1.11 — *Le calcul de l'inverse d'un élément $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ est de complexité $O(\log^2(n))$.*

Démonstration — Un élément $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ est représenté par un entier $a \in \{0, \ldots, n-1\}$ tel que $(a, n) = 1$. La détermination de son inverse se réduit à l'explicitation d'une identité de Bézout $au + nv = 1$, ce qui peur être fait via l'algorithme d'Euclide étendu, avec une complexité de $O(\log^2(n))$.

□

La ***fonction indicatrice d'Euler*** est l'application φ qui associe à un entier $n > 0$ le nombre d'entiers $m \in \{0, \ldots, n-1\}$ premiers avec n. Les premières valeurs de φ sont reportées dans le tableau ci-dessous.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8	8	16

Proposition 2.1.12 — *La fonction indicatrice d'Euler vérifie les propriétés suivantes :*

1. *Pour tout entier $n > 0$, le groupe $(Z/n\mathbb{Z})^\times$ est d'ordre $\varphi(n)$.*
2. *Étant donnés deux enties naturels $n, m > 0$ premiers entre eux, on a l'identité*
$$\varphi(nm) = \varphi(n)\varphi(m).$$
3. *Pour tout nombre premier p et tout entier $e > 0$, on a la relation*
$$\varphi(p^e) = p^{e-1}(p-1).$$

Démonstration — La première assertion découle directement de la proposition 2.1.10 et du fait que tout élément de $\mathbb{Z}/n\mathbb{Z}$ possède un unique représentant dans l'ensemble $\{0, \ldots, n-1\}$. Le théorème des restes chinois affirme que les anneaux $\mathbb{Z}/nm\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ sont isomorphes, ce qui implique que les groupes $(\mathbb{Z}/nm\mathbb{Z})^\times$ et $(\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/m\mathbb{Z})^\times$ sont isomorphes et en comparant leurs ordres on obtient le deuxième point. Finalement, les entiers de l'ensemble $\{0, \ldots, p^e - 1\}$ qui ne sont pas premiers avec p^e sont ceux qui sont divisibles par p ; ils s'écrivent alors comme pa, avec $a \in \{0, \ldots, p^{e-1} - 1\}$ et il en existe donc p^{e-1}, d'où la troisième affirmation. □

Ce dernier résultat permet de calculer explicitement $\varphi(n)$ lorsque l'on connaît la factorisation de n .

Corollaire 2.1.13 — *Pour tout entier n, on a l'identité*
$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right),$$
où p parcourt l'ensemble des nombres premiers divisant n.

Démonstration — En remarquant que l'identité 3 de la proposition précédente peut s'écrire comme
$$\varphi\left(p^e\right) = p^e \left(1 - \frac{1}{p}\right),$$
il suffit d'utiliser la multiplicativité de la fonction indicatrice d'Euler. □

Exercice 2.1.14 — Notons $\omega(n)$ le nombre de diviseurs premiers d'un entier $n > 0$ (comptés sans multiplicité). Montrer que l'on a les inégalités
$$\varphi(n) \geq \frac{n}{\omega(n)+1} \geq \frac{n}{\log_2(n)+1}.$$

Tel qu'il a été défini dans l'appendice, l'ordre d'un élément g d'un groupe fini G est le cardinal du sous-groupe $\langle g \rangle$ qu'il engendre.

Lemme 2.1.15 — *Soit G un groupe fini. L'ordre d'un élément $g \in G$ est le plus petit entier $d > 0$ tel que $g^d = 1$. En particulier, on a l'identité $g^{|G|} = 1$.*

Démonstration — L'application $f : \mathbb{Z} \to G$ définie par $f(n) = g^n$ est un homomorphisme de groupes. Son image coïncidant avec $\langle g \rangle$, on en déduit un isomorphisme entre les groupes $\mathbb{Z}/\ker(f)$ et $\langle g \rangle$. Le sous-groupe

$$\ker(f) = \{n \in \mathbb{Z} \mid g^n = 1\}$$

n'est pas trivial (sinon f serait injectif, ce qui est exclu, car G est fini). On remarquera que dans $\mathbb{Z}$, la notion d'idéal et de sous-groupe (par rapport à la somme) coïncident. D'après la démonstration du théorème 1.1.1, on a alors $\ker(f) = d\mathbb{Z}$, où d est le plus petit élément strictement positif de $\ker(f)$, i.e. le plus petit entier naturel non d nul tel que $g^d = 1$. La dernière assertion découle du théorème de Lagrange : en effet, l'ordre d du sous-groupe $\langle g \rangle$ divise $|G|$ et, en posant $|G| = dn$, on obtient les identités

$$g^{|G|} = g^{dn} = (g^d)^n = 1^n = 1.$$

□

Remarque 2.1.16 — Lorsque G est abélien, la dernière identité du lemme peut être obtenue de manière directe : en effet, le groupe G étant abélien, l'élément $x = \prod_{h \in G} h$ est bien défini. Pour tout $g \in G$, l'application $f : G \to G$ définie par $f(h) = gh$ est bijective. On a alors les identités

$$1 = xx^{-1} = x^{-1} \prod_{h \in G} h = x^{-1} \prod_{h \in G} gh = x^{-1} g^{|G|} \prod_{h \in G} h = g^{|G|} x x^{-1} = g^{|G|}.$$

Exercice 2.1.17 — Montrer qu'un groupe cyclique d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ et possède $\varphi(n)$ générateurs.

Le résultat suivant est un ingrédient fondamental dans la conception du cryptosystème RSA.

***Théorème 2.1.18* (Euler)** — *Soit $n > 0$ un entier. Pour tout entier a premier avec n, on a la congruence*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Démonstration — En posant $x = \bar{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$, la congruence de l'énoncé se traduit par l'identité $x^{\varphi(n)} = 1$ et découle directement du lemme 2.1.15 appliqué au groupe $(\mathbb{Z}/n\mathbb{Z})^\times$. □

Exercice 2.1.19 — Soient $a > 1$ et $n > 0$ deux entiers. Montrer que n divise $\varphi(a^n - 1)$.

Proposition 2.1.20 — *Pour tout nombre entier $n > 1$, on a l'inégalité $\varphi(n) \leq n-1$ et les conditions suivantes sont équivalentes :*

1. *On a l'égalité $\varphi(n) = n - 1$.*
2. *L'entier n est un nombre premier.*
3. *L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps.*

Démonstration — Pour $n > 1$, les entiers 0 et n ne sont pas premiers entre eux, ce qui implique qu'il existe au plus $n-1$ éléments de l'ensemble $\{0, \ldots, n-1\}$ premiers avec n.

Montrons les implications (1)⇒(2)⇒(3)⇒(1). Si $\varphi(n) = n-1$, tout entier non nul $1 < m < n$ est premier avec n (et, en particulier, $m \not| n$), d'où la primalité de n. Si l'entier n est premier, la proposition 1.1.16 affirme que l'idéal $n\mathbb{Z}$ est maximal, ou encore que l'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps (cf. l'appendice). Finalement, si cette dernière condition est remplie, d'après le premier point de la proposition 2.1.12, l'entier $\varphi(n)$ est l'ordre du groupe $(\mathbb{Z}/n\mathbb{Z})^\times = \mathbb{Z}/n\mathbb{Z} - \{0\}$, d'où $\varphi(n) = n-1$. □

Dans la suite, adoptant une convention usuelle, étant donné un nombre premier p, le corps $\mathbb{Z}/p\mathbb{Z}$ est noté $\mathbb{F}_p$.

Corollaire 2.1.21 **(Petit théorème de Fermat)** — *Pour tout $x \in \mathbb{F}_p$, on a l'identité $x^p = x$.*

Démonstration — L'assertion est immédiate pour $x = 0$. Pour $x \neq 0$, on a $x \in \mathbb{F}_p^\times$ (car $\mathbb{F}_p$ est un corps). D'après le théorème 2.1.18 et le lemme ci-dessus, on a l'identité $x^{p-1} = 1$, d'où la relation $x^p = x$. □

Remarque 2.1.22 — Ayant déterminé $\varphi(n)$ (ce qui est immédiat lorsque n est premier), le calcul de l'inverse d'un élémet de $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ peut être calculé en utilisant le théorème 2.1.18, qui amène à l'identité

$$x^{-1} = x^{\varphi(n)-1}.$$

La multiplication dans $\mathbb{Z}/n\mathbb{Z}$ étant de complexité $O(\log^2(n))$, par exponentiation rapide, on obtient un algorithme de calcul de l'inverse de complexité $O(\log^3(n))$.

2.2. Le cryptosystème RSA

2.2.1. Cryptosystèmes à clé publique — La cryptographie à clé publique est apparue en 1976 avec les travaux de Withfield Diffie et Martin Hellman. Un ***cryptosystème à clé publique***, également appelé ***cryptosystème asymétrique***, repose sur l'existence d'une ***clé publique*** pour le chiffrement, et d'une ***clé secrète*** pour le déchiffrement. Ces deux clés sont distinctes. Un utilisateur A qui souhaite envoyer un message à un utilisateur B, chiffre son message au moyen de la clé publique de B, et ce dernier au moyen de sa clé secrète, qu'il est seul à connaître, est alors en mesure de déchiffrer le message envoyé. Deux utilisateurs d'un cryptosystème à clé publique peuvent donc s'échanger des messages chiffrés, via un canal non sécurisé, et sans posséder de secret en commun. Son efficacité est basée sur le fait qu'il est impossible en un temps raisonnable de déterminer la clé secrète à partir de la clé publique.

2.2.2. Principe du protocole — Le protocole RSA est un cryptosystème à clé publique introduit en 1977 par Leonardo Adleman, Ronald Rivest et Adi Shamir. Sa sécurité repose sur le fait que connaissant un entier n, qui est le produit de deux grands nombre premiers p et q distincts, il est généralement très difficile, voire impossible pratiquement, de déterminer p et q, i.e. la factorisation de n. D'un point de vue théorique, le protocole repose sur le résultat suivant, qui est une conséquence du petit théorème de Fermat (cf. corollaire 2.1.21).

Proposition 2.2.1 — *Soient p et q deux nombres premiers distincts et posons $n = pq$. Pour tout entier naturel t congru à 1 modulo $\varphi(n)$ et tout élément $x \in \mathbb{Z}/n\mathbb{Z}$, on a l'identité $x^t = x$.*

Démonstration — D'après le théorème des restes chinois, l'anneau $\mathbb{Z}/n\mathbb{Z}$ est isomorphe à $\mathbb{F}_p \times \mathbb{F}_q$. Il suffit donc de vérifier l'identité $x^t = x$ pour tout $x \in \mathbb{F}_p$ et tout $x \in \mathbb{F}_q$. L'assertion étant immédiate pour $x = 0$, supposons $x \in \mathbb{F}_p$ non nul. Par hypothèse, on a $t = k\varphi(n) + 1$, avec $k \in \mathbb{N}$, et la multiplicativité de la fonction indicatrice d'Euler amène à l'expression $\varphi(n) = (p-1)(q-1)$, d'où les identités

$$x^t = x^{1+k\varphi(n)} = x \cdot x^{k(p-1)(q-1)} = x \cdot (x^{p-1})^{k(q-1)} = x,$$

la dernière égalité découlant du théorème 2.1.18 ou du corollaire 2.1.21. □

Nous pouvons maintenant décrire le protocole. Chaque utilisateur procède de la façon suivante :

- Il choisit deux nombres premiers p et q et determine ensuite les entier $n = pq$ et $\varphi(n) = (p-1)(q-1)$.
- Il choisit un entier e premier avec $\varphi(n)$ tel que $1 < e < \varphi(n)$. La classe de e modulo $\varphi(n)$ est donc inversible dans $\mathbb{Z}/\varphi(n)\mathbb{Z}$.
- Il détermine l'entier d tel que $1 < d < \varphi(n)$ et $ed \equiv 1 \mod \varphi(n)$. La classe de d modulo $\varphi(n)$ est donc l'inverse de la classe de e dans $\big(\mathbb{Z}/\varphi(n)\mathbb{Z}\big)^\times$.
- Il publie ensuite le couple (e, n), qui est sa ***clé publique***, et il conserve secret l'élément d, qui est sa ***clé secrète*** ou ***privée***.

Soit A un utilisateur dont la clé publique est (e, n) et la clé secrète est d. L'***algorithme de chiffrement*** de A est l'application $f_A : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ définie pour tout $x \in \mathbb{Z}/n\mathbb{Z}$ par $f_A(x) = x^e$. C'est une bijection de $\mathbb{Z}/n\mathbb{Z}$ et d'après la proposition 2.2.1, on a $f_A^{-1}(x) = x^d$. On dit que f_A^{-1} est l'***algorithme de déchiffrement*** de A et l'élément x^e est appelé ***cryptogramme***. Si une personne B souhaite envoyer un message secret à A sous la forme d'un élément $x_0 \in \mathbb{Z}/n\mathbb{Z}$, il utilise la clé publique de A en lui envoyant l'élément $f_A(x_0)$. Afin d'obtenir x_0, il suffit alors pour A d'utiliser sa clé secrète en calculant $f_A^{-1}(x_0^e)$.

Exemple 2.2.2 — Prenons $(e, n) = (239, 406121)$ comme clé publique. On a $n = pq$ avec $p = 101$ et $q = 4021$. Il est facile de vérifier que p et q sont premiers (si q n'était

pas premier il devrait posséder un diviseur premier plus petit que $63 = \lfloor\sqrt{4021}\rfloor$, et ce n'est pas le cas). On obtient

$$\varphi(n) = 100 \cdot 4020 = 402000.$$

Afin de déterminer la clé secrète, il s'agit de calculer l'inverse de 239 modulo 402000. On utilise l'algorithme d'Euclide. Avec la présentation adoptée de cet algorithme, on obtient le tableau suivant :

	1682	119	2	
402000	239	2	1	0
1	0	1	-119	
0	1	-1682	200159	

La clé secrète est donc $d = 200159$.

2.2.3. Signature — L'algorithme RSA fournit un moyen de signer, ou d'authentifier, les messages. Soit A un utilisateur ayant pour clé publique (e, n) et pour clé secrète d. Supposons que A souhaite envoyer à B un message $x \in \mathbb{Z}/n\mathbb{Z}$, sans se préoccuper de sa confidentialité, mais de sorte que B soit certain que c'est bien A qui lui a transmis x. Pour cela, A envoie à B le couple

$$(x, x^d) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

Avec la clé publique (e, n), B calcule alors

$$(x^d)^e = x^{de} = x.$$

Puisque A est seul à connaître d, B peut être a priori certain que c'est bien A l'expéditeur du message.

2.2.4. Cryptanalyse — Pour qu'un cryptosystème soit utilisable dans la pratique, il est nécessaire que le chiffrement et de déchiffrement (connaissant la clé secrète) puissent être effectués en un temps raisonnable. Idéalement, on souhaite que ces algorithmes soient en temps polynomial par rapport à la taille des clés. Dans la suite de se paragraphe, on fixe deux nombres premiers distincts p et q et l'on pose $n = pq$.

Proposition 2.2.3 — *Les algorithmes de chiffrement et de déchiffrement du protocole RSA utilisant un entier $n = pq$ sont de complexité $O(\log^3(n))$.*

Démonstration — Le chiffrement, ainsi que le déchiffrement sont juste des calculs de puissances dans $\mathbb{Z}/n\mathbb{Z}$. L'exposant étant inférieur à n, la proposition 2.1.5 affirme que la complexité est $O(\log^3(n))$. □

Remarque 2.2.4 — Il est également important de s'intéresser à la complexité de la mise en place du protocole lui-même. La clé publique est généralement choisie par un processus aléatoire. La détermination de la clé privée, qui se réduit au calcul de l'inverse de la clé publlique nodulo $\varphi(n)$, est de complexité $O(\log^2(n))$ (la complexité

est en fait dominée par la fonction $\log^2(\varphi(n)$, cette dernièrer étant elle-même dominée par $\log^2(n)$). Il ne reste qu'à déterminer une méthode efficace et rapide de construction des nombres premiers p et q. Cette question est cruciale en cryptographie, que ce soit d'un point de vue thérique ou pratique. Les contraintes de temps imposées à ce cours ne nous permettent malheureusement pas d'aborder ce sujet.

Considérons et une clé publique (e, n) utilisée lors d'un protocole RSA et notons d la cé secrète correspondante. Une personne souhaitant retrouver le message initial à partir de son cryptogramme peut commencer par essayer d'évaluer $\varphi(n)$, la clé secrète étant alors obtenue rapidement via l'algotithme d'Euclide. Cette démarche n'est pas très efficace. Le résultat suivant montre en effet que la connaissance de $\varphi(n)$ permet d'obtenir la factorisation de n par un algorithme de complexité polynomiale, là où le cryptosystème RSA repose justement sur la difficulté d'obtenir une telle factorisation (en un temps raisonnable).

Lemme 2.2.5 — *Connaisant n et $\varphi(n)$, il existe un algorithme de complexité $O(\log^3(n))$ permettant de déterminer p et q.*

Démonstration — Quitte à permuter p et q, on se réduit au cas $q < p$. Connaissant n et $\varphi(n)$, les entiers naturels

$$m = n - \varphi(n) + 1 = p + q \quad \text{et} \quad \Delta = m^2 - 4n = (p - q)^2$$

sont déterminés avec des algorithmes de complexités respectives $O(\log(n))$ (deux sommes) et $O(\log^2(n))$. En utilisant l'algorithme présenté dans le chapitre précédent, l'extraction de la racine carrée de Δ est de complexité $O(\log^3(n))$. L'identité

$$2p = m + \sqrt{\Delta}$$

Permet d'obtenir p en effectuant une somme et une division par 2 (un décalage à droite, en termes d'opérations sur les bits), pour une complexité de $O(\log(n))$. Globalement, cet algorithme de factorisation est donc de complexité $O(\log^3(n))$. □

Remarque 2.2.6 — Lors d'un protocole RSA, il est primordial de vérifier que le message x à envoyer soit premier avec n. En effet, dans la pratique, x ainsi que le cryptogramme $z = x^e$ sont représentés par des entiers naturels non nuls et strictement inférieurs à n. Si x et n n'étaient pas premiers entre eux, il en serait de même pour z et n. Leur pgcd, déterminé rapidement par l'algorithme d'Euclide, fournirait alors un diviseur non trivial de n, ce qui permettrait d'obtenir la factorisation de n et de déchiffrer ainsi tout cryptogramme. Ceci étant, lors d'une implémentation effective du protocole, la probabilité de tomber sur un élément x qui ne soit pas premier avec n est pratiquement nulle. En effet, en posant $n = pq$, avec $p < q$, on a les relations

$$\frac{\varphi(n)}{n} = 1 - \frac{1}{p} - \frac{1}{q} + \frac{1}{n} > 1 - \frac{2}{p}.$$

En particulier, si p est un nombre premier de 1024 bits, la probabilité qu'un entier $m < n$ pris au hasard ne soit pas premier avec n est inférieure à 2^{-1023}.

Il faut remarquer que, bien que suffisante, la connaissance de $\varphi(n)$ n'est pas vraiment indispensable pour pouvoir déchiffrer un message. Il est en fait suffisant de déterminer un entier r tel que $x^{er} = x$ pour tout $x \in \mathbb{Z}/n\mathbb{Z}$.

Proposition 2.2.7 — *Posons $m = (p-1) \vee (q-1)$. Pour tout entier $u > 0$, les conditions suivantes sont équivalentes :*

1. *$x^u = x$ pour tout $x \in \mathbb{Z}/n\mathbb{Z}$.*
2. *$u \equiv 1 \pmod{m}$.*

Démonstration — D'après le théorème des restes chinois, le groupe $\mathbb{Z}/n\mathbb{Z}$ est isomorphe à $\mathbb{F}_p \times \mathbb{F}_q$. La première condition est donc équivalente à $x^u = x$ pour tout $x \in \mathbb{F}_p$ et tout $x \in \mathbb{F}_q$. Soit $x \in \mathbb{F}_q$. Pour $x = 0$ on a toujours $x^u = x$. On peut donc se réduire au cas $x \in \mathbb{F}_p^\times$. La condition $x^u = x$ est alors équivalente à $x^{u-1} = 1$. Nous admettons ici le fait que le groupe $\mathbb{F}_p^\times$ est cyclique, d'ordre $p-1$ (ce résulat sera démontré dans le chapitre 3). Dans cette dernière condition, on peut alors se restreindre au cas où x est un générateur du groupe, auquel cas elle est vérifiée si et seulement si $p-1$ divise $u-1$. En procédant de manière analogue pour $\mathbb{F}_q$ on en déduit que la première condition de la proposition est équivalente à $p-1|u-1$ et $q-1|u-1$, ce qui se traduit par $m|u-1$. □

Corollaire 2.2.8 — *En posant $t = (p-1) \wedge (q-1)$, il existe t entiers r dans l'intervalle $[1, \varphi(n)[$ tels que $x^{er} = x$ pour tout $x \in \mathbb{Z}/n\mathbb{Z}$.*

Démonstration — D'après la proposition 2.2.7, la condition du corollaire est équivalente à $er \equiv 1 \pmod{m}$, qui admet une unique solution $r_0 \in \{1, \ldots, m-1\}$. On en déduit que r appartient à l'ensemble $\{r_0, r_0 + m, \ldots, r_0 + (t-1)m\}$, qui est de cardinal t. □

Un entier $r \in \{1, \ldots, \varphi(n) - 1\}$ vérifiant la condition du lemme est appelé ***clé de déchiffrement***. Lors du choix des nombres premiers p et q il est préférable de vérifier que le pgcd de $p-1$ et $q-1$ est petit, afin d'éviter l'existence de nombreuses clés de déchiffrement. L'existence de plusieurs clés de déchiffrement constitue également une faille dans la procédure de signature d'un message. En effet, elle permet juste d'affirmer que l'expéditeur possède une clé de déchiffrement, qui peut être différente de la clé secrète. Ceci dit, le nombre de clés de déchiffrement est majoré par $\sqrt{n} - 1$, et la probabilité d'en obtenir une de manière aléatoire est pratiquement nulle lorsque n est grand.

Exemples 2.2.9 —

1. Reprenons les valeurs $p = 101$ et $q = 4021$ de l'exemple précédent. Un simple calcul montre que $100 \wedge 4020 = 20$. Il existe donc 20 clés de déchiffrement, données explicitement par la formule $19259 + 20100k$, avec $k \in \{0, \ldots, 19\}$. La clé secrète est obtenue pour $k = 9$.
2. Si les nombres premiers p et q sont impairs (ce qui est toujours le cas dans la pratique), il existe toujours au moins deux clés de déchiffrement. Il en existe exactement deux si et seulement si $\frac{p-1}{2}$ et $\frac{q-1}{2}$ sont premiers entre eux. Tel est le cas par exemple si $p = 2p' + 1$ et $q = 2q' + 1$ avec p' et q' premiers. En supposant $p < q$, le nombre de clés de déchiffrement est maximal lorsque $p - 1$ divise $q - 1$, auquel cas il en existe exactement $p - 1$.

Exercice 2.2.10 — Afin d'utiliser le protocole RSA, Alice choisit les nombres premiers $p = 101$ et $q = 131$. Elle transmet ensuite la clé publique $(3901, 13231)$. Elle réalise assez vite que son choix était très mauvais. Pourquoi ?

2.3. Symbole de Legendre et carrés dans $\mathbb{Z}/n\mathbb{Z}$

2.3.1. Le symbole de Legendre — Dans la suite $p > 2$ désigne un nombre premier. Étant donné un entier n, le ***symbole de Legendre*** $(\frac{n}{p})$ est l'entier défini par la relation

$$\left(\frac{n}{p}\right) = \begin{cases} 0 \text{ si } p|n, \\ 1 \text{ si } p\not|n \text{ et n est un carré modulo } p, \\ -1 \text{ sinon.} \end{cases}$$

Un entier n tel que $(\frac{n}{p}) = 1$ est appelé ***résidu quadratique***. Si $(\frac{n}{p}) = -1$, on parle de ***non-résidu quadratique***. Par définition, le symbole de Legendre $(\frac{n}{p})$ ne dépend que de la classe de n modulo p. En effectuant une division euclidienne, on peut donc toujours se réduire au cas $0 \leq n < p$. De plus, étant donné $x \in \mathbb{F}_p$, on peut écrire $(\frac{x}{p})$ sans ambiguité. Notons $(\mathbb{F}_p^\times)^2$ le sous-groupe des carrés de $\mathbb{F}_p^\times$, i.e. l'image de l'homomorphisme $\mathbb{F}_p^\times \to \mathbb{F}_p^\times$ d'élévation au carré. On a alors $(\frac{x}{p}) = 1$ si et seulement si $x \in (\mathbb{F}_p^\times)^2$. Avec un légér abus de langage, les éléments de $(\mathbb{F}_p^\times)^2$ seront également appelés résidus quadratiques. Le résultat ci-dessous affirme que la moitié des éléments de $\mathbb{F}_p^\times$ sont des résidus quadratiques.

Lemme 2.3.1 — *Le groupe $(\mathbb{F}_p^\times)^2$ est d'ordre $(p-1)/2$.*

Démonstration — Le noyau de l'homomorphisme $\mathbb{F}_p^\times \to \mathbb{F}_p^\times$ d'élévation au carré étant le sous-groupe $\mu_2 = \{\pm 1\}$, le théorème d'isomorphisme pour les groupes affirme que son image, qui n'est autre que $(\mathbb{F}_p^\times)^2$, est d'ordre $(p-1)/2$. □

Théorème 2.3.2 **(Euler)** — *On a la congruence*

$$\left(\frac{n}{p}\right) \equiv n^{\frac{p-1}{2}} \pmod{p}.$$

Démonstration — L'assertion étant claire pour $x = 0$, supposons x non nul. Considérons l'homomorphisme de groupes $g : \mathbb{F}_p^\times \to \mathbb{F}_p^\times$ défini par $g(x) = x^{(p-1)/2}$. On doit montrer que pour tout $x \in \mathbb{F}_p$, on a l'identité $g(x) = \left(\frac{x}{p}\right)$. Les relations $g(x)^2 = x^{p-1} = 1$ impliquent que l'image de g est contenue dans le sous-groupe $\mu_2 = \{\pm 1\}$ de $\mathbb{F}_p^\times$. En admettant une fois encore que le groupe $\mathbb{F}_p^\times$ est cyclique et en fixant un de ses générateurs t, on a nécessairement $g(t) \neq 1$, ce qui implique que l'image de g coïncide avec μ_2 et, par suite, que $\ker(g)$ est d'ordre $(p-1)/2$. Par ailleurs le lemme 2.1.15 amène à l'inclusion $(\mathbb{F}_p^\times)^2 \subset \ker(g)$, qui est alors une égalité (il suffit de comparer les ordres). On a donc $(\frac{x}{p}) = 1$ (resp. $(\frac{x}{p}) = -1$) si et seulement si $g(x) = 1$ (resp. $g(x) = -1$), d'où $g(x) = (\frac{x}{p})$ pour tout $x \in \mathbb{F}_p^\times$. □

Remarque 2.3.3 — Les classes des entiers $0, 1$ et -1 modulo p étant deux à deux distinctes, le symbole de Legendre est univoquement déterminé par sa classe modulo p. En particulier, le théorème 2.3.2 fournit une méthode de calcul effectif de $(\frac{n}{p})$.

Corollaire 2.3.4 — *Étant donnés un nombre premier $p > 2$ et deux entiers n et m, on a l'identité*

$$\left(\frac{nm}{p}\right) = \left(\frac{n}{p}\right)\left(\frac{m}{p}\right).$$

Démonstration — D'après le théorème 2.3.2, on a les congruences

$$\left(\frac{nm}{p}\right) \equiv (nm)^{\frac{p-1}{2}} \equiv n^{\frac{p-1}{2}} m^{\frac{p-1}{2}} \equiv \left(\frac{n}{p}\right)\left(\frac{m}{p}\right) \pmod{p},$$

ce qui implique que l'entier $a = (\frac{nm}{p}) - (\frac{n}{p})(\frac{m}{p})$ est divisible par p. Les inégalité $|a| \leq 2 < p$ amènent alors à l'identité $a = 0$. □

Corollaire 2.3.5 — *Pour tout nombre premier $p > 2$, on a l'identité*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

En particulier, -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si p est congru à 1 modulo 4.

Démonstration — On procède exactement comme dans la démonstration du corollaire 2.3.4. □

Proposition 2.3.6 — *Étant donnés un nombre premier $p > 2$ et un entier naturel $n < p$, le calcul du symbole de Legendre $(\frac{n}{p})$ est de complexité $O(\log^3(p))$.*

Démonstration — D'après la remarque 2.3.3, il suffit de déterminer la classe de $(\frac{n}{p})$ modulo p. Le théorème 2.3.2 affirme que ceci revient à calculer $\bar{n}^{(p-1)/2}$ dans $\mathbb{F}_p$. La multiplication dans $\mathbb{F}_p$ étant de complexité $O(\log^2(p))$, en utilisant l'algorithme d'exponentiation rapide, on obtient une méthode de calcul du symbole de Legendre de complexité de $O(\log^3(p))$. □

Remarque 2.3.7 — En utilisant la ***loi de réciprocité quadratique*** pour le le ***symbole de Jacobi***, on obtient un algorithme de calcul de $(\frac{n}{p})$ de complexité $O(\log^2(p))$ (cf. le complément à ce chapitre).

2.3.2. Extraction de racines carrées dans $\mathbb{F}_p$ — Soit $p > 2$ un nombre premier. Du moment où l'on sait qu'un élément $x \in \mathbb{F}_p^\times$ est un carré, il est nécessaire de déterminer un algorithme de calcul de ses (deux) racines carrées. Dans ce cours, nous ne traiterons explicitement que le cas où p est congru à 3 modulo 4, qui est particulièrement simple. Dans le cas général, on dispose de méthodes efficaces, telles que l'algorithme de ***Cipolla***, ou celui de ***Tonelli-Shanks***, qui nécessitent néanmoins la connaissance d'un non-résidu quadratique de $\mathbb{F}_p^\times$.

Proposition 2.3.8 — *Soit $x \in \mathbb{F}_p^\times$ un résidu quadratique. Si p est congru à 3 modulo 4 alors l'élément*

$$y = x^{\frac{p+1}{4}}$$

est une racine carrée de x (l'autre étant égale à $-x$).

Démonstration — En s'appuyant sur le corollaire 2.3.2, on a les identités

$$y^2 = x^{\frac{p+1}{2}} = x \cdot x^{\frac{p-1}{2}} = x\left(\frac{x}{p}\right) = x.$$

□

Corollaire 2.3.9 — *Pour p congru à 3 modulo 4, l'extraction de racines carrées dans $\mathbb{F}_p$ est de complexité $O(\log^3(p))$.*

Démonstration — Il suffit d'appliquer la proposition précédente en utilisant l'algorithme d'exponentiation rapide. □

2.3.3. Carrés dans $\mathbb{Z}/n\mathbb{Z}$ — Au vu des applications en cryptographie, nous n'étudierons les carrés et les méthodes d'extraction de racines carrés dans $\mathbb{Z}/n\mathbb{Z}$ que dans le cas particulier où $n = pq$ est le produit de deux nombres premiers impairs $p \neq q$, qui sont fixés une fois pour toutes. Comme pour $\mathbb{F}_p$, un carré de $(\mathbb{Z}/n\mathbb{Z})^\times$ est appelé résidu quadratique. Étant donné un groupe abélien G, on note $G[2]$ le ***sous-groupe de 2-torsion***, formé par les éléments $g \in G$ tels que $g^2 = 1$.

Lemme 2.3.10 — *Le groupe $(\mathbb{Z}/n\mathbb{Z})^\times[2]$ est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*

Démonstration — Étant donnés deux groupes G et H, on montre facilement que l'identité $(G \times H)[2] = G[2] \times H[2]$. Le lemme découle alors du théorème des restes chinois, qui affirme que $(\mathbb{Z}/n\mathbb{Z})^\times$ est isomorphe à $\mathbb{F}_p^\times \times \mathbb{F}_q^\times$, et du fait que les groupes $\mathbb{F}_p^\times[2]$ et $\mathbb{F}_q^\times[2]$ sont isomorphes à $\mathbb{Z}/2\mathbb{Z}$. □

Corollaire 2.3.11 — *Un résidu quadratique de $(\mathbb{Z}/n\mathbb{Z})^\times$ possède 4 racines carrées.*

Démonstration — Soit $x = y^2$ un carré de $(\mathbb{Z}/n\mathbb{Z})^\times$. Un élément $z \in (\mathbb{Z}/n\mathbb{Z})^\times$ est une racine carrée de x si et seulement si $z^{-1}y$ appartient à $(\mathbb{Z}/n\mathbb{Z})^\times[2]$. Il suffit alors d'appliquer le lemme ci-dessus. □

Proposition 2.3.12 — *On a les propriétés suivantes :*

1. *Le sous-groupe des carrés de $(\mathbb{Z}/n\mathbb{Z})^\times$ est d'ordre $\frac{1}{4}\varphi(n)$.*
2. *Un élément $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ est un carré si et seulement si $(\frac{x}{p}) = (\frac{x}{q}) = 1$.*

Démonstration — L'élévation au carré définit un endomorphisme $(\mathbb{Z}/n\mathbb{Z})^\times$ ayant pour image le sous-groupe des carrés et pour noyau le groupe $(\mathbb{Z}/n\mathbb{Z})^\times[2]$. Le point 1 découle alors du théorème d'isomorphisme pour les groupes et du lemme 2.3.10. Le théorème des restes chinois implique que l'homomorphisme canonique $f : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{F}_p^\times \times \mathbb{F}_q^\times$ est un isomorphisme. Un élément $(x, y) \in \mathbb{F}_p^\times \times \mathbb{F}_q^\times$ étant un carré si et seulement s'il en est de même pour x et y, on obtient le point 2. □

Le ***problème de la résidualité quadratique***[1] consiste à déterminer si un élément de $(\mathbb{Z}/n\mathbb{Z})^\times$ est un résidu quadratique. Si l'on connaît la factorisation de n, le point 2 de la proposition 2.3.12 réduit la question au simple calcul de deux symboles de Legendre, ce qui peut être effectué par un algorithme de complexité $O(\log^3(n))$. Par contre, lorsque la factorisation de n n'est pas connue, on ne dispose pas d'algorithme de complexité polynomiale permettant de résoudre le problème. De nombreux protocoles cryptographiques se basent sur cette dichotomie. On retrouve une situation analogue lorsque l'on s'intéresse au problème d'extraction de racines carrées d'un résidu quadratique x de $\mathbb{Z}/n\mathbb{Z}$: si l'on connaît p et q, en appliquant les méthodes décrites dans les paragraphes précédents, on détermine facilement les racines carrées de x dans $\mathbb{F}_p$ et $\mathbb{F}_q$. Une identité de Bézout permet alors d'en déduire ses racines carrées dans $\mathbb{Z}/n\mathbb{Z}$. Si, par contre, on ne connaît pas la factorisation de n, la détermination des racines carrées de x est un problème difficile, équivalent à la factorisation de n, comme le montre le résultat ci-dessous.

Proposition 2.3.13 — *La connaissance de* 3 *racines carrées d'un résidu quadratique de $(\mathbb{Z}/n\mathbb{Z})^\times$ permet d'obtenir la factorisation de n par un algorithme de complexité $O(\log^2(n))$.*

Démonstration — Si $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ est une racine carrée d'un résidu quadratique, il en est de même pour $-x$. Soit $y \neq \pm x$ une troisième racine carrée. On obtient alors l'identité $(x - y)(x + y) = 0$. L'entier $d = (x - y, n)$ est différent de 1 (dans le cas contraire, on aurait $y = -x$) et de n (autrement, on obtiendrait $y = x$). On a donc $d = p$ ou $d = q$. En utilisant l'algorithme d'Euclide, la détermination de d est de complexité $O(\log^2(n))$, d'où le résultat. □

1. Dans la littérature, on retrouve également le terme résiduosité, un néologisme qui nous parraît plus que dissonant.

2.4. Applications cryptographiques

2.4.1. Le cryptosystème de Rabin — Le ***cryptosystème de Rabin*** est un protocole d'échange à clé publique basé sur la difficulté d'extraire des racines carrées dans $\mathbb{Z}/n\mathbb{Z}$ lorsque l'on ne connaît pas la factorisation de n. Voulant communiquer de manière confidentielle en utilisant un réseau non sécurisé, deux utilisateurs, Alice et Bob, procèdent de la manière suivante :

- Alice choisit deux nombres premiers distincts p et q congrus à 3 modulo 4, qui constituent sa clé secrète, et publie leur produit $n = pq$, qui est la clé publique.
- Afin d'envoyer un message $u \in \mathbb{Z}/n\mathbb{Z}$, Bob transmet à Alice l'élément $v = u^2$.
- Alice détermine les quatre racines carrées de u dans $\mathbb{Z}/n\mathbb{Z}$. L'une d'entre elles est le message original.

La phase de chiffrement se réduisant à une simple élévation au carré dans $\mathbb{Z}/n\mathbb{Z}$, elle est de complexité $O(\log^2(n))$. Connaissant la factorisation de n, la phase de déchiffrement nécessite l'extraction de racines carrées dans $\mathbb{F}_p$ et $\mathbb{F}_q$, qui peut être effectuée en appliquant la proposition 2.3.8. Elle est donc de complexité $O(\log^3(n))$. Si une tierce personne récupère le cryptogramme u, elle ne peut le déchiffrer, à moins connaître la factorisation de n.

2.4.2. Le protocole de Goldwasser-Micali — Ce cryptosystème se base sur le problème de la résiduosité quadratique (cf. la fin du paragraphe 2.3.3). C'est une fois encore un protocole à clé publique, qui se déroule de la manière suivante :

- Alice choisit deux nombres premiers impairs $p < q$ et calcule l'entier $n = pq$. Elle choisit ensuite un entier n tel que $(\frac{x}{p}) = (\frac{x}{q}) = -1$. Sa clé privée est le couple (p, q), la clé publique est le couple (x, n).
- Bob veut transmettre à Alice une suite de bits $(a_1, \ldots, a_r)$. Pour chaque $i \in \{1, \ldots, r\}$, il choisit un élément $x_i \in (\mathbb{Z}/n\mathbb{Z})^\times$ au hasard et calcule $y_i = x_i^2 x^{a_i}$. Il envoie ensuite à Alice la suite $(y_1, \ldots, y_r)$.
- Afin de déchiffrer le cryptogramme $(y_1, \ldots, y_r)$, en calculant $(\frac{y_i}{p})$ et $(\frac{y_i}{q})$, Alice détermine si y_i est un carré dans $\mathbb{Z}/n\mathbb{Z}$. Si c'est le cas, elle en déduit que $a_i = 0$, sinon, $a_i = 1$.

La phase de chiffrement est de complexité $O(r \log^2(n))$, car elle se réduit à r élévations au carré et à r multiplications (au plus) dans $\mathbb{Z}/n\mathbb{Z}$. Le déchiffrement ne nécessite que le calcul de deux symboles de Legendre. Il est donc de complexité $O(r \log^2(n))$. On remarquera que lors de la phase de déchiffrement, seul le calcul de $(\frac{y_i}{p})$ est nécessaire. On a en effet les identités

$$\left(\frac{y_i}{q}\right) = \left(\frac{x_i^2}{q}\right)\left(\frac{x}{q}\right)^{a_i} = \left(\frac{x}{q}\right)^{a_i} = \left(\frac{x}{p}\right)^{a_i} = \left(\frac{x_i^2}{p}\right)\left(\frac{x}{p}\right)^{a_i} = \left(\frac{y_i}{p}\right).$$

2.4.3. Alice et Bob jouent à pile ou face — Afin de jouer à pile ou face à distance, Alice et Bob procèdent de la manière suivante :

- Alice choisit deux nombres premiers distincts p et q et elle transmet leur produit $n = pq$ à Bob.
- Bob choisit au hasard un entier strictement positif $a < \frac{n}{2}$ (lancer de la pièce) et envoie à Alice son carré b modulo n.
- Alice détermine les quatre racines carrées de b modulo n. Seules deux d'entre elles sont représentées par des entiers positifs a et c inférieurs à $\frac{n}{2}$. Elle en choisit une, et l'envoie à Bob (elle parie que c'est l'entier a choisi par Bob).
- Si Bob n'est pas en mesure d'exhiber c, c'est que l'entier envoyé par Alice coïncide avec a ; elle a donc remporté son pari. En effet, ne connaissant pas la factorisation de n, Bob n'est pas en mesure d'extraire des racines carrées dans $\mathbb{Z}/n\mathbb{Z}$ (en un temps raisonnable) et ne peut donc pas tricher.

Si Alice et Bob veulent réitérer le pari, il est nécessaire de changer les valeurs de p et q. Dans le cas contaire, dès qu'Alice perd le pari, Bob est en mesure de factoriser n, car il connait toutes les racines carrées d'un élément de $\mathbb{Z}/n\mathbb{Z}$ (cf. la proposition 2.3.13), et peut donc tricher.

2.5. Complément : réciprocité quadratique et symbole de Jacobi

2.5.1. La loi de réciprocité quadratique — Nous allons commencer avec un résultat classique en théorie élémentaire des nombres.

***Théorème 2.5.1* (Wilson)** — *Pour tout nombre premier p, on a la congruence*

$$(p-1)! \equiv -1 \pmod{p}$$

Démonstration — La classe de $(p-1)!$ modulo p n'est autre que le produit des éléments de $\mathbb{F}_p^\times$. Étant donné un élément $x \in \mathbb{F}_p^\times$, si $x \neq x^{-1}$, les éléments x et x^{-1} apparaissent dans un tel produit et s'éliminent donc. On en déduit que la classe de $(p-1)!$ modulo p est le produit des éléments $x \in \mathbb{F}_p^\times$ tels que $x = x^{-1}$, ce qui se traduit par $x = \pm 1$. □

Corollaire 2.5.2 — *Soit $p > 2$ un nombre premier. En posant $m = (p-1)/2$, on a la congruence*

$$m!^2 \equiv (-1)^{m+1} \pmod{p}.$$

Démonstration — Le théorème de Wilson amène aux congruences

$$-1 \equiv (p-1)! \equiv \prod_{k=1}^{m} k(p-k) \equiv (-1)^m m!^2 \pmod{p},$$

d'où le résultat. □

Nous pouvons à présent énoncer et démontrer la ***loi de réciprocité quadratique***. Il existe à ce jour plus de 300 démonstrations différentes de ce résultat fondamental. Celle que nous proposons ici repose sur le théorème des restes chinois.

Théorème 2.5.3 — *Étant donnés deux nombres premiers impairs p et q, on a l'identité*

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right).$$

Démonstration — Le résultat étant trivial pour $p = q$, supposons p et q distincts. Notons G le quotient du groupe $\mathbb{F}_p^\times \times \mathbb{F}_q^\times$ par le sous-groupe $\{(1,1),(-1,-1)\}$. Notre but est de calculer de deux manières différentes le produit t de tous les éléments de G. Indiquons par $[x,y]$ l'image dans G de $(x,y) \in \mathbb{F}_p^\times \times \mathbb{F}_q^\times$ par la projection canonique $\mathbb{F}_p^\times \times \mathbb{F}_q^\times \to G$. Un élément de G s'écrit de manière unique comme $[a,b]$, avec $a,b \in \mathbb{Z}$ vérifiant $0 < a \leq n$ et $0 < b < q$. On obtient alors les relations

$$t = \prod_{g\in G} g = \prod_{a=1}^{n}\prod_{b=1}^{q-1} [a,b] = \prod_{a=1}^{n} \left[a^{q-1}, (q-1)!\right] = \left[(n!)^{2m}, ((q-1)!)^n\right].$$

Le théorème de Wilson amène alors à l'expression

$$t = \left[\left((n!)^2\right)^m, (-1)^n\right] = \left[(-1)^{m(n+1)}, (-1)^n\right] = \left[(-1)^{mn+n+m}, 1\right].$$

D'autre part, le théorème des restes chinois affirme que les groupes $(\mathbb{F}_p)^\times \times (\mathbb{F}_q)^\times$ et $(\mathbb{Z}/pq\mathbb{Z})^\times$ sont isomorphes. Un élément $x \in G$ s'écrit alors de manière unique comme $x = [a,a]$, où a appartient à l'ensemble $S \subset \{1,\ldots,\frac{pq-1}{2}\}$ formé par les entiers premier avec p et q. Remarquons maintenant qu'un entier appartenant à $\{1,\ldots,\frac{pq-1}{2}\}$ ne peut être à la fois divisible par p et q. En posant

$$A = \prod_{a\in S} a \quad \text{et} \quad B = \prod_{a=1}^{n} qa,$$

et, compte tenu des relations $\frac{pq-1}{2} = nq + m = mp + n$, on en déduit alors l'identité

$$AB = \prod_{\substack{a=1 \\ a\wedge p=1}}^{mp+n} a.$$

En appliquant le théorème 2.1.18, on en déduit les congruences

$$\begin{cases} B \equiv q^n n! \equiv \left(\frac{q}{p}\right) n! \pmod{p}, \\ \\ AB \equiv ((p-1)!)^m n! \equiv (-1)^m n! \pmod{p}, \end{cases}$$

et finalement

$$A \equiv (-1)^m \left(\frac{q}{p}\right) \pmod{p}.$$

De manière tout à fait analogue, on obtient la congruence

$$A \equiv (-1)^n \left(\frac{p}{q}\right) \pmod{q},$$

et le théorème découle des identités $t = [A,A] = [(-1)^{nm+n+m}, 1]$. □

Remarque 2.5.4 — La loi de réciprocité quadratique affirme que si p et q sont congrus à 3 modulo 4 alors $(\frac{p}{q}) = -(\frac{q}{p})$, sinon $(\frac{p}{q}) = (\frac{q}{p})$.

2.5.2. Le symbole de Jacobi — Soit n un entier naturel impair et considérons sa factorisation $n = \prod_{p|n} p^{e_p}$. Pour tout entier m, le ***symbole de Jacobi*** $\left(\frac{m}{n}\right)$ est l'entier défini par la relation

$$\left(\frac{m}{n}\right) = \prod_{p|n} \left(\frac{m}{p}\right)^{e_p}.$$

Si n est premier, on retrouve le symbole de Legendre usuel.

Proposition 2.5.5 — *Le symbole de Jacobi vérifie les propriétés suivantes :*

1. *On a* $(\frac{m}{n}) \in \{0, 1, -1\}$ *et* $(\frac{m}{n}) \neq 0$ *si et seulement si* n *et* m *sont premiers entre eux.*
2. *Le symbole de Jacobi* $(\frac{m}{n})$ *ne dépend que de la classe de* m *modulo* n*.*
3. *Quels que soient les entiers* u *et* v*, on a la relation*
$$\left(\frac{uv}{n}\right) = \left(\frac{u}{n}\right)\left(\frac{v}{n}\right).$$
4. *Quels que soient les entiers impairs* u *et* v*, on a la relation*
$$\left(\frac{m}{uv}\right) = \left(\frac{m}{u}\right)\left(\frac{m}{v}\right).$$

Démonstration — Ce sont toutes des conséquences directes de la définition du symbole de Jacobi et des propriétés du symbole de Legendre. □

Lemme 2.5.6 — *Pour tout entier impair* n*, posons* $\psi(n) = \frac{n-1}{2}$*. On a alors la congruence*

$$\psi(nm) \equiv \psi(n) + \psi(m) \pmod 2.$$

Démonstration — En posant $n = 2u + 1$ et $m = 2v + 1$, on a les identités

$$\psi(nm) \equiv \frac{(2u+1)(2v+1)-1}{2} \equiv 2uv + u + v \equiv \psi(n) + \psi(m) \pmod 2.$$

□

Corollaire 2.5.7 — *Pour tout entier impair* n*, on a l'identité*

$$\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}.$$

Démonstration — Considérons la factorisation $n = \prod_{p|n} p^{e_p}$. En combinant le corollaire 2.3.5 et le lemme 2.5.6, on obtient

$$\left(\frac{-1}{n}\right) = \prod_{p|n} \left(\frac{-1}{p}\right)^{e_p} = (-1)^{\sum_{p|n} e_p \psi(p)} = (-1)^{\psi(n)}.$$

□

Théorème 2.5.8 — *Étant donnés deux entiers naturels impairs n et m, on a l'identité*

$$\left(\frac{m}{n}\right) = (-1)^{\frac{n-1}{2}\frac{m-1}{2}} \left(\frac{n}{m}\right).$$

Démonstration — L'assertion étant trivialement vérifiée si n et m ne sont pas premiers entre eux, supposons que $(n,m)=1$. Pour tout entier impair r, posons une fois de plus $\psi(r) = \frac{r-1}{2}$. On procède comme dans la démonstration du corollaire 2.5.7 : en posant $n = \prod_i p_i^{a_i}$ et $m = \prod_i q_i^{b_i}$, la loi de réciprocité quadratique pour le symbole de Legendre amène aux identités

$$\left(\frac{m}{n}\right) = \prod_{i,j}\left(\frac{q_i}{p_j}\right)^{a_i b_j} = \prod_{i,j}(-1)^{a_i b_j \psi(p_i)\psi(q_j)}\left(\frac{p_i}{q_j}\right)^{a_i b_j} = (-1)^{\sum_{i,j} a_i b_j \psi(p_i)\psi(q_j)}\left(\frac{n}{m}\right).$$

Finalement, en appliquant le lemme 2.5.6, on obtient les congruences

$$\sum_{i,j} a_i b_j \psi(p_i)\psi(q_j) \equiv \sum_i a_i \psi(p_i) \sum_j b_j \psi(q_j) \equiv \sum_i a_i \psi(p_i)\psi(m) \equiv$$
$$\equiv \psi(n)\psi(m) \pmod 2.$$

□

Exercice 2.5.9 — Montrer que pour tout entier impair n, l'entier n^2-1 est divisible par 8.

Proposition 2.5.10 — *Pour tout entier impair $n \geq 3$, on a l'identité*

$$\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}.$$

En d'autres termes, on a $(\frac{2}{n}) = 1$ si et seulement si n est congru à ± 1 modulo 8.

Démonstration — On procède par récurrence sur l'entier n : pour $n=3$, on a les identités

$$\left(\frac{2}{3}\right) = -1 = (-1)^{\frac{3^2-1}{8}}.$$

Soit donc $n > 3$ un entier impair et supposons la propriété vérifiée pour $n-2$. On a alors les relations

$$\left(\frac{2}{n}\right) = \left(\frac{-1}{n}\right)\left(\frac{-2}{n}\right) = (-1)^{\frac{n-1}{2}}\left(\frac{n-2}{n}\right) = (-1)^{\frac{n-1}{2}}\left(\frac{n}{n-2}\right) =$$
$$= (-1)^{\frac{n-1}{2}}\left(\frac{2}{n-2}\right) = (-1)^{\frac{n-1}{2}}(-1)^{\frac{(n-2)^2-1}{8}} = (-1)^{\frac{4n-4+(n-2)^2-1}{8}} = (-1)^{\frac{n^2-1}{8}},$$

ce qui permet de conclure. La dernière assertion est juste une vérification directe (on remarquera que la parité de $(n^2-1)/8$ ne dépend que de la classe de n modulo 8). □

2.5.3. Calcul explicite du symbole de Jacobi — Soient n et m deux entiers impairs, avec $1 < n < m$. Nous terminons cette section en décrivant un algorithme efficace de calcul du symbole de Jacobi $(\frac{m}{n})$ ne nécessitant pas la connaissance de la factorisation de n. Cette méthode repose essentiellement sur la loi de réciprocité quadratique pour le symbole de Jacobi et sur une version modifiée de l'algorithme d'Euclide étendu.

- Pour $m = 1$, on obtient $(\frac{m}{n}) = 1$ et l'algorithme s'arrête.
- Pour $m > 1$, la loi de réciprocité quadratique amène à l'identité $(\frac{m}{n}) = \pm(\frac{n}{m})$, le signe ne dépendant que de la classe de n et m modulo 4.
- En considérant la division euclidienne modifiée $n = mq + r$, avec $|r| < m/2$, on obtient la relation $(\frac{n}{m}) = \left(\frac{r}{m}\right)$.
- Pour $r = 0$, on obtient les identités

$$\left(\frac{m}{n}\right) = \pm\left(\frac{r}{m}\right) = 0$$

  et l'algorithme s'arrête.
- Sinon, l'entier r possède une écriture unique du type $r = \pm 2^a b$, avec $b > 0$ impair. Par construction, on a l'inégalité $b < m/2$ et les identités

$$\left(\frac{r}{m}\right) = \left(\frac{\pm 1}{m}\right)\left(\frac{2}{m}\right)^a\left(\frac{b}{m}\right).$$

  La détermination de $(\frac{-1}{m})$ ne dépend que de la classe de m modulo 4. De même, $(\frac{2}{m})$ ne dépend que de la classe de m modulo 8. De plus, l'entier $(\frac{2}{m})^a$ est égal à $(\frac{2}{m})$ si a est impair et à 1 sinon.
- On répète le procédé en remplaçant $(\frac{m}{n})$ par $(\frac{b}{m})$.

Chaque étape de l'algorithme est de complexité polynomiale par rapport à la taille des entiers considérés. De manière plus précise, l'opération la plus coûteuse (en temps) est la division eucllidienne modifiée de n par m (cf. le troisième point ci-dessus), qui est de complexité $O(\log^2(n))$. La factorisation de r se réduit à une suite de décalages sur la droite et ne pose pas de problème. Finalement, ayant utilisé la division euclidienne modifiée, le nombre de boucles nécessaires pour que l'algorithme aboutisse est majoré par $\log_2(n)$. On en déduit que cette méthode de calcul du symbole de Jacobi est de complexité globale $O(\log^2(n))$ améliorant ainsi l'algorithme de calcul du symbole de Legendre découlant du théorème 2.3.2 (qui était de complexité $O(\log^3(n))$.

Exemple 2.5.11 — Calculons le symbole de Jacobi $(\frac{43}{143})$ de deux manières différentes :

- Tout d'abord en considérant la factorisation $143 = 11{\cdot}13$, on obtient les identités

$$\left(\frac{43}{143}\right) = \left(\frac{43}{11}\right)\left(\frac{43}{13}\right) = \left(\frac{-1}{11}\right)\left(\frac{4}{13}\right) = -1.$$

- Sans avoir recours à la factorisation de 143, la loi de réciprocité quadratique pour le symbole de Jacobi amène aux relations

$$\left(\frac{43}{143}\right) = -\left(\frac{143}{43}\right) = -\left(\frac{14}{43}\right) = -\left(\frac{2}{43}\right)\left(\frac{7}{43}\right) = -\left(\frac{43}{7}\right) =$$
$$= -\left(\frac{1}{7}\right) = -1.$$

CHAPITRE 3

CORPS FINIS ET LOGARITHME DISCRET

3.1. Rappels sur les polynômes à coefficients dans un corps

3.1.1. Structure d'anneau euclidien et propriétés arithmétiques — Dans ce paragraphe, on fixe un corps K et on rappelle brièvement les propriétés de l'anneau de polynômes $K[X]$. Comme pour les entiers, la plupart de ses propriétés algébriques et arithmétiques découle de l'existence d'une division euclidienne.

Lemme 3.1.1 — *Étant donnés deux polynômes $f, g \in K[X]$, avec $f \neq 0$, il existe un unique couple de polynômes $q, r \in K[X]$ tels que $g = fq + r$, avec $r = 0$ ou* $\deg(r) < \deg(f)$.

Démonstration — Posons $d = \deg(f)$. On montre d'abord l'existence des polynômes q et r. On, procède par récurrence sur le degré n de g. Pour $n < d$, il suffit de poser $q = 0$ et $r = g$. Soit donc $g \in K[X]$ un polynôme de degré $n \geq d$ et supposons la propriété vérifiée pour tout polynôme de degré strictement inférieur à n. Notons $a, b \neq 0$ les coefficients dominants respectifs de f et g. Le polynôme

$$h = g - ba^{-1}X^{n-d}f$$

est de degré strictement inférieur à n. Par hypothèse de récurrence, il existe un couple de polynômes $u, r \in K[X]$ tels que $h = fu + r$, avec $r = 0$ ou $\deg(r) < d$. En posant $q = u + ba^{-1}X^{n-d}$, on obtient alors la relation $g = fq + r$. Concernant l'unicité, l'identité $qf + r = 0$ se traduit par $qf = r$. Si r est non nul, q est également non nul, ce qui amène aux relations

$$\deg(f) \leq \deg(f) + \deg(q) = \deg(qf) = \deg(-r) < \deg(f),$$

ce qui est exclu. On a donc $r = 0$ et, par suite, $q = 0$ (car l'anneau $K[X]$ est intègre). □

Théorème 3.1.2 — *L'anneau $K[X]$ est principal.*

Démonstration — On procède exactement comme pour le théorème 1.1.4, en montrant qu'un idéal non nul de $K[X]$ est engendré par un de ses éléments de degré minimal. □

On rappelle qu'un polynôme $f \in K[X]$ est ***unitaire*** si son coefficient dominant est égal à 1.

Proposition 3.1.3 — *Un idéal non nul de $K[X]$ possède un un unique générateur unitaire. En particulier, il existe une bijection entre l'ensemble des idéaux non nuls de $K[X]$ et l'ensemble des polynômes unitaires de $K[X]$.*

Démonstration — L'anneau $K[X]$ étant principal, c'est une conséquence directe de l'identité $K[X]^\times = K^\times$ et du lemme 1.1.3. □

Toutes les constructions arithmétiques présentées pour $\mathbb{Z}$ dans le premier chapitre se transposent naturellement dans le contexte des anneaux de polynômes. Par exemple, le pgcd de deux polynômes non nuls $f, g \in K[X]$ est l'unique générauteur unitaire $f \wedge g$ de l'idéal $fK[X] + gK[X]$ et l'on dispose d'une identité de Bézout

$$f \wedge g = uf + vg,$$

avec $u, v \in K[X]$. Les polynômes f et g sont premiers entre eux si $f \wedge g = 1$. Dans ce cas, on peut appliquer le lemme de Gauss (cf. l'exercice 1.1.12). Le résultat ci-dessous est l'analogue de la proposition 1.1.8 ; sa démonstration étant essentiellement identique, elle est omise.

Proposition 3.1.4 — *Étant donné un polynôme non nul $f \in K[X]$, il existe une bijection naturelle entre l'ensemble des idéaux de $K[X]$ contenant $fK[X]$ et l'ensemble des diviseurs unitaires de f.*

De manière générale, un élément a d'un anneau A est ***irréductible*** s'il est non nul, non inversible et si ses diviseurs sont tous du type u ou ua, avec $u \in A^\times$. En d'autres termes un élément $b \in A$ divise a si et seulement s'il est inversible ou associé à a. Si l'anneau A est principal, ceci revient à affirmer que l'idéal aA est maximal, ou encore que l'anneau A/aA est un corps.

Exemple 3.1.5 — Un polynôme $f \in K[X]$ est irréductible si et seulement s'il est non constant et ne se réalise pas comme produit de deux polynômes non constants, ou, ce qui revient au même, si tout polynôme non nul de degré strictement inférieur à $\deg(f)$ est premier avec f (cette dernière caractérisation est l'analogue de la définition de nombre premier donnée dans le chapitre 1).

Théorème 3.1.6 — *Un polynôme non nul $f \in K[X]$ s'écrit de manière unique comme produit*

$$f = u \prod_p p^{e_p},$$

où p parcourt l'ensemble des polynômes unitaires irréductibles de $K[X]$, les entiers naturels e_p étant presque tous nuls (i.e. tous sauf un nombre fini d'entre eux) et $u \in K^\times$.

Démonstration — On adopte la même démarche que pour le théorème 1.1.17, en procédant par récurrence sur le degré de f. □

3.1.2. Racines et divisibilité — Un élément $x \in K$ est une ***racine*** d'un polynôme $f \in K[X]$ si $f(x) = 0$.

Lemme 3.1.7 — *Un élément $x \in K$ est une racine d'un polynôme $f \in K[X]$ si et seulement si $X - x$ divise f dans $K[X]$.*

Démonstration — Le polynôme $X - x$ étant non nul, considérons la division euclidienne

$$f = (X - x)q + r,$$

avec $\deg(r) < \deg(X - x) = 1$. Le polynôme r est constant, d'où l'identité $f(x) = r$. On a donc la relation $f(x) = 0$ si et seulement si $r = 0$, ce qui revient à affirmer que $X - x$ divise f. □

Proposition 3.1.8 — *Un polynôme non nul $f \in K[X]$ de degré n possède au plus n racines dans K.*

Démonstration — On procède par récurrence sur l'entier n. L'assertion étant claire pour $n = 0$, considérons un polynôme $f \in K[X]$ de degré $n > 0$ et supposons la propriété vérifiée pour tout polynôme non nul de degré strictement inférieur. Si f ne possède pas de racine dans K, l'affirmation est trivialement vérifiée. Sinon, ayant fixé $x \in K$ tel que $f(x) = 0$, d'après le lemme précédent, on a la factorisation $f = (X-x)g$, avec $g \in K[X]$ de degré $n - 1$. Par hypothèse de récurrence, g possède au plus $n - 1$ racines dans K, d'où le résultat. □

Remarque 3.1.9 — Ce résultat est en fait valable dans un quelconque anneau intègre, mais il est faux en général. Par exemple, le polynôme $2X$ possède les racines 0 et 2 dans $\mathbb{Z}/4\mathbb{Z}$. De même, les éléments $0, 1, 3$ et 4 de $\mathbb{Z}/6\mathbb{Z}$ sont des racines du polynôme $X^2 - X$.

La ***multiplicité*** d'une racine x d'un polynôme $f \in K[X]$ est le plus grand entier naturel e tel que $(X - x)^e$ divise f. Une racine de f est ***simple*** si sa multiplicité vaut 1.

3.1.3. Séparabilité, le polynôme dérivé — Soit K un corps. Le ***polynôme dérivé*** $f' \in K[X]$ d'un polynôme $f = \sum_n a_n X^n \in K[X]$ est défini de manière formelle par la relation

$$f' = \sum_n n a_n X^{n-1}.$$

On a alors l'identité $(f+g)' = f' + g'$ et on vérifie facilement la ***formule de Leibnitz***

$$(fg)' = f'g + fg'.$$

En général, on a l'inégalité $\deg(f') \leq \deg(f) - 1$, qui peut être stricte. Un polynôme $f \in K[X]$ est ***séparable*** si f et f' sont premiers entre eux.

Lemme 3.1.10 — *Soit $f \in K[X]$ un polynôme séparable. Tout diviseur non constant de f est séparable. En particulier, toutes les racines de f sont simples.*

Démonstration — Soit g un diviseur de f. Si g n'est pas séparable, il existe un polynôme non constant $h \in K[X]$ divisant g et g'. En posant $f = gu$, on en déduit que h divise f et $f' = g'u + u'g$, ce qui est absurde. Remarquons maintenant que pour tout $g \in K[X]$, le polynôme g^2 n'est pas séparable, car g divise son polynôme dérivé. En particulier, si x est une racine de f, alors $(X-x)^2$ ne divise pas f. □

Exercice 3.1.11 — Considérons deux polynômes $f, g \in K[X]$. Montrer que le produit fg est séparable si et seulement si f et g sont séparables et premiers entre eux.

3.2. Extensions de corps

3.2.1. Extensions de corps — De manière générale, une ***extension*** d'un corps K est la donnée d'un corps L et d'un homomorphisme d'anneaux (nécessairement injectif) $\iota : K \to L$, ce qui revient à munir L d'une structure de K-algèbre. Le plus souvent, K est un sous-corps de L, l'homomorphisme $\iota : K \to L$ n'étant autre que l'inclusion. Quitte à remplacer K par son image par ι, il est d'ailleurs toujours possible de se réduire à cette situation. On utilise la notation L/K pour indiquer une extension L de K. Étant données deux extensions L/K et F/L, on peut considérer l'***extension composée***, F/K.

Étant donnée une extension de corps L/K, Le corps L est muni d'une structure canonique de K-espace vectoriel. Sa dimension (pas nécessairement finie), est appelée ***degré*** de l'extension ; on la note $[L : K]$. L'extension est ***finie*** lorsque son degré est fini.

3.2.2. Construction explicite d'extensions finies — Le résultat ci-dessous est l'un des ingrédient principaux dans l'étude ainsi que dans la construction effective d'extensions finies de corps. Il illustre par ailleurs l'importance des anneaux des polynômes dans la théorie des corps.

Proposition 3.2.1 — *Soient K un corps et $f \in K[X]$ un polynôme irréductible de degré n. On a alors les propriétés suivantes :*

1. *L'anneau*
$$K_f = K[X]/fK[X]$$
est un corps.
2. *On a un homomorphisme canonique d'anneaux $K \to K_f$.*
3. *L'extension K_f/K est finie, de degré n. De manière plus précise, si $x \in K_f$ désigne la classe de X, alors les éléments $1, x, \dots, x^{n-1}$ forment une base du K-espace vectoriel K_f.*
4. *L'élément $x \in K_f$ est une racine de f.*

Démonstration — Le polynôme f étant irréductible, l'idéal $fK[X]$ est maximal (cf. le paragraphe 3.1.1) et l'anneau K_f est donc un corps. On a un homomorphisme naturel $K \to K_f$, obtenu en composant l'homomorphisme canonique $K \to K[X]$ avec la projection $K[X] \to K_f$ qui associe à g sa classe $\bar{g} = g + fK[X]$ modulo f. On a alors les identités
$$f(x) = f(\bar{X}) = \overline{f(X)} = 0,$$
ce qui implique que x est une racine de f. Finalement, étan donné $y \in K_f$, on a $y = \bar{g}$, avec $g \in K[X]$. En considérant la division euclidienne $g = fq + r$, avec $\deg(r) < n$, on obtient les identités
$$y = \bar{g} = \bar{r} = \overline{a_0 + a_1 X + \cdots + a_{n-1}X^{n-1}} = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1},$$
avec $a_0, \dots, a_{n-1} \in K$, ce qui implique que les éléments $1, \dots, x^{n-1}$ forment une famille génératrice du K-espace vectoriel K_f. De plus, étant donnée une relation de dépendance linéaire
$$a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} = 0,$$
dans K_f, avec $a_0, \dots, a_{n-1} \in K$, en posant
$$r = a_0 + a_1 X + \cdots + a_{n-1}X^{n-1} \in K[X],$$
on obtient $\bar{r} = 0$ dans K_f, ou encore $f|r$ dans $K[X]$, ce qui donne $r = 0$ (en comparant les degrés), d'où $a_1 = \cdots = a_{n-1} = 0$. Les éléments $1, x, \dots, x^{n-1}$ forment donc une base du K-espace vectoriel K_f. □

Corollaire 3.2.2 — *Soient K un corps et $f \in K[X]$ un polynôme non constant. Il existe une extension finie L/K dans laquelle f possède une racine.*

Démonstration — En fixant un diviseur irréductible g de f, le corps K_g de la proposition 3.2.1 est une extension finie de K et le polynôme g possède une racine dans K_g, celle-ci étant également une racine de f. □

3.2.3. Éléments algébriques, polynôme minimal — Considérons une extension de corps K/L. Comme d'habitude, on se réduit au cas où K est un sous-corps de L. Étant donné un élément $x \in L$, on dispose d'un homomorphisme d'évaluation

$$K[X] \xrightarrow{\phi_x} L$$

qui associe à un polynôme f sa valeur $f(x)$ en x. Son image, notée $K(x)$ est le plus petit sous-anneau de L contenant K et x ou, si l'on préfère, la plus petite sous-K-algèbre de L contenant x (cette dernière définition étant plus correcte dans le contexte général). Le noyau de l'homomorphisme ϕ_f est l'***idéal annulateur*** de x sur K. On le note généralement $\mathrm{Ann}_K(x)$. Si ce dernier est non nul, ce qui revient à affirmer qu'il existe un polynôme non constant $f \in K[X]$ tel que $f(x) = 0$, l'élément x est ***algébrique*** sur K. Dans ce cas l'idéal $\mathrm{Ann}_K(x)$ est engendré par un unique polynôme unitaire $f \in K[X]$, appelé ***polynôme minimal*** de x sur K. Un élément de L qui n'est pas algébrique sur K est ***transcendant*** sur K.

Exemple 3.2.3 — Tout élément x d'un corps K est algébrique sur K, car racine du polynôme $X - x \in K[X]$, qui est d'ailleurs son polynôme minimal sur K.

Une extension de corps L/K est ***algébrique*** si tout élément de L est algébrique sur K.

Proposition 3.2.4 — *Toute extension finie de corps est algébrique.*

Démonstration — Soit L/K une extension finie de corps. Pour tout $x \in L$, l'homomorphisme d'évaluation $\phi_x : K[X] \to L$ est une application K-linéaire. Le K-espace vectoriel $K[X]$ étant de dimension infinie, $\ker(\phi_x) = \mathrm{Ann}_K(x)$ ne peut être nul (sinon ϕ_x serait injectif). □

Exercice 3.2.5 — Montrer que tout idéal premier non nul d'un anneau principal est maximal.

Le résultat suivant décrit l'anneau $K(x)$ lorsque l'élément $x \in L$ est algébrique sur K.

Proposition 3.2.6 — *Soit K/L une extension de corps. Pour tout élément $x \in L$ algébrique sur K, on a les propriétés suivantes :*

1. *Le polynôme minimal f de x sur K est irréductible dans $K[X]$.*
2. *L'anneau $K(x)$ est un corps.*
3. *L'extension $K(x)/K$ est finie, de degré $n = \deg(f)$.*
4. *Les éléments $1, \ldots, x^{n-1}$ forment une base du K-espace vectoriel $K(x)$.*

Démonstration — L'anneau $K(x)$, qui est isomorphe à $K_f = K[X]/fK[X]$, est intègre, car sous-anneau de L (qui est un corps, donc intègre). On en déduit que $fK[X]$

est un idéal premier et non nul (car x est algébrique sur K), donc maximal (cf. l'exercice ci-dessus), ce qui est équivalent à l'irréductibilité de f dans $K[X]$. Il suffit alors d'appliquer la proposition 3.2.1. □

Une extension algébrique de corps L/K est ***simple*** s'il existe un élément $x \in L$ tel que $L = K(x)$. On dit alors que x est un ***élément primitif***. Dans ce cas, d'après le résultat ci-dessus L est nécessairement une extension finie de K, mais la réciproque n'est généralement pas vraie (nous verrons qu'elle est néanmoins valable pour les corps finis). D'un point de vue pratique, lorsqu'une extension L/K est simple, le corps $L = K(x)$ est isomorphe au quotient $K_f = K[X]/fK[X]$, où f est le polynôme minimal de x sur K et l'on dispose par ailleurs d'une base canonique dur K-espace vectoriel L (une fois que l'on a fixé l'élément primitif x). Ceci représente un avantage majeur, que ce soit d'un point de vue théorique (car on obtient une description explicite du corps L comme quotient d'un anneau de polynômes) ou effectif (les opérations algébriques dans L se réduisant à des opérations algébriques avec de polynômes dans K de degré strictement inférieur à $\deg(f)$).

3.3. Corps finis

3.3.1. Caractéristique, sous-corps premier — Étant donné un anneau A, il existe un unique homomorphisme d'anneaux $\mathbb{Z} \to A$. Son noyau est engendré par un unique entier natuel c, appelé ***caractéristique*** de A, et son image, qui est isomorphe à $\mathbb{Z}/c\mathbb{Z}$, est le plus petit sous-anneau de A. Si A est fini, on a nécessairement $c > 0$. Si, de plus, A est inègre, alors c est un nombre premier.

Exercice 3.3.1 — Montrer qu'un anneau fini et intègre est un corps. En déduire qu'un sous-anneau d'un corps fini est un corps fini.

D'après ce qui précède, si K est un corps fini, sa caractéristique est un nombre premier p et l'on obtient un homomorphisme canonique $\mathbb{F}_p \to K$. On identifiera toujours $\mathbb{F}_p$ à son image dans K, qui est le plus petit sous-corps de K (ou sous-anneau, cf. l'exercice ci-dessus), appele ***sous-corps premier*** de K.

3.3.2. Cardinal et degré — Dans ce paragraphe, nous allons voir que dans le cas des extensions corps fini, le cardinal et le degré sont étroitement liés. ce qui découle de considérations et de résultats de base d'algèbre linéaire (comme par exemple l'existence d'une base pour un espace vectoriel de dimension finie).

Proposition 3.3.2 — *Soit L/K une extension de corps finis de degré n. Si q et q' désignent les cardinaux respectifs de K et L, on a l'identité $q' = q^n$.*

Démonstration — En fixant une base, le K-espace vectoriel L s'identifie avec K^n, qui est de cardinal q^n. □

Corollaire 3.3.3 — *Étant donné un corps fini K de caractéristique p et cardinal q, on a l'identité $q = p^n$, avec $n = [K : \mathbb{F}_p]$.*

Démonstration — C'est un cas particulier du résultat précédent, en considérant l'extension $K/\mathbb{F}_p$. □

Bien que le résultat ci-dessous soit valable en toute généralité, nous ne l'énonçons que pour les coprs finis, sa démonstration étant particulièrement simple dans ce contexte.

Corollaire 3.3.4 — *Étant donnés deux extensions L/K et F/L de corps finis, l'extension composée F/K est finie et on a l'identité $[F : K] = [F : L][L : K]$.*

Démonstration — Une fois encore, le corps F étant fini, l'entier $[F : K]$ est nécessairement fini. Notons q, q' et q'' les cardinaux repectifs de K, L et F. D'après la proposition 3.3.2, on a alors les identités

$$q^{[F:K]} = q'' = q'^{[F:L]} = \left(q^{[L:K]}\right)^{[F:L]} = q^{[F:L][L:K]}.$$

□

3.3.3. Le groupe multiplicatif d'un corps fini — Étant donné un groupe fini G, l'ensemble

$$\mathfrak{e} = \{n \in \mathbb{Z} \mid g^n = 1 \ \forall g \in G\}$$

est un idéal de $\mathbb{Z}$. Il existe donc un unique entier naturel e, appelé ***exposant*** de G tel que $\mathfrak{e} = e\mathbb{Z}$. On vérifie facilement que e est le ppcm des ordres des éléments de G et le théorème de Lagrange affirme qu'il divise l'ordre de G.

Exercice 3.3.5 — Soient G un groupe et $g \in G$ un élément d'ordre fini n. Montrer que pour tout entier m, l'élément g^n est d'ordre $n/(m, n)$.

Lemme 3.3.6 — *Étant donné un groupe abélien fini G d'exposant e, il existe un élément de G d'ordre e.*

Démonstration — Il suffit de montrer qu'étánt donnés deux éléments $g, h \in G$ d'ordres respectifs n et m, il existe un élément de G d'ordre $[n, m]$. Commençons par remarquer que pour $(n, m) = 1$, l'élément xy est d'ordre nm. En effet, on a $(xy)^{nm} = 1$, ce qui implique que l'ordre d de xy divise nm. Par ailleurs, l'identité $(xy)^d = 1$ amène à $x^{dm} = 1$, ce qui implique qye n divise dm et le lemme de Gauss permet d'affirmer que n divise d. Ce même résultat implique alors que nm divise d, d'où l'égalité $d = nm$. Dans le cas général, considérons les factorisations $n = \prod_p p^{e_p}$

et $m = \prod_p p^{f_p}$. Pour tout nombre premier p, considérons les entiers a_p définis par

$$a_p = \begin{cases} e_p & \text{si } e_p \geq f_p, \\ \\ 0 & \text{sinon,} \end{cases} \qquad b_p = \begin{cases} 0 & \text{si } e_p \geq f_p, \\ \\ f_p & \text{sinon.} \end{cases}$$

En posant $n' = \prod_p p^{a_p}$ et $m' = \prod_p p^{b_p}$ on a alors $n'|n, m'|m, (n', m') = 1$ et $n'm' = [n, m]$. En particulier, les éléments $x' = x^{n/n'}$ et $y' = y^{m/m'}$ sont d'ordre n' et m' et, d'après ce qui précède, l'élément $x'y'$ est d'ordre $[n, m]$. □

Corollaire 3.3.7 — *Un groupe abélien fini est cyclique si et seulement si son exposant coïncide avec son ordre.*

Démonstration — Soit G un groupe abélien fini d'ordre n et exposant e. Si G est cyclique, il existe un élément d'ordre n, d'où $n|e$, puis $n = e$ (car e divise n). Si $e = n$, le lemme précédent affirme que G possède un élément d'ordre n et le sous-groupe qu'il engendre coïncide avec G (car ils ont même ordre). □

Théorème 3.3.8 — *Tout sous-groupe fini du groupe multiplicatif d'un corps est cyclique.*

Démonstration — Soient K un corps et G un sous-groupe fini de $K^\times$ d'ordre n et exposant e. Les éléments de G sont racines du polynôme $X^e - 1 \in K[X]$, d'où l'inégalité $n \leq e$ (cf. la proposition 3.1.8), qui est donc une égalité (car e divise n). Il suffit alors d'appliquer le dernier corollaire. □

Corollaire 3.3.9 — *Le groupe multiplicatif d'un corps fini est cyclique.*

Démonstration — C'est une conséquence immédiate du théorème ci-dessus. □

Corollaire 3.3.10 — *Soit K un corps fini de cardinal q. Le groupe $K^\times$ possède un élément d'ordre d si et seulement si d divise $q - 1$.*

Démonstration — Le groupe $K^\times$ étant d'ordre $q - 1$, une des implications est une conséquence du théorème de Lagrange. Récirpoquement, si d divise $q - 1$, le corollaire 3.3.9 affirme que $K^\times$ est cyclique et, en fixant un de ses générateurs x, l'élément $x^{(q-1)/d}$ est d'ordre d. □

Le résultat ci-dessous est un cas particulier du célèbre ***théorème de l'élément primitif***. Pour les corps finis, sa démonstration est particulièrement simple et découle de la cyclicité de leur groupe multiplicatif.

Théorème 3.3.11 — *Soit K un sous-corps d'un corps fini L. Il existe alors un élément $x \in L$ tel que $L = K(x)$.*

Démonstration — D'après le corollaire 3.3.9, le groupe $L^\times$ est cyclique. En fixant un de ses générateurs x, on en déduit que pour tout entier naturel n, l'élément x^n appartient à $K(x)$, d'où l'inclusion $L^\times \subset K(x)$. On a de plus $0 \in K(x)$, ce qui donne finalement l'inclusion $L = L^\times \cup \{0\} \subset K(x)$, qui est alors une égalité. □

3.3.4. L'automorphisme de Frobenius — Nous allons commencer ce paragraphe par un résultat général.

Lemme 3.3.12 — *Soient p un nombre premier et A un anneau de caractéristique p. Étant donnés $x, y \in A$, on a l'identité*

$$(x+y)^p = x^p + y^p.$$

Démonstration — Pour tout entier $n \in \{1, \dots, p-1\}$, le coefficient binomial $\binom{p}{n}$ est divisible par p, ce qui donne l'identité $\binom{p}{n} = 0$ dans A et, par suite, les relations

$$(x+y)^p = \sum_{n=0}^{p} \binom{p}{n} x^n y^{p-n} = x^p + y^p.$$

□

Si K est un corps fini de caractéristique p, le lemme ci-dessus implique que l'application $\mathrm{Fr} : K \to K$ définie par $\mathrm{Fr}(x) = x^p$ est un homomomorphisme d'anneaux, nécessairement injectif, donc bijectif. En d'autre termes, Fr est un automorphisme de K, appelé ***automorphisme de Frobenius***. De manière plus générale, si L/K est une extension de corps finis de caractérstique p, en notant $q = p^n$ le cardinal de K, l'application $\mathrm{Fr}_K : L \to L$ définie par

$$\mathrm{Fr}_K(x) = x^q = \mathrm{Fr}^n(x)$$

est un automorphisme de corps. Avec cette définition, on a donc $\mathrm{Fr}_{\mathbb{F}_p} = \mathrm{Fr}$. On remarquera que la définition de Fr_K ne dépend que du cardinal de K. Le résultat suivant est fondamental dans la théorie des corps finis.

Proposition 3.3.13 — *Soit K un corps fini de cardinal q. Dans $K[X]$, on a l'identité*

$$X^q - X = \prod_{x \in K} (X - x).$$

Démonstration — Soit x un élément de K. Pour $x = 0$, on a clairement la relation $x^q = x$. Si x est non nul, il appartient à $K^\times$, qui est d'ordre $q-1$. Le lemme 2.1.15 amène alors à l'identité $x^{q-1} = 1$, d'où la relation $x^q = x$. Tout élément de K est donc racine du polynôme $f = X^q - X$. Le polynôme $f - \prod_{x \in K}(X - x)$ étant de degré strictement inférieur à q et possèdant q racines, la proposition 3.1.8 affirme qu'il est nul. □

Corollaire 3.3.14 — *Soit K un sous-corps d'un corps fini L. Pour tout $x \in L$, on a $x \in K$ si et seulement si $\mathrm{Fr}_K(x) = x$.*

Démonstration — Notons q le cardinal de K. L'identité de la proposition 3.3.13 est valable dans $L[X]$. Pour tout $x \in L$, on a $\mathrm{Fr}_K(x) = x$ si et seulement si x est racine du polynôme $X^q - X$, ce qui se traduit par $x \in K$. □

Étant donné $x \in L$, les éléments $x, \mathrm{Fr}_K(x), \mathrm{Fr}_K^2(x), \ldots$ sont les ***conjugués*** de x sur K.

Proposition 3.3.15 — *Soit K un sous-corps d'un corps fini L. Étant donné un élément $x \in L$, en notant S l'ensemble de ses conjugués sur K, le polynôme*

$$f = \prod_{y \in S} (X - y) \in L[X]$$

appartient à $K[X]$ et est le polynôme minimal de x sur K.

Démonstration — En posant

$$\mathrm{Fr}_K(a_0 + a_1 X + \cdots + a_n X^n) = \mathrm{Fr}_K(a_0) + \mathrm{Fr}_K(a_1) X + \cdots + \mathrm{Fr}_K(a_n) X^n,$$

on étend Fr_K en un automorphisme de l'anneau $L[X]$. D'après le corollaire 3.3.14, pour tout $g \in L[X]$, on a $\mathrm{Fr}_K(g) = g$ si et seulement si $f \in K[X]$. L'automorphisme Fr_K permutant les éléments de S, on a $\mathrm{Fr}_K(f) = f$, d'où $f \in K[X]$. Notons $g \in K[X]$ le polynôme minimal de x sur K. Dans ce cas, pour tout $y \in S$, on a $g(y) = 0$, ou encore $(X - y) | g$ dans $L[X]$. Le lemme de Gauss implique alors que f divise g dans $L[X]$. Par ailleurs, on a $f(x) = 0$, d'où $f \in \mathrm{Ann}_K(x)$ et, par suite, $g | f$ dans $K[X]$, ce qui implique que g divise f dans $L[X]$. Les polynômes f et g sont donc associés. Étant tous deux unitaires, ils coïncident. □

Soit K un sous-corps d'un corps fini L. L'ensemble $\mathrm{Aut}(L)$ des automorphismes de corps de L est muni d'une structure naturelle de groupe (par rapport à la composition). Dans ce cas, l'ensemble

$$\mathrm{Gal}(L/K) = \{\sigma \in \mathrm{Aut}(L) \mid \sigma(x) = x \ \forall\, x \in K\}$$

est un sous-groupe de $\mathrm{Aut}(L)$ appelé ***groupe de Galois*** de l'extension L/K. D'après le corollaire 3.3.14, on a $\mathrm{Fr}_K \in \mathrm{Gal}(L/K)$.

Remarque 3.3.16 — Pour tout corps fini K de caractéristique p, on a l'identité $\mathrm{Aut}(K) = \mathrm{Gal}(K/\mathbb{F}_p)$. En d'autres termes, pour tout $\sigma \in \mathrm{Aut}(K)$ et tout $x \in \mathbb{F}_p$, on a $\sigma(x) = x$, ce qui découle de l'identité $\sigma(1) = 1$, qui amène aux relations $\sigma(\bar{n}) = \bar{n}$ pour tout $n \in \mathbb{Z}$ (ici $\bar{n}$ désigne la classe de n modulo p).

Théorème 3.3.17 — *Soit K un sous-corps d'un corps fini L. Le groupe* $\mathrm{Gal}(L/K)$ *est cyclique, d'ordre $[L : K]$, engendré par* Fr_K.

Démonstration — Soit x un générateur du groupe $L^\times$ et notons $f \in K[X]$ son polynôme minimal sur K. Étant donné $\sigma \in \mathrm{Gal}(L/K)$, on a alors les identités

$$f(\sigma(x)) = \sigma(f(x)) = \sigma(0) = 0,$$

ce qui implique que $\sigma(x)$ est une racine de f. D'après la proposition 3.3.15, il existe alors un entier naturel m tel que $\sigma(x) = \mathrm{Fr}_K^m(x)$. L'élément x étant un générateur de $L^\times$, on a alors $\sigma(y) = \mathrm{Fr}_K^m(y)$ pour tout $y \in L^\times$ et cette identité est donc vraie pour tout $y \in L$, d'où $\sigma = \mathrm{Fr}_K^m$, ce qui montre que le groupe $\mathrm{Gal}(L/K)$ est engendré par Fr_K. Finalement, en posant $n = [L : K]$, la proposition 3.3.13 se traduit par l'identité $\mathrm{Fr}_K^n(y) = \mathrm{Fr}_K(y)$ pour tout $y \in L$, d'où $\mathrm{Fr}_K^n = 1$, ce qui implique que l'ordre d de Fr_K dans $\mathrm{Gal}(L/K)$ divise n. Par ailleurs l'identité $\mathrm{Fr}_K^d(y) = y$, valable pour tout $y \in L$, implique les éléments de L sont racines du polynôme $X^{q^d} - X$, d'où $q^d \geq q^n$, ce qui amène à l'inégalité $d \geq n$, qui est alors une égalité (car d divise n). □

Corollaire 3.3.18 — *Pour tout corps fini K de caractéristique p et cardinal p^n, le groupe $\mathrm{Aut}(K)$ est cyclique, d'ordre n, engendré par l'automorphisme de Frobenius.*

Démonstration — Compte tenu de l'identité $\mathrm{Aut}(K) = \mathrm{Gal}(K/\mathbb{F}_p)$ (cf. la remarque ci-dessus), c'est un cas particulier du théorème 3.3.17. □

3.3.5. Existence et unicité — Soit K un corps (pas nécessairement fini). Un polynôme non constant $f \in K[X]$ est ***scindé*** si tous ses facteurs irréductibles sont de degré 1, ce qui revient à affirmer que toutes ses racines appartiennent à K. La proposition 3.3.13 affirme que si K est un corps fini de cardinal q, le polynôme $X^q - X$ est scindé dans $K[X]$ et même que c'est le produit des polynômes irréductibles unitaires de degré 1 de $K[X]$.

Lemme 3.3.19 — *Soient K un corps et $f \in K[X]$ un polynôme non constant. Il existe une extension L/K dans laquelle f est scindé.*

Démonstration — On procède par récurrence sur le degré $n \geq 1$ de f. L'assertion étant immédiate pour $n = 1$ (auquel cas, f est irréductible), soit $n > 1$ un entier et supposons la propriété vérifiée pout tout corps F et tout polynôme $g \in F[X]$ de degré strictement inférieur à n. Fixons un corps K et un polynôme $f \in K[X]$ de degré n. Daprès le corollaire 3.2.2, il existe une extension finie L/K dans laquelle f possède une racine x, d'où la factorisation $f = (X - x)g$, avec $g \in L[X]$ de degré $n - 1$. Par hypothèse de récurrence, il existe une extension finie F/L dans laquelle g est scindé et il en est alors de même pour f. □

Théorème 3.3.20 — *Pour tout corps fini K et tout entier $n > 0$, il existe une extension L/K de degré n.*

Démonstration — D'après le lemme précédent, il existe une extension F/K dans laquelle le polynôme $f = X^{q^n} - X$ est scindé. L'ensemble $L \subset F$ de ses racines n'est autre que l'ensemble des éléments $x \in F$ fixés par Fr_K^n, i.e. tels que $\mathrm{Fr}_K^n(x) = x$. On en déduit en particulier que L est un sous-anneau, donc un sous-corps de F (cf. l'exercice 3.3.1) contenant K. Finalement, le polynôme f étant séparable et scindé

dans $F[X]$, il possède $\deg(f) = q^n$ racines dans F, ce qui implique que L est un corps de cardinal q^n et l'extension L/K est donc de degré n. □

Corollaire 3.3.21 — *Pour tout nombre premier p et tout entier $n > 0$, il existe un corps fini de cardinal $q = p^n$.*

Démonstration — D'après le theorème 3.3.20, il existe une extension $K/\mathbb{F}_p$ de degré n, ce qui implique que K est de cardinal q. □

Corollaire 3.3.22 — *Pour tout corps fini K et tout entier $n > 0$, il existe un polynôme irréductible $f \in K[X]$ de degré n.*

Démonstration — D'après le théorème 3.3.20, il existe une extension L/K de degré n et le theorème 3.3.11 affirme que $L = K(x)$, avec $x \in L$. En appliquant la proposition 3.2.6, on en déduit alors que le polynôme minimal de x sur K est irréductible dans $K[X]$ et de degré n. □

Exercice 3.3.23 — Soit K un corps et considérons deux polynômes $f, g \in K[X]$, avec f irréductible. Montrer que f et g possèdent une racine commune dans une extension (finie) de K si et seulement si f divise g dans $K[X]$.

Théorème 3.3.24 — *Deux corps finis de même cardinal sont isomorphes.*

Démonstration — Soient p un nombre premier et $n > 0$ un entier. Fixons un polynôme irréductible $f \in \mathbb{F}_p[X]$ de degré n. Dans ce cas, le corps $K = \mathbb{F}_p[X]/f\mathbb{F}_p[X]$ est de cardinal $q = p^n$. Par construction, f possède une racine $x = \bar{X}$ dans K et la proposition 3.3.13 affirme que x est également racine du polynôme $X^q - X$. D'après l'exercice ci-dessus, le polynôme f divise $X^q - X$ dans $\mathbb{F}_p[X]$. Soit maintenant L un second corps fini de cardinal q. En appliquant une fois encore la proposition 3.3.13, le polynôme $X^q - X$ est scindé dans $L[X]$ et il en est alors de même pour f, qui le divise. En particulier, f possède une racine $y \in L$. Dans ce cas, f est nécessairment le polynôme minimal de y et le corps $\mathbb{F}_p(y) \subset L$, qui est isomorphe à K, est de cardinal q et coïncide donc avec L. □

D'après ce dernier résultat, il est possible de parler *du* corps fini à $q = p^n$ éléments, que l'on note généralement $\mathbb{F}_q$.

Proposition 3.3.25 — *Soit K un sous-corps d'un corps fini L. Il existe une bijection entre l'ensemble des diviseurs (positifs) du degré de l'extension L/K et l'ensemble des sous-corps de L contenant K.*

Démonstration — Soit F un sous-corps de L contenant K. D'après le corollaire 3.3.4, le degré d de l'extension F/K divise l'entier $n = [L : K]$. Réciproquement, étant donné un diviseur d de n, le polynôme $f_d = X^{q^d} - X$ divise $f_n = X^{q^n} - X$ dans $K[X]$, où q désigne le cardinal de K. D'après la proposition 3.3.13, le polynôme f_n est scindé dans $L[X]$, et il en est alors de même pour f_d. Comme dans la démonstration du

théorème 3.3.20, l'ensemble F de ses racines, qui est le sous-ensemble des éléments de L fixés par Fr_K^d, est un sous-corps de L contenant K et l'extension F/K est de degré d. On vérifie sans difficulté que ces deux constructions sont réciproques l'une de l'autre. □

3.4. Corps finis – aspect cryptographique

3.4.1. Complexité des opérations algébriques dans un corps fini — Soit $\mathbb{F}_q$ le corps fini de caractŕistique p et cardinal $q = p^n$. Voulant utiliser les corps finis dans des applications cryptographiques, il est nécessaire tout d'abord de s'intéresser à la taille d'un élément de $\mathbb{F}_q$, ainsi qu'à la complexité des opérations algébriques. Tout d'abord, d'après les résultats de la section précédente, le corps $\mathbb{F}_q$ est isomorphe au quotient $\mathbb{F}_p[X]/f\mathbb{F}_p[X]$, où $f \in \mathbb{F}_p[X]$ est un polynôme irréductible (unitaire) de degré n. Un élément de $\mathbb{F}_q$ est alors représenté par un unique polynôme $g \in \mathbb{F}_p[X]$ de degré strictement inférieur à n (cf. la proposition 3.2.1) ou, ce qui revient au même, à un élément de $\mathbb{F}_p^n$. Un élément de $\mathbb{F}_p$ est représenté par un unique entier naturel strictement inférieur à p, sa taille (i.e. le nombre de bits nécessaires pour l'encoder) est (inférieure ou) égale à $\ell_2(p) = \lfloor \log_2(p) \rfloor + 1$ (cf. le chapitre 1). On en déduit qu'un élément de $\mathbb{F}_q$ est de taille $n\ell_2(p)$, que l'on peut assimiler (asymptotiquement) à $n \log_2(p) = \log_2(q)$.

Voulant s'intéresser à la complexité des opérations algébriques dans $\mathbb{F}_q$, on commence à s'interesser à l'anneau $\mathbb{F}_p[X]$. Étant donnés deux polynômes non nuls $f = \sum_i a_i X^i$ et $g = \sum_i b_i X^i$ de $\mathbb{F}_p[X]$ de degré strictement inférieur à un entier n, la somme $f + g = \sum_i (a_i + b_i) X^i$ est obtenue en effectuant (au plus) n additions dans $\mathbb{F}_p$, pour une complexité de $O(n \log(p))$. La complexité du produit fg et de la division euclidienne de f par g sont obtenus de manière analogue, se réduisant à une suite d'opérations arithmétiques dans $\mathbb{F}_p$. Le résultat est résumé dans le tableau ci-dessous.

Opération	Complexité
Somme	$O(n \log(p))$
Produit, division euclidienne	$O(n^2 \log^2(p))$

Proposition 3.4.1 — *La somme, le produit et l'élévation à la puissance $m > 0$ dans $\mathbb{F}_q$ sont de complexités respectives $O(\log(q)), O(\log^2(q))$ et $O(\log(m) \log^2(q))$.*

Démonstration — D'après ce qui précède, on réalise explicitement $\mathbb{F}_q$ comme quotient $\mathbb{F}_p[X]/f\mathbb{F}_p[X]$, où $f \in \mathbb{F}_p[X]$ est un polynôme irréductible de degré n, fixé une fois pour toutes. Un élément de $\mathbb{F}_q$ est alors (univoquement) déterminé par un polynôme $g \in \mathbb{F}_p[X]$ de degré strictement inférieur à n. Si deux éléments $x, y \in \mathbb{F}_q$ sont associés respectivement à $g, h \in \mathbb{F}_p[X]$, alors $x+y$ est associé à $g+h$. Sa détermination est donc de complexité $O(n \log(p)) = O(\log(q))$. De même, le polynôme associé au produit xy est le reste de la division euclidienne de gh par f, ce qui donne une complexité de

$O(n^2 \log^2(n)) = O(\log^2(q))$. La complexité de l'élévation à la puissance m est obtenue en appliquant l'algorithme d'exponentiation rapide dans le groupe $\mathbb{F}_q^\times$. □

Remarque 3.4.2 — Dans $\mathbb{F}_q^\times$, l'identité $x^{q-1} = 1$ implique que x^{q-2} est l'inverse de x et peut donc être déterminé explicitement par un algorithme de complexité $O(\log^3(q))$. Des techniques efficaces pour le calcul de l'inverse peuvent également être obtenus en appliquant l'algorithme d'Euclide dans $\mathbb{F}_p[X]$.

Les opérations algébriques dans $\mathbb{F}_q$ étant de complexité polynômiale par rapport à la taille de ses éléments (telle qu'elle a été définie précédemment), les corps finis sont de bons candidats pour des applications cryptographiques.

3.4.2. Le problème du logarithme discret — Soit G un groupe cyclique d'ordre n. Pour tout générateur g de G, on a un isomorphisme de groupes

$$\exp_g : \mathbb{Z}/n\mathbb{Z} \to G$$

défini par $\exp_g(m) = g^m$. Sa réciproque, notée $\log_g$, est appelée ***logarithme discret en base*** g. En d'autres termes, $\log_g(x)$ est le seul élément m de $\mathbb{Z}/n\mathbb{Z}$ tel que $g^m = x$. Avec un leger abus de notation, on identifie souvent $\log_g(x)$ à l'entier de l'ensemble $\{0, 1, \ldots, n-1\}$ qui le représente. Quels que soient $x, y \in G$, on a la relation

$$\log_g(xy) = \log_g(x) + \log_g(y).$$

Étant donnés deux générateurs g_1 et g_2 de G, pour tout $x \in G$, on obtient l'identité

$$\log_{g_1}(x) = \log_{g_1}(g_2) \log_{g_2}(x).$$

En effet, en posant $u = \log_{g_1}(g_2) \in (\mathbb{Z}/n\mathbb{Z})^\times$ et $m = \log_{g_2}(x)$, on a les identités

$$x = g_2^m = (g_1^u)^m = g_1^{um}.$$

Ayant fixé G et g, le ***problème du logarithme discret*** consiste à déterminer un algorithme rapide de calcul de $\log_g$.

Exemple 3.4.3 — Pour $G = \mathbb{Z}/n\mathbb{Z}$, l'élément 1 est un générateur canonique et on a clairement $\log_1(x) = x$. En particulier, si $u \in (\mathbb{Z}/n\mathbb{Z})^\times$ est un second générateur, l'expression ci-dessus se traduit par $\log_u(x) = u^{-1}x$. Il s'en suit que la complexité du problème du logarithme discret sur $\mathbb{Z}/n\mathbb{Z}$ est $O(\log^2(n))$, car il se résume en une simple multiplication. D'un point de vue pratique, si u est représenté par un entier m, u^{-1} peut être obtenu rapidement via l'algorithme d'Euclide ou par exponentiation rapide (d'après le théorème d'Euler, l'inverse de u étant égal à $u^{\varphi(n)-1}$).

Exercice 3.4.4 — Soit G un groupe cyclique d'ordre n pair. Notons x le seul élément d'ordre 2. Montrer que pour tout générateur g de G, on a l'identité

$$\log_g(x) = \frac{n}{2}.$$

Les groupes cycliques G pour lesquels le problème du logarithme discret est difficile sont très utiles en cryptographie à clé publique. Nous en verrons plusieurs applications à la fin de ce chapitre. Au vu de l'exemple ci-dessus, le groupe $\mathbb{Z}/n\mathbb{Z}$ n'est pas un bon candidat. Par contre, il n'existe à ce jour aucun algorithme satisfaisant permettant de déterminer le logarithme discret pour les groupes multiplicatifs des corps finis ou pour les groupes des points rationnels sur une courbe elliptique définie sur un corps fini (hormis des cas exceptionnels).

3.4.3. Le cryptosystème El Gamal — Ce protocole, introduit par Taher ElGamal en 1984, concerne le problème de la confidentialité des messages envoyés, et son efficacité est basée sur la difficulté de résoudre le problème du logarithme discret dans des groupes cycliques bien choisis.

Le principe est le suivant : une personne, Alice, souhaite permettre à quiconque de lui envoyer des messages confidentiels. Pour cela, elle choisit au départ un groupe cyclique G d'ordre n pour lequel le problème du logarithme discret est réputé difficile. Elle fixe générateur g de G et procède ensuite de la manière suivante :

1. Elle choisit aléatoirement un entier a tel que $1 < a < n$, qui sera sa ***clé secrète***. Elle calcule g^a, qu'elle publie, et qui sera sa ***clé publique***. La clé publique de l'algorithme est donc au dápart le triplet (G, g, g^a).
2. Afin d'envoyer un message $m \in G$ à Alice, une personne Bob choisit aléatoirement un entier x tel que $1 < x < n$, et transmet à Alice le couple
$$(g^x, mg^{ax}).$$
C'est la ***phase d'encryptage*** du message m.
3. Dans la ***phase de décryptage***, Alice, ayant reçu le cryptogramme (u, v) et connaissant a, calcule l'élément u^{-a}. Elle effectue ensuite la multiplication de u^{-a} par v, ce qui, vu l'égalité
$$u^{-a}v = g^{-ax}mg^{ax} = m,$$
lui permet de retrouver le message initial.

Les corps finis sont particulièrement adaptés pour limplémentation du cryptosystème El-Gamal. Tout d'abord, le groupe $G = \mathbb{F}_q^\times$ est cyclique, d'ordre $q - 1$. Dans la mise en place du protocole, le choix du générateur g de G (ainsi que du polynôme irréductible permettant de construire explicitement $\mathbb{F}_q$) se fait de manière aléatoire et aboutit rapidement. La clé publique est alors obtenue par un algorithme de complexité $O(\log^3(q))$. De même, les phases d'encryptage et de décryptage sont de complexité $O(\log^3(q))$. Si ce n'est pour la détermination d'un générateur de G, l'ensemble des étapes est donc de complexité polynômiale (par rapport à la taille des éléments de $\mathbb{F}_q$). Par ailleurs, le problème du logarithme discret est réputé difficile pour le groupe $\mathbb{F}_q^\times$, ce qui assure la sécurité de la réalisation explicite du cryptosystème El Gamal via les (groupes multiplicatifs des) corps finis.

Exemple 3.4.5 — La classe de 3 est un générateur de $G = \mathbb{F}_{31}^{\times}$. Supposons que la clé publique d'Alice soit le triplet $(G, 3, 29)$. Bob envoie à Alice le message $(17, 18)$. Afin de retrouver le message m que Bob veut faire parvenir à Alice, il s'agit de trouver le logarithme discret de base 3 de 29, autrement dit, le plus petit entier $a \geq 1$ tel que l'on ait

$$3^a \equiv 29 \mod 31.$$

Dans G, on a $3^3 = -4$, $3^6 = 16$, d'où $3^9 = -64 = 29$ et $a = 9$. Vu que $17^{-1} = 11$, on a donc

$$m = 17^{-9} \cdot 18 = 11^9 \cdot 18.$$

On a $11^2 = -3$, d'où $11^8 = 19$ et $11^9 = -8$, puis $m = 11$.

3.4.4. Le protocole de Diffie-Hellman — Le protocole de Diffie-Hellman (ou Diffie-Hellman-Merkle), décrit en 1976 par Withfield Diffie et Martin Hellman et développé par Ralph C. Merkle, permet à deux personnes, Alice et Bob, de construire une clé secrète commune, qu'ils seront les seuls à connaître, afin de communiquer sur un canal non sécurisé en utilisant cette clé pour chiffrer leur correspondance. Leur procédé de fabrication est basé sur la difficulté de résoudre le problème du logarithme discret dans un groupe cyclique G d'ordre n. Soit g un générateur de G. Le couple (G, g) étant public, Alice et Bob procèdent de la manière suivante :

1. Alice choisit secrètement et aléatoirement un entier a tel que $1 < a < n$, et elle transmet à Bob publiquement l'élément $u = g^a$.
2. Bob choisit aussi secrètement un entier b tel que $1 < b < n$, et il transmet à Alice publiquement l'élément $v = g^b$.
3. Alice élève v à la puissance a, et elle obtient ainsi l'élément $v^a = g^{ab}$.
4. Bob élève u à la puissance b, obtenant de même $u^b = g^{ab}$.

Leur clé secrète commune est alors g^{ab}. Ils sont les seuls à la connaître, car quiconque disposant du couple (G, g), ainsi que des éléments g^a et g^b, ne peut pas en déduire g^{ab} sans la donnée de a ou b. On ne connaît pas d'autres moyens pour déterminer g^{ab}.

3.4.5. Protocoles de secret réparti — Un protocole de ***secret réparti***, ou de ***partage de secret*** est une procédure qui permet de résoudre le problème suivant : supposons d'avoir une donnée secrète (combinaison de coffre-fort, code de lancement de missiles balistiques,...) et que l'on veuille distribuer des informations partielles sur ce secret, appelées ***clés (privées)***, à n dépositaires de telle sorte que :

1. Chaque dépositaire reçoive une clé différente.
2. La connaissance de $k \leq n$ clés permette de retrouver facilement la donnée secrète.
3. La connaissance de $k - 1$ (ou moins) clés laisse la donnée secrète complètement indéterminée.

On parle de partage de secret à n participants et ***seuil*** k ou encore de ***schéma seuil*** (k, n).

Remarque 3.4.6 — La distribution de clés privées permet de hierarchiser le protocole de partage de secret : si certains dépositaires occupent une position privilégiée (dirigeants d'entreprise, généraux d'armée), ils peuvent recevoir plusieurs clés, ce qui leur permet d'obtenir la donnée secrète en faisant recours à un nombre inférieur d'autres dépositaires (voire aucun).

Le protocole de Shamir, que nous allons décrire ici, test l'un des meilleurs protocoles de secret partagé. Il peut être défini sur un corps quelconque mais, dans la pratique, on utilise toujours des corps finis. Il se base sur le simple lemme ci-dessous.

Lemme 3.4.7 — *Soit K un corps et considérons un sous-ensemble $S \subset K$ de cardinal $n+1$. Un polynôme $f \in K[X]$ de degré inférieur ou égal à n est univoquement déterminé par ses valeurs en les éléments de S.*

Démonstration — Pour tout $x \in S$, posons

$$\chi_x = \prod_{y \in S - \{x\}} \frac{X - y}{x - y} \in K[X].$$

Le polynôme χ_x est de degré n et, pour tout $y \in S$ on a

$$\chi_x(y) = \begin{cases} 1 & \text{si } y = x, \\ 0 & \text{si } y \neq x. \end{cases}$$

En posant

$$g = \sum_{x \in S} f(x)\chi_x \in K[X],$$

on obtient alors les identités $f(x) = g(x)$ pour tout $x \in S$. En particulier, le polynôme $h = f - g$, qui est de degré inférieur ou égal à n, possède au moins $n+1$ racines et est donc nul. □

Afin de partager une donnée secrète entre n dépositaires avec un seuil $k \leq n$, on procède de la manière suivante :

1. On fixe un corps (fini) K de cardinal $q > n$.
2. La donnée secrète est un élément $a \in K$.
3. On considère un polynôme f de degré inférieur ou égal à $k-1$ tel que $f(0) = a$. Les clés privées sont des couples $(x, f(x))$ avec $x \neq 0$.

Le lemme 3.4.7 affirme que la donnée de k clés privées permet de déterminer le polynôme f, et donc de calculer $f(0)$. La connaissance de $k-1$ clés privées $(x_1, a_1), \ldots, (x_{k-1}, a_{k-1})$ laisse la donnée secrète complètement indéterminée. En effet, pour tout $b \in K$, il existe un polynôme $g \in K[X]$ de degré inférieur ou égal à $k-1$ tel que $g(x_1) = a_1, \ldots, g(x_{k-1}) = a_{k-1}$ et $g(0) = b$.

Remarque 3.4.8 — Dans la pratique, en ayant k clés privées $(x_1, a_1), \ldots, (x_k, a_k)$, il n'est pas réellement nécessaire de déterminer le polynôme f pour obtenir la donnée secrète. En suivant les notations de la démonstration du lemme 3.4.7, il suffit de calculer $\chi_{x_1}(0), \ldots, \chi_{x_k}(0)$ et d'appliquer la formule

$$f(0) = \sum_{i=1}^{k} a_i \chi_{x_i}(0).$$

Ce protocole est à la fois simple et efficace. La création d'une clé privée est de complexité $O(k \log(k) \log^2(q))$ et la récupération de la donnée secrète en connaissant k clés privées est de complexité $O(k(k + \log(q)) \log^2(q))$.

Exemple 3.4.9 — Considérons le corps $\mathbb{F}_{25} = \mathbb{F}_5(\alpha)$, où α est une racine du polynôme $X^2 - 2$. Supposons que lors d'un protocole de Shamir sur $\mathbb{F}_{25}$ avec seuil $k = 3$ on ait récupéré les clés privées $(1, 2), (2, \alpha)$ et $(\alpha, 1)$. Afin de déterminer la donnée secrète, il faut reconstruire le polynôme f, qui est de degré inférieur ou égal à 2. En suivant la démonstration du lemme 3.4.7 et la remarque ci-dessus, on obtient les identités

$$\begin{cases} \chi_1(0) = 2\alpha - 1, \\ \chi_2(0) = \alpha + 1, \\ \chi_\alpha(0) = 2\alpha + 1, \end{cases}$$

ce qui donne finalement

$$f(0) = 2(2\alpha - 1) + \alpha(\alpha + 1) + 2\alpha + 1 = 2\alpha + 1.$$

3.4.6. La méthode des trois échanges — Ce protocole, proposé par Adi Shamir, s'applique dans un contexte très général. Il peut être résumé de façon imagée de la manière suivante : supposons que deux personnes, Alice et Bob, vivent sur deux îles voisines et qu'Alice veuille envoyer à Bob un coffre rempli de matériel précieux. N'ayant pas de bateau, le seul moyen est de le confier à des passeurs. Or, ces passeurs ont la fâcheuse habitude de dérober le contenu de leurs transports. Comment peut-elle s'y prendre pour être certaine que rien ne soit volé ? On se convainc rapidement qu'avec un seul trajet, le problème n'admet pas de solution. Alice a une idée astucieuse : elle cadenasse le coffre et l'envoie à Bob en gardant la clé. Ce dernier le cadenasse à son tour et le réexpédie à Alice. Le coffre possède désormais deux cadenas. Alice retire le sien et renvoie le coffre à Bob, qui peut alors l'ouvrir avec la certitude de récupérer la totalité de son contenu. Trois trajets permettent de sécuriser le transfert. Voulant appliquer ce principe en cryptographie algébrique, on retrouve Alice et Bob voulant communiquer de manière confidentielle en utilisant un canal non sécurisé. Ils procèdent de la manière suivante :

1. Alice considère un groupe cyclique G pour lequel le problème du logarithme discret est réputé difficile. Voulant envoyer le message $m \in G$, elle choisit un

élément $e \in (\mathbb{Z}/n\mathbb{Z})^\times$, où n désigne l'ordre de G, et transmet à Bob le couple (G, u), avec $u = m^e$ (premier cadenas).

2. Bob choisit à son tour un élément $d \in (\mathbb{Z}/n\mathbb{Z})^\times$ et renvoie à Alice l'élément $v = u^d$ (second cadenas).
3. Alice calcule l'inverse de e' de e modulo $\mathbb{Z}/n\mathbb{Z}$ et renvoie à Bob l'élément $w = v^{e'}$ (retrait du premier cadenas).
4. Finalement, Bob, ayant déterminé l'inverse d' de d modulo $\mathbb{Z}/n\mathbb{Z}$, il calcule $w^{d'}$ et récupère ainsi le message initial (retrait du second cadenas). On a en effet les relations
$$w^{d'} = v^{e'd'} = u^{de'd'} = u^{e'dd'} = u^{e'} = m^{ee'} = m.$$

On remarquera qu'un ingrédient essentiel de cette méthode est la commutativité du groupe $(\mathbb{Z}/n\mathbb{Z})^\times$.

3.5. Complément : attaques du problème du logarithme discret

3.5.1. Le calcul d'indice — La méthode suivante, de nature probabiliste, a été proposée par Maurice Kraitchik au début du vingtième siècle. Elle s'applique aux groupes $G = \mathbb{F}_p^\times$, avec p premier, mais possède de nombreuses généralisations.

Soient donc p un nombre premier et g un générateur de G. Considérons un ensemble B de « petits » nombres premiers différents de p. Un entier naturel est ***B*-friable** si ses diviseurs premiers sont contenus dans B. Fixons un représentant $n \in \{1, \dots, p-1\}$ de g. La première étape de l'algorithme consiste à déterminer les logarithmes discrets des éléments de B. Pour ce faire, on cherche des entiers $u \geq 0$ et v tels que $n^u + pv$ soit B-friable. Pour un tel choix, en posant
$$n^u + pv = (-1)^\nu \prod_{\ell \in B} \ell^{e_\ell},$$
on obtient alors la relation
$$\sum_{\ell \in B} e_\ell \log_g(\ell) = u + \nu \log_g(-1).$$
Supposons que l'on ait $r = \mathrm{Card}(B)$ de ces relations. On en déduit alors que les logarithmes discrets des éléments de B définissent une solution d'un système linéaire de r équations à r inconnues sur $\mathbb{Z}/(p-1)\mathbb{Z}$. Pour le résoudre, on peut utiliser les méthodes classiques de l'algèbre linéaire : on lui associe une matrice à coefficients dans $\mathbb{Z}/(p-1)\mathbb{Z}$ que l'on échelonne ensuite par la méthode du pivot de Gauss. Si on a de la chance, le système admet une unique solution ; sinon on cherche d'autres relations, ou on change l'ensemble B.

Supposons donc que l'on connaisse les logarithmes discrets des éléments de B. Soit $x \in G$, représenté par un entier a. Afin de calculer $\log_g(x)$, on essaie de déterminer

deux entiers $u \geq 0$ et v tels que $n^u a + pv$ soit B-friable. Si cette recherche aboutit, en posant

$$n^u a + pv = (-1)^\nu \prod_{\ell \in B} \ell^{e_\ell},$$

on obtient l'expression

$$\log_g(x) = -u + \nu \log_g(-1) + \sum_{\ell \in B} e_\ell \log_g(\ell).$$

Exemple 3.5.1 — On peut montrer que le groupe $(\mathbb{Z}/1019\mathbb{Z})^\times$ est engéndré par 2. On veut calculer $\log_2(352)$. En prenant $B = \{3, 5, 7\}$, on trouve les relations

$$\begin{cases} 2^3 + 5 \cdot 1019 = 3^6 \cdot 7, \\ 2^{10} - 1019 = 5, \\ 2^{11} - 1019 = 3 \cdot 7^3. \end{cases}$$

On en déduit donc le système linéaire dans $\mathbb{Z}/1018\mathbb{Z}$

$$\begin{cases} 6\log_2(3) + \log_2(7) = 3, \\ \log_2(5) = 10, \\ \log_2(3) + 3\log_2(7) = 11. \end{cases}$$

En le résolvant, on obtient $\log_2(3) = 958, \log_2(5) = 10$ et $\log_2(7) = 363$. Finalement, l'identité

$$2 \cdot 352 - 1019 = -3^2 \cdot 5 \cdot 7$$

amène à la relation

$$1 + \log_2(352) = \log_2(-1) + 2\log_2(3) + \log_2(5) + \log_2(7),$$

d'où l'identité $\log_2(352) = 761$.

3.5.2. L'algorithme Baby step - Giant step — Soit G un groupe cyclique d'ordre n, engendré par un élément g. Ayant fixé $x \in G$, on peut essayer de déterminer $\log_g(x)$ par « force brute » : on calcule $g, g^2, g^3, \ldots$ en multipliant successivement par g et à chaque étape on vérifie si l'élément obtenu coïncide avec x. Pour être certain d'aboutir quel que soit x, cette méthode nécessite n multiplications dans G. Par exemple, pour $G = \mathbb{F}_p^\times$, la multiplication étant de complexité $O(\log^2(p))$, cet algorithme a une complexité de $O(p\log^2(p))$. L'algorithme Baby step - Giant step permet de réduire considérablement le nombre de multiplication nécessaires. Notons $m = \lfloor \sqrt{n} \rfloor$ la partie entière de la racine carrée de n.

Lemme 3.5.2 — *Pour tout $x \in G$, il existe deux entiers naturels $u \leq m - 1$ et $v \leq m + 1$ tels que $x = g^{u+mv}$.*

Démonstration — En considérant l'élément $\log_g(x)$ comme un entier de l'ensemble $\{0, \ldots, n-1\}$, effectuons la division euclidienne

$$\log_g(x) = vm + u,$$

avec $0 \leq u < m$. On a alors l'identité $x = g^{u+vm}$ et les relations

$$v = \frac{\log_g(x) - u}{m} \leq \frac{n-1}{m} < \frac{n-1}{\sqrt{n}-1} = \sqrt{n} + 1 < m + 2,$$

d'où $v \leq m + 1$. □

L'algorithme Baby step - Giant step est défini de la manière suivante : ayant fixé $x \in G$, on calcule $g, g^2, \ldots, g^m$, en multipliant successivement chaque résultat par g (Baby step) et on considère l'ensemble

$$A = \{1, g, g^2, \ldots, g^{m-1}\}$$

On calcule ensuite $x, xg^{-m}, \ldots, g^{-m(m+1)}$ en multipliant successivement par g^{-m} (Giant step). À chaque étape, on vérifie si l'élément obtenu appartient à A. Le lemme ci-dessus affirme que l'algorithme aboutit. Globalement on n'effectue que $2m \leq 2\sqrt{n}$ multiplications dans G, là où la méthode par force brute en requiert n.

Remarque 3.5.3 — De manière générale, vérifier si deux éléments d'un ensemble coïncident est une opération qui a un coût en temps. Prenons l'exemple du groupe multiplicatif $G = \mathbb{F}_p^\times$, avec p premier : les algorithmes permettant de comparer deux éléments de G sont de complexité $O(\log(p))$. Tel qu'il est défini ici, l'algorithme Baby step - Giant step nécessite $m(m+1)$ comparaisons (au plus) et donne une complexité globale de $O(p \log(p))$, ce qui n'est pas réellement satisfaisant (le temps utilisé pour comparer les éléments prenant le dessus par rapport à celui nécessaire pour effectuer les multiplications). Il existe cependant des m'ethodes de tri permettant de ramener la complexité à $O(\sqrt{p} \log^2(p))$. L'algorithme Baby step - Giant step n'a un sens que si l'on utilise ces techniques.

APPENDICE A

RAPPELS D'ALGÈBRE

Cette appendice est un résumé des notions et des résultats fondamentaux d'algèbre utilisés dans le cours. Ils constituent le bagage essentiel de fin de parcours de licence.

A.1. Ensembles

A.1.1. Notations — Dans la suite, nous supposerons le lecteur familier avec les concepts et les construction de base de la théorie des ensembles. On ne rappellera donc pas les notions d'appartenance $x \in A$, d'inclusion $A \subset B$, d'union $A \cup B$ et d'intersection $A \cap B$, ainsi que la définition de produit cartésien $A \times B$, d'application $f : A \to B$ et de ses propriétés (injectivité, surjectivité, image, image réciproque,...) ou de l'ensemble $\mathcal{P}(E)$ des parties d'un ensemble E. Les ensembles seront généralement indiqués par des lettres majuscules $A, B, E, X, \ldots$ et leurs éléments par des minuscules $a, b, e, x, \ldots$. On réservera des symboles spéciaux pour des ensembles classiques tels que l'ensemble $\mathbb{N}$ des entiers naturels, l'ensemble $\mathbb{Z}$ des entiers relatifs, l'ensemble $\mathbb{Q}$ des nombres rationnels, l'ensemble $\mathbb{R}$ des nombres réels et finalement l'ensemble $\mathbb{C}$ des nombres complexes. Le ***cardinal*** d'un ensemble fini A, noté $\mathrm{Card}(A)$, est le nombre de ses éléments. Un ensemble A est ***infini*** s'il n'est pas fini ; on écrira alors simplement $\mathrm{Card}(A) = \infty$, sans aborder des notions plus fines de cardinaux et d'ordinaux, qui n'auraient pas leur place dans ce cours.

A.1.2. Relations — Une ***relation (binaire)*** sur un ensemble E est un sous-ensemble R du produit cartésien $E \times E$. Étant donné un couple $(x, y) \in R$, on dit que x est ***en relation*** avec y et on utilise les notations xRy. Parmi les différentes propriétés que peut vérifier une relation R sur E, nous retiendrons les suivantes :

- ***Reflexivité*** : quel que soit $x \in E$, on a xRx.
- ***Symétrie*** : quels que soient $x, y \in E$, si xRy alors yRx.
- ***Antisymétrie*** : quels que soient $x, y \in E$, si xRy et yRx alors $x = y$.
- ***Transitivité*** : quels que soient $x, y, z \in E$, si xRy et yRz alors xRz.

A.1.3. Relations d'ordre — Une relation R sur X qui est reflexive, antisymétrique et transitive est une ***relation d'ordre***; on dit aussi que R définit un ***ordre*** sur X. Dans ce contexte, et si aucune confusion n'est possible, on utilise la notation $x \leq y$ plutôt que xRy. De même, en suivant la convention usuelle, on écrit $x < n$ lorsque $x \leq y$ et $x \neq y$. L'ordre est ***total*** si, étant donnés $x, y \in X$ on a $x \leq y$ ou $y \leq x$. Un ***minorant*** d'un sous-ensemble U de X est un élément $x \in X$ tel que $x \leq u$ pour tout $u \in U$. On dit également que U est ***minoré*** par x. Si U est minoré par un élément de U, ce dernier est nécessairement unique; c'est le ***plus petit élément*** de U, noté $\min(U)$.

Remarque A.1.1 — Il est important de ne pas confondre les notions de plus petit élément de de ***borne inférieure***, qui est le plus grand des minorants (si jamais il existe). En effet, la borne inférieure d'un sous-ensemble n'est pas nécessairement un élément de ce dernier. Par exemple, tout intervalle ouvert et minoré de $\mathbb{R}$ possède une borne inférieure mais pas de plus petit élément.

A.1.4. Relations d'équivalence — Une ***relation d'équivalence*** R sur un ensemble X est une relation binaire reflexive, symétrique et transitive. Cette notion est fondamentale et reviendra souvent tout au long du cours. Le sous-ensemble $[x] \subset X$ des éléments qui sont en relation avec un élément fixé $x \in X$ est appelé ***classe de R-équivalence***, ou simplement ***classe d'équivalence*** de x. L'ensemble X se décompose en union disjointe de classes d'équivalence et on note X/R le sous-ensemble de $\mathcal{P}(X)$ formé par ces classes. On dit également que X/R est le ***quotient*** de X par la relation R.

A.2. Groupes abéliens

A.2.1. Définitions et premières propriétés — Un ***groupe*** est un ensemble G muni d'une loi de composition interne

$$\begin{aligned} G \times G &\to G \\ (x, y) &\mapsto x \cdot y \end{aligned}$$

vérifiant les propriétés suivantes :

- ***Associativité :*** quels que soient $x, y, z \in G$, on a l'identité
$$x \cdot (y \cdot z) = (x \cdot y) \cdot z.$$
- ***Élément neutre :*** il existe $e \in G$ tel que, pour tout $x \in G$, on a les identités
$$x \cdot e = e \cdot x = x.$$
- ***Inverse :*** pour tout $x \in G$, il existe $y \in G$ tel que
$$x \cdot y = y \cdot x = e.$$

Un groupe est ***abélien*** ou ***commutatif*** si, quels que soient $x, y \in G$, on a l'identité

$$x \cdot y = y \cdot x.$$

Bien que la plupart des résultats présentés dans cet appendice soient valables dans le contexte le plus générale, tous les groupes considérés dans la suite sont abéliens.

Le groupe G est ***fini*** si c'est un ensemble fini. Dans ce cas, son cardinal, plus souvent noté $|G|$, est appelé ***ordre*** du groupe.

Exemples A.2.1 —

1. L'ensemble réduit à un seul élément e, avec pour loi de composition
$$e \cdot e = e,$$
est un groupe, appelé ***groupe trivial***.
2. L'ensemble $\mathbb{Z}$ des entiers relatifs muni de la loi de composition $(x, y) \mapsto x + y$ est un groupe commutatif, d'élément neutre 0. On l'appelle le ***groupe additif*** des entiers relatifs. En remplaçant $\mathbb{Z}$ par $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$, on obtient respectivement le groupe additif des nombres rationnels, celui des nombres réels et celui des nombres complexes.
3. L'ensemble $\mathbb{Q}^\times$ des nombres rationnels non nuls, muni de la loi de composition $(x, y) \mapsto xy$ est un groupe commutatif, d'élément neutre 1. C'est le ***groupe multiplicatif*** des nombres rationnels non nuls. On définit de même les groupes multiplicatifs $\mathbb{R}^\times$ et $\mathbb{C}^\times$.
4. Soient $G_1, \ldots, G_n$ des groupes et considérons leur produit cartésien
$$G = G_1 \times \cdots \times G_n.$$
La loi de composition sur G définie par l'égalité
$$(x_1, \ldots, x_n) \cdot (y_1, \ldots, y_n) = (x_1 y_1, \ldots, x_n y_n),$$
munit G d'une structure de groupe. L'élément neutre est $(e_1, \ldots, e_n)$, où e_i est l'élément neutre de G_i. L'inverse d'un élément $x = (x_1, \ldots, x_n)$ est donné par la formule
$$x^{-1} = (x_1^{-1}, \ldots, x_n^{-1}).$$
Le groupe $(G, \cdot)$ est appelé ***produit direct*** des groupes $G_1, \ldots, G_n$, ou encore ***groupe produit*** de $G_1, \ldots, G_n$.

Fixons un élément x d'un groupe G. Pour tout entier naturel n, on définit l'élément x^n de manière récursive en posant $x^0 = e$ et $x^{n+1} = x \cdot x^n$. Si n est un entier négatif, on pose $x^n = y^{-n}$, où y est l'inverse de x. On vérifie alors facilement l'identité

$$x^{n+m} = x^n \cdot x^m,$$

de laquelle on déduit la seconde identité

$$(x^n)^m = x^{nm},$$

les deux étant valables pour tout choix d'entiers n et m. En particulier, l'élément x^{-1} coïncide avec l'inverse de x.

Remarque A.2.2 — La loi de composition sous-jacente à un groupe est généralement notée multiplicativement $(x, y) \mapsto xy$, ou additivement $(x, y) \mapsto x + y$. En notation multiplicative, on note généralement 1 l'élément neutre. En notation additive, on parle d'***opposé*** plutôt que d'inverse, utilisant le symbole 0 pour l'élément neutre. Pour tout entier n, on écrit alors nx au lieu de x^n. Par exemple, l'opposé de x est égal à $(-1)x$, noté simplement $-x$.

A.2.2. Sous-groupes, groupes quotient — Un sous-ensemble H d'un groupe G est un ***sous-groupe*** si les conditions suivantes sont remplies :

- L'élément neutre 1 appartient à H.
- Quels que soient $x, y \in H$, l'élément xy appartient à H.
- Pour tout $x \in H$, l'inverse x^{-1} de x appartient à H.

En d'autres termes, un H est un sous-groupe si c'est un groupe lorsque l'on le munit de la loi de composition induite par celle de G.

Exemples A.2.3 —

1. Les sous-ensembles G et $\{1\}$ sont des sous-groupes de G. Le sous-groupe $\{1\}$ s'appelle le ***sous-groupe trivial*** de G. Avec un leger abus de notation, il sera simplement noté 1 (ou 0 si l'on adopte la notation additive).
2. Le sous-ensemble de $\mathbb{R}^\times$ formé par les nombres réels strictement positifs, ainsi que le groupe $\mu_2 = \{\pm 1\}$, sont des sous-groupes de $\mathbb{R}^\times$.
3. Si n est un entier relatif, le sous-ensemble
$$n\mathbb{Z} = \{nm \mid m \in \mathbb{Z}\}$$
est un sous-groupe de $\mathbb{Z}$.
4. L'intersection d'une famille (finie ou infinie) de sous-groupes d'un groupe est un sous-groupe.

La relation binaire sur G définie par $x \sim y$ si et seulement si $xy^{-1} \in H$ est une relation d'équivalence. L'ensemble quotient $G/\sim$ est noté G/H. Dans la suite, on désigne par $[g] \in G/H$, la classe d'équivalence d'un élément $g \in G$. On a alors l'identité
$$[g] = gH = \{gh \mid h \in H\}.$$

Remarque A.2.4 — Si le groupe G est noté noté additivement, la relation d'équivalence définie précédemment s'écrit alors sous la forme $x \sim_y$ si et seulement si $x - y \in H$. La classe $[g] \in G/H$ d'un élément de $g \in G$ est alors notée $g + H$.

Étant donnés $x, y \in G/H$ soient $g, h \in G$ tels que $x = [g]$ et $y = [h]$. Dans ce cas, l'élément $xy = [gh] \in G/H$ ne dépend que de x et y et pas du choix des représentants g et h choisis. En effet, si $x = [g']$ et $y = [h']$, ce qui se traduit par $g' = gu$ et $h' = hv$, avec $u, v \in H$, on obtient les identités $g'h' = ghw$, avec $w = uv \in H$ (ici, la commutativité de G joue un rôle crucial), d'où $[g'h'] = [gh]$. On définit ainsi une loi de composition sur G/H et on vérifie sans difficulté que ce dernier est alors muni d'une structure de groupe, appelé ***quotient*** de G par (rapport à) H.

A.2.3. Parties génératrices, groupes finiment engendrés — Considérons un sous-ensemble non vide S d'un groupe G. L'ensemble H des éléments de G s'écrivant comme produit fini de puissances d'éléments de S (une telle écriture n'étant pas nécessairement unique) est un sous-groupe de G. On le note généralement $\langle S \rangle$ et on vérifie facilement qu'il coïncide avec l'intersection des sous-groupes de G contenant S. On dit alors que H est ***engendré*** par S, que S est une ***famille génératrice*** ou encore un ***système de générateurs*** de H. Tout sous-groupe H de G possède une famille génératrice. Il suffit en effet de considérer le système de générateurs formé par H lui-même.

Un groupe G (ou l'un de ses sous-groupes) est ***finiment engendré*** s'il possède un système fini de générateurs. Si G est fini, il est clairement finiment engendré. On dit que G est ***monogène*** s'il est engendré par un unique élément g, ce qui revient à affirmer que tout élément de G s'écrit de manière (pas nécessairement unique) comme g^n (ou ng, en notation additive), avec n entier. Finalement, le groupe G est ***cyclique*** lorsqu'il est fini et monogène. L'***ordre*** d'un élément $g \in G$ est par définition l'ordre du sous-groupe $\langle g \rangle$ qu'il engendre (ce dernier pouvant être infini).

Exemple A.2.5 — Le groupe $\mathbb{Z}$ est monogène, les entiers 1 et -1 étant ses uniques générateurs.

A.2.4. Le théorème de Lagrange — Soit H un sous-groupe d'un groupe (abélien) G. Si le groupe quotient G/H est fini, son ordrel, noté $(G : H)$ est l'***indice*** de H dans G. Si G est fini, il en est de même pour H et G/H. Le résultat ci-dessous est incontournable et fondamental en théorie des groupes finis.

Théorème A.2.6 **(Lagrange)** — *Pour tout sous-groupe H d'un groupe fini G, on a l'identité*

$$|G| = |H| \cdot (G : H).$$

En particulier, l'ordre de H divise celui de G.

Démonstration — Pour tout $g \in G$, les classes d'équivalence $[1] = H$ et $[g] = gH$ sont en bijection via l'application qui à h associe gh et ont donc même cardinal, égal à $|H|$. Le résultat s'en déduit aussitôt, car G est la réunion disjointe de ses classes d'équivalence modulo H. □

A.2.5. Homomorphismes — Une application $f : G \to G'$ d'un groupe G dans un groupe G' est un ***homorphisme*** si

$$f(xy) = f(x)f(y)$$

quels que soient $x, y \in G$. L'homomorphisme f est un ***isomorphisme*** s'il est bijectif, on dit alors que G et G' sont ***isomorphes***. Un ***automorphisme*** d'un groupe G est un isomorphisme $f : G \to G$.

Exemples A.2.7 —

1. Soit G un groupe. Étant donné un élément $x \in G$, l'application $f_x : \mathbb{Z} \to G$ définie par $f_x(n) = x^n$ est un homomorphisme de groupes. Son image est le sous-groupe monogène $\langle x \rangle$ de G engendré par x.
2. Pour tout sous-groupe H d'un groupe G, l'application

   $$\pi : G \to G/H$$

   définie par $\pi(g) = [g] = gH$ est un homomorphisme de groupes, ce qui résulte de la définition de la loi de groupe sur G/H.

Soit $f : G \to G'$ un homomorphisme de groupes. L'image $f(H)$ par f d'un sous-groupe H de G est un sous-groupe de G' et que, réciproquement, l'image réciproque $f^{-1}(H')$ de d'un sous-groupe H' de G' est un sous-groupe de G. L'***image*** de f est le sous-groupe $\mathrm{Im}(f) = f(G)$ de G'. Son ***noyau***, noté $\ker(f)$ le sous-groupe $f^{-1}(1)$ de G. On a donc

$$\ker(f) = \{x \in G \mid f(x) = 1\}.$$

Lemme A.2.8 — *Soit $f : G \to G'$ un homomorphisme de groupes. Le sous-groupe $\ker(f)$ est trivial si et seulement si f est injectif.*

Démonstration — Supposons f injectif et soit x un élément de $\ker(f)$. On a les égalités $f(x) = 1 = f(1)$, d'où $x = 1$. Le sous-groupe $\ker(f)$ est donc trivial. Réciproquement, pour $\ker(f) = 1$, soient x et y deux éléments de G tels que $f(x) = f(y)$. On a $f(x)f(y)^{-1} = 1$ i.e. $f(xy^{-1}) = 1$, d'où $xy^{-1} = 1$, puis $x = y$. □

Proposition A.2.9 — *Un homomorphisme de groupes $f : G \to G'$ induit une bijection entre les sous-groupes de $\mathrm{Im}(f)$ et les sous-groupes de G contenant $\ker(f)$.*

Démonstration — Nous avons déjà vu que si H est un sous-groupe de G, alors $f(H)$ est un sous-groupe de G', clairement contenu dans $\mathrm{Im}(f)$. Réciproquement, si H' est un sous-groupe de $\mathrm{Im}(f)$, alors $f^{-1}(H')$ est un sous-groupe de G contenant $\ker(f)$ (car 1 appartient à H'). Il suffit de vérifier que ces deux applications sont inverses l'une de l'autre. De manière générale, en considérant f juste en tant qu'application, on a l'inclusion $f(f^{-1}(H')) \subset H'$ pour tout sous-ensemble H' de G' et cette inclusion

est une égalité si et seulement si H' est contenu dans $\mathrm{Im}(f)$. Soit maintenant H un sous-groupe de G. On vérifie facilement que l'ensemble

$$H\ker(f) = \{hk \mid h \in H, k \in \ker(f)\}$$

est un sous-groupe de G et que l'on a l'identité

$$f^{-1}(f(H)) = H\ker(f).$$

En particulier, si H contient $\ker(f)$ on a bien l'identité $f^{-1}(f(H)) = H$. □

Remarque A.2.10 — Soit H un sous-groupe d'un groupe G. Si dans la proposition ci-dessus on considère la projection canonique $G \to G/H$, on en déduit une bijection entre les sous-groupes de G contenant H et les sous-groupes de G/H, i.e. tout sous-groupe de G/H est du type K/H, où K est un sous-groupe de K contenant H.

Le résulat suivant, connu sous le nom de ***théorème d'isomorphisme (pour les groupes)***, est un outil fondamental en théorie des groupes.

Théorème A.2.11 — *Étant donné un homomorphisme de groupes $f : G \to G'$, les groupes $G/\ker(f)$ et $\mathrm{Im}(f)$ sont isomorphes.*

Démonstration — L'application $\varphi : G/\ker(f) \to \mathrm{Im}(f)$ qui associe à une classe $x = g\ker(f)$ l'élément $f(g)$ est bien définie. En effet, si h est un second élément de x, on a l'identité $h = gk$, avec $k \in \ker(f)$, d'où les relations

$$f(h) = f(gk) = f(g)f(k) = f(g).$$

Étant donnés deux éléments $x = u\ker(f)$ et $y = v\ker(f)$ de G/H, on a les identités

$$\varphi(xy) = f(uv) = f(u)f(v) = \varphi(x)\varphi(y),$$

ce qui montre que φ est un homomorphisme. Ce dernier est surjectif, car étant donné $w = f(u) \in \mathrm{Im}(f)$, on a par définition $w = \varphi(x)$, avec $x = u\ker(f)$. Il est également injectif, car pour $x = u\ker(f)$, l'identité $\varphi(x) = 1$ se traduit par la relation $f(u) = 1$, ou encore $u \in \ker(f)$, d'où les identités

$$x = u\ker(f) = \ker(f).$$

□

A.3. Anneaux

A.3.1. Anneaux et sous-anneaux — Un ***anneau*** A est un ensemble muni de deux lois de composition, une ***somme*** $(x, y) \mapsto x + y$ et un ***produit*** $(x, y) \mapsto xy$, telles que les conditions suivantes soient vérifiées :

- L'ensemble A est un groupe par rapport à la somme.
- Le produit est associatif et possède un élément neutre.

- Le produit est distributif par rapport à la somme, i.e. quels que soient $x, y, z \in A$, on a les relations

$$x(y+z) = xy + xz \quad \text{et} \quad (x+y)z = xz + yz.$$

Si la multiplication est commutative, autrement dit, si l'on a $xy = yx$ quels que soient $x, y \in A$, on dit que A est ***commutatif***. Sauf mention explicite du contraire, tous les anneaux considérés dans la suite seront supposés commutatifs.

On notera 0 l'élément neutre de A pour la somme et 1 l'élément neutre pour le produit. Un anneau réduit à un élément, i.e. pour lequel on a $1 = 0$, est dit ***nul***. Avec un léger abus de notation, on écrira alors $A = 0$.

Exemples A.3.1 —

1. En munissant $\mathbb{Z}$ des deux lois de composition usuelles (addition et multiplication) on obtient l'anneau des entiers relatifs, qui est commutatif. Les ensembles $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ munis de l'addition de la multiplication usuelles (construites à partir de celles de $\mathbb{Z}$) sont également des anneaux commutatifs.
2. Soient $A_1, \ldots, A_n$ des anneaux. D'après la section précédente, on peut alors considérer le groupe (additif)

$$A = A_1 \times \cdots \times A_n,$$

produit direct des groupes (additifs) $A_1, \ldots, A_n$. L'ensemble A possède une structure naturelle d'anneau, le produit étant défini par la relation

$$(x_1, \ldots, x_n)(y_1, \ldots, y_n) = (x_1 y_1, \ldots, x_n y_n).$$

Si tous les anneaux A_i sont commutatifs, il en est de même pour A. On dit que A est le ***produit direct*** des A_i, ou encore l'***anneau produit*** des A_i. Notons que l'élément neutre multiplicatif de A est $(1, \ldots, 1)$.

Un sous-ensemble B d'un anneau A est un ***sous-anneau*** si les conditions suivantes sont vérifiées :

- B est un sous-groupe additif de A.
- Quels que soient $x, y \in B$, leur produit xy appartient à B.
- L'élément neutre multiplicatif 1 de A appartient à B.

On vérifie que si B est un sous-anneau de A, alors B muni des deux lois de composition induites par celles de A est un anneau.

A.3.2. Idéaux et anneaux quotient — Un sous-ensemble $\mathfrak{a}$ d'un anneau A est un ***idéal*** si les deux conditions suivantes sont vérifiées :

- L'ensemble $\mathfrak{a}$ est un sous-groupe additif de A.
- Quels que soient $x \in \mathfrak{a}$ et $y \in A$, leur produit xy est un élément de $\mathfrak{a}$.

Exemples A.3.2 —

1. Tout anneau A possède deux idéaux particuliers : l'***idéal nul*** 0, formé par le seul élément neutre pour la somme et l'anneau A lui-même. Un idéal non nul et différent de A est ***propre***.
2. Dans $\mathbb{Z}$, tout sous-groupe est automatiquement un idéal.
3. Soit a un élément d'un anneau A. L'ensemble des éléments de la forme ab, où b parcourt A, est un idéal de A. On l'appelle idéal ***monogène*** engendré par a et on le note aA ou simplement (a).

Un idéal $\mathfrak{a}$ d'un anneau A étant un sous-groupe par rapport à la somme, on peut considérer le groupe quotient

$$A/\mathfrak{a} = \{a + \mathfrak{a} \mid a \in A.\}$$

On définit une nouvelle loi de composition interne sur $A/\mathfrak{a}$ (le produit) en posant

$$(a + \mathfrak{a})(b + \mathfrak{a}) = ab + \mathfrak{a}.$$

On vérifie facilement qu'elle est bien définie et qu'elle munit le groupe abélien $A/\mathfrak{a}$ d'une structure d'anneau, appelé ***quotient*** de A par rapport à $\mathfrak{a}$.

A.3.3. Homomorphismes — Étant donnés deux anneaux A et B, une application $f : A \to B$ est un ***homomorphisme*** si elle vérifie les porpriétés suivantes :

- L'application f est un homomorphisme de groupes additifs.
- Quels que soient $a, b \in A$, on a l'identité $f(ab) = f(a)f(b)$.
- On a la relation $f(1) = 1$.

Exemples A.3.3 —

1. Étant donné un anneau, l'application $\iota : \mathbb{Z} \to A$ définie par

   $$\iota(n) = n \cdot 1 = 1 + \cdots (n) \cdots + 1$$

   pour $n \in \mathbb{N}$ et par $\iota(-n) = -\iota(n)$ est un homomorphisme d'anneaux. C'est d'ailleurs l'unique. En effet, un homomorphisme d'anneaux $f : \mathbb{Z} \to A$ est un homomorphisme de groupes, univoquement déterminé par l'image du générateur 1 du groupe monogène $\mathbb{Z}$, celle-ci étant imposée la condition $f(1) = 1$.
2. Pour tout idéal $\mathfrak{a}$ d'un anneau A, la projection $A \to A/\mathfrak{a}$ est un homomorphisme d'anneaux.
3. Considérons des anneaux $A_1, \ldots, A_n$ et notons $A = A_1 \times \cdots \times A_n$ leur produit. Pour tout $i \in \{1, \ldots, n\}$, l'application $\pi_i : A \to A_i$ qui associe à $(a_1, \ldots, a_n)$ l'élément a_i est un homomorphisme d'anneaux, appelé ***projection canonique***. Il est important de remarquer que l'application $f_i : A_i \to A$ définie par $f_i(a) = (0, \ldots, 0, a, 0, \ldots, 0)$ vérifie les relations $f(a + b) = f(a) + f(b)$ et $f(ab) = f(a)f(b)$ quels que soient $a, b \in A_i$ mais que ce n'est néanmoins pas un homomorphisme d'anneaux car $f(1)$ n'est pas l'unité de A.

Soit $f : A \to B$ un homomorphisme d'anneaux. On vérifie facilement que l'ensemble $\mathrm{Im}(f)$, appelé ***image*** de f est un sous-anneau de B et que, pour tout idéal $\mathfrak{a}$ de A, son image $f(\mathfrak{a})$ par f est un idéal de $\mathrm{Im}(f)$ (mais généralement pas de B). De même, pour tout idéal $\mathfrak{b}$ de B, l'ensemble $f^{-1}(\mathfrak{b})$ est un idéal de A. Le ***noyau*** $\ker(f)$ d'un homomorphisme d'anneaux $f : A \to B$ est l'ensemble

$$\ker(f) = f^{-1}(0) = \{a \in A \mid f(a) = 0\}.$$

En d'autres termes, $\ker(f)$ est le noyau de l'application f, considérée en tant qu'homomorphisme de groupes additifs. Au vu de ce qui précéde, c'est un idéal.

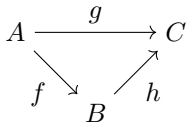
Proposition A.3.4 — *Un homomorphisme d'anneaux $f : A \to B$ est injectif si et seulement si $\ker(f) = 0$. De plus, l'application f induit une bijection entre l'ensemble des idéaux de $\mathrm{Im}(f)$ et l'ensemble des idéaux de A contenant $\ker(f)$.*

Démonstration — On procède exactement comme pour la proposition A.2.9 et le lemme qui la précède. □

Remarque A.3.5 — Pour tout idéal $\mathfrak{a}$ de A, en considérant la projection $A \to A/\mathfrak{a}$, on obtient une bijection entre les idéaux de $A/\mathfrak{a}$ et les idéaux de A contenant $\mathfrak{a}$, i.e. tout idéal de $A/\mathfrak{a}$ s'écrit comme $\mathfrak{b}/\mathfrak{a}$, où $\mathfrak{b}$ est un idéal de A contenant $\mathfrak{a}$.

Le résultat suivant est l'analogue du théorème d'isomorphisme pour les homomorphismes de groupes. Nous en donnons une version à peine plus détaillée.

Théorème A.3.6 — *Considérons deux homomorphismes d'anneaux $f : A \to B$, et $g : A \to C$, avec f surjectif. Si $\ker(f)$ est contenu dans $\ker(g)$ alors il existe un unique homomorphisme d'anneaux $h : B \to C$ tel que $g = hf$. On dit alors que le le diagramme*



est commutatif.

Démonstration — On reprend essentiellement la même construction que pour le théorème A.2.11 : étant donné $b \in B$, soit $a \in A$ tel que $f(a) = b$. On pose alors $h(b) = g(a)$. Si $a' \in A$ vérifie $f(a') = b$, on a $a - a' \in \ker(f) \subset \ker(g)$, d'où $g(a) = g(a')$. L'application $h : B \to C$ est donc bien définie. Étant donnés $b = f(a)$ et $b' = f(a')$, on a $b + b' = f(a + a')$, ce qui donne

$$h(b + b') = g(a + a') = g(a) + g(a') = h(b) + h(b').$$

De même, l'identité $bb' = f(aa')$ amène aux relations

$$h(bb') = g(bb') = g(b)g(b') = h(b)h(b').$$

Finalement, on a $f(1) = 1$ et donc $h(1) = 1$. On a montré que h est un homomorphisme d'anneaux. Concernant son unicité, si $h' : B \to C$ est une second homomorphisme vérifiant la propriété de l'énoncé, on a $hf = h'f$. Pour $b = f(a) \in B$, on obtient alors les identités

$$h(b) = hf(a) = h'f(a) = h'(b).$$

□

Corollaire A.3.7 — *Étant donné un homomorphisme d'anneaux $f : A \to B$, les anneaux $A/\ker(f)$ et $\mathrm{Im}(f)$ sont canoniquement isomorphes.*

Démonstration — Quitte à remplacer B par $\mathrm{Im}(f)$, on peut supposer f surjectif. Considérons la projection canonique $g : A \to A/\ker(f)$. On a $\ker(f) = \ker(g)$ et le résultat précédent affirme qu'il existe un unique couple d'homomorphismes $h : A/\ker(f) \to B$ et $k : B \to A/\ker(f)$ tels que $g = kf$ et $f = hg$. Mais dans ce cas, on obtient $f = hkf$, d'où $hk = 1$, par surjectivité de f et, de même, on a l'identité $kh = 1$. □

A.3.4. Éléments réguliers, inversibles et diviseurs de zéro — Un élément a d'un anneau A est ***régulier*** si, pour tout $b \in A$, l'identité $ab = 0$ est équivalente à $b = 0$. En d'autres termes, a est régulier s'il vérifie la ***propriété d'effacement*** par rapport au produit : étant donnés $b, c \in A$, on a $ab = ac$ si et seulement si $b = c$. Un idéal $\mathfrak{a}$ de A est ***principal*** s'il est monogène et engendré par un élément régulier, ce qui revient à affirmer qu'il existe un élément $a \in \mathfrak{a}$ tel que l'homomorphisme de groupes additifs $A \to \mathfrak{a}$ qui associe à $b \in A$ l'élément ab soit bijectif. Un anneau A est ***intègre*** si tous ses éléments non nuls sont réguliers. En d'autres termes, A est intègre si et seulement si le produit de deux éléments non nuls est non nul. Dans un anneau intègre, la notion d'idéal monogène et d'idéal principal coïncident et tout sous-anneau d'un anneau intègre est intègre. Finalement, l'anneau A est ***principal*** si tous ses idéaux non nuls sont principaux (en particulier, A est intègre).

Exemple A.3.8 — L'anneau $\mathbb{C}$ est intègre. Il en est donc de même pour ses sous-anneaux $\mathbb{Z}, \mathbb{Q}$ et $\mathbb{R}$. Tout corps est clairement principal. D'après la classification de ses sous-groupes (qui coïncident avec ses idéaux) l'anneau $\mathbb{Z}$ est principal.

Un 'élément $a \in A$ est une ***unité***, ou un ***élément inversible*** s'il existe $b \in A$ tel que $ab = 1$ (on rappelle que l'anneau A est supposé commutatif). On dit alors que b est l'***inverse*** de a. Un élément inversible est régulier, la réciproque étant fausse en général. L'ensemble $A^\times$ des unités de A est un groupe (multiplicatif), appelé ***groupe des unités***. Un ***corps*** est un anneau non nul dans lequel tout élément non nul est inversible. Un corps est automatiquement intègre.

Exemple A.3.9 — Les anneaux $\mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$ sont des corps mais il n'en est pas de même pour $\mathbb{Z}$, le groupe $\mathbb{Z}^\times$ étant réduit aux éléments 1 et -1.

Remarque A.3.10 — Un élément a d'un anneau A est inversible si et seulement si $aA = A$. En effet, si a est inversible, d'inverse b, on a l'identité $1 = ab \in aA$, d'où $c = abc \in aA$ pour tout $c \in A$, ou encore $aA = A$. Réciproquement, pour $aA = A$, on a en particulier $1 \in A$, d'où l'existence d'un élément $b \in A$ tel que $ab = 1$.

Proposition A.3.11 — *Soient $A_1, \ldots, A_n$ des anneaux et notons A leur produit direct. On a alors l'identité*

$$A^\times = A_1^\times \times \cdots \times A_n^\times.$$

Démonstration — Tout d'abord, on a l'inclusion $A_1^\times \times \cdots \times A_n^\times \subset A^\times$, l'inverse de $(a_1, \ldots, a_n)$ étant donné par $(a_1^{-1}, \ldots, a_n^{-1})$. Réciproquement, si $(a_1, \ldots, a_n) \in A$ est inversible, d'inverse $(b_1, \ldots, b_n)$, on obtient les identités

$$(a_1, \ldots, a_n)(b_1, \ldots, b_n) = (a_1 b_1, \ldots, a_n b_n) = (1, \ldots, 1),$$

ce qui implique que pour tout entier $i \in \{1, \ldots, n\}$, l'élément $a_i \in A_i$ est inversible, d'inverse b_i, d'où l'inclusion $A^\times \subset A_1^\times \times \cdots \times A_n^\times$, qui est alors une égalité. □

Un élément $a \in A$ qui n'est pas régulier est un ***diviseur de zéro***, ce qui revient à affirmer qu'il existe un élément non nul $b \in A$ tel que $ab = 0$. On dit que a est ***nilpotent*** s'il existe un entier strictement positif n tel que $a^n = 0$. L'anneau A est ***réduit*** s'il ne possède pas de nilpotents non nuls.

A.3.5. Idéaux premiers et maximaux — Un idéal $\mathfrak{p}$ d'un anneau A est ***premier*** si $\mathfrak{p} \neq A$ et, si quels que soient $a, b \in A$, la relation $ab \in \mathfrak{p}$ implique que $a \in \mathfrak{p}$ ou $b \in \mathfrak{p}$. L'idéal $\mathfrak{p}$ est ***maximal*** s'il n'est contenu dans aucun idéal propre de A. En d'autres termes, si $\mathfrak{a}$ est un idéal de A contenant $\mathfrak{p}$, on a $\mathfrak{a} = \mathfrak{p}$ ou $\mathfrak{a} = A$.

Lemme A.3.12 — *Un anneau non nul A est un corps si et seulement s'il ne possède pas d'idéaux autres que 0 et A.*

Démonstration — Si A est un corps et $\mathfrak{a}$ est un idéal non nul, en fixant un élément non nul $a \in \mathfrak{a}$, on obtient $aA = A$ (cf. la remarque A.3.10), et donc $\mathfrak{a} = A$. Récirpoquement, pour tout élément non nul $a \in A$, l'idéal aA étant non nul, il coïncide avec A et l'élément a est alors inversible. □

Ce dernier résultat implique en particulier que tout homomorphisme $f : K \to A$ d'un corps K dans un anneau A non nul est injectif. En effet, on a $\ker(f) \neq A$ (car $f(1) = 1 \neq 0$), d'où $\ker(f) = 0$.

Proposition A.3.13 — *Un idéal $\mathfrak{a}$ de A est premier (resp. maximal) si et seulement si le quotient $A/\mathfrak{a}$ est intègre (resp. un corps).*

Démonstration — Notons $\bar{a}$ l'élément $a + \mathfrak{a}$ de $A/\mathfrak{a}$. On remarquera que $\bar{a}\bar{b} = \overline{ab}$ (c'est une conséquence directe du fait que la projection $A \to A/\mathfrak{a}$ est un homomorphisme d'anneaux) et que $\bar{a} = 0$ si et seulement si $a \in \mathfrak{a}$. On en déduit immédiatement

l'équivalence entre l'intégrité de $A/\mathfrak{a}$ et la primalité de $\mathfrak{a}$. Maintenant, d'après la proposition A.3.4 et la remarque qui la suit, il existe une bijection entre les idéaux de $A/\mathfrak{a}$ et les idéaux de A contenant $\mathfrak{a}$. Le lemme précédent affirme alors que $A/\mathfrak{a}$ est un corps si et seulement si $\mathfrak{a}$ est maximal. □

Corollaire A.3.14 — *Tout idéal maximal est premier.*

Démonstration — En effet, d'après le résultat précédent si $\mathfrak{p}$ est un idéal maximal d'un anneau A, le quotient $A/\mathfrak{p}$ est un corps, qui est intègre, ce qui implique que $\mathfrak{p}$ est premier. □

Le résultat élémentaire ci-dessous sera très utile dans la suite du cours.

Lemme A.3.15 — *Si un idéal premier d'un anneau contient le produit d'une famille finie d'idéaux alors il contient l'un d'entre eux.*

Démonstration — Soit $\mathfrak{p}$ un idéal premier d'un anneau A contenant le produit d'une famille finie $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ d'idéaux et supposons qu'il ne contienne aucun d'entre eux. Pour tout $i \in \{1, \ldots, n\}$, choisissons un élément $a_i \in \mathfrak{a}_i$ n'appartenant pas à $\mathfrak{p}$. Par hypothèse, le produit $a_1 \cdots a_n$ appartient à $\mathfrak{p}$ mais ce dernier ne contient aucun des facteurs, contredisant sa primalité. □