Cours Math Comp
Partie Algèbre

Pierre-Alain Fouque

Contents

Chapter 1

Arithmétique

1.1 Plus grand commun diviseur

La notion de pgcd de deux entiers joue un rôle très important en cryptographie. Rappelons ici ses principales propriétés. Soient $\mathbb{N}$ l'ensemble des entiers naturels et $\mathbb{Z}$ celui des entiers relatifs. Toute partie non vide $\mathbb{N}$ possède un plus petit élément.

Proposition 1. *(Division euclidienne). Soient a et b des entiers relatifs avec $b \neq 0$. Il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{Z}$ tel que l'on ait*

$$a = bq + r \text{ et } 0 \leq r < |b|.$$

On dit que q est le quotient et que r est le reste de la division euclidienne de a par b.

Démonstration : Considérons l'ensemble

$$A = \{a - bk : k \in \mathbb{Z}\} \cap \mathbb{N}.$$

C'est une partie non vide de $\mathbb{N}$. Par suite, $\mathbb{A}$ possède un plus petit élément r. Puisque r appartient à A, c'est un entier naturel et il existe $q \in \mathbb{Z}$ tel que $a - bq = r$. Vérifions que l'on a $r < |b|$. Supposons le contraire. On obtient

$$0 \leq r - |b| = a - b(q + \varepsilon) \in A \text{ avec } \varepsilon = \pm 1.$$

L'inégalité $r - |b| < r$ contredit alors le caractère minimal de r, d'où l'assertion d'existence. Soient (q, r) et (q', r') dans $\mathbb{Z} \times \mathbb{Z}$ tels que l'on ait

$$a = bq + r = bq' + r' \text{ avec } 0 \leq r < |b| \text{ et } 0 \leq r' < |b|.$$

On a $|q - q'||b| = |r' - r|$. Puisque r et r' sont positifs, $|r - r'|$ est inférieur ou égal à r ou r', d'où $|r - r'| < |b|$. On obtient $|q - q'| < 1$, d'où $q = q'$ puis $r = r'$, ce qui établit l'unicité.

Afin de définir le plus grand commun diviseur de deux entiers, une façon de procéder est de décrire préalablement les sous-groupes de $\mathbb{Z}$. Pour tout $n \in \mathbb{N}$, l'ensemble $n\mathbb{Z}$ des multiples de n est un sous-groupe de $\mathbb{Z}$. Inversement:

Lemma 1. *Soit H un sous-groupe de $\mathbb{Z}$. Il existe un unique entier $n \in \mathbb{N}$ tel que $H = n\mathbb{Z}$.*

Démonstration : Si $H = \{0\}$ l'entier $n = 0$ convient. Supposons $H \neq \{0\}$. L'ensemble $A = H \cap \mathbb{N}^*$ n'est pas vide, car si n est dans H, alors $-n$ l'est aussi. Soit n le plus petit élément de A. Vérifions que l'on a $H = n\mathbb{Z}$. Tout d'abord, H étant un sous-groupe de $\mathbb{Z}$, et n étant dans H, $n\mathbb{Z}$ est contenu dans H. Inversement, soit x un élément de H. On a $n \neq 0$. Il existe donc q et r dans $\mathbb{Z}$ tels que $x = nq + r$ avec $0 \leq r < n$ (prop. 1). Puisque x et nq appartiennent à H, il en est de même de r. Le caractère minimal de n entraîne $r = 0$, donc x appartient à $n\mathbb{Z}$. Par ailleurs, si l'on a $n\mathbb{Z} = m\mathbb{Z}$ avec m et n dans $\mathbb{N}$, alors m divise n et n divise m, d'où $m = n$.

Soient a et b des entiers relatifs non tous les deux nuls. L'ensemble

$$a\mathbb{Z} + b\mathbb{Z} = \big\{au + bv : u, v \in \mathbb{Z}\big\},$$

est un sous-groupe de $\mathbb{Z}$. Il existe donc un unique entier $d \geq 1$ tel que l'on ait

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

Définition 1. *L'entier d s'appelle le plus grand commun diviseur de a et b (greatest common divisor - gcd), ou en abrégé le pgcd de a et b. On note souvent $d = \gcd(a, b)$.*

Avec cette définition, on a de fait la propriété de Bézout, à savoir qu'il existe des entiers relatifs u et v tels que l'on ait

$$d = au + bv. \tag{1.1}$$

On en déduit directement la caractérisation du pgcd de deux entiers :

Lemma 2. *Le pgcd de a et b est l'unique entier naturel satisfaisant les conditions suivantes :*

1. *c'est un diviseur de a et b.*
2. *Il est multiple de tout diviseur commun de a et b.*

Définition 2. *On dit que a et b sont premiers entre eux, ou que a est premier avec b, si l'on a $\gcd(a, b) = 1$.*

Comme conséquence de (1.1), on obtient :

Lemma 3. *Les entiers a et b sont premiers entre eux si et seulement si il existe u et v dans $\mathbb{Z}$ tels que $au + bv = 1$.*

Corollaire 1. *Les entiers $\frac{a}{d}$ et $\frac{b}{d}$ sont premiers entre eux.*

Corollaire 2. ***(Théorème de Gauss).*** *Soit c un entier relatif tel que a divise bc et que a soit premier avec b. Alors a divise c.*

Démonstration : Il existe u et v dans $\mathbb{Z}$ tels que $au + bv = 1$. On obtient l'égalité $(ac)u + (bc)v = c$, d'où l'assertion.

Exemples 1.1. 1) Soient a et b des entiers naturels tels que $a > b$. On a

$$\gcd(a, b) = \gcd(b, a - b).$$

En effet, un entier divise a et b si et seulement si il divise b et $a - b$. Cette égalité, utilisée récursivement, permet de calculer le gcd de a et b. Par exemple, on a

$$\gcd(48, 30) = \gcd(30, 18) = \gcd(18, 12) = \gcd(12, 6) = \gcd(6, 6) = 6.$$

Ce procédé est à la base de l'algorithme d'Euclide (voir ci-dessous).

2) Démontrons que tout entier $n \geq 7$ peut s'écrire sous la forme

$$n = a + b \text{ avec } \gcd(a, b) = 1 \text{ et } a \geq 2, b \geq 2.$$

Si n est impair, la décomposition $n = a + b$ avec $a = 2$ et $b = n - 2$ convient. Supposons n multiple de 4. En posant $n = 4k$, on a $n = a + b$ avec $a = 2k - 1$ et $b = 2k + 1$. Deux nombres impairs consécutifs étant premiers entre eux, on obtient l'assertion dans ce cas. Supposons $n = 2 \bmod 4$. Posons $n = 4k + 2$. On a alors $n = a + b$ avec $a = 2k + 3$ et $b = 2k - 1$. L'inégalité $n \geq 7$ entraîne $k \geq 2$, donc a et b sont au moins égaux à 2. On a $a - b = 4$, donc le gcd de a et b divise 4. Puisque a et b sont impairs, ils sont donc premiers entre eux, d'où le résultat.

3) Soient a et b des entiers relatifs tels que $a > b$. Il existe une infinité d'entiers $n \in \mathbb{N}$ tels que $a+n$ et $b+n$ soient premiers entre eux. Tel est le cas des entiers n de la forme

$$n = (a-b)k + 1 - b,$$

où k est un entier plus grand que $\frac{b-1}{a-b}$. En effet, si d est un diviseur positif de $a+n$ et $b+n$, alors d divise $a-b$, et l'égalité $b+n = (a-b)k+1$ implique $d = 1$.

4) Pour tout $n \in \mathbb{N}$, posons $F_n = 2^{2^n} + 1$. Un tel entier s'appelle un nombre de Fermat. Soient m et n deux entiers naturels distincts. Vérifions que F_m et F_n sont premiers entre eux. Supposons $n > m$. On a

$$F_n = (2^{2^m})^{2^{n-m}} + 1 = (F_m - 1)^{2^{n-m}} + 1 = 2 \bmod F_m.$$

Par suite, tout diviseur commun de F_m et F_n divise 2, d'où l'assertion vu que F_m et F_n sont impairs.

Remarque 1. ***(Plus petit commun multiple).*** *Étant donnés des entiers relatifs a et b non nuls, l'ensemble $a\mathbb{Z} \cap b\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$. L'entier naturel m tel que*

$$a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z} \tag{1.2}$$

s'appelle le plus petit commun multiple de a et b (least common multiplier - lcm). On écrit en abrégé $m = \operatorname{lcm}(a,b)$. Il est caractérisé par le fait que c'est un multiple de a et b et que tout multiple de a et b est un multiple de m. De plus, on a l'égalité

$$\gcd(a,b)\operatorname{lcm}(a,b) = |ab|. \tag{1.3}$$

En effet, si $d = \gcd(a,b)$, d'après (1.2) l'entier $\frac{m}{d}$ est le ppcm de $\frac{a}{d}$ et $\frac{b}{d}$. Puisque $\frac{a}{d}$ et $\frac{b}{d}$ sont premiers entre eux, afin d'établir (1.3) on se ramène au cas où $d = 1$. Il s'agit donc de prouver que si a et b sont premiers entre eux, $|ab|$ est le ppcm de a et b. D'abord, $|ab|$ est multiple de a et b. Par ailleurs, si c est un multiple de a et b, il existe des entiers r et s tels que $c = ar = bs$, et d'après le théorème de Gauss a divise s, donc c est multiple de $|ab|$, d'où la formule (1.3).

1.2 L'algorithme d'Euclide

Soient a et b deux entiers naturels tels que

$$a > b \geq 1.$$

On va détailler ici l'algorithme d'Euclide étendu, qui permet de déterminer le pgcd de a et b, et de plus d'expliciter une relation de Bézout entre a et b, autrement dit, d'expliciter des entiers relatifs u et v tels que l'on ait $\gcd(a,b) = au + bv$.

On construit pour cela une suite finie d'entiers naturels $(r_i)_{i\geq 0}$, que l'on appelle la suite des restes (associée à a et b), par le procédé suivant : on pose

$$r_0 = a \text{ et } r_1 = b.$$

Supposons construits $r_0, r_1, \cdots, r_i$ où $i \geq 1$. Si $r_i \neq 0$, on définit alors r_{i+1} comme étant le reste de la division euclidienne de r_{i-1} par r_i. Si $r_i = 0$, le procédé s'arrête et la suite des restes est alors formée des entiers $r_0, r_1, \cdots, r_{i-1}, r_i$. Il existe un unique entier $n \geq 1$ tel que la condition suivante soit satisfaite :

$$0 < r_n < r_{n-1} < \ldots < r_1 < r_0 \text{ et } r_{n+1} = 0.$$

Proposition 2. *On a $r_n = \gcd(a,b)$.*

Démonstration : Soit i un entier tel que $1 \leq i \leq n$. Il existe $q_i \in \mathbb{Z}$ tel que l'on ait

$$r_{i-1} = q_i r_i + r_{i+1} \text{ avec } 0 \leq r_{i+1} < r_i. \tag{1.4}$$

On a l'égalité

$$\gcd(r_{i-1}, r_i) = \gcd(r_i, r_{i+1}).$$

Par suite, on a $\gcd(a,b) = \gcd(r_0, r_1) = \gcd(r_1, r_2) = \ldots = \gcd(r_{n-1}, r_n) = r_n$. Le pgcd de a et b est donc le dernier reste non nul r_n dans la suite des restes que l'on a construite. Il existe ainsi u et v dans $\mathbb{Z}$ tels que l'on ait

$$r_n = au + bv.$$

Le problème qui nous intéresse alors est d'expliciter un tel couple (u, v). On construit pour cela deux suites d'entiers $(u_i)_{0 \leq i \leq n}$ et $(v_i)_{0 \leq i \leq n}$ en posant

$$u_0 = 1, u_1 = 0 \text{ et } v_0 = 0, v_1 = 1,$$

$$u_{i+1} = u_{i-1} - u_i q_i \text{ et } v_{i+1} = v_{i-1} - v_i q_i \text{ pour tout } i = 1, \ldots, n-1,$$

où q_i est défini par l'égalité (1.4), autrement dit, où q_i est le quotient de la division euclidienne de r_{i-1} par r_i.

Proposition 3. *On a $r_n = au_n + bv_n$.*

Démonstration : Il suffit de vérifier que pour tout i tel que $0 \leq i \leq n$, on a l'égalité $r_i = au_i + bv_i$. Elle est vraie si $i = 0$ et $i = 1$. Considérons un entier k vérifiant les inégalités $1 \leq k < n$ tel que l'on ait $r_i = au_i + bv_i$ pour tout $i \leq k$.On a alors

$$r_{k+1} = r_{k-1} - q_k r_k = (u_{k-1}a + v_{k-1}b) - q_k(u_k a + v_k b) = au_{k+1} + bv_{k+1},$$

d'où l'égalité annoncée.

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

	q_1	q_2	$\ldots$	q_{n-1}	q_n	
$r_0 = a$	$r_1 = b$	r_2	$\ldots$	r_{n-1}	r_n	0
1	0	u_2	$\ldots$	u_{n-1}	u_n	
0	1	v_2	$\ldots$	v_{n-1}	v_n	

Exemple. Avec $a = 20825$ et $b = 455$, on obtient le tableau :

	45	1	3	3	
20825	455	350	105	35	0
1	0	1	-1	4	
0	1	-45	46	-183	

On a donc $\gcd(a,b) = 35$ et l'on obtient la relation de Bézout

$$4 \times 20825 - 183 \times 455 = 35.$$

Avec les notations précédentes, l'entier n est le nombre de divisions euclidiennes à effectuer pour déterminer r_n. On dit que n est le nombre de pas nécessaires dans l'algorithme d'Euclide pour obtenir le pgcd de a et b. Donnons une majoration de n.

Théorème 1. *On a l'inégalité*

$$n \leq \frac{3}{2\log 2} \log b + 1.$$

Afin de prouver cet énoncé, introduisons la suite de Fibonacci définie par les égalités

$$U_0 = 0, U_1 = 1 \text{ et } U_{k+1} = U_k + U_{k-1} \text{ pour } k \geq 1.$$

On vérifie par récurrence que pour tout $k \geq 1$, on a l'égalité matricielle

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^k = \begin{pmatrix} U_{k+1} & U_k \\ U_k & U_{k-1} \end{pmatrix}.$$

On en déduit par exemple l'égalité

$$U_{k+1}U_{k-1} - U_k^2 = (-1)^k,$$

qui entraîne que U_k et U_{k+1} sont premiers entre eux.

Proposition 4. ***(Lamé, 1845).*** *Posons $d = \gcd(a, b)$. On a*

$$a \geq dU_{n+2} \text{ et } b \geq dU_{n+1}. \tag{1.5}$$

Démonstration : Si $n = 1$, l'entier a est alors multiple de b et l'on a

$$d = b \text{ et } a \geq 2b.$$

Vu que l'on a $U_2 = 1$ et $U_3 = 2$, les inégalités (1.5) sont donc vérifiées dans ce cas. Supposons $n \geq 2$ et l'énoncé vrai pour l'entier $n - 1$. Le premier pas de l'algorithme transforme le couple (a, b) en (b, c), où c est le reste de la division euclidienne de a par b (avec les notations utilisées précédemment on a $c = r_2$). Par définition, l'algorithme d'Euclide, partant du couple (b, c) pour obtenir d, s'arrête au bout de $n - 1$ pas. D'après l'hypothèse de récurrence, on obtient

$$b \geq dU_{n+1} \text{ et } c \geq dU_n.$$

Puisque l'on a $a \geq b + c$, on en déduit l'inégalité

$$a \geq d(U_{n+1} + U_n) = dU_{n+2},$$

ce qui prouve la condition (1.5) pour l'entier n.

Remarque 2. *Pour tout $k \geq 1$, le pgcd de U_{k+2} et U_{k+1} est 1, et sa détermination par l'algorithme d'Euclide nécessite k pas. Avec $a = U_{k+2}$ et $b = U_{k+1}$, les inégalités (1.5) sont donc des égalités.*

Lemma 4. *Pour tout $k \in \mathbb{N}$, on a*

$$U_{k+1} \geq 2^{\frac{2(k-1)}{3}}.$$

Démonstration : C'est vrai pour $k = 0$ et $k = 1$. Soit k un entier ≥ 1 tel que cette inégalité soit vraie pour les entiers $k - 1$ et k. On a

$$U_{k+2} = U_{k+1} + U_k \geq 2^{\frac{2(k-1)}{3}} + 2^{\frac{2(k-2)}{3}}.$$

L'inégalité

$$2^{-\frac{2}{3}} + 2^{-\frac{4}{3}} \geq 1$$

entraîne alors le résultat.

Le théorème se déduit comme suit. D'après la proposition 4, on a $U_{n+1} \leq b$. Compte tenu du lemme 4, on obtient

$$2^{\frac{2(n-1)}{3}} \leq b,$$

et la majoration annoncée.

1.3 Nombres premiers

Définition 3. *On appelle nombre premier tout entier $p \geq 2$ dont les seuls diviseurs positifs sont 1 et p.*

Lemma 5. *Soit p un entier ≥ 2. Alors, p est premier si et seulement si p n'est pas le produit de deux entiers strictement plus grands que 1.*

Démonstration : Si l'on a $p = ab$ avec a et b strictement plus grands que 1, alors a divise p et a est distinct de 1 et p, donc p n'est pas premier. Inversement, si p n'est pas premier, il a un diviseur positif a autre que 1 et p. On a alors $p = ab$, où a et b sont ≥ 2.

Proposition 5. *Tout entier $n \geq 1$ est un produit de nombres premiers. En particulier, tout entier $n \geq 2$ possède un diviseur premier.*

Démonstration : On procède par récurrence sur n. Notons $P(n)$ la propriété : n est un produit de nombres premiers. La propriété $P(1)$ est vraie car 1 est le produit vide des nombres premiers. Considérons un entier $n \geq 2$ tel que $P(k)$ soit vraie pour tout entier k tel que $1 \leq k < n$. Il s'agit de démontrer que $P(n)$ est vraie. Tel est le cas si n est premier. Si n n'est pas premier, il existe des entiers a et b strictement plus grands que 1 tels que $n = ab$. On a $1 \leq a < n$ et $1 \leq b < n$, donc $P(a)$ et $P(b)$ sont vraies, d'où le résultat.

Corollaire 3. ***(Euclide).*** *L'ensemble des nombres premiers est infini.*

Démonstration : Supposons que cet ensemble soit fini de cardinal n. Soient $p_1, \ldots, p_n$ ses éléments. Posons $N = 1 + p_1 \ldots p_n$. On a $N \geq 2$, donc N possède un diviseur premier p. L'entier p divise $p_1 \ldots p_n$, d'où l'on déduit que p divise 1, ce qui conduit à une contradiction.

Remarque 3. *1) Ce résultat peut aussi se déduire de la proposition 5 et du fait que deux nombres de Fermat distincts sont premiers entre eux.*

2) Donnons une démonstration, due à Euler, du fait que la somme

$$\sum_p \frac{1}{p}$$

où p parcourt l'ensemble des nombres premiers, est infinie. Cela entraîne évidemment le corollaire 3. Soit N un entier ≥ 1. D'après la proposition 5, tout entier compris entre 1 et N s'écrit comme un produit de nombres premiers $p \leq N$, affectés d'exposants inférieurs ou égaux à la partie entière de $\frac{\log N}{\log p}$. Il en résulte l'inégalité

$$\sum_{n=1}^{N} \frac{1}{n} \leq \prod_{\substack{p \leq N \\ p \text{ premier}}} \left(1 + \frac{1}{p} + \ldots + \frac{1}{p^{t_p}}\right) \text{ où } t_p = \left\lfloor \frac{\log N}{\log p} \right\rfloor,$$

d'où

$$\sum_{n=1}^{N} \frac{1}{n} \leq \prod_{\substack{p \leq N \\ p \text{ premier}}} \sum_{k \geq 0} \frac{1}{p^k} = \prod_{p \leq N} \frac{1}{1 - \frac{1}{p}}.$$

Pour tout nombre premier $p \leq N$, on a

$$-\log\left(1 - \frac{1}{p}\right) = \sum_{k \geq 1} \frac{1}{kp^k} \leq \frac{1}{p} + \frac{1}{p^2}\left(\frac{1}{1 - \frac{1}{p}}\right) \leq \frac{1}{p} + \frac{1}{(p-1)^2}.$$

On obtient

$$\log \sum_{n=1}^{N} \frac{1}{n} \leq \sum_{p \leq N} \frac{1}{p} + \sum_{p \leq N} \frac{1}{(p-1)^2} \leq \sum_{p \leq N} \frac{1}{p} + \sum_{n \leq N} \frac{1}{n^2}.$$

La série $\sum \frac{1}{n}$ étant divergente et la somme $\sum \frac{1}{n^2}$ étant finie, cela implique le résultat.

Lemma 6. ***(Lemme d'Euclide).*** *Soient a, b des entiers naturels et p un nombre premier tels que p divise ab. Alors, p divise l'un des entiers a et b.*

Démonstration. La démonstration qui suit est due à Gauss. Supposons que p ne divise pas a. Il s'agit de montrer que p divise b. Considérons l'ensemble

$$A = \big\{n \geq 1 : p \text{ divise } an\big\}.$$

Il est non vide, car par exemple p appartient à A. Soit m le plus petit élément de A. D'après l'hypothèse faite sur a, on a l'inégalité

$$m \geq 2. \tag{1.6}$$

Soit n un élément de A. Vérifions que m divise n. Il existe des entiers q et r tels que l'on ait $n = mq + r$ avec $0 \leq r < m$. On a l'égalité $an - (am)q = ar$, d'où l'on déduit que p divise ar (car n et m sont dans A). Puisque l'on a $r < m$, r n'est pas dans A, d'où $r = 0$ et notre assertion. Les entiers p et b étant dans A, il en résulte que m divise p et b. L'inégalité (1.6) et le fait que p soit premier entraînent alors $p = m$. Par suite, p divise b.

Corollaire 4. *Si un nombre premier divise un produit d'entiers relatifs, il divise l'un de ces entiers. En particulier, si un nombre premier divise un produit de nombres premiers, il est égal à l'un d'eux.*

Le théorème suivant s'appelle parfois le théorème fondamental de l'arithmétique.

Théorème 2. *Tout entier $n \geq 2$ s'écrit de façon unique sous la forme*

$$n = p_1^{n_1} \dots p_r^{n_r}, \tag{1.7}$$

où les n_i sont des entiers naturels non nuls, et où les p_i sont des nombres premiers vérifiant $p_{i-1} < p_i$ pour tout $i = 2, \dots, r$. On dit que l'égalité (1.7) est la décomposition de n en produit de nombres premiers.

Démonstration : L'assertion d'existence résulte de la proposition 5. Prouvons l'assertion d'unicité. Supposons que l'on ait

$$n = p_1^{n_1} \dots p_r^{n_r} = q_1^{m_1} \dots q_s^{m_s},$$

où les p_i et q_i sont premiers tels que $p_1 < \dots < p_r, q_1 < \dots < q_s$, et où les n_i et m_i sont des entiers naturels non nuls. On déduit du corollaire 4 que l'on a

$$\{p_1, \dots, p_r\} = \{q_1, \dots, q_s\}.$$

Par suite, on a $r = s$. De plus, p_1 est le plus petit élément de $\{p_1, \dots, p_r\}$ et q_1 est le plus petit élément de $\{q_1, \dots, q_r\}$, d'où $p_1 = q_1$, puis $p_i = q_i$ pour tout i. Par ailleurs, s'il existe un indice i tel que $ni \neq m_i$, par exemple $n_i < m_i$, alors p_i divise un produit de nombres premiers tous distincts de lui-même, d'où une contradiction (cor 4).

Remarque 4. *Soit n un entier ≥ 2. Si n n'est pas premier, alors n possède un diviseur premier p tel que $p^2 \leq n$. En effet, si n n'est pas premier, il existe deux entiers a et b strictement plus grands que 1 tels que $n = ab$. Supposons $a \leq b$. Puisque $a \geq 2$, a possède un diviseur premier p. En particulier, p divise n et l'on a $p^2 \leq ap \leq ab = n$.*

Par exemple, 641 est premier, sinon il devrait exister un nombre premier $p < 25$ divisant 641. Or les nombres premiers plus petits que 25 sont $2, 3, 5, 7, 11, 13, 17, 19$ et 23, et aucun d'eux ne divise 641.

Remarque 5. *Soient a et b des entiers ≥ 2. Supposons connues leurs décompositions en facteurs premiers. Dans ce cas, il est immédiat de déterminer leur pgcd d. Pour tout nombre premier p, l'exposant de p dans la décomposition en facteurs premiers de d est le minimum des exposants de p intervenant dans celles de a et b. Cela étant, on ne parvient pas en général à factoriser un entier, ayant plus de deux cent cinquante chiffres décimaux, en produit de nombres premiers. L'efficacité de certains cryptosystèmes est précisément basée sur cette difficulté.*

1.4 La fonction de comptage des nombres premiers

Notons, comme il est d'usage, π la fonction de comptage des nombres premiers. Pour tout réel x positif, $\pi(x)$ est le nombre des nombres premiers inférieurs ou égaux à x. Par exemple, on a

$$\pi(2) = 1, \quad \pi(100) = 25, \quad \pi(105) = 9592, \quad \pi(108) = 5761455, \quad \pi(109) = 50847534.$$

La plus grande valeur connue de la fonction π se situe aujourd'hui aux environs de 10 . Il importe en cryptographie de connaître le comportement de $\pi(x)$ quand x tend vers l'infini, notamment dans l'étude des tests de primalité et des méthodes de factorisation. En analysant des tables de nombres premiers, Gauss et Legendre à la fin du dix-huitième siècle ont observé que si x est "assez grand", la probabilité pour qu'un entier proche de x soit premier semblait être $\frac{1}{\log x}$. Cela les a conduit à conjecturer, sous une forme ou une autre, que $\frac{x}{\log x}$ devait être une bonne approximation asymptotique de $\pi(x)$. Cela s'est avéré exact. J. Hadamard et C. de la Vallée Poussin ont démontré indépendamment en 1896 le résultat suivant.

Théorème 3. ***(Théorème des nombres premiers).*** *Quand x tend vers l'infini, on a*

$$\pi(x) \simeq \frac{x}{\log x}.$$

Sa démonstration relève de la théorie analytique des nombres. La fonction logarithme-intégral

$$\mathrm{Li}(x) = \int_2^x \frac{dt}{\log t}$$

est intimement liée à ce théorème. Lorsque x tend vers l'infini, on vérifie par exemple avec une intégration par parties que l'on a

$$\mathrm{Li}(x) \simeq \frac{x}{\log x}.$$

Les fonctions $\mathrm{Li}(x)$ et $\pi(x)$ sont donc équivalentes quand x tend vers l'infini. C'est d'ailleurs sous cette forme que Gauss avait formulé sa conjecture sur $\pi(x)$. En fait, $\mathrm{Li}(x)$ est une bien meilleure approximation de $\pi(x)$ que $\frac{x}{\log x}$. Par exemple, on a

$$\pi(10^{21}) = 21127269486018731928, \qquad \mathrm{Li}(10^{21}) \equiv 21127269486616126181,3,$$

$$\frac{10^{21}}{\log 10^{21}} \equiv 20680689614440563221,4.$$

Le terme d'erreur $\pi(x) - \mathrm{Li}(x)$ a été l'objet de recherches intensives durant le vingtième siècle, et est encore loin d'avoir livré tous ses secrets. La différence $\pi(x) - \mathrm{Li}(x)$ est liée à l'hypothèse de Riemann concernant les zéros de la fonction zéta. Rappelons que la fonction ζ de Riemann est une fonction holomorphe sur $\mathbb{C} \setminus \{1\}$, ayant un pôle simple en 1, où le résidu est 1, telle que

$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s} \text{ pour } \mathrm{Re}(s) > 1.$$

Dans le demi-plan $\mathrm{Re}(s) > 0$ privé de 1, on a l'égalité

$$\zeta(s) = \frac{s}{s-1} - s \int_1^{+\infty} \frac{\{u\}}{u^{1+s}} du \text{ avec } \{u\} = u - \lfloor u \rfloor,$$

où $\lfloor u \rfloor$ est la partie entière de u. Riemann a proposé cette conjecture, qui est centrale en mathématiques:

Conjecture (Hypothèse de Riemann). *Tous les zéros de la fonction ζ dans la bande critique $0 < \mathrm{Re}(s) < 1$ sont sur la droite $\mathrm{Re}(s) = \frac{1}{2}$.*

Signalons qu'il est relativement facile de démontrer que l'on a $\zeta(s) \neq 0$ pour tout s dans le demi-plan $\mathrm{Re}(s) \geq 1$. Von Koch a établi en 1901 que l'hypothèse de Riemann est équivalente à l'estimation suivante:

$$\pi(x) - \mathrm{Li}(x) = O(\sqrt{x}\log x).^1$$

Plus précisément, l'hypothèse de Riemann équivaut à l'énoncé suivant :

Conjecture. *Pour tout $x \geq 3$, on a*

$$|\pi(x) - \mathrm{Li}(x)| \leq \sqrt{x}\log x.$$

P. Chebyshev, vers le milieu du dix-neuvième siècle, est le premier à avoir établi des résultats importants concernant l'estimation asymptotique de la fonction $\pi(x)$. Il a démontré que $\frac{x}{\log x}$ est effectivement le bon ordre de grandeur de $\pi(x)$, en prouvant les inégalités,

$$0,9\frac{x}{\log x} \leq \pi(x) \leq 1,2\frac{x}{\log x} \text{ pour tout } x \geq 30.$$

Cela implique au passage l'existence d'un nombre premier entre n et $2n$ pour tout entier $n \geq 1$, ce résultat étant connu sous le nom de postulat de Bertrand. De plus, il avait prouvé que si $\frac{\pi(x)\log x}{x}$ possède une limite à l'infini, alors cette limite est 1. Cela étant, la difficulté essentielle du théorème des nombres premiers est d'établir que la limite de $\frac{\pi(x)\log x}{x}$ existe quand x tend vers l'infini. On va se limiter ici à démontrer un énoncé qui ne permet pas de retrouver le postulat de Bertrand, mais qui néanmoins met en évidence l'ordre de grandeur de $\pi(x)$.

Théorème 4. *Pour tout nombre réel $x \geq 2$, on a*

$$\left(\frac{\log 2}{2}\right)\frac{x}{\log x} \leq \pi(x) \leq (9\log 2)\frac{x}{\log x}.$$

Considérons les fonctions arithmétiques traditionnellement notées Λ, Ψ et θ. La fonction Λ de von Mangolt est définie sur $\mathbb{N}$ par

$$\Lambda(n) = \begin{cases} \log p & \text{si } n = p^\alpha \text{ avec } p \text{ premier et } \alpha \geq 1 \\ 0 & \text{sinon.} \end{cases}$$

Les fonctions Ψ et θ sont définies sur $\mathbb{R}$ par

$$\Psi(x) = \sum_{n \leq x} \Lambda(n) \text{ et } \theta(x) = \sum_{\substack{p \leq x \\ p \text{ premier}}} \log p.$$

Pour tout entier $N \geq 1$, on vérifie directement que l'on a

$$\exp(\Psi(N)) = \mathrm{lcm}(1, \ldots, N), \tag{1.8}$$

où $\mathrm{lcm}(1, \ldots, N)$ est le plus petit commun multiple des entiers naturels non nuls inférieurs ou égaux à N.

Démonstration du théorème 4: 1) Démontrons la minoration. Vérifions que l'on a

$$\Psi(2n+1) \geq 2n\log 2 \text{ pour tout } n \in \mathbb{N}. \tag{1.9}$$

[1] Étant données des fonctions f et g définies sur un intervalle de la forme $[a, +\infty[$ à valeurs réelles, la relation

$$f(x) = O(g(x)) \text{ quand } x \text{ tend vers } +\infty,$$

signifie qu'il existe un nombre $M > 0$ tel que pour tout x assez grand, on ait

$$|f(x)| \leq M|g(x)|.$$

Considérons pour cela l'intégrale

$$I = \int_0^1 x^n (1-x)^n dx.$$

D'après la formule du binôme de Newton, I est une somme de nombres rationnels dont les dénominateurs sont tous plus petits que $2n+1$. De plus, on a $I > 0$ (une fonction continue positive sur $[0,1]$, d'intégrale nulle sur $[0,1]$, est nulle). Compte tenu de (1.8), il en résulte que $\exp(\Psi(2n+1))I$ est un entier naturel non nul. Par ailleurs, on a $4x^2 - 4x + 1 = (2x-1)^2 \geq 0$, d'où $x(1-x) \leq \frac{1}{4}$ pour tout $x \in [0,1]$. On en déduit que l'on a

$$I \leq \frac{1}{4^n}.$$

On obtient ainsi les inégalités

$$1 \leq \exp(\Psi(2n+1))I \leq \frac{\exp(\Psi(2n+1))}{4^n},$$

ce qui entraîne (1.9). Soit alors x un nombre réel au moins 6. Soit n l'entier naturel tel que

$$2n-1 \leq x \leq 2n+1.$$

La fonction Ψ étant croissante, on a $\Psi(x) \geq \Psi(2n-1)$. D'après (1.9), on obtient

$$\Psi(x) \geq 2(n-1)\log 2 > (x-3)\log 2.$$

Puisque $x \geq 6$, on a $x - 3 \geq \frac{x}{2}$, d'où l'inégalité

$$\Psi(x) \geq \frac{x \log 2}{2}.$$

Par ailleurs, dans la somme des $\Lambda(n)$ pour $n \leq x$, la contribution relative à chaque nombre premier $p \leq x$ est $r_p \log p$, où p^{r_p} est la plus grande puissance de p inférieure à x. Cette contribution est donc inférieure à $\log x$, ce qui implique

$$\Psi(x) \leq \pi(x) \log x,$$

d'où la minoration annoncée pour $x \geq 6$. Elle vaut en fait dès que $x \geq 2$, car la fonction $f(x) = \frac{x}{\log x}$ est décroissante sur $[2,e]$, croissante sur $[e,+\infty[$, et l'on a

$$\pi(x) = 1 = \frac{\log 2}{2} f(2) \text{ si } x \in [2,e], \quad \pi(x) = 1 \geq \frac{\log 2}{2} f(3) \text{ si } x \in [e,3[,$$

$$\pi(x) \geq 2 \geq \frac{\log 2}{2} f(6) \text{ si } x \in [3,6].$$

2) Passons à la minoration. Vérifions que l'on a

$$\theta(2^r) \leq 2^{r+1} \log 2 \text{ pour tout } r \in \mathbb{N}. \tag{1.10}$$

On a $(2n)! = (n!)^2 C_{2n}^n$, donc pour tout $n \in \mathbb{N}$,

$$\prod_{\substack{n<p\leq 2n \\ p \text{ premier}}} p \text{ divise } C_{2n}^n.$$

D'après l'égalité $(1+1)^{2n} = 2^{2n}$, on a $C_{2n}^n \leq 2^{2n}$. Il en résulte que l'on a

$$\theta(2n) - \theta(n) = \sum_{n<p\leq 2n} \log p \leq 2n \log 2.$$

On obtient alors (1.10) par récurrence. Soit t la partie entière de $\frac{\log x}{\log 2}$. Par définition, on a

$$2^t \leq x < 2^{t+1}.$$

En utilisant (1.10), on en déduit les inégalités

$$\theta(x) \leq \theta(2^{t+1}) \leq 2^{t+2} \log 2 \leq 4x \log 2.$$

En particulier, on a

$$\sum_{\sqrt{x}<p\leq x} \log p \leq 4x \log 2.$$

Cela implique

$$(\pi(x) - \pi(\sqrt{x}))\frac{\log x}{2} \leq 4x \log 2,$$

d'où, vu que $\pi(\sqrt{x})$ est plus petit que $\sqrt{x}$,

$$\pi(x) \leq \frac{8x \log 2}{\log x} + \sqrt{x}.$$

En étudiant les variations de la fonction qui à x associe $\sqrt{x}\log 2 - \log x$, on constate que l'on a

$$\sqrt{x} \leq \frac{x \log 2}{\log x} \text{ dès que } x \geq 16,$$

d'où le résultat dans ce cas. Par ailleurs, pour tout $x \in [2, 16]$, on a x

$$\pi(x) \leq \pi(16) = 6 \leq 9 \log 2 \text{ et } 1 \leq \frac{x}{\log x}.$$

Cela termine la démonstration du théorème.

1.5 Numération en base b

Considérons un entier $b \geq 2$.

Théorème 5. *Soit x un entier naturel non nul. On peut écrire x de manière unique sous la forme*

$$x = a_n b^n + a_{n-1} b^{n-1} + \ldots + a_1 b + a_0, \tag{1.11}$$

où n est un entier naturel, où $a_0, \ldots, a_n$ sont des entiers tels que $0 \leq a_i \leq b-1$ et où a_n est non nul. On dit que $x = a_n a_{n-1} \ldots a_1 a_0$ est l'écriture de x en base b et l'on écrit parfois $x = (a_n \cdots a_0)_b$.

Démonstration : Démontrons l'assertion d'existence. Notons pour cela $P(x)$ la propriété : x possède une écriture de la forme (1.11) comme indiquée dans l'énoncé. La propriété $P(1)$ est vraie, avec $n = 0$ et $a_0 = 1$. Considérons alors un entier $x \geq 2$ et supposons que la propriété $P(k)$ soit vraie pour tout entier k tel que $1 \leq k < x$. Il s'agit de démontrer que $P(x)$ est vraie. Tel est le cas si l'on a $x < b$, en prenant $n = 0$ et $a_0 = x$ dans (1.11).

Supposons donc $x \geq b$. Il existe des entiers q et a_0 tels que l'on ait $x = bq + a_0$ avec $0 \leq a_0 < b$. L'inégalité $x \geq b$ entraîne $q \geq 1$. Par suite, on a $q < bq \leq x$. La propriété $P(q)$ étant vraie, il existe un entier $n \geq 1$ tel que l'on ait $q = a_n b^{n-1} + \cdots + a_2 b + a_1$, où les a_i sont entiers vérifiant les inégalités $0 \leq a_i \leq b-1$ et où $a_n \neq 0$. L'égalité $x = bq + a_0$ entraîne alors que $P(x)$ est vraie, d'où l'assertion d'existence.

Prouvons l'assertion d'unicité. On remarque pour cela que l'entier n intervenant dans (1.11) vérifie les inégalités

$$b^n \leq x < b^{n+1}.$$

En effet, la première inégalité est immédiate et le fait que les a_i soient compris entre 0 et $b-1$ entraîne que l'on a

$$x \leq (b-1)(b^n + b^{n-1} + \ldots + b + 1) = b^{n+1} - 1 < b^{n+1}.$$

Il en résulte que n est la partie entière de $\frac{\log x}{\log b}$. Tout revient donc à démontrer que si l'on a

$$x = a_n b^n + a_{n-1} b^{n-1} + \cdots + a_1 b + a_0 = c_n b^n + c_{n-1} b^{n-1} + \cdots + c_1 b + c_0,$$

avec $a_n c^n \neq 0$ et $0 \leq a_i, c_i \leq b-1$, alors $a_i = c_i$ pour tout i. Vu le caractère d'unicité du reste de la division euclidienne de x par b, on a $a_0 = c_0$. On obtient ensuite l'assertion en procédant par récurrence finie sur les indices des coefficients.

Remarque 6. *Pour tout entier $x \geq 1$, le nombre de chiffres intervenant dans l'écriture de x en base b est $1 + \left\lfloor \frac{\log x}{\log b} \right\rfloor$.*

Exemple. On vérifie que l'on a $101 = 2^6 + 2^5 + 2^2 + 1$, de sorte que l'écriture de 101 en base 2 est 1100101 i.e. on a $101 = (1100101)_2$. Donnons une application de ce théorème.

Calcul "rapide" de la puissance d'un entier. L'existence de l'écriture en base 2 des entiers permet d'accélérer le calcul de la puissance d'un entier. Plus précisément, considérons deux entiers $x \geq 1$ et $n \geq 1$. Afin de calculer x^n, il faut a priori effectuer $n-1$ multiplications. En fait, la détermination de l'écriture de n en base 2 permet de calculer x^n en effectuant au plus la partie entière de

$$\frac{2 \log n}{\log 2}$$

multiplications. En effet, soit

$$n = 2^{i_k} + 2^{i_{k-1}} + \cdots + 2^{i_1} + 2^{i_0},$$

le développement de n en base 2 avec $i_0 < i_1 \cdots < i_k$. On a l'égalité

$$x^n = x^{2^{i_k}} \times x^{2^{i_{k-1}}} \times \ldots \times x^{2^{i_1}} \times x^{2^{i_0}}.$$

On peut effectuer le calcul de $x^{2^{i_k}}$ avec i_k multiplications, ce qui fournit aussi le calcul des autres termes $x^{2^{i_j}}$ pour $0 \leq j \leq k$. On peut donc calculer x^n avec $i_k + k$ multiplications. Par ailleurs, on a

$$k \leq i_k \text{ et } 2^{i_k} \leq n \text{ i.e. } i_k \leq \frac{\log n}{\log 2}.$$

On obtient

$$i_k + k \leq \frac{2 \log n}{\log 2}.$$

d'où notre assertion.

Exemple On a vu plus haut que l'on a $101 = 2^6 + 2^5 + 2^2 + 1$. Le calcul de x^{101} peut donc se faire avec neuf multiplications, au lieu de cent a priori.

1.6 Le théorème chinois

Pour tout entier $n \geq 1$, rappelons que $\mathbb{Z}/n\mathbb{Z}$ désigne l'anneau des entiers modulo n.

Théorème 6. ***(Théorème chinois).*** *Soient m et n des entiers naturels non nuls premiers entre eux. L'application*

$$f : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z},$$

définie pour tout $a \in \mathbb{Z}$ par l'égalité

$$f(a) = (a + m\mathbb{Z}, a + n\mathbb{Z}),$$

est un morphisme d'anneaux surjectif, de noyau $mn\mathbb{Z}$. En particulier, les anneaux $\mathbb{Z}/mn\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ sont isomorphes, via l'application qui à tout élément $a + mn\mathbb{Z}$ de $\mathbb{Z}/mn\mathbb{Z}$ associe le couple $(a + m\mathbb{Z}, a + n\mathbb{Z})$.

Remarque 7. *Le contenu essentiel de cet énoncé réside dans le fait que f soit une application surjective de $\mathbb{Z}$ sur $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Autrement dit, étant donnés des entiers relatifs a et b, il existe $c \in \mathbb{Z}$ tel que l'on ait*

$$c = a \bmod m \text{ et } c = b \bmod n. \tag{1.12}$$

Démonstration : Il résulte directement de la définition de la structure d'anneau produit sur $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ que f est un morphisme d'anneaux. Vérifions que l'on a

$$\mathrm{Ker}(f) = mn\mathbb{Z}.$$

Si a est un élément de $\mathrm{Ker}(f)$, on a $(a + m\mathbb{Z}, a + n\mathbb{Z}) = (m\mathbb{Z}, n\mathbb{Z})$, autrement dit, on a $a = 0 \bmod m$ et $a = 0 \bmod n$. Puisque m et n sont premiers entre eux, on en déduit que mn divise a, i.e. que $a \in mn\mathbb{Z}$. Inversement, si a est dans $mn\mathbb{Z}$, alors a est divisible par m et n, donc a est dans $\mathrm{Ker}(f)$, d'où l'assertion.

Prouvons que f est surjectif. Considérons pour cela un élément $(a + m\mathbb{Z}, b + n\mathbb{Z})$ de $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Puisque m et n sont premiers entre eux, il existe des entiers u et v tels que l'on ait

$$mu + nv = 1. \tag{1.13}$$

Posons alors

$$c = b(mu) + a(nv). \tag{1.14}$$

On vérifie que l'on a les congruences $c = a \bmod m$ et $c = b \bmod n$, autrement dit que l'on a $f(c) = (a + m\mathbb{Z}, b + n\mathbb{Z})$, d'où l'assertion, et le résultat.

Remarque 8. *La démonstration précédente est effective, au sens où si a et b sont deux entiers relatifs donnés, elle permet d'expliciter un entier c vérifiant les congruences (1.12). En effet, il suffit pour cela de déterminer des entiers u et v vérifiant l'égalité (1.13), ce que l'on peut faire en utilisant par exemple l'algorithme d'Euclide. On peut alors prendre comme entier c celui défini par l'égalité (1.14). Il est unique modulo $mn\mathbb{Z}$.*

Exemple Soit n un entier naturel impair. Notons r le nombre de ses diviseurs premiers. Soit S l'ensemble des solutions dans l'anneau $\mathbb{Z}/n\mathbb{Z}$ de l'équation

$$x^2 = 1.$$

En notant $|S|$ le cardinal de S, vérifions que l'on a

$$|S| = 2^r. \tag{1.15}$$

Soit $n = p_1^{n_1} \cdots p_r^{n_r}$ la décomposition de n en produits de nombres premiers. Soit

$$f : \mathbb{Z}/n\mathbb{Z} \to \prod_{i=1}^{r} \mathbb{Z}/p_i^{n_i}\mathbb{Z},$$

le morphisme d'anneaux défini par $f(x + n\mathbb{Z}) = (x + p_!^{n_1}\mathbb{Z}, \cdots, x + p_r^{n_r}\mathbb{Z})$. D'après le théorème chinois, c'est un isomorphisme. Posons

$$T = \{(\varepsilon_1 + p1^{n_1}\mathbb{Z}, \ldots, \varepsilon_r + p_r^{n_r}\mathbb{Z}) : \varepsilon_i = \pm 1 \text{ pour } i = 1, \cdots, r\}.$$

Vérifions que l'on a

$$S = f^{-1}(T). \tag{1.16}$$

Soit $x + n\mathbb{Z}$ un élément de S. Pour tout $i = 1, \ldots, r$, on a $x^2 = 1 \bmod p_i^{n_i}$. Le pgcd de $x - 1$ et $x + 1$ est 1 ou 2. Puisque n est impair, $p_i^{n_i}$ divise donc $x - 1$ ou bien $x + 1$. Par suite, $f(x + n\mathbb{Z})$ est dans T, et S

est contenu dans $f^{-1}(T)$. Inversement, si $x + n\mathbb{Z}$ est dans $f^{-1}(T)$, on a $x^2 = 1 \bmod p_i^{n_i}$ pour tout i. Cela implique $x^2 = 1 \bmod n$, autrement dit, $x + n\mathbb{Z}$ est dans S, d'où (1.16). Puisque T est de cardinal 2^r (les p_i sont impairs), il en est de même de S. Cela établit l'égalité (1.15).

Afin d'expliciter S, on est donc amené à résoudre les systèmes de r congruences

$$x = \varepsilon_1 \bmod p_1^{n_1}, \cdots, x = \varepsilon_r \bmod p_r^{n_r},$$

pour les 2^r systèmes de signes $(\varepsilon_1, \ldots, \varepsilon_r)$. Il suffit en fait d'en résoudre 2^{r-1} par un choix convenable de systèmes de signes, en prenant ensuite les solutions opposées à celles déjà obtenues.

Par exemple, si $n = 735$, l'ensemble S est formé des classes modulo n des entiers $\pm 1, \pm 146, \pm 244$ et ± 344. Il convient de remarquer que la résolution de l'équation $x^2 = 1$ dans $\mathbb{Z}/n\mathbb{Z}$ nécessite, a priori, la connaissance de la factorisation de n en produit de nombres premiers. Si l'on savait résoudre cette équation sans utiliser cette factorisation, il serait alors facile de trouver la factorisation de n. En effet, si a est un entier tel que $a^2 = 1 \bmod n$ et $a \neq \pm 1 \bmod n$, le calcul du pgcd de $a+1$ (ou $a-1$) avec n fournit un diviseur non trivial de n. Le problème de la factorisation des entiers serait ainsi résolu, et la sécurité de nombreux cryptosystèmes serait complètement remise en cause. On aura l'occasion de revenir sur ce problème.

1.7 La fonction indicatrice d'Euler

Il s'agit de la fonction $\varphi : \mathbb{N}* \to \mathbb{N}$ définie comme suit.

Définition 4. ***(Fonction indicatrice d'Euler).*** *Pour tout $n \geq 1$, l'entier $\varphi(n)$ est le nombre des entiers compris entre 1 et n, et premiers avec n. Autrement dit, $\varphi(n)$ est le nombre des entiers k pour lesquels on a*

$$1 \leq k \leq n \text{ et } \gcd(k, n) = 1.$$

Par exemple, on a $\varphi(1) = 1, \varphi(2) = 1, \varphi(3) = 2$, et pour tout nombre premier p, on a $\varphi(p) = p - 1$. Plus généralement :

Lemma 7. *Pour tout nombre premier p et tout entier $r \geq 1$, on a*

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

Démonstration : Il y a p^{r-1} entiers multiples de p entre 1 et p^r, d'où l'assertion.

Explicitons $\varphi(n)$ pour tout $n \geq 1$. On va voir en particulier que $\frac{\varphi(n)}{n}$ ne dépend que de l'ensemble des diviseurs premiers de n. Considérons pour cela le groupe $(\mathbb{Z}/n\mathbb{Z})^*$ formé des éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$. Rappelons d'abord l'énoncé suivant :

Lemma 8. *Soit n un entier ≥ 1. Soient a un entier et $\bar{a}$ sa classe modulo $n\mathbb{Z}$. Alors, $\bar{a}$ est inversible dans l'anneau $\mathbb{Z}/n\mathbb{Z}$ si et seulement si a et n sont premiers entre eux. Autrement dit, on a*

$$(\mathbb{Z}/n\mathbb{Z})^* = \{\bar{a} : 1 \leq a \leq n \text{ et } \gcd(a, n) = 1\}.$$

Démonstration : Supposons $\bar{a}$ inversible. Il existe $b \in \mathbb{Z}$ tel que l'on ait $ab = 1 \bmod n$, autrement dit, il existe $c \in \mathbb{Z}$ tel que $ab + nc = 1$, ce qui prouve que a et n sont premiers entre eux. Inversement, il existe des entiers u et v tels que l'on ait $au + nv = 1$. Ainsi $\bar{a}$ est inversible, d'inverse la classe de u modulo n.

Corollaire 5. *L'ordre de $(\mathbb{Z}/n\mathbb{Z})^*$ est $\varphi(n)$.*

Corollaire 6. *L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.*

Démonstration : L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si tous ses éléments non nuls sont inversibles. Par suite, $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si $\varphi(n) = n - 1$, ce qui implique l'assertion.

Corollaire 7. *Soient m et n des entiers naturels non nuls premiers entre eux. On a*

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

Démonstration : Les entiers m et n étant premiers entre eux, les anneaux $\mathbb{Z}/mn\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ sont isomorphes (th. 6). Les groupes des éléments inversibles de ces anneaux ont donc le même ordre. Le corollaire 5 et le lemme 7 entraînent alors le résultat.

Théorème 7. *Soit n un entier ≥ 1. On a l'égalité*

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right), \tag{1.17}$$

où p parcourt l'ensemble des diviseurs premiers de n.

Démonstration : On peut supposer $n \geq 2$. Soit $\{p_1, \ldots, p_r\}$ l'ensemble des diviseurs premiers de n. Soit

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

la décomposition en facteurs premiers de n. D'après le corollaire 7, on a

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

Par ailleurs, on a (lemme 7)

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

d'où l'égalité (1.17).

Indiquons quelques propriétés de la fonction φ.

Corollaire 8. *Pour tout $n \geq 3$, l'entier $\varphi(n)$ est pair.*

Démonstration : Compte tenu de l'égalité (1.17), si n possède un diviseur premier impair p, alors $p - 1$ est pair, et il en est donc de même de $\varphi(n)$. Si n est une puissance de 2, disons $n = 2^r$ avec $r \geq 2$, alors $\varphi(n) = 2^{r-1}$.

Corollaire 9. *Soient m et n des entiers naturels non nuls tels que m divise n. Alors $\varphi(m)$ divise $\varphi(n)$.*

Démonstration : Soit P_m (resp. P_n) l'ensemble des diviseurs premiers de m (resp. de n). On a les égalités (th. 7)

$$\frac{\varphi(n)}{\varphi(m)} = \frac{n}{m} \prod_{p \in P_n - P_m} \left(1 - \frac{1}{p}\right). \tag{1.18}$$

Pour tout nombre premier $p \in P_n - P_m$, p divise n sans diviser m, donc p divise $\frac{n}{m}$. Il en résulte que le second membre de l'égalité (1.18) est un entier.

L'implication réciproque de ce corollaire est fausse, comme le montre les égalités $\varphi(3) = \varphi(4) = 2$. Remarquons que l'énoncé précédent peut aussi se déduire du résultat suivant, qui est une conséquence du théorème chinois :

Lemma 9. *Soient m et n des entiers naturels non nuls tels que m divise n. L'application $f : (\mathbb{Z}/n\mathbb{Z})^* \to (\mathbb{Z}/m\mathbb{Z})^*$ définie par $f(a + n\mathbb{Z}) = a + m\mathbb{Z}$, est un morphisme de groupes surjectif de $(\mathbb{Z}/n\mathbb{Z})^*$ sur $(\mathbb{Z}/m\mathbb{Z})^*$.*

Démonstration : On remarque d'abord que f est bien définie. Le fait que f soit un morphisme de groupes résulte directement de la définition. On écrit ensuite n sous la forme $n = m'r$, où m et m' ont les mêmes facteurs premiers et où r est premier à m'. L'entier m divise m' et r est premier à m. Soit $d + m\mathbb{Z}$ un élément de $(\mathbb{Z}/m\mathbb{Z})^*$. D'après le théorème chinois, il existe un entier a tel que

$$a = d \bmod m \text{ et } a = 1 \bmod r.$$

Vérifions que a est premier à n. Supposons qu'il existe un nombre premier p qui divise a et n. Alors, p ne divise pas r, donc p divise m'. Par suite, p divise m et d, ce qui contredit le fait que d et m sont. premiers entre eux. On a ainsi $f(a+n\mathbb{Z}) = d+m\mathbb{Z}$, d'où l'assertion.

Lemma 10. *Pour tout $n \geq 1$, on a l'égalité*

$$n = \sum_{d|n} \varphi(d),$$

où d parcourt l'ensemble des diviseurs de n.

Démonstration : Considérons l'ensemble $F = \{\frac{1}{n}, \frac{2}{n}, \cdots, \frac{n-1}{n}, \frac{n}{n} = 1\}$. Pour tout diviseur d de n, posons $F_d = \{d : 1 \leq a \leq d \text{ et } \gcd(a,d) = 1\}$. L'ensemble F est la réunion disjointe des F_d, d'où le résultat vu que le cardinal de F est n et que celui de F_d est $\varphi(d)$.

Terminons ce paragraphe en citant l'une des nombreuses conjectures concernant la fonction φ. Celle-ci a été proposée par Carmichael en 1922 :

Conjecture. Quel que soit $n \geq 1$, il existe un entier $m \neq n$ tel que $\varphi(m) = \varphi(n)$.

C'est évident si n est impair, vu que l'on a dans ce cas $\varphi(2n) = \varphi(n)$, ou bien si $n = 2m$ avec m impair, car on a alors $\varphi(n) = \varphi(m)$. Toute la difficulté concerne les entiers n divisibles par 4. On sait que s'il existe un entier n contredisant cette conjecture, il doit avoir plus de 10^7 chiffres décimaux. Signalons cependant qu'il existe des entiers n pour lesquels il n'existe pas d'entiers impairs m tels que $\varphi(m) = \varphi(n)$. Tel est par exemple le cas de $n = 2^9 \times 257^2$. Notons par ailleurs, qu'un entier $a \geq 1$ étant donné, il n'existe qu'un nombre fini d'entiers m tels que $\varphi(m) = a$ (c'est une conséquence du théorème 7). En fait, sans en faire la liste, très peu de résultats ont été démontrés sur cette conjecture.

1.8 Le théorème d'Euler

Euler a démontré cet énoncé en 1760 :

Théorème 8. *Soit n un entier naturel non nul. Pour tout entier a premier avec n, on a*

$$a^{\varphi(n)} = 1 \bmod n. \tag{1.19}$$

Pour le vérifier, on peut utiliser directement le théorème de Lagrange, ou bien le cas particulier "abélien" de ce théorème dont la démonstration se simplifie alors notablement.

Proposition 6. *Soit G un groupe abélien fini d'ordre n, d'élément neutre e. Pour tout $x \in G$, on a $x^n = e$.*

Démonstration : Soit x un élément de G. L'application qui à $g \in G$ associe gx est une bijection de G. On en déduit l'égalité

$$\prod_{g\in G} gx = \prod_{g\in G} g.$$

Il convient ici de noter que les produits ne dépendent pas de l'ordre choisi des éléments car G est abélien. On obtient

$$x^n \prod_{g\in G} g = \prod_{g\in G} g,$$

ce qui conduit à l'égalité $x^n = e$.

On obtient alors la congruence (1.19), en prenant $G = (\mathbb{Z}/n\mathbb{Z})^*$ qui est d'ordre $\varphi(n)$.

Corollaire 10. ***(Petit théorème de Fermat).*** *Soit p un nombre premier. Pour tout entier a non divisible par p, on a*

$$a^{p-1} = 1 \bmod p.$$

En particulier, pour tout entier a, on a $a^p = a \bmod p$.

Démonstration : Cela résulte de l'égalité $\varphi(p) = p - 1$.

Exemples. 1) Vérifions que l'écriture décimale de 3^{1000}, qui possède quatre cent soixante dix huit chiffres, se termine par 01. Il s'agit de déterminer l'entier a compris entre 0 et 99 tel que $3^{1000} = a \bmod 100$. On a $\varphi(100) = 40$. D'après le théorème d'Euler, on obtient $3^{40} = 1 \bmod 100$. Puisque $1000 = 40 \times 25$, on a donc $3^{1000} = 1 \bmod 100$, d'où $a = 1$.

2) Vérifions que l'écriture décimale de 2^{1000}, qui possède trois cent deux chiffres, se termine par 76. Le raisonnement précédent ne s'applique pas directement (car 2 n'est pas premier avec 100). On a $2^{1000} = 0 \bmod 4$. L'idée est alors de déterminer la congruence de 2^{1000} modulo 25 et d'utiliser le théorème chinois. On a $2^{20} = 1 \bmod 25$ (théorème d'Euler), d'où $2^{1000} = 1 \bmod 25$. Il en résulte que $2^{1000} = -24 \bmod 100$ (cf. le théorème chinois), d'où l'assertion.

Les applications du théorème d'Euler sont innombrables, on en verra notamment en cryptographie. Donnons ici une illustration de ce théorème, en prouvant un résultat concernant la non primalité des entiers de la forme $2^{2^n} + k$ où k est un entier.

Proposition 7. ***(Schinzel).*** *Soit k un entier relatif distinct de 1. Il existe une infinité d'entiers n tels que $2^{2^n} + k$ ne soit pas un nombre premier.*

Démonstration : On peut supposer k impair. Soit a un entier naturel. Il suffit de prouver l'existence d'un entier n tel que $2^{2^n} + k$ ne soit pas premier et que $2^{2^n} + k > a$. Puisque k est distinct de 1, il existe $s \in \mathbb{N}$ et un entier impair h tels que

$$k - 1 = 2^s h.$$

Soit t un entier naturel tel que l'on ait

$$p = 2^{2^t} + k > a \text{ et } t > s.$$

On peut supposer que p est un nombre premier. Il existe un entier impair h_1 tel que

$$p - 1 = 2^s h_1.$$

D'après le théorème d'Euler, on a

$$2^{\varphi(h_1)} = 1 \bmod h_1,$$

d'où l'on déduit la congruence

$$2^{s+\varphi(h_1)} = 2^s \bmod p - 1.$$

Puisque l'on a $t > s$, on obtient

$$2^{t+\varphi(h_1)} = 2^t \bmod p - 1.$$

L'entier p étant premier impair, on a $2^{p-1} = 1 \bmod p$. Il en résulte que

$$2^{2^{t+\varphi(h_1)}} + k = 0 \bmod p.$$

L'entier $2^{2^{t+\varphi(h_1)}} + k$, qui est strictement plus grand que p, n'est donc pas premier. Il est plus grand que a, d'où le résultat.

On conjecture que cet énoncé est aussi vrai si $k = 1$, mais on ne sait pas le démontrer. Pour autant, les seuls entiers n connus tels que F_n soit premier sont ceux inférieurs ou égaux à 4, et on pense qu'il n'y a qu'un nombre fini d'entiers F_n premiers. Par exemple, F_5 est divisible par 641. On le constate en écrivant que l'on a

$$641 = 5^4 + 2^4 = 5.2^7 + 1,$$

d'où $5.2^7 = -1 \bmod 641$, puis $5^4.2^{28} = 1 \bmod 641$ et $2^{32} + 1 = 0 \bmod 641$.

1.9 Groupes cycliques

Les groupes cycliques sont utilisés en cryptographie notamment en ce qui concerne le problème du logarithme discret. Rappelons leurs principales propriétés.

Soit G un groupe fini d'ordre n, d'élément neutre e. Il est dit cyclique s'il possède un élément d'ordre n. Dans ce cas, un tel élément s'appelle un générateur de G. Un groupe cyclique est en particulier abélien. Si x est un générateur de G, on a

$$G = \{e, x, \ldots, x^{n-1}\}.$$

Par exemple, pour tout $n \geq 1$, le groupe additif $\mathbb{Z}/n\mathbb{Z}$ est cyclique d'ordre n. La classe de 1 en est un générateur. À isomorphisme près, c'est le seul groupe cyclique d'ordre n. On utilisera le fait que pour tout entier k, et tout élément y de G (cyclique ou non) d'ordre m, l'ordre de y^k est

$$\frac{m}{\gcd(m,k)}.$$

En effet, si $d = \gcd(m,k)$, on a $(y^k)^{\frac{m}{d}} = (y^m)^{\frac{k}{d}} = e$. Par ailleurs, si u est un entier tel que $(y^k)^u = e$, alors m divise uk, donc $\frac{m}{d}$ divise $\frac{uk}{d}$. Les entiers $\frac{m}{d}$ et $\frac{k}{d}$ étant premiers entre eux, $\frac{m}{d}$ divise u, d'où l'assertion.

Théorème 9. *Soit G un groupe cyclique d'ordre n.*

1) Tout sous-groupe de G est cyclique.

2) Pour tout diviseur $d \geq 1$ de n, l'ensemble

$$H_d = \{a \in G : a^d = e\}$$

est un sous-groupe de G d'ordre d.

3) L'application qui à d associe H_d est une bijection entre l'ensemble des diviseurs de n et l'ensemble des sous-groupes de G. En particulier, pour tout diviseur d de n, H_d est l'unique sous-groupe d'ordre d de G.

Démonstration : Soit x un générateur de G.

1) Soit H un sous-groupe de G. Considérons le plus petit entier $\delta \geq 1$ tel que x^δ appartienne à H. Le sous-groupe de G engendré par x^δ est contenu dans H. Montrons qu'il est égal à H. Soit y un élément de H. Il existe un entier m tel que l'on ait $y = x^m$.

Par ailleurs, il existe des entiers q et r tels que l'on ait $m = \delta q + r$, avec $0 \leq r < \delta$. On en déduit que x^r est dans H, et donc que r est nul. D'où $m = \delta q$, et $y = (x^\delta)^q$ appartient au sous-groupe de G engendré par x^δ, d'où l'assertion.

2) Soit d un diviseur ≥ 1 de n. L'ensemble H_d est un sous-groupe de G. En effet, e appartient à H_d, et pour tous $a, b \in H_d$, on a

$$(ab)^d = a^d b^d = e \text{ et } (a^{-1})^d = (a^d)^{-1} = e,$$

de sorte que ab et a^{-1} sont dans H_d. On a

$$(x^{\frac{n}{d}})^d = x^n = e,$$

donc $x^{\frac{n}{d}}$ appartient à H_d . L'élément $x^{\frac{n}{d}}$ étant d'ordre d, l'ordre de H_d est divisible par d. Par ailleurs, H_d est cyclique (assertion 1). Si y est un générateur de H_d, on a $y^d = e$, donc l'ordre de H_d, qui est celui de y, divise d. Ainsi, H_d est d'ordre d.

3) Soit H un sous-groupe de G. Vérifions que l'on a $H = H_d$ où d est l'ordre de H, ce qui prouvera que l'application considérée est une surjection. Pour tout $z \in H$ on a $z^d = e$, donc H est contenu dans H_d. Puisque H_d est d'ordre d, on a donc $H = H_d$. Il reste à montrer que cette application est une injection : si d et d' sont deux diviseurs de n tels que $H_d = H_{d'}$, vu que H_d et $H_{d'}$ ont le même ordre, on a $d = d'$.

Corollaire 11. *Soit G un groupe cyclique d'ordre n. Pour tout entier $k \geq 1$, l'ensemble*

$$\{a \in G : a^k = e\}$$

est un sous-groupe de G d'ordre $\gcd(k, n)$.

Démonstration : Soit k un entier naturel non nul. Posons $H = \{a \in G : a^k = e\}$ et $d = \gcd(k, n)$. Le fait que H soit un sous-groupe de G se vérifie comme ci-dessus. Par ailleurs, en utilisant la propriété de Bézout, on constate directement que $H = H_d$, d'où le résultat (th. 9).

Exemple. Tout groupe fini d'ordre un nombre premier est cyclique. Ses éléments autres que l'élément neutre en sont des générateurs.

Une question importante concerne la description des générateurs d'un groupe cyclique. En particulier, combien y a-t-il de générateurs dans un groupe cyclique d'ordre n ?

Théorème 10. *Soient G un groupe cyclique d'ordre n et x un générateur de G.*
1) L'ensemble des générateurs de G est

$$\{x^k : 1 \leq k \leq n \text{ et } \gcd(k, n) = 1\}.$$

En particulier, G possède exactement $\varphi(n)$ générateurs.
2) Pour tout diviseur d de n, il y a exactement $\varphi(d)$ éléments d'ordre d dans G.

Démonstration : 1) On a $G = \{x, \cdots, x^{n-1}, x^n\}$. Pour tout k compris entre 1 et n, l'ordre de x^k est $\frac{n}{\gcd(n,k)}$. Par suite, x^k est d'ordre n si et seulement si on a $\gcd(n, k) = 1$.

2) Il existe un unique sous-groupe H_d d'ordre d de G, à savoir l'ensemble des $a \in G$ tels que $a^d = e$ (th. 9). L'ensemble des éléments d'ordre d de G est donc contenu dans H_d, et cet ensemble est formé des générateurs de H_d. Puisque H_d est cyclique, il a exactement $\varphi(d)$ générateurs.

Exemple. Pour tout $n \geq 1$, l'ensemble des générateurs du groupe additif $\mathbb{Z}/n\mathbb{Z}$ est formé des classes d'entiers premiers avec n.

Vérifions le lemme suivant que l'on utilisera plus loin.

Lemma 11. *Soient H et K des groupes cycliques. Le groupe produit $H \times K$ est cyclique si et seulement si les ordres de H et K sont premiers entre eux.*

Démonstration : Notons m et n les ordres de H et K respectivement. Pour tout $(a, b) \in H \times K$, l'ordre de (a, b) est le plus petit commun multiple des ordres de a et b. Supposons m et n premiers entre eux. Si x est un générateur de H et y un générateur de K, l'ordre de (x, y) est donc mn et $H \times K$ est cyclique. Inversement, supposons $H \times K$ cyclique. Soit (a, b) un de ses générateurs. Les éléments a et b sont alors respectivement des générateurs de H et K. Par suite, a est d'ordre m et b est d'ordre n. Il en résulte que mn est le plus petit commun multiple de m et n, d'où $\gcd(m, n) = 1$.

1.10 Le groupe $(\mathbb{Z}/p^n\mathbb{Z})^*$ où p est premier impair

On va démontrer qu'il est cyclique pour tout $n \geq 1$. Commençons par traiter le cas où $n = 1$, autrement dit, par établir que $(\mathbb{Z}/p\mathbb{Z})^*$ est un groupe cyclique.

Lemma 12. *Soit G un groupe fini d'ordre m, d'élément neutre e. Supposons que pour tout diviseur d de m, l'ensemble des éléments $x \in G$ tels que $x^d = e$ soit de cardinal au plus d. Alors G est cyclique.*

Démonstration : Soient d un diviseur de m et A_d l'ensemble des éléments de G d'ordre d. Vérifions que le cardinal de A_d est 0 ou $\varphi(d)$. Supposons pour cela qu'il existe un élément $x \in G$ d'ordre d. Soit H le sous-groupe de G engendré par x. Il est d'ordre d. D'après l'hypothèse faite, tout élément $y \in G$ tel que $y^d = e$ appartient donc à H. En particulier, les éléments d'ordre d de G sont ceux de H. Puisque H est cyclique d'ordre d, il y en a $\varphi(d)$ (th. 10), d'où l'assertion. Par ailleurs, G est la réunion disjointe des A_d où d parcourt l'ensemble des diviseurs de m. S'il existait un diviseur d de m tel que A_d soit vide, on aurait ainsi (lemme 10)

$$|G| < \sum_{d|m} \varphi(d) = m,$$

d'où une contradiction. En particulier, G a un élément d'ordre m i.e. G est cyclique.

Proposition 8. *Pour tout nombre premier p, le groupe $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique.*

Démonstration : Si p est premier, l'anneau $\mathbb{Z}/p\mathbb{Z}$ est un corps commutatif. Pour tout entier $d \geq 1$, le polynôme $X^d - 1 \in (\mathbb{Z}/p\mathbb{Z})[X]$ a donc au plus d racines dans $(\mathbb{Z}/p\mathbb{Z})^*$. Le lemme précédent entraîne alors le résultat.

On ne connaît pas de procédé, autre que la recherche exhaustive, permettant de déterminer un générateur de $(\mathbb{Z}/p\mathbb{Z})^*$. Citons à ce propos la conjecture d'Artin :

Conjecture. Soit a un entier relatif distinct de -1 qui n'est pas un carré. Il existe une infinité de nombres premiers p tels que la classe de a soit un générateur de $(\mathbb{Z}/p\mathbb{Z})^*$.

Signalons que conjecturalement, pour tout nombre premier $p \geq 3$ il existe un entier naturel $a < 2(\log p)^2$ tel que $a + p\mathbb{Z}$ soit un générateur de $(\mathbb{Z}/p\mathbb{Z})^*$.

Avant de démontrer le résultat annoncé établissons le lemme suivant.

Lemma 13. *Soient p un nombre premier impair et a un entier. Pour tout $n \in \mathbb{N}$, on a*

$$(1 + pa)^{p^n} = 1 + p^{n+1}a \bmod p.$$

Démonstration : On procède par récurrence sur n. Cette congruence est vraie si $n = 0$. Supposons qu'elle le soit pour un entier $n \in \mathbb{N}$. Puisque p divise C_p^j pour $j = 1, \ldots, p-1$, on obtient

$$(1 + pa)^{p^{n+1}} = (1 + p^{n+1}a)^p \bmod p^{n+3}.$$

Par ailleurs, on a

$$(1 + p^{n+1}a)^p = 1 + p^{n+2}a + C_p^2 p^{2n+2}a^2 \bmod p^{n+3}.$$

On a $p \neq 2$, donc p divise C_p^2 et $C_p^2 p^{2n+2}a^2$ est divisible par p^{n+3} (y compris si $n = 0$). Cela entraîne le résultat.

Théorème 11. *Soient p un nombre premier impair et n un entier ≥ 1. Le groupe $(\mathbb{Z}/p^n\mathbb{Z})^*$ est cyclique d'ordre $p^{n-1}(p-1)$. Plus précisément, soit a un entier naturel tel que $a + p\mathbb{Z}$ soit un générateur de $(\mathbb{Z}/p\mathbb{Z})^*$.*

1. *Si $a^{p-1} \neq 1 \bmod p^2$, alors $a + p^n\mathbb{Z}$ est un générateur de $(\mathbb{Z}/p^n\mathbb{Z})^*$.*
2. *Si $a = 1 \bmod p^2$, alors $(a + p) + p^n\mathbb{Z}$ est un générateur de $(\mathbb{Z}/p^n\mathbb{Z})^*$.*

Démonstration : Vérifions d'abord que l'on a

$$a^{p-1} \neq 1 \bmod p^2 \text{ ou bien } (a + p)^{p-1} \neq 1 \bmod p^2. \tag{1.20}$$

Supposons pour cela $a^{p-1} = 1 \bmod p^2$. On a

$$(a + p)^{p-1} = a^{p-1} + p(p-1)a^{p-2} \bmod p^2,$$

d'où la congruence

$$(a + p)^{p-1} = 1 + p(p-1)a^{p-2} \bmod p^2.$$

Puisque p ne divise pas a, on en déduit que $(a + p)^{p-1} - 1$ n'est pas divisible par p^2, d'où la condition (1.20). Soit alors x l'un des entiers a et $a + p$ pour lequel on a

$$x^{p-1} \neq 1 \bmod p^2. \tag{1.21}$$

Tout revient à démontrer que $x + p^n\mathbb{Z}$ est un générateur de $(\mathbb{Z}/p^n\mathbb{Z})^*$. Soit r l'ordre de $x + p^n\mathbb{Z}$. D'après l'hypothèse faite sur a, l'ordre de x modulo p est $p - 1$. La congruence

$$x^r = 1 \bmod p$$

entraîne que $p-1$ divise r. Par ailleurs, r divise $\varphi(p^n) = p^{n-1}(p-1)$. Il existe donc un entier s tel que

$$r = p^s(p-1) \text{ avec } 0 \leq s \leq n-1. \tag{1.22}$$

D'après la condition (1.21), il existe un entier k tel que

$$x^{p-1} = 1 + kp \text{ avec } k \neq 0 \bmod p.$$

Puisque p est impair, on déduit alors du lemme 13 que l'on a

$$x^r = 1 + p^{s+1}k \bmod p.$$

Parce que p^n divise $x^r - 1$, et que p ne divise pas k, on a donc $n \leq s+1$. Compte tenu de (1.22), on obtient $s = n-1$, d'où $r = \varphi(p^n)$ et le résultat.

Exemple. Pour tout $n \geq 1$, la classe de 2 est un générateur du groupe $(\mathbb{Z}/3^n\mathbb{Z})^*$. En effet, $2 + 3\mathbb{Z}$ est un générateur de $(\mathbb{Z}/3\mathbb{Z})^*$ et l'on a $2^2 \neq 1 \bmod 9$.

1.11 Le groupe $(\mathbb{Z}/2^n\mathbb{Z})^*$

Le groupe $(\mathbb{Z}/2\mathbb{Z})^*$ est trivial et $\mathbb{Z}/4\mathbb{Z})^*$ est cyclique d'ordre 2. Considérons un entier $n \geq 3$. On va établir que $(\mathbb{Z}/2^n\mathbb{Z})^*$ est isomorphe au groupe $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z}, +)$. Posons

$$U(n) = \{a + 2^n\mathbb{Z} : a = 1 \bmod 4\}.$$

C'est un sous-groupe de $(\mathbb{Z}/2^n\mathbb{Z})^*$. On a $(\mathbb{Z}/2^n\mathbb{Z})^* = \{\pm 1\}U(n)$ et l'application

$$f : \{\pm 1\} \times U(n) \to (\mathbb{Z}/2^n\mathbb{Z})^*$$

définie par

$$f((\varepsilon, a + 2^n\mathbb{Z})) = \varepsilon a + 2^n\mathbb{Z} \text{ avec } \varepsilon = \pm 1,$$

est un isomorphisme de groupes.

Proposition 9. *Le groupe $U(n)$ est cyclique, d'ordre 2^{n-2}, et il est engendré par la classe de 5.*

Démonstration : Vu ce qui précède, l'ordre de $U(n)$ est $\frac{\varphi(2^n)}{2} = 2^{n-2}$. Par ailleurs, la classe de 5 est dans $U(n)$. Tout revient à prouver que l'ordre de $5 + 2^n\mathbb{Z}$ dans $(\mathbb{Z}/2^n\mathbb{Z})^*$ est 2^{n-2}. Pour cela, on vérifie par récurrence sur n que l'on a

$$5^{2^{n-3}} = 1 + 2^{n-1} \bmod 2^n.$$

Par suite, l'ordre de $5 + 2^n\mathbb{Z}$ ne divise pas 2^{n-3}. Vu que l'on a (prop **??**)

$$5^{2^{n-2}} = 1 \bmod 2^n,$$

l'ordre de la classe de 5 est donc 2^{n-2}.

On en déduit le résultat annoncé :

Théorème 12. *Pour tout $n \geq 3$, le groupe $(\mathbb{Z}/2^n\mathbb{Z})^*$ est isomorphe au groupe produit $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z}, +)$.*

Pour tout $n \geq 3$, les éléments de $(\mathbb{Z}/2^n\mathbb{Z})^*$ sont d'ordre divisant 2^{n-2}, en particulier il n'est pas cyclique.

Comme conséquence des théorèmes 11 et 12, et du théorème chinois, on obtient la liste, établie par Gauss, des entiers $m \geq 1$ tels que le groupe $(\mathbb{Z}/m\mathbb{Z})^*$ soit cyclique.

Théorème 13. ***(Gauss, 1801).*** *Les entiers $m \geq 1$ tels que $(\mathbb{Z}/m\mathbb{Z})^*$ soit un groupe cyclique sont* 1, 2, 4, *et ceux de la forme p^r et $2p^r$ où p est un nombre premier impair.*

Démonstration : Si p est premier impair, les groupes $(\mathbb{Z}/p^r\mathbb{Z})^*$ et $(\mathbb{Z}/2p^r\mathbb{Z})^*$ sont isomorphes. Pour tout entier m intervenant dans l'énoncé, $(\mathbb{Z}/m\mathbb{Z})^*$ est donc un groupe cyclique (th. 11).

Inversement, soit m un entier ≥ 3 tel que $(\mathbb{Z}/m\mathbb{Z})^*$ soit cyclique. Soit

$$m = \prod_{i=1}^{t} p_i^{n_i},$$

la décomposition de m en produit de nombres premiers p_i, avec $p_i \neq p_j$ si $i \neq j$ et $n_i \geq 1$. Les groupes

$$(\mathbb{Z}/m\mathbb{Z})^* \text{ et } \prod_{i=1}^{t} (\mathbb{Z}/p_i^{n_i}\mathbb{Z})^*$$

sont isomorphes (cf. le théorème chinois). Compte tenu du lemme 11, il en résulte que m est de la forme $2^s p^r$ où p est un nombre premier impair. Si $r = 0$, le théorème 12 implique $s = 2$ (car $m \geq 3$). Si $r \geq 1$, on obtient $s = 0$ ou $s = 1$, d'où le résultat.

Exemple. Vérifions que $(\mathbb{Z}/4418\mathbb{Z})^*$ est cyclique engendré par la classe de 5. Ce groupe est cyclique, d'ordre 2162, car $4418 = 2 \times 47$. Il suffit d'établir que $5 + 47^2\mathbb{Z}$ est un générateur de $(\mathbb{Z}/47^2\mathbb{Z})^*$. Démontrons pour cela que la classe de 5 est un générateur de $(\mathbb{Z}/47\mathbb{Z})^*$. Déterminons l'ordre multiplicatif de 2 modulo 47. On a

$$2^{16} = (2^8)^2 = 21^2 = 18 \bmod 47,$$

d'où l'on déduit que $2^{23} = 1 \bmod 47$, puis que 23 est l'ordre cherché. Par ailleurs, -1 est d'ordre 2 modulo 47. Il en résulte que la classe de -2 est un générateur de $(\mathbb{Z}/47\mathbb{Z})^*$. Les générateurs de $(\mathbb{Z}/47\mathbb{Z})^*$ sont donc les éléments $(-2)^k + 47\mathbb{Z}$ avec $\gcd(k, 46) = 1$ (il y en a vingt-deux). On a $2^8 = 21 \bmod 47$ puis

$$-2^9 = 5 \bmod 47,$$

d'où l'assertion. On vérifie ensuite à l'aide d'une calculatrice que l'on a $5^{46} \neq 1 \bmod 47$. Le théorème 11 entraîne alors le résultat.

Chapter 2

Loi de Réciprocité quadratique

2.1 Symbole de Legendre

Soient m et n des entiers relatifs. On dit que m est un résidu quadratique modulo n si $m + n\mathbb{Z}$ est un carré dans $\mathbb{Z}/n\mathbb{Z}$, autrement dit, s'il existe $a \in \mathbb{Z}$ tel que l'on ait

$$m = a^2 \bmod n.$$

Dans ce cas, on dit aussi que m est un carré modulo n.

Définition 5. *Soient p un nombre premier et n un entier relatif. On note $\left(\frac{n}{p}\right)$ l'entier défini comme suit. On a :*

1. $\left(\frac{n}{p}\right) = 0$ *si p divise n.*
2. $\left(\frac{n}{p}\right) = 1$ *si p ne divise pas n et si n est un résidu quadratique modulo p.*
3. $\left(\frac{n}{p}\right) = -1$ *si n n'est pas un résidu quadratique modulo p.*

L'expression $\left(\frac{n}{p}\right)$ s'appelle le symbole de Legendre. L'entier $\left(\frac{n}{p}\right)$ ne dépend que de la classe de n modulo p.

Exemples.

1. On a $\left(\frac{n}{2}\right) = 1$ si n est impair et $\left(\frac{n}{2}\right) = 0$ si n est pair. On a ainsi $\left(\frac{n}{2}\right) = n \bmod 2$.
2. Vérifions la congruence
$$\left(\frac{n}{3}\right) = n \bmod 3.$$
Si 3 divise n, on a $\left(\frac{n}{3}\right) = 0$. Si $n = 1 \bmod 3$, on a $\left(\frac{n}{3}\right) = 1$. Si $n = -1 \bmod 3$, vu que -1 n'est pas un carré modulo 3, on obtient $\left(\frac{n}{3}\right) = \left(\frac{-1}{3}\right) = -1$, d'où la formule annoncée.

Proposition 10. *Soit p un nombre premier impair. On a*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}. \tag{2.1}$$

Ainsi, -1 est un carré modulo p si et seulement si on a $p = 1 \bmod 4$.

Démonstration : Supposons $\left(\frac{-1}{p}\right) = 1$. Il existe $n \in \mathbb{Z}$ tel que l'on ait $-1 = n^2 \bmod p$. Le sous-groupe de $(\mathbb{Z}/p\mathbb{Z})^*$ engendré par la classe de n est d'ordre 4, d'où $p = 1 \bmod 4$. Inversement, si 4 divise $p - 1$, le groupe $(\mathbb{Z}/p\mathbb{Z})^*$ étant cyclique, il possède un sous-groupe cyclique d'ordre 4. Si x est un générateur de ce sous-groupe, on a $x^2 = -1$, d'où $\left(\frac{-1}{p}\right) = 1$. Par suite, on a $\left(\frac{-1}{p}\right) = 1$ si et seulement si p est congru à 1 modulo 4, ce qui entraîne (2.1).

2.2 Le critère d'Euler

Il permet de calculer le symbole de Legendre.

Théorème 14. ***(Critère d'Euler).*** *Soit p un nombre premier impair. Pour tout entier relatif n, on a*

$$\left(\frac{n}{p}\right) = n^{\frac{p-1}{2}} \bmod p. \tag{2.2}$$

Démonstration : Commençons par établir le lemme suivant :

Lemma 14. *Soit p un nombre premier impair. L'ensemble des carrés de $(\mathbb{Z}/p\mathbb{Z})^*$ est un sous-groupe de $(\mathbb{Z}/p\mathbb{Z})^*$ d'ordre $\frac{p-1}{2}$.*

Démonstration : L'application $(\mathbb{Z}/p\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^*$ qui à x associe x^2 est un morphisme de groupes. Son noyau est $\{\pm 1\}$. Il est d'ordre 2 car $p \neq 2$. L'image de ce morphisme, qui est le sous-groupe des carrés de $(\mathbb{Z}/p\mathbb{Z})^*$, est donc d'ordre $\frac{p-1}{2}$.

Le théorème 14 se déduit comme suit. Soit n un entier relatif. La congruence (2.2) est vraie si p divise n. Supposons que p ne divise pas n. On a $n^{p-1} = 1 \bmod p$. Puisque $\mathbb{Z}/p\mathbb{Z}$ est un corps, on a donc

$$n^{\frac{p-1}{2}} = \pm 1 \bmod p. \tag{2.3}$$

Par ailleurs, le polynôme $X^{\frac{p-1}{2}} - 1 \in (\mathbb{Z}/p\mathbb{Z})[X]$ a au plus $\frac{p-1}{2}$ racines. On déduit du lemme 14 que ses racines sont exactement les $\frac{p-1}{2}$ carrés de $(\mathbb{Z}/p\mathbb{Z})^*$. On obtient l'équivalence

$$\left(\frac{n}{p}\right) = 1 \text{ si et seulement si } n^{\frac{p-1}{2}} = 1 \bmod p.$$

La condition (2.3) entraîne alors le résultat.

Remarque 9. *Soit p un nombre premier impair. Parmi les entiers compris entre 1 et $p-1$, il y en a exactement la moitié qui sont des résidus quadratiques modulo p (lemme 14). On a donc la formule*

$$\sum_{k=1}^{p-1} \left(\frac{k}{p}\right) = 0. \tag{2.4}$$

Exemple. Le critère d'Euler permet de calculer $\left(\frac{n}{p}\right)$ en utilisant le calcul "rapide" de la puissance d'un entier. Par exemple, on obtient que $\left(\frac{5}{23}\right) = -1$ en écrivant que l'on a

$$11 = 2^3 + 2 + 1 \text{ puis } 5^{11} = 5^{2^3} \times 5^2 \times 5 = -1 \bmod 23.$$

Corollaire 12. *Soit p un nombre premier. Quels que soient les entiers m et n, on a*

$$\left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{n}{p}\right). \tag{2.5}$$

De plus, si n n'est pas divisible par p, on a

$$\left(\frac{mn^2}{p}\right) = \left(\frac{m}{p}\right). \tag{2.6}$$

Démonstration : Si $p = 2$, l'égalité (2.5) provient du fait que mn est pair si et seulement si m ou n l'est. Si $p \neq 2$, elle se déduit du critère d'Euler. Quant à l'égalité (2.6), elle résulte de (2.5) et de la définition du symbole de Legendre.

Remarque 10. *On peut déduire de la formule (2.5) l'énoncé suivant :*

Proposition 11. *Soit p un nombre premier impair. Soit n le plus petit entier naturel qui ne soit pas un résidu quadratique modulo p. On a*

$$n < 1 + \sqrt{p}.$$

Démonstration : Soit m le plus petit entier naturel tel que $mn > p$. Puisque p est premier, on a donc $n(m-1) < p$ i.e. $mn - p < n$. D'après le caractère minimal de n, on a donc avec la formule (2.5) les égalités

$$1 = \left(\frac{mn-p}{p}\right) = \left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{n}{p}\right) = -\left(\frac{m}{p}\right).$$

Par suite, on a $m \geq n$. Le résultat s'ensuit vu que l'on a

$$(n-1)^2 < n(n-1) \leq n(m-1) < p.$$

Citons à ce propos la conjecture de Vinogradov :

Conjecture. Soit ε un nombre réel > 0. Pour tout nombre premier p assez grand, le plus petit entier naturel qui ne soit pas un résidu quadratique modulo p est inférieur à p^{ε}.

Par exemple, Hudson et Williams ont démontré en 1979 que si p est un nombre premier impair non congru à 1 modulo 8, le plus petit entier naturel n qui ne soit pas un résidu quadratique modulo p est inférieur à $p^{\frac{2}{5}} + 12p^{\frac{1}{5}} + 33$. On a ainsi $n < 1,54p^{\frac{2}{5}}$ dès que p (non congru à 1 modulo 8) est plus grand que 10^7.

Exemple. Soient p un nombre premier impair et n un entier non divisible par p. Afin de calculer le symbole $\left(\frac{n}{p}\right)$, on peut utiliser la méthode suivante. Posons $a = n + p\mathbb{Z}$. Supposons donné un anneau commutatif A, contenant le corps $\mathbb{Z}/p\mathbb{Z}$, dans lequel a soit un carré. Soit b un élément de A tel que $a = b^2$. Puisque a est inversible dans A, il en est de même de b. Par suite, on a

$$n^{\frac{p-1}{2}} + p\mathbb{Z} = a^{\frac{p-1}{2}} = \frac{b^p}{b}.$$

On a donc $b^p = \pm b$ et d'après le critère d'Euler on obtient:

$$\left(\frac{n}{p}\right) = 1 \text{ si } b^p = b \text{ et } \left(\frac{n}{p}\right) = -1 \text{ si } b^p = -b. \tag{2.7}$$

Tout revient alors à calculer b^p.

Voyons dans cette direction comment déterminer $\left(\frac{5}{p}\right)$. En suivant une démonstration de Gauss de la loi de réciprocité quadratique (voir après), l'idée est de prendre pour A l'anneau quotient

$$A = (\mathbb{Z}/p\mathbb{Z})[X]/(\Phi_5) \text{ où } \Phi_5(X) = \sum_{j=0}^{4} X^j \in (\mathbb{Z}/p\mathbb{Z})[X].$$

(Φ_5 est le cinquième polynôme cyclotomique.) On identifie $\mathbb{Z}/p\mathbb{Z}$ à un sous-anneau de A, via la flèche $n + p\mathbb{Z} \mapsto n1_A$ où $1_A = 1 + (\Phi_5)$. Notons α la classe de X modulo Φ_5. On a $\alpha^5 = 1$. Considérons "la somme de Gauss"

$$b = \sum_{i=1}^{4} \left(\frac{i}{5}\right)\alpha^i.$$

Dans A, on vérifie que l'on a

$$b^2 = 5.$$

Par ailleurs, on a $p1_A = 0$, d'où $b^p = \alpha^p - \alpha^{2p} - \alpha^{3p} + \alpha^{4p}$. On en déduit que l'on a

$$b^p = b \text{ si } p = \pm 1 \bmod 5 \text{ et } b^p = -b \text{ si } p = \pm 2 \bmod 5.$$

D'après (2.7), on obtient

$$\left(\frac{5}{p}\right) = 1 \text{ si } p = \pm 1 \bmod 5 \text{ et } \left(\frac{5}{p}\right) = -1 \text{ si } p = \pm 2 \bmod 5.$$

Pour tout p premier impair, on a ainsi la relation

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right). \tag{2.8}$$

La formule (2.8) est un cas particulier de la loi de réciprocité quadratique, qui affirme que pour tous nombres premiers impairs p et q distincts, on a

$$\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{q}{p}\right).$$

Il existe plus de deux cent vingt preuves connues de ce résultat. On en donnera une dans laquelle intervient des sommes de racines l'unité, appelées sommes de Gauss, analogues à celle de l'exemple précédent. Auparavant, on va établir la formule permettant de calculer le symbole $\left(\frac{2}{p}\right)$, et en donner des exemples d'applications.

2.3 Le symbole $\left(\frac{2}{p}\right)$

Proposition 12. *Soit p un nombre premier impair. On a*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}. \tag{2.9}$$

Ainsi, 2 est un carré modulo p si et seulement si on a $p = \pm 1 \bmod 8$.

Démonstration : Posons

$$S = \{1, \ldots, \frac{p-1}{2}\}.$$

Etant donné $a \in \mathbb{Z}$ non divisible par p, pour tout $s \in S$ il existe un unique élément $s_a \in S$ tel que l'on ait

$$as = e_s(a)s_a \bmod p \text{ avec } e_s(a) = \pm 1.$$

Lemma 15. ***(Gauss).*** *Soit a un entier relatif non divisible par p. On a*

$$\left(\frac{a}{p}\right) = \prod_{s \in S} e_s(a).$$

Démonstration : Vérifions que l'application $f : S \to S$ définie par $f(s) = s_a$ est une bijection de S. Soient s et s' des éléments de S tels que $f(s) = f(s')$. On obtient $e_s(a)s = e_{s'}(a)s' \bmod p$, d'où $s = \pm s' \bmod p$, ce qui implique $s = s'$. Par la suite, f est injective, d'où l'assertion. Il en résulte que l'on a

$$a^{\frac{p-1}{2}} \prod_{s \in S} s = \prod_{s \in S} (as) = \prod_{s \in S} e_s(a) \prod_{s \in S} s_a \bmod p,$$

d'où

$$a^{\frac{p-1}{2}} \prod_{s \in S} s = \prod_{s \in S} e_s(a) \prod_{s \in S} s \bmod p$$

puis la congruence

$$a^{\frac{p-1}{2}} = \prod_{s \in S} e_s(a) \bmod p.$$

D'après le critère d'Euler, on obtient ainsi

$$\prod_{s\in S} e_s(a) = \left(\frac{a}{p}\right) \bmod p,$$

d'où le résultat car les deux membres de cette congruence valent ± 1 et p est impair.

La proposition 12 se déduit comme suit. On utilise le lemme précédent avec $a = 2$. Pour tout $s \in S$, on a

$$e_s(2) = 1 \text{ si } 2s \in S \text{ et } e_s(2) = -1 \text{ sinon.}$$

Par suite, on a (lemme 15)

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

où $n(p)$ est le nombre d'entiers u tels que

$$\frac{p-1}{4} < u \leq \frac{p-1}{2}.$$

Supposons $p = \pm 1 \bmod 8$. On a $p = \pm 1 + 8k$ où $k \in \mathbb{N}$, et l'on vérifie que $n(p) = 2k$. Si l'on a $p = 3 + 8k$ où $k \in \mathbb{N}$, on obtient $n(p) = 2k + 1$. Si $p = -3 + 8k$ où $k \in \mathbb{N}$, on a $n(p) = 2k - 1$. Cela conduit à la formule (2.9).

Exemple. Démontrons qu'il existe une infinité de nombres premiers congrus à 7 modulo 8. Supposons le contraire. Soient $\{p_1, \ldots, p_n\}$ l'ensemble des nombres premiers congrus à 7 modulo 8. Posons

$$N = (4p_1 \ldots p_n)^2 - 2.$$

Soit p un diviseur premier impair de N. On a $2 = (4p_1 \ldots p_n)^2 \bmod p$, donc 2 est un carré modulo p. Par suite, on a $p = \pm 1 \bmod 8$ (prop. 12). Compte tenu de l'égalité

$$\frac{N}{2} = 8(p_1 \ldots p_n)^2 - 1,$$

il existe donc un diviseur premier q de N qui est congru à -1 modulo 8. Ainsi q est l'un des p_i, ce qui conduit à une contradiction.

Exemple. Voyons une illustration du critère d'Euler et de la proposition 12, concernant la primalité des nombres de Fermat

$$F_n = 2^{2^n} + 1.$$

Prouvons que pour tout $n \geq 2$, les facteurs premiers de F_n sont congrus à 1 modulo 2^{n+2}. Soit p un facteur premier de F_n. On a

$$2^{2^n} = -1 \bmod p \text{ et } 2^{2^{n+1}} = 1 \bmod p.$$

Par suite, l'ordre de 2 modulo p est 2^{n+1}. D'après le théorème de Lagrange, 2^{n+1} divise $p - 1$. En particulier, on a $p = 1 \bmod 8$, d'où $\left(\frac{2}{p}\right) = 1$. D'après le critère d'Euler, on obtient

$$2^{\frac{p-1}{2}} = 1 \bmod p,$$

donc 2^{n+1} divise $\frac{p-1}{2}$, d'où l'assertion. En testant les entiers congrus à 1 modulo 128, on constate par exemple que $2^{32} + 1$ est le produit de deux nombres premiers, avec l'égalité

$$2^{32} + 1 = 641 \times 6700417.$$

Exemple. Soit p un nombre premier. Supposons que p soit de la forme

$$p = 1 + 4q \text{ avec } q \text{ premier.}$$

Vérifions que la classe de 2 est un générateur de $(\mathbb{Z}/p\mathbb{Z})^*$. Soit d l'ordre multiplicatif de 2 modulo p. Puisque q est premier, on a $d \in \{1, 2, 4, q, 2q, 4q\}$. On a $p \neq 3$ et $p \neq 5$, d'où $d = q$, $2q$ ou $4q$. Supposons $d \neq 4q$. Dans ce cas, on obtient la congruence

$$2^{\frac{p-1}{2}} = 1 \bmod p.$$

D'après le critère d'Euler, 2 est donc un résidu quadratique modulo p. Cela conduit à une contradiction vu que p est congru à 5 modulo 8.

2.4 Sommes de Gauss

Soit q un nombre premier impair. Soient A un anneau commutatif, d'élément neutre multiplicatif $1 = 1_A$. Soit α un élément de A tels que

$$1 + \alpha + \ldots + \alpha^{q-1} = 0. \tag{2.10}$$

On a $\alpha^q = 1$, autrement dit α est une racine q-ième de l'unité. L'élément α^i et l'entier $\left(\frac{i}{q}\right)$ ne dépendent que de la classe de i modulo q. Considérons la somme de Gauss

$$\tau = \sum_{i \in \mathbb{Z}/q\mathbb{Z}} \left(\frac{i}{q}\right)\alpha^i = \sum_{i=0}^{q-1} \left(\frac{i}{q}\right)\alpha^i.$$

Théorème 15. *1. On a l'égalité*

$$\tau^2 = (-1)^{\frac{q-1}{2}} q.$$

2. Soit p un nombre premier impair distinct de q. Supposons que l'on ait $p\alpha = 0$. On a

$$\tau^p = \left(\frac{p}{q}\right)\tau.$$

Commençons par établir le lemme suivant :

Lemma 16. *Soit k un entier non divisible par q. On a*

$$\sum_{i=1}^{q-1} \left(\frac{i(i-k)}{q}\right) = -1.$$

Démonstration : Pour tout i entre 1 et $q-1$, i est inversible modulo q. Notons i^{-1} son inverse modulo q compris entre 1 et $q-1$. On a (cor. 12)

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

Par ailleurs, l'application $(\mathbb{Z}/q\mathbb{Z}) \to \mathbb{Z}/q\mathbb{Z} \setminus \{1\}$ qui à la classe de i associe celle de $1 - ki^{-1}$ est une bijection. Par suite, on a

$$\sum_{i=1}^{q-1} \left(\frac{i(i-k)}{q}\right) = \sum_{\substack{i=0 \\ i\neq 1}}^{q-1} \left(\frac{i}{q}\right) = \sum_{i=1}^{q-1} \left(\frac{i}{q}\right) - \left(\frac{1}{q}\right).$$

La formule (2.4) entraîne alors le résultat.

Démonstration du théorème 15 : 1) On a (prop. 10)

$$(-1)^{\frac{q-1}{2}}\tau^2 = \left(\frac{-1}{q}\right)\tau^2 = \sum_{i,j} \left(\frac{-1}{q}\right)\left(\frac{i}{q}\right)\left(\frac{j}{q}\right)\alpha^i\alpha^j = \sum_{i,j} \left(\frac{-ij}{q}\right)\alpha^{i+j}.$$

Puisque $\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ est la réunion disjointe des ensembles

$$\{(i,j) \in \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} : i+j = k+q\mathbb{Z}\} \text{ pour } k = 0, \cdots, q-1,$$

on en déduit que

$$(-1)^{\frac{q-1}{2}}\tau^2 = \sum_{k=0}^{q-1} s_k \alpha^k \text{ avec } s_k = \sum_{i=0}^{q-1} \left(\frac{i(i-k)}{q}\right).$$

On a $s_0 = q-1$. Si k n'est pas nul, on a $s_k = -1$ (lemme 16). D'après (2.10),on obtient

$$(-1)^{\frac{q-1}{2}}\tau^2 = (q-1) - \sum_{k=1}^{q-1} \alpha^k = q - \sum_{k=0}^{q-1} \alpha^k = q,$$

et l'égalité annoncée.

2) Compte tenu du fait que $p\alpha = 0$ et que p est impair, on a

$$\tau^p = \left(\sum_{i\in\mathbb{Z}/q\mathbb{Z}} \left(\frac{i}{q}\right)\alpha^i\right)^p = \sum_{i\in\mathbb{Z}/q\mathbb{Z}} \left(\frac{i}{q}\right)^p \alpha^{ip} = \sum_{i\in\mathbb{Z}/q\mathbb{Z}} \left(\frac{i}{q}\right)\alpha^{ip}.$$

Par ailleurs, p est inversible modulo q, donc l'application qui à i associe ip est une bijection de $\mathbb{Z}/q\mathbb{Z}$. Il en résulte que l'on a

$$\left(\frac{p}{q}\right)\tau^p = \sum_{i\in\mathbb{Z}/q\mathbb{Z}} \left(\frac{ip}{q}\right)\alpha^{ip} = \sum_{j\in\mathbb{Z}/q\mathbb{Z}} \left(\frac{j}{q}\right)\alpha^j = \tau,$$

ce qui entraîne le résultat.

Exemple. Vérifions que l'on a

$$\tau = \sum_{i=0}^{q-1} \alpha^{i^2} \tag{2.11}$$

Notons R l'ensemble des carrés de $(\mathbb{Z}/q\mathbb{Z})^*$. On a les égalités

$$\tau = \sum_{i\in(\mathbb{Z}/q\mathbb{Z})^*} \left(\frac{i}{q}\right)\alpha^i = \sum_{i\in R} \alpha^i - \sum_{i\in(\mathbb{Z}/q\mathbb{Z})^* - R} \alpha^i.$$

Compte tenu de (2.10), on obtient

$$\tau = 2\sum_{i\in R} \alpha^i + 1.$$

Par ailleurs, on a

$$\sum_{i\in R} \alpha^i = \sum_{i=1}^{\frac{q-1}{2}} \alpha^{i^2} = \sum_{i=\frac{q+1}{2}}^{q-1} \alpha^{i^2},$$

d'où la formule (2.11).

2.5 La loi de réciprocité quadratique

Elle a été conjecturée par Euler en 1783, et a été démontrée par Gauss en 1796.

Théorème 16. ***(Gauss).*** *Soient p et q deux nombres premiers impairs distincts. On a*

$$\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{q}{p}\right).$$

Autrement dit, on a

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \text{ si } p \text{ ou } q \text{ est congru à 1 modulo 4,}$$

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right) \text{ sinon.}$$

Démonstration : Posons

$$A = \mathbb{Z}/p\mathbb{Z}[X]/(\Phi_q) \text{ où } \Phi_q = 1 + X + \ldots + X^{q-1}.$$

Rappelons que $\mathbb{Z}/p\mathbb{Z}$ s'identifie à un sous-anneau de A, via la flèche $n + p\mathbb{Z} \mapsto n1_A$ où $1_A = 1 + (\Phi_q)$. Soit α la classe de X modulo Φ_q. On a

$$1 + \alpha + \ldots + \alpha^{q-1} = 0.$$

Posons

$$\tau = \sum_{i \in \mathbb{Z}/q\mathbb{Z}} \left(\frac{i}{q}\right) \alpha^i.$$

On a (th. 15)

$$\tau^2 = (-1)^{\frac{q-1}{2}} q.$$

D'après le critère d'Euler, on a

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

On en déduit que l'on a dans A les égalités

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

Puisque $p = 0$ dans A, on a

$$\tau^p = \left(\frac{p}{q}\right)\tau.$$

Par ailleurs, q étant distinct de p, τ^2 est inversible dans A, donc τ l'est aussi, d'où l'égalité

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

Vu que p est impair, on obtient dans $\mathbb{Z}$ l'égalité

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

autrement dit,

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

ce qui entraîne le résultat car $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

Exemples. 1) Vérifions que l'on a

$$\left(\frac{101}{641}\right) = -1.$$

En utilisant la loi de réciprocité, on obtient

$$\left(\frac{101}{641}\right) = \left(\frac{641}{101}\right) = \left(\frac{35}{101}\right) = \left(\frac{5}{101}\right)\left(\frac{7}{101}\right) = \left(\frac{101}{5}\right)\left(\frac{101}{7}\right) = \left(\frac{3}{7}\right) = -\left(\frac{7}{3}\right) = -1.$$

2) Soit p un nombre premier congru à ± 2 modulo 5. Vérifions que l'équation

$$x^2 + py^2 = 5z^2$$

n'a pas de solutions dans $\mathbb{Z}^3$, autres que $(0,0,0)$. Soit (x,y,z) une solution non triviale. On peut supposer x, y et z premiers entre eux dans leur ensemble. Par suite, p ne divise pas z, donc 5 est un carré modulo p. On obtient une contradiction car

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = -1.$$

2.6 Symbole de Jacobi et réciprocité

Le symbole de Jacobi est une généralisation du symbole de Legendre.

Définition 6. *Soient m un entier relatif et n un entier naturel impair. On note $\left(\frac{m}{n}\right)$ l'entier défini comme suit*

1) On a $\left(\frac{m}{1}\right) = 1$.

2) Supposons $n \geq 3$. Soit $n = p_1 \dots p_r$ la décomposition de n en produit de nombres premiers, les facteurs n'étant pas nécessairement distincts. On pose

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

L'expression $\left(\frac{m}{n}\right)$ s'appelle le symbole de Jacobi. On peut aussi définir le symbole de Jacobi si n est pair. Le cas où n est impair nous suffira pour la suite, notamment en ce qui concerne les critères de primalité.

Proposition 13. *Soient m un entier relatif et n un entier naturel impair.*

1. *On a $\left(\frac{m}{n}\right) = 0, -1$ ou 1.*
2. *On a $\left(\frac{m}{n}\right) = 0$ si et seulement si m et n ne sont pas premiers entre eux.*
3. *L'entier $\left(\frac{m}{n}\right)$ ne dépend que la classe de m modulo n.*
4. *Soient m' un entier relatif et n' un entier naturel impair. On a*

$$\left(\frac{mm'}{n}\right) = \left(\frac{m}{n}\right)\left(\frac{m'}{n}\right) \text{ et } \left(\frac{m}{nn'}\right) = \left(\frac{m}{n}\right)\left(\frac{m}{n'}\right).$$

5. *Si m et n sont premiers entre eux, on a*

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

Démonstration : Les trois premières assertions sont des conséquences directes des définitions des symboles de Legendre et de Jacobi. Soit $n = p_1 \dots p_r$ la décomposition de n en produit de nombres premiers (éventuellement répétés). On a

$$\left(\frac{mm'}{n}\right) = \prod_{i=1}^{r} \left(\frac{mm'}{p_i}\right) = \prod_{i=1}^{r} \left(\frac{m}{p_i}\right)\left(\frac{m'}{p_i}\right)\left(\frac{m}{n}\right)\left(\frac{m'}{n}\right).$$

Quant à la seconde égalité de l'assertion 4, on l'obtient en considérant les décompositions en facteurs premiers de n et n'. La dernière assertion se déduit des assertions 1, 2 et 4.

Remarque 11. *1) L'égalité* $\left(\frac{m}{n}\right) = 1$ *n'implique pas que* m *soit un carré modulo* n*. Par exemple, on a*

$$\left(\frac{14}{51}\right) = \left(\frac{14}{3}\right)\left(\frac{14}{17}\right) = \left(\frac{-1}{3}\right)\left(\frac{-3}{17}\right) = 1,$$

pour autant 14 n'est pas un carré modulo 51, vu que ce n'est déjà pas un carré modulo 3. Cela étant, l'égalité $\left(\frac{m}{n}\right) = -1$ *entraîne que* m *n'est pas un carré modulo* n*.*

2) Si n *est un nombre premier impair, on a* $\left(\frac{m}{n}\right) = m^{\frac{n-1}{2}} \bmod n$ *(critère d'Euler). Ce n'est plus vrai si* n *n'est pas premier. Par exemple, on a*

$$\left(\frac{14}{51}\right) = 1 \text{ et } 14^{25} = 20 \bmod 51.$$

Vérifions cette congruence. On a $14^{25} = -1 \bmod 3$ *(en particulier* $14^{25} \neq 1 \bmod 51$*) et* $14^{25} = (-3)^{25} \bmod 17$*. D'après le petit théorème de Fermat, on a* $(-3)^{16} = 1 \bmod 17$*, d'où* $14^{25} = -3^9 \bmod 17$*. Par ailleurs, on a*

$$\left(\frac{-3}{17}\right) = 3^8 \bmod 17 \text{ et } \left(\frac{-3}{17}\right) = \left(\frac{-1}{17}\right)\left(\frac{3}{17}\right) = \left(\frac{17}{3}\right) = -1.$$

On obtient $14^{25} = 3 \bmod 17$*, d'où l'assertion en utilisant le théorème chinois.*

Il n'y a donc pas de rapport en général entre le symbole de Jacobi $\left(\frac{m}{n}\right)$ *et l'entier* $m^{\frac{n-1}{2}}$*. Cette remarque est à la base du test de primalité de Solovay-Strassen.*

La loi de réciprocité quadratique s'étend aux symboles de Jacobi.

Théorème 17. *Soient* m *et* n *des entiers naturels impairs. On a.*

$$\left(\frac{m}{n}\right) = (-1)^{\frac{(m-1)(n-1)}{4}} \left(\frac{n}{m}\right).$$

Autrement dit, on a

$$\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right) \text{ si } m \text{ ou } n \text{ est congru à } 1 \text{ modulo } 4,$$

$$\left(\frac{m}{n}\right) = -\left(\frac{n}{m}\right) \text{ sinon.}$$

Démonstration : Si m et n ne sont pas premiers entre eux, on a $\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right) = 0$. Si m ou n vaut 1, on a $\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right) = 1$. Dans ces deux cas, on a l'égalité annoncée.

Supposons m et n au moins égaux à 3 et premiers entre eux. Soient

$$m = p_1 \dots p_r \text{ et } n = q_1 \dots q_s$$

les décompositions de m et n en produits de nombres premiers. On a (prop. 13)

$$\left(\frac{m}{n}\right) = \prod_{i,j} \left(\frac{p_i}{q_j}\right) \text{ et } \left(\frac{n}{m}\right) = \prod_{i,j} \left(\frac{q_j}{p_i}\right).$$

En appliquant la loi de réciprocité quadratique rs fois, on en déduit l'égalité

$$\left(\frac{m}{n}\right) = (-1)^t \left(\frac{n}{m}\right),$$

où t est le nombre de couples (i,j) tels que p_i et q_j soient congrus à 3 modulo 4. Il en résulte que l'on a $\left(\frac{m}{n}\right) = -\left(\frac{n}{m}\right)$ si et seulement si il y a un nombre impair de nombre premiers congrus à 3 modulo 4 dans chacune des factorisations de m et n. Par ailleurs, un produit de nombres premiers impairs est congru à 3 modulo 4 si et seulement si il y a un nombre impair de nombres premiers congrus à 3 modulo 4 dans ce produit. Ainsi, $\left(\frac{m}{n}\right) = -\left(\frac{n}{m}\right)$ si et seulement si m et n sont congrus à 3 modulo 4, d'où le résultat.

Exemples. 1) Calculons $\left(\frac{323}{1443}\right)$. On a

$$\left(\frac{323}{1443}\right) = -\left(\frac{1443}{323}\right) = -\left(\frac{151}{323}\right) = \left(\frac{323}{151}\right) = \left(\frac{21}{151}\right) = \left(\frac{151}{21}\right) = \left(\frac{4}{21}\right) = 1.$$

2) Pour tout entier naturel impair n, on a les formules

$$\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}} \text{ et } \left(\frac{2}{n}\right) = (-1)^{\frac{m-1}{2}}. \tag{2.12}$$

Ces égalités sont vraies si $n = 1$. Supposons $n \geq 3$. Soit f l'application définie sur l'ensemble des entiers naturels impairs par l'égalité

$$f(m) = (-1)^{\frac{m-1}{2}}.$$

Pour tous a et b impairs, on vérifie, en examinant les classes de a et b modulo 4, que l'on a

$$f(ab) = f(a)f(b).$$

Soit $n = p_1^{n_1} \cdots p_r^{n_r}$ la décomposition en facteurs premiers de n. On a ainsi

$$f(n) = \prod_{i=1}^{r} f(p_i)^{n_i}.$$

Par ailleurs, pour tout $i = 1, \cdots, r$, on a $f(p_i) = \left(\frac{-1}{p_i}\right)$, d'où l'égalité $f(n) = \left(\frac{-1}{n}\right)$ par définition du symbole de Jacobi.

On procède de même pour l'autre égalité, en posant pour tout m impair

$$g(m) = (-1)^{\frac{m^2-!}{8}}.$$

Pour tous a et b impairs, on vérifie, en examinant les classes de a et b modulo 8, que l'on a $g(ab) = g(a)g(b)$, et l'on conclut comme ci-dessus.

3) Soient m un entier relatif et n un entier naturel impair. Vérifions que m ne dépend que de la classe de n modulo $4|m|$, autrement dit, que si n' est un entier naturel, on a l'implication

$$n = n' \bmod 4|m| \text{ implique } \left(\frac{m}{n}\right) = \left(\frac{m}{n'}\right). \tag{2.13}$$

Supposons m impair positif. Si m ou n est congru à 1 modulo 4, on a $\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right)$. Puisque $\left(\frac{n}{m}\right)$ ne dépend que de la classe de n modulo m, on a $\left(\frac{n}{m}\right) = \left(\frac{n'}{m}\right)$. On a $n = n' \bmod 4$, $\left(\frac{n'}{m}\right) = \left(\frac{m}{n'}\right)$, puis $\left(\frac{m}{n}\right) = \left(\frac{m}{n'}\right)$. Supposons que $m = n = 3 \bmod 4$. Dans ce cas, on a $\left(\frac{m}{n}\right) = -\left(\frac{n}{m}\right) = -\left(\frac{n'}{m}\right)$. Puisque m et n sont congrus à 3 modulo 4, on a $\left(\frac{n'}{m}\right) = -\left(\frac{m}{n'}\right)$, d'où l'assertion dans ce cas.

Si m est impair négatif, en posant $m = -t$, on a (première égalité de (2.12))

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

ce qui, d'après le cas déjà traité, entraîne (2.13).

Supposons m pair. Posons $m = 2^r t$, avec t impair. On a

$$\left(\frac{m}{n}\right) = \left(\frac{2}{n}\right)^r \left(\frac{t}{n}\right).$$

La congruence $n = n' \bmod 4|m|$ implique $n = n' \bmod 8$, d'où (seconde égalité de (2.12))

$$\left(\frac{2}{n}\right)^r = \left(\frac{2}{n'}\right)^r.$$

Puisque $n = n' \bmod 4|t|$, on a

$$\left(\frac{t}{n}\right) = \left(\frac{t}{n'}\right),$$

d'où l'implication (2.13).

Chapter 3

Arithmétique sur $K[X]$ et ses quotients

Dans tout ce chapitre la lettre K désigne un corps commutatif. Rappelons que l'on a défini l'anneau $K[X]$ des polynômes à une indéterminée à coefficients dans K. Les propriétés arithmétiques de l'anneau $K[X]$ sont essentiellement les mêmes que celles de l'anneau $\mathbb{Z}$, ce qui s'explique par le fait que ce sont des anneaux intègres, dont tous les idéaux sont principaux. On dit que de tels anneaux sont principaux. On démontrera que $K[X]$ est un anneau principal.

3.1 Degré - Division euclidienne

Définissons ce que l'on appelle le degré d'un élément de K[X]. On considère pour cela l'ensemble $\mathbb{N} \cup \{-\infty\}$ obtenu en adjoignant à $\mathbb{N}$ un élément noté $-\infty$, que l'on munit de la structure d'ensemble ordonné qui induit l'ordre usuel sur $\mathbb{N}$ et telle que $-\infty \leq n$ pour tout entier naturel n. Tout ensemble non vide de $\mathbb{N} \cup \{-\infty\}$ possède ainsi un plus petit élément. On prolonge par ailleurs la loi additive de $\mathbb{N}$ à cet ensemble en posant $(-\infty) + n = n + (-\infty) = -\infty$ et $(-\infty) + (-\infty) = -\infty$. On définit alors l'application degré

$$\deg : K[X] \to \mathbb{N} \cup \{-\infty\},$$

de la façon suivante :

Définition 7. *Soit $F = (a_i)_{i \geq 0}$ un polynôme à coefficients dans K.*

1. *Si $F = 0$ i.e. si tous les a_i sont nuls, on pose $\deg(F) = -\infty$.*
2. *Si F n'est pas nul, $\deg(F)$ est le plus grand entier $n \geq 0$ tel que $a_n \neq 0$.*

On dit que $\deg(F)$ est le degré de F.

Si $F \in K[X]$ est non nul, le coefficient de $X^{\deg(F)}$ est appelé le coefficient dominant de F. C'est le coefficient du terme de plus haut degré de F. S'il vaut 1, le polynôme F est dit unitaire.

Lemma 17. *Soient P et Q deux éléments de $K[X]$.*

1. *On a $\deg(P+Q) \leq \max\Big(\deg(P), deg(Q)\Big)$ avec égalité si $\deg(P) \neq \deg(Q)$.*
2. *On a $\deg(PQ) = \deg(P) + \deg(Q)$.*

Démonstration : On vérifie que ces assertions sont vraies si l'un des polynômes P et Q est nul. Supposons P et Q non nuls. Posons

$$P = a_0 + \ldots + a_r X^r \text{ mod } etQ = b_0 + \ldots + b_s X^s \text{ avec } a_r b_s \neq 0.$$

On a évidemment $\deg(P+Q) \leq \max(r,s)$ avec égalité si $r \neq s$. Par ailleurs, on a une égalité de la forme $PQ = a_r b_s X^{r+s} + R$ où $R \in K[X]$ est de degré $< r+s$. Puisque K est un anneau intègre (c'est un corps), on a $a_r b_s \neq 0$ de sorte que le degré de PQ est $r+s$.

Corollaire 13. *L'anneau $K[X]$ est intègre et le groupe de ses éléments inversibles est K i.e. est l'ensemble des éléments non nuls de K*[1]*.*

Démonstration : L'anneau $K[X]$ n'est pas nul et est commutatif. D'après l'assertion 2 du lemme 17, quels que soient P et Q dans $K[X]$, si $PQ = 0$ alors $\deg(P)$ ou bien $deg(Q)$ vaut $-\infty$, autrement dit, on a $P = 0$ ou bien $Q = 0$, donc $K[X]$ est intègre. Par ailleurs, si $PQ = 1$, on a $\deg(P) + \deg(Q) = 0$, ce qui entraîne $\deg(P) = \deg(Q) = 0$, d'où le résultat.

Le théorème de division euclidienne est le suivant :

Théorème 18. ***(Division euclidienne)*** *Soient A et B deux polynômes de $K[X]$ tels que $B \neq 0$. Alors, il existe un unique couple (Q,R) de polynômes de $K[X]$ tel que*

$$A = BQ + R \text{ avec } \deg R < \deg B.$$

On dit que Q est le quotient et que R est le reste de la division euclidienne de A par B.

Démonstration : On prouve le lemme suivant :

Lemma 18. *Soient U et V des polynômes de $K[X]$ tels que $V \neq 0$ et que l'on ait $\deg(U) \geq \deg(V)$. Alors, il existe $Q \in K[X]$ tel que l'on ait*

$$\deg(U - VQ) < \deg(U).$$

Démonstration : Puisque V est non nul, il en est de même de U. Soit a_k le coefficient dominant de U et b_q celui de V (de sorte que $\deg(U) = k$ et $\deg(V) = q$). On a par hypothèse $k \geq q$. Posons

$$Q = \frac{a_k}{b_q} X^{k-q}.$$

On constate que l'on a $\deg(U - VQ) < deg(U)$, d'où le lemme.

Le théorème 18 se déduit comme suit. Démontrons l'assertion d'existence. On considère l'ensemble

$$S = \{A - BQ | Q \in K[X]\}.$$

Le sous-ensemble de $\mathbb{N} \cup \{-\infty\}$ formé des degrés des éléments de S possède un plus petit élément r. Considérons un polynôme $Q \in K[X]$ tel que

$$\deg(A - BQ) = r.$$

Il s'agit de montrer que l'on a $r < \deg(B)$. Supposons le contraire i.e. que l'on a $r \geq \deg(B)$. On a $B \neq 0$. Compte tenu du lemme 18, il existe $Q' \in K[X]$ tel que le polynôme

$$A - BQ - Q'B = A - B(Q + Q')$$

soit de degré strictement plus petit que r. Puisque ce polynôme est dans S, le caractère minimal de r conduit alors à une contradiction.

[1] Ce résultat est faux si K est remplacé par un anneau non intègre. Par exemple, le polynôme $F = 2X + 1 \in \mathbb{Z}/4\mathbb{Z}[X]$ vérifie l'égalité $F^2 = 1$ (on note ici 2 la classe de 2 et 1 la classe de 1 modulo $4\mathbb{Z}$). On a aussi dans cet anneau $(2X)^2 = 0$.

Prouvons l'assertion d'unicité. Soient Q et Q_1 éléments de $K[X]$ tels que l'on ait

$$\deg(A - BQ) < \deg(B) \text{ et } \deg(A - BQ_1) < \deg(B).$$

On déduit de l'assertion 1 du lemme 17 que l'on a

$$\deg\Big((A - BQ) - (A - BQ_1)\Big) = \deg\Big(B(Q_1 - Q)\Big) < \deg(B).$$

D'après l'assertion 2 de ce lemme, on a ainsi $\deg(Q_1 - Q) < 0$, ce qui entraîne $Q_1 = Q$ et le résultat[2].

Exercice 1. Déterminer le quotient et le reste de la division euclidienne de $X^3 + X^2 + 1$ par $X^2 + X + 1$ dans $(\mathbb{Z}/2\mathbb{Z})[X]$.

Définition 8. *Soient A et B deux polynômes de $K[X]$. On dit que B divise A, ou que A est multiple de B, s'il existe $Q \in K[X]$ tel que $A = BQ$. Si $B \neq 0$ cela signifie que le reste de la division euclidienne de A par B est nul.*

Lemma 19. *Soient A et B deux polynômes non nuls de $K[X]$ tels que A divise B et que B divise A. Il existe $\lambda \in K$ non nul tel que $A = \lambda B$. On dit alors que A et B sont associés.*

Démonstration : Il existe Q et Q_1 dans $K[X]$ tels que $A = BQ$ et $B = AQ_1$, d'où $A(1 - QQ_1) = 0$. Par suite, on a $QQ_1 = 1$, autrement dit Q est inversible, d'où l'assertion (cor. 13).

3.2 Idéaux de $K[X]$ - pgcd - ppcm

Commençons par décrire tous les idéaux de $K[X]$. Rappelons que si P est un polynôme de $K[X]$, l'ensemble $(P) = \Big\{PR | R \in K[X]\Big\}$ des multiples de P est un idéal de $K[X]$. C'est l'idéal de $K[X]$ engendré par P.

Théorème 19. *Soit I un idéal non nul de $K[X]$. Il existe un unique polynôme unitaire $P \in K[X]$ tel que l'on ait $I = (P)$.*

Démonstration : Il existe P non nul dans I de degré minimum (parmi les éléments non nuls de I). Quitte à multiplier P par un élément convenable de K, on peut supposer que P est unitaire. Vérifions que l'on a $I = (P)$. D'abord tout multiple de P appartient à I. Inversement, soit A un élément de I. D'après le théorème de division euclidienne, il existe Q et R dans $K[X]$ tels que l'on ait $A = PQ + R$ avec $\deg(R) < \deg(P)$. Puisque A est dans I, le polynôme $R = A - PQ$ est aussi dans I. Le caractère minimal de P entraîne alors $R = 0$, d'où $A = PQ \in (P)$. Cela établit l'assertion d'existence. Considérons alors des polynômes unitaires F et G de $K[X]$ tels que $I = (F) = (G)$. En exprimant le fait que F est dans (G) et que G est dans (F), on constate que F et G sont associés (lemme 20).

Puisqu'ils sont unitaires, on a donc $F = G$.

pgcd de deux polynômes

Considérons deux polynômes A et B de $K[X]$ non tous les deux nuls, ainsi que l'ensemble

$$I = \Big\{AU + BV | U, V \in K[X]\Big\}.$$

On vérifie que I est un idéal non nul de $K[X]$. D'après le théorème 19, il existe donc un unique polynôme unitaire $D \in K[X]$ tel que l'on ait

$$I = (D). \tag{3.1}$$

Définition 9. *On dit que D est le plus grand commun diviseur de A et B, ou en abrégé, le pgcd de A et B.*

[2]Cette démonstration montre que le théorème de division euclidienne est aussi valable si l'on remplace K par un anneau commutatif quelconque à condition de supposer que le coefficient dominant de B soit un élément inversible.

Avec cette définition, on a de fait la propriété de Bézout dans $K[X]$, à savoir qu'il existe U et V dans $K[X]$ tels que l'on ait

$$D = AU + BV. \tag{3.2}$$

Cela étant, il convient de vérifier la propriété attendue du pgcd de deux polynômes :

Théorème 20. *Soit F un polynôme unitaire de $K[X]$. Alors, F est le pgcd de A et B si et seulement si les deux conditions suivantes sont vérifiées :*

1. *le polynôme F divise A et B.*
2. *Tout diviseur de A et B dans $K[X]$ divise F.*

Démonstration : En exprimant le fait que A et B appartiennent à I, on constate que D divise A et B. Par ailleurs, d'après (2), si un polynôme de $K[X]$ divise A et B, alors il divise D. Par suite, D vérifie les conditions 1 et 2. Inversement, soit $F \in K[X]$ réalisant ces conditions. L'égalité (2) et la condition 1 entraînent que F divise D. D'après la condition 2, D divise F. Puisque D et F sont unitaires, on a donc $F = D$.

Définition 10. *On dit que A et B sont premiers entre eux, ou que A est premier avec B, si l'on a $D = 1$.*

On a ainsi l'énoncé suivant (égalité (2) et th. 5.5) :

Corollaire 14. *Les polynômes A et B sont premiers entre eux si et seulement si il existe U et V dans $K[X]$ tels que $AU + BV = 1$.*

Théorème 21. *(Gauss) Soient F, G et H des polynômes de $K[X]$ tels que F divise GH et que F soit premier avec G. Alors, F divise H.*

Démonstration : Il existe $U, V \in K[X]$ tels que $UF+VG = 1$ (cor. 14), d'où l'égalité $(UH)F+V(GH) = H$, donc F divise H.

Remarque 12. *Compte tenu du théorème de division euclidienne, afin de déterminer le pgcd de deux polynômes, et d'obtenir explicitement une relation de Bézout, on peut utiliser, comme dans le cas de l'anneau $\mathbb{Z}$, l'algorithme d'Euclide.*

Exercice 2. Déterminer une relation de Bézout entre les polynômes $(X-1)^3$ et $(X+1)^3$ dans $\mathbb{Q}[X]$.

Exercice 3. Soient m et n deux entiers naturels non nuls. Montrer que le pgcd des polynômes $X^m - 1$ et $X^n - 1$ est $X^d - 1$ où $d = \gcd(m, n)$.

ppcm de deux polynômes

Considérons deux polynômes non nuls A et B de $K[X]$. L'ensemble $(A) \cap (B)$ est un idéal de $K[X]$. Il existe donc un unique polynôme unitaire $M \in K[X]$ tel que l'on ait

$$(A) \cap (B) = (M). \tag{3.3}$$

Définition 11. *On dit que M est le plus petit commun multiple de A et B, ou en abrégé, le ppcm de A et B.*

Théorème 22. *Soit F un polynôme unitaire de $K[X]$. Alors, F est le ppcm de A et B si et seulement si les deux conditions suivantes sont vérifiées : 1) le polynôme F est un multiple de A et B. 2) Tout multiple de A et B dans $K[X]$ est un multiple de F.*

Démonstration : Supposons $F = M$. Puisque M appartient à (A) et (B), le polynôme M est un multiple de A et B. Par ailleurs, si un polynôme de $K[X]$ est multiple de A et B, il est dans (M), c'est donc un multiple de M. Inversement, soit $F \in K[X]$ réalisant les conditions 1 et 2. On déduit de la condition 1 que F est dans (M). D'après la condition 2, M est dans (F). Par suite, on a $(M) = (F)$, puis $F = M$ vu que F et M sont unitaires.

Proposition 14. *Soit D le pgcd de A et B. On a $(AB) = (DM)$.*

Démonstration : Il s'agit de démontrer l'égalité d'idéaux

$$\left(\frac{AB}{D^2}\right) = \left(\frac{M}{D}\right).$$

L'entier M/D est le ppcm de A/D et B/D (cf. th. 22). Par ailleurs, les polynômes A/D et B/D sont premiers entre eux. On se ramène ainsi à prouver l'assertion dans le cas où $D = 1$. Supposons donc A et B premiers entre eux et vérifions que l'on a $(AB) = (M)$. Le polynôme AB est un multiple de A et B. Par ailleurs, soit C un multiple de A et B. Compte tenu du théorème 22, tout revient à vérifier que C est un multiple de AB. Il existe R et S dans $K[X]$ tels que $C = RA$ et $C = SB$. On a $RA = SB$, donc A divise SB. Puisque A est par hypothèse premier avec B, on déduit du théorème de Gauss que A divise S, ce qui entraîne le résultat.

3.3 Polynômes irréductibles

Définition 12. *Un polynôme de $K[X]$ est dit irréductible (dans $K[X]$) si son degré est supérieur ou égal à 1 et si l'ensemble de ses diviseurs est formé des éléments non nuls de K et des polynômes qui lui sont associés*[3].

Autrement dit, un polynôme $P \in K[X]$ de degré ≥ 1 est irréductible s'il ne possède pas de diviseur $Q \in K[X]$ tel que $1 \leq \deg(Q) \leq \deg(P) - 1$. Tel est le cas des polynômes de degré 1. Rappelons que ce sont les seuls si K est le corps $\mathbb{C}$ des nombres complexes. Deux polynômes irréductibles de $K[X]$ sont premiers entre eux ou sont associés. Un polynôme qui n'est pas irréductible est dit réductible.

Exercice 4. Montrer que le seul polynôme irréductible de degré 2 dans $(\mathbb{Z}/2\mathbb{Z})[X]$ est $X^2 + X + 1$.

Exercice 5. Soit p un nombre premier. Quel est le nombre de polynômes unitaires de degré 2 dans l'anneau $(\mathbb{Z}/p\mathbb{Z})[X]$? Montrer que le nombre de polynômes irréductibles unitaires de degré 2 dans cet anneau est $\frac{p(p-1)}{2}$.

Exercice 6. Montrer que le polynôme $X^2 - 2$ est irréductible dans $\mathbb{Q}[X]$.

Soit $\mathbb{P}$ l'ensemble des polynômes irréductibles unitaires de $K[X]$. Comme dans le cas de l'anneau $\mathbb{Z}$, on a le résultat suivant, qui est le théorème fondamental de l'arithmétique de $K[X]$:

Théorème 23. *Soit P un polynôme non nul de $K[X]$. Alors, P s'écrit de manière unique sous la forme*

$$P = \lambda \prod_{F \in \mathbb{P}} F^{n_F}, \tag{3.4}$$

où $\lambda \in K$, et où les n_F sont des entiers naturels nuls sauf un nombre fini d'entre eux.

Démonstration : Cet énoncé est vrai si le degré de P est nul, auquel cas on prend $\lambda = P$ et tous les n_F nuls. Considérons alors un entier $n \geq 1$. Supposons que le résultat soit vrai pour tous les polynômes de degré $\leq n - 1$ et que l'on ait $\deg(P) = n$. Soit E l'ensemble de tous les diviseurs de P de degré ≥ 1. Cet ensemble n'est pas vide car P est dans E. Il existe donc un élément $Q \in E$ de degré minimum. Ce polynôme est irréductible. Il existe $R \in K[X]$ tel que $P = QR$. On a $\deg(R) \leq n - 1$. D'après l'hypothèse de récurrence, R possède une décomposition de la forme (3.4), et il en est donc de même de P. Cela établit l'assertion d'existence. Vérifions l'assertion d'unicité. Prouvons pour cela le résultat suivant :

Lemma 20. *Soit A un polynôme irréductible divisant un produit de polynômes $A_1 \cdots A_r$ dans $K[X]$. Alors, A divise l'un des A_i.*

[3]Cette définition est un cas particulier de la notion générale d'élément irréductible dans un anneau commutatif. Si A est un tel anneau, un élément $a \in A$ est dit irréductible s'il n'est pas inversible et si ses seuls diviseurs sont les éléments inversibles et les ua où u est inversible. Les nombres premiers et leurs opposés sont les éléments irréductibles de $\mathbb{Z}$. À titre indicatif, $2X$ n'est pas irréductible dans $\mathbb{Z}[X]$.

Démonstration : Supposons le contraire. Puisque A est irréductible, cela signifie que pour tout $i = 1, \cdots, r$, les polynômes A et A_i sont premiers entre eux. Il existe donc des polynômes U_i et V_i dans $K[X]$ tels que l'on ait

$$U_i A + V_i A_i = 1 \text{ pour } i = 1, \cdots, r.$$

Par ailleurs, il existe $R \in K[X]$ tel que l'on ait

$$1 = \prod_{i=1}^{r} (U_i A + V_i A_i) = RA + \prod_{i=1}^{r} V_i A_i,$$

ce qui entraîne que A divise 1, et conduit à une contradiction.

Le théorème se déduit comme suit. Supposons que l'on ait deux décompositions de la forme (3.4) :

$$P = \lambda \prod_{F \in \mathbb{P}} F^{n_F} = \mu \prod_{F \in \mathbb{P}} F^{m_F}. \tag{3.5}$$

Soit F un élément de $\mathbb{P}$ tel que $n_F = 0$. Il résulte du lemme 20 que l'on a $m_F = 0$. Par suite, pour tout $F \in \mathbb{P}$, n_F est nul si et seulement si tel est le cas de m_F. Considérons alors $F \in \mathbb{P}$ tel que $n_F > 0$. On a donc $m_F > 0$. En divisant les membres (3.5) par F, on obtient des égalités analogues avec un polynôme de degré $\leq n - 1$. D'après l'hypothèse de récurrence, on a donc $\lambda = \mu$, $n_G = m_G$ pour tout $G \neq F$, et $n_F - 1 = m_F - 1$ i.e. $n_F = m_F$. D'où le théorème.

Comme conséquence des théorèmes 20, 22 et 23, on obtient l'énoncé suivant :

Corollaire 15. *Soient P et Q deux polynômes non nuls de K[X]. Soient*

$$P = \lambda \prod_{F \in \mathbb{P}} F^{n_F} \text{ et } Q = \mu \prod_{F \in \mathbb{P}} F^{m_F},$$

les décompositions de P et Q en produit d'éléments de $\mathbb{P}$. Soient D et M respectivement le pgcd et le ppcm de P et Q. On a alors

$$D = \lambda \prod_{F \in \mathbb{P}} F^{Min(n_F, m_F)} \text{ et } M = \mu \prod_{F \in \mathbb{P}} F^{Max(n_F, m_F)}.$$

Pour tout $F \in \mathbb{P}$, l'égalité

$$\min(n_F, m_F) + \max(n_F, m_F) = n_F + m_F,$$

entraîne alors l'égalité d'idéaux

$$(DM) = (PQ),$$

déjà démontrée dans la proposition 14.

Exercice 7. Déterminer la décomposition en produit de facteurs irréductibles du polynôme $X^4 + 1$ dans $\mathbb{R}[X]$, $(\mathbb{Z}/2\mathbb{Z})[X]$, $(\mathbb{Z}/3\mathbb{Z})[X]$ et $(\mathbb{Z}/5\mathbb{Z})[X]$. En utilisant la théorie des corps finis, qui fera l'objet du chapitre suivant, on peut en fait démontrer que le polynôme X^4+1 est réductible dans $(\mathbb{Z})/p\mathbb{Z})[X]$ pour tout nombre premier p, tout en étant irréductible dans l'anneau $\mathbb{Z}[X]$.

3.4 Racines d'un polynôme

Définition 13. *Soit $P = a_0 + \ldots + a_n X^n$ un polynôme de $K[X]$. On appelle fonction polynôme associée à P l'application $\tilde{P} : K \to K$ définie par*

$$\tilde{P}(x) = \sum_{i=0}^{n} a_i x^i \text{ quel que soit } x \in K.^4.$$

[4]On obtient ainsi une application $\Phi : K[X] \to F(K, K)$, de $K[X]$ à valeurs dans l'ensemble des applications de K dans K, définie par $\Phi(P) = \tilde{P}$. C'est un homomorphisme d'anneaux. Si K est un corps fini, cette application n'est pas injective : par exemple si $K = \mathbb{Z}/p\mathbb{Z}$ où p est premier, on a $x^p - x = 0$ pour tout $x \in K$, pour autant le polynôme $X^p - X$ n'est pas nul. Si K est infini, l'application Φ est injective comme on le constatera plus loin.

Pour tout $a \in K$ fixé, l'application $K[X] \to K$ qui à $P \in K$ associe $\tilde{P}(a)$ est un homomorphisme d'anneaux. Étant donnés $P \in K[X]$ et $a \in K$, on notera par abus $P(a)$ l'élément $\tilde{P}(a)$.

Définition 14. *Soient P un élément de $K[X]$ et a un élément de K. On dit que a est une racine de P si l'on a $P(a) = 0$.*

Lemma 21. *Soient P un élément de $K[X]$ et a un élément de K. On a $P(a) = 0$ si et seulement si $X - a$ divise P*[5]*.*

Démonstration : Supposons $P(a) = 0$. D'après le théorème de division euclidienne, il existe Q et R dans $K[X]$ tels que $P = (X-a)Q + R$ avec $\deg(R) < 1$. On a $P(a) = 0$, d'où $R(a) = 0$. Puisque R est un élément de K, on a donc $R = 0$. La réciproque est immédiate.

Remarque 13. *1) Un polynôme de $K[X]$ de degré ≥ 2 qui possède une racine dans K est réductible (lemme 21). Par ailleurs, les polynômes de $K[X]$ de degré 1 sont irréductibles et cependant ils ont une racine dans K.*

2) Soit P un polynôme de $K[X]$ de degré 2 ou 3. Alors, P est irréductible si et seulement si P n'a pas de racines dans K. C'est une conséquence de la première remarque et du fait que si $P = AB$ où $A, B \in K[X]$ sont non inversibles, alors le degré de P étant 2 ou 3, on a $\deg(A) = 1$ ou bien $\deg(B) = 1$, de sorte que P a une racine dans K.

3) Il est faux en général que la condition "P n'a pas de racines dans K" entraîne que P soit irréductible, comme le montre le polynôme $(X^2+1)^2 \in \mathbb{R}[X]$: il est réductible dans $\mathbb{R}[X]$ et sans racines dans R.

Exercice 8. Démontrer que les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 ayant un discriminant négatif (on utilisera le fait que tout polynôme à coefficients dans $\mathbb{R}$ possède une racine dans $\mathbb{C}$).

Si $a \in K$ est une racine de $P \in K[X]$, il importe souvent de connaître la plus grande puissance de $X - a$ qui divise P. Cela conduit à la notion d'ordre de multiplicité.

Définition 15. *(Ordre de multiplicité d'une racine) Soient P un polynôme non nul de $K[X]$ et $a \in K$ une racine de P. On appelle ordre de multiplicité de a (dans P) le plus grand entier naturel r tel que P soit divisible par $(X-a)^r$. Si $r = 1$, on dit que a est racine simple de P, et si $r \geq 2$, on dit que a est une racine multiple de P.*

Afin de calculer r, il convient de définir la notion de polynôme dérivé :

Définition 16. ***(Polynôme dérivé).*** *Soit $P = a_0 + a_1X + \cdots + a_nX^n$ un polynôme de $K[X]$. On appelle polynôme dérivé de P, et on le note P', le polynôme*

$$P' = \sum_{i=1}^{n} i a_i X^{i-1}.$$

En particulier, si $\deg(P) = 0$, on a $P' = 0$. On vérifie que toutes les règles de dérivation usuelles sur les fonctions d'une variable réelle restent valables dans ce contexte. En effet, pour tous P et Q dans $K[X]$, $\lambda \in K$ et $n \geq 1$, on a les relations

$$(P+Q)' = P' + Q', (\lambda P)' = \lambda P', (PQ)' = P'Q + PQ', P^n = nP^{n-1}P'.$$

[5]On peut évidemment définir, comme ci-dessus, la notion de racine d'un polynôme à coefficients dans un anneau commutatif K quelconque. Vérifions que cet énoncé est encore valable dans ce cas. Soient P un élément de $K[X]$ et $a \in K$ tels que $P(a) = 0$, et Y une autre indéterminée. En substituant à X le polynôme $a + Y \in K[Y]$, on obtient dans cet anneau le polynôme

$$P(a+Y) = a_0 + a_1Y + \cdots + a_nY^n$$

avec des $a_i \in K$. On a donc $P(a) = a_0$, d'où l'on déduit que $P(a+Y) = P(a) + YQ(Y)$ où $Q \in K[Y]$. En substituant Y par $X - a$, on a ainsi les égalités

$$P(X) = P(a) + (X-a)H(X) = (X-a)H(X),$$

où $H \in K[X]$, par suite $X - a$ divise P.

Proposition 15. *Soit P un polynôme de $K[X]$. Pour qu'un élément $a \in K$ soit racine simple de P, il faut et il suffit que l'on ait $P(a) = 0$ et $P'(a) \neq 0$.*

Démonstration : Soit a une racine de P. On a $P = (X - a)Q$ où $Q \in K[X]$. Par ailleurs, on a $P' = Q + (X - a)Q'$, d'où $Q(a) = P'(a)$. Si a est une racine simple, on a $Q(a) \neq 0$, d'où $P'(a) \neq 0$. Inversement, si $P'(a) \neq 0$, il en est de même de $Q(a)$. Par suite, $X - a$ ne divise pas Q, ce qui entraîne que $(X - a)^2$ ne divise pas P i.e. que a est racine simple de P.

Théorème 24. *Soient P un polynôme de $K[X]$ et $a_1, \ldots, a_k$ des éléments de K, distincts deux à deux, qui sont racines de P d'ordre de multiplicité $n_1, \ldots, n_k$ respectivement. Alors, il existe un polynôme $Q \in K[X]$, tel que l'on ait*

$$P = Q \prod_{i=1}^{k} (X - a_i)^{n_i},$$

et que $Q(a_i)$ soit non nul pour tout $i = 1, \ldots, k$.

Démonstration : On procède par récurrence sur k. L'énoncé est vrai si $k = 1$. Considérons un entier $k \geq 2$ tel que cet énoncé soit vrai pour l'entier $k - 1$. Il existe donc $R \in K[X]$ tel que l'on ait

$$P = R \prod_{i=1}^{k-1} (X - a_i)^{n_i}.$$

Par ailleurs, $(X - a_k)^{n_k}$ divise P et est premier avec le produit des $(X - a_i)^{n_i}$ pour i compris entre 1 et $k - 1$. En effet dans le cas contraire, d'après le lemme 20, $X - a_k$ devrait diviser l'un des facteurs $(X - a_i)^{n_i}$ ce qui conduit à une contradiction vu que $a_k \neq a_i$ pour $i = 1, \ldots, k - 1$. D'après le théorème de Gauss (th. 21), $(X - a_k)^{n_k}$ divise donc R, ce qui entraîne le résultat.

Corollaire 16. *Soit P un polynôme non nul de degré n dans $K[X]$. Alors, P possède au plus n racines distinctes dans K.*

Remarque 14. *En fait, ce résultat est encore vrai si l'anneau de base est un anneau intègre quelconque: soit F un polynôme de degré $n \geq 0$ à coefficients dans un anneau intègre A. Alors, F possède au plus n racines dans A. Pour le démontrer, on procède par récurrence sur n. Si $n = 0$, alors F est un élément non nul de A, donc ne possède aucune racine et le résultat est démontré dans ce cas. Supposons alors F de degré $n \geq 1$ et le résultat démontré pour tous les polynômes de degré $\leq n-1$. Soit $a \in A$ une racine de F. Il existe $Q \in A[X]$ tel que $F = (X - a)Q$ (lemme 21). Puisque A est intègre, le degré de Q est $n - 1$ (cela se justifie comme dans le lemme 17). Par ailleurs, si $b \in A$ est une racine de F distincte de a, on a $(b - a)Q(b) = 0$, d'où $Q(b)$ car A est intègre. Ainsi les racines de F autres que a sont celles de Q. D'après l'hypothèse de récurrence, Q possède au plus $n - 1$ racines dans A, donc F en possède au plus n, d'où le résultat.*

En revanche, ce résultat est faux en général si A n'est pas un anneau intègre. On le constate par exemple en considérant le polynôme $(X - 2)(X - 3) \in (\mathbb{Z}/6\mathbb{Z})[X]$, qui est de degré 2, et qui possède quatre racines dans $\mathbb{Z}/6\mathbb{Z}$, à savoir les classes de 0, 2, 3 et 5. Tel est aussi le cas du polynôme $2X \in (\mathbb{Z}/4\mathbb{Z})[X]$ qui possède comme racines les classes de 0 et de 2 modulo $4\mathbb{Z}$. Il existe aussi des anneaux non intègres sur lesquels il existe des polynômes de degré 2 ayant une infinité de racines. En effet, soient E un ensemble infini et A l'anneau formé de l'ensemble des parties de E muni de la différence symétrique Δ et de l'intersection comme addition et multiplication. Rappelons que si U et V sont deux parties de E, on a par définition $U \triangle V = U \cup V \setminus U \cap V$. L'élément neutre additif est l'ensemble vide et l'élément neutre multiplicatif est l'ensemble E. Toute partie U de E est alors racine du polynôme $X^2 + X \in A[X]$, qui a donc une infinité de racines si E est infini: on a ici $U^2 + U = (U \cap U) \triangle U = U \triangle U = \emptyset$.

Signalons le résultat suivant (exercice) : soit A un anneau commutatif non nul qui n'est pas isomorphe à $\mathbb{Z}/4\mathbb{Z}$ ni à $(\mathbb{Z}/2\mathbb{Z})[X]/(X^2)$. Alors, A est intègre si et seulement si tout polynôme unitaire de $A[X]$ de degré 2 a au plus deux racines dans A.

Démonstration : Si P possédait (au moins) $n+1$ racines dans K il serait divisible par un polynôme de $K[X]$ de degré $n+1$, ce qui contredit le fait que P soit de degré n.

Ce résultat entraîne le fait que l'application $\Phi : K[X] \to F(K,K)$ définie par l'égalité $\Phi(P) = \tilde{P}$ est injective si K est infini. En effet, si la fonction polynôme $\tilde{P}$ associée à P est nulle sur K, cela signifie que P a une infinité de racines (car K est infini), et d'après le résultat précédent, P doit être le polynôme nul. Par suite, sur un corps infini, on peut identifier $K[X]$ et l'anneau des fonctions polynômes sur K i.e. l'image de Φ.

Comme application de ce qui précède, démontrons le théorème de Wilson (1741-1793), qui est une caractérisation des nombres premiers :

Théorème 25. *(Wilson) Soit p un entier ≥ 2. Alors, p est premier si et seulement si $(p-1)!+1$ est divisible par p.*

Démonstration : Supposons que p soit un nombre premier. Il résulte du petit théorème de Fermat que pout tout a compris entre 1 et $p-1$, l'élément $a+p\mathbb{Z}$ est racine du polynôme $X^{p-1}-1 \in (\mathbb{Z}/p\mathbb{Z})[X]$. D'après le théorème 24, on en déduit que l'on a dans cet anneau

$$X^{p-1}-1 = \prod_{a=1}^{p-1}(X-\bar{a}).$$

En exprimant le fait que les termes constants sont les mêmes, on obtient l'égalité dans le corps $\mathbb{Z}/p\mathbb{Z}$:

$$-\bar{1} = (-1)^{p-1}\prod_{a=1}^{p-1}\bar{a}.$$

Autrement dit, on a la congruence

$$-\bar{1} = (-1)^{p-1}(p-1)! \bmod .p,$$

par suite p divise $(p-1)!+1$. Inversement, supposons $(p-1)!+1$ divisible par p. Si ℓ est un diviseur positif de p autre que p, alors ℓ divise $(p-1)!$, d'où $\ell = 1$ et le fait que p soit un nombre premier.

Remarque 15. *1) Pour démontrer le théorème 25 on peut aussi utiliser l'argument suivant. Supposons p premier. Dans le corps $\mathbb{Z}/p\mathbb{Z}$, les seuls éléments égaux à leur inverse sont ± 1. Il en résulte que l'on a (en regroupant chaque terme du produit avec son inverse modulo p)*

$$\prod_{k=2}^{p-2} k = 1 \bmod p.$$

Par suite, on a $(p-1)! = p-1 \bmod p$ i.e. $(p-1)!+1 = 0 \bmod p$.

2) Le théorème de Wilson est un test de primalité, mais il n'est pas efficace car le calcul de $(p-1)!$ nécessite beaucoup d'opérations. Signalons que si p est un nombre premier, on définit le quotient de Wilson

$$W(p) = \frac{(p-1)!+1}{p},$$

qui est donc un entier. On dit que p est un nombre premier de Wilson si p divise $W(p)$, autrement dit, si l'on a $(p-1)!+1 = 0 \bmod p^2$. Par exemple, 5 et 13 sont des nombres premiers de Wilson. La question de savoir s'il existe une infinité de tels nombres premiers est ouverte. En dehors de 5 et 13, on ne connaît qu'un seul autre nombre premier de Wilson, à savoir 563 (découvert en 1953). Il n'y en a pas d'autres plus petits que 5.10^8.

3.5 Les algèbres quotients de $K[X]$ modulo un idéal

Étant donné un idéal I de $K[X]$, on va définir dans ce paragraphe une structure naturelle de K-algèbre sur l'ensemble quotient $K[X]/I$. Afin de définir une structure de K-algèbre, il faut définir une structure d'anneau et une structure de K-espace vectoriel. Rappelons la définition de cette notion en commençant par celle d'espace vectoriel sur K.

Définition 17. *On appelle K-espace vectoriel tout ensemble E muni d'une structure définie par la donnée :*

1. *d'une loi de groupe abélien sur E ;*
2. *d'une application $K \times E \to E$, notée $(\lambda, x) \mapsto \lambda x$, souvent appelée loi de composition externe, pour laquelle on a les relations*

$$(\lambda + \mu)x = \lambda x + \mu x, (x + y) = x + y, \lambda(\mu x) = (\lambda\mu)x, 1x = x,$$

quels que soient $x, y \in E$ et $\lambda, \mu \in K$.

Définition 18. *On appelle K-algèbre tout ensemble E muni d'une structure définie par la donnée :*

1. *de deux lois de composition sur E, une addition $+$ et une multiplication $\times$, telles que $(E, +, \times)$ soit un anneau,*
2. *d'une loi de composition externe $K \times E \to E$, notée $(\lambda, x) \mapsto x$, qui avec la loi additive $+$, munie E d'une structure de K-espace vectoriel, de telle sorte que la condition suivante soit satisfaite :*
3. *quels que soient $\lambda \in K$ et $x, y \in E$, on a*

$$\lambda(x \times y) = (\lambda x) \times y = x \times (\lambda y). \tag{3.6}$$

On définit la notion d'homomorphisme de K-algèbres entre deux K-algèbres. Ce sont les applications K-linéaires qui sont en même temps des homomorphismes d'anneaux. Deux K-algèbres sont dites isomorphes si elles sont liées par un homomorphisme bijectif. On omet très souvent, par abus, la notation $\times$ dans les calculs dans les K-algèbres. Cela ne prête pas à confusion pourvu que l'on précise la nature des éléments que l'on compose. La condition (6) s'écrit alors

$$\lambda(xy) = (\lambda x)y = x(\lambda y) \text{ quels que soient } \lambda \in K \text{ et } x, y \in E.$$

Exemples 5.1.

1. Pour tout $n \geq 1$, l'ensemble $K^n = K \times \cdots \times K$ (n facteurs) est muni d'une structure de K-algèbre, pour laquelle la structure d'anneau est définie et la loi externe est donnée par l'égalité

$$\lambda(x_1, \ldots, x_n) = (\lambda x_1, \ldots, \lambda x_n) \text{ quels que soient } \lambda \in K \text{ et } (x_1, \ldots, x_n) \in K^n.$$

   Notons que l'on a $\lambda(x_1, \ldots, x_n) = (\lambda, \ldots, \lambda)(x_1, \ldots, x_n)$, et que l'application $K \to K^n$ qui à λ associe $(\lambda, \ldots, \lambda)$ est un homomorphisme de K-algèbres injectif, que l'on appelle le plongement diagonal de K dans K^n.

2. Si L est un surcorps (commutatif) de K, alors L est muni de la structure de K-algèbre, pour laquelle la structure d'anneau sur L est celle donnée dans sa définition de corps et la loi externe $K \times L \to L$ est celle qui au couple $(\lambda, x) \in K \times L$ associe le produit λx dans L.

3. L'anneau $K[X]$ est muni de la structure de K-algèbre pour laquelle la structure d'anneau est celle définie précédemment et la loi externe $K \times K[X] \to K[X]$ est celle qui au couple (λ, P) associe le polynôme λP obtenu en multipliant dans K les coefficients de P par λ.

4. L'anneau des matrices carrées $M_n(K)$ est aussi naturellement muni d'une structure de K-algèbre (exercice : expliciter cette structure).

Structure de K-algèbre sur le quotient de $K[X]$ modulo un idéal

Considérons un idéal I de $K[X]$. Nous allons munir ici l'ensemble quotient $K[X]/I$ d'une structure de K-algèbre. Pour tout $P \in K[X]$, posons $\bar{P} = P + I$ la classe de P modulo I. Rappelons que P est le sous-ensemble de $K[X]$ formé des polynômes Q tels que $P - Q$ appartienne à I. L'ensemble $K[X]/I$ est muni de la structure d'anneau définie par les égalités

$$\bar{P} + \bar{Q} = \overline{P + Q}, \tag{3.7}$$

$$\bar{P}\bar{Q} = \overline{PQ}, \tag{3.8}$$

quels que soient P et Q dans $K[X]$. L'élément neutre additif est $\bar{0} = I$ et l'élément neutre multiplicatif est $\bar{1}$.

Cet anneau est aussi muni d'une structure de K-espace vectoriel définie comme suit. Tout d'abord, muni de son addition définie par l'égalité (3.7), $K[X]/I$ est un groupe abélien. Par ailleurs, l'application

$$K \times K[X]/I \to K[X]/I$$

qui au couple $(\lambda, \bar{P}) \in K \times K[X]/I$ associe $\overline{\lambda P}$ réalise la condition 2 de la définition 17. Avec les notations de cette définition, on a donc l'égalité

$$\lambda \bar{P} = \overline{\lambda P}. \tag{3.9}$$

Il convient de vérifier que cette définition a bien un sens, autrement dit, qu'elle ne dépend que de la classe de P et non pas d'un de ses représentants. Considérons pour cela P et Q dans $K[X]$ tels que $\bar{P} = \bar{Q}$. Le polynôme $P - Q$ appartient à I, par suite $\lambda(P - Q)$ est aussi dans I. De l'égalité $\lambda(P - Q) = \lambda P - \lambda Q$, on déduit alors que $\overline{\lambda P} = \overline{\lambda Q}$, d'où notre assertion. Les relations de la condition 2 sont alors des conséquences directes des égalités (3.7) et (3.9). Les égalités (3.7), (3.8) et (3.9) munissent ainsi $K[X]/I$ d'un structure de K-algèbre.

Remarque 16. *1. Il résulte des égalités (3.8) et (3.9) que l'on a pour tous $\lambda \in K$ et $P \in K[X]$,*

$$(\lambda + I)(P + I) = \lambda P + I = \lambda(P + I). \tag{3.10}$$

2. Supposons I distinct de $K[X]$. Le corps K est isomorphe à un sous-anneau de $K[X]/I$. En effet, soit $i : K \to K[X]/I$ l'application définie par

$$i(\lambda) = \lambda + I.$$

Puisque l'on a $I \neq K[X]$, i est un homomorphisme d'anneaux injectif. En effet, il résulte des définitions que i est un homomorphisme d'anneaux. Par ailleurs, soit λ dans K tel que $\lambda + I = 0$ i.e. tel que λ soit dans I. Puisque l'on a $I \neq K[X]$, et que les éléments non nuls de K sont inversibles dans $K[X]$, on a donc $\lambda = 0$ et i est injectif. Ainsi $i(K)$ est un sous-anneau de $K[X]/I$ isomorphe à K. Au cours des calculs dans l'algèbre $K[X]/I$, on identifie toujours K et $i(K)$. Avec cette identification, la multiplication dans $K[X]/I$ par un élément de K se note de la même façon que la loi externe de K sur $K[X]/I$ (cf. l'égalité (3.10) dans laquelle $\lambda + I$ est identifié à λ).

Si I n'est pas nul, il existe alors un polynôme P tel que l'on ait $I = (P)$ (th. 19) (on peut si on le souhaite demander que P soit unitaire, auquel cas il y a unicité de P, mais peu importe ici). Le chapitre suivant est consacré, entre autres, à l'étude des algèbres $K[X]/(P)$ dans le cas où K est un corps fini. Décrivons maintenant quelques propriétés des algèbres $K[X]/(P)$ en termes du polynôme P, que l'on utilisera dans la suite. Commençons par une propriété fondamentale concernant la structure de K-espace vectoriel.

Théorème 26. *Soit P un polynôme de $K[X]$ degré $n \geq 0$. Le K-espace vectoriel $K[X]/(P)$ est de dimension finie n. Plus précisément, en posant $\alpha = X + (P)$, le système $(\alpha_i)_{0 \leq i \leq n-1}$ est une K-base de $K[X]/(P)$.*

Démonstration : Vérifions que $(\alpha_i)_{0\leq i\leq n-1}$ est un système libre. Soient $0,\ldots,n-1$ des éléments de K tels que

$$\sum_{i=0}^{n-1}\lambda_i\alpha^i=0.$$

Cette égalité signifie que l'on a

$$\sum_{i=0}^{n-1}\lambda_i X^i\in(P).$$

Puisque P est de degré n, cela entraîne que tous les λ_i sont nuls. Démontrons que le système considéré est générateur. Soit ξ un élément de $K[X]/(P)$. Il existe un polynôme $F\in K[X]$ tel que $\xi=F+(P)$. On a $P\neq 0$. D'après le théorème de division euclidienne, il existe Q et R dans $K[X]$ tels que l'on ait $F=PQ+R$ avec $\deg(R)<\deg(P)$. On a donc $\xi=\bar{R}$, ce qui entraîne notre assertion et le résultat.

Le lemme suivant est d'un usage constant pour effectuer des calculs dans les K-algèbres quotients de $K[X]$:

Lemma 22. *Soit $P=a_0+a_1X+\ldots+a_nX^n\in K[X]$ un polynôme degré $n\geq 0$. Posons $\alpha=X+(P)\in K[X]/(P)$. On a l'égalité*

$$\sum_{i=0}^{n}a_i\alpha^i=0. \tag{3.11}$$

Démonstration : On a $\bar{P}=0$. Cette égalité signifie que l'on a

$$\sum_{i=0}^{n}\overline{a_iX^i}=\sum_{i=0}^{n}a_i\bar{X}^i=0,$$

d'où l'assertion.

Remarque 17.

1. *Dans l'énoncé du théorème 26, si $n=0$, alors la dimension de $K[X]/(P)$ est nulle et la base vide est une base de cet espace vectoriel. Cela était prévisible vu que P est dans ce cas un élément non nul de K, donc est inversible dans $K[X]$, par suite $(P)=K[X]$ et le quotient $K[X]/(P)$ est l'anneau nul.*

2. *Le théorème 26 se traduit par l'égalité*

$$K[X]/(P)=\left\{\sum_{i=0}^{n-1}a_i\alpha^i|a_i\in K\right\}.$$

3. *En identifiant K et son image dans $K[X]/(P)$, l'égalité (3.11) s'obtient alors en substituant X par α dans P (cf. (3.10)). Elle peut donc aussi s'écrire $P(\alpha)=0$.*

4. *Si I est l'idéal nul, $K[X]/I$ est isomorphe comme K-algèbre à $K[X]$. En particulier, $K[X]/I$ est dans ce cas un K-espace vectoriel de dimension infinie (une K-base de $K[X]$ est formée des $(X^n)_{n\geq 0}$).*

5. *Soient x et y deux élément de $K[X]/(P)$ ($P\in K[X]$ de degré $n\geq 1$). Ils s'écrivent de manière unique sous la forme*

$$x=\sum_{i=0}^{n-1}a_i\alpha^i\ \text{ et }\ y=\sum_{i=0}^{n-1}b_i\alpha^i,$$

où les a_i et b_i sont dans K. Les coordonnées de $x+y$ dans la base (α^i) sont les a_i+b_i. Il est moins simple d'obtenir les coordonnées du produit xy. Afin de les déterminer, on utilise l'égalité fondamentale (3.11). On peut alors procéder de deux façons. La première consiste par exemple à déterminer le reste R de la division euclidienne du polynôme produit $(\sum a_iX^i)(\sum b_iX^i)$ par P. On a alors

$$xy=R(\alpha),$$

et R étant de degré $\leq n-1$, on obtient les coordonnées cherchées. On peut aussi utiliser directement l'égalité (3.11), afin de déduire les coordonnées des α^k pour $k \geq n$, puis celles de xy.

Le résultat qui suit concerne la structure d'anneau de $K[X]/(P)$, qui n'est autre que l'analogue d'un théorème sur la description des éléments inversibles des quotients de $\mathbb{Z}$.

Théorème 27. *Soit P un polynôme de $K[X]$ de degré $n \geq 0$. Le groupe des éléments inversibles de l'anneau $K[X]/(P)$ est formé des classes de polynômes $F \in K[X]$ telles que F soit premier avec P.*

Démonstration : Soit F un polynôme de $K[X]$ premier avec P. Il existe U et V dans $K[X]$ tels que $UP + VF = 1$. On a donc $\bar{V}\bar{F} = 1$, ce qui prouve que F est inversible. Inversement, soit F un élément inversible de $K[X]/(P)$. Il existe alors $Q \in K[X]$ tel que $\bar{F}\bar{Q} = 1$. Cette égalité signifie que $FQ - 1$ appartient à (P), autrement dit qu'il existe $U \in K[X]$ tel que $FQ + UP = 1$, donc F et P sont premiers entre eux, d'où le résultat.

Corollaire 17. *Soit P un polynôme de $K[X]$ de degré $n \geq 0$. Les conditions suivantes sont équivalentes :*

1. *l'anneau $K[X]/(P)$ est intègre.*
2. *Le polynôme P est irréductible dans $K[X]$.*
3. *L'anneau $K[X]/(P)$ est un corps.*

Démonstration : Supposons que $K[X]/(P)$ soit intègre. Tout d'abord, P n'est pas inversible, sinon on a $(P) = K[X]$ et $K[X]/(P)$ est l'anneau nul, ce qui est exclu par définition. Soit F un diviseur de P. Il s'agit de montrer que F est inversible ou bien que F et P sont associés. Il existe $Q \in K[X]$ tel que $P = FQ$, d'où $\bar{F}\bar{Q} = 0$. Par hypothèse, cela entraîne que $\bar{F} = 0$ ou bien que $\bar{Q} = 0$. Si $\bar{F} = 0$, alors F est dans (P) i.e. P divise F, donc P et F sont associés. Si $\bar{Q} = 0$, alors Q et P sont associés, par suite on a $\deg(F) = 0$ i.e. F est inversible. Cela prouve que P est irréductible dans $K[X]$. Supposons alors P irréductible dans $K[X]$ et prouvons que tout élément non nul $\bar{F}$ de $K[X]/(P)$ est inversible. Puisque P est irréductible et que P ne divise pas F, les polynômes F et P sont premiers entre eux. D'après le théorème 27, F est donc inversible, donc $K[X]/(P)$ est un corps. La dernière implication est immédiate.

On déduit de ce qui précède le résultat fondamental suivant :

Théorème 28. *Soit P un polynôme irréductible de $K[X]$. Il existe un corps commutatif L contenant K comme sous-corps et possédant les deux propriétés suivantes :*

1. *le polynôme P a une racine dans L.*
2. *Le K-espace vectoriel L est de dimension finie sur K, égale au degré de P.*

Démonstration : Puisque P est irréductible, l'anneau $A = K[X]/(P)$ est un corps (cor. 17). Soit $i : K \to A$ l'application définie pour tout $\lambda \in K$ par $i(\lambda) = \lambda + (P)$. Soient Z le complémentaire de $i(K)$ dans A, et L la réunion des ensembles K et Z. L'application $\psi : A \to L$ définie pour tout $\lambda \in K$ et tout $x \in Z$ par

$$\psi(i(\lambda)) = \lambda \text{ et } \psi(x) = x,$$

est une bijection de A sur L. Par transport de structure via ψ, on peut donc munir L d'une structure de K-algèbre : pour tous ξ_1 et ξ_2 dans L, on définit l'addition et la multiplication par les formules :

$$\xi_1 + \xi_2 = \psi\big(\psi^{-1}(\xi_1) + \psi^{-1}(\xi_2)\big) \text{ et } \xi_1 \times \xi_2 = \psi\big(\psi^{-1}(\xi_1) \times \psi^{-1}(\xi_2)\big),$$

la loi externe de K sur L étant définie pour tous $\lambda \in K$ et $\xi \in L$ par l'égalité

$$\lambda \cdot \xi = \psi(\lambda \cdot \psi^{-1}(\xi)).$$

Par définition des lois de composition sur L, les K-algèbres A et L sont isomorphes via ψ et l'on a $\psi(i(K)) = K$. En particulier, L est de dimension finie sur K, égale au degré de P (th. 26), et L est un surcorps de K. Il reste à vérifier que P a une racine dans L. Soit α la classe de X modulo (P). On a $\bar{P} = 0$, autrement dit, si $P = a_0 + \cdots + a_n X^n$, on a $i(a_0) + \cdots + i(a_n)\alpha^n = 0$ et en prenant l'image par ψ des deux membres de cette égalité, on obtient $P(\psi(\alpha)) = 0$ i.e. $\psi(\alpha)$ est une racine de P dans L, d'où le résultat.

Remarque 18. *1. Dans la démonstration précédente, on a utilisé le fait qu'étant donnés deux ensembles X et Y, il en existe un autre contenant à la fois X et Y, à savoir leur réunion. Il convient de noter que cela est un axiome de la théorie des ensembles.*

2. Si $P \in K[X]$ n'est pas irréductible, de degré ≥ 1, il existe aussi un surcorps de K dans lequel P a une racine, car P est produit de polynômes irréductibles (th. 23).

3. Considérons la question suivante : soit L un corps commutatif contenant K dans lequel le polynôme P a une racine. Alors, P a-t-il toutes ses racines dans L, autrement dit, P est-il produit de polynômes de degré 1 dans $L[X]$? La réponse est négative en général. En effet, prenons par exemple $K = \mathbb{Q}$ et $P = X^3 - 2 \in \mathbb{Q}[X]$. Soient α la racine réelle de P et L le sous-ensemble de $\mathbb{R}$ formé des éléments $a + b\alpha + c\alpha^2$ où $a, b, c \in \mathbb{Q}$. Alors, L est un sous-corps de $\mathbb{R}$ et α est la seule racine de P dans L vu que ses deux autres racines, $j\alpha$ et $j\alpha^2$ avec $j^3 = 1$ et $j \neq 1$, ne sont pas réelles. Cela étant, on démontrera au chapitre suivant que la réponse est positive si K et L sont des corps finis.

Exemples 2.

1. Prenons $K = \mathbb{Z}/2\mathbb{Z}$ et $P = X^3 + X + 1 \in K[X]$. Puisque P est de degré 3 et qu'il n'a pas de racines dans $\mathbb{Z}/2\mathbb{Z}$, il est irréductible dans $(\mathbb{Z}/2\mathbb{Z})[X]$. Le quotient $K[X]/(P)$ est donc un corps et un espace vectoriel de dimension 3 sur $\mathbb{Z}/2\mathbb{Z}$. En particulier, c'est un corps à huit éléments (cf. la décomposition des éléments dans une base). Vérifions que P a toutes ses racines dans K. Si α est la classe de X modulo (P), on a $P(\alpha) = 0$, ce qui entraîne

$$P = (X - \alpha)(X^2 + \alpha X + 1 + \alpha^2).$$

On vérifie ensuite que α^2 et $\alpha^4 = \alpha + \alpha^2$ sont racines de $X^2 + \alpha X + 1 + \alpha^2$. (Le corps considéré ayant huit éléments, on peut par exemple tester tous les éléments pour trouver les racines. Notons que les formules classiques de résolution d'une équation du second degré ne fonctionnent pas ici car $2 = 0$. On peut aussi remarquer que si β est racine d'un polynôme de$(\mathbb{Z}/2\mathbb{Z})[X]$, il en est de même de β^2 : cf. la formule du binôme de Newton. Cette remarque sera généralisée au chapitre suivant). On a donc (puisque -1 = 1 dans K)

$$P = (X + \alpha)(X + \alpha^2)(X + \alpha + \alpha^2).$$

2. Prenons $K = \mathbb{Q}$ et $P = X^3 + X + 1 \in \mathbb{Q}[X]$. La $\mathbb{Q}$-algèbre $\mathbb{Q}[X]/(P)$ est de dimension 3 (pour tout corps K, la dimension d'une K-algèbre est sa dimension en tant que K-espace vectoriel). Si $\alpha = X + (P)$, le système $(1, \alpha, \alpha^2)$ est une $\mathbb{Q}$-base de $\mathbb{Q}[X]/(P)$. On a $P(\alpha) = 0$. Explicitons les coordonnées de l'élément $\alpha^5 + 1$ dans la base $(1, \alpha, \alpha^2)$. On peut effectuer pour cela la division euclidienne du polynôme $X^5 + 1$ par P. On trouve

$$X^5 + 1 = (X^2 - 1)P + (-X^2 + X + 2),$$

de sorte que l'on obtient $\alpha^5 + 1 = -\alpha^2 + \alpha + 2$ et les coordonnées cherchées sont donc $(2, 1, -1)$. Vérifions que $\mathbb{Q}[X]/(P)$ est un corps, autrement dit que P est irréductible dans $\mathbb{Q}[X]$. Puisque P est de degré 3, il s'agit de montrer que P n'a pas de racines dans $\mathbb{Q}$. On utilise pour cela le lemme suivant très utile en pratique :

Lemma 23. *Soit $F = a_0 + \cdots a_{n-1}X^{n-1} + X^n \in \mathbb{Z}[X]$ un polynôme unitaire de degré n. Alors, si F a une racine dans $\mathbb{Q}$, elle est dans $\mathbb{Z}$ et elle divise a_0.*

Démonstration : Soit β une racine de F dans $\mathbb{Q}$. Posons $\beta = u/v$, où u et v sont deux entiers premiers entre eux. On a l'égalité

$$v^n a0 + a_1 v^{n-1} u + \ldots + a_{n-1} v u^{n-1} + u_n = 0.$$

Il en résulte que v divise u^n, puis que $v = \pm 1$ car u et v sont premiers entre eux. Ainsi

β est dans $\mathbb{Z}$. Par ailleurs, u divise $v^n a_0 = \pm a_0$, d'où le lemme.

Notre assertion s'en déduit aussitôt : si F a une racine dans $\mathbb{Q}$, cette racine est ± 1, qui n'est pas racine de F.

À titre indicatif, déterminons les coordonnées de l'inverse de l'élément $1+\alpha$ dans la base $(1, \alpha, \alpha^2)$. Voici une méthode possible. On considère le $\mathbb{Q}$-endomorphisme ψ de $\mathbb{Q}[X]/(P)$ défini par $a \mapsto a(1+\alpha)$ (c'est l'endomorphisme de multiplication par $1+\alpha$). C'est un endomorphisme bijectif. La matrice de ψ dans la base considérée est

$$M = \begin{pmatrix} 1 & 0 & -1 \\ 1 & 1 & -1 \\ 0 & 1 & 1 \end{pmatrix}.$$

On vérifie que l'inverse de M est

$$M^{-1} = \begin{pmatrix} 2 & -1 & 1 \\ -1 & 1 & 0 \\ 1 & -1 & 1 \end{pmatrix}.$$

L'image de 1 par ψ^{-1} est alors l'élément cherché. On trouve ainsi

$$(1+\alpha)^{-1} = 2 - \alpha + \alpha^2.$$

Une autre méthode consiste à utiliser l'algorithme d'Euclide. On trouve que l'on a la relation de Bézout

$$(1+X)(X^2 - X + 2) - (X^3 + X + 1) = 1,$$

d'où de nouveau l'égalité ci-dessus.

3. Vérifions que le corps $\mathbb{C}$ des nombres complexes est isomorphe à $\mathbb{R}[X]/(X^2+1)$. On remarque d'abord que X^2+1, n'ayant pas de racines dans $\mathbb{R}$, est irréductible dans $\mathbb{R}[X]$, donc $\mathbb{R}[X]/(X^2+1)$ est un corps. C'est par ailleurs un espace vectoriel de dimension 2 sur $\mathbb{R}$. Considérons alors l'application $\psi : \mathbb{R}[X] \to \mathbb{C}$ définie par $\psi(F) = F(i)$ où $i^2 = -1$ (cette égalité signifie que l'on a choisi implicitement une racine carrée i de -1 dans $\mathbb{C}$). C'est un homomorphisme de corps. Il est surjectif puisque $\psi(a+bX) = a+ib$ pour tous $a, b \in \mathbb{R}$. Vérifions que son noyau est (X^2+1), ce qui, compte tenu d'un théorème, prouvera notre assertion. Tout d'abord, il est immédiat de constater que l'idéal (X^2+1) est contenu dans $Ker(\psi)$. Inversement, soit F un élément de $Ker(\psi)$. Il existe deux polynômes Q et R de $\mathbb{R}[X]$ tels que $F = (X^2+1)Q + R$ avec $\deg(R) \leq 1$. On a donc $\psi(F) = \psi(R) = 0$. Par suite, si $R = aX + b$, on a l'égalité $ai + b = 0$, d'où $a = b = 0$ puis $R = 0$, donc F appartient à (X^2+1). On a ainsi $\ker(\psi) = (X^2+1)$. Vu que ψ est $\mathbb{R}$-linéaire, on a en fait montré que les $\mathbb{R}$-algèbres $\mathbb{C}$ et $\mathbb{R}[X]/(X^2+1)$ sont isomorphes. On pourrait ainsi poser par définition $\mathbb{C} = \mathbb{R}[X]/(X^2+1)$[6].

Nous verrons dans le chapitre suivant que tous les corps finis s'obtiennent par une construction analogue à la précédente qui fait passer de $\mathbb{R}$ à $\mathbb{C}$.

[6]Rappelons que l'on peut définir le corps $\mathbb{C}$ comme le produit cartésien $\mathbb{R} \times \mathbb{R}$ muni des deux lois de compositions suivantes : pour tous (x, y) et $(z, t) \in \mathbb{R} \times \mathbb{R}$, on pose

$$(x, y) + (z, t) = (x + z, y + t) \text{ (l'addition)},$$

$$(x, y) \times (z, t) = (xz - yt, xt + yz) \text{ (la multiplication)}.$$

On vérifie alors que le triplet $(\mathbb{C}, +, \times)$ est un corps commutatif, appelé corps des nombres complexes. L'application de $\mathbb{R}$ dans $\mathbb{C}$ qui à x associe $(x, 0)$ est un homomorphisme de corps, donc est injectif. On note i l'élément $(0, 1)$. En identifiant $\mathbb{R}$ et son image dans $\mathbb{C}$, on a alors l'égalité attendue $i^2 = -1$ et tout nombre complexe s'écrit de façon unique sous la forme $a + ib$ avec $a, b \in \mathbb{R}$.

Chapter 4

Corps finis - Construction

L'objectif de ce chapitre est de construire les corps finis et de donner quelques applications à la cryptographie. On admettra dans toute la suite le résultat suivant, dont la démonstration dépasserait le niveau de ce cours :

Théorème 29. ***(Wedderburn 1882 - 1948)*** *Tout corps fini est commutatif.*

Les premiers exemples de corps finis sont les quotients de l'anneau $\mathbb{Z}$

$$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z},$$

où p est un nombre premier. Compte tenu du chapitre précédent, d'autres exemples sont fournis par les quotients

$$\mathbb{F}_p[X]/(F),$$

où F est un polynôme irréductible de $\mathbb{F}_p[X]$. Ce sont en effet des corps (cor. **??**), et ils sont finis, puisqu'ils sont de dimension finie sur $\mathbb{F}_p$. Nous reviendrons sur ce point, et démontrerons que l'on obtient de la sorte tous les corps finis. On prouvera dans les sept premiers paragraphes les énoncés suivants :

1. tout corps fini contient un sous-corps isomorphe à un corps $\mathbb{F}_p$.
2. Le cardinal d'un corps fini est une puissance d'un nombre premier.
3. Le groupe multiplicatif d'un corps fini est cyclique.
4. Tout corps fini K de cardinal p^n est isomorphe à $\mathbb{F}_p[X]/(F)$, où F est un polynôme irréductible de degré n dans $\mathbb{F}_p[X]$.
5. Pour tout nombre premier p et tout entier $n \geq 1$, il existe un corps à p^n éléments et il est unique à isomorphisme près.

Il est assez simple de démontrer les quatre premiers résultats, notamment les 1, 2 et 4. Le cinquième l'est beaucoup moins.

4.1 Caractéristique d'un anneau

Soit A un anneau. Notons 1_A l'élément neutre multiplicatif de A. Soit $f : \mathbb{Z} \to A$ l'application de $\mathbb{Z}$ dans A définie par

$$f(m) = m1_A \text{ pour tout } m \in \mathbb{Z}. \tag{4.1}$$

C'est un homomorphisme d'anneaux de $\mathbb{Z}$ dans A (et d'ailleurs le seul). Son noyau est un idéal de $\mathbb{Z}$. Il existe donc un unique entier naturel n tel que l'on ait

$$Ker(f) = n\mathbb{Z}.$$

Définition 19. *L'entier n est la caractéristique de A.*

Lemma 24. *Si A est intègre, sa caractéristique est nulle ou est un nombre premier. Tel est en particulier le cas si A est un corps commutatif.*

Démonstration : L'anneau $\mathbb{Z}/n\mathbb{Z}$ est isomorphe à un sous-anneau de A, à savoir l'image de f. Puisque A est intègre, il en est donc de même de $\mathbb{Z}/n\mathbb{Z}$. Si n n'est pas nul, $\mathbb{Z}/n\mathbb{Z}$ est alors un corps , et n est un nombre premier.

Théorème 30. *Soit K un corps commutatif d'élément neutre multiplicatif 1_K. Soit m un entier relatif.*

1. *Supposons K de caractéristique zéro. On a $m1_K = 0$ si et seulement si $m = 0$. Dans ce cas, K contient un sous-corps isomorphe à $\mathbb{Q}$.*
2. *Supposons K de caractéristique un nombre premier p. On a $m1_K = 0$ si et seulement si p divise m. Dans ce cas, K contient un sous-corps isomorphe à $\mathbb{F}_p$.*

Démonstration : Supposons K de caractéristique 0. L'homomorphisme f défini par (1) est alors injectif, d'où l'équivalence annoncée. L'application de $\mathbb{Q}$ dans K qui à $a/b \in \mathbb{Q}$ associe $a1_K(b1_K)^{-1}$, prolonge f de $\mathbb{Z}$ à $\mathbb{Q}$, et est un homomorphisme de corps. (Notons que b étant non nul, on a $b1_K \neq 0$ et l'on vérifie que f est bien définie). Son image est donc un sous-corps de K isomorphe à $\mathbb{Q}$. Si K est de caractéristique p, le noyau de f est l'idéal $p\mathbb{Z}$. Par suite, on a $m1_K = 0$ i.e. m appartient au noyau de f si et seulement si p divise m. L'image de f est alors un sous-corps de K isomorphe à $\mathbb{F}_p$.

Par exemple $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont de caractéristique 0. Pour tout p premier, $\mathbb{F}_p$ est de caractéristique p. On obtient aussitôt les résultats 1 et 2 énoncés précédemment :

Corollaire 18. *Soit K un corps fini. La caractéristique de K est un nombre premier p et K contient un sous-corps isomorphe à $\mathbb{F}_p$. De plus, il existe un entier $n \geq 1$ tel que le cardinal de K soit p^n.*

Démonstration : Puisque K est fini, K ne contient pas de sous-corps isomorphe à $\mathbb{Q}$. La caractéristique de K est donc un nombre premier p et K contient un sous-corps isomorphe à $\mathbb{F}_p$ (th. 30). Par suite, K est naturellement muni d'une structure d'espace vectoriel sur $\mathbb{F}_p$ (cf. exemples 5.1). Le corps K étant fini, la dimension de K sur $\mathbb{F}_p$ est aussi finie. Si n est cette dimension, K est donc isomorphe, comme espace vectoriel, à $\mathbb{F}_p^n$, et K est de cardinal p^n.[1]

Corollaire 19. *Soit K un corps fini de cardinal p. Alors, K est isomorphe à $\mathbb{F}_p$.*

Démonstration : C'est immédiat vu que K contient un sous-corps isomorphe à $\mathbb{F}_p$.

Corollaire 20. *Soient K un corps fini, de caractéristique p, et F un polynôme irréductible de degré n dans $K[X]$. Alors, $K[X]/(F)$ est un corps fini, de caractéristique p, et son cardinal est $|K|^n$.*

Démonstration : Le corps $K[X]/(F)$ contenant un sous-corps isomorphe à K (remarque 18), sa caractéristique est la même que celle de K i.e. est p. Par ailleurs, le K-espace vectoriel $K[X]/(F)$ est de dimension n (th. 26), donc est isomorphe à K^n, d'où le résultat.

4.2 Groupe multiplicatif d'un corps fini

Démontrons dans ce paragraphe le résultat 3 annoncé.

Théorème 31. *Soient K un corps commutatif et H un sous-groupe fini de K. Alors H est un groupe cyclique.*

[1] Rappelons que deux espaces vectoriels sur un corps sont isomorphes si et seulement si ils ont la même dimension. En particulier, tout espace vectoriel de dimension n sur K est isomorphe à K^n (le fait que K soit fini n'intervient pas ici). Pour justifier que $|K| = p^n$, on peut aussi choisir une base de K sur $\mathbb{F}_p$. Les coordonnées des éléments de K étant dans $\mathbb{F}_p$, il y a p choix possibles pour chaque coordonnée, d'où les p^n éléments attendus, puisque tout élément de K s'écrit de façon unique comme une combinaison linéaire des vecteurs d'une base.

En particulier :

Corollaire 21. *Si K est un corps fini, le groupe multiplicatif K^* est cyclique.*

Démonstration du théorème 31 : On utilise les deux lemmes ci-dessous.

Lemma 25. *Soient G un groupe abélien multiplicatif, et x, y deux éléments de G d'ordre m et n premiers entre eux. Alors, xy est d'ordre mn.*

Démonstration : Puisque G est abélien, on a $(xy)^{mn} = e$, où e est l'élément neutre de G. L'ordre de xy divise donc mn. Par ailleurs, il existe u et v dans $\mathbb{Z}$ tels que l'on ait $mu + nv = 1$ (Bézout). On a

$$(xy)^{um} = y^{um} = y^{1-vn} = y \text{ et } (xy)^{vn} = x^{vn} = x^{1-um} = x.$$

Considérons alors un entier $r \geq 1$ tel que $(xy)^r = e$. On a $(xy)^{rum} = y^r = e$, et de même $x^r = e$. Il en résulte que r est un multiple de m et n, donc aussi de mn vu que l'on a $\gcd(m, n) = 1$, d'où le résultat.

Lemma 26. *Soient G un groupe abélien fini et x, y deux éléments de G. Il existe dans G un élément dont l'ordre est le ppcm des ordres de x et y.*

Démonstration : Notons multiplicativement la loi de composition de G. Soient α l'ordre de x et β celui de y. Soit R l'ensemble des diviseurs premiers de α pour lesquels on a $v_p(\alpha) > v_p(\beta)$, et S l'ensemble des diviseurs premiers de β pour lesquels on a $v_p(\beta) \geq v_p(\alpha)$. Posons

$$a = \prod_{p \in R} p^{v_p(\alpha)} \text{ et } b = \prod_{p \in S} p^{v_p(\beta)}.$$

Il existe deux entiers r et s tels que l'on ait

$$\alpha = ar \text{ et } \beta = bs.$$

Posons alors

$$z = x^r y^s \in G.$$

L'élément x^r est d'ordre a et y^s est d'ordre b. Par ailleurs, a et b sont premiers entre eux. Puisque G est abélien, z est donc d'ordre ab (lemme 25), qui n'est autre que le ppcm de α et β.

Le théorème 31 se déduit comme suit : soit m l'ordre de H. Puisque H est fini, il existe un élément de H d'ordre maximum n. Le corps K étant commutatif, H est en particulier abélien, donc pour tout élément de H d'ordre d, il existe un élément de H d'ordre le ppcm de d et n (lemme 26). Par suite, on a le plus petit commun multiple de d et n et n, donc d divise n. Ainsi, les ordres de tous les éléments de H divisent n. Le polynôme $X^n - 1 \in K[X]$ ayant au plus n racines dans K, on en déduit que l'on a $m \leq n$. Puisque n divise m, on a donc $m = n$. Il existe ainsi un élément d'ordre m dans H, ce qui établit le théorème[2].

[2]On peut aussi utiliser le résultat suivant : soit G un groupe multiplicatif fini d'ordre n, d'élément neutre e. On suppose que pour tout diviseur d de n, l'ensemble des éléments $y \in G$ tels que $y^d = e$, est de cardinal au plus d. Alors, G est cyclique d'ordre n.

En effet, soit d un diviseur de n. Vérifions que l'ensemble des éléments de G d'ordre d est vide ou bien que son cardinal est $\varphi(d)$, où φ est la fonction indicatrice d'Euler. Supposons qu'il existe $x \in G$ d'ordre d. Le sous-groupe $\langle x \rangle$ de G engendré par x est cyclique d'ordre d. Soit T l'ensemble des éléments $y \in G$ tels que $y^d = e$. Le groupe $\langle x \rangle$ est contenu dans T, et d'après l'hypothèse faite sur G, on a donc $T = \langle x \rangle$. Il en résulte que l'ensemble des éléments d'ordre d de G est formé des générateurs de $\langle x \rangle$, et il y en a $\varphi(d)$. D'où l'assertion. Pour tout diviseur d de n, notons alors Φ_d l'ensemble des éléments d'ordre d de G. Le groupe G étant la réunion disjointe de Φ_d, on a donc

$$n = \sum_{d|n} |\Phi_d| \leq \sum_{d|n} \varphi(d).$$

S'il existait un diviseur d de n tel que $|\Phi_d| = 0$, on aurait ainsi

$$n < \sum_{d|n} \varphi(d),$$

et une contradiction d'après le cours. En particulier, n n'est pas vide, autrement dit, il existe dans G un élément d'ordre n i.e. G est cyclique d'ordre n.

Le théorème 31 se déduit alors du fait que pour tout diviseur d de l'ordre de H, le polynôme $X^d - 1 \in K[X]$ a au plus d racines dans K, donc en particulier dans H.

Corollaire 22. *Soit K un corps fini de cardinal q. Le groupe K possède exactement $\varphi(q-1)$ générateurs, où φ est la fonction indicatrice d'Euler. De plus, si α est un générateur de K, alors l'ensemble des générateurs de K^* est*

$$\left\{\alpha^k | 1 \leq k \leq q-1 \text{ et } \gcd(k, q-1) = 1\right\}.$$

Démonstration : C'est une conséquence directe du corollaire 6.4.
Exercice 1. On considère le polynôme $P = X^4 + X + 1 \in \mathbb{F}_2[X]$.

1. Montrer que $K = \mathbb{F}_2[X]/(P)$ est un corps.

2. Quelle est la caractéristique de K, le cardinal de K ?

3. Soit α la classe de X modulo (P). Montrer que α est un générateur de K. Combien il y a-t-il de générateurs dans K ? Déterminer leurs coordonnées dans la base $(1, \alpha, \alpha^2, \alpha^3)$ de K sur $\mathbb{F}_2$.

4.3 Corps finis comme quotients de $\mathbb{F}_p[X]$

Voici le quatrième résultat annoncé :

Théorème 32. *Soit K un corps fini de cardinal p^n. Il existe un polynôme $F \in \mathbb{F}_p[X]$ irréductible de degré n tel que les corps K et $\mathbb{F}_p[X]/(F)$ soient isomorphes.*

Démonstration : Soit α un générateur de K. On considère l'application

$$\psi : \mathbb{F}_p[X] \to K$$

définie pour tout $P = \sum a_i X^i \in \mathbb{F}_p[X]$ par l'égalité

$$\psi(P) = \sum a_i \alpha^i,$$

où l'on identifie ici $a_i \in \mathbb{F}_p$ avec n'importe quel entier relatif dont la classe modulo p est a_i. Cela est licite car K est de caractéristique p. C'est un homomorphisme d'anneaux. Il est surjectif vu que α est un générateur de K^*. Le noyau de ψ est un idéal I de $\mathbb{F}_p[X]$ et $\mathbb{F}_p[X]/I$ est donc un anneau isomorphe à K. L'idéal I n'est pas nul, sinon K serait isomorphe à $\mathbb{F}_p[X]$, or $\mathbb{F}_p[X]$ n'est pas un corps. Il existe donc un polynôme $F \in \mathbb{F}_p[X]$ tel que $I = (F)$ (th. 19). Puisque $\mathbb{F}_p[X]/(F)$ est un corps, F est donc irréductible (cor. 16). Par ailleurs, si m est le degré de F, le cardinal de $\mathbb{F}_p[X]/(F)$ est p^m (cor. 20), d'où $m = n$ et le résultat.

Il en résulte que les corps finis de cardinal p^n s'obtiennent exclusivement à partir de polynômes irréductibles de degré n dans $\mathbb{F}_p[X]$. Par conséquent, compte tenu du corollaire 20 et du théorème 32, on obtient l'énoncé suivant :

Proposition 16. *Soient p un nombre premier et n un entier ≥ 1. Les deux assertions suivantes sont équivalentes :*

1. *il existe un corps à p^n éléments.*

2. *Il existe un polynôme irréductible de degré n dans $\mathbb{F}_p[X]$.*

Il s'agit donc maintenant de démontrer l'existence de polynômes irréductibles de tout degré $n \geq 1$ dans $\mathbb{F}_p[X]$. Il s'agira aussi de démontrer que si U et V sont deux polynômes irréductibles de degré n dans $\mathbb{F}_p[X]$, alors les corps $\mathbb{F}_p[X]/(U)$ et $\mathbb{F}_p[X]/(V)$ sont isomorphes (unicité à isomorphisme près des corps à p^n éléments).

Exercice 2. Démontrer l'existence de corps à 27, puis à 125 éléments.

4.4 Construction et unicité des corps à p^2 éléments

Soit p un nombre premier. On va démontrer directement l'énoncé suivant, qui est un cas particulier de celui que l'on a en vue.

Théorème 33. *Il existe, à isomorphisme près, un unique corps de cardinal p^2.*

Démonstration : Supposons $p = 2$. Le polynôme $X^2 + X + 1 \in \mathbb{F}_2[X]$ étant irréductible sur $\mathbb{F}_2$, l'anneau

$$\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2 + X + 1),$$

est donc un corps à quatre éléments. Puisqu'il n'existe qu'un seul polynôme irréductible de degré 2 de $\mathbb{F}_2[X]$, le corps $\mathbb{F}_4$ est donc le seul corps à isomorphisme près de cardinal 4.

Supposons désormais p impair. Il existe $p(p-1)/2$ polynômes irréductibles unitaires de degré 2 dans $\mathbb{F}_p[X]$[3]. Il existe donc des corps à p^2 éléments.

Vérifions l'unicité annoncée. Considérons pour cela deux corps de cardinal p^2. Il s'agit de montrer qu'ils sont isomorphes, autrement dit, que si U et V sont deux polynômes irréductibles unitaires de degré 2 dans $\mathbb{F}_p[X]$, les corps

$$K = \mathbb{F}_p[X]/(U) \text{ et } K' = \mathbb{F}_p[X]/(V),$$

sont isomorphes (th. 32). Posons $U = X^2 + bX + c \in \mathbb{F}_p[X]$. Puisque p est impair, on a l'égalité

$$U = \left(X + \frac{b}{2}\right)^2 - \frac{b^2 - 4c}{4},$$

ce qui permet de se ramener au cas où U et V sont de la forme

$$U = X^2 - d \text{ et } \ V = X^2 - d',$$

avec d et d' deux éléments de $\mathbb{F}_p$ qui ne sont pas des carrés dans $\mathbb{F}_p$. Posons

$$\alpha = X + (U) \in K \text{ et } \alpha' = X + (V) \in K'.$$

. On va démontrer que

$$d' \in K^2,$$

i.e. qu'il existe $\zeta \in K$ tel que $\zeta^2 = d'$. Cette assertion entraîne le résultat. En effet, une fois cette condition démontrée, on vérifie alors que l'application $\psi : K' \to K$ définie par

$$\psi(a + b\alpha') = a + b\zeta,$$

est un isomorphisme de corps, de K' sur K. (C'est un homomorphisme de corps, il est donc injectif, puis surjectif car K et K' ont le même cardinal). On cherche ainsi x et y dans $\mathbb{F}_p$ tels que l'on ait

$$d' = (x + y\alpha)^2.$$

Compte tenu du fait que $(1, \alpha)$ est une base de K sur $\mathbb{F}_p$, on obtient les relations

$$d' = x^2 + dy^2 \text{ et } 2xy = 0$$

. On a $2 \neq 0$ car p est impair, et nécessairement $y \neq 0$, car d' n'est pas un carré dans $\mathbb{F}_p$. Par suite, x doit être nul, et tout revient donc à montrer qu'il existe $y \in \mathbb{F}_p$ tel que

$$y^2 = \frac{d'}{d},$$

autrement dit, à montrer que le produit dd' est un carré dans $\mathbb{F}_p$. Cela résulte du lemme suivant :

[3]On procède comme suit. Tout d'abord, il y a p^2 polynômes unitaires de degré 2 dans $\mathbb{F}_p[X]$. Ceux qui sont réductibles sur $\mathbb{F}_p$ sont de la $(X - a)(X - b)$ avec a et b dans $\mathbb{F}_p$. Il y en a p pour lesquels $a = b$ et $p(p-1)/2$ pour lesquels $a \neq b$. On obtient ainsi $p^2 - p - p(p-1)/2 = p(p-1)/2$ polynômes irréductibles unitaires de degré 2 dans $\mathbb{F}_p[X]$.

Lemma 27. *Le produit de deux éléments de $\mathbb{F}_p^*$, qui ne sont pas des carrés dans $\mathbb{F}_p^*$, est un carré dans $\mathbb{F}_p^*$.*

Démonstration : Posons $G = \mathbb{F}_p^*$ et considérons l'application $f : G \to G$ qui à x associe x^2. C'est un homomorphisme de groupes dont l'image est le sous-groupe G^+ des carrés de $\mathbb{F}_p^*$. Son noyau est $\{\pm 1\}$ (le polynôme $X^2 - 1$ a deux racines dans $\mathbb{F}_p$ qui sont ± 1). On en déduit que (p est impair)

$$|G^+| = \frac{p-1}{2} \text{ et } \left|G/G^+\right| = 2. \tag{4.2}$$

Le groupe G/G^+ est donc d'ordre 2, d'élément neutre G^+, et si G^- désigne l'ensemble des éléments de $\mathbb{F}_p^*$ qui ne sont pas des carrés, on a

$$G/G^+ = \{G^+, G^-\}.$$

En particulier, on a $G^-.G^- = G^+$, ce qui établit le lemme.
Cela termine la démonstration du théorème 33.

Remarque 19. *Dans le cas où p est impair congru à 3 modulo 4, il est facile d'expliciter concrètement un corps à p^2 éléments. En effet, dans ce cas -1 n'est pas un carré dans $\mathbb{F}_p$ et $\mathbb{F}_p[X]/(X^2+1)$ est donc un corps à p^2 éléments. Pour le vérifier, il suffit de démontrer l'énoncé qui suit :*

Lemma 28. *Soit p un nombre premier impair. On a l'équivalence*

$$-1 \in \mathbb{F}_p^2 \iff p = 1 \bmod 4.$$

Démonstration : On peut utiliser directement la première égalité de (1). Si -1 est un carré dans $\mathbb{F}_p$, on a ainsi dans $\mathbb{F}_p$ l'égalité

$$(-1)^{(p-1)/2} = 1,$$

ce qui entraîne $p = 1 \bmod 4$. Inversement, supposons $p = 1 \bmod 4$. Puisque 4 divise $p-1$ et que $\mathbb{F}_p^*$ est cyclique d'ordre $p-1$, le groupe $\mathbb{F}_p^*$ possède donc un sous-groupe H d'ordre 4 cyclique. Si x est un générateur de H, on a $x^4 = 1$, d'où $x^2 = -1$ et le résultat.

Exercice 3. Soit K un corps fini de cardinal q et de caractéristique p. On note K^2 l'ensemble des éléments de K qui sont des carrés dans K i.e. l'ensemble des x^2 où x est dans K.

1. Si $p = 2$ montrer que $K^2 = K$.
2. Si p est distinct de 2, montrer que $|K^2| = (q+1)/2$.
3. En déduire que tout élément de K est la somme de deux carrés dans K.
4. Supposons $p \geq 3$. Montrer qu'un élément non nul $x \in K$ est un carré dans K si et seulement si on a $x^{(q-1)/2} = 1$.

4.5 Polynômes irréductibles sur un corps fini

On va démontrer dans ce paragraphe le résultat suivant :

Théorème 34. *Soient K un corps de cardinal q et n un entier naturel non nul. L'ensemble des diviseurs irréductibles du polynôme $X^{q^n} - X \in K[X]$ est formé des polynômes irréductibles de $K[X]$ de degré divisant n. Plus précisément, on a l'égalité*

$$X^{q^n} - X = \prod F, \tag{4.3}$$

où F parcourt l'ensemble des polynômes irréductibles unitaires de $K[X]$ de degré divisant n.

La démonstration repose sur plusieurs lemmes intermédiaires, qui sont par eux mêmes intéressants d'un point de vue pratique. On suppose dans ce qui suit que K est un corps fini de caractéristique p et de cardinal q (qui est donc une puissance de p).

Lemma 29. *Soit k un entier naturel. On a l'égalité*

$$(x+y)^{p^k} = x^{p^k} + y^{p^k} \text{ quels que soient } x, y \in K.$$

Démonstration : Procédons par récurrence sur k. L'énoncé est vrai si $k = 0$. Soit alors k un entier ≥ 0 tel que l'égalité annoncée soit vérifiée. Pour tous $x, y \in K$, on a

$$(x+y)^{p^{k+1}} = \left((x+y)^{p^k}\right)^p = \left(x^{p^k} + y^{p^k}\right)^p,$$

la dernière égalité provenant de l'hypothèse de récurrence. Par ailleurs, pour tout entier $j = 1, \cdots, p-1$, le coefficient binomial C_p^j est divisible par p[4]. La formule du binôme de Newton entraîne alors l'égalité $(x+y)^{p^{k+1}} = x^{p^{k+1}} + y^{p^{k+1}}$, et le résultat[5].

Lemma 30. *Soit L un corps fini contenant K.*

1. *Pour tout $x \in L$, x appartient à K si et seulement si on a $x^q = x$.*
2. *Pour tout $F \in L[X]$, F appartient à $K[X]$ si et seulement si on a $F(X^q) = F(X)^q$.*

Démonstration : 1) Soit x un élément de L. Si x est dans K, vu que K est un groupe d'ordre $q-1$, on a $x^{q-1} = 1$, d'où $x^q = x$. Par ailleurs, le polynôme $X^q - X \in L[X]$ possède au plus q racines, donc K est l'ensemble de ses racines, d'où l'assertion 1. 2) Soit $F = \sum a_k X^k$ un polynôme de $L[X]$. On a

$$F(X)^q = \left(\sum a_k X^k\right)^q = \sum a_q^k X^{kq}$$

[6]. D'après la première assertion, F appartient à $K[X]$ si et seulement si $a_k^q = a_k$ pour tout k, ce qui entraîne le résultat.

Lemma 31. *Soient F un polynôme unitaire irréductible de $K[X]$ et L un corps fini contenant K dans lequel F a une racine α. Il existe un plus petit entier $r \geq 1$ tel que l'on ait $\alpha^{q^r} = \alpha$. On a $r = \deg(F)$ et l'égalité*

$$F = \prod_{i=0}^{r-1} \left(X - \alpha^{q^i}\right).$$

Démonstration : Il existe un entier $m \geq 1$ tel que le cardinal de L soit q^m. On a $\alpha^{q^m} = \alpha$, donc il existe un plus petit entier $r \geq 1$ tel que l'on ait $\alpha^{q^r} = \alpha$. Par ailleurs, α étant racine de F, on déduit du lemme 30 que les éléments α^{q^i} pour $i = 1, \cdots, r-1$ sont aussi des racines de F. Posons

$$G = \prod_{i=0}^{r-1} \left(X - \alpha^{q^i}\right).$$

[4]Rappelons l'argument. Pour tout $j = 1, \ldots, p-1$, on a en effet, $j!(p-j)!C_p^j = p!$, et puisque p ne divise pas $j!(p-j)!$, il en résulte que p divise C_p^j (lemme de Gauss).

[5]Bien qu'inutile pour la démonstration du théorème 34, signalons une conséquence du lemme 29. Soit $f : K \to K$ l'application définie pour tout $x \in K$ par $f(x) = x^p$. Alors, f est automorphisme de K. On l'appelle l'automorphisme de Frobenius de K. En effet, f est un homomorphisme de groupes (lemme 29). Par ailleurs, on a l'égalité $(xy)^p = x^p y^p$ pour tous $x, y \in K$ (K est commutatif) et $f(1) = 1$, donc f est un homomorphisme de corps. Son noyau est un idéal de K, donc est nul puisque ce dernier est distinct de K. Ainsi, f est une injection de K dans K, donc aussi une surjection car K est fini. C'est donc un automorphisme de K. Si $|K| = p^N$, on a $f^N = id$ (on note f^N l'application itérée N fois de f et id l'identité de K). De plus, N est le plus petit entier $i \geq 1$ tel que $f^i = id$, car si $i < N$, le polynôme $X^{p^i} - X$ ne peut avoir $p^N > p^i$ racines dans K. Il en résulte que les automorphismes $id, f, \ldots, f^{N-1}$ sont deux à deux distincts. Ils forment un groupe cyclique d'ordre N, que l'on appelle le groupe de Galois de K (sur $\mathbb{F}_p$).

[6]Cette dernière égalité se démontre en utilisant le lemme 6.6, et en procédant par récurrence sur le nombre de monômes de F.

Puisque les α^{q^i} pour $i = 0, \cdots, r-1$ sont distincts deux à deux[7], il en résulte G divise F dans $L[X]$ (th. 5.7). De plus, on a les égalités

$$G(X)^q = \prod_{i=0}^{r-1} \left(X - \alpha^{q^i} \right)^q = \prod_{i=0}^{r-1} \left(X^q - \alpha^{q^{i+1}} \right) = G(X^q).$$

On en déduit que G appartient à $K[X]$ (lemme 6.7). Le quotient et le reste de la division euclidienne de F par G étant indépendants du corps de base, vu leur caractère d'unicité, on en déduit que G divise F dans $K[X]$. Le polynôme F étant irréductible, G étant de degré au moins 1, et F et G étant unitaires, on a donc $F = G$, d'où le résultat.

Remarque 20. *Le lemme 6.8 montre qu'un polynôme irréductible F de $K[X]$ qui a une racine dans un surcorps fini L de K, a toutes ses racines dans L, comme annoncé dans les remarques 5.6. De plus, si r est le degré de F, et si $\alpha \in L$ est une racine de F, alors les racines de F sont les α^{q^i} pour $i = 0, \ldots, r-1$.*

Fin de la démonstration du théorème 34.
Soit $F \in K[X]$ un polynôme irréductible unitaire de degré r. Il s'agit de démontrer l'équivalence suivante :

$$F \text{ divise } X^{q^n} - X \iff r \text{ divise } n. \tag{4.4}$$

Considérons un corps fini L contenant K dans lequel F a une racine α : un tel corps L existe (th. **??**). D'après le lemme 31, r est le plus petit entier ≥ 1 tel que $\alpha^{q^r} = \alpha$ et l'on a l'égalité

$$F = \prod_{i=0}^{r-1} \left(X - \alpha^{q^i} \right). \tag{4.5}$$

Par ailleurs, on a

$$\alpha^{q^{ir}} = \alpha \text{ pour tout } i \geq 0. \tag{4.6}$$

En effet, cette égalité est vraie si $i = 0$, et si elle est vérifiée pour un entier $i \geq 0$, on a

$$\alpha^{q^{(i+1)r}} = (\alpha^{q^{ir}})^{q^r} = \alpha^{q^r} = \alpha,$$

donc elle l'est aussi pour $i + 1$.

Supposons alors que F divise $X^{q^n} - X$. Puisque $F(\alpha) = 0$, on a $\alpha^{q^n} = \alpha$. Il existe deux entiers naturels t et s tels que l'on ait $n = rt + s$ avec $0 \leq s < r$. On a donc

$$\alpha^{q^n} = (\alpha^{q^{tr}})^{q^s}.$$

D'après (4.6), on a $\alpha^{q^{tr}} = \alpha$. Par suite, on a $\alpha = \alpha^{q^s}$, ce qui d'après le caractère minimal de r, entraîne $s = 0$, ainsi r divise n.

Inversement, supposons que r divise n. On déduit de (4.6) que l'on a $\alpha^{q^n} = \alpha$, autrement dit, que α est racine du polynôme $X^{q^n} - X$. Les éléments

$$\alpha, \alpha^q, \ldots, \alpha^{q^{r-1}},$$

[7] On peut justifier cette assertion comme suit. Supposons qu'il existe deux entiers i et j compris entre 0 et $r-1$ tels que $i < j$ et $\alpha^{q^i} = \alpha^{q^j}$. On a alors l'égalité

$$\left(\frac{\alpha^{q^{j-i}}}{\alpha} \right)^{q^i} = 1.$$

Il s'agit d'en déduire que $\alpha^{q^{j-i}} = \alpha$, ce qui conduira à une contradiction vu le caractère minimal de r. Tout revient ainsi à démontrer que pour tout $y \in L$, l'égalité $y^q = 1$ entraîne $y = 1$. Les entiers q et $q^m - 1$ étant premiers entre eux, il existe u et v dans $\mathbb{Z}$ tels que l'on ait $uq + v(q^m - 1) = 1$. Pour tout $y \in L$, on a $y^{q^m - 1} = 1$. Par suite, si $y^q = 1$, on obtient $y = y^{uq + v(q^m - 1)} = 1$, et notre assertion.

sont donc des racines deux à deux distinctes de $X^{q^n} - X$. Il résulte de (4.5) que F divise $X^{q^n} - X$ dans $L[X]$, donc aussi dans $K[X]$ car F est à coefficients dans K. Cela prouve l'équivalence (4.4).

On déduit de ce qui précède, et du théorème 33, une égalité de la forme

$$X^{q^n} - X = \prod_F F^{n_F},$$

où F parcourt l'ensemble des polynômes irréductibles unitaires de $K[X]$ de degré divisant n, et où les n_F sont des entiers naturels non nuls. Tout revient alors à démontrer que les n_F sont égaux à 1. Étant donné un tel polynôme F, on a $X^{q^n} - X = F^{n_F}Q$ où $Q \in K[X]$, d'où l'on déduit, en considérant les polynômes dérivés des deux membres de cette égalité (on a $q1_K = 0$ car K est de caractéristique p),

$$-1 = n_F F^{n_F - 1} F'Q + F^{n_F} Q'.$$

Par suite, $F^{n_F - 1}$ divise -1 dans $K[X]$, ce qui entraîne $n_F = 1$ et le résultat.

Exercice 4. Factoriser $X^8 - X \in \mathbb{F}_2[X]$ en produit de polynômes irréductibles de $\mathbb{F}_2[X]$.

4.6 Théorème d'existence

On considère dans ce paragraphe un corps fini K de cardinal q.

Notation. Pour tout entier $m \geq 1$, on note $I_m(q)$ le nombre de polynômes irréductibles unitaires de degré m de $K[X]$.

Pour tout $n \geq 1$, la formule (4.3) permet de calculer $I_n(q)$. En effet, dans le produit intervenant dans (4.3) il y a $I_d(q)$ facteurs de degré d pour chaque diviseur d de n. En considérant les degrés des polynômes de chaque membre, on obtient ainsi

$$q^n = \sum_{d|n} I_d(q) d. \tag{4.7}$$

Le théorème d'existence annoncé au début sur les corps finis est une conséquence de l'énoncé suivant :

Théorème 35. *Pour tout $n \geq 1$, on a $I_n(q) > 0$.*

Démonstration : On procède par récurrence sur n. Le résultat est vrai si $n = 1$ (pour tout $a \in K$, $X - a$ est irréductible dans $K[X]$). Considérons alors un entier $n \geq 2$, et supposons le résultat démontré pour tout entier $d < n$. En utilisant la formule (4.7), on obtient l'égalité

$$q^d = dI_d(q) + \sum_{d'|d, d'<d} I_{d'}(q) d' \text{ pour tout } d < n.$$

D'après l'hypothèse de récurrence, on a donc

$$q^d > dI_d(q) \text{ pour tout } d < n.$$

La formule

$$q^n = nI_n(q) + \sum_{d|n, d<n} dI_d(q)$$

entraîne alors les inégalités

$$q^n < nI_n(q) + \sum_{d|n, d<n} q^d \leq nI_n(q) + \sum_{k=0}^{n-1} q^k = nI_n(q) + \frac{q^n - 1}{q - 1} < nI_n(q) + q^n,$$

d'où $I_n(q) > 0$ et le résultat.

Corollaire 23. *Pour tout entier $n \geq 1$ et tout nombre premier p, il existe un corps de cardinal p^n.*

Démonstration : C'est une conséquence directe du théorème 35, appliqué avec $q = p$, et de la proposition 16.

4.7 Théorème d'unicité

Il s'agit de démontrer l'énoncé suivant :

Théorème 36. *Deux corps finis ayant le même nombre d'éléments sont isomorphes.*

Démonstration : Soient K et L des corps à q éléments et p leur caractéristique. On a $q = p^n$ pour un entier $n \geq 1$. Il existe un polynôme irréductible $F \in \mathbb{F}_p X]$, de degré n, tel que K soit isomorphe à $\mathbb{F}_p[X] = (F)$ (th. 32). Le polynôme F divise $X^q - X \in \mathbb{F}_p[X]$ (th.34). Par ailleurs, pour tout $x \in L$, on a $x^q = x$. On a donc l'égalité

$$X^q - X = \prod_{a \in L} (X - a).$$

Le polynôme F possède ainsi une racine $a \in L$. Considérons l'application

$$\psi \ : F_p[X] \to L$$

définie pour tout $P \in F_p[X]$ par $\psi(P) = P(a)$. C'est un morphisme d'anneaux. Vu que F est irréductible dans $F_p[X]$ et que $F(a) = 0$, le noyau de ψ est l'idéal (F). Il en résulte que $\mathbb{F}_p[X] = (F)$ est isomorphe à l'image de ψ, qui n'est autre que L, car L et $\mathbb{F}_p[X] = (F)$ ont le même cardinal. Cela entraîne que les corps K et L sont isomorphes.

Ce résultat justifie l'abus courant consistant à parler "du" corps à q éléments. On le note souvent $\mathbb{F}_q$, y compris si q n'est pas premier, mais une puissance d'un nombre premier. On a par exemple

$$\mathbb{F}_8 = \mathbb{F}_2[X] = (X^3 + X + 1);\ \mathbb{F}_{81} = F_3[X] = (X^4 + X^3 + 2);\ \mathbb{F}_{125} = \mathbb{F}_5[X]/(X^3 + X + 1);$$
$$\mathbb{F}_{p^2} = \mathbb{F}_p[X]/(X^2 + 1) \text{ si } p \text{ est premier congru à 3 modulo 4.}$$

Chapter 5

Extensions de corps et Algorithme de Berlekamp

5.1 Introduction

Les constructions de $\mathbb{C}$ reposent sur le fait de créer un sur-corps de $\mathbb{R}$ qui contienne une racine du polynôme X^2+1. Plus généralement, si k est un corps commutatif et si P est un polynôme de $k[X]$ sans racine dans k, il serait intéressant d'avoir un procédé permettant de construire un sur-corps K de k où P possède au moins une racine, voire toutes ses racines. Un tel procédé est expliqué dans ce chapitre et il utilise le corps de rupture d'un polynôme et le corps des racines d'un polynôme.

5.2 Éléments algébriques et transcendants

5.2.1 Notations

On note k un corps commutatif et K un corps commutatif contenant k, structuré par les mêmes lois de k. On dit que K est un *sur-corps* de k ou que k est un *sous-corps* de K. Soit a un élément de K.

Comme l'intersection de sous-anneaux de K est encore un sous-anneau, il est facile de vérifier que l'intersection de tous les sous-anneaux de K contenant k et a est le plus petit sous-anneau de K contenant k et a (au sens de l'inclusion). On pose alors:

Définition 20. *On note $k[a]$ le plus petit sous-anneau de K contenant le corps k et l'élément a. On dit que $k[a]$ est l'anneau engendré par k et a.*

De même, on peut définir le plus petit sous-corps de K contenant k et a comme l'intersection de tous les sous-corps de K contenant k et a.

Définition 21. *On note $k(a)$ le plus petit sous-corps de K contenant le corps k et l'élément a. On dit que $k(a)$ est le corps engendré par k et a.*

Si $k[X]$ désigne l'algèbre des polynômes à une indéterminée et à coefficients dans k, alors:

Théorème 37. *L'anneau $k[a]$ engendré par k et a est formé de toutes les expressions polynomiales en a et à coefficients dans k:*

$$k[a] = \{P(a) | P \in k[X]\}.$$

Démonstration: L'ensemble $\mathcal{A} = \{P(a) | P \in k[X]\}$ est un sous-anneau de K puisqu'il n'est pas vide (il contient 0) et vérifie:

$$P(a), Q(a) \in \mathcal{A} \Rightarrow \left\{ \begin{array}{ll} P(a) - Q(a) & = (P-Q)(a) \in \mathcal{A} \\ P(a) \times Q(a) & = (P \times Q)(a) \in \mathcal{A} \end{array} \right.$$

C'est le plus petit sous-anneau de K contenant k et a car si A est un sous-anneau de K contenant k et a, alors A contient nécessairement toutes les expressions polynomiales en a de la forme:

$$c_n a^n + c_{n-1} a^{n-1} + \ldots + c_1 a + c_0$$

où $n \in \mathbb{N}$ et où les coefficients c_i appartiennent à k, donc $\mathcal{A} \subset A$. □

5.2.2 Définitions

Définition 22. *Un élément $a \in K$ est dit algébrique sur k s'il existe un polynôme $P(X)$ non nul de $k[X]$ tel que $P(a) = 0$, transcendant sur k dans le cas contraire.*

Comme $(\sqrt{2})^2 = 2$, le nombre réel irrationnel $\sqrt{2}$ est algébrique sur $\mathbb{Q}$. Le nombre complexe i annule le polynôme $X^2 + 1$ à coefficients réels, donc est algébrique sur $\mathbb{R}$. Les nombres complexes j et $\sqrt[7]{19}$ sont algébriques sur $\mathbb{R}$ car j est racine du polynôme $X^3 - 1$ et $\sqrt[7]{19}$ de $X^7 - 19$. On rappelle que π et e sont transcendants sur $\mathbb{Q}$.

5.2.3 Propriétés

L'image du morphisme d'algèbres: $\phi_a : k[X] \to K$ qui à $P(X)$ associe $P(a)$ est égale à $k[a]$. L'anneau $k[a]$ est intègre puisqu'inclus dans le corps K. Comme tout anneau intègre, $k[a]$ possède un corps des fractions, et on sait que ce corps des fractions est isomorphe au plus petit sous-corps de K contenant $k[a]$, donc isomorphe à $k(a)$. On identifiera $k(a)$ au corps des fractions de $k[a]$.

Le noyau de ϕ_a est formé de tous les polynômes $P(X)$ qui admettent a comme racine: $\ker \phi_a = \{P \in k[X] | P(a) = 0\}$, et par décomposition canonique

$$k[X]/\ker \phi_a \simeq k[a].$$

Le noyau $\ker \phi_a$ est un idéal de $k[X]$ et comme $k[X]$ est un anneau principal (puisque k est un corps), il est principal (i.e. monogène, engendré par un seul élément). Deux cas se présentent:

Premier cas. Si a est transcendant sur k, alors $\ker \phi_a = \{0\}$ et le morphisme $\phi_a : k[X] \to K$ est injectif, donc induit un isomorphisme d'anneau $\phi_a : k[X] \to k[a]$. Les anneaux $k[X]$ et $k[a]$ sont isomorphes, donc ils admettent le même corps des fractions à isomorphisme près. Si $k(X)$ et $k(a)$ désignent ces corps des fractions, on a $k(X) \simeq k(a)$ et

$$k(a) = \left\{ \frac{u(a)}{v(a)} | (u, v) \in k[X] \times (k[X] \setminus \{0\}) \right\}.$$

On connaît les expressions de tous les éléments du corps $k(a)$.

Deuxième cas. Si a est algébrique sur k, alors $\ker \phi_a \neq \{0\}$, et il existe un polynôme non nul $m_a \in k[X]$ tel que:

$$\ker \phi_a = (m_a) = \text{ idéal engendré par } m_a.$$

On montre que ce polynôme m_a est irréductible: si $m_a(X) = P(X)Q(X)$, alors $P(a)Q(a) = 0$ donc $P(a) = 0$ ou $Q(a) = 0$. Si $P(a) = 0$ alors m_a divise P, donc $\deg m_a \leq \deg P$. Mais alors $\deg P + \deg Q \leq \deg P$ implique $\deg Q = 0$ et le polynôme Q est une constante. On raisonne de même si $Q(a) = 0$. On a $m_a = PQ$ implique P ou Q est constant, ce qui est équivalent à m_a irréductible dans $k[X]$.

Si on impose à m_a d'être unitaire, coefficient de degré maximum égal à 1, alors m_a est unique. En effet, si m_a et m'_a sont deux polynômes irréductibles et unitaires tel que $\ker \phi_a = (m_a) = (m'_a)$, alors m_a divise m'_a et réciproquement, donc $\deg m_a = \deg m'_a$ et s'il existe $P \in k[X]$ tel que $m'_a = Pm_a$, alors $\deg m'_a = \deg P + \deg m_a$ et on obtient $\deg P = 0$, donc P est une constante. Comme m_a et m'_a sont unitaires, $P = 1$ et $m_a = m'_a$.

On peut donc poser:

Définition 23. *Si a est algébrique sur k, l'unique polynôme irréductible et unitaire m_a de $k[X]$ tel que $\ker \phi_a = (m_a)$ est appelé le polynôme irréductible (ou polynôme minimal) de a sur k. Le degré de m_a est appelé le degré de a sur k, noté $\deg a = \deg m_a$.*

Exemple: Le nombre complexe j est algébrique sur $\mathbb{R}$ car il annule $X^3 - 1$. On a aussi $j^2 + j + 1 = 0$, et le polynôme $X^2 + X + 1$ est irréductible dans $\mathbb{R}[X]$. Il s'agit du polynôme minimal de j, le degré de j est 2.

Si a est algébrique sur k de polynôme minimal m_a, la décomposition canonique du morphisme ϕ_a donne $k[X]/(m_a) \simeq k[a]$, l'isomorphisme correspondant aux structures d'anneaux et de k-espace vectoriels. Comme m_a est un polynôme irréductible de $k[X]$, l'idéal (m_a) est maximal et l'anneau $k[X]/(m_a)$ est un corps. L'anneau $k[a]$ sera un corps et on obtient $k(a) = k[a]$. Le plus petit anneau et le plus petit corps contenant k et a sont les mêmes.

En conclusion:

Théorème 38. *1. Si a est transcendant sur k, $k[a] \simeq k[X]$ et $k(a) \simeq k(X)$ où $k(X)$ est le corps des fractions de $k[X]$ (c'est le corps des fractions rationnelles sur k).*

2. Si a est algébrique sur k, le plus petit corps contenant k et a coïncident. Si m_a désigne le polynôme irréductible de a sur k: $k[a] \simeq k(a) \simeq k[X]/(m_a)$.

5.3 Adjonction d'une racine

On s'intéresse au problème suivant: Étant donné un corps k et un polynôme non nul f à coefficient dans k, peut-on construire un sur-corps K de k sur lequel f possède au moins une racine ?

Ce problème admet une solution évidente si f possède une racine dans k. Si aucun élément de k est racine pour f, on peut échanger f par un polynôme irréductible unitaire P intervenant dans la décomposition de f en produit de facteurs irréductibles. On sait que $k[X]$ est un anneau principal, donc factoriel dès que k est un corps commutatif. En effet, il existe une division euclidienne dans $k[X]$ ce qui fait de $k[X]$ un anneau euclidien, et on sait qu'un anneau euclidien est principal et qu'un anneau principal est factoriel.

Puisque P est irréductible, l'idéal (P) engendré par P est maximal et l'anneau $k[X]/(P)$ est un corps. On pose $K = k[X]/(P)$. Notons $\pi : k[X] \to K = k[X]/(P)$ la projection de $k[X]$ sur K. C'est un morphisme surjectif d'anneaux. Notons $j = \pi|_k : k \to K$ la restriction de ce morphisme à k. C'est encore un morphisme d'anneaux, mais entre deux corps cette fois. C'est donc un morphisme de corps, injectif car:

$$j(a) = j(b) \Rightarrow j(a-b) = 0 \Rightarrow a - b \in (P) \Rightarrow P|(a-b) \Rightarrow a = b.$$

L'injection $j : k \to K$ permet de plonger k dans K. De façon plus rigoureuse, on dira que $j(k)$ est un sous-corps de K isomorphe à k et on peut identifier k à $j(k)$ en posant $a = j(a)$ pour tout $a \in k$.

Notons $P(X) = a_0 + a_1 X + \ldots + a_n X^n$ et $\bar{1}, \bar{X}, \ldots, \bar{X}^n$ les classes des polynômes $1, X, \ldots, X^n$ dans $k[X]/(P)$. Posons $a = \bar{X} = \pi(X)$. Comme π est un morphisme d'anneaux,

$$\pi(P) = \pi(a_0) + \pi(a_1)\pi(X) + \ldots + \pi(a_n)\pi(X)^n,$$

et comme k est identifié à $j(k)$ on peut écrire $\pi(a_0) = a_0, \ldots, \pi(a_n) = a_n$ et donc $\pi(P) = a_0 + a_1\bar{X} + \ldots + a_n\bar{X}^n = P(\bar{X})$, soit:

$$\pi(P) = a_0 + a_1\alpha + \ldots + a_n\alpha^n = P(\alpha).$$

Cette formule est vraie quelque soit le polynôme P de $k[X]$ mais ici P engendre l'idéal $\ker \pi$, donc $\pi(P) = 0$, ce qui donne $P(\alpha) = 0$. On vient d'établir que α est une racine de P dans un sur-corps K de k construit pour la circonstance. En conclusion:

Théorème 39. *Étant donnés un corps k et un polynôme non constant f à coefficients dans k, il est possible de construire un sur-corps K de k sur lequel f admet une racine.*

Définition 24. *La méthode que l'on vient de décrire est appelé procédé d'adjonction d'une racine.*

On note que l'élément α de $K = k[X]/(P)$ est algébrique sur k, puisque racine de P, et comme P est irréductible, on a: $K = k(\alpha) = k[\alpha]$. On vérifie que K est un k-espace vectoriel de dimension finie $\deg P$:

Théorème 40. *Si P est un polynôme irréductible de $k[X]$ de degré d, alors $K = k[X]/(P)$ est un k-espace vectoriel de dimension d, et $(1, \alpha, \ldots, \alpha^{d-1})$ est une base de K.*

Démonstration: $K = k[X]/(P)$ est un k-espace vectoriel car c'est le quotient d'un espace vectoriel par un sous-espace vectoriel. Soit $\pi : k[X] \to K = k[X]/(P)$ la projection canonique. Tout élément x de K s'écrit $x = \pi(f)$ avec $f \in k[X]$ et la formule précédente donne $x = \pi(f) = f(\alpha)$.

Par division euclidienne, $f = Pq + r$ avec $r(X) = a_{d-1}X^{d-1} + \ldots + a_0$ et $a_i \in k$ donc,

$$x = f(\alpha) = P(\alpha)f(\alpha + r(\alpha)) = r(\alpha) = a_{d-1}\alpha^{d-1} + \ldots + a_1\alpha + a_0,$$

ce qui prouve bien que $(1, \alpha, \ldots, \alpha^{d-1})$ est un système générateur du k-espace vectoriel K.

C'est un système libre car si $r(\alpha) = a_{d-1}\alpha^{d-1} + \ldots + a_1\alpha + a_0 = 0$, alors $\pi(r) = r(\alpha) = 0$ donc $r \in \ker \pi = (P)$, ce qui montre que P divise r. Comme $\deg r < \deg P$, c'est impossible sauf si $r = 0$ (en tant que polynôme), ce qui implique $a_{d-1} = \ldots = a_1 = a_0 = 0$. □

Théorème 41. *Soit K un sur-corps de k. Si a est algébrique sur k:*

$$k(a) = k[a] \simeq k[X]/(m_a)$$

où m_a désigne le polynôme minimal de a et le plus petit corps $k(a)$ de K contenant k et a est un k-espace vectoriel de dimension le degré de a (c'est-à-dire le degré de m_a).

Démonstration: On a $k(a) = k[a] \simeq k[X]/(P)$ d'après le théorème 38 et $\dim_k k(a) = \deg m_a = \deg a$ d'après le théorème 40. □

Le théorème 40 est utile car il permet de donner une description des éléments de K. Si par exemple $k = \mathbb{Q}$ et $P(X) = X^2 + X + 1$, l'adjonction d'une racine de P à $\mathbb{Q}$ permet de construire le corps $\mathbb{Q}/(P)$ dont les éléments s'écriront sous la forme $aj + b$ avec $(a, b) \in \mathbb{Q}^2$. Les opérations sur K sont bien connues: l'addition est triviale et le produit $(aj + b)(a'j + b')$ s'obtient en développant et en utilisant la relation $P(j) = j^2 + j + 1 = 0$ pour diminuer les exposants de j et obtenir que des puissances de j inférieures à 1.

$$(aj+b)(a'j+b') = aa'j^2 + (ab'+ba')j + bb' = aa'(-j-1) + (ab'+ba')j + bb' = (ab'+ba'-aa')j + bb'-aa'.$$

Exemples:

1. Soit $d \in \mathbb{Q}_+^*$ qui ne soit pas un carré dans $\mathbb{Q}$ (par exemple $d = 7$). L'adjonction d'une racine du polynôme $X^2 - d$ au corps des rationnels $\mathbb{Q}$ permet de construire une extension finie de $\mathbb{Q}$ dont les éléments s'écrivent $a + b\xi$ où ξ vérifie $\xi^2 = d$. C'est une extension $\mathbb{Q}[\xi]$ que l'on peut aussi noter $\mathbb{Q}[\sqrt{d}]$. Le polynôme $X^2 - d$ est le polynôme minimal de ξ sur $\mathbb{Q}$ et ξ et algébrique de degré 2 sur $\mathbb{Q}$. De plus,

$$\mathbb{Q}(\xi) = \mathbb{Q}[\xi] \simeq \mathbb{Q}[X]/(X^2 - d).$$

2. L'adjonction d'une racine i du polynôme $X^2 + 1$ de $\mathbb{R}[X]$ permet de construire le corps

$$\mathbb{R}[i] \simeq \mathbb{R}[X]/(X^2 + 1)$$

dans lequel il existe un élément $\bar{X}$ tel que $\bar{X}^2 = -1$. On pose $\bar{X} = i$ et il est facile de voir que $\mathbb{R}[i] = \mathbb{C}$ le corps des complexes (à isomorphisme près).

Le procédé d'adjonction d'une racine permet d'introduire la notion de corps de rupture d'un polynôme:

Définition 25. *On appelle corps de rupture de $f \in k[X]$ tout élément minimal dans l'ensemble des corps contenant k et contenant au moins une racine de f.*

La minimalité d'un tel corps de rupture doit s'entendre pour la relation "inclusion" entre les ensembles. Un corps de rupture $f \in k[X]$ est donc un corps K tel que:

- K est un sur-corps de k contenant au moins une racine de f;
- Pour tout sur-corps L de k contenant au moins une racine de f: $k \subset L \subset K \Rightarrow L = K$.

On démontre l'unicité:

Théorème 42. *Un corps de rupture d'un polynôme irréductible P est unique à isomorphisme près. Plus précisément, tous les corps de rupture d'un polynôme irréductible $P \in k[X]$ sont isomorphes au corps $k[X]/(P)$.*

Démonstration: Si K et K' sont deux corps de rupture d'un polynôme P irréductible dans $k[X]$, et si α, β sont des racines de P, respectivement dans K et K', alors P est le polynôme minimal de α sur K et K' (à une constante multiplicative près), et la décomposition canonique du morphisme d'anneaux: $\Psi : k[X] \to K$ qui à f associe $f(\alpha)$ donne un morphisme d'anneaux $\Psi^* : k[X]/(P) \to \mathrm{Im}\Psi$. Comme $k[X]/(P)$ est un corps, il en sera de même de $\mathrm{Im}\Psi$, et Ψ^* sera un isomorphisme de corps. Le corps K étant supposé minimal dans l'ensemble des extensions de k qui contiennent au moins une racine de P, on aura $K = \mathrm{Im}\Psi$, soit $K \simeq k[X]/(P)$. Il suffit de recommencer avec. K' à la place de K pour obtenir $K' \simeq k[X]/(P) \simeq K$. □

Construire un corps de rupture d'un polynôme, c'est faire le premier pas pour construire des corps des racines.

Théorème 43. *Étant donnés un corps k et un nombre fini de polynômes non constants $f_1, \ldots, f_n$ à coefficients dans k, il est toujours possible de construire un sur-corps K de k sur lequel chacun des polynômes f_i admet une racine.*

Démonstration: Par le procédé d'adjonction d'une racine utilisé dans la démonstration du théorème 39 on sait construire une extension simple $k(\alpha_1)$ de k sur laquelle f_1 admet une racine α_1. On peut continuer en considérant f_2 comme un polynôme de $k(\alpha_1)[X]$ et d'utiliser le procédé d'adjonction de racine pour construire une extension $(k(\alpha_1))(\alpha_2)$ contenant une racine α_2 de f_2. On pose $k(\alpha_1, \alpha_2) = (k(\alpha_1))(\alpha_2)$ et on continue. Une récurrence finie permet d'obtenir sur un corps $K = k(\alpha_1, \alpha_2, \ldots, \alpha_n)$. □

5.4 Extensions finies

Définition 26. *On appelle extension d'un corps k tout corps K contenant k et muni d'une loi additive et d'une loi multiplicative qui généralisent celles de k. Autrement dit, une extension d'un corps k est un sur-corps de k.*

Définition 27. *Une extension K de k est dite finie ou de degré fini, si K est un espace vectoriel de dimension finie sur k. Si $\dim_k K = n$, on dit que K est une extension finie de degré n sur k ou plus simplement, une extension de degré n sur k. On pose alors*

$$[K : k] = \dim_k K = n.$$

Définition 28. *Une extension K de k est simple s'il existe un élément $a \in K$ tel que $K = k(a)$. Dans ce cas, on dit que a est un élément primitif de K sur k.*

On peut remarquer que:

- Le procédé d'adjonction d'une racine d'un polynôme irréductible P permet de construire une extension simple de degré fini d'après théorème 39.
- Avec les définitions de la section 5.2, si $k \subset K$ et si a est un élément de K algébrique sur k, alors $k(a) \simeq k[X]/(m_a)$ donc $k(a)$ est une extension simple de degré fini de k, et d'après le théorème 40 on a alors:
$$[k(a) : k] = \dim_k k(a) = \deg a = \deg m_a.$$

Théorème 44. *Si a est algébrique sur k, le corps $k(a)$ est un k-espace vectoriel de dimension $d = \deg a$ dont une base est $(1, a, \ldots, a^{d-1})$. C'est aussi une extension de k de degré fini d.*

Une extension simple n'est pas forcément de degré fini. Il suffit de prendre un élément a transcendant sur k. Comme il n'est racine d'aucun polynôme à coefficients sur k, le système $(a^n)_{n\in\mathbb{N}}$ est libre dans le k-espace vectoriel $k(a)$ qui ne peut pas être de dimension finie.

Théorème 45. *Si F, G, et H désignent 3 sous-corps d'un corps K tels que $F \subset G \subset H$ et si H est une extension finie de degré finie de G et si G est une extension de degré finie de F, alors H est une extension de degré fini de F et:*

$$[H : F] = [H : G] \times [G : F].$$

Démonstration: Posons $[G : F] = p$ et $[H : G] = n$. Soient $(g_1, \ldots, g_p)$ une base du F-espoace vectoriel G et $(h_1, \ldots, h_n)$ une base du G-espace vectoriel H. N'importe quel vecteur x de H s'écrit sous la forme $x = \sum_{i=1}^{n} x_i h_i$ avec $x_i \in G$ et on peut écrire chacun des vecteur x_i sous la forme $x_i = \sum_{j=1}^{p} \lambda_{ij} g_j$ avec $\lambda_{ij} \in F$, ce qui donne

$$x = \sum_{i=1}^{n} \sum_{j=1}^{p} \lambda_{ij}(h_i g_j),$$

et le système $(h_i g_j)_{1\leq i\leq n, 1\leq j\leq p}$ engendre le F-espace vectoriel H. C'est aussi un système libre puisque $\sum_{i=1}^{n} \sum_{j=1}^{p} \lambda_{ij}(h_i g_j) = 0$ implique $\sum_{j=1}^{p} \lambda_{ij} g_j = 0$ pour tout i, d'où $\lambda_{ij} = 0$ pout tout i, j puisque les systèmes $(g_1, \ldots, g_p)$ et $(h_1, \ldots, h_n)$ sont libres. En conclusion, $(h_i g_j)_{1\leq i\leq n, 1\leq j\leq p}$ est une base de H et $[H : F] = np = [H : G] \times [G : F]$. □

5.5 Corps des racines d'un polynôme

Théorème 46. *Si f est un polynôme de degré $n \geq 1$ sur un corps k, alors il existe une extension finie K de k sur laquelle f possède n racines. De plus, $[K : k] \leq n!$.*

Démonstration: Posons $K_0 = k$. On réitère le procédé d'adjonction de racine. Les théorèmes **??** montrent l'existence d'une extension simple K_1 de k sur laquelle f possède une racine α_1 et avec $[K_1 : k] \leq \deg f = n$. On peut écrire $f(X) = (X - \alpha_1) f_2(X)$ dans $K_1[X]$ avec $\deg f_2 = n - 1$. Mais il existe aussi une extension K_2 de K_1 où f_2 possède au moins une racine α_2 et $[K_2 : K_1] \leq \deg f_2 = n - 1$. On continue ainsi pour obtenir une tour de corps:

$$k \subset K_1 \subset K_2 \subset \ldots \subset K_n$$

telle que pour tout i, $[K_i : K_{i-1}] \leq n - i + 1$ et f possède au moins i racines dans K_i. Il ne reste plus qu'à poser $K = K_n$ pour que les n racines de f, comptées avec multiplicité appartiennent à K. Il suffit enfin d'utiliser le théorème 45 pour obtenir:

$$[K : k] \leq [K_n : K_{n-1}] \times [K_{n-1} : K_{n-2}] \times \ldots \times [K_1 : K_0] \leq 1 \times 2 \times \ldots \times n = n!$$

□

Définition 29. *Soit $f \in k[X]$. On appelle corps de factorisation de f sur k toute extension finie de K sur laquelle f admet toutes ses racines, autrement dit s'écrit comme un produit de facteurs du premier degré.*

Le théorème 46 montre que tout polynôme f de $k[X]$ admet au moins un corps de factorisation.

Définition 30. *Soit $f \in k[X]$. On appelle corps des racines (corps de décomposition, ou corps de factorisation totale) de f sur k tout corps de factorisation minimal de f sur k (pour la relation d'inclusion entre les ensembles), c'est un corps K tel que:*

- *est un corps de factorisation de f sur k;*
- *pour tout corps de factorisation L de f sur k tel que $k \subset L \subset K$, on a $L = K$.*

On peut montrer que tous les corps des racines d'un polynôme sont isomorphes, et on peut parler du corps des racines.

5.6 Extensions algébriques

Définition 31. *Une extension K d'un corps k est dite algébrique si tout élément de K est algébrique sur k.*

Théorème 47. *Toute extension finie K de k est une extension algébrique de k et le degré de tout élément a de K est toujours un diviseur du degré $[K : k]$ de l'extension.*

Démonstration: Soit $[K : k] = n$. Si $a \in k$, le système de vecteurs $(1, a, a^2, \ldots, a^n)$ est de cardinal $n + 1$ strictement supérieur à la dimension n du k-espace vectoriel K. Il s'agit d'un système lié et il existe $(\lambda_0, \ldots, \lambda_n) \in k^{n+1} \subset \{(0, \ldots, 0\}$ telle que $\lambda_n a^n + \ldots + \lambda_1 x + \lambda_0 = 0$. Cela montre que a est algébrique sur k. Par définition, $\deg a = [k(a) : k]$, et les inclusions $k \subset k(a) \subset K$ permettent d'écrire

$$[K : k] = [K : k(a)] \times [k(a) : k] = [K : k(a)] \times \deg a$$

ce qui prouve que $\deg a$ divise n. □

Le théorème précédent énonce que toute extension finie est une extension algébrique. La réciproque est fausse.

Théorème 48. *Si a est algébrique sur k, le corps $k(a)$ est une extension algébrique de k et $[k(a) : k] = \deg a$.*

Démonstration: Si a est algébrique sur k, le théorème 44 montre que $k(a)$ est une extension finie de k de degré $\deg a$, donc a fortiori une extension algébrique de k d'après le théorème 47. □

Théorème 49. *Soit k un sous-corps de K. L'ensemble A de tous les éléments algébriques de K sur k est un corps.*

Démonstration: Soient $a, b \in A$. Le corps $k(a)$ et une extension de degré fini de k. L'élément b, algébrique sur k, sera aussi un élément algébrique sur $k(a)$. Le corps $k(a, b) = k(a)(b)$ engendré par k, a et b sera une extension de degré fini de $k(a)$ d'après le théorème 44. On peut donc appliquer le théorème 45 et affirmer que $k(a, b)$ est une extension de degré fini de k et:

$$[k(a, b) : k] = [k(a, b) : k(a)] \times [k(a) : k].$$

Comme $k(a, b)$ est une extension finie de k, le théorème 47 montre que c'est une extension algébrique de k, et en particulier les éléments $a \pm b, ab$ et a/b (si $b \neq 0$), qui appartiennent à $k(a, b)$ sont algébrique sur k. □

Définition 32. *Le corps A du théorème précédent est appelé fermeture algébrique de k dans K. C'est la plus grande extension algébrique de k contenue dans K.*

Théorème 50. *Si F, G, et H sont des corps tels que $F \subset G \subset H$, et si G (resp. H) est une extension algébrique de F (resp. G), alors H est une extension algébrique de F.*

Démonstration: Soit $a \in H$. Par hypothèse, a est algébrique sur G, donc est une racine d'un polynôme $P(X) = \sum_{i=0}^{n} g_i X^i$ avec $g_0, \ldots g_n \in G$. Chacun des éléments g_i est algébrique sur F donc le corps $L = F(g_0, \ldots, g_n)$ est une extension finie de F. Comme $P(a) = 0$, l'élément a est algébrique sur L, et donc $L(a)$ est une extension finie de L. Finalement, on a une tour d'extension finies:

$$F \subset L \subset L(a)$$

et $L(a)$ est une extension finie de F (Théorème 45), et donc a est algébrique sur F (Théorème 47). □

5.7 Applications

5.7.1 Construction de $\mathbb{C}$

Le polynôme $X^2 + 1$ est irréductible dans $\mathbb{R}[X]$ puisque de degré 2 et ne possédant pas de racine dans $\mathbb{R}$. L'anneau-quotient $\mathbb{R}[X]/(X^2 + 1)$ est donc un corps. Ce résultat peut se retrouver directement.

On sait que le quotient d'un anneau commutatif par un idéal est un anneau. Montrer que $\mathbb{R}[X]/(X^2+1)$ est un corps, revient à montrer que tout élément non nul $\bar{P}$ de $\mathbb{R}[X]/(X^2+1)$ est inversible. Si $\bar{P} \neq \bar{0}$, alors X^2+1 ne divise pas $P(X)$ et comme X^2+1 est irréductible dans $\mathbb{R}[X]$, les polynômes X^2+1 et $P(X)$ sont premiers entre eux. Le théorème de Bézout est vrai dans tout anneau principal donc dans $\mathbb{R}[X]$ et il existe deux polynômes $U(X)$ et $V(X)$ tels que

$$(X^2+1)U(X) + P(X)V(X) = 1.$$

Il suffit de passer aux classes pour obtenir $\bar{P}\bar{V} = \bar{1}$ dans $\mathbb{R}[X]/(X^2+1)$, ce qui prouve que $\bar{P}$ rest inversible.

On pose $\mathbb{C} = \mathbb{R}[X]/(X^2+1)$ et on dit que $\mathbb{C}$ est le *corps des nombres complexes*. L'ensemble $\mathbb{C} = \mathbb{R}[X]/(X^2+1)$ est structuré en espace vectoriel sur $\mathbb{R}$ en tant que quotient d'un espace vectoriel par un sous-espace vectoriel. La classe de $\bar{X}$ du polynôme X est une racine du polynôme X^2+1. C'est évident par construction car $\bar{X}^2 + 1 = \overline{X^2+1} = \bar{0}$. Ceci prouve que nous avons construit un corps qui contient une racine de -1. C'est bien le procédé d'adjonction de racine.

Enfin, on vérifie que $\mathbb{R}$ s'injecte dans $\mathbb{C}$ en respectant les structures de corps. On peut le vérifier directement ici comme conséquence de:

Théorème 51. *$\mathcal{B} = (\bar{1}, \bar{X})$ est une base du $\mathbb{R}$-espace vectoriel $\mathbb{C}$.*

Démonstration: En utilisant la division euclidienne par X^2+1, on peut écrire que tout polynôme $P(X)$ de $\mathbb{R}[X]$ sous la forme:

$$P(X) = (X^2+1)Q(X) + aX + b$$

avec $Q(X) \in \mathbb{R}[X]$ et $a, b \in \mathbb{R}$. On en déduit $\bar{P} = a\bar{X} + \bar{1}$ donc que tout élément $\bar{P} \in \mathbb{C}$ s'écrit comme combinaison linéaire de $\bar{1}$ et $\bar{X}$, ce qui montre que $\mathcal{B}$ engendre $\mathbb{C}$.

Si $a\bar{X} + b\bar{1} = \bar{0}$, alors X^2+1 divise $aX+b$ et donc $a = b = 0$ puisqu'un polynôme de degré 2 ne peut pas diviser un polynôme non nul de degré inférieur strictement à 2. Ceci montre que $\mathcal{B}$ est un système libre. □

L'application $j : \mathbb{R} \to \mathbb{C}$ qui à a associe $a\bar{1}$ est un morphisme de corps qui permet d'identifier $\mathbb{R}$ au sous-corps $j(\mathbb{R})$ de $\mathbb{C}$ en posant $a = a\bar{1} = \bar{a}$ pour tout $a \in \mathbb{R}$. En posant $i = \bar{X}$, on constate que tout $z \in \mathbb{C}$ s' écrit de façon unique: $z = a\bar{1} + b\bar{X} = a + bi$, avec $a, b \in \mathbb{R}$ et i un nombre complexe tel que $i^2 = -1$.

5.7.2 Extensions quadratiques de $\mathbb{Q}$

Définition 33. *On appelle corps quadratique toute extension de degré 2 de $\mathbb{Q}$, autrement dit contenant $\mathbb{Q}$ et qui est un $\mathbb{Q}$-espace vectoriel de dimension 2.*

Comme $\mathbb{C}$ est la clôture algébrique de $\mathbb{Q}$, on peut supposer qu'un corps quadratique est inclus dans $\mathbb{C}$ à isomorphisme près.

Le plus petit sous-corps de $\mathbb{C}$ contenant $\mathbb{Q}$ et i est $\mathbb{Q}(i) = \{a+ib | a, b \in \mathbb{Q}\}$. C'est une extension quadratique de $\mathbb{Q}$. De façon plus générale, si d est un entier relatif sans facteurs carrés et différent de 1 et si $\sqrt{d}$ désigne l'une des racine de l'équation $x^2 = d$ dans $\mathbb{C}$, il est facile de voir que le plus petit sous-corps de $\mathbb{C}$ contenant $\mathbb{Q}$ et $\sqrt{d}$ est $\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} | a, b \in \mathbb{Q}\}$, et que le corps ainsi obtenu est une extension quadratique de $\mathbb{Q}$.

La notation $\sqrt{d}$ n'est parfaitement définie que si $d > 0$. Quand $d \in \mathbb{R}^*_-$, $\sqrt{d}$ désigne l'un des nombres complexes $i\sqrt{d}$ ou $-i\sqrt{d}$ et on devrait écrire $\mathbb{Q}(\sqrt{d}) = \{a + bi\sqrt{-d} | a, b \in \mathbb{Q}\}$.

Théorème 52. *Tout corps quadratique est de la forme $\mathbb{Q}(\sqrt{d})$ où d est un entier relatif sans facteur carré différent de 1. La réciproque est vraie.*

Démonstration: Si d est un entier relatif sans facteur carré et différent de 1, le polynôme minimal de $\sqrt{d}$ sur $\mathbb{Q}$ est $X^2 - d$ et le théorème 40 montre que $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{d}) = \deg(X^2 - d) = 2$. Ceci prouve la réciproque.

Si k est un corps quadratique, $\dim_{\mathbb{Q}} k = [k : \mathbb{Q}] = 2$ et tout élément a de $k \setminus \mathbb{Q}$ est algébrique sur $\mathbb{Q}$, de degré 2. En effet, d'après le théorème 47, k est une extension finie de $\mathbb{Q}$ donc tout élément a de k est algébrique sur $\mathbb{Q}$, de degré: $\deg a = [\mathbb{Q}(a) : \mathbb{Q}$ un diviseur de $[k : \mathbb{Q}]$. De plus,

$$2 \leq \deg a = \dim_{\mathbb{Q}} \mathbb{Q}(a) = [\mathbb{Q}(a) : \mathbb{Q}] \leq [k : \mathbb{Q}] = 2$$

donc $\deg a = 2$. On en déduit que $k = \mathbb{Q}(a) = \{x_0 + x_1 a | x_0, x_1 \in \mathbb{Q}\}$. On sait que le degré de a est aussi le degré du polynôme minimal m_a de a. On peut donc écrire

$$m_a(X) = X^2 + uX + v$$

avec $(u, v) \in \mathbb{Q}^2$. Le discriminant du trinôme $X^2 + uX + v$ est $\Delta = u^2 - 4v$ et ses racines complexes sont $-u \pm \sqrt{\Delta}$ où $\sqrt{\Delta}$ désigne l'une des solutions de l'équation $x^2 = \Delta$ dans $\mathbb{C}$. Si $a = -u + \epsilon\sqrt{\Delta}$, avec $\epsilon = \pm 1$, on obtient $k = \mathbb{Q}(a) = \mathbb{Q}(\sqrt{\Delta})$. Comme $\Delta \in \mathbb{Q}$, il existe $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$, tel que:

$$\Delta = \frac{p}{q} = \frac{pq}{q^2}$$

donc $k = \mathbb{Q}(\sqrt{pq})$. Il suffit d'écrire pq de la forme $pq = r^2 d$ où d est un entier relatif sans facteur carré pour obtenir $k = \mathbb{Q}(\sqrt{pq}) = \mathbb{Q}(r\sqrt{d}) = \mathbb{Q}(\sqrt{d})$. □

Définition 34. *Un corps quadratique $\mathbb{Q}(\sqrt{d})$ (avec d un entier relatif sans facteur carré et différent de 1) est dit réel si $d > 0$ et imaginaire si $d < 0$.*

Théorème 53. *Soient d, d' deux entiers relatifs tels que $\sqrt{d} \notin \mathbb{Q}$ et $\sqrt{d'} \notin \mathbb{Q}$. Alors les corps $\mathbb{Q}(\sqrt{d})$ et $\mathbb{Q}(\sqrt{d'})$ sont isomorphes si et seulement si il existe un nombre rationnel r tel que $d' = r^2 d$.*

Démonstration: La condition est suffisante puisque $\mathbb{Q}(\sqrt{r^2 d}) = \mathbb{Q}(r\sqrt{d}) = \mathbb{Q}(\sqrt{d})$. Montrons qu'elle est nécessaire. S'il existe un isomorphisme de corps φ de $\mathbb{Q}(\sqrt{d})$ sur $\mathbb{Q}(\sqrt{d'})$ alors nécessairement:

- Pour tout $n \in \mathbb{N}$, $\varphi(n) = n$. En effet, comme φ est un morphisme de corps, $\varphi(1) = 1$ et par récurrence on a: si $\varphi(n) = n$ au rang n, on a $\varphi(n+1) = \varphi(n) + \varphi(1) = n + 1$.
- Pour tout $n \in \mathbb{Z}$, $\varphi(n) = n$. En effet si $n = -m$ avec $m \in \mathbb{N}$, on peut écrire $\varphi(-m) + \varphi(m) = \varphi(0) = 0$, d'où $\varphi(-m) = -\varphi(m) = -m$.
- Pour tout $r \in \mathbb{Q}$, $\varphi(r) = r$. En effet si $r = p/q$ avec $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$, on a $\varphi(p) = \varphi(qr) = \varphi(q)\varphi(r)$, d'où:
$$\varphi(r) = \frac{\varphi(p)}{\varphi(q)} = \frac{p}{q} = r.$$

Finalement, φ laisse invariant tous les éléments de $\mathbb{Q}$ et pour tous $a, b \in \mathbb{Q}$, on a:

$$\varphi(a + b\sqrt{d}) = \varphi(a) + \varphi(b)\varphi(\sqrt{d}) = a + b\varphi(\sqrt{d}).$$

Connaître φ revient à déterminer $\varphi(\sqrt{d})$. De $\varphi(d) = \varphi((\sqrt{d})^2) = (\varphi(\sqrt{d}))^2$, on en déduit $\varphi(\sqrt{d}) = \pm\sqrt{d}$. Ainsi $\sqrt{d} \in \mathbb{Q}(\sqrt{d'})$ et il existe $a, b \in \mathbb{Q}$ tels que $\sqrt{d} = a + b\sqrt{d'}$. Nécessairement, $d = a^2 + b^2 d' + 2ab\sqrt{d'}$, donc:

$$\sqrt{d'} = \frac{d - a^2 - b^2 d'}{2ab}$$

dès que $ab \neq 0$. C'est impossible car $\sqrt{d'}$ n'appartient pas à $\mathbb{Q}$. Donc $ab = 0$ et comme b ne peut pas être nul (autrement $\sqrt{d} = a$ et $\sqrt{d} \in \mathbb{Q}$), on obtient $a = 0$ et $\sqrt{d} = b\sqrt{d'}$, d'où $d = b^2 d'$. □

Théorème 54. *Les seuls automorphismes du corps $K = \mathbb{Q}(\sqrt{d})$ (où d est un entier relatif sans facteur carré et distinct de 1) sont l'identité et l'application (conjugaison): $\sigma : K \to K$ qui à $a + b\sqrt{d}$ associe $a - b\sqrt{d}$.*

Démonstration: On constate que l'identité et σ sont des automorphismes de K. Réciproquement, si $\varphi : K \to K$ est un automorphisme de corps, on procède comme dans la preuve du théorème précédent pour voir que φ laisse invariant tous les éléments de $\mathbb{Q}$ et que

$$\forall a, b \in \mathbb{Q},\ \varphi(a + b\sqrt{d}) = \varphi(a) + \varphi(b)\varphi(\sqrt{d}) = a + b\varphi(\sqrt{d}).$$

Ici, encore $\varphi(d) = \varphi(\sqrt{d})^2) = (\varphi(\sqrt{d}))^2$ donne $\varphi(\sqrt{d}) = \pm\sqrt{d}$ de sorte que φ soit égale à σ ou à l'identitié. □

5.8 Groupes de Galois d'un corps fini

Le groupe de Galois $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ de $\mathbb{F}_{q^m}$ sur $\mathbb{F}_q$ est par définition le groupe des automorphismes du corps $\mathbb{F}_{q^m}$ laissant $\mathbb{F}_q$ invariant point par point. On connaît au moins un élément qui est l'automorphisme de Frobenius:

$$\begin{aligned}\sigma : \mathbb{F}_{q^m} &\to \mathbb{F}_q \\ x &\mapsto x^q.\end{aligned}$$

On sait que:

- Si $f(x) = x^m + a_{m-1}x^{m-1} + \ldots + a_0$ est un polynôme irréductible unitaire de $\mathbb{F}_1[x]$ et si α est une racine de f dans une extension quelconque de $\mathbb{F}_q$, alors $\mathbb{F}_{q^m} \simeq \mathbb{F}_q[\alpha]$. On peut donc identifier ces deux corps et écrire $\mathbb{F}_{q^m} = \mathbb{F}_q[\alpha]$. Dans ce cas, on dit que α est un élément primitif de $\mathbb{F}_{q^m}$ et que f est le polynôme minimal de α sur $\mathbb{F}_q$.

- Toutes les racines de $f(x)$ sont simples et ce sont $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha q^{m-1}$. Ces puissances de α sont appelées les conjugués de α par rapport à $\mathbb{F}_q$. Si $\zeta \in \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$, pour tout $x \in \mathbb{F}_q$,

  $$\zeta(f(x)) = \zeta(x^m + a_{m-1}x^{m-1} + \ldots + a_1x + a_0) = \zeta(x)^m + a_{m-1}\zeta(x)^{m-1} + \ldots + a_0 = f(\zeta(x)),$$

  et donc

  $$f(x) = 0 \Rightarrow f(\zeta(x)) = 0 \Rightarrow \zeta(x) \in \left\{\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}\right\}.$$

  Il existe ainsi $i \in \{0, 1, \ldots, m-1\}$, tel que $\zeta(x) = \alpha^{q^i}$. Mais on sait que tout élément de $x \in \mathbb{F}_{q^m}$ s'écrit comme combinaison linéaire à coefficients dans $\mathbb{F}_q$ de $1, \alpha, \ldots, \alpha^{m-1}$, i.e. sous la forme $x = x_0 + x_1\alpha + \ldots + x_{m-1}\alpha^{m-1}$, avec $x_i \in \mathbb{F}_q$, on obtient:

  $$\zeta(x) = x_0 + x_1\alpha^{q^i} + \ldots + x_{m-1}x^{q^i(m-1)} = (x_0 + x_1\alpha + \ldots + x_{m-1}\alpha^{m-1})^{q^i} = x^{q^i}.$$

  Ceci prouve que ζ transforme x en x^{q^i}, c'est-à-dire que $\zeta = \sigma^i$. Réciproquement, pour tout entier i, l'application σ^i est bien un élément de $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$.

- On remarque enfin que les applications $\sigma^j, (0 \leq j \leq m-1)$, sont distinctes entre elles deux à deux car elles transforment α en des éléments distincts α^{q^j} distincts. Comme l'ordre de σ est m, $\sigma^m = Id$, et $\sigma^i \neq Id$ pour tout $i \in \{0, 1, \ldots, m-1\}$.

Théorème 55. *Le groupe de Galois de* $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ *de* $\mathbb{F}_{q^m}$ *sur* $\mathbb{F}_q$ *est cyclique et engendré par l'automorphisme de Frobenius* $\sigma(x) = x^q$. *Autrement dit,*

$$\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q) = \{Id, \sigma, \sigma^2, \ldots, \sigma^{m-1}\} \simeq \mathbb{Z}/m\mathbb{Z}.$$

5.9 Traces, normes et discriminants

Soit L une extension finie de degré n d'un corps commutatif K. À tout élément $x \in L$, on associe l'application $u_x : L \to L$ qui à y associe xy. Cette application est un endomorphisme du K-espace vectoriel L. Notons $\mathcal{L}_K(L)$ l'ensemble des endomorphismes de L. L'application de $L \to \mathcal{L}_K(L)$ qui à $x \in L$ associe u_x est un morphisme d'algèbre qui permet d'identifier L à un sous-corps de $\mathcal{L}_K(L)$ et ainsi représenter tout élément de L par une matrice carrée d'ordre n à coefficients dans K. On pose:

Définition 35. *La trace (resp. le déterminant) de l'application* $u_x \in \mathcal{L}_K(L)$ *est appelée la trace (resp. norme) de* x. *On les note* $\mathrm{Tr}_{L/K}(x) = Tru_x$ *et* $\mathrm{N}_{L/K}(x) = \det u_x$. *Le polynôme caractéristique* $\chi_{L/K}(x)(X) = \det(XId - u_x)$ *de* u_x *sera appelé le polynôme caractéristique de* x*:*

$$\chi_{L/K}(x)(X) = X^n - (\mathrm{Tr}_{L/K}(x))X^{n-1} + \ldots + (-1)^n\mathrm{N}_{L/K}(x).$$

Proposition 17. *Si L est une extension finie de degré n d'un corps commutatif K, alors:*

1. $\mathrm{Tr}_{L/K} : L \to K$ *est une forme K-linéaire;*
2. *pour tout $x \in K$,* $\mathrm{Tr}_{L/K}(x) = nx$;
3. $\mathrm{N}_{L/K} : L \to K$ *est multiplicative, i.e. pour tout $x, y \in L$,* $\mathrm{N}_{L/K}(xy) = \mathrm{N}_{L/K}(x)\mathrm{N}_{L/K}(y)$.

Démonstration: Pour 1), les fonctions Tr et $x \mapsto u_x$ sont K-linéaires et donc pour tous $x, y \in L$ et tout $\lambda \in K$, on a

$$\mathrm{Tr}_{L/K}(x + \lambda y) = \mathrm{Tr}_{L/K}(u_{x+\lambda y}) = \mathrm{Tr}_{L/K}(u_x + \lambda u_y) = \mathrm{Tr}_{L/K}(u_x) + \lambda \mathrm{Tr}_{L/K}(u_y) = \mathrm{Tr}_{L/K}(x) + \lambda \mathrm{Tr}_{L/K}(y)$$

et $\mathrm{Tr}_{L/K} : L \to K$ est bien une application K-linéaire à valeurs dans K, i.e. une forme K-linéaire. Pour 2), si $x \in K$ (x est un scalaire), alors l'application u_x est l'homothétie de rapport x donc sa matrice dans une base quelconque est xI où I est la matrice identité de taille n. On a donc: $\mathrm{Tr}_{L/K}(x) = \mathrm{Tr} u_x = \mathrm{Tr}(xI) = nx$. Pour 3), pour tous $x, y \in L$, $\mathrm{N}_{L/K}(xy) = \det u_{xy}$ et $u_{xy} = u_x \circ u_y$ donc $\mathrm{N}_{L/K}(xy) = \det u_{xy} = \det(u_x) \times \det(u_y) = \mathrm{N}_{L/K}(x) \times \mathrm{N}_{L/K}(y)$. □

Dans le cas d'un corps fini, comme le groupe de Galois $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ de $\mathbb{F}_{q^m}$ sur $\mathbb{F}_q$ est cyclique et engendré par l'automorphisme de Frobenius $x \mapsto \sigma(x) = x^q$, on a:

Théorème 56. *Soit $\mathbb{F}_{q^m}$ l'extension finie de $\mathbb{F}_q$ et $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ le groupe de Galois. Pour tout $x \in \mathbb{F}_{q^m}$,*

$$\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(x) = x + x^q + \ldots + x^{q^{m-1}} = \sum_{\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)} \sigma(x)$$

et

$$\mathrm{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(x) = x \cdot x^q \cdot \ldots \cdot x^{q^{m-1}} = \prod_{\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)} \sigma(x).$$

5.10 Algorithme de Berlekamp

Il peut paraître surprenant, mais vrai, que la factorisation de polynômes est un problème plus facile que la factorisation d'entiers et on commence par factoriser des polynômes modulo de petits nombres premier p. Comme K est un corps commutatif, l'anneau $K[X]$ est principal, donc factoriel. Tout polynôme non nul f de $\mathbb{F}_q[X]$ admet donc une décomposition en produit de facteurs irréductibles unitaires de la forme $f = af_1^{\alpha_1} \ldots f_k^{alpha_k}$ où $a \in \mathbb{F}_q^*$ et les f_i sont des polynômes unitaires irréductibles et les α_i sont des entiers naturels.

Supposons qu'on nous donne un polynôme $g(x)$ de degré n et on veut décider s'il est irréductible ou le factoriser en facteurs irréductibles. Un cas facile à gérer est quand $g(x)$ contient un facteur carré, *i.e.* un facteur de la forme $p(x)^2$. Dans ce cas, $p(x)$ divise $\gcd(g(x), g'(x))$ où $g'(x)$ est le polynôme dérivé de g. Sur un domaine discret, la dérivation n'a pas l'interprétation en terme de "pente" comme dans les réels, et on le calcule de façon syntaxique en définissant la dérivée de x^d comme étant dx^{d-1} et en l'étendant par linéarité. Il n'est pas difficile de vérifier que tous les théorèmes s'appliquent et en particulier la dérivée de $p(x)^2 h(x)$ est $p(x)^2 h'(x) + 2p'(x)p(x)h(x)$. Ainsi, le facteur $p(x)$ peut être retrouvé en utilisant l'algorithme d'Euclide appliquée aux polynômes.

On peut remarquer que sur un corps fini, $g'(x)$ peut être identiquement nul même si $g(x)$ n'est pas constant. Ceci arrive mod$p$ quand $g(x) = h(x^p)$ for un polynôme h. Dans ce cas $\gcd(g(x), g'(x)) = g(x)$ et on n'obtient pas une factorisation non triviale. Cependant, mod$p$ il est vrai que $h(x^p) = h(x)^p$ et on peut procéder simplement pour factoriser h. Concentrons-nous sur le cas $p = 2$ et nous verrons ensuite comment étendre les résultats à un p plus général. Gardons en mémoire que tous les calculs sont fait mod2.

La clé de notre algorithme est l'application

$$f(x) \mapsto f(x)^2 \bmod g(x)$$

des polynômes de degrés au plus $n-1$. C'est une application linéaire car $(f_1(x), f_2(x))^2 = f_1(x)^2 + f_2(x)^2$ en caractéristique 2. On s'intéresse aux points fixes de cette application, *i.e.* aux polynômes $f(x)$ tels que

$$f(x) = f(x)^2 \bmod g(x) \tag{5.1}$$

Si g est irréductible, alors travailler $\bmod g(x)$ est équivalent à travailler dans le corps $\mathbb{F}_{2^n}$ et comme dans tout corps une équation quadratique a au plus 2 solutions, il est facile de voir que l'équation donnée a exactement 2 solutions qui sont les constantes 0 et 1.

Si g est le produit d'un nombre de polynômes irréductibles (disons 2 pour rendre les choses plus concrètes), la situation change. Soit $g(x) = g_1(x)g_2(x)$ alors d'après le théorème des restes chinois, chaque polynôme $f \bmod g$ peut se représenter par la paire (f_1, f_2) avec $f(x) = f_i(x) \bmod g_i(x)$. Alors f résout l'équation ssi f_1 la résout $\bmod g_1$ et f_2 la résout $\bmod g_2$. Comme on sait que l'ensemble des solutions mod des polynômes irréductibles, ceci implique que l'on a 4 solutions $\bmod g(x)$. Il s'agit de (quand on les écrit par paires, *i.e.* la première composante est le reste $\bmod g_1$ et le second $\bmod g_2$) $(0,0), (1,1), (0,1)$ et $(1,0)$. Les deux premières solutions correspondent aux racines habituelles $f(x)$ étant les constantes 0 et 1 alors que les 2 autres sont plus intéressantes. Si $f_{(0,1)}(x)$ est le polynôme correspondant à la troisième solution, alors $\gcd(g(x), f_{(0,1)}(x)) = g_1(x)$ et notre problème est résolu. Dans le cas général, le nombre de points fixes est 2^ℓ où ℓ est le nombre de facteurs irréductibles dans g. Voyons comment ceci fonctionne sur une paire d'exemples.

Exemples. Soit $g(x) = x^5 + x^2 + 1$. Alors avec notre application:

$$1 \mapsto 1, \quad x \mapsto x^2, \quad x^2 \mapsto x^4, \quad x^3 \mapsto x^6 = x^3 + x, \quad x^4 \mapsto x^8 = x^2 \cdot x^6 = x^5 + x^3 = x^3 + x^2 + 1.$$

Ainsi dans la base $(1, x, x^2, x^3, x^4)$, notre application est donnée par la matrice:

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

Comme on recherche les points fixes de cette application définie par M, on veut chercher le noyau de l'application donnée par la matrice $M + I$ où I est la matrice identité, *i.e.* on veut étudier la matrice:

$$M + I = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Il est facile de vérifier que le noyau de cette matrice est donné par le seul vecteur $(1, 0, 0, 0, 0)$ et donc $x^5 + x^2 + 1$ est irréductible.

Exemples. Soit $g(x) = x^5 + x + 1$. Cette fois:

$$1 \mapsto 1, \quad x \mapsto x^2, \quad x^2 \mapsto x^4, \quad x^3 \mapsto x^6 = x^2 + x, \quad x^4 \mapsto x^8 = x^2 \cdot x^6 = x^4 + x^3.$$

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

ce qui donne

$$M + I = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

Le noyau de cette matrice est engendré par $(1,0,0,0,0)$ et $(0,1,0,1,1)$. Le premier est la solution triviale, alors que le second vecteur correspond au polynôme $x^4 + x^3 + x$. En calculant $\gcd(x^5 + x + 1, x^4 + x^3 + x)$ avec Euclide étendu, on obtient:

$$x^5 + x + 1 = (x+1)(x^4 + x^3 + x) + x^3 + x^2 + 1 \tag{5.2}$$

$$x^4 + x^3 + x = x(x^3 + x^2 + 1). \tag{5.3}$$

Finalement, la division donne $x^5 + x + 1 = (x^3 + x^2 + 1)(x^2 + x + 1)$ qui est la factorisation complète.

Calculer le noyau est un algorithme classique d'algèbre linéaire et peut se faire en utilisant l'élimination gaussienne. Comme le pgcd se calcule même plus vite, on obtient: on peut factoriser un polynôme de degré n sur $\mathbb{F}_2$ en facteurs irréductibles en temps $O(n^3)$.

Nous avons en fait seulement établi comment factoriser un polynôme non irréductible en 2 facteurs. On laisse les détails de compléter la factorisation dans le même temps comme un exercice. On remarque cependant que le calcul du noyau n'a pas besoin d'être refait et donc la partie difficile du calcul peut être réutilisée.

5.10.1 Factoriser des polynômes dans des corps plus grand

Voyons ce qui se passe pour des premiers p autre que 2. La plupart du travail se transfert sans changement et en particulier on doit étudier l'application:

$$f(x) \mapsto f(x)^p = f(x^p) \bmod g(x)$$

qui est encore une application linéaire. L'ensemble des points fixes de cette application est un sous-espace linéaire des polynômes de degré au plus $n-1$ de dimension ℓ où ℓ est le nombre de facteurs irréductibles de g. Ces points fixes sont tous les polynômes $h(x)$ tels que h est une constante (polynôme de degré 0) $\bmod g_i$ pour chaque facteur irréductible g_i de g. Si g n'est pas irréductible, alors dans le cas $\bmod 2$, il était vrai que pout tout point fixe non constant h, $\gcd(h,g)$ était non trivial. Ceci n'est pas vrai pour des p plus grand, *e.g.* pour $p = 3$, on peut avoir $g(x) = g_1(x)g_2(x)$ et $h(x) = 1 \bmod g_1(x)$ et $h(x) = 2 \bmod g_2(x)$, alors h est un point fixe alors que $\gcd(h,g) = 1$. Cependant, il est aussi vrai que pour un i, $0 \le i \le p-2$, $\gcd(h+i,g)$ est non trivial. Ainsi, $p-1$ calculs de pgcd est toujours suffisant pour trouver un facteur non trivial.

Analysons le temps de calcul de cet algorithme. Par simplicité, comptons le nombre d'opérations qui sont fait sur des entiers $\bmod p$ plutôt que des opérations sur les bits. Supposons que $p \le n$. Alors en utilisant $x^{p(i+1)} = x^p(x^{pi})$ il est facile de voir que chaque colonne de la matrice M peut se calculer à partir de la précédente en $O(np)$ opérations. Déterminer le noyau se fait par élimination gaussienne en $O(n^3)$ opérations et finalement chaque pgcd peut se faire en $O(n^2)$ opérations, ce qui donne un total de $O(pn^2 + n^3) = O(n^3)$ opérations sur des entiers $\bmod p$.

Si p est grand, alors le coût $O(pn^2)$ devient le coût dominant. Cependant, dans le premier cas (construction de la matrice M) on peut être plus rapide. On peut précalculer $x^p \bmod g(x)$ avec $O(\log p)$ élévations au carré et multiplication par x et on peut le calculer avec $O(n^2 \log p)$ opérations. Chaque colonne suivante peut se calculer en $O(n^2)$ opérations. Ainsi, la première partie de l'algorithme qui détermine le nombre de facteurs irréductibles peut se faire en $O(n^2 \log p + n^3)$ opérations. Cependant, la seconde étape (factorisation de g non irréductibles) est inefficace pour de grand p.

Pour obtenir un algorithme efficace pour un grand p on a besoin de faire une remarque supplémentaire. L'inefficacité vient du fait que si h est un point fixe, alors on sait que $h(x) \bmod g_1(x)$ est l'un des nombres $0, 1, \ldots, p-1$ mais on ne sait pas lequel. On a besoin de réduire ce choix. L'idée est de considérer $h(x)^{(p-1)/2}$.

Comme pour tout $a \neq 0 \bmod p$, on a $a^{(p-1)/2} = \pm 1$ (la moitié des as donne chaque choix), on est dans une meilleure situation. La seconde étape est ainsi transformée en

$$\text{Pourunpointfixealeatoire } \ h\text{calculer } \ \gcd(h^{(p-1)/2} - 1, g(x)).$$

Le polynôme $h^{(p-1)/2} \bmod g(x)$ peut se calculer en $O(n^2 \log p)$ opérations par la méthode des élévations au carré. Il est possible de montrer qu'avec probabilité au moins $1/2$, le pgcd précédent est non trivial. Ainsi, on a une méthode qui s'exécute en temps $O(n^2 \log p + n^3)$. On remarque que la réponse est toujours correcte car l'étape déterminant le nombre de facteurs irréductibles est déterministe. On rassemble tout cela dans le théorème.

Théorème 57. *Factoriser des polynômes dans $\mathbb{F}_p$ peut se faire en $O(n^3 + n^2 \log p)$ opérations sur des éléments du corps. Les algorithmes sont probabilistes et le temps de calcul est en moyenne. La réponse est toujours correcte.*

Chapter 6

Réduction de réseaux

Le problème du vecteur le plus court est au cœur des aspects calculatoires de la géométrie des nombres. L'algorithme d'approximation présenté ici a de nombreuses applications en théorie algorithmique des nombres et en cryptographie. Deux des plus importantes applications sont l'obtention d'algorithmes polynomiaux pour factoriser les polynômes sur le corps des rationnels et la résolution du problème du sac-à-dos.

Définition 36. *Étant donné n vecteurs linéairement indépendants $\mathbf{a}_1, \ldots, \mathbf{a}_n \in \mathbb{Q}^n$, trouver un vecteur (non nul) le plus court, pour la norme euclidienne du module ($\mathbb{Z}$-espace vectoriel, lattice en anglais) engendré par ces vecteurs. Le module $\mathcal{L}$ engendré par $\mathbf{a}_1, \ldots, \mathbf{a}_n$ est l'ensemble des combinaisons linéaires entières de ces vecteurs, i.e. $\mathcal{L} = \{\lambda_1 \mathbf{a}_1 + \ldots + \lambda_n \mathbf{a}_n | \lambda_i \in \mathbb{Z}\}$.*

Remarque 21. *Nous ne considérerons que des modules de rang total, c'est-à-dire des modules qui remplissent entièrement l'espace dans lequel ils sont définis. La plupart des résultats s'étendent au cas général mais les preuves sont plus compliquées.*

Nous allons présenter un algorithme ayant un facteur d'approximation exponentiel (en n) pour ce problème. La recherche d'un algorithme ayant un facteur d'approximation polynomial est un problème ouvert depuis plus de trente ans. Néanmoins, il est important de remarquer que cet algorithme de facteur d'approximation exponentiel est très efficace et très utilisé en pratique.

Le vecteur le plus court d'un module unidimensionnel engendré par deux entiers est tout simplement le plus grand diviseur commun des deux entiers qui se calcule en temps polynomial avec l'algorithme d'Euclide. En dimension 2, le problème du vecteur le plus court se résout aussi en temps polynomial. C'est une conséquence de l'algorithme de Gauss formulé initialement dans le langage des formes quadratiques. Il sera instructif de commencer par étudier ces deux algorithmes puisque l'algorithme de Gauss est une généralisation de celui d'Euclide et que l'algorithme en dimension n est une généralisation de celui de Gauss.

6.1 Bases, déterminants et défaut d'orthogonalité

Tous les vecteurs sont considérés en ligne. Nous noterons $\boldsymbol{A}$ la matrice $n \times n$ dont les lignes sont les vecteurs $\mathbf{a}_1, \ldots, \mathbf{a}_n$ données en entrée. Soient $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathcal{L}$ des vecteurs et $\boldsymbol{B}$ la matrice $n \times n$ dont les lignes sont $\mathbf{b}_1, \ldots, \mathbf{b}_n$. Puisque $\mathbf{a}_1, \ldots, \mathbf{a}_n$ engendrent $\mathbf{b}_1, \ldots, \mathbf{b}_n$, $\boldsymbol{B} = \boldsymbol{\Lambda}\boldsymbol{A}$, où $\boldsymbol{\Lambda}$ est une matrice $n \times n$ à coefficients entiers. Ainsi, $\det \boldsymbol{B}$ est un multiple entier de $\det \boldsymbol{A}$. Nous dirons que $\mathbf{b}_1, \ldots, \mathbf{b}_n$ forment une *base* du module $\mathcal{L}$ si le module engendré par ces vecteurs est exactement $\mathcal{L}$. On dira qu'une matrice carrée à coefficients entiers est *unimodulaire* si son déterminant est ± 1. Remarquons que l'inverse d'une matrice unimodulaire est aussi unimodulaire.

Théorème 58. *Pour tous les vecteurs $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathcal{L}$, les propositions suivantes sont équivalentes:*

1. *$\mathbf{b}_1, \ldots, \mathbf{b}_n$ forment une base du module $\mathcal{L}$;*

2. $|\det \boldsymbol{B}| = |\det \boldsymbol{A}|$;

3. *il existe une matrice* $n \times n$ *unimodulaire* $\boldsymbol{U}$ *telle que* $\boldsymbol{B} = \boldsymbol{U}\boldsymbol{A}$.

Démonstration: Puisque $\mathbf{a}_1, \ldots, \mathbf{a}_n$ engendrent $\mathbf{b}_1, \ldots, \mathbf{b}_n$, $\boldsymbol{B} = \boldsymbol{\Lambda}\boldsymbol{A}$, où $\boldsymbol{\Lambda}$ est une matrice $n \times n$ à coefficients entiers.

$1 \Rightarrow 2$**:** Si $\mathbf{b}_1, \ldots, \mathbf{b}_n$ est une base de $\mathcal{L}$, ils engendrent $\mathbf{a}_1, \ldots, \mathbf{a}_n$. Donc, $\boldsymbol{A} = \boldsymbol{\Lambda}'\boldsymbol{B}$ où $\boldsymbol{\Lambda}'$ est une matrice $n \times n$ à coefficients entiers. Ainsi, $\det \boldsymbol{\Lambda} \det \boldsymbol{\Lambda}' = 1$. Or les déterminants de $\boldsymbol{\Lambda}$ et $\boldsymbol{\Lambda}'$ sont des entiers, et donc $\det \boldsymbol{\Lambda} = \pm 1$, et $|\det \boldsymbol{\Lambda} = \pm 1$, et $\det \boldsymbol{B}| = |\det \boldsymbol{A}|$.

$2 \Rightarrow 3$**:** Comme $\det \boldsymbol{B}| = |\det \boldsymbol{A}|$, nous avons $\det \boldsymbol{A} = \pm 1$, c'est-à-dire $\boldsymbol{\Lambda}$ est unimodulaire.

$3 \Rightarrow 1$**:** Comme $\boldsymbol{U}$ est unimodulaire, $\boldsymbol{U}^{-1}$ aussi. Or, $\boldsymbol{A} = \boldsymbol{U}^{-1}\boldsymbol{B}$. Les vecteurs $\mathbf{a}_1, \ldots, \mathbf{a}_n$ s'écrivent donc comme des combinaisons linéaires entières de $\mathbf{b}_1, \ldots, \mathbf{b}_n$, qui forment donc une base de $\mathcal{L}$.

Le théorème 58 signifie que le déterminant d'une base est un invariant du module, au signe près. Nous appellerons $|\det \boldsymbol{A}|$ le *déterminant du module* $\mathcal{L}$ que l'on notera $\det \mathcal{L}$. Observons que $\det \mathcal{L}$ est le volume du parallélépipède défini par vecteurs de base. Ce théorème nous dit que l'on peut passer d'une base à une autre par des transformations unimodulaires. Nous l'utiliserons dans nos algorithmes.

La base idéale pour notre problème est orthogonale, car toute base orthogonale contient un plus court vecteur de $\mathcal{L}$. Cependant, une telle base n'existe pas toujours. Par exemple, le module bidimensionnel suivant n'admet pas de base orthogonale.

On notera $\|\mathbf{a}\|$ la norme euclidienne d'un vecteur $\mathbf{a}$. Rappelons que l'inégalité de Hadamard affirme que, pour toute matrice $n \times n$ réelle $\boldsymbol{A}$,

$$|\det \boldsymbol{A}| \leq \|\mathbf{a}_1\| \cdots \|\mathbf{a}_n\|.$$

De plus cette inégalité est une égalité ssi une. ligne de $\boldsymbol{A}$ est nulle ou bien toutes les lignes sont deux à deux orthogonales. Ainsi, pour toute base $\mathbf{b}_1, \ldots, \mathbf{b}_n$ d'un module $\mathcal{L}$,

$$\det \mathcal{L} \leq \|\mathbf{b}_1\| \cdots \|\mathbf{b}_n\|.$$

Puisqu'aucun des vecteurs n'est nul, cette inégalité est une égalité ssi la base est orthogonale. Nous appellerons le *défaut d'orthogonalité* d'une base $\mathbf{b}_1, \ldots, \mathbf{b}_n$ la quantité:

$$\frac{\|\mathbf{b}_1\| \cdots \|\mathbf{b}_n\|}{\det \mathcal{L}}.$$

Puisque $\det \mathcal{L}$ est un invariant, plus le défaut d'orthogonalité est petit, plus les vecteurs doivent être courts.

On dira qu'une famille de vecteurs $\mathbf{b}_1, \ldots, \mathbf{b}_k \in \mathcal{L}$ linéairement indépendants est *primitive* si on peut la compléter en une base de $\mathcal{L}$. On dira qu'un vecteur $\mathbf{a} \in \mathcal{L}$ est *le plus court vecteur dans sa direction* si $x\mathbf{a}$ n'est pas un vecteur de $\mathcal{L}$ pour tout $0 < |x| < 1$. Il est facile de déterminer si un vecteur seul est primitif.

Théorème 59. *Un vecteur* $\mathbf{a} \in \mathcal{L}$ *est primitif ssi* $\mathbf{a}$ *et le plus court dans sa direction.*

Démonstration: Supposons qu'il existe une base $\boldsymbol{B}$ de $\mathcal{L}$ contenant $\mathbf{a}$. Puisque $\mathbf{a}$ est le plus court vecteur dans sa direction, $\gcd(\lambda_1, \ldots, \lambda_n)$ vaut 1. Par conséquent, il existe une matrice $n \times n$ unimodulaire $\boldsymbol{\Lambda}$ dont la première ligne est $\lambda_1, \ldots, \lambda_n$ (Montrer-le). Posons $\boldsymbol{B} = \boldsymbol{\Lambda}\boldsymbol{A}$. D'après le théorème précédent, $\boldsymbol{B}$ est une base de $\mathcal{L}$ qui contient $\mathbf{a}$. □

6.2 Les algorithmes d'Euclide et de Gauss

En dimension 1, le module engendré par un unique vecteur $\mathbf{a}$ est l'ensemble des multiples de $\mathbf{a}$. Le problème du vecteur le plus court en dimension 1 est donc trivial. Considérons plutôt le problème suivant: étant donné deux entiers a et b, considérer l'ensemble des entiers obtenus par combinaison linéaire entière de a et b, et trouver le plus petit entier positif de ce module. Il s'agit de trouver le pgcd de a et b.

Quitte à échanger a et b, supposons que $a \geq b \geq 0$. L'idée de l'algorithme d'Euclide est de remplacer les entrées de départ par d'autres plus petites en remarquant que $\gcd(a,b) = \gcd(a-b,b)$. En réitérant, on est amené à trouver le plus petit entier en valeur absolue de l'ensemble $\{|a-mb||m \in \mathbb{Z}\}$. Notons-le c. Si $c = 0$, alors $\gcd(a,b) = b$ et nous avons terminé. Sinon, $\gcd(a,b) = \gcd(b,c)$ et nous pouvons réitérer sur la paire (b,c). Comme $c \leq b/2$, ce processus termine au bout d'au plus $\log_2 b$ itérations.

Étudions maintenant l'algorithme de Gauss en dimension 2. En dimension 2, il existe une condition plus faible que l'orthogonalité pour garantir qu'une base contient un vecteur le plus court. Notons θ l'angle entre les deux vecteurs de la base $\mathbf{b}_1$ et $\mathbf{b}_2$, $0° < \theta < 180°$. Alors, $\det \mathcal{L} = \|\mathbf{b}_1\| \cdot \|\mathbf{b}_2\| \sin\theta$. Quitte à échanger $\mathbf{b}_1$ et $\mathbf{b}_2$, supposons $|\mathbf{b}_1| \leq |\mathbf{b}_2|$.

Théorème 60. *Si $60° \leq \theta \leq 120°$, alors $\mathbf{b}_1$ est un vecteur court le plus court du module $\mathcal{L}$.*

Démonstration: Supposons par l'absurde qu'il existe un vecteur $\mathbf{b} \in \mathcal{L}$ plus court que $\mathbf{b}_1$. Puisque $\mathbf{b}_1$ et $\mathbf{b}_2$ sont tous deux primitifs, $\mathbf{b}$ ne peut pas être multiple de $\mathbf{b}_1$ ou $\mathbf{b}_2$. Une simple énumération des cas, montre que tout vecteur $\mathbf{b}$ fait un angle inférieur à $60°$ avec l'un des quatre vecteurs $\mathbf{b}_1$, $\mathbf{b}_2$, $-\mathbf{b}_1$, ou $-\mathbf{b}_2$.

Notons $\boldsymbol{D}$ la matrice 2×2 dont les lignes sont $\mathbf{b}$ et le vecteur, parmi $\mathbf{b}_1$, $\mathbf{b}_2$, $-\mathbf{b}_1$, ou $-\mathbf{b}_2$, qui fait un angle $< 60°$ avec $\mathbf{b}$. Remarquons que $|\det \boldsymbol{D}|$ est non nul et qu'il est strictement inférieur à $\det \mathcal{L} = \|\mathbf{b}_1\| \cdot \|\mathbf{b}_2\| \sin\theta$, ce qui contredit que $\det \boldsymbol{D}$ est un multiple entier de $\det \mathcal{L}$. Le vecteur $\mathbf{b}_1$ est donc bien un vecteur le plus court de $\mathcal{L}$. □

Notons le produit scalaire par $\cdot$ et posons

$$\mu_{21} = \frac{\mathbf{b}_2 \cdot \mathbf{b}_1}{\|\mathbf{b}_1\|^2}.$$

Observons que $\mu_{21}\mathbf{b}_1$ est la projection de $\mathbf{b}_2$ sur la direction de $\mathbf{b}_1$. La proposition suivante suggère un algorithme pour trouver une base satisfaisant la condition du théorème 60.

Proposition 18. *Si une base $\{\mathbf{b}_1, \mathbf{b}_2\}$ vérifie:*

- $\|\mathbf{b}_1\| \leq \|\mathbf{b}_2\|$ *et*
- $|\mu_{21}| \leq 1/2$,

alors $60° \leq \theta \leq 120°$

Démonstration: Remarquons que

$$\cos\theta = \frac{\mathbf{b}_2 \cdot \mathbf{b}_1}{\|\mathbf{b}_1\| \cdot \|\mathbf{b}_2\|} = \frac{\mu_{21}\|\mathbf{b}_1\|}{\|\mathbf{b}_2\|}.$$

Ainsi, d'après les deux conditions, $|\cos\theta| \leq 1/2$. D'où, $60° \leq \theta \leq 120°$. □

Gauss proposa l'algorithme suivant pour transformer une base arbitraire en une base qui satisfait les conditions énoncées ci-dessus.

Remarquons que les opérations en jeu consistent à échanger les lignes de $\boldsymbol{B}$ et à soustraire un multiple d'une ligne à l'autre. Ces opérations sont clairement unimodulaires (la valeur absolue du déterminant est inchangée). Par conséquent, nous conservons bien une base de $\mathcal{L}$.

Clairement, après l'étape 2(a), $|\mu_{21}| \leq 1/2$. Remarquons que cette étape est très similaire à l'algorithme du pgcd d'Euclide. Elle minimise la projection de $\mathbf{b}_2$ sur $\mathbf{b}_1$ en soustrayant à $\mathbf{b}_2$ un nombre convenable de fois $\mathbf{b}_1$. Puisque $\|\mathbf{b}_1\| \cdot \|\mathbf{b}_2\|$ décroît à chaque itération, l'algorithme doit terminer (il n'y a qu'un nombre fini de vecteurs de $\mathcal{L}$ à l'intérieur d'une boule donnée. La preuve que l'algorithme termine en temps polynomial est laissée au lecteur ou peut être trouvée dans ...

6.3 Orthogonalisation de Gram-Schmidt

Ceci nous permettra dans la section suivante de minorer OPT, c'est-à-dire la longueur du plus court vecteur du module $\mathcal{L}$.

1. Initialisation. quitte à échanger $\mathbf{b}_1$ et $\mathbf{b}_2$, $\|\mathbf{b}_1\| \leq \|\mathbf{b}_2\|$.
2. Tant que les conditions de la proposition 18 ne sont pas vraies, faire:
   a Si $|\mu_{21}| > 1/2$, faire $\mathbf{b}_2 := \mathbf{b}_2 - m\mathbf{b}_1$, où m est l'entier le plus proche de μ_{21}.
   b Si $\|\mathbf{b}_1\| \geq \|\mathbf{b}_2\|$, échanger $\mathbf{b}_1$ et $\mathbf{b}_2$
3. Renvoyer $\mathbf{b}_1$

Figure 6.1: **Algorithme Gauss (Vecteur le plus court en dimension 2).**

Intuitivement l'*orthogonalisation de Gram-Schmidt* de la base $\mathbf{b}_1, \cdots, \mathbf{b}_n$ donne les n "hauteurs" du parallélépipède défini par cette base. Formellement, il s'agit d'un ensemble de vecteurs 2 à 2 orthogonaux $\mathbf{b}_1^*, \cdots, \mathbf{b}_n^*$, tels que $\mathbf{b}_1^* = \mathbf{b}_1$ et $\mathbf{b}_i^*$ est la composante de $\mathbf{b}_i$ orthogonale à $\mathbf{b}_1^*, \ldots, \mathbf{b}_{i-1}^*$ pour $2 \leq i \leq n$. Le vecteur $\mathbf{b}_i^*$ s'obtient en soustrayant à $\mathbf{b}_i$ ses composantes selon les. directions de $\mathbf{b}_1^*, \ldots, \mathbf{b}_{i-1}^*$; nous avons. la relation de récurrence suivante:

$$\mathbf{b}_1^* = \mathbf{b}_1 \tag{6.1}$$

$$\mathbf{b}_i^* = \mathbf{b}_i - \sum_{j=1}^{i-1} \frac{\mathbf{b}_i \cdot \mathbf{b}_j^*}{\|\mathbf{b}_j^*\|^2} \mathbf{b}_j^* \quad i = 2, \ldots, n \tag{6.2}$$

Pour $1 \leq j < i \leq n$, posons:

$$\mu_{ij} = \frac{\mathbf{b}_i \cdot \mathbf{b}_j^*}{\|\mathbf{b}_j^*\|^2},$$

et $\mu_{ii} = 1$. Alors,

$$\mathbf{b}_i = \sum_{j=1}^{i} \mu_{ij} \mathbf{b}_j^*. \tag{6.3}$$

Pour $j \leq i$, nous noterons $\mathbf{b}_i(j)$ la composante de $\mathbf{b}_i$ orthogonale à $\mathbf{b}_1, \ldots, \mathbf{b}_{j-1}$, c'est-à-dire:

$$\mathbf{b}_i(j) = \mu_{ij} \mathbf{b}_j^* + \mu_{i,j+1} \mathbf{b}_{j+1}^* + \ldots + \mathbf{b}_i^*.$$

Il est facile de montrer que:

$$\det \mathcal{L} = \|\mathbf{b}_1^*\| \cdots \|\mathbf{b}_n^*\|.$$

Le défaut d'orthogonalité de la base peut donc se réécrire:

$$\frac{\|\mathbf{b}_1\| \cdots \|\mathbf{b}_n\|}{\|\mathbf{b}_1^*\| \cdots \|\mathbf{b}_n^*\|} = \frac{1}{\sin\theta_2 \cdots \sin\theta_n},$$

où θ_i est l'angle que forme $\mathbf{b}_i$ avec le sous-espace vectoriel engendré par $\mathbf{b}_1, \ldots, \mathbf{b}_{i-1}$, pour $2 \leq i \leq n$. Cet angle est défini ainsi: soit $\mathbf{b}_i'$ la projection de $\mathbf{b}_i$ sur le sous-espace engendré par $\mathbf{b}_1, \ldots, \mathbf{b}_{i-1}$, alors

$$\theta_i = \arccos\left(\frac{\|\mathbf{b}_i'\|}{\|\mathbf{b}_i\|}\right).$$

6.4 Algorithme en dimension n

Généraliser l'algorithme de réduction de base à n'importe quelle dimension a été un résultat important, mais les blocs de base sont simple. L'idée de base est plus ou moins prédictible. On utilise simplement la récursion et tout ce qu'on recherche est de réduire la dimension du problème. Cette dernière est atteint en prenant des projections orthogonales. On doit faire attention cependant afin d'éviter un temps de calcul exponentiel.

Supposons que l'on ait un base $b_1, b_2, \ldots, b_n$ à réduire. Définissons:

$$b_1^* = b_1, \tag{6.4}$$
$$b_i^* = b_i \text{ projection orthogonale sur } b_1, \ldots, b_{i-1}, 2 \leq i \leq n, \tag{6.5}$$
$$e_1^* = \text{vecteur unitaire dans la direction} b_i^*, \tag{6.6}$$
$$\beta_i = |b_i^*|. \tag{6.7}$$

On a calculé l'*orthogonalisation de Gram-Schmidt* et dans la base orthogonale (e_i^*), la base est la suivante:

$$b_1 = (\beta_1, 0, \ldots, 0), \tag{6.8}$$
$$b_2 = (\mu_{12}, \beta_2, 0, \ldots, 0), \tag{6.9}$$
$$\vdots \tag{6.10}$$
$$b_n = (\mu_{1n}, \mu_{2n}, \ldots, \mu_{(n-1)n}, \beta_n). \tag{6.11}$$

Le lemme suivant prouve l'importance des nombres β_i.

Lemma 32. *Pour tout vecteur $v \neq 0^n$ tel que $v \in L$, on a $\|v\| \geq \min_{i=1}^n \beta_i$.*

Démonstration. Supposons que $v = \sum_{i=1}^n a_i b_i$ avec a_i des entiers et soit i_0 la coordonnée la plus grande telle que $a_i \neq 0$. Alors, la coordonnée a_{i_0} de v dans la base (e_i^*) est $a_{i_0}\beta_{i_0}$ est donc

$$\|v\| \geq |a_{i_0}\beta_{i_0}| \geq \min_{i=1}^{n} \beta_i. \quad \square$$

Nous sommes prêt pour l'algorithme LLL qui est apparu la première fois dans un article de Lenstra, Lenstra et Lovász. Ce papier prouve un algorithme en temps polynomial pour factoriser des polynômes sur les entiers. La sous-routine pour trouver un vecteur court dans un réseau est dûe à Lovász seul. Á la vue du théorème précédent, et du fait que b_1 soit le vecteur le plus court, la clé de l'algorithme est de garantir qu'aucun β_i est beaucoup plus petit que β_1 qui est la longueur de b_1. Par conséquent, si β_{i+1}^2 est plus petit que $\frac{1}{2}\beta_i^2$ on peut échanger b_i et b_{i+1} afin de rendre β_i plus petit. De cette façon, on pousse les valeurs plus petites vers les indices les plus petits. L'algorithme est le suivant:

Avant d'analyser l'algorithme, décrivons en détail comment effectuer la première étape. La clé est l'ordre dans lequel satisfaire les conditions: on va garantir que $\mu_{(n-1)n}$ est petit en soustrayant un multiple entier de b_{n-1} à b_n. Ensuite, on va garantir que $\mu_{(n-2)(n-1)}$ et $\mu_{(n-2)n}$ en soustrayant un multiple entier convenable de b_{n-2} à b_{n-1} et b_n respectivement. On peut remarquer que cela ne va pas changer $\mu_{(n-1)n}$! On va ensuite prendre en compte $\mu_{(n-3)j}$ etc. Ce processus ressemble à l'élimination Gaussienne.

Notre analyse doit répondre aux 2 questions:

1. Est-ce que le résultat est bon, *i.e.* de combien le vecteur b_1 est-il plus long que le vecteur court à la terminaison de l'algorithme ?

2. Combien d'itérations sont nécessaires dans le pire des cas et combien de temps prend une itération ?

On répond à la première question par:

Lemma 33. *À la fin de l'algorithme, la longueur du vecteur b_1 est au plus $2^{(n-1)/2}$ fois la taille du vecteur court de L.*

Algorithme LLL
Entrée: une base et son orthogonalisation
Sortie: une base réduite

1. arranger la base telle que $|\mu_{ij}| \leq \frac{1}{2}\beta_i$,
2. **for** $1 \leq i \leq n-1$ et $2 \leq j \leq n$
3. **if** $\exists i : \beta_{i+1}^2 \leq \frac{1}{2}\beta_i^2$
4. échange b_i et b_{i+1} et **goto** 1

Figure 6.2:

Figure 6.3: **Algorithme LLL.**

Démonstration. La condition de terminaison donne:

$$\beta_1^2 \leq 2\beta_2^2 \leq \ldots \leq 2^{n-1}\beta_n^2,$$

et par le lemme 32, on a

$$|b_1| = \beta_1 \leq 2^{\frac{n-1}{2}} \min_{i=1}^{n} \beta_i \leq 2^{\frac{n-1}{2}} |\text{le vecteur court de L}|. \quad \square$$

Pour répondre à la deuxième question, analysons d'abord le temps nécessaire à une itération. L'étape la plus gourmande en temps est de rendre les μ_{ij} petit, ce qui est similaire à l'élimination Gaussienne et prend un temps $O(n^3)$. Ensuite, on borne le nombre d'itérations. Considérons un échange et notons b_i' la nouvelle valeur de b_i (et de façon similaire pour les autres valeurs). Supposons que l'on échange b_2 et b_3. Après l'échange, on a $\beta_2' = |b_2'^*| =$ la longueur de la partie de b_2' qui est orthogonale à b_1, mais $b_2' = b_3$, donc

$$\beta_2' = \sqrt{\beta_3^2 + \mu_{23}^2} \leq \sqrt{\frac{1}{2}\beta_2^2 + \frac{1}{4}\beta_2^2} = \sqrt{\frac{3}{4}}\beta_2.$$

Maintenant β_4 qui est la partie de b_4 qui est orthogonale à b_1, b_2 et b_3. Comme cet ensemble de vecteurs ne change pas quand on échange b_2 et b_3, β_4 reste inchangé et pour $j \geq 4$, on a $\beta_j' = \beta_j$ et comme $\det(L) = \prod_{i=1}^n \beta_i = \prod_{i=1}^n \beta_i'$, on a:

$$\beta_3' = \frac{\beta_2\beta_3}{\beta_2'} \geq \sqrt{\frac{4}{3}}\beta_3.$$

Donc, on conclut qu'un échange à i va modifier seulement β_i et β_{i+1}, parmi lesquels le premier diminue et le second augmente. De plus, on a minoré le taux de changement. Examinons comment un échange affecte le produit $B = \prod_{j=1}^n \beta_j^{n-j}$ (appelé le potentiel). La partie intéressante est

$$\beta_i^{n-i}\beta_{i+1}^{n-i-1} = \beta_i \underbrace{(\beta_i\beta_{i+1})^{n-i-1}}_{\text{inchange}},$$

et donc B décroît par le même facteur comme un β_i particulier à chaque itération.

Si la longueur du plus long vecteur a une longueur D initialement, alors $\beta_j \leq D$, ce qui implique qu'au départ:

$$B \leq \prod_{j=1}^{n} D^{n-j} = D^{\frac{n(n-1)}{2}},$$

et à la fin $B \geq 1$ car

$$\beta_1 \geq 1 (\text{longueur} de b_1) \tag{6.12}$$

$$\beta_1 \beta_2 \geq 1 (\det \left(\begin{pmatrix} b_1 \\ b_2 \end{pmatrix} (b_1^T b_2^T) \right) = \beta_1^2 \beta_2^2, \text{un entier}) \vdots \tag{6.13}$$

$$\beta_1 \beta_2 \ldots \beta_j \geq 1 \tag{6.14}$$

$$\vdots \tag{6.15}$$

$$\beta_1 \beta_2 \ldots \beta_n = \det(L) \geq 1, \tag{6.16}$$

et B est le produit de ces nombres.

Ainsi, on peut voir que le nombre d'itérations est $O(n^2 \log D)$ et que le temps de calcul total de l'algorithme est $O(n^5 \log D)$ opérations sur les nombres. Pour terminer l'analyse, on devrait prendre en compte la précision nécessaire pendant les calculs. Ceci est très technique et on omet ces détails. En pratique cependant, il faut faire très attention et on doit au moins doubler la précision en grande dimension. On termine en énonçant le théorème:

Théorème 61. *Étant donnée une base d'un réseau en dimension n où chaque vecteur de la base a une longueur au plus D, l'algorithme LLL trouve un vecteur dans L qui est au plus $2^{(n-1)/2}$ fois plus long que le vecteur court. L'algorithme s'exécute en temps $O(n^5 \log D)$ opérations sur les nombres.*