# 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* — C'est un cas particulier du lemme A.3.19, car le coefficient dominant de $g$ est non nul, donc inversible. □

***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 générateur unitaire $(f, g)$ de l'idéal $fK[X] + gK[X]$ et l'on dispose d'une identité de Bézout

$$(f, g) = uf + vg,$$

avec $u, v \in K[X]$. Les polynômes $f$ et $g$ sont premiers entre eux si $(f, g) = 1$. Dans ce cas, on peut appliquer le lemme de Gauss (cf. l'exercice 1.1.11). Le résultat ci-dessous est l'analogue de la proposition 1.1.7 ; 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 1.1.16, 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, un survol

**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 $\iota$, 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 $1, x, \ldots, x^{n-1}$ 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 $a_0, \ldots, a_{n-1} \in K$, ce qui implique que les éléments $1, \ldots, x^{n-1}$ 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 $a_0, \ldots, a_{n-1} \in K$, 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 $1, x, \ldots, x^{n-1}$ 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

$$K[X] \xrightarrow{\mathrm{ev}_x} L$$

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 $\mathrm{ev}_f$ 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 $\mathrm{ev}_x : K[X] \to L$ est une application $K$-linéaire. Le $K$-espace vectoriel $K[X]$ étant de dimension infinie, $\ker(\mathrm{ev}_x) = \mathrm{Ann}_K(x)$ ne peut être nul (sinon $\mathrm{ev}_x$ 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 – théorie générale

**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 $\mathrm{Fr}_K$ 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 2.1.13 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 $\mathrm{Fr}_K$ 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 $\mathrm{Fr}_K$ 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 $\mathrm{Fr}_K$.*

*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 $\mathrm{Fr}_K$. 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 $\mathrm{Fr}_K$ 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 $\mathrm{Fr}_K^n$, 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 $\mathrm{Fr}_K^d$, 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 $\{0,1,\dots,n-1\}$ 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. 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.