Arithmétique
M1 Mathématiques Fondamentales
Université Paris-Saclay

Benjamin Schraen

Année 2021-2022

Table des matières

Chapitre 1

Divisibilité et congruences

1.1 Divisibilité dans l'anneau des entiers

On note $\mathbb{Z}$ l'anneau des entiers relatifs. Si $a \in \mathbb{Z}$ et si $b \in \mathbb{Z} \smallsetminus \{0\}$, on dit que b *divise* a et on note $b \mid a$ s'il existe $c \in \mathbb{Z}$ tel que $a = bc$.

1.1.1 Le PGCD

Proposition (Division euclidienne)**.** *Soit $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$. Il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que $a = bq + r$ et $r < b$. En particulier $b \mid a$ si et seulement si $r = 0$.*

Cette proposition implique que l'anneau $\mathbb{Z}$ est euclidien. C'est en particulier un anneau principal. Pour la commodité du lecteur nous le redémontrons.

Théorème 1.1. *L'anneau $\mathbb{Z}$ est principal. Cela signifie qu'il est intègre et que tous ses idéaux sont de la forme $\mathbb{Z}c$.*

Démonstration. Soit $I \subset \mathbb{Z}$ un idéal. Supposons $I \neq 0$ et soit $b \in I$ le plus petit élément de $I \cap \mathbb{N}^*$. Si $a \in I$, on effectue la division euclidienne de a par b, on a donc $a = bq + r$ avec $0 \leqslant r < b$. Comme a et b sont dans I, on a également $r \in I$. Par définition de b, on a nécessairement $r = 0$ et donc $a \in \mathbb{Z}b$. Ceci prouve que $I \subset \mathbb{Z}b$, l'inclusion réciproque est immédiate. Ainsi $I = \mathbb{Z}b$. □

Rappelons que deux éléments a et b d'un anneau commutatif et intègre A sont dits *associés* s'il existe un élément inversible $c \in A^\times$ tel que $a = bc$. Deux éléments sont associés si et seulement si ils engendrent le même idéal.

Comme le groupe des inversibles de $\mathbb{Z}$ est l'ensemble $\{\pm 1\}$, on a $\mathbb{Z}a = \mathbb{Z}b$ si et seulement si $a = \pm b$ et tout idéal de $\mathbb{Z}$ est engendré par un unique élément de $\mathbb{N}$.

Définition. *Soit $k \geqslant 1$ un entier et soient $a_1, \ldots, a_k$ des entiers relatifs. Le* plus grand commun diviseur*, aussi nommé pgcd, de $a_1, \ldots, a_k$ est l'unique entier naturel $a_1 \wedge \cdots \wedge a_k$ tel que*

$$\mathbb{Z}(a_1 \wedge \cdots \wedge a_k) = \mathbb{Z}a_1 + \cdots + \mathbb{Z}a_k.$$

Remarque. a) Sauf si $a = b = 0$, l'entier $a \wedge b$ est le plus grand entier divisant a et b. En effet, si d divise à la fois a et b, on a $\mathbb{Z}a \subset \mathbb{Z}d$ et $\mathbb{Z}b \subset \mathbb{Z}d$, donc $\mathbb{Z}(a \wedge b) \subset \mathbb{Z}d$ et d divise $a \wedge b$. On en conclut que

$$d \leqslant |a \wedge b| = a \wedge b.$$

b) Si $a_1, \ldots, a_k$ sont des entiers et si $1 \leqslant \ell \leqslant k$, on a

$$\mathbb{Z}a_1 + \cdots + \mathbb{Z}a_k = (\mathbb{Z}a_1 + \cdots + \mathbb{Z}a_\ell) + \mathbb{Z}a_{\ell+1} + \cdots + \mathbb{Z}a_k$$

de sorte que

$$a_1 \wedge \cdots \wedge a_k = (a_1 \wedge \cdots \wedge a_\ell) \wedge a_{\ell+1} \wedge \cdots \wedge a_k.$$

On peut donc calculer le pgcd de k entiers par dévissage si l'on sait calculer le pgcd de deux entiers quelconques.

c) Si $(a, b) \in \mathbb{Z}^2$, on a $1 \wedge a = 1$, $0 \wedge a = |a|$ et, si $k \in \mathbb{Z}$, $(ka) \wedge (kb) = |k|(a \wedge b)$. Si $(a, b, c) \in \mathbb{Z}^3$, on a

$$a \wedge (bc) \mid (a \wedge b)(a \wedge c)$$

comme il se déduit de l'inclusion

$$(\mathbb{Z}a + \mathbb{Z}b)(\mathbb{Z}a + \mathbb{Z}c) \subset \mathbb{Z}a + \mathbb{Z}(bc).$$

L'algorithme d'Euclide permet de déterminer le pgcd de deux entiers a et b. Supposons que a et b sont dans $\mathbb{N}^*$. Quitte à échanger les rôles de a et b, on peut supposer que $a \geqslant b$. On définit alors deux suites $(a_n)_{n\geqslant 0}$ et $(b_n)_{n\geqslant 0}$ par récurrence en posant $a_0 = a$, $b_0 = b$. Si $b_n = 0$, on s'arrête, et si $b_n \neq 0$, on définit a_{n+1} et b_{n+1} en effectuant la division euclidienne de a_n par b_n :

$$a_n = q_n b_n + r_n, \quad 0 \leqslant r_n < b_n.$$

On pose alors $a_{n+1} = b_n$ et $b_{n+1} = r_n$. Comme $a_n \wedge b_n = b_n \wedge r_n$, la suite $(a_n \wedge b_n)_{n\geqslant 0}$ est constante. Comme de plus la suite (b_n) est strictement décroissante, on obtient $b_n = 0$ pour une certaine valeur de b. Le pgcd de a et b est alors le dernier terme b_n non nul.

Exemple. Pour calculer le pgcd de 31467 et 2047, on procède comme suit :

$$\begin{array}{cccc}
a_0 = 31467 & b_0 = 2047 & q_0 = 15 & r_0 = 762 \\
a_1 = 2047 & b_1 = 762 & q_1 = 2 & r_1 = 523 \\
a_2 = 762 & b_2 = 523 & q_2 = 1 & r_2 = 239 \\
a_3 = 523 & b_3 = 239 & q_3 = 2 & r_3 = 45 \\
a_4 = 239 & b_4 = 45 & q_4 = 5 & r_4 = 14 \\
a_5 = 45 & b_5 = 14 & q_5 = 3 & r_5 = 3 \\
a_6 = 14 & b_6 = 3 & q_6 = 4 & r_6 = 2 \\
a_7 = 3 & b_7 = 2 & q_7 = 1 & r_7 = 1.
\end{array}$$

Ainsi $31467 \wedge 2047 = 1$.

1.1.2 Coprimalité

Deux entiers a et b sont dit *premiers entre eux* si leur pgcd vaut 1. Des entiers $a_1, \ldots, a_k$ sont dits *premiers entre eux dans leur ensemble* si $a_1 \wedge a_2 \wedge \cdots \wedge a_k = 1$. Les entier $a_1, \cdots, a_k$ sont dits *premiers entre eux deux à deux* si $a_i \wedge a_j = 1$ pour tous $1 \leqslant i \neq j \leqslant k$.

Remarque. a) Une famille d'entiers premiers entre eux deux à deux forme une famille d'entiers premiers entre eux dans leur ensemble. La réciproque est fausse comme le montre l'exemple de la famille d'entiers $6, 10, 15$.

b) Si $d = a_1 \wedge \cdots \wedge a_k$ est non nul, alors les entiers $\frac{a_1}{d}, \cdots, \frac{a_k}{d}$ sont premiers entre eux dans leur ensemble.

Théorème 1.2. *Soient a, b, c des entiers. Si $a \mid (bc)$ et si a et b sont premiers entre eux, alors $a \mid c$.*

Démonstration. Comme $a \wedge b = 1$, il existe $(\lambda, \mu) \in \mathbb{Z}^2$ tel que $a\lambda + b\mu = 1$. En multipliant cette égalité par c, on obtient $c = (ac)\lambda + (bc)\mu$. Comme a divise ac et bc, on a $a \mid c$. □

Corollaire. *Si $b \mid a$ et si $c \mid a$ et si $b \wedge c = 1$, alors $(bc) \mid a$. Plus généralement si $b_1, \ldots, b_k$ sont des diviseurs de a premiers entre eux deux à deux, alors*

$$\prod_{i=1}^{k} b_i \mid a.$$

Démonstration. On a $a = bk$ pour un entier $k \in \mathbb{Z}$. Comme $c \mid bk$ et $b \wedge c = 1$, le théorème 1.2 implique que c divise k, donc bc divise a. Le deuxième énoncé s'en déduit par récurrence sur k. □

1.1.3 Un premier cas d'équation diophantienne

On cherche à résoudre le problème suivant : on se donne des entiers relatifs $a_1, \ldots, a_k, n$. On cherche alors à déterminer explicitement les éléments de l'ensemble

$$\{(x_1, \ldots, x_n) \in \mathbb{Z}^n \mid a_1x_1 + \cdots + a_kx_k = n\}. \tag{1.1}$$

Pour que cet ensemble soit non vide, une condition nécessaire et suffisante est que

$$n \in \mathbb{Z}a_1 + \cdots + \mathbb{Z}a_k = \mathbb{Z}(a_1 \wedge \cdots \wedge a_k),$$

c'est-à-dire que $a_1 \wedge \cdots \wedge a_k \mid n$.

On peut donc supposer que $\delta = a_1 \wedge \cdots \wedge a_k$ divise n et on remarque que, pour $(x_1, \ldots, x_k) \in \mathbb{Z}^k$,

$$a_1x_1 + \cdots + a_kx_k = n \Leftrightarrow \left(\frac{a_1}{\delta}\right) x_1 + \cdots + \left(\frac{a_k}{\delta}\right) x_k = \left(\frac{n}{\delta}\right).$$

On sait donc déterminer l'ensemble (1.1) dans le cas général si on sait le déterminer dans le cas où $\delta = 1$.

Si $k = 1$, la solution est évidente. Nous allons montrer qu'il est possible de déterminer (1.1) par récurrence sur k. Supposons donc que l'on sache résoudre le problème pour $k-1$ entiers. Supposons de plus que $\delta = 1$. On suppose de plus que tous les entier a_i sont non nuls car dans le cas contraire on est ramené au problème à $k-1$ inconnues.

Supposons dans un premier temps que l'on connaisse déjà un élément $(\lambda_1, \ldots, \lambda_k)$ de l'ensemble (1.1). Si $(x_1, \ldots, x_k)$ est un autre élément de (1.1), alors

$$a(x_1 - \lambda_1) + \cdots + a_k(x_k - \lambda_k) = 0.$$

Posons alors $\delta_1 = a_2 \wedge \cdots \wedge a_k \neq 0$. Alors $a_1 \wedge \delta_1 = 1$, et on peut écrire

$$a_2(x_2 - \lambda_2) + \cdots + a_k(x_k - \lambda_k) = \delta_1 X_1$$

pour un entier $X_1 \in \mathbb{Z}$. On a donc $a_1(x_1 - \lambda_1) + \delta_1 X_1 = 0$ et on déduit du théorème 1.2 que $\delta_1 \mid (x_1 - \lambda_1)$ et donc $x_1 = \lambda_1 + \delta_1\lambda$ pour un certain $\lambda \in \mathbb{Z}$. On a alors $X_1 = -\lambda a_1$. Pour tout entier $\lambda \in \mathbb{Z}$, l'équation $a_2y_2 + \cdots + a_ky_k = -\lambda a_1\delta_1$ a des solutions dans $\mathbb{Z}^{k-1}$ que l'on sait déterminer explicitement par récurrence, on sait déterminer explicitement l'ensemble (1.1).

Il reste donc à déterminer explicitement au moins une solution de l'équation

$$a_1x_1 + \cdots + a_kx_k = n$$

lorsque $a_1 \wedge \cdots \wedge a_k \mid n$. On procède encore par récurrence sur k. On se ramène facilement au cas où $\delta = n = 1$.

Commençons par traiter le cas où $k = 2$, c'est-à-dire le problème de trouver deux entiers x et y tels que $ax + by = 1$ si a et b sont deux entiers relatifs fixés vérifiant $a \wedge b = 1$. On se ramène au cas où $b > 0$ et on applique l'algorithme d'Euclide pour construire des suites (a_i), (b_i), (q_i) et (r_i) telles que

$$a_0 = a, b_0 = b, a_i = b_iq_i + r_i, 0 \leqslant r_i < b_i, a_{i+1} = b_i, b_{i+1} = r_i.$$

Il existe un indice ℓ tel que $r_\ell = 1$. On « remonte » alors l'algorithme d'Euclide de la façon suivante :

$$\begin{aligned} 1 &= a_\ell - b_\ell q_\ell = b_{\ell-1} - b_\ell q_\ell = b_{\ell-1} - r_{\ell-1}q_\ell \\ &= b_{\ell-1} - (a_{\ell-1} - q_{\ell-1}b_{\ell-1})q_\ell = -a_{\ell-1}q_\ell + b_{\ell-1}(1 + q_{\ell-1}q_\ell) \\ &= \cdots \\ &= a_0x + b_0y. \end{aligned}$$

Cet algorithme est parfois appelé *algorithme d'Euclide étendu.*

Exemple. En appliquant l'algorithme d'Euclide à la paire $(67, 59)$, on obtient

$$\begin{array}{cccc} a_0 = 67 & b_0 = 59 & q_0 = 1 & r_0 = 8 \\ a_1 = 59 & b_1 = 8 & q_1 = 7 & r_1 = 3 \\ a_2 = 8 & b_2 = 3 & q_2 = 2 & r_2 = 2 \\ a_3 = 3 & b_3 = 2 & q_3 = 1 & r_3 = 1. \end{array}$$

On a donc

$$\begin{aligned} 1 &= 3 - 2 \\ &= 3 - (8 - 3 \cdot 2) = -8 + 3 \cdot 3 \\ &= -8 + (59 - 8 \cdot 7) \cdot 3 = 59 \cdot 3 - 8 \cdot 22 \\ &= 59 \cdot 3 - (67 - 59) \cdot 22 = -67 \cdot 22 + 59 \cdot 25. \end{aligned}$$

Le couple $(-22, 25)$ est donc solution de l'équation $67x + 59y = 1$.

Dans le cas général, on pose $\delta_1 = a_2 \wedge \cdots \wedge a_k$. On commence par rechercher une solution à l'équation $a_1 x + \delta_1 y = 1$ puis, par récurrence à l'équation

$$\delta_1 y = a_2 x_2 + \cdots + a_k x_k.$$

1.1.4 Nombres premiers

Si $a \in \mathbb{Z}$ et si p est un nombre premier, alors a et p sont premiers entre eux si et seulement si p ne divise pas a. En effet $a \wedge p$ est un diviseur de p, il est donc égal à 1 ou p.

Proposition. *Si p est premier et si $p \mid ab$, alors $p \mid a$ ou $p \mid b$. En particulier si $p \mid a^n$, alors $p \mid a$.*

Corollaire. *Si p et q sont deux nombres premiers distincts, alors pour tous $m \geqslant 1$ et $n \geqslant 1$, les entiers p^m et q^n sont premiers entre eux.*

Théorème 1.3. *Tout entier naturel $n \geqslant 1$ s'écrit de façon unique, à l'ordre près, comme produit de nombres premiers.*

Démonstration. La preuve se fait par récurrence sur $n \geqslant 1$.

Si $n = 1$, le résultat est vrai car 1 est égal au produit indexé par l'ensemble vide.

Supposons $n \geqslant 2$ et le théorème vrai pour tout entier $1 \leqslant m < n$.

Si n est premier, alors n est un produit de nombres premiers et ce d'une seule façon, par définition même d'un nombre premier.

Si n n'est pas premier, alors $n = ab$ avec des entiers $1 < a, b < n$. Par récurrence, a et b sont des produits de nombres premiers, donc n également. Montrons l'unicité de la décomposition de n en produit de nombres premires. Supposons donc que

$$n = p_1^{\alpha_1} \cdots p_r^{\alpha_r} = q_1^{\beta_1} \cdots q_s^{\beta_s}$$

où $p_1 < \cdots < p_r$ et $q_1 < \cdots < q_s$ sont des nombres premiers et $\alpha_i \geqslant 1$, $\beta_j \geqslant 1$ des entiers. On a $p_1 \mid n$. Il existe donc $1 \leqslant j \leqslant s$ tel que $p_1 \mid q_j$. Comme q_j est premier, on a $p_1 = q_j$. Ainsi $p_1 \geqslant q_1$. De façon symétrique, on montre que $q_1 \geqslant p_1$ et donc que $p_1 = q_1$. Comme $p_1 \neq q_j$ pour $j > 1$, on a $p_1^{\alpha_1} \wedge q_j^{\beta_j}$ pour $j > 1$ et donc, puisque $p_1^{\alpha_1} \mid n$, $p_1^{\alpha_1} \mid q_1^{\beta_1} = p_1^{\beta_1}$, ce qui implique $\alpha_1 \leqslant \beta_1$. De façon symétrique, $\beta_1 \leqslant \alpha_1$ et donc $\alpha_1 = \beta_1$. On en déduit que

$$p_2^{\alpha_1} \cdots p_r^{\alpha_r} = q_2^{\beta_2} \cdots q_s^{\alpha_s} < n.$$

Par récurrence, on en déduit que $r = s$, $p_i = q_i$ et $\alpha_i = \beta_i$ pour $i > 1$. □

1.2 Les anneaux $\mathbb{Z}/n\mathbb{Z}$

1.2.1 Rappels sur $\mathbb{Z}/n\mathbb{Z}$

Pour $n \geqslant 1$ entier, l'anneau $\mathbb{Z}/n\mathbb{Z}$ est l'anneau quotient de l'anneau $\mathbb{Z}$ par l'idéal $\mathbb{Z}n$. C'est donc un anneau commutatif. Notons $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ l'application quotient et $\overline{m}$ pour $\pi(m)$ si $m \in \mathbb{Z}$. Lorsque l'on veut insister sur la dépendance en n, on utilise aussi la notation $\overline{m}_n$ pour $\pi(m)$. La division euclidienne permet de remarquer que

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \ldots, \overline{n-1}\} \text{ et } \operatorname{Card}(\mathbb{Z}/n\mathbb{Z}) = n.$$

Proposition. *Soit $n \in \mathbb{N}^*$. Si $m \in \mathbb{Z}$, on a $\overline{m} \in (\mathbb{Z}/n\mathbb{Z})^\times$ si et seulement si $m \wedge n = 1$.*

Démonstration. On a en effet

$$\begin{aligned} m \wedge n = 1 &\Leftrightarrow \exists (a,b) \in \mathbb{Z}^2, \quad am + bn = 1 \\ &\Leftrightarrow \exists \overline{a} \in \mathbb{Z}/n\mathbb{Z}, \quad \overline{am} = \overline{1}. \end{aligned}$$

□

Proposition. *Soit $n \geqslant 1$ un entier. Les assertions suivantes sont équivalentes :*

(i) n est premier ;

(ii) l'anneau $\mathbb{Z}/n\mathbb{Z}$ est intègre ;

(iii) l'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps.

Démonstration. L'anneau $\mathbb{Z}/n\mathbb{Z}$ est fini. C'est donc un corps si et seulement si il est intègre. Par ailleurs, l'anneau $\mathbb{Z}/n\mathbb{Z}$ est intègre si et seulement si pour tous x et y dans $\mathbb{Z}/n\mathbb{Z}$, $xy = \overline{0}$ implique $x = \overline{0}$ ou $y = \overline{0}$, c'est-à-dire si et seulement si, pour tous $a, b \in \mathbb{Z}$, $n \mid ab$ implique $n \mid a$ ou $n \mid b$. Cette dernière assertion est bien équivalente au fait que n est premier si $n \neq 1$. Remarquons au passage que $\mathbb{Z}/n\mathbb{Z}$ est l'anneau nul si et seulement si $n = 1$ et que l'anneau nul n'est pas intègre. □

On note φ la *fonction indicatrice d'Euler* définie sur $\mathbb{N}^*$ par

$$\varphi(n) = \begin{cases} \operatorname{Card}(\mathbb{Z}/n\mathbb{Z})^\times = \operatorname{Card}\{1 \leqslant m \leqslant n \mid m \wedge n = 1\} & \text{si } n \geqslant 2 \\ 1 & \text{si } n = 1. \end{cases}$$

Exemple. Si p est un nombre premier, on a $\varphi(p) = 1$ et, si $k \geqslant 1$ $\varphi(p^k) = p^k - p^{k-1} = p^k(1 - \frac{1}{p})$.

1.2.2 Le théorème des restes (ou théorème chinois)

Théorème 1.4. *Soient m et n deux éléments de $\mathbb{N}^*$ premiers entre eux. L'application*

$$\begin{array}{ccc} \mathbb{Z}/mn\mathbb{Z} & \xrightarrow{\psi} & (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}) \\ \overline{a}_{mn} & \longmapsto & (\overline{a}_m, \overline{a}_n) \end{array}$$

est un isomorphisme d'anneaux.

Démonstration. L'application ψ est bien définie et c'est un morphisme d'anneaux. Comme les ensembles de départ et d'arrivée ont le même cardinal, il suffit de prouver que ψ est une application injective. Comme ψ est en particulier un morphisme de groupes additifs, il suffit de prouver que $\mathrm{Ker}(\psi) = \{\overline{0}_{mn}\}$. On a en effet, pour $a \in \mathbb{Z}$,

$$\overline{a}_{mn} \in \mathrm{Ker}(\psi) \Leftrightarrow m \mid a \text{ et } n \mid a \Leftrightarrow mn \mid a \Leftrightarrow \overline{a}_{mn} = \overline{0}_{mn}. \qquad \square$$

Remarque. Il peut être utile de savoir calculer l'application ψ^{-1} explicitement. Si $(a, b) \in \mathbb{Z}^2$, déterminer $\psi^{-1}(\overline{a}_m, \overline{a}_n)$ revient à déterminer un entier $k \in \mathbb{Z}$ tel que $\begin{cases} k \equiv a\,[m] \\ k \equiv b\,[n] \end{cases}$. On a en effet $\psi^{-1}((\overline{a}_m, \overline{b}_n)) = \overline{k}_{mn}$. On commence par chercher $(\alpha, \beta) \in \mathbb{Z}^2$ tel que

$$\begin{cases} \alpha \equiv 1\,[m] \\ \alpha \equiv 0\,[n] \end{cases} \qquad \begin{cases} \beta \equiv 0\,[m] \\ \beta \equiv 1\,[n] \end{cases} .$$

On pose alors $k = a\alpha + b\beta$. Pour trouver α et β il suffit de déterminer $(x, y) \in \mathbb{Z}^2$ tel que $mx + ny = 1$ en utilisant l'algorithme d'Euclide étendu. On peut alors prendre $\alpha = ny$ et $\beta = mx$.

Corollaire. *Soit $n \in \mathbb{N}^*$ tel que $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ avec $p_1 < \cdots < p_r$ premiers. On a alors un isomorphisme d'anneaux*

$$\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{\alpha_r}\mathbb{Z}.$$

Corollaire. *Soit $n \in \mathbb{N}^*$ tel que $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ avec $p_1 < \cdots < p_r$ premiers. Alors*

$$\varphi(n) = \varphi(p_1^{\alpha_1}) \cdots \varphi(p_r^{\alpha_r}).$$

1.3 Polynômes

1.3.1 Rappels

Soit A un anneau commutatif. On note $A[X]$ l'anneau des polynômes en une indéterminée à coefficients dans A. Si $P \in A[X]$ et $Q \in A[X] \setminus \{0\}$, on dit que Q *divise* P, et on note $Q \mid P$, s'il existe $R \in A[X]$ tel que $P = QR$.

Proposition (Division euclidienne pour les polynômes)**.** *Soit $P \in A[X]$ et soit $Q \in A[X] \setminus \{0\}$ de coefficient dominant inversible. Alors il existe un unique couple $(R, S) \in A[X]^2$ tel que $\deg R < \deg Q$ et $A = QR + S$.*

Démonstration. Commençons par prouver l'existence de (R, S). Remarquons déjà que si $\deg(P) < \deg(Q)$, alors on peut prendre $R = 0$ et $S = P$.

Raisonnons alors par récurrence généralisée sur le degré de P. Si $\deg(P) = -\infty$, on est dans le cas où $\deg(P) < \deg(Q)$ qui a déjà été traité.

Supposons donc l'existence de la division euclidienne de P par Q prouvée pour tout polynôme P de degré $\leqslant N$. Soit P un polynôme de degré $N+1$. Le cas où $\deg(P) < \deg(Q)$ a déjà été vu, on peut donc supposer de plus que $\deg(P) \geqslant \deg(Q)$. Notons $n = \deg(Q)$, p_{N+1} le coefficient dominant de P et q_n le coefficient dominant de Q. Comme $q_n \in A^\times$, on peut poser

$$P_1 = P - p_{N+1} d_n^{-1} X^{N+1-n} Q.$$

Le polynôme $p_{N+1} q_n^{-1} X^{N+1-n} q$ est de degré $N+1$ et de coefficient dominant p_{N+1}, on en conclut que P et $p_{N+1} q_n^{-1} X^{N+1-n} Q$ ont même degré $N+1$ et mêmes coefficients dominants, donc que leur différence P_1 est de degré $\leqslant N$. Par récurrence, il existe $(R_1, S_1) \in K[X]^2$ tel que $P_1 = R_1 Q + S_1$ et $\deg(S_1) < \deg(Q)$. On peut donc écrire

$$P = P_1 + p_{N+1} q_n^{-1} X^{N+1-n} Q = R_1 D + S_1 + p_{N+1} q_n^{-1} X^{N+1-n} Q = (R_1 + p_{N+1} q_n^{-1} X^{N+1-n}) Q + S_1.$$

On peut donc prendre $R = R_1 + p_{N+1} q_n^{-1} X^{N+1-n}$ et $S = S_1$.

Montrons à présent l'unicité de la division euclidienne. Supposons qu'il existe des couples (R_1, S_1) et $(R2, S_2)$ tels que

$$P = R_1 Q + S_1 = R_2 Q + S_2$$

et $\deg(S_1), \deg(S_2) < \deg(Q)$. On a alors

$$S_1 - S_2 = (R_2 - R_1) Q.$$

Supposons par l'absurde que $R_2 - R_1 \neq 0$. On a alors, puisque Q est de coefficient dominant inversible,

$$\deg(S_1 - S_2) = \deg(Q) + \deg(R_2 - R_1) \geqslant \deg(Q).$$

Comme par ailleurs $\deg(S_1 - S_2) < \deg(Q)$, on aboutit à une contradiction. On en conclut que $R_2 = R_1$ et donc que $S_1 = S_2$. □

Dans le cas particulier où l'anneau A est un corps K, la condition sur Q est équivalente à $Q \neq 0$. On en déduit que l'anneau $K[X]$ est euclidien. Il est en particulier principal et factoriel. On en déduit, comme dans la cas de l'anneau $\mathbb{Z}$,

Théorème 1.5. *Si K est un corps commutatif, tout polynôme unitaire $P \in K[X]$ s'écrit de façon unique à l'ordre près comme un produit de polynôme irréductibles et unitaires.*

Exemple. Dans $\mathbb{R}[X]$, on a

$$X^4 + 1 = (X^2 + \sqrt{2}X + 1)(X^2 - \sqrt{2}X + 1).$$

Dans $\mathbb{Q}[X]$, on a

$$X^4 - 1 = (X^2 + 1)(X - 1)(X + 1).$$

Remarque. Si K est un corps fini et si $P \in K[X] \setminus \{0\}$, l'anneau $K[X]/(P)$ est un anneau fini. Ces anneaux ont des propriétés fort similaires à celles des anneaux $\mathbb{Z}/n\mathbb{Z}$. Il existe effectivement une arithmétique dans $K[X]$ parallèle à celle que nous allons étudier dans ce cours.

1.3.2 Polynômes à coefficients entiers

L'anneau $\mathbb{Z}[X]$ n'est pas un anneau principal. On peut en effet montrer que l'idéal engendré par 2 et X n'est pas principal. En effet supposons qu'il existe un polynôme $P \in \mathbb{Z}[X]$ tel que $P\mathbb{Z}[X] = 2\mathbb{Z}[X] + X\mathbb{Z}[X]$. Alors $P \mid 2$ donc P est de degré 0. Comme $P \mid X$, on a $P = \pm 1$. Cependant les éléments Q de $2\mathbb{Z}[X] + X\mathbb{Z}[X]$ vérifient tous $2 \mid Q(0)$. L'idéal engendré par 2 et X n'est pas principal.

Le résultat suivant montre que les racines rationnelles d'un polynôme de $\mathbb{Z}[X]$ sont faciles à déterminer.

Théorème 1.6. *Soit $P = \sum_{i=0}^{\deg(P)} a_i X^i \in \mathbb{Z}[X] \setminus \{0\}$. Si $x = \frac{p}{q} \in \mathbb{Q}$ est une racine de P, avec $p \wedge q = 1$, alors $p \mid a_0$ et $q \mid a_{\deg(P)}$.*

Démonstration. On a

$$P\left(\frac{p}{q}\right) = 0 \Leftrightarrow a_{\deg(P)} p^{\deg(P)} + a_{\deg(P)-1} p^{\deg(P)-1} q + \cdots + a_0 q^{\deg(P)} = 0.$$

Ainsi $p \mid a_0 q^{\deg(P)}$ et, comme $p \wedge q = 1$, on a $p \wedge q^{\deg(P)} = 1$ donc $p \mid a_0$. On montre de même que $q \mid q_{\deg(P)} p^{\deg(P)}$ et donc que $q \mid a_{\deg(P)}$. □

Soit $n \geqslant 1$ un entier. On définit un morphisme surjectif d'anneaux en posant

$$\begin{array}{ccc} \mathbb{Z}[X] & \longrightarrow & \mathbb{Z}/n\mathbb{Z}[X] \\ P = \sum_{i=0}^{d} a_i X^i & \longmapsto & \overline{P} = \sum_{i=0}^{d} \overline{a_i} X^i. \end{array}$$

Son noyau est l'idéal $\{\sum_{i=0}^{d} a_i X^i \mid \forall i \geqslant 0,\ n \mid a_i\}$ qui est aussi l'idéal principal engendré par l'entier n (vu comme polynôme constant).

Définition. *Soit $P = \sum_{i=0}^{\deg(P)} a_i X^i \in \mathbb{Z}[X]$. On définit le* contenu *du polynôme P comme le pgcd de ses coefficients. On le note $c(P)$. On dit que le polynôme P est* primitif *si $c(P) = 1$.*

Si $n \in \mathbb{N}^*$ et $P \in \mathbb{Z}[X]$, on a donc $n \mid c(P)$ si et seulement si $P \equiv 0\,[n]$.

Lemme. *Pour P, Q deux éléments de $\mathbb{Z}[X]$, on a $c(PQ) = c(P)c(Q)$.*

Démonstration. Si $k \in \mathbb{Z}$ et $P \in \mathbb{Z}[X]$, on a $c(kP) = |k|c(P)$. On peut donc se ramener facilement au cas où $c(P) = c(Q) = 1$. Supposons par l'absurde que $c(PQ) \neq 1$. Ceci implique qu'il existe un nombre premier p tel que $p \mid c(PQ)$ et donc tel que $\overline{PQ} = 0$ dans $\mathbb{Z}/p\mathbb{Z}[X]$. Comme $\overline{PQ} = \overline{P} \cdot \overline{Q}$, on a $\overline{P} \cdot \overline{Q} = 0$ dans $\mathbb{Z}/p\mathbb{Z}[X]$. Comme $\mathbb{Z}/p\mathbb{Z}$ est un corps, l'anneau des polynômes $\mathbb{Z}/p\mathbb{Z}[X]$ est un anneau intègre. On a donc $\overline{P} = 0$ ou $\overline{Q} = 0$, c'est-à-dire $p \mid c(P)$ ou $p \mid c(Q)$, ce qui est absurde. □

Définition. *Soit A un anneau. Un élément x de A est dit* irréductible *si x n'est pas inversible et si $x = ab$ avec $a, b \in A$ implique $a \in A^\times$ ou $b \in A^\times$.*

Proposition. *Soit $P \in \mathbb{Z}[X]$. Supposons que $P = QR$ dans l'anneau $\mathbb{Q}[X]$. Il existe alors des nombres rationnels $\alpha, \beta \in \mathbb{Q}^\times$ tels que $\alpha\beta = 1$ et $\alpha Q \in \mathbb{Z}[X]$, $\beta R \in \mathbb{Z}[X]$.*

Démonstration. On peut supposer $P \neq 0$. Dans le cas contraire, le résultat est facile. Comme Q et R sont dans $\mathbb{Q}[X]$, il existe $d_1, d_2 \in \mathbb{N}^*$ tels que $d_1 Q \in \mathbb{Z}[X]$ et $d_2 R \in \mathbb{Z}[X]$. On a alors $d_1 d_2 P \in \mathbb{Z}[X]$. On a de plus $c(d_1 d_2 P) = d_1 d_2 c(P)$ et $c(d_1 d_2 P) = c(d_1 Q)c(d_2 R)$. Posons alors $\alpha = \frac{d_1}{c(d_1 Q)}$ et $\beta = \frac{d_2 c(P)}{c(d_2 R)}$. On a bien, par définition de $c(d_1 Q)$ et $c(d_2 R)$, $\alpha Q \in \mathbb{Z}[X]$ et $\beta R \in \mathbb{Z}[X]$. De plus $\alpha\beta = \frac{d_1 d_2 c(P)}{c(d_1 Q)c(d_2 R)} = 1$. □

Théorème 1.7. *Soit $P \in \mathbb{Z}[X]$ un polynôme primitif. Pour que P soit irréductible dans $\mathbb{Z}[X]$, il faut et il suffit que P soit irréductible dans $\mathbb{Q}[X]$.*

Démonstration. Supposons que P est réductible dans $\mathbb{Z}[X]$. On peut donc écrire $P = QR$ avec $Q \notin \mathbb{Z}[X]^\times$ et $R \notin \mathbb{Z}[X]^\times$. Comme $c(P) = 1$ et que $c(P) = c(Q)c(R)$, on en déduit que $c(Q) = c(R) = 1$. Les polynômes Q et R, n'étant pas inversibles, ne peuvent être constants. On a donc $Q \notin \mathbb{Q}[X]^\times$ et $R \notin \mathbb{Q}[X]^\times$. Ainsi P est réductible dans $\mathbb{Q}[X]$.

Supposons réciproquement que P est réductible dans $\mathbb{Q}[X]$. On peut écrire $P = QR$ avec $Q, R \in \mathbb{Q}[X]$ et $\deg(Q) \geqslant 1$, $\deg(R) \geqslant 1$. On peut donc trouver α et β dans $\mathbb{Q}^\times$ vérifiant $\alpha\beta = 1$, $Q_1 = \alpha Q \in \mathbb{Z}[X]$ et $R_1 = \beta R \in \mathbb{Z}[X]$. Ainsi $P = Q_1 R_1$ avec $\deg(Q_1) = \deg(Q) \geqslant 1$ et $\deg(R_1) = \deg(R) \geqslant 1$, de sorte que Q_1 et R_1 ne sont pas inversibles dans $\mathbb{Z}[X]^\times$. On en conclut que P est réductible dans $\mathbb{Z}[X]$. □

Corollaire. *Les éléments irréductibles de $\mathbb{Z}[X]$ sont les polynômes constants de la forme $\pm p$ où p est un nombre premier et les polynômes primitifs irréductibles dans $\mathbb{Q}[X]$.*

Démonstration. Soit P un polynôme irréductible de $\mathbb{Z}[X]$. On peut donc écrire $P = c(P)P_1$ avec P_1 primitif. Si $c(P) \notin \mathbb{Z}^\times$, alors $c(P) \notin \mathbb{Z}[X]^\times$, donc P_1 est inversible, c'est-à-dire $P_1 = \pm 1$. Comme $c(P)$ doit être irréductible dans $\mathbb{Z}$, $P = \pm 1 c(P) = \pm p$ pour un nombre premier p. Si $c(P) \in \mathbb{Z}^\times$, alors P_1 est primitif et irréductible, donc est irréductible dans $\mathbb{Q}[X]$. □

Corollaire. *Tout polynôme non nul de $\mathbb{Z}[X]$ s'écrit de façon unique à l'ordre près comme produit d'un élément de $\mathbb{Z}$ et de polynômes primitifs irréductibles à terme dominant positif.*

Démonstration. On rappelle que si A est factoriel, l'anneau $A[X]$ est factoriel. Comme $\mathbb{Z}$ est factoriel, l'anneau $\mathbb{Z}[X]$ l'est aussi. Comme $\mathbb{Z}[X]^\times = \mathbb{Z}^\times$, le résultat est une conséquence de la classification des éléments irréductibles de $\mathbb{Z}[X]$. □

Exemple. La décomposition du polynôme $12X^2 - 3$ en produit d'irréductibles dans $\mathbb{Z}[X]$ est

$$12X^2 - 3 = 3 \cdot (2X - 1) \cdots (2X + 1).$$

Théorème 1.8 (Critère d'Eisenstein)**.** *Soit $P(X) = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$ un polynôme à coefficients entiers. On suppose qu'il existe un nombre premier p tel que $p \nmid a_n$, $p \mid a_i$ pour $0 \leqslant i \leqslant n-1$ et $p^2 \nmid a_0$. Le polynôme $P(X)$ est alors irréductible dans $\mathbb{Q}[X]$.*

Démonstration. Comme $p \mid a_0$ mais $p \nmid a_n$, on a nécessairement $n \geqslant 1$. Comme $p \nmid a_n$, on a $p \nmid c(P)$. Le polynôme $c(P)^{-1}P \in \mathbb{Z}[X]$ a donc exactement les mêmes propriétés que P mais est de plus primitif. Comme P est irréductible dans $\mathbb{Q}[X]$ si et seulement si $c(P)^{-1}P$ l'est, on peut supposer sans perte de généralité que $c(P) = 1$. Supposons donc $c(P) = 1$ et supposons par l'absurde que P est réductible dans $\mathbb{Q}[X]$. Alors on peut écrire $P = QR$ avec $\deg(Q), \deg(R) \geqslant 1$ et $Q, R \in \mathbb{Z}[X]$. De plus $c(P) = 1$ implique $c(Q) = c(R) = 1$. En réduisant $P = QR$ modulo le nombre premier p, on obtient $\overline{QR} = \overline{P} \neq \overline{0}$ dans $\mathbb{Z}/p\mathbb{Z}[X]$. Par ailleurs $\overline{P} = \gamma X^n$ pour un certain $\gamma \in (\mathbb{Z}/p\mathbb{Z})^\times$. Comme X est irréductible dans $\mathbb{Z}/p\mathbb{Z}[X]$ et que $\mathbb{Z}/p\mathbb{Z}[X]$ est principal, on en déduit que $\overline{Q}$ est de la forme αX^r et $\overline{R}$ est de la forme βX^s avec $\alpha\beta = \gamma$ et $r + s = n$. Comme $r \leqslant \deg(Q)$, $s \leqslant \deg(R)$ et $\deg(Q) + \deg(R) = \deg(P) = n$, on a $r = \deg(Q) \geqslant 1$ et $s = \deg(R) \geqslant 1$ de sorte que les termes constants de Q et R sont divisibles par p, ou encore $p \mid Q(0)$ et $p \mid R(0)$. On en conclut que $p^2 \mid P(0) = Q(0)R(0)$, ce qui contredit $p^2 \nmid a_0$. □

Exemple. Soit p un nombre premier. Soit $\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1$ de sorte que $X^p - 1 = \Phi_p(X)(X - 1)$. Le polynôme $\Phi_p(X)$ est irréductible dans $\mathbb{Q}[X]$ si et seulement si $\Phi_p(X + 1)$ est irréductible dans $\mathbb{Q}[X]$. Par ailleurs

$$\Phi_p(X+1) = \frac{(1+X)^p - 1}{X} = \sum_{i=0}^{p-1} \binom{p}{i+1} X^i = \sum_{i=0}^{p-1} a_i X^i.$$

On a $a_{p-1} = 1$ et $p \mid a_i$ si $0 \leqslant i \leqslant p-2$ et enfin $a_0 = p$. On en conclut que $\Phi_p(X + 1)$, et donc $\Phi_p(X)$, est irréductible dans $\mathbb{Q}[X]$.

1.4 Étude du groupe $(\mathbb{Z}/n\mathbb{Z})^\times$

Le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^\times$ joue un rôle très important dans nombre de procédés cryptographiques.

1.4.1 Le petit théorème de Fermat

Théorème 1.9 (Fermat)**.** *Soit $a \in \mathbb{Z}$ et soit p un nombre premier tel que $p \nmid a$. Alors $a^{p-1} \equiv 1\,[p]$.*

Démonstration. Comme p est premier, $\mathbb{Z}/pZ$ est un corps et le groupe $(\mathbb{Z}/p\mathbb{Z})^\times$ est de cardinal $p-1$. Le théorème de Lagrange implique alors que $\overline{a}^{p-1} = \overline{1}$ pour tout $\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^\times$, c'est-à-dire $a^{p-1} \equiv 1\,[p]$ pour tout $p \nmid a$. □

Remarque. On en déduit que si p est premier, $a^p \equiv a\,[p]$ pour tout $a \in \mathbb{Z}$.

La généralisation suivante du petit théorème de Fermat est due à Euler, la démonstration est identique.

Théorème 1.10 (Euler)**.** *Soit $n \in \mathbb{N}^*$ et soit $a \in \mathbb{Z}$ tel que $a \wedge n = 1$, alors $a^{\varphi(n)} \equiv 1\,[n]$.*

1.4.2 Nombres de Carmichael

Inversement, on peut se demander si un entier $n \geqslant 2$ vérifiant $a^{n-1} \equiv 1\,[n]$ pour tout a premier avec n est toujours premier. La réponse est non. Il existe effectivement de tels entiers. Un entier $m \geqslant 2$ non premier et tel que $a^{m-1} \equiv 1\,[m]$ pour tout $a \wedge m = 1$ est appelé *nombre de Carmichael*. Le plus petit d'entre eux est

$$561 = 3 \cdot 11 \cdot 13.$$

On a en effet

$$a^2 \equiv 1\,[3] \Rightarrow a^{560} \equiv 1\,[3]$$
$$a^{10} \equiv 1\,[11] \Rightarrow a^{560} \equiv 1\,[11]$$
$$a^{16} \equiv 1\,[17] \Rightarrow a^{560} \equiv 1\,[17] \text{ car } 16 \mid 560.$$

On peut montrer que les nombres de Carmichael ont les propriétés suivantes

- un nombre de Carmichael est sans diviseur carré ;
- si m est de Carmichael et $p \mid m$ est premier, alors $p - 1 \mid m - 1$;
- un nombre de Carmichael m possède au moins 3 diviseur premiers ;
- il existe une infinité de nombres de Carmichael (Alford, Granville et Pomerance, 1994).

Exemple. Les entiers suivants sont des nombres de Carmichael

$$561, 1729, 2465, 10585, 101101 \ldots$$

On peut montrer une version beaucoup plus faible du théorème d'Alford, Granville et Pomerance.

Proposition. *Soit $a \geqslant 2$ un entier. Il existe une infinité de $m \in \mathbb{Z}$ non premiers tels que $a^{m-1} \equiv 1\,[m]$.*

Démonstration. Soit p un nombre premier impair tel que $p \nmid a(a^2-1)$. Posons alors $m = \frac{a^{2p}-1}{a^2-1} = \frac{a^p-1}{a-1}\frac{a^p+1}{a+1}$. Comme $p \geqslant 3$ et $a \geqslant 2$, $a^p - 1 > a - 1$ et $a^p + 1 > a + 1$, donc m n'est pas premier.

Par ailleurs, on a

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

Le petit théorème de Fermat implique que $p \mid a^{p-1} - 1$. Comme $p - 1$ est pair, on a $a^2 - 1 \mid a^{p-1} - 1$ et, puisque $a^2 - 1$ et p sont premiers entre eux, $p(a^2-1) \mid a^{p-1} - 1$. Comme a ou $a^{p-1}+1$ est pair, on a $2 \mid a^2(a^{p-1}+1)$ de sorte que $2p(a^2-1) \mid (a^2-1)(m-1)$. On en conclut donc que $2p \mid m - 1$.

Ainsi $a^{2p} = 1 + m(a^2-1) \equiv 1\,[m]$ et donc $a^{m-1} \equiv 1\,[m]$. □

À titre d'illustration, nous donnons le critère de primalité suivant, mais qui n'est guère utile car il implique de savoir factoriser $m - 1$.

Proposition. *Soit $a \in \mathbb{Z}$ et soit $m \geqslant 2$ un entier vérifiant $a^{m-1} \equiv 1\,[m]$ et $a^\ell \not\equiv 1\,[m]$ pour tout diviseur ℓ de $m - 1$ tel que $\ell \neq m - 1$. Alors m est un nombre premier.*

Démonstration. Soit d l'ordre de $\overline{a}$ dans le groupe $(\mathbb{Z}/m\mathbb{Z})^\times$. Par hypothèse, $d \mid m - 1$. Comme $\overline{a}^\ell \neq \overline{1}$ pour tout diviseur strict de $m - 1$, on a $d = m - 1$. De plus le théorème d'Euler implique que $d \mid \varphi(m)$ de sorte que $m - 1 \mid \varphi(m)$. Comme $\varphi(m) \leqslant m - 1$, on a $\varphi(m) = m - 1$, ce qui implique que m est premier. □

1.4.3 Structure des groupes $(\mathbb{Z}/n\mathbb{Z})^\times$

Si $n \geqslant 2$, on peut écrire $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ avec $p_1 < p_2 < \cdots < p_r$ premiers et $\alpha_i \geqslant 1$ entiers. Le théorème des restes implique que

$$(\mathbb{Z}/n\mathbb{Z})^\times \simeq (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_r\mathbb{Z})^\times.$$

Il suffit donc d'étudier la structure des groupes $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ pour p premier et $\alpha \geqslant 1$ entier.

Théorème 1.11. *Si p est un nombre premier, le groupe $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique.*

Démonstration. Nous allons prouver plus généralement que si K est un corps commutatif fini, alors $K^\times$ est cyclique. Soit N le cardinal de K. Le théorème de structure des groupes abéliens fini implique que si G est un groupe abélien fini, alors G contient un élément dont l'ordre est le ppcm de tous les ordres des éléments de G. On applique ce résultat au groupe $k^\times$ et on note d le ppcm de tous les ordres de $K^\times$. On a donc $x^d = 1$ pour tout $x \in K^\times$. Comme K est un corps commutatif, le polynôme $X^d - 1$ a au plus d racines

dans K. On a donc $N-1 \leqslant d$. Par ailleurs, $K^\times$ contient un élément d'ordre d. On a donc $d \leqslant N-1$, ce qui permet de conclure que $d = N-1$ et que $K^\times$ contient un élément d'ordre $N-1$, ce groupe est donc cyclique. □

Exemple. Le groupe $(\mathbb{Z}/7\mathbb{Z})^\times$ est engendré par $\overline{3}$. On a en effet $\overline{3}^2 = \overline{2}$ et $\overline{3}^3 = -\overline{1}$, donc $\overline{3}$ est d'ordre 6.

On peut en profiter pour mentionner la célèbre conjecture d'Artin sur les racines primitives.

Conjecture (Conjecture d'Artin)**.** *Soit $a \in \mathbb{N}^*$ un entier qui n'est pas un carré parfait. Alors il existe une infinité de nombre premier p tels que $\overline{a}$ est un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$.*

Remarque. On sait (Hooley, 1967) que la conjecture d'Artin est une conséquence de l'hypothèse de Riemann généralisée (GRH) dont nous parlerons plus tard. On sait aussi qu'il existe une infinité de valeurs de a pour lesquelles la conjecture d'Artin est vraie (Gupta et Murty, 1984) et même qu'il existe au plus deux valeurs de a pour lesquels la conjecture est fausse (Heath-Brown, 1986). On ne connaît malheureusement aucune valeur explicite de a pour laquelle la conjecture est vraie. On par exemple juste dire que parmi 2, 3 et 5 il y a au moins un nombre vérifiant la conjecture.

Théorème 1.12. *Soit p un nombre premier impair et soit $\alpha \geqslant 1$ un entier. Le groupe $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est cyclique d'ordre $p^{\alpha-1}(p-1)$.*

Démonstration. Considérons le morphisme d'anneaux $\mathbb{Z}/p^\alpha\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ définie par $\overline{a}_{p^\alpha} \mapsto \overline{a}$. Si $a \in \mathbb{Z}$, on a $a \wedge p = 1$ si et seulement si $a \wedge p^\alpha = 1$, ainsi $\overline{a}_{p^\alpha} \in \mathbb{Z}/p^\alpha\mathbb{Z}$ si et seulement si $\overline{a}_p \in \mathbb{Z}/p\mathbb{Z}$. On en déduit un morphisme surjectif de groupes $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$. Notons G_α son noyau. Comme $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est un groupe de cardinal $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$, une comparaison des cardinaux montre que G_α est de cardinal $p^{\alpha-1}$. Soit $a \in \mathbb{Z}$ tel que $\overline{a}_p$ engendre le groupe $(\mathbb{Z}/p\mathbb{Z})^\times$ et posons $g = \overline{a}_{p^\alpha}$ et $h = g^{p^{\alpha-1}}$. Puisque $\overline{a}_p^{p-1} = \overline{1}_p$, les éléments g et h ont même image dans $(\mathbb{Z}/p\mathbb{Z})^\times$. Comme de plus $g^{p^{\alpha-1}(p-1)} = 1$ d'après le théorème de Lagrange, on a $h^{p-1} = 1$, ce qui prouve que l'élément h est d'ordre exactement $p-1$. Notons H le sous-groupe de $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ engendré par h. Comme G_α est un groupe de cardinal $p^{\alpha-1}$, on a $G_\alpha \cap H = \{1\}$ et, par cardinalité, $(\mathbb{Z}/p^{\alpha-1}\mathbb{Z})^\times$ est isomorphe au groupe produit $G_\alpha \times H$. Comme H est cyclique d'ordre $p-1$, le groupe $(\mathbb{Z}/p^{\alpha-1}\mathbb{Z})^\times$ est cyclique d'ordre $p^{\alpha-1}(p-1)$ dès lors que l'on sait que G_α est cyclique d'ordre $p^{\alpha-1}$.

Nous allons en fait prouver que l'élément $\overline{1+p}_{p^\alpha}$ est un générateur de G_α. Pour cela, il suffit de vérifier que $(1+p)^{p^{\alpha-2}} \not\equiv 1\,[p]^\alpha$. On vérifie en effet par récurrence sur $s \geqslant 0$ que $(1+p)^{p^s} \equiv 1 + p^{s+1}\,[p^{s+2}]$, ce qui suffit puisque $1 + p^{\alpha-1} < p^\alpha$. La congruence est évidemment vrai pour $s = 0$. Supposons qu'elle est vraie pour $s \geqslant 0$. On a alors $(1+p)^{p^s} = 1 + kp^{s+1}$ pour un entier $k \equiv 1\,[p]$. On a donc

$$(1+p)^{p^{s+1}} = (1+kp^{s+1})^p = 1 + kp^{s+2} + \sum_{i=2}^{p} \binom{p}{i} (kp^{s+1})^i.$$

Si $i \geqslant 3$, on a $s+3 \leqslant i(s+1)$, donc $p^{s+3} \mid (kp^{s+1})^i$ et, puisque $p \geqslant 3$, on a $p \mid \binom{p}{2}$, ce qui prouve $p^3 \mid \binom{p}{2}(kp^{s+1})^2$. On a donc $(1+p)^{p^{s+1}} \equiv 1 + kp^{s+2} \equiv 1 + p^{s+2}\,[p^{s+3}]$. □

Il reste à s'occuper du cas où $p = 2$. Dans ce cas, on peut remarquer que $(\mathbb{Z}/4\mathbb{Z})^\times = \{\overline{1}, -\overline{1}\}$ est cyclique mais que $(\mathbb{Z}/8\mathbb{Z})^\times = \{\pm\overline{1}, \pm\overline{3}\}$ ne l'est pas, puisque $3^2 \equiv 1\,[8]$.

Théorème 1.13. *Soit $\alpha \geqslant 2$. Alors le noyau du morphisme surjectif de groupes $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times \to (\mathbb{Z}/4\mathbb{Z})^\times$ défini par réduction modulo 4 est cyclique d'ordre $2^{\alpha-2}$ et il existe un isomorphisme de groupes*

$$(\mathbb{Z}/2^\alpha\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\alpha-2}\mathbb{Z}.$$

Démonstration. Notons G_α le noyau de ce morphisme. On montre que l'élément $\overline{1+4}_{2^\alpha} = \overline{5}_{2^\alpha}$ est un générateur de G_α. Il suffit de prouver que $5^{2^{\alpha-3}} \not\equiv 1\,[2]^\alpha$ si $\alpha \geqslant 3$. C'est une conséquence de la congruence $5^{2^s} \equiv 1 + 2^{s+2}\,[2^{s+3}]$ pour tout entier $s \geqslant 0$. On montre cette congruence par récurrence sur s. Elle est trivialement vraie pour $s = 0$. Supposons alors que $5^{2^s} = 1 + k2^{s+2}$ avec k impair. On a alors

$$5^{2^{s+1}} = (1 + k2^{s+2})^2 = 1 + k2^{s+3} + k^2 2^{2s+4}.$$

Comme $2s + 4 \geqslant s + 4$, on a $5^{2^{s+1}} \equiv 1 + 2^{s+3}\,[2^{s+4}]$.

Soit $H = \{\pm\overline{1}_{2^\alpha}\}$ le sous-groupe de $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ engendré par $-\overline{1}_{2^\alpha}$. Comme $H \cap G_\alpha = \{1\}$, on obtient par cardinalité un isomorphisme de groupes $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times \simeq H \times G_\alpha$. □

Corollaire. *Soit $n \geqslant 2$ un entier. Pour que le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ soit cyclique, il faut et il suffit que n soit de la forme p^α ou $2p^\alpha$ avec p premier impair et $\alpha \geqslant 1$ entier ou que $n \in \{2, 4\}$.*

Démonstration. Commençons par plusieurs remarques.

— Si G_1 et G_2 sont deux groupes abéliens finis de cardinaux respectifs n_1 et n_2 vérifiant $n_1 \wedge n_2 \neq 1$, alors le groupe abélien fini $G_1 \times G_2$ n'est pas cyclique.

— Un sous-groupe d'un groupe cyclique est cyclique.

Supposons alors $(\mathbb{Z}/n\mathbb{Z})^\times$ cyclique et posons $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ avec $p_1 < \cdots < p_r$ premiers. Posons également $G_i = (\mathbb{Z}/p_i\mathbb{Z})^\times$. Il suit des deux remarques ci-dessus que les entiers $\mathrm{Card}(G_1), \ldots, \mathrm{Card}(G_r)$ sont premiers entre eux deux à deux. Parmi ces entiers, il y en a au plus un qui est pair et donc, parmi $p_1, \ldots, p_r$ il y a au plus un nombre impair. On en conclut que $r \leqslant 2$ et que

$$\{p_1, p_2\} = \begin{cases} \{2, p\} & p \text{ impair} \\ \{p\} & p \text{ impair} \\ \{2\} & \end{cases}$$

Comme de plus $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ est cyclique si et seulement si $\alpha \leqslant 2$, on en conclut que $n \in \{2, 4, p^\alpha, 2p^\alpha, 4p^\alpha\}$ pour un nombre premier p impair et un entier $\alpha \geqslant 1$. Comme $\varphi(p^\alpha)$

est pair, le groupe $(\mathbb{Z}/4p^\alpha\mathbb{Z})^\times$ n'est pas cyclique. Ainsi n est de la forme $2, 4, p^\alpha, 2p^\alpha$. Réciproquement on vérifie facilement que pour ces valeurs, le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique. □

Chapitre 2

Fonctions arithmétiques

2.1 Définitions et premières propriétés

2.1.1 Définitions

On appelle *fonction arithmétique* une application de $\mathbb{N}^*$ dans $\mathbb{C}$. Une fonction arithmétique f est dite *multiplicative* si elle vérifie les conditions suivantes

$$f(1) = 1$$
$$\forall (m,n) \in (\mathbb{N}^*)^2 \text{ tel que } m \wedge n = 1, \quad f(mn) = f(m)f(n).$$

Une fonction arithémtique f est dite *complètement multiplicative* si

$$f(1) = 1$$
$$\forall (m,n) \in (\mathbb{N}^*)^2, \quad f(mn) = f(m)f(n).$$

La notion de fonction arithmétique complètement multiplicative peut sembler plus naturel, mais nous rencontrerons en pratique un grand nombre de fonctions arithmétiques qui sont multiplicatives mais non complètement multiplicatives.

Une fonction arithmétique multiplicative est donc déterminée par ses valeurs sur l'ensemble des nombres de la forme p^k où p est un nombre premier et $k \geqslant 1$ un entier. Une fonction arithmétique complètement multiplicative est déterminée par ses valeurs sur l'ensemble des nombres premiers.

Exemple. a) La fonction indicatrice d'Euler φ est une fonction arithmétique qui est multiplicative mais pas complètement multiplicative.

b) La fonction constante $\mathbb{1}$ est complètement multiplicative.

c) La fonction e définie comme δ_1, la fonction indicatrice du singleton $\{1\}$ est complètement multiplicative.

d) Considérons la fonction arithmétique « nombre de diviseurs », c'est-à-dire la fonction $d : \mathbb{N}^* \to \mathbb{C}$ définie par $d(n) = \mathrm{Card}\{d \in \mathbb{N}^* \mid d \mid n\}$. C'est une fonction multiplicative. On a en effet, si $m \wedge n = 1$ et $d \mid mn$, l'entier d peut s'écrire de façon unique sous la forme $d_1 d_2$ où $d_1 \mid m$ et $d_2 \mid n$. L'unicité vient du fait que $d_1 = m \wedge d$ et $d_2 = n \wedge d$. L'existence vient du fait qu'en posant $d_1 = m \wedge d$ et $d_2 = n \wedge d$, on a $d = d_1 d_2$ puisque $m \wedge n = 1$.

e) La fonction $\mathrm{Id} : \mathbb{N}^* \to \mathbb{N}^*$ est également une fonction arithmétique complètement multiplicative.

2.1.2 Loi de composition

Notons $\mathcal{F}$ l'ensemble $\mathcal{F}(\mathbb{N}^*, \mathbb{C})$ de toutes les fonctions arithmétiques. C'est un $\mathbb{C}$-espace vectoriel. Cet espace est de plus muni d'une loi de *composition arithmétique* définie comme suit. Si f et g sont deux éléments de $\mathcal{F}$, on définit une fonction arithmétique $f * g$ en posant

$$\forall n \in \mathbb{N}^*, \quad (f * g)(n) = \sum_{\substack{d \geqslant 1 \\ d \mid n}} f(d) g\left(\frac{n}{d}\right) = \sum_{\substack{(d_1, d_2) \in (\mathbb{N}^*)^2 \\ d_1 d_2 = n}} f(d_1) g(d_2).$$

Théorème 2.1. *Le triplet $(\mathcal{F}, +, *)$ est un anneau commutatif d'unité $e = \delta_1$. Son groupe des inversibles est donné par*

$$\mathcal{F}^\times = \{f \in \mathcal{F} \mid f(1) \neq 0\}.$$

Démonstration. Il faut prouver que la loi de composition arithmétique est associative, commutative, distributive par rapport à $+$ et d'élément neutre e.

La commutativité et la distributivité sont immédiates. Prouvons l'associativité. Si f, g, h sont dans $\mathcal{F}$, on a, pour $n \in \mathbb{N}^*$,

$$\begin{aligned}
((f * g) * h)(n) &= \sum_{\substack{(d_1, d_2) \in (\mathbb{N}^*)^2 \\ d_1 d_2 = n}} (f * g)(d_1) h(d_2) \\
&= \sum_{\substack{(d_1, d_2) \in (\mathbb{N}^*)^2 \\ d_1 d_2 = n}} \left(\sum_{\substack{(\delta, \delta') \in (\mathbb{N}^*)^2 \\ \delta \delta' = d_1}} f(\delta) g(\delta') \right) h(d_2) \\
&= \sum_{\substack{(\delta_1, \delta_2, \delta_3) \in (\mathbb{N}^*)^3 \\ \delta_1 \delta_2 \delta_3 = n}} f(\delta_1) g(\delta_2) h(\delta_3).
\end{aligned}$$

On montre de même que

$$(f * (g * h))(n) = \sum_{\substack{(\delta_1, \delta_2, \delta_3) \in (\mathbb{N}^*)^3 \\ \delta_1 \delta_2 \delta_3 = n}} f(\delta_1) g(\delta_2) h(\delta_3)$$

et on en déduit l'associativité. La fonction e est neutre pour $*$ car, si $f \in \mathcal{F}$ et $n \in \mathbb{N}^*$, on a

$$(e * f)(n) = \sum_{\substack{(d_1,d_2)\in(\mathbb{N}^*)^2 \\ d_1 d_2 = n}} \underbrace{e(d_1)f(d_2)}_{\neq 0 \Rightarrow d_1 = 1} = f(n).$$

Prouvons enfin que $f \in \mathcal{F}^\times$ si et seulement si $f(1) \neq 0$. Si $f \in \mathcal{F}^\times$, on a $e = f * f^{-1}$ et donc $1 = e(1)f(1)f^{-1}(1)$ de sorte que $f(1) \neq 0$.

Supposons réciproquement que $f(1) \neq 0$. Il suffit de montrer qu'il existe une fonction $g \in \mathcal{F}$ telle que $f * g = e$. On construit g par récurrence. Plus précisément, montrons par récurrence sur n, qu'il existe des nombres $g(k) \in \mathbb{C}$, $1 \leqslant k \leqslant n$ tels que

$$\forall 1 \leqslant m \leqslant n, \quad \sum_{\substack{d\geqslant 1 \\ d|m}} f(d)g\left(\frac{m}{d}\right) = e(m).$$

Comme $f(1) \neq 1$, l'hypothèse est vraie pour $n = 1$, il suffit de prendre $g(1) = f(1)^{-1}$. Supposons le résultat vrai pour n et montrons le pour $n+1$. Suffit de trouver un nombre $g(n+1) \in \mathbb{C}$ tel que

$$\sum_{\substack{d\geqslant 1 \\ d|n+1}} f(d)g\left(\frac{n+1}{d}\right) = e(n+1) = 0.$$

Il suffit donc de poser

$$g(n+1) = -f(1)^{-1} \sum_{\substack{d>1 \\ d|m}} f(d)g\left(\frac{m}{d}\right). \qquad \square$$

On note $\mathcal{M} \subset \mathcal{F}^\times$ l'ensemble des fonctions multiplicatives et $\mathcal{M}^c \subset \mathcal{M}$ l'ensemble des fonctions complètement multiplicatives.

Théorème 2.2. *L'ensemble $\mathcal{M}$ est un sous-groupe de $(\mathcal{F}^\times, *)$. On a de plus, pour $f \in \mathcal{M}^c$ et $(g,h) \in \mathcal{M}^2$,*

$$f \cdot (g * h) = (f \cdot g) * (f \cdot h).$$

Démonstration. Montrons que $\mathcal{F}$ est stable par $*$. Il faut donc prouver que si f et g sont deux fonctions multiplicatives, alors $f * g$ est multiplicative. Soient donc $(m,n) \in (\mathbb{N}^*)^2$ tel que $m \wedge n = 1$. Rappelons que l'on a une bijection

$$\begin{array}{ccc} \{d_1 \in \mathbb{N}^* \mid d_1 \mid n\} \times \{d_2 \in \mathbb{N}^* \mid d_2 \mid n\} & \longrightarrow & \{d \in \mathbb{N}^* \mid d \mid n\} \\ (d_1, d_2 & \longmapsto & d_1 d_2. \end{array}$$

On a donc

$$\begin{aligned}(f*g)(mn) &= \sum_{\substack{d\geqslant 1\\ d|mn}} f(d)g\left(\frac{mn}{d}\right) = \sum_{\substack{(d_1,d_2)\in(\mathbb{N}^*)^2\\ d_1|m\\ d_2|n}} f(d_1d_2)g\left(\frac{mn}{d_1d_2}\right)\\ &\sum_{\substack{(d_1,d_2)\in(\mathbb{N}^*)^2\\ d_1|m\\ d_2|n}} f(d_1)f(d_2)g\left(\frac{m}{d_1}\right)g\left(\frac{n}{d_2}\right)\\ &= \left(\sum_{\substack{d_1\geqslant 1\\ d_1|m}} f(d_1)g\left(\frac{m}{d_1}\right)\right)\left(\sum_{\substack{d_2\geqslant 1\\ d_2|n}} f(d_2)g\left(\frac{n}{d_2}\right)\right)\\ &= (f*g)(m)(f*g)(n)\end{aligned}$$

de sorte que $f*g\in\mathcal{M}$.

Montrons que $\mathcal{F}$ est stable par inverse. Soit $f\in\mathcal{M}$. Il faut prouver que $f^{-1}\in\mathcal{M}$. Soit g l'unique fonction multiplicative telle que, pour p premier et $k\geqslant 1$, $g(p^k)=f^{-1}(p^k)$. Posons $h=f*g$. Il faut prouver que $h=e$, on aura alors $g=f^{-1}$ et donc $f^{-1}\in\mathcal{M}$. Comme h est multiplicative, il suffit de prouver que $h(p^k)=0$ pour tout nombre premier p et tout entier $k\geqslant 1$. On a

$$\begin{aligned}h(p^k) &= \sum_{i=0}^{k} f(p^i)g(p^{k-i}) = \sum_{i=0}^{k} f(p^i)f^{-1}(p^{n-i})\\ &= (f*f^{-1})(p^k) = 0\end{aligned}$$

par définition de g et f^{-1}.

Vérifions la dernière propriété. Supposons que $f\in\mathcal{M}^c$ et $(g,h)\in\mathcal{M}^2$. Si $n\in\mathbb{N}^*$, on a

$$\begin{aligned}(f\cdot(g*h))(n) &= f(n)\sum_{\substack{d\geqslant 1\\ d|n}} g(d)h\left(\frac{n}{d}\right) = \sum_{\substack{d\geqslant 1\\ d|n}} f(n)g(d)h\left(\frac{n}{d}\right)\\ &= \sum_{\substack{d\geqslant 1\\ d|n}} f(d)g(d)f\left(\frac{n}{d}\right)h\left(\frac{n}{d}\right) = ((f\cdot g)*(f\cdot h))(n).\end{aligned}$$ □

2.1.3 Construction de fonctions arithmétiques multiplicatives

La fonction de Möbius La fonction constante $\mathbb{1}$ est un élément de $\mathcal{F}$. On note μ son inverse pour la loi $*$. Comme $\mathbb{1}$ est multiplicative, la fonction μ l'est aussi. La fonction arithmétique μ est appelée *fonction de Möbius*. Par définition de μ, on a donc $\mathbb{1}*\mu=e$ et

$\mu(1) = 1$. Déterminons ses autres valeurs. Si p est un nombre premier, la relation $\mathbb{1} * \mu = e$ implique $\mu(p) + \mu(1) = 0$, c'est-à-dire $\mu(p) = -1$. On a également $\mu(p^2) + \mu(p) + \mu(1) = 0$, ce qui implique $\mu(p^2) = 0$. En raisonnant par récurrence, on vérifie immédiatement que $\mu(p^k) = 0$ pour tout entier $k \geqslant 2$. Comme μ est multiplicative, on a donc

$$\forall n \in \mathbb{N}^*, \quad \mu(n) = \begin{cases} (-1)^k & \text{si } n \text{ est un produit de } k \text{ nombres premiers distincts;} \\ 0 & \text{sinon.} \end{cases}$$

Exemple. Rappelons que la fonction indicatrice d'Euler φ est définie, pour $q \in \mathbb{N}^*$, par la formule

$$\varphi(q) = \sum_{\substack{1 \leqslant n \leqslant q \\ n \wedge q = 1}} 1 = \sum_{1 \leqslant n \leqslant q} e(n \wedge q) = \sum_{1 \leqslant n \leqslant q} (\mu * \mathbb{1})(n \wedge q).$$

Comme un entier $d \geqslant 1$ divise $n \wedge q$ si et seulement il divise n et q, on a

$$\varphi(q) = \sum_{n=1}^{q} \sum_{\substack{d \geqslant 1 \\ d|n \\ d|q}} \mu(d) = \sum_{\substack{d \geqslant 1 \\ d|n}} \mu(d) \sum_{\substack{1 \leqslant n \leqslant q \\ d|q}} 1 = \sum_{\substack{d \geqslant 1 \\ d|q}} \mu(d) \frac{q}{d}.$$

Ainsi $\varphi = \mu * \mathrm{Id}$ et donc $\mathrm{Id} = \varphi * \mathbb{1}$. On a donc prouvé que, pour $n \in \mathbb{N}^*$,

$$n = \sum_{\substack{d \geqslant 1 \\ d|n}} \varphi(d).$$

Les fonctions diviseurs Si $k \in \mathbb{N}^*$, on note d_k la fonction arithmétique $\underbrace{\mathbb{1} * \cdots * \mathbb{1}}_{k \text{ fois}}$. Comme la fonction $\mathbb{1}$ est complètement multiplicative, la fonction d_k est multiplicative. Dans le cas particulier où $k = 2$ on retrouve la fonction « nombre de diviseurs » :

$$d_2(n) = \sum_{\substack{\delta \geqslant 1 \\ \delta | n}} \mathbb{1}(\delta) \mathbb{1}(\tfrac{n}{\delta}) = \mathrm{Card}\{(d_1, d_2) \in (\mathbb{N}^*)^2 \mid n = d_1 d_2\}.$$

Plus généralement, une récurrence sur k montre que

$$d_k(n) = \mathrm{Card}\{(d_1, \ldots, d_k) \in (\mathbb{N}^*)^k \mid n = d_1 d_2 \cdots d_k\}.$$

Comme la fonction d_k est multiplicative, elle est complètement déterminée par ses valeurs sur les entiers de la forme p^m où p est un nombre premier. Calculons directement $d_k(p^m)$.

$$\begin{aligned} &\mathrm{Card}\{(d_1, \ldots, d_k) \in (\mathbb{N}^*)^k \mid d_1 d_2 \cdots d_k = p^m\} \\ &\qquad = \mathrm{Card}\{(m_1, m_2, \ldots, m_k) \in \mathbb{N}^k \mid m = \sum_{i=1}^{k} m_i\} \end{aligned}$$

L'ensemble dont le cardinal apparaît sur la droite est en bijection avec l'ensemble des fonctions strictement croissantes $h : \{1, \dots, k\} \to \{0, 1, \dots, m+k-1\}$ telles que $h(k) = m+k-1$. En effet, on peut associer à un k-uplet d'enters $(m_1, \dots, m_k)$ tel que $\sum_{i=1}^{k} m_i = m$ la fonction h définie par $h(i) = n_1 + \cdots + n_i + i - 1$ et réciproquement, à une telle fonction h, le k-uplet $(m_1, \dots, m_k)$ où $m_i = h(i)-h(i-1)-(i-1)$. Ces deux fonctions sont bien réciproques l'une de l'autre. Enfin, on peut remarquer que les fonctions strictement croissantes $h : \{1, \dots, k\} \to \{0, \dots, m+k-1\}$ vérifiant $h(k) = m+k-1$ sont uniquement déterminées par l'ensemble de leurs $k-1$-ièmes premières valeurs, qui forment une partie de cardinal $k-1$ de $\{0, \dots, m+k-2\}$. Ainsi $d_k(p^m)$ est égal au nombre de parties à $k-1$ éléments dans $\{0, \dots, m+k-2\}$. On a donc

$$d_k(p^m) = \binom{m+k-1}{k-1} = \binom{m+k-1}{m}.$$

Les fonctions sommes de diviseurs Si $k \geqslant 1$ est un entier, on pose $\sigma_k = \mathbb{1} * (\mathrm{Id})^k$. Comme $\mathbb{1}$ est Id^k sont complètement multiplicatives, la fonction σ_k est multiplicative. Ses valeurs sont les

$$\sigma_k(n) = \sum_{\substack{d \geqslant 1 \\ d|n}} d^k.$$

La fonction de von Mangoldt Dans tout ce cours, on note log la fonction *logarithme népérien*. La fonction de von Mangodlt est définie comme le produit $\Lambda = \log * \mu$. De sorte que $\log = \Lambda * \mathbb{1}$. Si $n \geqslant 2$ est un entier, on peut écrire $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ où $p_1 < \cdots < p_r$ sont des nombres premiers. Les seuls diviseurs d de n pour lesquels $\mu(d) \neq 0$ sont les $\prod_{i \in I} p_i$ où I est une partie de $\{1, \dots, r\}$. On a donc

$$\begin{aligned}
\Lambda(n) &= \sum_{I \subset \{1,\dots,r\}} (-1)^{\mathrm{Card}(I)} \log\left(\frac{n}{\prod_{i \in I} p_i}\right) \\
&= \sum_{I \subset \{1,\dots,r\}} (-1)^{\mathrm{Card}(I)} \log(n) - \sum_{I \subset \{1,\dots,r\}} (-1)^{\mathrm{Card}(I)} \sum_{i \in I} \log(p_i) \\
&= \log(n) \sum_{k=0}^{r} (-1)^k \binom{r}{k} - \sum_{i=1}^{r} \log(p_i) \sum_{i \in I \subset \{1,\dots,r\}} (-1)^{\mathrm{Card}(I)} \\
&= \sum_{i=1}^{r} \log(p_i) \sum_{J \subset \{1,\dots,r\} \smallsetminus \{i\}} (-1)^{\mathrm{Card}(J)}.
\end{aligned}$$

Nous avons donc $\Lambda(n) = \log(p_1)$ si $r = 1$ et $\Lambda(n) = 0$ si $r > 1$.

2.1.4 Produits eulériens

Si $n \in \mathbb{N}^*$ est un entier, nous utiliserons très souvent l'abus de notation $\prod_{p \leqslant n}$ pour $\prod_{\substack{p \in \mathcal{P} \\ p \leqslant n}}$ où $\mathcal{P}$ désigne l'ensemble des nombres premiers.

Si (a_p) est une suite de nombres complexes indexée par les nombres premiers et si la suite $\left(\prod_{p\leqslant n} a_p\right)$ est une suite convergente, on note $\prod_p a_p$ sa limite.

Théorème 2.3. *Soit f une fonction arithmétique telle que la série $\sum_{n\geqslant 1} f(n)$ est absolument convergente. Si f est multiplicative, on a*

$$\sum_{n\geqslant 1} f(n) = \prod_p \left(\sum_{k\geqslant 0} f(p^k)\right).$$

Si de plus f est complètement multiplicative, alors $|f(p)| < 1$ pour tout nombre premier p et on a

$$\sum_{n\geqslant 1} f(n) = \prod_p \left(\frac{1}{1-f(p)}\right).$$

Démonstration. Soit $N \geqslant 1$ un entier. Supposons dans un premier temps que la fonction f est multiplicative. La famille $(f(n))_{n\geqslant 1}$ est sommable. En particulier la série $\sum_{k\geqslant 0} f(p^k)$ est absolument convergente. Soient $p_1, \ldots, p_r$ les nombres premiers plus petits que N. La formule du produit de Cauchy nous donne donc

$$\prod_{p\leqslant N}\left(\sum_{k=0}^{+\infty} f(p^k)\right) = \sum_{(n_1,\ldots,n_r)\in\mathbb{N}^r}\prod_{i=1}^{r} f(p_i^{n_i}) = \sum_{(n_1,n_2,\ldots,n_r)\in\mathbb{N}^r} f\left(\prod_{i=1}^{r} p_i^{n_i}\right).$$

Soit $\mathcal{A}_N$ l'ensemble des entiers $n \in \mathbb{N}^*$ dont les diviseurs premiers sont compris entre 1 et N. L'anneau $\mathbb{Z}$, étant factoriel, on a

$$\prod_{p\leqslant N}\left(\sum_{k\geqslant 0} f(p^k)\right) = \sum_{n\in\mathcal{A}_N} f(n).$$

Comme $\mathbb{N}$ est l'union de tous les ensembles $\mathcal{A}_N$ et que la famille $(f(n))_{n\geqslant 0}$ est sommable, on en conclut que la suite $\left(\prod_{p\leqslant N}\sum_{k\geqslant 0} f(p^k)\right)$ converge vers $\sum_{n\geqslant 1} f(n)$, c'est-à-dire

$$\prod_{p}\left(\sum_{k\geqslant 0} f(p^k)\right) = \sum_{n\geqslant 1} f(n).$$

Si f est complètement multiplicative, on a $f(p^k) = f(p)^k$ si p est un nombre premier et $k \geqslant 1$ entier. En particulier pour que la famille $(f(n))_{n\geqslant 1}$ soit sommable, il faut que $|f(p)| < 1$ pour tout nombre premier p. On a de plus

$$\sum_{k\geqslant 0} f(p^k) = \sum_{k\geqslant 0} f(p)^k = \frac{1}{1-f(p)}.$$

□

Si $f \in \mathcal{F}$ et si $s \in \mathbb{C}$, on appelle *série de Dirichlet associée à* f la série

$$D(f,s) = \sum_{n \geqslant 1} \frac{f(n)}{n^s}$$

définie aux valeurs de $s \in \mathbb{C}$ pour lesquelles elle est convergente. Si $f \in \mathcal{M}^c$ et si $s \in \mathbb{C}$ est telle que la série $D(f,s)$ est absolument convergente, on a alors

$$D(f,s) = \prod_p \left(\frac{1}{1 - f(p)p^{-s}} \right).$$

Il s'agit du *développement en produit eulérien* de la série $D(f,s)$.

Exemple. Dans le cas $f = \mathbb{1}$, la série de Dirichlet obtenue est le *fonction zeta de Riemann*

$$\zeta(s) = \sum_{n \geqslant 1} \frac{1}{n^s}.$$

La convergence de cette série est absolue pour $\mathrm{Re}(s) > 1$. Le développement en produit eulérien est alors

$$\zeta(s) = \prod_p \left(\frac{1}{1 - p^{-s}} \right).$$

2.1.5 Fonctions sommatoires

Soit $f \in \mathcal{F}$ une fonction arithmétique. Sa *fonction sommatoire* notée M_f est la fonction $\mathbb{R} \to \mathbb{C}$ définie par

$$M_f(x) = \sum_{\substack{n \in \mathbb{N}^* \\ n \leqslant x}} f(n)$$

pour tout $x \in \mathbb{R}$. Dans la suite de cours, nous utiliserons la notation $\sum_{n \leqslant x}$ pour désigner $\sum_{\substack{n \in \mathbb{N}^* \\ n \leqslant x}}$. La fonction M_f est une fonction localement constante sur $\mathbb{R}$. Remarquons que si f et g sont deux fonctions arithmétiques, on a, pour $x \in \mathbb{R}$,

$$\begin{aligned} M_{f*g}(x) &= \sum_{n \leqslant x} \sum_{d \mid n} f(d) g\left(\frac{n}{d}\right) = \sum_{d \leqslant x} f(d) \sum_{\substack{n \leqslant x \\ d \mid n}} g\left(\frac{n}{d}\right) \\ &= \sum_{d \leqslant x} f(d) M_g\left(\frac{x}{d}\right). \end{aligned} \tag{2.1}$$

Théorème 2.4. *Soient f et g deux fonctions arithmétiques sommables. Alors la fonction arithmétique $f * g$ est sommable également et on a*

$$\sum_{n \geqslant 1} (f*g)(n) = \left(\sum_{n \geqslant 1} f(n) \right) \left(\sum_{n \geqslant 1} g(n) \right).$$

En particulier, en toute valeur $s \in \mathbb{C}$ telle que les séries $D(f,s)$ et $D(g,s)$ sont absolument convergentes, $D(f*g,s)$ est absolument convergente et $D(f*g,s) = D(f,s)D(g,s)$.

Démonstration. Comme f et g sont sommables, les fonctions $M_{|f|}$ et $M_{|g|}$ sont croissantes et ont pour limite en $+\infty$ les sommes $\sum_{n\geqslant 1}|f(n)|$ et $\sum_{n\geqslant 1}|g(n)|$. On a alors, pour tout $x\in\mathbb{R}$,

$$M_{|f*g|}(x)\leqslant M_{|f|*|g|}(x)=\sum_{n\leqslant x}|f(n)|M_{|g|}\left(\frac{x}{n}\right)\leqslant\left(\sum_{n\geqslant 1}|f(n)|\right)\left(\sum_{n\geqslant 1}|g(n)|\right)<\infty.$$

On peut écrire

$$M_{f*g}(x)=\sum_{n\leqslant x}f(n)M_g\left(\frac{x}{n}\right)$$

où $M_g(\frac{x}{n})\to\sum_{n\geqslant 1}g(n)$ quand x tend vers $+\infty$. Par convergence dominée, on en conclut que

$$\lim_{x\to+\infty}M_{f*g}(x)=\left(\sum_{n\geqslant 1}f(n)\right)\left(\sum_{n\geqslant 1}g(n)\right)$$

et le résultat. □

Nous utiliserons très souvent le résultat dans l'étude des fonctions sommatoires.

Lemme (Sommation par parties)**.** *Soit $g\in\mathcal{F}$ une fonction arithmétique. Soit $0\leqslant a<b$ deux nombres réels et soit $f\in\mathcal{C}^1([a,b],\mathbb{C})$ une fonction de classe $\mathcal{C}^1$. On a alors*

$$\sum_{\substack{n\in\mathbb{N}^*\\ a<n\leqslant b}}f(n)g(n)=M_g(b)f(b)-M_g(a)f(a)-\int_a^b f'(t)M_g(t)\,dt.$$

Démonstration. Remarquons tout de suite que, puisque M_g est une fonction continue par morceaux, l'intégrale dans le terme de droite est bien définie.

Remarquons dans un premier temps que l'on peut se ramener au cas où a et b sont entiers. On a en effet

$$\sum_{\substack{n\in\mathbb{N}^*\\ a<n\leqslant b}}f(n)g(n)=\sum_{n=\lfloor a\rfloor+1}^{\lfloor b\rfloor}f(n)g(n)$$

et, puisque M_g est constante sur les intervalles $[\lfloor a\rfloor,a]$ et $[\lfloor b\rfloor,b]$,

$$\int_{\lfloor a\rfloor}^a f'(t)M_g(t)\,dt=M_g(a)(f(a)-f(\lfloor a\rfloor))=M_g(a)f(a)-M_g(\lfloor a\rfloor)f(\lfloor a\rfloor)$$
$$\int_{\lfloor b\rfloor}^b f'(t)M_g(t)\,dt=M_g(b)(f(b)-f(\lfloor b\rfloor))=M_g(b)f(b)-M_g(\lfloor b\rfloor)f(\lfloor b\rfloor).$$

On peut donc supposer que $a \in \mathbb{N}$ et $b \in \mathbb{N}^*$. On a alors

$$\begin{aligned}
\sum_{n=a+1}^{b} f(n)g(n) &= \sum_{n=a+1}^{b} f(n)(M_g(n) - M_g(n-1)) \\
&= \sum_{n=a+1}^{b} f(n)M_g(n) - \sum_{n=a+1}^{b} f(n)M_g(n-1) \\
&= \sum_{n=a+1}^{b} f(n)M_g(n) - \sum_{n=a}^{b-1} f(n+1)M_g(n) \\
&= f(b)M_g(b) - f(a)M_g(a) - \sum_{n=a}^{b-1} M_g(n)(f(n+1) - f(n)) \\
&= f(b)M_g(b) - f(a)M_g(a) - \sum_{n=a}^{b-1} \int_n^{n+1} f'(t)M_g(t)\,dt \\
&= f(b)M_g(b) - f(a)M_g(a) - \int_a^b f'(t)M_g(t)\,dt. \qquad \square
\end{aligned}$$

2.2 La suite des nombres premiers

La suite des nombres premiers est la suite $(p_n)_{n\geqslant 1}$ où p_n désigne le n-ième nombre premier. On a

$$p_1 = 2, p_3 = 2, p_3 = 5, \ldots, p_9 = 23, \ldots$$

Si $x \in \mathbb{R}$, on pose

$$\pi(x) = \mathrm{Card}\{n \in \mathbb{N}^* \mid p_n \leqslant x\} = \sum_{p \leqslant x} 1.$$

Théorème 2.5 (Euclide)**.** *La fonction π tend vers $+\infty$ quand n tend vers $+\infty$.*

Démonstration. Cet énoncé est une façon pompeuse de dire qu'il existe une infinité de nombres premiers. Rappelons la preuve d'Euclide. Si $k \in \mathbb{N}^*$, posons $N_k = p_1 \cdots p_k + 1$. Si p est un diviseur premier de N_k, on a $p \notin \{p_1, \ldots, p_k\}$. On en déduit que l'ensemble des nombres premiers est infini. $\square$

La preuve précédente nous permet d'obtenir une borne inférieure concernant la taille de $\pi(x)$. On en déduit en effet que, pour tout $k \in \mathbb{N}^*$, on a $p_{k+1} \leqslant p_1 \cdots p_k + 1$. On en déduit, par récurrence sur $n \geqslant 1$ que

$$\forall n \geqslant 1, \quad p_n \leqslant 2^{2^{n-1}}.$$

Si $x \geqslant 2$ est un nombre réel, soit n le plus grand entier tel que $p_n \leqslant x$. On a alors $\pi(x) = n$. On vient de voir que $x < p_{n+1} \leqslant 2^{2^n}$. On en déduit $\log(x) \leqslant 2^n \log(2)$ et donc

$\log\log(x) \leqslant n\log(2) + \log\log(2) = \pi(x)\log(2) + \log\log(2)$. On a donc montré que

$$\pi(x) \geqslant \frac{\log\log(x) - \log\log(2)}{\log(2)}.$$

Il s'agit d'une minoration explicite de $\pi(x)$ dont le seul mérite est de montrer que π tend vers $+\infty$. Nous allons voir que cette minoration est très mauvaise.

En étudiant les tables de nombres premiers, Gauss et Legendre ont conjecturé, vers la fin du XVIIIème siècle que

$$\pi(x) \sim_{x\to+\infty} \frac{x}{\log(x)}.$$

Cette conjecture a été démontrée indépendamment par Hadamard et de La Vallée-Poussin en 1896, un siècle plus tard.

Remarque. On peut montrer que l'équivalent de $\pi(x)$ conjecturé par Gauss et Legendre est équivalent à $p_n \sim_{n\to+\infty} n\log(n)$.

2.2.1 Les fonctions de Tchebychev

L'équivalence recherchée $x \sim \pi(x)\log(x)$ suggère qu'il peut être intéressant de compter les nombres premiers en les pondérant par leur logarithme. C'est une bonne raison pour définir les quantités suivantes, pour $x \in \mathbb{R}$:

$$\theta(x) = \sum_{p\leqslant x} \log(p)$$
$$\psi(x) = \sum_{p^n\leqslant x} \log(p).$$

Remarquons que la fonction θ est la fonction sommatoire de la fonction arithmétique $\mathbb{1}_{\mathcal{P}}\log$, alors que la fonction ψ est la fonction sommatoire de la fonction de von Mangoldt Λ.

Le résultat suivant montre qu'étudier la fonction π revient à étudier les fonctions θ et ψ.

Théorème 2.6. *Soient $0 < A \leqslant B$ deux nombres réels. Les assertions suivantes sont équivalentes :*

(i) il existe une fonction $\varepsilon : \mathbb{R} \to \mathbb{R}_+$ telle que $\lim\limits_{+\infty} \varepsilon = 0$ et

$$Ax - x\varepsilon(x) \leqslant \psi(x) \leqslant Bx + x\varepsilon(x);$$

(ii) il existe une fonction $\varepsilon : \mathbb{R} \to \mathbb{R}_+$ telle que $\lim\limits_{+\infty} \varepsilon = 0$ et

$$Ax - x\varepsilon(x) \leqslant \theta(x) \leqslant Bx + x\varepsilon(x);$$

(iii) il existe une fonction $\varepsilon : \mathbb{R} \to \mathbb{R}_+$ *telle que* $\lim_{+\infty} \varepsilon = 0$ *et*

$$A\frac{x}{\log(x)} - \frac{x}{\log(x)}\varepsilon(x) \leqslant \pi(x) \leqslant B\frac{x}{\log(x)} + \frac{x}{\log(x)}\varepsilon(x).$$

Démonstration. Commençons par vérifier l'équivalence entre (i) et (ii). On a clairement $\theta(x) \leqslant \psi(x)$ pour tout $x \in \mathbb{R}$. De plus

$$\psi(x) - \theta(x) = \sum_{\substack{p^n \leqslant x \\ n \geqslant 2}} \log(p) \leqslant \sum_{p \leqslant \sqrt{x}} \log(p) \left(\left\lfloor \frac{\log(x)}{\log(p)} \right\rfloor - 1 \right)$$

car $p^n \leqslant x \Leftrightarrow n\log(p) \leqslant \log(x) \Leftrightarrow n \leqslant \left\lfloor \frac{\log(x)}{\log(p)} \right\rfloor$. On en déduit que

$$0 \leqslant \psi(x) - \theta(x) \leqslant \log(x) \sum_{p \leqslant \sqrt{x}} \leqslant \sqrt{x}\log(x)$$

pour $x > 0$, ce qui implique l'équivalence recherchée.

Supposons (ii) et posons $g = \mathbb{1}_{\mathcal{P}} \log$ de sorte que $\theta = M_g$. Pour $x > 1$, le lemme de sommation par parties implique, en choisissant $1 < \alpha < 2$,

$$\begin{aligned} \pi(x) &= \sum_{\alpha < n \leqslant x} g(n)\log(n)^{-1} = \frac{\theta(x)}{\log(x)} - \frac{\theta(\alpha)}{\log(\alpha)} + \int_\alpha^x \frac{\theta(t)}{t\log^2(t)}\,dt \\ &= \frac{\theta(x)}{\log(x)} + \int_2^x \frac{\theta(t)}{t\log^2(t)}\,dt. \end{aligned}$$

Sous l'hypothèse (ii), on peut trouver un réel $B_1 > B$ tel que $\theta(x) \leqslant B_1 x$ pour tout $x \geqslant 2$. On en conclut que

$$\left| \int_2^x \frac{\theta(t)}{t\log^2(t)}\,dt \right| \leqslant B_1 \int_2^x \frac{dt}{\log^2(t)}.$$

Comme $\frac{1}{\log^2(t)} =_{+\infty} o(\frac{\log(t)-1}{\log^2(t)})$, et que l'intégrale de la fonction $\frac{\log -1}{\log^2}$ diverge, on en conclut que

$$\int_2^x \frac{dt}{\log^2(t)} =_{+\infty} o\left(\int_2^x \frac{\log(t)-1}{\log^2(t)}\,dt \right) = o\left(\frac{x}{\log(x)} \right).$$

Ceci prouve l'assertion (iii).

Enfin supposons que (iii) est vérifiée. On a $\theta = M_{h\log}$ où $h = \mathbb{1}_{\mathcal{P}}$ est la fonction indicatrice de l'ensemble des nombres premiers. Par sommation par parties, on obtient cette fois, pour $1 < \alpha < 2$,

$$\theta(x) = \pi(x)\log(x) - \pi(\alpha)\log(\alpha) - \int_\alpha^x \frac{\pi(t)}{t}\,dt = \pi(x)\log(x) - \int_2^x \frac{\pi(t)}{t}\,dt.$$

Sous l'hypothèse (iii), on peut trouver un réel $B_1 > B$ tel que $\pi(x) \leqslant B_1 \frac{x}{\log(x)}$ pour tout $x \geqslant 2$. Comme $\log(t)^{-1} =_{+\infty} o(1)$, on en déduit que

$$\theta(x) - \pi(x)\log(x) =_{+\infty} o(x)$$

ce qui implique (ii). □

2.2.2 L'encadrement de $\psi(x)$

Théorème 2.7 (Tchebychev)**.** *Pour tout réel $x \geqslant 2$, on a*

$$x\log(2) - 1 - 3\log(x) \leqslant \psi(x) \leqslant 2x\log(2) + \frac{3}{\log(2)}(\log x)^2.$$

On déduit donc des théorème 2.6 et 2.7 qu'il existe une fonction $\varepsilon : \mathbb{R} \to \mathbb{R}_+$ tendant vers 0 en $+\infty$ et telle que

$$\forall x \geqslant 2, \quad (\log 2)\frac{x}{\log(x)} - \frac{x}{\log(x)}\varepsilon(x) \leqslant \pi(x) \leqslant (2\log(2))\frac{x}{\log(x)} + \frac{x}{\log(x)}\varepsilon(x).$$

Nous utiliserons le lemme suivant qui permet de remplacer une somme par une intégrale.

Lemme. *Soit $f : [1, +\infty[\to \mathbb{R}_+$ une fonction croissante. Alors pour tout réel $x \geqslant 1$, on a*

$$\int_1^x f + f(1) - f(x) \leqslant \sum_{n \leqslant x} f(n) \leqslant \int_1^x f + f(x).$$

Démonstration. Remarquons déjà que la fonction f est croissante. Elle est donc mesurable et bornée sur tout intervalle de la forme $[1, x]$. Elle est donc intégrable sur de tels intervalles.

Pour tout entier $n \geqslant 1$, on a $f(n) \leqslant \int_n^{n+1} f \leqslant f(n+1)$. On en conclut que

$$\sum_{n \leqslant x} f(n) = \sum_{n \leqslant \lfloor x \rfloor - 1} f(n) + f(\lfloor x \rfloor) \leqslant \sum_{n \leqslant \lfloor x \rfloor - 1} \int_n^{n+1} f + f(x) = \int_1^x f + f(x).$$

Concernant l'autre inégalité, on a

$$\begin{aligned}\sum_{n \leqslant x} f(n) = \sum_{n=2}^{\lfloor x \rfloor} f(n) + f(1) &\geqslant \int_1^{\lfloor x \rfloor} f + f(1) \geqslant \int_1^x f + f(1) - \int_{\lfloor x \rfloor}^x f \\ &\geqslant \int_1^x f + f(1) - f(x)(x - \lfloor x \rfloor) \geqslant \int_1^x f + f(1) - f(x).\end{aligned}$$

□

Preuve du théorème 2.7. On part de l'égalité $\log = \Lambda * \mathbb{1}$, équivalente à l'égalité $\Lambda = \log * \mu$. L'idée est de remplacer la fonction μ par une fonction v plus simple à utiliser mais vérifiant l'égalité $\sum_{n \leqslant x} \frac{v(n)}{n} = 0$. On pose pour cela

$$v(n) = \begin{cases} 1 & \text{si } n = 1 \\ -2 & \text{si } n = 2 \\ 0 & \text{si } n \geqslant 3. \end{cases}$$

On calcule alors la fonction sommatoire Z de $v * \log = v * \mathbb{1} * \Lambda = w * \Lambda$ où w est la fonction arithmétique $v * \mathbb{1}$. En utilisant la formule (2.1), on obtient

$$Z(x) = \sum_{d \leqslant x} v(d) M_{\log}\left(\frac{x}{d}\right) = M_{\log}(x) - 2M_{\log}\left(\frac{x}{2}\right).$$

Par ailleurs, on peut calculer explicitement w ce qui nous donne

$$w(n) = \begin{cases} 1 & \text{si } n \text{ est impair} \\ 1 - 2 = -1 & \text{si } n \text{ est pair} \end{cases}$$

de sorte que

$$Z(x) = \sum_{d \leqslant x} (-1)^{d+1} \psi\left(\frac{x}{d}\right) = \psi(x) - \psi\left(\frac{x}{2}\right) + \psi\left(\frac{x}{3}\right) + \cdots$$

Il faut maintenant obtenir un encadrement correct de $M_{\log}$. Comme la fonction log est croissante, une comparaison avec une intégrale nous donne, pour $x \geqslant 1$,

$$\int_1^x \log - \log(x) \leqslant M_{\log}(x) \leqslant \int_1^x \log + \log(x).$$

Comme $\int_1^x \log = x \log(x) - x + 1$, on en déduit

$$\begin{aligned} x \log(x) - x + 1 - \log(x) - 2\left(\frac{x}{2}\log\frac{x}{2} - \frac{x}{2} + 1 + \log\frac{x}{2}\right) &\leqslant Z(x) \\ &\leqslant x \log(x) - x + 1 + \log(x) - 2\left(\frac{x}{2}\log\frac{x}{2} - \frac{x}{2} + 1 - \log\frac{x}{2}\right). \end{aligned}$$

Ce qui donne

$$x \log(2) - 1 - 3\log(x) + 2\log(2) \leqslant Z(x) \leqslant x \log(2) - 1 + 3\log(x) - 2\log(2).$$

Nous pouvons à présent utiliser les bornes obtenues sur Z pour en déduire des bornes sur la fonction ψ. En effet, par croissance de la fonction ψ, on a $\psi(\frac{x}{n}) - \psi(\frac{x}{n+1}) \geqslant 0$ pour tout réel $x \geqslant 1$ et tout entier $n \geqslant 1$. En particulier, pour tout réel $x \geqslant 2$,

$$\psi(x) - \psi(\tfrac{x}{2}) \leqslant Z(x) \leqslant \psi(x).$$

On en déduit immédiatement la borne inférieure

$$\psi(x) \geqslant x\log(2) - 1 - 3\log(x) + 2\log(2).$$

Par ailleurs, on a les inégalités suivantes

$$\begin{aligned}
\psi(x) - \psi(\tfrac{x}{2}) &\leqslant x\log(2) - 1 + 3\log(x)\\
\psi(\tfrac{x}{2}) - \psi(\tfrac{x}{4}) &\leqslant \tfrac{x}{2}\log(2) - 1 + 3\log(\tfrac{x}{2})\\
&\vdots\\
\psi(\tfrac{x}{2^n}) - \psi(\tfrac{x}{2^{n+1}}) &\leqslant \tfrac{x}{2^n}\log(2) - 1 + 3\log(\tfrac{x}{2^n})\\
&\vdots
\end{aligned}$$

En sommant ces inégalités pour n allant de 0 à $\ell = \max\{k \mid 2 \leqslant \frac{x}{2^k}\}$, on obtient

$$\psi(x) \leqslant \left(\sum_{n\geqslant 0}\frac{1}{2^n}\right) x\log(2) + 3(\ell+1)\log(x) - (\ell+1).$$

Comme $\ell = \lfloor \frac{\log(x)}{\log(2)} \rfloor - 1$, on a finalement

$$\psi(x) \leqslant 2x\log(2) + \frac{3}{\log(2)}(\log x)^2. \qquad \square$$

2.3 Quelques applications des estimées de Tchebychev

2.3.1 La constante d'Euler

Le lemme de sommation par parties nous donne la description suivante des sommes harmoniques. Pour $x \geqslant 1$ réel,

$$\begin{aligned}
\sum_{n\leqslant x}\frac{1}{n} &= \frac{\lfloor x\rfloor}{x} - \frac{\lfloor \frac{1}{2}\rfloor}{\frac{1}{2}} - \int_{\frac{1}{2}}^{x} -\frac{\lfloor t\rfloor}{t^2}\,dt = \frac{\lfloor x\rfloor}{x} + \int_1^x \frac{\lfloor t\rfloor}{t^2}\,dt\\
&= 1 - \frac{\{x\}}{x} + \int_1^x \frac{t-\{t\}}{t^2}\,dt\\
&= \log(x) + 1 - \frac{\{x\}}{x} - \int_1^x \frac{\{t\}}{t^2}\,dt.
\end{aligned}$$

Cette dernière écriture est très intéressante car la fonction $t \mapsto \frac{\{t\}}{t^2}$ est intégrable sur $[1,+\infty[$ de sorte que

$$\sum_{n\leqslant x}\frac{1}{n} =_{+\infty} \log(x) + \gamma + O(x^{-1})$$

où $\gamma = 1 - \int_1^{+\infty} \frac{\{t\}}{t^2}\, dt$. Le réel γ est appelé la *constante d'Euler*. On sait très peu de choses sur ce nombre réel, pas même s'il est irrationnel. Il apparaît souvent dans les formules faisant intervenir la fonction ζ et la suite des nombres premiers.

Soit $s \in \mathbb{C}$ tel que $\mathrm{Re}(s) > 1$. En appliquant le lemme de sommation par parties aux sommes partielles des nombres n^{-s}, on montre que

$$\begin{aligned}\zeta(s) &= \lim_{x\to+\infty} \left(\frac{\lfloor x \rfloor}{x^s} + s\int_1^{+\infty} \frac{\lfloor t \rfloor}{t^{s+1}}\, dt \right) = s\int_1^{+\infty} \frac{\lfloor t \rfloor}{t^{s+1}}\, dt \\ &= s\int_1^{+\infty} \frac{dt}{t^s} - s\int_1^{+\infty} \frac{\{t\}}{t^{s+1}}\, dt \\ &= \frac{1}{s-1} + 1 - s\int_1^{+\infty} \frac{\{t\}}{t^{s+1}}\, dt.\end{aligned}$$

Remarquons que la fonction $s \mapsto \{t\}t^{-(s+1)}$ est holomorphe sur $\mathbb{C}$. De plus si $a > 0$, on a $|\{t\}t^{-(s+1)}| \leqslant t^{-(a+1)}$ et $\int_1^{+\infty} t^{-(a+1)}\, dt < +\infty$. Ainsi la fonction $s \mapsto \int_1^{+\infty} \{t\}t^{-(s+1)}\, dt$ est holomorphe sur toute partie de $\mathbb{C}$ de la forme $\{s \in \mathbb{C} \mid \mathrm{Re}(s) \geqslant a\}$ et donc sur $\{s \in \mathbb{C} \mid \mathrm{Re}(s) > 0\}$. On a donc montré que la fonction ζ admet un prolongement en une fonction méromorphe sur $\{s \in \mathbb{C} \mid \mathrm{Re}(s) > 0\}$ et que ce prolongement a un unique pôle, c'est un pôle simple en 1 de résidu 1.

2.3.2 Les théorèmes de Mertens

Les résultats suivants ont été obtenus par Mertens autour de 1874.

Théorème 2.8. *On a les comportements asymptotiques suivants pour $x \in \mathbb{R}$:*

$$(i) \sum_{n\leqslant x} \frac{\Lambda(n)}{n} =_{+\infty} \log(x) + O(1); \tag{2.2}$$

$$(ii) \sum_{p\leqslant x} \frac{\log(p)}{p} = \log(x) + O(1); \tag{2.3}$$

$$(iii) \sum_{p\leqslant x} \frac{1}{p} = \log\log(x) + \gamma + \sum_p \left[\log\left(1 - \frac{1}{p}\right) + \frac{1}{p} \right] + O(\log(x)^{-1}); \tag{2.4}$$

$$(iv) \prod_{p\leqslant x} \left(1 - \frac{1}{p}\right) \sim_{+\infty} \frac{e^{-\gamma}}{\log(x)}. \tag{2.5}$$

La formule (2.3) est également connue sous le nom de *premier théorème de Mertens* et la formule (2.5) sous le nom de *formule de Mertens*.

Démonstration. Commençons par comparer les formules (i) et (ii). On utilise l'encadre-

ment

$$0 \leqslant \sum_{n\leqslant x} \frac{\Lambda(n)}{n} - \sum_{p\leqslant x} \frac{\log(p)}{p} \leqslant \sum_{\substack{p^m\leqslant x\\ m\geqslant 2}} \frac{\log(p)}{p^m}$$
$$\leqslant \sum_p \log(p)\left(\frac{1}{p^2}+\cdots\right) = \sum_p \log(p)\frac{1}{p(p-1)} < +\infty$$

qui montre que (i) implique (ii).

Montrons (i). On utilise pour cela la formule $\log = \Lambda * \mathbb{1}$. Ainsi

$$\sum_{n\leqslant x}(\Lambda*\mathbb{1})(n) = \sum_{n\leqslant x}\log(n) = M_{\log}(x) = x\log(x)+O(x)$$

et par ailleurs

$$\sum_{n\leqslant x}(\Lambda*\mathbb{1})(n) = \sum_{d\leqslant x}\Lambda(d)M_{\mathbb{1}}\left(\frac{x}{d}\right) = \sum_{d\leqslant x}\Lambda(d)\left\lfloor\frac{x}{d}\right\rfloor = x\sum_{d\leqslant x}\frac{\Lambda(d)}{d} - \sum_{d\leqslant x}\Lambda(d)\left\{\frac{x}{d}\right\}.$$

Or on a $\left|\sum_{d\leqslant x}\Lambda(d)\{\frac{x}{d}\}\right| \leqslant \psi(x)$, donc d'après le théorème de Tchebychev, ce dernier terme est en $O(x)$. On en conclut que

$$x\sum_{d\leqslant x}\frac{\Lambda(d)}{d} = x\log(x)+O(1)$$

et le résultat.

Il est immédiat de vérifier que la formule (iii) implique la formule (iv) en passant à l'exponentielle. Il reste donc à vérifier (iii). Posons, pour $x\in\mathbb{R}$,

$$S(x) = \sum_{p\in x}\frac{\log(p)}{p} =_{+\infty} \log(x)+O(1)$$

où le comportement asymptotique est donné par (ii). Pour $\delta\geqslant 0$ réel, et $x\in\mathbb{R}$, on pose également

$$C_\delta(x) = \sum_{p\leqslant x}\frac{1}{p^{1+\delta}}.$$

En utilisant la formule de sommation par parties avec $1<\alpha<2$, on obtient, pour $x\in\mathbb{R}$,

$$C_0(x) = \sum_{\alpha<p\leqslant x}\frac{1}{p} = \frac{S(x)}{\log(x)} + \int_\alpha^x \frac{S(t)}{t\log^2(t)}\,dt = \frac{S(x)}{\log(x)} + \int_2^x \frac{S(t)}{t\log^2(t)}\,dt.$$

On note alors r la fonction $S-\log$ que l'on a prouvé plus haut être bornée. On a

$$C_0(x) = 1 + \frac{r(x)}{\log(x)} + \int_2^x \frac{dt}{t\log(t)} + \int_2^x \frac{r(t)}{t\log^2(t)}\,dt$$
$$= 1 + \frac{r(x)}{\log(x)} + \log\log(x) - \log\log(2) + \int_2^x \frac{r(t)}{t\log^2(t)}\,dt.$$

L'intégrale $\int_2^x \frac{r(t)}{t\log^2(t)}\,dt$ converge car r est bornée et

$$\int_2^x \frac{dt}{t\log^2(t)} = \log(2)^{-1} - \log(x)^{-1}.$$

On peut donc écrire

$$C_0(x) =_{+\infty} \log\log(x) + A + O(\log(x)^{-1}) \tag{2.6}$$

où $A = 1 - \log\log(2) + \int_2^{+\infty} \frac{r(t)}{t\log^2(t)}\,dt$. Il reste donc essentiellement à prouver que

$$A = \gamma + \sum_p \left[\log\left(1 - \frac{1}{p}\right) + \frac{1}{p}\right].$$

Pour cela nous allons faire varier δ. Si $\delta > 0$, la fonction C_δ a une limite en $+\infty$ que nous notons $C_\delta(\infty)$. De plus, par sommation par parties, on obtient, pour $x \geqslant 2$,

$$C_\delta(x) = x^{-\delta}C_0(x) + \delta\int_2^x \frac{C_0(t)}{t^{1+\delta}}\,dt.$$

En utilisant l'estimation (2.6), on voit que l'intégrale apparaissant sur la droite est convergente et on obtient

$$C_\delta(\infty) = \delta\int_2^{+\infty} \frac{C_0(t)}{t^{1+\delta}}\,dt.$$

L'idée est à présent de faire apparaître A en étudiant le comportement de $C_\delta(\infty)$ quand δ tend vers 0. Pour cela, posons, pour $x \geqslant 2$,

$$E(x) = C_0(x) - \log\log(x) - A =_{+\infty} O(\log(x)^{-1}).$$

Il existe donc un réel $B > 0$ tel que $E(x) \leqslant B\log(x)^{-1}$ pour $x \geqslant 2$. On en déduit

$$\delta\left|\int_2^{+\infty} \frac{E(t)}{t^{1+\delta}}\,dt\right| \leqslant B\delta\int_2^{+\infty} \frac{dt}{\log(t)t^{1+\delta}} = B\delta\int_{\delta\log(2)}^{+\infty} e^{-u}\frac{du}{u}.$$

Comme $e^{-u}u^{-1} \sim_0 u^{-1}$, on en déduit que

$$\delta\int_{\delta\log(2)}^{+\infty} e^{-u}\frac{du}{u} \sim_0 \delta\int_{\delta\log(2)}^{1} \frac{du}{u} = -\delta(\log(\delta) + \log\log(2)).$$

Ainsi

$$C_\delta(\infty) =_0 \delta\int_2^{+\infty} \frac{\log\log(t)}{t^{1+\delta}}\,dt + A\delta\int_2^{+\infty} \frac{dt}{t^{1+\delta}} + o(1).$$

On peut préférer réécrire cette expression en intégrant à partir de 1 pour obtenir

$$\begin{aligned} C_\delta(\infty) &=_0 \delta\int_1^{+\infty} \frac{\log\log(t)}{t^{1+\delta}}\,dt + A\delta\int_1^{+\infty} \frac{dt}{t^{1+\delta}} + o(1) = \delta\int_1^{+\infty} \frac{\log\log(t)}{t^{1+\delta}}\,dt + A + o(1) \\ &=_0 \int_0^{+\infty} e^{-u}\log\left(\frac{u}{\delta}\right)du + A + o(1) \\ &=_0 \int_0^{+\infty} e^{-u}\log(u)\,du + A - \log(\delta) + o(1). \end{aligned}$$

Pour $x \geqslant 2$, la somme partielle $C_\delta(x)$ est proche du logarithme d'une somme partielle harmonique. En effet l'inégalité

$$\forall |x| \leqslant \frac{1}{2}, \quad |\log(1-x)+x| \leqslant |x|^2$$

montre que la série de fonctions $\delta \mapsto \sum_p [\log(1-p^{-\delta})+p^{-\delta}]$ converge uniformément sur $[1,+\infty[$ de sorte que

$$\sum_p \left[\log\left(1-\frac{1}{p}\right)+\frac{1}{p}\right] = \lim_{\delta\to 0}(-\log(\zeta(1+\delta))+C_\delta(\infty)).$$

Comme on sait par ailleurs que $\zeta(1+\delta) =_0 \delta^{-1}+O(1)$, on en déduit que $\log(\zeta(1+\delta)) =_0 -\log(\delta)+O(\delta)$ et donc on obtient

$$\sum_p \left[\log\left(1-\frac{1}{p}\right)+\frac{1}{p}\right] = \int_0^{+\infty} e^{-u}\log(u)\,du + A.$$

Il reste donc à prouver l'égalité $\int_0^{+\infty} e^{-u}\log(u)\,du = -\gamma$.

Pour prouver cette dernière égalité, on peut considérer la suite de fonctions $(f_n)_{n\geqslant 1}$ de $[0,+\infty[$ vers $\mathbb{R}$ définie par $f_n(t)=0$ si $t \geqslant n$ et $f_n(t)=(1-tn^{-1})^n$ si $t \leqslant n$. Cette suite de fonction converge vers $t \mapsto e^{-t}$ tout en étant dominée par cette fonction. On en conclut que

$$\int_0^{+\infty} e^{-u}\log(u)\,du = \lim_{n\to+\infty}\int_0^{+\infty} f_n(u)\log(u)\,du.$$

Par ailleurs un changement de base montre que

$$\int_0^{+\infty} f_n(u)\log(u)\,du = \int_0^{n} f_n(u)\log(u)\,du = \frac{n}{n+1}\left(\log(n)-\sum_{k=0}^{n}\frac{1}{k+1}\right).$$

On en déduit le résultat. □

Le nombre réel $A=\gamma+\sum_p[\log(1+p^{-1})+p^{-1}]$ est appelé *constante de Mertens*.

2.4 Quelques comportements en moyenne

Pour conclure ce chapitre, donnons quelques illustrations du comportement en moyenne des fonctions arithmétiques faisant intervenir la constante d'Euler.

Si $n \in \mathbb{N}^*$, on pose

$$\omega(n) = \mathrm{Card}\{p \in \mathcal{P} \mid p \mid n\}$$
$$\Omega(n) = \mathrm{Card}\{(p,m) \in \mathcal{P}\times\mathbb{N}^* \mid p^m \mid n\}.$$

Théorème 2.9.

$$(i)\ \sum_{n\leqslant x}\omega(n) =_{+\infty} x\log\log(x) + Ax + O\left(\frac{x}{\log(x)}\right); \tag{2.7}$$

$$(ii)\ \sum_{n\leqslant x}\Omega(n) =_{+\infty} x(\log\log(x) + A + \sum_{p}\frac{1}{p(p-1)} + o(x); \tag{2.8}$$

$$(iii)\ \sum_{n\leqslant x} d(n) =_{+\infty} x\log(x) + (2\gamma-1)x + O(\sqrt{x}). \tag{2.9}$$

Démonstration. Commençons par prouver l'équivalent (i). On a

$$\sum_{n\leqslant x}\omega(n) = \sum_{n\leqslant x}\sum_{p|n} 1 = \sum_{p\leqslant x}\left\lfloor\frac{x}{p}\right\rfloor = \sum_{p\leqslant x}\frac{x}{p} - \sum_{p\leqslant x}\left\{\frac{x}{p}\right\} = x\sum_{p\leqslant x}\frac{1}{p} - \sum_{p\leqslant x}\left\{\frac{1}{p}\right\}.$$

D'après le théorème de Tchebychev, on a $\sum_{p\leqslant x}\{xp^{-1}\} \leqslant \pi(x) =_{+\infty} O(x\log(x)^{-1})$. Ainsi la formule de Mertens nous donne

$$\sum_{n\leqslant x}\omega(n) = x\log\log(x) + Ax + O\left(\frac{x}{\log(x)}\right).$$

Passons au point (ii). Encore une fois, on utilise le fait que des sommes sur les nombres premiers ou sur les puissances de nombres de premiers diffèrent peu.

$$\begin{aligned}\sum_{n\leqslant x}\Omega(n) &= \sum_{n\leqslant x}\sum_{\substack{p,k\\ p^k|n}} 1 = \sum_{n\leqslant x}\left(\omega(n) + \sum_{\substack{p,k\geqslant 2\\ p^k|n}} 1\right)\\ &= \sum_{n\leqslant x}\omega(n) + \sum_{\substack{p,k\geqslant 2\\ p^k\leqslant x}}\left\lfloor\frac{x}{p^k}\right\rfloor = \sum_{n\leqslant x}\omega(n) + x\sum_{\substack{p,k\geqslant 2\\ p^k\leqslant x}}\frac{1}{p^k} - \sum_{\substack{p,k\geqslant 2\\ p^k\leqslant x}}\left\{\frac{x}{p^k}\right\}.\end{aligned}$$

D'une part

$$\sum_{p,k\geqslant 2}\frac{1}{p} = \sum_{p}\frac{1}{p(p-1)} < +\infty.$$

D'autre part on a

$$\sum_{\substack{p,k\geqslant 2\\ p^k\leqslant x}}\left\{\frac{x}{p^k}\right\} \leqslant \sum_{\substack{p,k\geqslant 2\\ p^k\leqslant x}}\frac{\log(p)}{\log(p)} \leqslant \frac{\psi(x)-\theta(x)}{\log(2)} = O(\sqrt{x}\log(x))$$

comme on l'a déjà vu. On en déduit le résultat.

Le point (iii) est une illustration de la *méthode de l'hyperbole*. On peut en effet écrire

$$\sum_{n\leqslant x} d(n) = \sum_{\substack{(d_1,d_2)\in(\mathbb{N}^*)^2\\ d_1d_2\leqslant x}} 1.$$

Il s'agit donc de compter le nombre de point à coordonnées entières et strictement positives se trouvant dans la zone située sous l'hyperbole d'équation $d_1 d_2 = x$.

$$\begin{aligned}
\sum_{n\leqslant x} d(n) &= \sum_{d_1\leqslant\sqrt{x}} \sum_{d_2\leqslant\frac{x}{d_1}} 1 + \sum_{d_2\leqslant\sqrt{x}} \sum_{d_1\leqslant\frac{x}{d_1}} 1 - \sum_{\substack{d_1\leqslant\sqrt{x}\\ d_2\leqslant\sqrt{x}}} 1 \\
&= 2\sum_{d\leqslant\sqrt{x}} \left\lfloor \frac{x}{d} \right\rfloor - \lfloor\sqrt{x}\rfloor^2 = 2\sum_{d\leqslant\sqrt{x}} \frac{x}{d} + O(\sqrt{x}) - x \\
&= 2x(\log(\sqrt{x}) + \gamma + O(\sqrt{x}^{-1})) - x + O(\sqrt{x}) \\
&= x\log(x) + (2\gamma - 1)x + O(\sqrt{x}).
\end{aligned}$$

□

Chapitre 3

Caractères

3.1 Le symbole de Legendre

3.1.1 Motivations

Fixons $m \in \mathbb{N}^*$. On cherche à résoudre des équations algébriques dans l'anneau $\mathbb{Z}/m\mathbb{Z}$. Le cas des équations de degré 1 fait appel à des techniques déjà bien rodées dans ce cours. En effet, soit $a, b \in \mathbb{Z}$ et cherchons à résoudre l'équation $\overline{a}x = \overline{b}$ dans $\mathbb{Z}/m\mathbb{Z}$, ce qui revient à chercher les entiers x tels qu'il existe $k \in \mathbb{Z}$ vérifiant $ax = b + km$. Soit $\delta = a \wedge m$. On a déjà vu que cette équation a des solutions si et seulement si δ divise b. Supposons que c'est le cas et posons $a = \delta a'$, $b = \delta b'$ et $m = \delta m'$ de sorte que a' et m' sont premiers entre eux. Dans ce cas $\overline{a'} \in (\mathbb{Z}/m\mathbb{Z})^\times$ et on est ramené à résoudre l'équation $\overline{a'}x = \overline{b'}$ dans $\mathbb{Z}/m'\mathbb{Z}$ dont l'unique solution est $\overline{a'}^{-1}\overline{b'}$ que l'on sait résoudre explicitement. On a donc montré que l'équation $\overline{a}x = \overline{b}$ a exactement δ solutions dans $\mathbb{Z}/m\mathbb{Z}$.

Passons à présent aux équations de degré 2 et commençons par le cas $x^2 \equiv a\,[m]$. Le théorème des restes nous invite à factoriser m en produit de facteurs premiers, c'est-à-dire à écrire $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ où $p_1 < \cdots < p_r$ sont des nombres premiers et les α_i des éléments de $\mathbb{N}^*$. La congruence $x^2 \equiv a\,[m]$ est donc équivalente au système de congruences

$$\forall 1 \leqslant i \leqslant r, \quad x^2 \equiv a\,[p_i^{\alpha_i}].$$

On s'est donc ramené à étudier le cas où $m = p^k$ avec p premier.

Commençons par considérer le cas où $a = 0$, alors $p^k \mid x^2$ si et seulement si $p^{\lceil \frac{k}{2} \rceil} \mid x$. On peut donc supposer $a = \lambda p^\nu$ avec $0 \leqslant \nu < k$ et $p \nmid \lambda$. Alors

$$x^2 \equiv a\,[p^k] \Leftrightarrow x^2 = p^\nu(\lambda + \ell p^{k-\nu})$$

pour un $\ell \in \mathbb{Z}$. Si ν est impair, il n'y a pas de solution mais si ν est pair et $\nu = 2\nu'$, $x \in \mathbb{Z}$ vérifie $x^2 \equiv a\,[p^k]$ si et seulement si $x = p^{\nu'}x_1$ avec $x_1^2 \equiv \lambda\,[p]^{k-\nu}$. On s'est donc ramené au cas où $p \nmid a$. Ce dernier est cas traité par le résultat suivant.

Théorème 3.1. *Soit p un nombre premier et soient $k \in \mathbb{N}^*$ et $a \in \mathbb{Z}$ tels que $a \wedge p = 1$.*

(i) Si $p = 2$, la congruence $x^2 \equiv a\,[p^k]$ a des solutions si et seulement si $k = 1$ ou $k = 2$ et $a \equiv 1\,[4]$ ou $k \geqslant 3$ et $a \equiv 1\,[8]$.

(ii) Si p est impair, la congruence $x^2 \equiv a\,[p^k]$ a des solutions si et seulement si $a^{\frac{p-1}{2}} \equiv 1\,[p]$.

Démonstration. Commençons par traiter le cas où $p = 2$. Le cas où $k = 1$ est immédiat. Si $x \in \mathbb{Z}$ est impair, alors $x^2 \equiv 1\,[4]$. La condition est donc nécessaire. Elle est suffisante car 1 est évidemment solution de $x^2 \equiv 1\,[4]$. Si $k \geqslant 3$ et $x^2 \equiv a\,[2^k]$, on a en particulier $x^2 \equiv a\,[8]$. Comme tous les éléments du groupes $(\mathbb{Z}/8\mathbb{Z})^\times$ sont d'ordre 2, on en conclut que $x^2 \equiv 1\,[8]$ et donc $a \equiv 1\,[8]$ est une condition nécessaire. Cette condition est suffisante. En effet, on sait que le noyau du morphisme de réduction $(\mathbb{Z}/2^k\mathbb{Z})^\times \to (\mathbb{Z}/4\mathbb{Z})^\times$ est engendré par la classe de 5. Si $a \equiv 1\,[8]$, on peut donc écrire $\overline{a} = \overline{5}^m$ pour un certain $m \in \mathbb{N}$ dans $\mathbb{Z}/2^k\mathbb{Z}$. Cherchons alors $\overline{x}$ sous la forme $\overline{5}^r$ pour un certain entier $r \in \mathbb{Z}$. On a alors

$$5^{2r} \equiv 5^m\,[2^k] \Leftrightarrow 2r \equiv m\,[2^{k-2}].$$

Comme $a \equiv 1\,[8]$, l'entier m est pair et cette congruence a une solution.

Supposons désormais p premier impair. Remarquons que si $x^2 \equiv a\,[p^k]$, alors $x^2 \equiv\,[p]$ et donc $a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1\,[p]$ d'après le petit théorème de Fermat. La condition est donc nécessaire. Réciproquement supposons $a^{\frac{p-1}{2}} \equiv 1\,[p]$. On sait que le groupe $(\mathbb{Z}/p^k\mathbb{Z})^\times$ est cyclique, fixons g un générateur de ce groupe et fixons $m \in \mathbb{N}$ tel que $\overline{a} = g^m$. La relation $a^{\frac{p-1}{2}} \equiv 1\,[p]$, nous donne $\frac{p-1}{2}m \equiv 0\,[p-1]$, c'est-à-dire m pair. Il suffit donc de choisir $\overline{x} = g^{\frac{m}{2}}$ pour obtenir une solution. □

Au vu des considérations précédentes, il paraît judicieux d'introduire la définition suivante. Si $m \in \mathbb{N}^*$, un entier $a \in \mathbb{Z}$ est dit *résidu quadratique* modulo m si l'équation $x^2 \equiv a\,[m]$ admet une solution dans $\mathbb{Z}$.

Nous avons en particulier prouvé que si p est nombre premier impair, les résidus quadratiques modulo p sont les entiers a tels que $p \mid a$ ou $a^{\frac{p-1}{2}} \equiv 1\,[p]$.

3.1.2 Définition et propriétés

Soit p un nombre premier impair et soit $a \in \mathbb{Z}$. On appelle *symbole de Legendre* de a et p la quantité

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } p \text{ divise } a; \\ 1 & \text{si } a \text{ est résidu quadratique modulo } p \text{ et } p \nmid a; \\ -1 & \text{sinon.} \end{cases}$$

Exemple. Dans $\mathbb{Z}/5\mathbb{Z}$, on a

$$(\mathbb{Z}/5\mathbb{Z})^\times = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$$

avec $\overline{2}^2 = \overline{3}^2 = \overline{4}$ et $\overline{1}^2 = \overline{4}^2 = \overline{1}$ de sorte que

$$\left(\frac{a}{5}\right) = \begin{cases} 0 & \text{si } a \equiv 0\,[5]; \\ 1 & \text{si } a \equiv 1 \text{ ou } 4\,[5]; \\ -1 & \text{si } a \equiv 2 \text{ ou } 3\,[5]. \end{cases}$$

Théorème 3.2. *Soit p un nombre premier impair. Soient a et b deux entiers.*

(i) si $a \equiv b\,[p]$, alors $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$;

(ii) on a $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\,[p]$;

(iii) on a $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$;

(iv) il y a exactement $\frac{p-1}{2}$ résidus quadratiques premiers à p modulo p et $\frac{p-1}{2}$ non résidus quadratiques modulo p ;

(v) on a $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & si\ p \equiv 1\,[4] \\ -1 & si\ p \equiv 3\,[4] \end{cases}$.

Démonstration. Le point (i) est évident. Prouvons le (ii). Si $p \mid a$ ou si a est résidu quadratique modulo p, cette formule a déjà été prouvée dans la section précédente. Supposons donc a non résidu quadratique. En particulier $p \nmid a$. De plus le petit théorème de Fermat implique que $\overline{a}^{p-1} = \overline{1}$ dans $\mathbb{Z}/p\mathbb{Z}$. Ainsi l'élément $\overline{a}^{\frac{p-1}{2}}$ est de carré égal à $\overline{1}$ dans $\mathbb{Z}/p\mathbb{Z}$. Comme $\mathbb{Z}/p\mathbb{Z}$ est un corps commutatif, le polynôme $X^2 - \overline{1}$ a au plus deux solutions dans $\mathbb{Z}/p\mathbb{Z}$ de sorte que $\overline{a} \in \{\pm\overline{1}\}$. Comme a n'est pas résidu quadratique, on a $\overline{a}^{\frac{p-1}{2}} = -\overline{1}$ et donc

$$a^{\frac{p-1}{2}} \equiv -1 = \left(\frac{a}{p}\right)\,[p].$$

Le point (iii) est alors une conséquence immédiate de (ii). En effet, on en déduit que $\left(\frac{ab}{p}\right) \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\,[p]$. Comme p est impair, on a, pour x et y dans $\{0, \pm 1\}$, $x \equiv y\,[p]$ si et seulement si $x = y$. Ainsi $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

Pour le point (iv), on remarque que, puisque $\mathbb{Z}/p\mathbb{Z}$ est un corps commutatif, le polynôme $X^{\frac{p-1}{2}} - 1$ a au plus $\frac{p-1}{2}$ solutions dans $\mathbb{Z}/p\mathbb{Z}$. Ainsi il y a au plus $\frac{p-1}{2}$ résidus quadratiques modulo p qui sont premiers à p. Par ailleurs le morphisme de groupes $(\mathbb{Z}/p\mathbb{Z}_p)^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$ défini par $x \mapsto x^{\frac{p-1}{2}}$ est un morphisme de groupes dont l'image est contenu dans $\{\pm\overline{1}\}$. Le cardinal de son noyau est donc supérieur ou égal à $\frac{p-1}{2}$. Comme son noyau est par ailleurs l'ensemble des résidus quadratiques modulo p premiers à p, on en déduit le résultat.

Le point (v) est une conséquence de la congruence $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}}\,[p]$ et du fait que deux éléments de $\{\pm 1\}$ sont égaux si et seulement si ils sont congrus modulo p (car $p \geqslant 3$). □

3.1.3 Une autre description du symbole de Legendre

Soit p un nombre premier impair. Si $a \in \mathbb{Z}$, on appelle *résidu minimal absolu* de a modulo p l'unique entier $\tilde{a}$ tel que $a \equiv \tilde{a}\,[p]$ et $-\frac{p-1}{2} \leqslant \tilde{a} \leqslant \frac{p-1}{2}$. Cet entier existe. En effet si r désigne le reste de la division euclidienne de a par p, on a $\tilde{a} = r$ si $r \leqslant \frac{p-1}{2}$ et $\tilde{a} = r - p$ si $r \geqslant \frac{p+1}{2}$.

On pose alors

$$\nu_p(a) = \mathrm{Card}(\{1 \leqslant k \leqslant \frac{p-1}{2} \mid \widetilde{ka} < 0\}).$$

Exemple. Si $p = 11$ et $a = 4$, on a

k	1	2	3	4	5
$\widetilde{4k}$	4	-3	1	5	-2

Ainsi $\nu_{11}(4) = 2$.

Théorème 3.3 (Gauss)**.** *Si $p \nmid a$, on a $\left(\frac{a}{p}\right) = (-1)^{\nu_p(a)}$.*

Démonstration. Soit $1 \leqslant k \leqslant \frac{p-1}{2}$ un entier. Posons $\widetilde{ka} = \varepsilon_k m_k$ où $\varepsilon_k \in \{\pm 1\}$ et $1 \leqslant m_k \leqslant \frac{p-1}{2}$. Supposons que $1 \leqslant k, \ell \leqslant \frac{p-1}{2}$ vérifient $m_k = m_\ell$. Alors $ka \equiv \pm \ell a\,[p]$ et donc, puisque $a \wedge p = 1$, $k \equiv \pm \ell\,[p]$. Si $k \equiv -\ell\,[p]$, on a $p \mid k + \ell$, ce qui contredit $2 \leqslant k + \ell \leqslant p - 1$. Ainsi $k \equiv \ell\,[p]$ et $k = \ell$. On en déduit que l'application $k \mapsto m_k$ est une permutation de l'ensemble $\{1, \ldots, \frac{p-1}{2}\}$. On peut donc écrire

$$\prod_{k=1}^{\frac{p-1}{2}} (ka) \equiv (-1)^{\nu_p(a)} \prod_{k=1}^{\frac{p-1}{2}} k = (-1)^{\nu_p(a)} \left(\frac{p-1}{2}\right)! \,[p].$$

Comme $\prod_{k=1}^{\frac{p-1}{2}} (ka) = a^{\frac{p-1}{2}} (\frac{p-1}{2})!$ et que $p \nmid \frac{p-1}{2}!$, on en conclut que $a^{\frac{p-1}{2}} \equiv (-1)^{\nu_p(a)}\,[p]$ et, puisque $p \geqslant 3$, on a $\left(\frac{a}{p}\right) = (-1)^{\nu_p(a)}$. □

Lorsque $a = 2$ un phénomène intéressant, que nous allons mettre à profit, se produit. Prenons par exemple $p = 13$.

k	1	2	3	4	5	6
ε_k	1	1	1	-1	-1	-1

Tous les 1 sont à gauche et tous les -1 à droite. C'est un phénomène général que nous allons utiliser pour calculer $\left(\frac{2}{p}\right)$.

Théorème 3.4. *Soit p un nombre premier impair. On a*

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

ou de façon équivalente $\left(\frac{2}{p}\right) = 1$ si et seulement si $p \equiv \pm 1\,[8]$.

Démonstration. Si $1 \leqslant k \leqslant \frac{p-1}{2}$ est un entier, on a $2 \leqslant 2k \leqslant p-1$. Ainsi $\widetilde{2k} > 0$ si et seulement si $2k \leqslant \frac{p-1}{2}$, c'est-à-dire si et seulement si $k \geqslant \frac{p-1}{4}$. On en déduit que $\nu_p(2) = \frac{p-1}{2} - \lfloor \frac{p-1}{4} \rfloor$. Calculons ce nombre selon la congruence de p modulo 4. Si $p \equiv 1\,[4]$, on a $\nu_p(2) = \frac{p-1}{4}$ et donc

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{si } p \equiv 1\,[8] \\ -1 & \text{si } p \equiv 5\,[8]. \end{cases}$$

Si $p \equiv 3\,[4]$, on a $\nu_p(2) = \frac{p+1}{4}$ et donc

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{si } p \equiv 7\,[8] \\ -1 & \text{si } p \equiv 3\,[8]. \end{cases}$$

On en déduit le résultat. □

3.1.4 La loi de réciprocité quadratique

Nous venons de prouver que la fonction $p \mapsto \left(\frac{2}{p}\right)$ est périodique de période 8. On peut se demander plus généralement si, étant donné un nombre premier q, la fonction $p \mapsto \left(\frac{q}{p}\right)$ est périodique. La réponse à cette question est fournie par la *loi de réciprocité quadratique*. Conjecturée par Euler, elle fut démontrée par Gauss en 1801.

Théorème 3.5 (Loi de réciprocité quadratique)**.** *Si p et q sont deux nombres premiers impairs, on a*

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

Démonstration. Nous allons utiliser les formules $\left(\frac{q}{p}\right) = (-1)^{\nu_p(q)}$ et $\left(\frac{p}{q}\right) = (-1)^{\nu_q(p)}$. Remarquons que, pour $1 \leqslant k \leqslant \frac{p-1}{2}$, on a

$$\widetilde{kq} < 0 \Leftrightarrow \exists \ell \in \mathbb{Z}, \quad -\frac{p}{2} < kq - \ell p < 0.$$

Si $\widetilde{kq} < 0$, un entier ℓ comme ci-dessus est unique. On en déduit que

$$\begin{aligned} \nu_p(q) &= \mathrm{Card}\left\{(x,y) \in \mathbb{Z}^2 \mid 0 < x < \frac{p}{2},\ -\frac{p}{2} < xq - yp < 0\right\} \\ &= \mathrm{Card}\left\{(x,y) \in \mathbb{Z}^2 \mid 0 < x < \frac{p}{2},\ x\frac{q}{p} < y < x\frac{q}{p} + \frac{1}{2}\right\}. \end{aligned}$$

Remarquons que si $0 < x < \frac{p}{2}$ et $y < x\frac{q}{p} + \frac{1}{2}$, alors $y < \frac{q}{2}$ puisque q est impair. En posant $R = \mathbb{Z}^2 \cap]0, \frac{p}{2}[\times]0, \frac{q}{2}[$, on en déduit

$$\nu_p(q) = \mathrm{Card}\left\{(x,y) \in R \mid x\frac{q}{p} < y < x\frac{q}{p} + \frac{1}{2}\right\}.$$

On montre de même que

$$\nu_p(q) = \mathrm{Card}\left\{(x,y) \in R \mid x\frac{q}{p} - \frac{1}{2} < y < x\frac{q}{p}\right\}.$$

On en déduit que

$$\frac{p-1}{2}\frac{q-1}{2} - \nu_p(q) - \nu_q(p) = \mathrm{Card}\underbrace{\left\{(x,y) \mid y \geqslant x\frac{q}{p} + \frac{1}{2}\right\}}_{A} + \mathrm{Card}\underbrace{\left\{(x,y) \mid y \leqslant x\frac{q}{p} - \frac{1}{2}\right\}}_{B}.$$

Les deux ensembles A et B ont le même cardinal. En effet, on définit une bijection $f : A \to B$ en posant $f(x,y) = (\frac{p+1}{2} - x, \frac{q+1}{2} - y)$. Ainsi $\frac{p-1}{2}\frac{q-1}{2} - \nu_p(q) - \nu_q(p)$ et pair et on en déduit

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

Exemple. La loi de réciprocité quadratique permet d'accélérer le calcul du symbole de Legendre. Considérons les deux nombres premiers 379 et 397. Comme 397 est congru à 1 modulo 4, on a

$$\left(\frac{379}{397}\right) = \left(\frac{397}{379}\right) = \left(\frac{18}{379}\right) = \left(\frac{2}{379}\right)\left(\frac{9}{379}\right) = \left(\frac{2}{379}\right) = -1.$$

Donc 379 n'est pas un carré modulo 397.

Déterminons à quelle condition sur le nombre premier $p \neq 3$ impair, l'entier 3 est résidu quadratique modulo p. La loi de réciprocité quadratique nous donne

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

Comme $(\frac{p}{3}) = 1$ si et seulement si $p \equiv 1\,[3]$, on en conclut que

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{si } p \equiv 1 \text{ ou } 11\,[12] \\ -1 & \text{si } p \equiv 5 \text{ ou } 7\,[12]. \end{cases}$$

En particulier la fonction $p \mapsto \left(\frac{3}{p}\right)$ est 12-périodique.

De façon plus générale, si q est un nombre premier, la fonction $p \mapsto \left(\frac{q}{p}\right)$ est périodique sur l'ensemble des nombres premiers impairs et de période 8 si $q = 2$, q si $q \equiv 1\,[4]$ et $4q$ si $q \equiv 3\,[4]$.

3.1.5 Le symbole de Jacobi

On aimerait désormais étendre la définition du symbole de Legendre $\left(\frac{-}{p}\right)$ a des dénominateurs plus généraux que les nombres premiers. Soit $a \in \mathbb{Z}$ un entier et soit

$b \in \mathbb{N}^*$ un entier *impair*. Le *symbole de Jacobi* de a et b est la quantité

$$\left(\frac{a}{b}\right) = \prod_{i=1}^{r} \left(\frac{a}{p_i}\right)$$

où $b = p_1 \cdots p_r$ avec les p_i premiers.

Remarquons que si a est un résidu quadratique modulo b, alors a est un résidu quadratique modulo p_i pour tout i, de sorte que $\left(\frac{a}{p_i}\right) \in \{0, 1\}$. Ainsi, la relation $\left(\frac{a}{b}\right) = -1$ implique que a n'est pas résidu quadratique modulo b. Cependant la réciproque est fausse. En effet la relation $\left(\frac{a}{b}\right) = 1$ n'implique pas nécessairement que a est résidu quadratique modulo b. Prenons par exemple le cas de $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{15}\right) = (-1)^2 = 1$. On vérifie facilement que 2 n'est pas résidu quadratique modulo 15 puisque 2 ne l'est pas modulo 3.

Le symbole de Jacobi a cependant des propriétés calculatoires très proches de celles du symbole de Legendre.

Théorème 3.6. *Soient $a_1, a_2 \in \mathbb{Z}$ et soient $b_1, b_2 \in \mathbb{N}^*$ deux entiers impairs.*

(i) On a $a_1 \equiv a_2 \,[b_1] \Rightarrow \left(\frac{a_1}{b_1}\right) = \left(\frac{a_2}{b_1}\right)$;

(ii) on a $\left(\frac{a_1 a_2}{b_1}\right) = \left(\frac{a_1}{b_1}\right)\left(\frac{a_2}{b_1}\right)$;

(iii) on a $\left(\frac{a_1}{b_1 b_2}\right) = \left(\frac{a_1}{b_1}\right)\left(\frac{a_2}{b_2}\right)$;

(iv) on a $\left(\frac{-1}{b_1}\right) = (-1)^{\frac{b_1-1}{2}}$;

(v) on a $\left(\frac{2}{b_1}\right) = (-1)^{\frac{b_1^2-1}{8}}$;

(vi) on a $\left(\frac{b_1}{b_2}\right) = \left(\frac{b_2}{b_1}\right)(-1)^{\frac{b_1-1}{2}\frac{b_2-1}{2}}$.

Démonstration. Les propriétés (i) à (iii) sont immédiates d'après la définition du symbole de Jacobi.

Pour prouver (iv) à (v), il suffit de prouver les deux assertions suivantes et d'utiliser les propriétés analogues du symbole de Legendre : si $r_1, \ldots, r_m$ sont des entiers impairs, alors

$$\sum_{i=1}^{m} \frac{r_i - 1}{2} \equiv \frac{r_1 \cdots r_m - 1}{2} \,[2]$$
$$\sum_{i=1}^{m} \frac{r_i^2 - 1}{8} \equiv \frac{r_1^2 \cdots r_m^2 - 1}{8} \,[2].$$

Une récurrence immédiate sur m nous ramène à prouver le cas où $m = 2$. Supposons donc $m = 2$. Comme r_1 et r_2 sont impairs, on a $(r_1 - 1)(r_2 - 1) \equiv 0\,[4]$ de sorte que $r_1 r_2 + 1 \equiv r_1 + r_2\,[4]$. En retranchant 2 de chaque côté et en divisant par 2, on obtient $\frac{r_1 r_2 - 1}{2} \equiv \frac{r_1 - 1}{2} + \frac{r_2 - 1}{2}\,[2]$. Pour la seconde congruence, on utilise le fait que $r_i^2 \equiv 1\,[4]$ pour $i = 1, 2$ de sorte que $(r_1^2 - 1)(r_2^2 - 1) \equiv 0\,[16]$. □

L'intérêt du symbole de Jacobi est qu'il permet d'accélérer le calcul du symbole de Legendre en remplaçant des factorisations d'entier par des divisions euclidiennes et des divisions par 2.

Exemple.

$$\left(\frac{161}{379}\right) = \left(\frac{379}{161}\right) = \left(\frac{57}{161}\right) = \left(\frac{161}{57}\right) = \left(\frac{-10}{57}\right) = \left(\frac{10}{57}\right) = \left(\frac{5}{57}\right) = \left(\frac{57}{5}\right) = \left(\frac{2}{5}\right) = -1.$$

Ainsi 161 n'est pas résidu quadratique modulo 379.

Théorème 3.7. *Soit $a \in \mathbb{N}^*$ un entier qui n'est pas un carré parfait. Alors il existe une infinité de nombres premiers p tels que a n'est pas un résidu quadratique modulo p.*

Démonstration. Remarquons tout de suite que l'on peut choisir a sans facteur carré car, si $a = bc^2$ et p est un nombre premier ne divisant pas a, alors a est résidu quadratique modulo p si et seulement si c l'est.

On peut donc supposer que a s'écrit $a = 2^e q_1 \cdots q_r$ où $e \in \{0, 1\}$ et les $q_1 < \cdots < q_r$ sont des nombres premiers impairs.

Commençons par traiter le cas où $a = 2$. Choisissons $\ell_1, \ldots, \ell_k$ des nombres premiers > 3 distincts et posons $b = 8\ell_1 \cdots \ell_k + 3$. Soit p un nombre premier divisiant b. Alors $p \notin \{2, 3, \ell_1, \ldots, \ell_k\}$. Comme $b \equiv 3\,[8]$, on a $\left(\frac{2}{b}\right) = -1$. Il existe donc un diviseur premier p de b tel que $\left(\frac{2}{p}\right) = -1$.

Supposons à présent que $a \neq 2$. On a donc $r \geqslant 1$. Soient $\ell_1, \ldots, \ell_k$ des nombres premiers distincts de 2 et des q_i. Soit $b \in \mathbb{N}^*$ tel que

$$\begin{cases} \forall 1 \leqslant i \leqslant k, & b \equiv 1\,[\ell_i] \\ \forall 1 \leqslant j \leqslant r-1 & b \equiv 1\,[q_j] \\ b \equiv 1\,[8] \\ b \equiv s\,[q_r]. \end{cases}$$

où s est non résidu quadratique modulo q_r. On en déduit que $\left(\frac{2}{b}\right) = 1$ et $\left(\frac{q_i}{b}\right) = \left(\frac{b}{q_i}\right)$ puisque $b \equiv 1\,[4]$. De plus $\left(\frac{b}{q_i}\right) = 1$ pour $1 \leqslant i \leqslant r-1$ et $\left(\frac{b}{q_r}\right) = -1$. On en déduit que $\left(\frac{a}{b}\right) = -1$. Il existe donc un diviseur premier p de b tel que $\left(\frac{a}{p}\right) = -1$. Par ailleurs, on a $p \notin \{2, q_1, \ldots, q_r, \ell_1, \ldots, \ell_k\}$.

On a donc montré que, pour toute liste finie de nombres premiers, il existe un nombre premier p n'appartenant pas à cette liste et tel que $\left(\frac{a}{p}\right) = -1$. Il existe donc une infinité de nombres premiers p tels que a n'est pas résidu quadratique modulo p. □

3.2 Caractères de $\mathbb{F}_p^\times$

3.2.1 Définition

Soit p un nombre premier. L'anneau $\mathbb{Z}/p\mathbb{Z}$ est alors un corps. Lorsque p est premier, nous utiliserons la notation $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Un *caractère* de $\mathbb{F}_p^\times$ est un morphisme de groupes

$$\chi : (\mathbb{F}_p^\times, \times) \to (\mathbb{C}^\times, \times).$$

Exemple. a) Le caractère trivial, noté ε, est défini par $\varepsilon(a) = 1$ pour tout $a \in \mathbb{F}_p^\times$.

b) Le symbole de Legendre $\left(\frac{\cdot}{p}\right)$ est aussi un caractère de $\mathbb{F}_p^\times$.

Plus généralement, considérons χ un caractère quelconque de $\mathbb{F}_p^\times$. Comme il s'agit d'un morphisme de groupes, on a nécessairement $\chi(1) = 1$. Soit $a \in \mathbb{F}_p^\times$. Comme le groupe $\mathbb{F}_p^\times$ est fini de cardinal $p-1$, on a nécessairement $\chi(a)^{p-1} = \chi(a^{p-1}) = \chi(1) = 1$. Ainsi le nombre complexe $\chi(a)$ est une racine $p-1$-ième de l'unité. On a donc en particulier $|\chi(a)| = 1$ et $\chi(a^{-1}) = \chi(a)^{-1} = \overline{\chi(a)}$ où l'on note $\overline{z}$ le complexe conjugué d'un nombre complexe z.

Souvent, il peut être pratique de prolonger χ en une fonction définie sur $\mathbb{F}_p = \mathbb{F}_p^\times \cup \{0\}$. On choisit la convention suivante

$$\chi(0) = \begin{cases} 0 & \text{si } \chi \neq \varepsilon \\ 1 & \text{si } \chi = \varepsilon. \end{cases}$$

Remarquons que, avec cette convention, pour tout $(a, b) \in \mathbb{F}_p^2$, on a $\chi(ab) = \chi(a)\chi(b)$.

Le résultat suivant résume quelques unes des propriétés d'un caractère de $\mathbb{F}_p^\times$.

Théorème 3.8. *Soit χ un caractère de $\mathbb{F}_p^\times$. Alors*

(i) $\chi(1) = 1$;

(ii) si $a \in \mathbb{F}_p^\times$, $\chi(a) \in \mu_{p-1}$;

(iii) si $a \in \mathbb{F}_p^\times$, $\chi(a^{-1}) = \chi(a)^{-1} = \overline{\chi(a)}$;

(iv) $\sum_{t \in \mathbb{F}_p} \chi(t) = \begin{cases} 0 & \text{si } \chi \neq \varepsilon \\ p & \text{si } \chi = \varepsilon. \end{cases}$

Démonstration. Les propriétés (i) à (iii) ont déjà été démontrées. Concentrons-nous sur (iv). Si $\chi = \varepsilon$, c'est évident étant donné notre convention de prolongement en 0. Supposons donc $\chi \neq \varepsilon$. Cela signifie qu'il existe $a \in \mathbb{F}_p^\times$ tel que $\chi(a) \neq 1$. En remarquant que l'application $t \mapsto at$ est une permutation de $\mathbb{F}_p$, on a

$$\sum_{t \in \mathbb{F}_p} \chi(t) = \sum_{t \in \mathbb{F}_p} \chi(at) = \chi(a) \sum_{t \in \mathbb{F}_p} \chi(t).$$

Comme $\chi(a) \neq 1$, on en conclut que $\sum_{t \in \mathbb{F}_p} \chi(t) = 0$. □

3.2.2 Structure du groupe des caractères

Considérons χ_1 et χ_2 deux caractères de $\mathbb{F}_p^\times$. L'application $\chi_1\chi_2$ de $\mathbb{F}_p^\times$ dans $\mathbb{C}^\times$ associant le nombre complexe $\chi_1(a)\chi_2(a)$ à $a \in \mathbb{F}_p^\times$ est un autre caractère de $\mathbb{F}_p^\times$. On vérifie facilement que l'ensemble des caractères de $\mathbb{F}_p^\times$ est un groupe pour cette loi de composition interne. Son élément neutre est le caractère trivial ε est l'inverse du caractère χ est le caractère $\chi^{-1} = \overline{\chi}$.

Remarque. Il faut prendre garde au prolongement à $\mathbb{F}_p$ quand on parle du produit de caractères, il n'est pas toujours vrai que $(\chi_1\chi_2)(0)\chi_1(0)\chi_2(0)$. Prenons par exemple $\chi \neq 1$. Alors

$$(\chi\chi^{-1})(0) = \varepsilon(0) = 1 \neq 0 = \chi(0)\chi^{-1}(0).$$

On sait que le groupe $\mathbb{F}_p^\times$ est cyclique de cardinal $p-1$. Soit g un générateur de ce groupe. Un caractère χ de $\mathbb{F}_p^\times$, est intégralement déterminé par le nombre complexe $\chi(g)$. En effet tout élément de $\mathbb{F}_p^\times$ est de la forme g^n et $\chi(g^n) = \chi(g)^n$. Réciproquement si $z \in \mu_{p-1}$, on peut construire un caractère χ tel que $\chi(g) = z$. Il suffit de poser $\chi(g^n) = z^n$ pour $n \in \mathbb{Z}$. Il faut juste penser à vérifier que cette définition est cohérente. En effet si $g^n = g^m$, on a $p-1 \mid n-m$. Ainsi $z^n = z^m$ puisque $z \in \mu_{p-1}$. On vient donc de démontrer que l'application $\chi \mapsto \chi(g)$ induit une bijection de l'ensemble des caractères de $\mathbb{F}_p^\times$ sur μ_{p-1}.

On note $\widehat{\mathbb{F}_p^\times}$ le groupe des caractères de $\mathbb{F}_p^\times$. L'application $\begin{array}{ccc} \widehat{\mathbb{F}_p^\times} & \to & \mu_{p-1} \\ \chi & \mapsto & \chi(g) \end{array}$ est bijective et c'est visiblement un morphisme de groupes, c'est donc un isomorphisme de groupes. On a donc prouvé une partie du théorème suivant.

Théorème 3.9. *Le groupe des caractères de $\mathbb{F}_p^\times$ est un groupe cyclique de cardinal $p-1$. De plus, un caractère χ de $\mathbb{F}_p^\times$ est un générateur du groupe des caractères si et seulement si χ est une bijection de $\mathbb{F}_p^\times$ sur μ_{p-1}. On en déduit que si $a \in \mathbb{F}_p^\times \smallsetminus \{1\}$, il existe au moins un caractère χ tel que $\chi(a) \neq 1$.*

Démonstration. La première partie du théorème a déjà été démontrée. Démontrons l'assertion concernant les générateurs du groupe des caractères. Soit g un générateur de $\mathbb{F}_p^\times$. Comme l'application $\chi \mapsto \chi(g)$ est un isomorphisme de $\widehat{\mathbb{F}_p^\times}$ sur μ_{p-1}, χ est un générateur de $\widehat{\mathbb{F}_p^\times}$ si et seulement si $\chi(g)$ est un générateur de μ_{p-1}. Comme $\chi(\mathbb{F}_p^\times) = \chi(g)^{\mathbb{Z}}$, on en conclut que χ est un générateur de $\widehat{\mathbb{F}_p^\times}$ si et seulement si χ est une surjection de $\mathbb{F}_p^\times$ sur μ_{p-1}, c'est-à-dire si et seulement si χ est une bijection de $\mathbb{F}_p^\times$ sur μ_{p-1}.

Il reste à vérifier que si $a \neq 1$, il existe un caractère χ tel que $\chi(a) \neq 1$. On choisit χ un générateur de $\widehat{\mathbb{F}_p^\times}$. Comme χ est une bijection de $\mathbb{F}_p^\times$ sur μ_{p-1}, on a $\chi(a) \neq 1 = \chi(1)$. □

Remarque. a) Pour construire un générateur de $\widehat{\mathbb{F}_p^\times}$, on peut commencer par fixer un générateur g de $\mathbb{F}_p^\times$ et considérer l'unique caractère vérifiant $\chi(g) = e^{\frac{2\pi i}{p}}$.

b) Les groupes $\widehat{\mathbb{F}_p^\times}$ et $\mathbb{F}_p^\times$ sont tous deux cycliques de cardinal $p-1$. Ils sont donc isomorphes. Cependant il n'existe pas vraiment d'isomorphisme privilégié entre ces deux groupes. De même que pour construire un isomorphisme entre $\widehat{\mathbb{F}_p^\times}$ et μ_{p-1}, il faut commencer par choisir un générateur g de $\mathbb{F}_p^\times$ et il n'y a pas vraiment de choix canonique.

Corollaire. *Soit $a \in \mathbb{F}_p$. On a alors*

$$\sum_{\chi \in \widehat{\mathbb{F}_p^\times}} \chi(a) = \begin{cases} 1 & \text{si } a = 0 \\ p-1 & \text{si } a = 1 \\ 0 & \text{si } a \in\not\in \{0,1\}. \end{cases}$$

Démonstration. Les cas où $a \in \{0,1\}$ sont immédiat. Concentrons-nous sur le cas $a \notin \{0,1\}$. Soit λ un caractère de $\mathbb{F}_p^\times$ tel que $\lambda(a) \neq 0$. Comme $\widehat{\mathbb{F}_p^\times}$ est un groupe, l'application $\chi \mapsto \lambda\chi$ est une permutation de $\widehat{\mathbb{F}_p^\times}$. On a alors

$$\sum_{\chi \in \widehat{\mathbb{F}_p^\times}} \chi(a) = \sum_{\chi \in \widehat{\mathbb{F}_p^\times}} (\lambda\chi)(a) = \lambda(a) \sum_{\chi \in \widehat{\mathbb{F}_p^\times}} \chi(a).$$

Comme $\lambda(a) \neq 1$, on en conclut que $\sum_{\chi \in \widehat{\mathbb{F}_p^\times}} \chi(a) = 0$. □

3.2.3 Sommes de Gauss

Soit p un nombre premier. Posons $\zeta_p = e^{\frac{2\pi i}{p}}$. Il s'agit d'un générateur du groupe μ_p.

Définition. *Soit $a \in \mathbb{F}_p$ et soit χ un caractère de $\mathbb{F}_p^\times$. La* somme de Gauss *associée à a et χ est la quantité*

$$g_a(\chi) = \sum_{t \in \mathbb{F}_p} \chi(t)\zeta_p^{at}.$$

Remarque. La fonction $a \mapsto g_a(\chi)$ est un analogue discret de la transformée de Fourier de l'application χ. En effet, si f est une fonction 1-périodique de $\mathbb{R}$ dans $\mathbb{C}$, c'est-à-dire une application de $\mathbb{R}/\mathbb{Z}$ dans $\mathbb{C}$, on a $\widehat{f}(n) = \int_0^1 f(t)e^{-2\pi int}\,dt$ et les fonctions $t \mapsto e^{2\pi int}$ sont des morphismes du groupe $\mathbb{R}/\mathbb{Z}$ dans $\mathbb{C}^\times$. De même si f est une fonction de $\mathbb{R}$ dans $\mathbb{C}$, sa transformée de Fourier est l'application $\hat{f}(x) = \int_{\mathbb{R}} f(t)e^{-2\pi ixt}\,dt$ et $t \mapsto e^{2\pi ixt}$ est un morphismes de groupes de $(\mathbb{R},+)$ dans $\mathbb{C}^\times$.

Toutes ces opérations peuvent se généraliser dans un même cadre : l'intégration sur les groupes localement compacts.

Théorème 3.10.

(i) Si $a \in \mathbb{F}_p^\times$ et si $\chi \neq \varepsilon$ est un caractère de $\mathbb{F}_p^\times$, on a $g_a(\chi) = \chi(a)^{-1}g_1(\chi)$.

(ii) Si $\chi \neq \varepsilon$, on a $g_0(\chi) = 0$ et $|g_a(\chi)| = \sqrt{p}$ pour $a \neq 0$.

(iii) Si $a \neq 0$, on a $g_a(\varepsilon) = 0$.

(iv) On a $g_0(\varepsilon) = p$.

Démonstration. Commençons par prouver le point (i). On a

$$\chi(a)g_a(\chi) = \sum_{t\in\mathbb{F}_p} \chi(a)\chi(t)\zeta_p^{at} = \sum_{t\in\mathbb{F}_p} \chi(at)\zeta_p^{at} = \sum_{t\in\mathbb{F}_p} \chi(t)\zeta_p^{t} = g_1(\chi).$$

D'où le résultat.

Le point le plus délicat est sans doute le point (ii). On commence par calculer

$$g_0(\chi) = \sum_{t\in\mathbb{F}_p} \chi(t) = 0.$$

D'après (i), il suffit alors de prouver que $|g_1(\chi)| = \sqrt{p}$ pour $\chi \neq \varepsilon$ car $|g_a(\chi)| = |g_1(\chi)|$ si $a \neq 0$ et $\chi \neq \varepsilon$. On utilise cette observation pour calculer de deux façons la somme suivante

$$\begin{aligned}\sum_{a\in\mathbb{F}_p} g_a(\chi)\overline{g_a(\chi)} &= \sum_{a\in\mathbb{F}_p^\times} g_a(\chi)\overline{g_a(\chi)} = (p-1)|g_1(\chi)|^2 \\ &= \sum_{a\in\mathbb{F}_p} \left(\sum_{t\in\mathbb{F}_p} \chi(t)\zeta_p^{at}\right)\left(\sum_{t\in\mathbb{F}_p} \overline{\chi(t)}\zeta_p^{-at}\right) = \sum_{(t,u)\in\mathbb{F}_p^2} \chi(t)\overline{\chi(u)} \underbrace{\sum_{a\in\mathbb{F}_p} \zeta_p^{a(t-u)}}_{=0 \text{ si } t\neq u} \\ &= \sum_{t\in\mathbb{F}_p} |\chi(t)|^2 p = p(p-1).\end{aligned}$$

On en conclut que $|g_1(\chi)|^2 = p$.

Les cas (iii) et (iv) sont des calculs explicites et sans difficulté. □

Le théorème précédent implique donc que, si χ est un caractère non trivial, on peut écrire $g_1(\chi) = \sqrt{p}e^{i\theta}$. Les sommes de Gauss sont des objets ayant un rôle très important en arithmétique, les décrire le plus précisément possible est donc un problème important. Malheureusement l'argument θ est compliqué à appréhender. Nous allons à présent nous concentrer sur le cas où le caractère est quadratique, c'est-à-dire vérifie $\chi^2 = 1$.

3.2.4 Sommes de Gauss quadratiques

On dit qu'un caractère χ de $\mathbb{F}_p^\times$ est *quadratique* si $\chi^2 = \varepsilon$ et $\chi \neq \varepsilon$. Lorsque p est un nombre premier impair, il existe un unique caractère quadratique de $\mathbb{F}_p^\times$, il s'agit du symbole de Legendre. La somme de Gauss associée au symbole de Legendre possède une autre interprétation. Posons

$$G(p) = \sum_{t\in\mathbb{F}_p} \zeta_p^{t^2} = \sum_{t=0}^{p-1} e^{\frac{2\pi i t^2}{p}}.$$

Théorème 3.11. *Si p est un nombre premier impair, on a $G(p) = g_1\left(\left(\frac{-}{p}\right)\right)$.*

Démonstration. Rappelons que si $a \in \mathbb{F}_p$, le symbole de Legendre encode le fait que l'équation $X^2 = a$ ait ou non des solutions. Il permet plus précisément de préciser exactement combien cette équation a de solutions. Comme $\mathbb{F}_p$ est un corps, si $a \in \mathbb{F}_p^\times$ est un carré, disons $a = b^2$. Alors les solutions de l'équations $X^2 = a$ sont b et $-b$ et, puisque $p \geqslant 3$, ces deux solutions sont distinctes. Par contre l'équation $X^2 = 0$ a une unique solution qui est 0. On a donc

$$\mathrm{Card}\{x \in \mathbb{F}_p \mid x^2 = a\} = \begin{cases} 1 & \text{si } a = 0 \\ 2 & \text{si } a \neq 0 \text{ et } \left(\frac{a}{p}\right) = 1 \\ 0 & \text{si } a \neq 0 \text{ et } \left(\frac{a}{p}\right) = -1. \end{cases}$$

Ainsi $\mathrm{Card}\{x \in \mathbb{F}_p \mid x^2 = a\} = 1 + \left(\frac{a}{p}\right)$. On en déduit

$$G(p) = \sum_{a \in \mathbb{F}_p} \left(1 + \left(\frac{a}{p}\right)\right) \zeta_p^a = g_1(\varepsilon) + g_1\left(\left(\frac{-}{p}\right)\right) = g_1\left(\left(\frac{-}{p}\right)\right). \qquad \square$$

Nous allons à présent calculer explicitement la quantitué $G(p)$. Pour simplifier les notations, posons $\chi = \left(\frac{-}{p}\right)$. Remarquons dans un premier temps que, puisque χ est quadratique, alors $\chi = \chi^{-1} = \overline{\chi}$. Ainsi

$$\overline{g(\chi)} = \sum_{t \in \mathbb{F}_p} \chi(t)\zeta_p^{-t} = g_{-1}(\chi) = \chi(-1)^{-1} g_1(\chi) = \chi(-1) g_1(\chi).$$

On en déduit que

$$p = g(\chi)\overline{g(\chi)} = \chi(-1) g(\chi)^2.$$

Comme $\chi(-1) = (-1)^{\frac{p-1}{2}}$, on a $g(\chi)^2 = (-1)^{\frac{p-1}{2}} p$ et donc

$$g(\chi) = \begin{cases} \pm\sqrt{p} & \text{si } p \equiv 1\,[4] \\ \pm i\sqrt{p} & \text{si } p \equiv 3\,[4]. \end{cases}$$

Le signe précis qui intervient dans cette égalité est un peu plus compliqué à déterminer précisément.

Théorème 3.12 (Gauss)**.** *Si p est un nombre premier impair et si $\chi = \left(\frac{-}{p}\right)$, on a*

$$g(\chi) = \begin{cases} \sqrt{p} & \textit{si } p \equiv 1\,[4] \\ i\sqrt{p} & \textit{si } p \equiv 3\,[4]. \end{cases}$$

Lemme. *Soit p un nombre premier impair. On a alors*

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

Démonstration. De l'égalité entre polynômes de $\mathbb{F}_p[X]$:

$$(X-1)(1+X+\cdots+X^{p-1}) = X^p - 1 = \prod_{i=0}^{p-1}(X-\zeta_p^i),$$

on tire l'égalité

$$1+X+\cdots+X^{p-1} = \prod_{i=1}^{p-1}(X-\zeta_p^i).$$

En évaluant cette égalité en $X=1$, on obtient la factorisation $p = \prod_{i=1}^{p-1}(1-\zeta_p^i)$. Remarquons à présent que tout élément de $\mathbb{F}_p^\times$ s'écrit de façon unique sous la forme $\overline{4k-2}$ ou $-\overline{4k-2}$ pour un entier $1 \leqslant k \leqslant \frac{p-1}{2}$. En effet si $4k-2 \equiv \pm(4\ell-2)\,[p]$ pour $1 \leqslant k, \ell \leqslant \frac{p-1}{2}$, on a $p \mid k-\ell$ ou $p \mid k+\ell-1$. La deuxième possibilité est exclue car $3 \leqslant k+\ell-1 \leqslant p-2$. On en conclut que $k=\ell$ et que le signe est $+$. On peut donc écrire

$$p = \prod_{k=1} \frac{p-1}{2}\left((1-\zeta_p^{4k-2})(1-\zeta_p^{-(4k-2)})\right) = \prod_{k=1}^{\frac{p-1}{2}}\left(\zeta_p^{2k-1}-\zeta_p^{-(2k-1)}\right)^2$$
$$(-1)^{\frac{p-1}{2}}\prod_{k=1}^{\frac{p-1}{2}}\left(\zeta_p^{2k-1}-\zeta_p^{-(2k-1)}\right)^2.$$

□

Lemme. *Soit p un nombre premier impair. On a alors*

$$\prod_{k=1}^{\frac{p-1}{2}}\left(\zeta_p^{2k-1}-\zeta_p^{-(2k-1)}\right) = \begin{cases}\sqrt{p} & \text{si } p \equiv 1\,[4]\\ i\sqrt{p} & \text{si } p \equiv 3\,[4].\end{cases}$$

Démonstration. D'après le lemme précédent, on a

$$\prod_{k=1}^{\frac{p-1}{2}}(\zeta_p^{2k-1}-\zeta_p^{-(2k-1)}) = \prod_{k=1}^{\frac{p-1}{2}} 2i\sin\left(\frac{2\pi(2k-1)}{p}\right) = 2^{\frac{p-1}{2}} i^{\frac{p-1}{2}} \prod_{k=1}^{\frac{p-1}{2}}\sin\left(\frac{4k-2}{p}\pi\right).$$

Pour $1 \leqslant k \leqslant \frac{p-1}{2}$, on a $\frac{4k-2}{p}\pi \in]0,2\pi[$ et $\frac{4k-2}{p}\pi \in]0,\pi[$ si et seulement si $k < \frac{p+2}{4}$. Le produit $\prod_{k=1}^{\frac{p-1}{2}}\sin\left(\frac{(2k-1)\pi}{p}\right)$ a donc exactement $\frac{p-1}{2} - \lfloor\frac{p+2}{4}\rfloor$ termes négatifs, c'est-à-dire $\frac{p-1}{2}$ termes négatifs si $p \equiv 1\,[4]$ et $\frac{p-3}{4}$ termes négatifs si $p \equiv 3\,[4]$. On en conclut que

$$\prod_{k=1}^{\frac{p-1}{2}}\left(\zeta_p^{2k-1}-\zeta_p^{-(2k-1)}\right) = \begin{cases} i^{\frac{p-1}{2}}(-1)^{\frac{p-1}{4}}\sqrt{p} & \text{si } p \equiv 1\,[4]\\ i^{\frac{p-1}{2}}(-1)^{\frac{p-3}{4}}\sqrt{p} & \text{si } p \equiv 3\,[4].\end{cases}$$

Ce qui donne le résultat. □

Preuve du théorème 3.12. Posons $\chi = \left(\frac{-}{p}\right)$. On sait déjà que $g_1(\chi) = \varepsilon \prod_{k=1}^{\frac{p-1}{2}} (\zeta_p^{2k-1} - \zeta_p^{-(2k-1)})$ pour $\varepsilon \in \{1, -1\}$. Les lemmes précédents montrent qu'il suffit de prouver que $\varepsilon = 1$. Posons

$$P = \sum_{j=1}^{p-1} \chi(j) X^j - \varepsilon \prod_{j=1}^{\frac{p-1}{2}} (X^{2j-1} - X^{p-(2j+1)}) \in \mathbb{Z}[X].$$

Par choix de ε, on a donc $P(\zeta_p) = 0$. Rappelons que le polynôme $\Phi_p = 1 + X + \cdots + X^{p-1}$ est irréductible dans $\mathbb{Q}[X]$ et possède ζ_p comme racine. On en déduit que Φ_p divise P dans $\mathbb{Q}[X]$. Comme le polynôme Φ_p est primitif, on en déduit que cette division a lieu dans $\mathbb{Z}[X]$. On a de même $\Phi_p(1+X) \mid P(1+X)$. En réduisant modulo p cette relation, on en conclut que $\overline{Phi_p(1+X)} \mid \overline{P(1+X)}$ dans $\mathbb{F}_p[X]$. Par ailleurs $\overline{\Phi_p(1+X)} = X^{p-1}$. On en déduit que les coefficients des termes de degré $< p-1$ de $P(1+X)$ sont divisibles par p.

Par ailleurs le terme non de plus petit degré du polynôme $\prod_{j=1}^{\frac{p-1}{2}} (X^{2j-1} - X^{p-(2j+1)})$ est en degré $\frac{p-1}{2}$. En effet, pour $1 \leqslant k \leqslant \frac{p-1}{2}$, on a

$$(1+X)^{2k-1} - (1+X)^{p-(2k-1)} \equiv (4k-2-p)X \,[X^2].$$

On observe même que le coefficient du terme de degré $\frac{p-1}{2}$ vaut $\prod_{k=1}^{\frac{p-1}{2}} (4k-2-p)$. Déterminons ensuite le coefficient de degré $\frac{p-1}{2}$ de

$$\sum_{j=1}^{p-1} \left(\frac{j}{p}\right) (1+X)^j = \sum_{j=1}^{p-1} \sum_{i=0}^{j} \binom{j}{i} \chi(j) X^j = \sum_{i=0}^{p-1} \left(\sum_{j=i}^{p-1} \binom{j}{i} \chi(j) \right) X^i.$$

Il s'agit de $\sum_{j=\frac{p-1}{2}}^{p-1} \chi(j) \binom{j}{\frac{p-1}{2}}$.

On a donc prouvé que

$$\sum_{j=\frac{p-1}{2}}^{p-1} \chi(j) \binom{j}{\frac{p-1}{2}} \equiv \varepsilon \prod_{k=1}^{\frac{p-1}{2}} (4k-2) \,[p].$$

En multipliant cette congruence par $(\frac{p-1}{2})!$ et en utilisant $\chi(j) \equiv j^{\frac{p-1}{2}} \,[p]$, on obtient

$$\sum_{j=\frac{p-1}{2}}^{p-1} j^{\frac{p-1}{2}} \prod_{\ell=0}^{\frac{p-3}{2}} (j-\ell) \equiv \varepsilon \left(\frac{p-1}{2}\right)! \prod_{k=1}^{\frac{p-1}{2}} (4k-2) \,[p].$$

Comme $\mathbb{F}_p^\times$ est un groupe cyclique de cardinal $p-1$, on vérifie facilement que

$$\sum_{j=1}^{p-1} j^k \equiv \begin{cases} 0 \,[p] & \text{si } p-1 \nmid k \\ p-1 \,[p] & \text{si } p-1 \mid k. \end{cases}$$

En remarquant que $j \mapsto \prod_{\ell=0}^{\frac{p-3}{2}}(j-\ell)$ est un polynôme en j de degré $\frac{p-1}{2}$, on en conclut que

$$p-1 \equiv \sum_{j=\frac{p-1}{2}}^{p-1} j^{\frac{p-1}{2}} \prod_{\ell=0}^{\frac{p-3}{2}}(j-\ell) \equiv \varepsilon\left(\frac{p-1}{2}\right)! \prod_{k=1}^{\frac{p-1}{2}}(4k-2)\,[p].$$

Par ailleurs

$$\prod_{k=1}^{\frac{p-1}{2}}(4k-2) = 2^{\frac{p-1}{2}} \prod_{k=1}^{\frac{p-1}{2}}(2k-1) = 2^{\frac{p-1}{2}}(p-1)! \left(\prod_{k=1}^{\frac{p-1}{2}}(2k)\right)^{-1} = \prod_{k=\frac{p+1}{2}}^{p-1} k.$$

Finalement $\varepsilon(p-1)! \equiv -1\,[p]$ et on déduit du théorème de Wilson que $\varepsilon \equiv 1\,[p]$. Comme $p \geqslant 3$, on a $\varepsilon = 1$. □

3.2.5 Sommes de Jacobi

Soit p un nombre premier. Soient χ et λ deux caractères de $\mathbb{F}_p^\times$. La *somme de Jacobi* associée à χ et λ est la quantité

$$J(\chi,\lambda) = \sum_{\substack{(a,b)\in\mathbb{F}_p^2 \\ a+b=1}} \chi(a)\lambda(b).$$

Les sommes de Jacobi peuvent s'exprimer en termes de sommes de Gauss.

Théorème 3.13. *(i) Si $\chi \neq \varepsilon$, $\lambda \neq \varepsilon$ et $\chi\lambda \neq \varepsilon$, on a*

$$J(\chi,\lambda) = \frac{g_1(\chi)g_1(\lambda)}{g_1(\chi\lambda)}.$$

(ii) Si $\chi \neq \varepsilon$, on a $J(\chi,\chi^{-1}) = -\chi(-1)$.

(iii) Si $\chi \neq \varepsilon$, on a $J(\chi,\varepsilon) = J(\varepsilon,\chi) = 0$.

(iv) On a $J(\varepsilon,\varepsilon) = p$.

Démonstration. Prouvons (i). On a

$$g_1(\chi)g_1(\lambda) = \left(\sum_{t\in\mathbb{F}_p} \chi(t)\zeta_p^t\right)\left(\sum_{u\in\mathbb{F}_p} \lambda(u)\zeta_p^u\right) = \sum_{(t,u)\in\mathbb{F}_p^2} \chi(t)\lambda(u)\zeta_p^{t+u}$$

$$= \sum_{a\in\mathbb{F}_p}\left(\sum_{\substack{(t,u)\in\mathbb{F}_p^2 \\ t+u=a}} \chi(t)\lambda(u)\right)\zeta_p^a.$$

Si $a = 0$, on a $\sum_{\substack{(t,u)\in\mathbb{F}_p^2 \\ t+u=a}} \chi(t)\lambda(u) = \sum_{t\in\mathbb{F}_p} \lambda(-1)(\chi\lambda)(t) = 0$ puisque $\chi\lambda \neq \varepsilon$. Si $a \neq 0$, on a une bijection

$$\begin{array}{ccc} \{(t,u) \in \mathbb{F}_p^2 \mid t+u=1\} & \xrightarrow{\sim} & \{(t,u) \in \mathbb{F}_p^2 \mid t+u=a\} \\ (t,u) & \longmapsto & (at,au) \end{array}$$

de sorte que

$$\sum_{\substack{(t,u)\in\mathbb{F}_p^2 \\ t+u=a}} \chi(t)\lambda(u) = \sum_{\substack{(t,u)\in\mathbb{F}_p^2 \\ t+u=1}} \chi(at)\lambda(au) = \chi(a)\lambda(a) \sum_{\substack{(t,u)\in\mathbb{F}_p^2 \\ t+u=1}} \chi(t)\lambda(u) = (\chi\lambda)(a)J(\chi,\lambda).$$

Ainsi

$$g_1(\chi)g_1(\lambda) = \sum_{a\in\mathbb{F}_p} (\chi\lambda)(a)J(\chi,\lambda)\zeta_p^a = g_1(\chi\lambda)J(\chi,\lambda).$$

Comme $g_1(\chi\lambda) \neq 0$, puisque $|g_1(\chi\lambda)| = \sqrt{p}$, on obtient le résultat.

Passons au (ii). Soit $\chi \neq \varepsilon$. Alors

$$J(\chi,\chi^{-1}) = \sum_{t\in\mathbb{F}_p} \chi(t)\chi(1-t)^{-1} = \sum_{t\in\mathbb{F}_p\smallsetminus\{0,1\}} \chi(t(1-t)^{-1}).$$

Comme l'application $t \mapsto t(1-t)^{-1}$ induit une bijection de $\mathbb{F}_p \smallsetminus \{0,1\}$ sur $\mathbb{F}_p \smallsetminus \{0,-1\}$, on a

$$J(\chi,\chi^{-1}) = \sum_{u\in\mathbb{F}_p\smallsetminus\{0,-1\}} \chi(u) = -\chi(-1)$$

puisque $\sum_{u\in\mathbb{F}_p} \chi(u) = 0$ et $\chi(0) = 0$.

Les points (iii) et (iv) sont immédiats. □

Corollaire. *Soient χ et λ deux caractères non triviaux de $\mathbb{F}_p^\times$ tels que $\chi\lambda \neq \varepsilon$. On a alors $|J(\chi,\lambda)| = \sqrt{p}$.*

3.2.6 Applications

Nous allons étudier les valeurs premières prises par certaines formes quadratiques très particulières.

Théorème 3.14.

(i) Soit p un nombre premier impair. Il existe $(a,b) \in \mathbb{Z}^2$ tel que $p = a^2 + b^2$ si et seulement si $p \equiv 1\,[4]$.

(ii) Soit p un nombre premier impair et différent de 3. Il existe $(a,b) \in \mathbb{Z}^2$ tel que $p = a^2 - ab + b^2$ si et seulement si $p \equiv 1\,[3]$.

Démonstration. Commençons par prouver le point (i). Supposons $p \equiv 1\,[4]$. Le groupe $\widehat{\mathbb{F}_p^\times}$ est alors cyclique de cardinal $p-1$ donc de cardinal divisible par 4. Il possède donc un élément χ d'ordre 4. Comme $\chi^4 = \varepsilon$, on a $\chi(\mathbb{F}_p^\times) \subset \{1, -1, i, -i\}$. En conséquence

$$J(\chi, \chi) \in \mathbb{Z}[i] = \{a + bi \mid (a, b) \in \mathbb{Z}^2\}.$$

Par ailleurs $\chi \neq \varepsilon$ et $\chi^2 \neq \varepsilon$ puisque χ est d'ordre 4. On en conclut que $|J(\chi, \chi)| = \sqrt{p}$, c'est-à-dire $|J(\chi, \chi)|^2 = p$. Soit $(a, b) \in \mathbb{Z}^2$ tel que $J(\chi, \chi) = a + bi$. On a donc $a^2 + b^2 = |J(\chi, \chi)|^2 = p$. Réciproquement supposons qu'il existe $(a, b) \in \mathbb{Z}^2$ tel que $p = a^2 + b^2$. Comme p n'est pas un carré, $0 < |a|, |b| < p$ et donc a et b ne sont pas divisible par p. On a donc, dans $\mathbb{F}_p$, $(\overline{a}\overline{b}^{-1})^2 = -1$ de sorte que $\left(\frac{-1}{p}\right) = 1$ et donc $p \equiv 1\,[4]$.

Passons au (ii). Supposons $p \equiv 1\,[3]$. Cette fois-ci le groupe cyclique $\widehat{\mathbb{F}_p^\times}$ possède un élément χ d'ordre 3. On a $\chi \neq \varepsilon$ et $\chi^2 \neq \varepsilon$ de sorte que $|J(\chi, \chi)|^2 = p$. Par ailleurs, $\chi(\mathbb{F}_p^\times) \subset \{1, j, j^2\}$ avec $j = e^{\frac{2\pi i}{3}}$. Comme $j^2 = -1 - j$, on a

$$J(\chi, \chi) \in \mathbb{Z}[j] = \{a + bj \mid (a, b) \in \mathbb{Z}^2\}.$$

Soit $(a, b) \in \mathbb{Z}^2$ tel que $J(\chi, \chi) = a + bj$. On a alors

$$p = |a + bj|^2 = a^2 - ab + b^2.$$

Réciproquement supposons qu'il existe $(a, b) \in \mathbb{Z}^2$ tel que $a^2 - ab + b^2 = p$. On a $p \nmid a$ et $p \nmid b$. En effet, supposons un instant que $p \mid a$. On en déduit alors $p \mid b$ et donc $p^2 \mid p$, ce qui est absurde. Posons $x = -\overline{a}\overline{b}^{-1} \in \mathbb{F}_p$. On a alors $x^2 + x + 1 = 0$ de sorte que $x \neq 1$ (car $p \neq 3$) et $x^3 = 1$. Ainsi $\mathbb{F}_p^\times$ possède un élément d'ordre 3 et donc $3 \mid p - 1$. □

Un nombre complexe $z \in \mathbb{C}$ est dit *constructible* s'il existe une suite finie de sous-corps de $\mathbb{C}$

$$\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_n$$

telle que $z \in K_n$ et $[K_i : K_{i-1}] = 2$ pour tout $1 \leqslant i \leqslant n$. Un nombre constructible z est donc algébrique. De plus $[\mathbb{Q}(z) : \mathbb{Q}] \mid 2^n$ de sorte que son degré est nécessairement une puissance de 2. On montre facilement que l'ensemble des nombres constructibles de $\mathbb{C}$ est un sous-corps de $\mathbb{C}$.

Remarque. On peut montrer qu'un nombre complexe est constructible si et seulement si il est l'affixe d'un point du plan que l'on peut construire à la règle et au compas à partir des points d'affixes 0 et 1.

Nous allons à présent déterminer quelles racines p-ième de l'unité sont constructibles pour p premier.

Théorème 3.15. *Soit p un nombre premier. Alors ζ_p est constructible si et seulement si $p = 2^n + 1$ pour un certain entier $n \geqslant 0$.*

Remarque. Les nombres ζ_3, ζ_5, ζ_{17} sont constructibles.

Démonstration. On a montré que le polynôme $\Phi_p(X)$ est irréductible dans $\mathbb{Q}[X]$ et de degré $p-1$. C'est donc le polynôme minimal de ζ_p sur $\mathbb{Q}$ et $[\mathbb{Q}(\zeta_p):\mathbb{Q}] = p-1$. On en conclut que si ζ_p est constructible, alors $p-1$ est une puissance de 2. Montrons la réciproque.

Commençons par un lemme intermédiaire.

Lemme. *Soit $n \geqslant 2$ un entier et soit p un nombre premier tel que $p \equiv 1\,[n]$. Soit χ un caractère d'ordre n de $\mathbb{F}_p^\times$. On a alors*

$$g_1(\chi)^n = \chi(-1)pJ(\chi,\chi)J(\chi,\chi^2)\cdots J(\chi,\chi^{n-2}).$$

Démonstration. Si $n = 2$, on a $\chi^2 = \varepsilon$ et on a déjà montré que $g_1(\chi)^2 = \chi(-1)p$. Supposons donc $n > 2$. Montrons par récurrence sur $2 \leqslant k \leqslant n-1$ que

$$g_1(\chi)^k = J(\chi,\chi)J(\chi,\chi^2)\cdots J(\chi,\chi^{k-1})g_1(\chi^k).$$

On a $\chi^2 \neq \varepsilon$, donc $g_1(\chi)^2 = J(\chi,\chi)g_1(\chi^2)$ ce qui donne la formule pour $k = 2$. Supposons le résultat démontré pour $2 \leqslant k \leqslant n-2$. On a alors $\chi^{k+1} \neq \varepsilon$, de sorte que

$$\begin{aligned} g_1(\chi)^{k+1} = g_1(\chi)^k g_1(\chi) &= J(\chi,\chi)J(\chi,\chi^2)\cdots J(\chi,\chi^{k-1})g_1(\chi^k)g_1(\chi) \\ &= J(\chi,\chi)J(\chi,\chi^2)\cdots J(\chi,\chi^{k-1})g_1(\chi^{k+1})J(\chi,\chi^k). \end{aligned}$$

On a donc

$$g_1(\chi)^n = J(\chi,\chi)\cdots J(\chi,\chi^{n-2})g_1(\chi^{n-1})g_1(\chi).$$

Comme $\chi^{n-1} = \overline{\chi}$, on a $g_1(\chi^{n-1}) = \overline{g_{-1}(\chi)} = \chi(-1)\overline{g_1(\chi)}$ (car $\chi(-1) \in \mathbb{R}$). Ainsi $g_1(\chi^{n-1})g_1(\chi) = \chi(-1)p$, ce qui donne le résultat. □

Revenons à la démonstration du théorème. Supposons donc que $p = 2^n + 1$ pour un certain entier $n \geqslant 1$. On commence par exprimer ζ_p en terme de sommes de Gauss. On a

$$\sum_{\chi\in\widehat{\mathbb{F}_p^\times}} g_1(\chi) = \sum_{\chi\in\widehat{\mathbb{F}_p^\times}} \sum_{t=0}^{p-1} \chi(t)\zeta_p^t = \sum_{t=0}^{p-1} \left(\sum_{\chi\in\widehat{\mathbb{F}_p^\times}} \chi(t) \right) \zeta_p^t.$$

Rappelons que $\sum_\chi \chi(t)$ vaut 0 sauf si $t = 0$, où la somme vaut 1 ou si $t = 1$, où la somme vaut $p-1$. On a donc

$$\sum_{\chi\in\widehat{\mathbb{F}_p^\times}} g_1(\chi) = 1 + (p-1)\zeta_p.$$

On en conclut que si $g_1(\chi)$ est constructible pour tout caractère χ de $\mathbb{F}_p^\times$, alors ζ_p est constructible.

Soit χ un caractère de $\mathbb{F}_p^\times$. Alors χ est d'ordre 2^m pour un certain entier $0 \leqslant m \leqslant n$. On a donc

$$g_1(\chi)^{2^m} = \chi(-1)pJ(\chi,\chi)\cdots J(\chi,\chi^{2^m-2}).$$

Remarquons que comme χ et χ^i sont d'ordre un diviseur de 2^m, ils prennent leur valeurs dans μ_{2^m} de sorte que $J(\chi,\chi^i) \in \mathbb{Q}(\zeta_{2^m})$. Comme $[\mathbb{Q}(\zeta_{2^{i+1}}) : \mathbb{Q}(\zeta_{2^i})] = 2$ pour $i \geqslant 1$ et $\mathbb{Q}(\zeta_2) = \mathbb{Q}$, on en conclut que tous les éléments de $\mathbb{Q}(\zeta_{2^m})$ sont constructibles. Ainsi toutes les sommes de Jacobi $J(\chi,\chi^i)$ sont constructibles et $g_1(\chi)^{2^m}$ est constructible. Comme $g_1(\chi)$ est obtenu à partir de $g_1(\chi)^{2^m}$ par une suite d'extractions de racines carrées, $g_1(\chi)$ est constructible. C'est ce que l'on cherchait. □

3.2.7 Nombres de solutions d'équations dans les corps finis

Dans un premier temps, nous allons utiliser la théorie des caractères pour déterminer le nombre de solutions de l'équation $X^n = a$ dans $\mathbb{F}_p$ où p est un nombre premier. Supposons dans un premier temps que $a \neq 0$. Rappelons que $\mathbb{F}_p^\times$ est un groupe cyclique. Fixons g un générateur de ce groupe et posons $a = g^\alpha$ pour un certain $\alpha \in \mathbb{Z}$. Recherchons les solutions de $X^n = a$ sous la forme g^ξ avec $\xi \in \mathbb{Z}$. On a alors

$$(g^\xi)^n = g^\alpha \Leftrightarrow n\xi \equiv \alpha\,[p-1].$$

On a déjà étudié ce type de congruence. Elle admet des solutions si et seulement si le pgcd δ de n et $p-1$ divise α. Supposons que ce soit le cas, on a alors

$$n\xi \equiv \alpha\,[p-1] \Leftrightarrow \frac{n}{\delta}\xi \equiv \frac{\alpha}{\delta}\,[\frac{p-1}{\delta}].$$

Cette congruence a alors une unique solution modulo $\frac{p-1}{\delta}$, c'est-à-dire δ solutions modulo $p-1$. Par ailleurs remarquons que la condition $\delta \mid \alpha$ est équivalente à

$$\frac{p-1}{\delta}\alpha \equiv 0\,[p-1] \Leftrightarrow a^{\frac{p-1}{\delta}} = 1.$$

Théorème 3.16. *Soit $a \in \mathbb{F}_p$. Soit $n \geqslant 1$ un entier et soit $N(X^n = a) = \mathrm{Card}\{x \in \mathbb{F}_p \mid x^n = a\}$. Posons $d = n \wedge (p-1)$. On a alors*

$$N(X^n = a) = \sum_{\substack{\chi \in \widehat{\mathbb{F}_p^\times} \\ \chi^d = \varepsilon}} \chi(a).$$

Démonstration. Remarquons que comme le groupe $\widehat{\mathbb{F}_p^\times}$ est cyclique et que $d \mid p-1$, il y a exactement d caractères de $\mathbb{F}_p^\times$ tels que $\chi^d = \varepsilon$. Décomposons la preuve en trois cas

Cas 1. Si $a = 0$, comme $\mathbb{F}_p$ est un corps, on a $N(X^n = 0) = 1$. Par ailleurs $\sum_{\chi^d=\varepsilon} \chi(0) = \varepsilon(0) = 1$.

Cas 2. Supposons $a \neq 0$ et $N(X^n = a) > 0$. Alors l'équation $X^n = a$ a des solutions. Comme $d \mid n$, il existe donc $b \in \mathbb{F}_p$ tel que $a = b^d$. On en déduit que, si $\chi^d = 1$, on a alors $\chi(a) = \chi(b)^d = 1$. Ainsi

$$\sum_{\chi^d=\varepsilon} \chi(a) = d.$$

Par ailleurs, on a déjà remarqué que, dans ce cas, $N(X^n = a) = d$.

Cas 3. Supposons à présent $N(X^n = a) = 0$. On sait alors que $a^{\frac{p-1}{d}} \neq 1$. Soit λ un élément de $\widehat{\mathbb{F}_p^\times}$ tel que $\lambda(a^{\frac{p-1}{d}}) = \lambda^{\frac{p-1}{d}}(a) \neq 1$. Ainsi le caractère $\psi = \lambda^{\frac{p-1}{d}}$ est un caractère tel que $\psi^d = \varepsilon$ et $\psi(a) \neq 0$. La multiplication par ψ induit donc une permutation du sous-groupe de $\widehat{\mathbb{F}_p^\times}$ constitué des éléments d'ordre divisant d. On en conclut que

$$\sum_{\chi^d=\varepsilon} \chi(a) = \sum_{\chi^d=\varepsilon} (\psi\chi)(a) = \psi(a) \sum_{\chi^d=\varepsilon} \chi(a).$$

Comme $\psi(a) \neq 1$, on en conclut que

$$\sum_{\chi^d=\varepsilon} \chi(a) = 0 = N(X^n = a).$$

On a donc démontré l'égalité dans tous les cas. □

Théorème 3.17. *Soit $p \geqslant 5$ un nombre premier tel que $p \equiv 1\,[3]$. Soit $d \in \mathbb{Z}$. Notons N_p le nombre de couples $(x, y) \in \mathbb{F}_p^2$ vérifiant l'équation $Y^2 = X^3 + d$. Si $p \nmid d$, on a*

$$|N_p - p| < 2\sqrt{p}.$$

Démonstration. Comme $p \equiv 1\,[3]$, il existe un caractère χ de $\mathbb{F}_p^\times$ qui est d'ordre 3. L'ensemble des caractères θ de $\mathbb{F}_p^\times$ tels que $\theta^3 = \varepsilon$ est donc $\{\varepsilon, \chi, \chi^2\}$. Posons également $\psi = \left(\frac{\cdot}{p}\right)$ l'unique caractère d'ordre 2 de $\mathbb{F}_p^\times$. On peut alors décrire N_p en utilisant la formule suivante

$$\begin{aligned}
N_p &= \sum_{\substack{(a,b)\in\mathbb{F}_p^2 \\ a+b=d}} N(Y^2 = a)N(X^3 = -b) = \sum_{\substack{(a,b)\in\mathbb{F}_p^2 \\ a+b=d}} N(Y^2 = a)N(X^3 = b) \\
&= \sum_{\substack{(a,b)\in\mathbb{F}_p^2 \\ a+b=d}} (1 + \psi(a))(1 + \chi(b) + \chi^2(b)) \\
&= \sum_{\substack{(a,b)\in\mathbb{F}_p^2 \\ a+b=d}} (1 + \psi(a) + \chi(b) + \chi^2(b) + \psi(a)\chi(b) + \psi(a)\chi^2(b)) \\
&= p + \sum_{\substack{(a,b)\in\mathbb{F}_p^2 \\ a+b=d}} \psi(a)\chi(b) + \sum_{\substack{(a,b)\in\mathbb{F}_p^2 \\ a+b=d}} \psi(a)\chi^2(b) \\
&= p + \psi(d)\chi(d)J(\psi, \chi) + \psi(d)\chi(d)^2 J(\psi, \chi^2).
\end{aligned}$$

Remarquons que, puisque $\chi\psi \neq \varepsilon$ et $\chi^2\psi \neq \varepsilon$, on a $|J(\psi,\chi)| = |J(\psi,\chi^2)| = \sqrt{p}$, on a

$$|N_p - p| \leqslant |J(\psi,\chi)| + |J(\psi,\chi^2)| = 2\sqrt{p}.$$

L'inégalité est en fait stricte puisque $2\sqrt{p}$ n'est pas un entier. □

Remarque. Si $\equiv 2\,[3]$, l'application $x \mapsto x^3$ est un permutation de $\mathbb{F}_p$, on en déduit que, dans ce cas, on a toujours $N_p = p$.

3.3 Caractères de Dirichlet

Nous allons à présent généraliser la notion de caractère aux groupes $(\mathbb{Z}/n\mathbb{Z})^\times$ pour tout entier $n \geqslant 2$. Plus généralement, nous allons définir la notion de caractère pour tout groupe abélien fini.

Soit G un groupe abélien fini. On appelle *caractère* de G un morphisme de groupes $G \to \mathbb{C}^\times$. On note $\widehat{G}$ l'ensemble de tous les caractères de G. Si χ est un caractère de G et $g \in G$, le nombre complexe $\chi(g)$ est d'ordre fini et vérifie donc $|\chi(g)| = 1$. On peut également munir $\widehat{G}$ d'une structure de groupe en posant, pour $\chi_1, \chi_2 \in G$ et $g \in G$, $(\chi_1\chi_2)(g) = \chi_1(g)\chi_2(g)$. Nous avons déjà rencontré ces définitions dans le cas particulier de $G = \mathbb{F}_p^\times$ pour p premier. Dans le cas de $\mathbb{F}_p^\times$, la situation était simplifiée par le fait que le groupe $\mathbb{F}_p^\times$ est cyclique. Ce n'est pas vrai pour un groupe abélien fini quelconque. Dans cette optique, le résultat suivant pourra être utile.

Théorème 3.18. *Soient $G_1, \ldots, G_r$ des groupes abéliens finis. L'application $\widehat{G} \to \widehat{G_1} \times \cdots \times \widehat{G_r}$ définie par $\chi \mapsto (\chi|_{G_1}, \ldots, \chi|_{G_r})$ est un isomorphisme de groupes.*

Démonstration. Il suffit de vérifier que l'application qui associe à la donnée de caractères $\chi_1, \ldots, \chi_r$ de $G_1, \ldots, G_r$ le caractère de G définie $(a_1, \ldots, a_r) \mapsto \chi_1(a_1)\cdots\chi_r(a_r)$ est réciproque du morphisme de l'énoncé. □

On peut désormais considérer le cas particulier où $G = (\mathbb{Z}/n\mathbb{Z})^\times$ avec $n \geqslant 2$ entier. On peut alors décomposer $n = p_1^{\alpha_1}\cdots p_r^{\alpha_r}$ où $p_1 < \cdots < p_r$ sont premier. L'isomorphisme $(\mathbb{Z}/n\mathbb{Z})^\times \simeq (\mathbb{Z}/p_1^{\alpha_1})^\times \times \cdots \times (\mathbb{Z}/p_r^{\alpha_r})^\times$ montre alors que se donner un caractère de $(\mathbb{Z}/n\mathbb{Z})^\times$ revient à se donner un caractère du groupe $(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^\times$ pour tout $1 \leqslant i \leqslant r$.

Théorème 3.19. *Si G est un groupe abélien fini, les deux groupes G et $\widehat{G}$ sont isomorphes. Si de plus $g \in G$ est différent de l'élément neutre, il existe $\chi \in \widehat{G}$ tel que $\chi(g) \neq 1$.*

Démonstration. Commençons par traiter le cas où G est cyclique, ce qui se fait comme pour le groupe $\mathbb{F}_p^\times$. On choisit un générateur g de G et on remarque que l'application $\chi \mapsto \chi(g)$ induit un isomorphisme de $\widehat{G}$ sur le groupe des racines m-ièmes de l'unités où $m = \mathrm{Card}(G)$. Le cas général se déduit alors du théorème de structure des groupes abéliens finis qui implique que tout groupe abélien fini est isomorphe à un produit de groupes cycliques. On utilise alors le résultat sur le groupe dual d'un groupe produit. □

Corollaire. *Soit G un groupe abélien fini. Si $\chi \in \widehat{G}$, on a*

$$\sum_{g\in G} \chi(g) = \begin{cases} 0 & \text{si } \chi \neq e_{\widehat{G}} \\ \mathrm{Card}(G) & \text{sinon.} \end{cases}$$

Si $g \in G$, on a

$$\sum_{\chi\in\widehat{G}} \chi(g) = \begin{cases} 0 & \text{si } g \neq e_G \\ \mathrm{Card}(G) & \text{sinon.} \end{cases}$$

Soit $n \geqslant 2$. Si χ est un caractère de $(\mathbb{Z}/n\mathbb{Z})^\times$, on peut prolonger χ en une fonction de $\mathbb{Z}$ dans $\mathbb{C}$ en posant

$$\chi(a) = \begin{cases} 0 & \text{si } a \wedge n \neq 1 \\ \chi(a \bmod n) & \text{si } a \wedge n = 1. \end{cases}$$

La fonction χ est alors périodique de période n et vérifie la propriété $\chi(mn) = \chi(m)\chi(n)$ pour tous $m, n \in \mathbb{Z}$. En particulier, restreinte à $\mathbb{N}^*$ on obtient une fonction arithmétique complètement multiplicative.

Tout ceci nous amène à introduire la notion de *caractère de Dirichlet*.

Définition. *Soit $n \geqslant 2$ un entier. Un* caractère de Dirichlet *de module n est une application $\chi : \mathbb{Z} \to \mathbb{C}$ vérifiant*

(i) pour tout $a \in \mathbb{Z}$, $\chi(a + n) = \chi(a)$;

(ii) un entier a est premier à n si et seulement si $\chi(a) \neq 0$;

(iii) pour tout $(a, b) \in \mathbb{Z}^2$, on a $\chi(ab) = \chi(a)\chi(b)$.

Il est évident que les caractères de Dirichlet de module n sont en bijection naturelle avec les caractères du groupe $(\mathbb{Z}/n\mathbb{Z})^\times$.

Les résultats concernant les caractères de $(\mathbb{Z}/n\mathbb{Z})^\times$ impliquent alors le résultat suivant.

Théorème 3.20. *Soit $n \geqslant 2$ un entier. Pour la loi de multiplication, l'ensemble des caractères de Dirichlet de module n est un groupe abélien fini de cardinal $\varphi(n)$. Son élément neutre estle caractère χ_0 défini par $\chi_0(a) = 1$ si $a \wedge n = 1$ et $\chi_0(a) = 0$ sinon. De plus, on a*

$$\forall a \in \mathbb{Z}, \quad \frac{1}{\varphi(n)} \sum_{\chi \bmod n} \chi(a) = \begin{cases} 1 & \text{si } a \equiv 1\,[n] \\ 0 & \text{sinon.} \end{cases}$$

$$\forall \chi \bmod n, \quad \frac{1}{\varphi(n)} \sum_{a=0}^{n-1} \chi(a) = \begin{cases} 1 & \text{si } \chi = \chi_0 \\ 0 & \text{sinon} \end{cases}$$

où l'on a utilisé l'abbréviation $\chi \bmod n$ pour « χ est un caractère de Dirichlet modulo n ».

Chapitre 4

Méthodes analytiques

4.1 Le théorème des nombres premiers

4.1.1 Séries de Dirichlet

Soit f une fonction arithmétique. La *série de Dirichlet* associée à f est la série de fonctions

$$s \mapsto D(f)(s) = \sum_{n \geqslant 1} \frac{a_n}{n^s}$$

définie sur l'ensemble des $s \in \mathbb{C}$ où elle converge.

Théorème 4.1. *Soit f une fonction arithmétique. On suppose que la série $D(f)(s_0)$ converge en $s_0 = \sigma_0 + it_0$, avec $\sigma_0, t_0 \in \mathbb{R}$.*

(i) Soit $0 \leqslant \theta \leqslant \frac{\pi}{2}$. La série $D(f)$ converge uniformément sur l'ensmble $\{s \in \mathbb{C} \mid \mathrm{Re}(s) \geqslant \sigma_0$ et $|\mathrm{Arg}(s - s_0)| \leqslant \theta\}$.

(ii) La fonction $D(f)$ est holomorphe sur $\{s \in \mathbb{C} \mid \mathrm{Re}(s) > \sigma_0\}$.

(iii) La série $D(f)$ converge absolument pour $\mathrm{Re}(s) > \sigma_0 + 1$.

(iv) Si la fonction arithmétique f est non nulle, il existe un réel $\sigma_1 > \sigma_0$ tel que

$$\forall s \in \{s \in \mathbb{C} \mid \mathrm{Re}(s) \geqslant \sigma_1\}, \quad D(f)(s) \neq 0.$$

(v) Si la série $D(f)$ converge absolument en s_0, alors elle converge normalement sur $\{s \in \mathbb{C} \mid \mathrm{Re}(s) \geqslant \sigma_0\}$.

Démonstration. Prouvons (i). Quitte à remplacer f par la fonction arithmétique $n \mapsto f(n)n^{-s_0}$, on peut supposer que $s_0 = 0$ et donc que la série $\sum_{n \geqslant 1} f(n)$ est convergente. Posons $D_N(s) = \sum_{k=1}^{N} f(n)n^{-s}$ pour $N \geqslant 1$ et $D_0 = 0$. Pour $M \geqslant 1$ entier et $x > M$ réel, posons également $A_M(x) = \sum_{M < n \leqslant x} f(n)$. On applique le procédé de sommation

par parties à la fonction arithémique $f\mathbb{1}_{]M,+\infty[}$ et on obtient l'égalité

$$D_N(s) - D_M(s) = \sum_{n=M+1}^{N} \frac{f(n)}{n^s} = \frac{A_M(N)}{N^s} + s\int_M^N \frac{A_M(t)}{t^{s+1}}\,dt.$$

Comme la série $\sum f(n)$ est convergente, on peut poser $\varepsilon_M = \sup_{N>M}|A_M(N)|$ qui tend vers 0 quand M tend vers $+\infty$. En posant $\sigma = \mathrm{Re}(s)$, on en déduit

$$|D_N(s) - D_M(s)| \leqslant \frac{\varepsilon_M}{N^\sigma} + \varepsilon_M|s|\int_M^N \frac{dt}{t^{\sigma+1}}.$$

Comme $\sigma = |s|\cos(\mathrm{Arg}(s))$, on a $|s| \leqslant \frac{\sigma}{\cos\theta}$ de sorte que

$$|D_N(s) - D_M(s)| \leqslant \frac{\varepsilon_M}{N^\sigma} + \frac{\varepsilon_M}{\cos\theta}(M^{-\sigma} - N^{-\sigma}) \leqslant \varepsilon_M(1 + (\cos\theta)^{-1}).$$

On en déduit la convergence uniforme.

Le (ii) est alors une conséquence immédiate du (i) et du fait qu'une limite uniforme de fonctions holomorphes est holomorphe.

Prouvons le (iii). Supposons que $\sigma = \mathrm{Re}(s) > \sigma_0 + 1$. La suite $(f(n)n^{-s_0})_{n\geqslant 1}$ est bornée, on a donc

$$\left|\frac{f(n)}{n^s}\right| \leqslant (\sup_{n\geqslant 1}|f(n)n^{-s_0}|)\frac{1}{n^{\sigma-\sigma_0}}.$$

Comme $\sigma - \sigma_0 > 1$, on en déduit la convergence absolue de la série par comparaison avec une série de Riemann.

Prouvons (iv). Posons $n_0 = \min\{n \in \mathbb{N}^* \mid f(n) \neq 0\}$. Posons alors $D(f)(s) = \frac{f(n_0)}{n_0^s}(1 + g(s))$ où g est la fonction définie par $g(s) = \frac{n_0^s}{f(n_0)}(\sum_{k\geqslant 1}\frac{f(n_0+k)}{(n_0+k)^s})$. Soit $s \in \mathbb{C}$ tel que $\sigma = \mathrm{Res}(s) > \sigma_0 + 2$. On a alors

$$|g(s)| \leqslant \frac{n_0^\sigma}{f(n_0)}\frac{1}{(n_0+1)^{\sigma-\sigma_0-2}}\sum_{k\geqslant 1}\frac{|f(n_0+k)|}{(n_0+k)^{\sigma_0+2}}.$$

Le (iii) montre que la série définissant $g(s)$ converge absolument. De plus on a

$$|g(s)| \leqslant \left(\frac{n_0}{n_0+1}\right)^{\sigma-\sigma_0-2}\frac{n_0^{\sigma_0+2}}{|f(n_0)|}\sum_{k\geqslant 1}\frac{|f(n_0+k)|}{(n_0+k)^{\sigma_0+2}} \to_{\sigma\to+\infty} 0.$$

Il existe donc $\sigma_1 \geqslant \sigma_0 + 2$ tel que $|g(s)| \leqslant \frac{1}{2}$ dès que $\mathrm{Re}(s) \geqslant \sigma_1$, et donc $D(f)(s) \neq 0$.

Le point (v) est immédiat car $|\frac{f(n)}{n^s}| \leqslant \frac{f(n_0)}{n^{\sigma_0}}$ dès que $\mathrm{Re}(s) \geqslant \sigma_0$. □

On déduit en particulier de ce résultat que la fonction arithmétique f est entièrement déterminée par la fonction holomorphe $D(f)$ dès lors que son domaine de convergence est non vide. On voit aussi qu'il existe un $c \in \mathbb{R} \cup \{-\infty, +\infty\}$ tel que

$$\Pi_c = \{s \in \mathbb{C} \mid \mathrm{Re}(s) > c\} \subset \{s \in \mathbb{C} \mid D(f)(s) \text{ converge}\} \subset \overline{\Pi}_c = \{s \in \mathbb{C} \mid \mathrm{Re}(s) \geqslant c\}.$$

Ce nombre c est appelé *abscisse de convergence* de la série de Dirichlet $D(f)$. On le note aussi σ_c. Plus explicitement, on a

$$\sigma_c = \inf\{\sigma \in \mathbb{R} \mid D(f)(\sigma) \text{ converge}\}.$$

On peut également considérer l'*abscisse de convergence absolue* définie par

$$\sigma_a = \inf\{\sigma \in \mathbb{R} \mid \sum_{n\geqslant 1} |f(n)|n^{-\sigma} \text{ converge}\}.$$

On déduit du théorème 4.1 que

$$\sigma_c \leqslant \sigma_a \leqslant \sigma_c + 1.$$

De plus, la fonction $D(f)$ est holomorphe sur l'ouvert Π_{σ_c}.

Théorème 4.2. *Soient f et g deux fonctions arithmétiques. Alors la série $D(f+g,s)$ converge en les valeurs de s où les deux séries $D(f,s)$ et $D(g,s)$ convergent. On a alors $D(f+g,s) = D(f,s) + D(g,s)$. On a donc $\sigma_c(f+g) \leqslant \max(\sigma_c(f), \sigma_c(g))$. Si $D(f,s)$ et $D(g,s)$ convergent absolument, $D(f*g,s)$ converge absolument et $D(f*g,s) = D(f,s)D(g,s)$. Ainsi $\sigma_a(f*g) \leqslant \max(\sigma_a(f), \sigma_a(g))$.*

Démonstration. L'assertion concernant la somme est évidente et celle concernant le produit est arithmétique est une conséquence du théorème 2.4. □

4.1.2 Exemples

Si $f = \mathbb{1}$, on a $D(f,s) = \zeta(s)$. Son abscisse de convergence absolue et son abscisse de convergence sont égales à 1.

Si $n \geqslant 1$, on a $|\mu(n)| \leqslant 1$. Ainsi la série de Dirichlet $D(\mu,s)$ a une abscisse de convergence absolue $\sigma_a(\mu) \leqslant 1$. De plus, si $\mathrm{Res}(s) > 1$, on a alors

$$D(\mu,s)\zeta(s) = D(e,s) = 1$$

de sorte que $\zeta(s) \neq 0$ pour $\mathrm{Re}(s) > 1$ et

$$\frac{1}{\zeta(s)} = \sum_{n\geqslant 1} \frac{\mu(n)}{n^s}.$$

Rappelons que $d(n)$ désigne le nombre de diviseurs de n dans $\mathbb{N}^*$. On a $d = \mathbb{1} * \mathbb{1}$, de sorte que $\sigma_a(d) \leqslant 1$. Par ailleurs, $d(n) \geqslant 1 = \mathbb{1}(n)$ pour tout $n \geqslant 1$, donc $\sigma_a(d) \geqslant \sigma_a(\mathbb{1}) = 1$. Enfin, la fonction d est positive donc $\sigma_c(d) = \sigma_a(d) = 1$. De plus, pour $\mathrm{Re}(s) > 1$, on a

$$\sum_{n\geqslant 1} \frac{d(n)}{n^s} = \zeta(s)^2.$$

Théorème 4.3. *Soit f une fonction arithmétique. L'abscisse de convergence de la fonction arithmétique $f\log$ est $\leqslant \sigma_c(f)$. De plus, si $s \in \Pi_{\sigma_c(f)}$, on a*

$$D(f,s)' = -\sum_{n\geqslant 1} \frac{f(n)\log n}{n^s} = -D(f\log, s).$$

Démonstration. On sait que si $(h_n)_{n\geqslant 1}$ est une suite de fonctions holomorphes convergeant uniformément vers f sur un ouvert Ω de $\mathbb{C}$, alors la suite $(h_n')_{n\geqslant 1}$ converge uniformément sur tout compact de Ω vers la fonction f'. On obtient le théorème en appliquant ce résultat à $h_n(s) = \sum_{k=1}^n f(k)k^{-s}$ à tous les ouverts de la forme $\{s \in \mathbb{C} \mid \mathrm{Re}(s) \geqslant \sigma, |\mathrm{Arg}(s)| \leqslant \theta\}$ pour $\sigma > \sigma_c(f)$ et $\theta < \frac{\pi}{2}$. □

On en déduit par exemple une expression pour la dérivée de la fonction ζ :

$$\forall s \in \Pi_1, \quad \zeta'(s) = -\sum_{n\geqslant 1} \frac{\log n}{n^s}.$$

Comme $\log \geqslant 0$, sur $\mathbb{N}^*$, on a $\sigma_c(\log) = \sigma_a(\log) = 1$. On en déduit que la fonction $\Lambda = \mu * \log$ a une abscisse de convergence absolue qui est $\leqslant 1$ et, pour $s \in \Pi_1$,

$$\sum_{n\geqslant 1} \frac{\Lambda(n)}{n^s} = -\frac{\zeta'(s)}{\zeta(s)}.$$

4.1.3 Produits eulériens

On rappelle que si f est une fonction arithmétique multiplicative, on a

$$\forall s \in \Pi_{\sigma_a(f)}, \quad D(f,s) = \prod_p \left(1 + \frac{f(p)}{p^s} + \frac{f(p^2)}{p^{2s}} + \cdots + \frac{f(p^n)}{p^{ns}} + \cdots\right).$$

Si f est de plus complètement multiplicative, alors

$$\forall s \in \Pi_{\sigma_a(f)}, \quad D(f,s) = \prod_p \left(1 - \frac{f(p)}{p^s}\right)^{-1}.$$

On en déduit par exemple, si χ est un caractère de Dirichlet modulo N, que

$$\forall s \in \Pi_1, \quad D(\chi,s) = \sum_{n\geqslant 1} \frac{\chi(n)}{n^s} = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}.$$

4.1.4 La fonction Γ

On définit, pour $s \in \Pi_0$,

$$\Gamma(s) = \int_0^{+\infty} t^{s-1} e^{-t}\, dt = \int_0^{+\infty} t^s e^{-t} \frac{dt}{t}.$$

Une intégration par parties nous donne

$$\forall s \in \Pi_0, \quad \Gamma(s+1) = s\Gamma(s).$$

Une récurrence immédiate montre que $\Gamma(s+n) = (s+n-1)(s+n-2)\cdots(s+1)s\Gamma(s)$ pour tout $s \in \Pi_1$ et $n \geqslant 1$. Comme on calcule immédiatement que $\Gamma(1) = 1$, on en déduit $\Gamma(n) = (n-1)!$ pour $n \in \mathbb{N}^*$. Par ailleurs la formule

$$\Gamma(s) = \frac{1}{s(s+1)\cdots(s+n-1)}\Gamma(s+n)$$

pour tout $n \in \mathbb{N}^*$ permet de définir un prolongement analytique de Γ en une fonction holomorphe sur $\mathbb{C} \setminus -\mathbb{N}$. La même formule nous donne alors, pour $n \in \mathbb{N}$,

$$\Gamma(s) \sim_{s \to -n} \frac{(-1)^n}{n!} \frac{1}{s+n}$$

ce qui prouve que Γ peut se prolonger, de façon unique, en une fonction méromorphe sur $\mathbb{C}$ dont les pôles sont exactement les points de $-\mathbb{N}$. De plus, le pôle en $-n$ est simple et de résidu $\frac{(-1)^n}{n!}$.

On peut montrer plus précisément que le prolongement analytique de la fonction Γ vérifie une équation fonctionnelle.

Théorème 4.4 (Formule des compléments)**.** *Pour $s \in \mathbb{C} \setminus \mathbb{Z}$, on a*

$$\Gamma(s)\Gamma(1-s) = \frac{\pi}{\sin(\pi s)}.$$

Démonstration. Pour $s \in \mathbb{C} \setminus \mathbb{Z}$, on a

$$\Gamma(s+1)\Gamma(1-(s+1)) = s\Gamma(s)\Gamma(-s) = -\Gamma(s)\Gamma(1-s).$$

Ainsi la fonction $s \mapsto F(s) = \Gamma(s)\Gamma(1-s) - \frac{\pi}{\sin(\pi s)}$ est 2-périodique. Remarquons de plus que la fonction $s \mapsto \Gamma(s)\Gamma(1-s)$ a un pôle en $n \in \mathbb{Z}$ qui est simple de résidu $(-1)^n$ et qu'il en est de même de la fonction $s \mapsto \frac{\pi}{\sin(\pi s)}$. Ceci implique que la fonction F est en fait holomorphe sur $\mathbb{C}$.

Pour $0 \leqslant \operatorname{Re} s \leqslant 1$, on a

$$\begin{aligned} |\Gamma(s)| = |s^{-1}\Gamma(s+1)| &\leqslant |s|^{-1} \int_0^{+\infty} t^{\operatorname{Re}(s)} e^{-t}\, dt \\ &\leqslant |s|^{-1} \left(\int_0^1 t^{\operatorname{Re}(s)}\, dt + \int_1^{\infty} te^{-t}\, dt \right) \leqslant |s|^{-1} \left(\frac{1}{\operatorname{Re}(s)+1} + 2 \right) \leqslant \frac{3}{|s|}. \end{aligned}$$

Par ailleurs, en utilisant l'inégalité $|1-z| \geqslant |1-|z||$,

$$|\sin(\pi s)| = \frac{|e^{\pi i s} - e^{-\pi i s}|}{2} = \frac{e^{-\pi \operatorname{Im}(s)}}{2}|1 - e^{-2\pi i s}| \geqslant \frac{e^{-\pi \operatorname{Im}(s)}}{2}|1 - e^{2\pi \operatorname{Im}(s)}|.$$

On en conclut que

$$|F(s)| \leqslant \frac{9}{\operatorname{Im}(s)^2} + \left(\frac{e^{-\pi \operatorname{Im}(s)}}{2}|1 - e^{2\pi \operatorname{Im}(s)}|\right)^{-1}$$

et donc que $F(s) \to 0$ quand $|\operatorname{Im}(s)| \to +\infty$ uniformément en $\operatorname{Re}(s)$. La fonction F, étant continue, est donc bornée sur la bande $\{0 \leqslant \operatorname{Re}(s) \leqslant 1\}$. Par 2-périodicité et imparité, elle est bornée sur $\mathbb{C}$. Comme elle est de plus holomorphe, le théorème du maximum local montre qu'elle est constante sur $\mathbb{C}$. Comme elle tend vers 0 quand $\operatorname{Im}(s)$ tend vers $+\infty$, on en déduit que $F = 0$. On a donc prouvé l'égalité recherchée. □

En évaluant cette formule en $s = \frac{1}{2}$, on obtient $\Gamma(\frac{1}{2})^2 = \pi$ et donc $\Gamma(\frac{1}{2}) = \sqrt{\pi}$ qui est équivalente à l'égalité

$$\int_{\mathbb{R}} e^{-t^2}\, dt = \sqrt{\pi}.$$

Par ailleurs on en déduit que $\Gamma(s) \neq 0$ si $s \notin \mathbb{Z}$. De plus Γ a un pôle aux points de $-\mathbb{N}$ et $\Gamma(n) = (n-1)! \neq 0$ si $n \in \mathbb{N}^*$. On a donc prouvé que

$$\forall s \in \mathbb{C}, \quad \Gamma(s) \neq 0.$$

De façon équivalente, la fonction $\frac{1}{\Gamma}$ est holomorphe sur $\mathbb{C}$ et ses zéros sont simples, ce sont les points de $-\mathbb{N}$.

La formule suivante peut également être utile.

Théorème 4.5 (Formule de duplication)**.** *Pour $s \in \mathbb{C}$, on a*

$$\Gamma(s)\Gamma\left(s + \frac{1}{2}\right) = 2^{1-2s}\sqrt{\pi}\Gamma(2s).$$

Démonstration. La démonstration peut se mener comme celle de la formule des compléments. □

4.1.5 La fonction Zeta de Riemann

Rappelons qu'il s'agit de la série de Dirichlet associée à la fonction arithmétique $\mathbb{1}$. Ses rayons de convergence et de convergence absolue valent 1.

Lemme. *Soit $f : [0, +\infty[\to \mathbb{C}$ une fonction de classe $\mathcal{C}^\infty$ vérifiant de plus $f(t) =_{+\infty} O(t^{-n})$ pour tout $n \geqslant 1$. Alors la fonction définie par $L(f,s) = \frac{1}{\Gamma(s)}\int_0^\infty t^s f(t)\frac{dt}{t}$ pour $s \in \Pi_0$ admet un prolongement holomorphe à $\mathbb{C}$ tel que*

$$\forall n \in \mathbb{N}, \quad L(f,-n) = (-1)^n f^{(n)}(0).$$

Démonstration. Commençons par remarquer que sous nos hypothèses, la fonction $s \mapsto \int_0^\infty t^s f(t)\frac{dt}{t}$ est holomorphe sur Π_0.

Supposons dans un premier temps que le support de la fonction f est inclus dans $]0,+\infty[$. Alors la fonction $s \mapsto \int_0^\infty t^s f(t)\frac{dt}{t}$ est même définie et holomorphe sur $\mathbb{C}$. Comme la fonction $\frac{1}{\Gamma}$ est holomorphe sur $\mathbb{C}$ et s'annule en tout point de $-\mathbb{N}$, on en conclut que $L(f,-n)=0$ si $n\in\mathbb{N}$. Comme dans ce cas, $f^{(n)}(0)=0$, la formule recherchée est trivialement vraie.

Supposons maintenant que f est à support compact. Supposons que son support est contenu dans $[0,A]$ pour un certain $A>0$. On a alors, pour $\operatorname{Re} s>0$,

$$\int_0^\infty t^s f(t)\frac{dt}{t} = \left[\frac{1}{s}t^s f(t)\right]_0^A - \frac{1}{s}\int_0^A t^{s+1}f'(t)\frac{dt}{t} = -\frac{1}{s}\int_0^\infty t^{s+1}f'(t)\frac{dt}{t}.$$

On en conclut que $L(f,s) = -L(f',s+1)$ et $L(f,s)=(-1)^n L(f^{(n)},s+n)$ pour tout $s\in\Pi_0$ et $n\in\mathbb{N}$. On en déduit que $s\mapsto L(f,s)$ se prolonge en une fonction holomorphe sur $\mathbb{C}$ tel que, pour tout $n\in\mathbb{N}$,

$$L(f,-n) = (-1)^{n+1}L(f^{(n+1)},1) = (-1)^{n+1}\int_0^A f^{(n+1)}(t)\,dt = (-1)^n f^{(n)}(0).$$

Pour traiter le cas général, on choisir une fonction $\varphi : [0,+\infty[\to \mathbb{R}$ de classe $\mathcal{C}^\infty$ telle que $\varphi(x)=1$ pour $x\leqslant 1$ et $\varphi(x)=0$ pour $x\geqslant 2$. On décompose alors $L(f,s) = L(f\varphi,s)+L(f(1-\varphi),s)$. La fonction $f(1-\varphi)$ vérifie les hypothèses du premier cas et $f\varphi$ les hypothèses du second cas. □

Considérons alors la fonction définie sur $[0,+\infty[$ par $f(t)=\frac{t}{e^t-1}$. Il s'agit d'une fonction développable en série entière sur $[0,+\infty[$. On note $B_n = f^{(n)}(0)$ pour $n\in\mathbb{N}$ de sorte que

$$f(t) = \sum_{n\geqslant 0}\frac{B_n}{n!}t^n$$

pour $t\in[0,+\infty[$. De plus, on a $B_n\in\mathbb{Q}$. Le nombre rationnel est appelé n-ième *nombre de Bernoulli*.

Exemple. On a $B_1=-\frac{1}{2}$, $B_2=\frac{1}{6}$, $B_4=-\frac{1}{30}$, $B_6=\frac{1}{42}$... On a $B_{2n+1}=0$ pour $n\geqslant 1$.

Théorème 4.6. *La fonction ζ se prolonge en une fonction méromorphe sur $\mathbb{C}$ ayant un unique pôle simple en $s=1$ de résidu 1. De plus, si $n\in\mathbb{N}$, on a*

$$\zeta(-n) = (-1)^n\frac{B_{n+1}}{n+1}\in\mathbb{Q}.$$

Démonstration. Pour $s\in\Pi_1$, on considère

$$\Gamma(s)\zeta(s) = \sum_{n\geqslant 1}\int_0^{+\infty}\frac{t^s}{n^s}e^{-t}\frac{dt}{t} = \int_0^{+\infty}t^s\left(\sum_{n\geqslant 1}e^{-nt}\right)\frac{dt}{t} = \int_0^{+\infty}t^s\frac{1}{e^t-1}\frac{dt}{t} = \Gamma(s-1)L(f,s-1)$$

où $f(t) = \frac{t}{e^t-1}$. On en déduit que $\zeta(s) = \frac{\Gamma(s-1)}{\Gamma(s)} L(f, s-1) = \frac{1}{s-1} L(f, s-1)$. Le résultat est alors une conséquence immédiate du lemme 4.1.5. Les caractéristiques du pôle en 1 se déduisent de l'égalité $L(f, 0) = f(0) = 1$ et, pour $n \in -\mathbb{N}$, on a

$$\zeta(-n) = -\frac{1}{n+1} L(f, -n-1) = (-1)^n \frac{B_{n+1}}{n+1}. \qquad \square$$

Nous allons à présent en dire un peu plus sur le prolongement de la fonction ζ à $\mathbb{C}$. Nous allons prouver que ce dernier possède une équation fonctionnelle.

Pour $s \in \mathbb{C}$, on pose $\xi(s) = \pi^{\frac{s}{2}} \Gamma(\frac{s}{2}) \zeta(s)$.

Théorème 4.7. *La fonction méromorphe ξ vérifie l'équation fonctionnelle*

$$\xi(1-s) = \xi(s).$$

La preuve de ce théorème repose sur l'équation fonctionnelle d'une « série theta » reposant elle-même sur la célèbre formule de Poisson.

Soit $f : \mathbb{R} \to \mathbb{C}$ une fonction intégrable. La *transformée de Fourier* de f comme est la fonction $\widehat{f} : \mathbb{R} \to \mathbb{C}$ définie par

$$\forall x \in \mathbb{R}, \quad \widehat{f}(x) = \int_{\mathbb{R}} f(t) e^{-2\pi i x t} \, dt.$$

Lemme (Formule de Poisson)**.** *Soit $f : \mathbb{R} \to \mathbb{C}$ une fonction de classe $\mathcal{C}^2$ telle que f, f' et f'' sont toutes les trois intégrables sur $\mathbb{R}$. On a alors*

$$\sum_{n \in \mathbb{Z}} f(n) = \sum_{n \in \mathbb{Z}} \widehat{f}(n).$$

Démonstration. Remarquons que puisque f'' est intégrable, la fonction f' est bornée. Le caractère intégrable de f implique en particulier que, pour tout $x \in \mathbb{R}$, la famille $f(x+n)_{n \in \mathbb{Z}}$ est sommable et la fonction $g : \mathbb{R} \to \mathbb{C}$ définie par

$$\forall x \in \mathbb{R},\ g(x) = \sum_{n \in \mathbb{Z}} f(x+n)$$

est bornée. Elle est de plus continue et 1-périodique. Calculons les coefficients de Fourier de la fonction g. Pour $n \in \mathbb{Z}$, on a

$$\widehat{g}(n) = \int_0^1 g(t) e^{-2\pi i n t} \, dt = \sum_{k \in \mathbb{Z}} \int_0^1 f(k+t) e^{-2\pi i n t} \, dt = \sum_{k \in \mathbb{Z}} \int_k^{k+1} f(t) e^{-2\pi i n t} \, dt = \widehat{f}(n).$$

Comme f est de classe $\mathcal{C}^2$ et que f' et f'' sont intégrables, on a $\widehat{f}(x) =_{\pm\infty} O(x^{-2})$. Ainsi la famille des coefficients de Fourier de g est sommable. On en conclut que g est égale à la somme de sa série de Fourier, c'est-à-dire

$$\forall x \in \mathbb{R}, \quad g(x) = \sum_{n \in \mathbb{Z}} \widehat{g}(n) e^{2\pi i n x}.$$

En évaluant cette égalité en $x = 0$, on obtient la formule de Poisson. $\square$

Pour $t > 0$, on pose $\theta(t) = \sum_{n\in\mathbb{Z}} e^{-\pi n^2 t}$. Cette série est appelée *série theta*.

Lemme. *Pour $t > 0$, on a $\theta(t) = t^{-\frac{1}{2}}\theta(t^{-1})$.*

Démonstration. Soit $t > 0$. Nous allons appliquer la formule de Poisson à la fonction f_t définie, pour $x \in \mathbb{R}$, par $f_t(x) = e^{-\pi x^2 t}$. Il s'agit d'une fonction $\mathcal{C}^\infty$ dont toutes les dérivées successives sont intégrables. Il faut donc calculer la transformée de Fourier de f_t. Remarquons que $f_t'(x) = -2\pi x t f_t(x)$ et que

$$\widehat{f_t}'(x) = \int_{\mathbb{R}} -2\pi i u e^{-\pi u^2 t} e^{-2\pi i u x}\, du = -\int_{\mathbb{R}} 2\pi t^{-1} x e^{-\pi u^2 t} e^{2\pi i u x}\, du = -2\pi t^{-1} x \widehat{f_t}(x).$$

Les fonctions $f_{t^{-1}}$ et $\widehat{f_t}$ sont donc solutions de la même équation différentielle ordinaire de degré 1, il existe donc un nombre réel C tel que $\widehat{f_t} = C f_{t^{-1}}$. On peut évaluer cette égalité en $x = 0$ pour déterminer C. On obtient

$$C = \widehat{f_t}(0) = \int_{\mathbb{R}} e^{-\pi u^2 t}\, du = t^{-\frac{1}{2}} \int_{\mathbb{R}} e^{-\pi u^2}\, du = t^{-\frac{1}{2}}.$$

La formule recherchée est alors une conséquence de la formule de Poisson :

$$\theta(t) = \sum_{n\in\mathbb{Z}} f_t(n) = \sum_{n\in\mathbb{Z}} \widehat{f_t}(n) = t^{-\frac{1}{2}} \sum_{n\in\mathbb{Z}} f_{t^{-1}}(n) = t^{-\frac{1}{2}}\theta(t^{-1}). \qquad \square$$

Preuve de l'équation fonctionnelle de la fonction ξ. Soit $s \in \Pi_1$. On a alors

$$\begin{aligned}
\xi(s) = \pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) &= \sum_{n\geqslant 1} \int_0^{+\infty} \pi^{-\frac{s}{2}} n^{-s} t^{\frac{s}{2}} e^{-t} \frac{dt}{t} \\
&= \sum_{n\geqslant 1} \int_0^{+\infty} t^{\frac{s}{2}} e^{-\pi n^2 t} \frac{dt}{t} = \int_0^{+\infty} t^{\frac{s}{2}} \left(\sum_{n\geqslant 1} e^{-\pi n^2 t}\right) \frac{dt}{t} \\
&= \int_0^{+\infty} t^{\frac{s}{2}} \frac{1}{2}(\theta(t) - 1) \frac{dt}{t}.
\end{aligned}$$

Remarquons que

$$\frac{1}{2}(\theta(t) - 1) \sim_{+\infty} e^{-t}$$

de sorte que la fonction

$$s \to \int_1^{+\infty} t^{\frac{s}{2}} \frac{1}{2}(\theta(t) - 1) \frac{dt}{t}$$

est définie et holomorphe sur $\mathbb{C}$. Nous allons donc couper l'intégrale en 1 et utiliser

l'équation fonctionnelle de θ :

$$\begin{aligned}
\xi(s) &= \int_0^1 t^{\frac{s}{2}}\frac{1}{2}(\theta(t)-1)\frac{dt}{t} + \int_1^{+\infty} t^{\frac{s}{2}}\frac{1}{2}(\theta(t)-1)\frac{dt}{t} \\
&= \int_1^{+\infty} t^{-\frac{s}{2}}\frac{1}{2}(\theta(t^{-1})-1)\frac{dt}{t} + \int_1^{+\infty} t^{\frac{s}{2}}\frac{1}{2}(\theta(t)-1)\frac{dt}{t} \\
&= \int_1^{+\infty} t^{-\frac{s}{2}}\frac{1}{2}(t^{\frac{1}{2}}\theta(t)-1)\frac{dt}{t} + \int_1^{+\infty} t^{\frac{s}{2}}\frac{1}{2}(\theta(t)-1)\frac{dt}{t} \\
&= \int_1^{+\infty} t^{\frac{1-s}{2}}\frac{1}{2}(\theta(t)-1)\frac{dt}{t} + \int_1^{+\infty} t^{\frac{s}{2}}\frac{1}{2}(\theta(t)-1)\frac{dt}{t} + \int_1^{+\infty}\frac{1}{2}(t^{\frac{1-s}{2}}-t^{-\frac{s}{2}})\frac{dt}{t} \\
&= \underbrace{\int_1^{+\infty} t^{\frac{s}{2}}\frac{1}{2}(\theta(t)-1)\frac{dt}{t} + \int_1^{+\infty} t^{\frac{1-s}{2}}\frac{1}{2}(\theta(t)-1)\frac{dt}{t}}_{A} - \underbrace{\left(\frac{1}{s}+\frac{1}{1-s}\right)}_{B}.
\end{aligned}$$

Comme nous l'avons plus haut, le terme A est holomorphe sur $\mathbb{C}$ et reste invariant si l'on remplace s par $1-s$. Le terme B est méromorphe sur $\mathbb{C}$ et vérifie la même condition d'invariance. La fonction ξ se prolonge donc à $\mathbb{C}$ en une fonction méromorphe vérifiant $\xi(s) = \xi(1-s)$. Notons au passage que la fonction ξ a exactement deux pôles : en 0 et en 1. □

Donnons quelques conséquences remarquables de cette équation fonctionnelle.

Corollaire. *La fonction ξ ne s'annule pas en dehors de la bande $\{s \in \mathbb{C} \mid 0 \leqslant \mathrm{Re}(s) \leqslant 1\}$. De plus, les seuls zéros de la fonction ζ hors de la bande $\{s \in \mathbb{C} \mid 0 \leqslant \mathrm{Re}(s) \leqslant 1\}$ sont les éléments de $-2\mathbb{N}^*$.*

Démonstration. Comme les fonctions $s \mapsto \Gamma(s/2)$ et ζ ne s'annulent pas sur l'ouvert Π_1, la fonction ξ ne s'y annule pas non plus. En utilisant l'équation fonctionnelle, on en conclut qu'elle ne s'annule pas pour $\mathrm{Re}(s) < 0$. On en déduit le résultat pour la fonction ζ en remarquant que les seuls zéros de la fonction $s \mapsto \Gamma(s/2)^{-1}$ de partie réelle < 0 sont les éléments de $-2\mathbb{N}^*$. □

Corollaire. *Si $n \in \mathbb{N}^*$, on a*

$$\zeta(2n) = -\frac{1}{2}(2\pi i)^{2n}\frac{B_{2n}}{(2n)!}.$$

Démonstration. L'équation fonctionnelle de ξ nous donne $\xi(2n) = \xi(1-2n)$. Ainsi en utilisant successivement la formule des compléments, la formule de duplication et la

formule donnant la valeur de $\zeta(1-2n)$, on obtient

$$\begin{aligned}\zeta(2n) &= \pi^n\Gamma(n)^{-1}\Gamma\left(\frac{1}{2}-n\right))\pi^{\frac{2n-1}{2}}\zeta(1-2n)\\ &= \pi^{2n}\Gamma(n)^{-1}\Gamma\left(n+\frac{1}{2}\right)^{-1}\sin\left(\frac{\pi}{2}+\pi n\right)\zeta(1-2n)\\ &= \pi^{2n}(-1)^n 2^{2n-1}\Gamma(2n)^{-1}\zeta(1-2n)\\ &= \frac{1}{2}(2\pi i)^{2n}\frac{B_{2n}}{(2n)!}.\end{aligned}$$

□

Remarque. 1) Les zéros de ζ hors de la bande $\{s\in\mathbb{C}\mid 0\leqslant \mathrm{Re}(s)\leqslant 1\}$ sont appelés *zéros triviaux* de la fonction ζ.

2) Il est conjecturé que les seuls zéros de ζ dans la bande $\{s\in\mathbb{C}\mid 0\leqslant \mathrm{Re}(s)\leqslant 1\}$ ont une partie réelle égale à $1/2$, autrement dit sont situés sur l'axe de symétrie de l'équation fonctionnelle. Cette conjecture, connue sous le nom d'*Hypothèse de Riemann* reste non démontrée ou infirmée à ce jour.

3) On sait très peu de choses sur les valeurs de $\zeta(n)$ lorsque n est un entier impair supérieur à 3. On sait que $\zeta(3)$ est irrationnel (Apéry, 1978) et qu'il existe une infinité d'entiers positifs impairs n tels que $\zeta(n)$ est irrationnel (Rivoal, 2000).

4.1.6 La fonction zeta sur la droite $\mathrm{Re}(s)=1$

Le but de cette partie est de prouver le résultat suivant, dû à Hadamard et de la Vallée-Poussin.

Théorème 4.8. *Si $t\in\mathbb{R}^\times$, on a $\zeta(1+it)\neq 0$.*

Démonstration. Pour $(\sigma,t)\in\,]1,+\infty[\,\times\mathbb{R}$, on pose

$$f(\sigma+it)=\zeta(\sigma)^3\zeta(\sigma+it)^4\zeta(\sigma+2it).$$

Rappelons que si $|z|<1$, on pose

$$\log(1+z)=\sum_{n\geqslant 1}\frac{(-1)^{n-1}}{n}z^n.$$

On a alors $\log|1+z|=\mathrm{Re}(\log(1+z))$. Si p est premier, et $(\sigma,t)\in\,]1,+\infty[\,\times\mathbb{R}$, on a $|p^{-\sigma+it}|<1$ de sorte que

$$\begin{aligned}\log|f(\sigma+it)| &= -3\sum_p\log\left|1-\frac{1}{p^\sigma}\right|-4\sum_p\log\left|1-\frac{1}{p^{\sigma+it}}\right|-\sum_p\log\left|1-\frac{1}{p^{\sigma+2it}}\right|\\ &= 3\sum_p\sum_{k\geqslant 1}\frac{1}{k}p^{-k\sigma}+4\sum_p\sum_{k\geqslant 1}\frac{1}{k}\,\mathrm{Re}(p^{-k(\sigma+it)})+\sum_p\sum_{k\geqslant 1}\frac{1}{k}\,\mathrm{Re}(p^{-k(\sigma+2it)})\\ &= \sum_p\sum_{k\geqslant 1}\frac{1}{k}p^{-k\sigma}(3+4\cos(kt\log(p))+\cos(2kt\log(p))).\end{aligned}$$

Remarquons alors que, pour $\theta \in \mathbb{R}$,

$$\begin{aligned} 3 + 4\cos(\theta) + \cos(2\theta) &= 3 + 4\cos(\theta) + 2\cos^2(\theta) - 1 \\ &= 2(1 + 2\cos(\theta) + \cos^2(\theta)) = 2(1 + \cos\theta)^2 \geqslant 0. \end{aligned}$$

On en conclut que

$$\forall \sigma > 1,\ \forall t \in \mathbb{R}, \quad |f(\sigma + it)| \geqslant 1. \tag{4.1}$$

Soit $t \in \mathbb{R}^\times$ et supposons par l'absurde que $\zeta(1+it) = 0$. Soit $r \geqslant 1$ l'ordre du zéro de ζ en $1+it$. On a donc $\zeta(\sigma+it) \sim_{\sigma\to 1} c(\sigma-1)^r$ pour un certain $c \neq 0$. Comme par ailleurs $\zeta(\sigma) \sim_{\sigma\to 1} (\sigma-1)^{-1}$, on a

$$\zeta(\sigma)^3\zeta(\sigma+it)^4 \sim_{\sigma\to 1} c(\sigma-1)^{4r-3}$$

et donc, puisque ζ n'a pas de pôle en $1+2it$,

$$\lim_{\sigma\to 1} \zeta(\sigma)^3\zeta(\sigma+it)^4\zeta(\sigma+2it) = 0$$

ce qui contredit l'inégalité (4.1). □

4.1.7 Le théorème taubérien d'Ikehara

Théorème 4.9 (Théorème d'Ikehara)**.** *Soit $h : [0,+\infty[\to [0,+\infty[$ une fonction croissante et continue par morceaux. On suppose qu'il existe un nombre réel $\sigma_0 > 0$ tel que, pour $s \in \Pi_{\sigma_0}$, la fonction $t \mapsto e^{-st}h(t)$ est intégrable sur $[0,+\infty[$ et qu'il existe un réel $A > 0$ tel que la fonction*

$$s \mapsto \int_0^{+\infty} e^{-st}h(t)\,dt - \frac{A}{s-\sigma_0}$$

se prolonge une fonction continue sur $\overline{\Pi}_{\sigma_0}$. Alors

$$\lim_{t\to+\infty} e^{-\sigma_0 t}h(t) = A.$$

Avant de démontrer ce théorème, nous allons en déduire une version adaptée aux séries de Dirichlet.

Théorème 4.10. *Soit f une fonction arithmétique à valeurs dans $[0,+\infty[$ d'abscisse de convergence $\sigma_0 = \sigma_c(f) = \sigma_a(f)$. On suppose qu'il existe un nombre réel $A > 0$ tel que la fonction holomorphe*

$$s \mapsto D(f,s) - \frac{A}{s-\sigma_0}$$

se prolonge en une fonction continue sur $\overline{\Pi}_{\sigma_0}$. Alors

$$M_f(x) = \sum_{n\leqslant x} f(n) \sim_{x\to+\infty} A\sigma_0^{-1}x^{\sigma_0}.$$

Démonstration. Pour $t \geqslant 0$, posons $h(t) = \sum_{n \leqslant e^t} f(n) = M_f(e^t)$. La fonction h est à valeurs positives, croissante et continue par morceaux sur $[0, +\infty[$. Pour tout $\varepsilon > 0$, on a

$$\sum_{n \leqslant x} f(n) \leqslant x^{\sigma_0+\varepsilon} \sum_{n \leqslant x} \frac{f(n)}{n^{\sigma_0+\varepsilon}} = x^{\sigma_0+\varepsilon} D(f, \sigma_0 + \varepsilon) = O(x^{\sigma_0+\varepsilon}).$$

On en déduit que la fonction $t \mapsto h(t)e^{-st}$ est intégrable pour tout $s \in \Pi_{\sigma_0}$. Calculons

$$\begin{aligned}
\int_0^{+\infty} h(t)e^{-st}\,dt &= \int_1^{+\infty} u^{-(1+s)} M_f(u)\,du \\
&= \lim_{N \to +\infty} \int_1^N u^{-(1+s)} M_f(u)\,du \\
&= \lim_{N \to +\infty} \frac{1}{s} \sum_{n \leqslant N} n^{-s} f(n) - s^{-1} N^{-s} M_f(N) \\
&= s^{-1} D(f, s),
\end{aligned}$$

le passage de la deuxième ligne à la troisième ligne découlant d'une sommation par parties. On a alors, pour $s \in \Pi_{\sigma_0}$,

$$\int_0^{+\infty} h(t)e^{-st}\,dt - \frac{\sigma_0^{-1} A}{s - \sigma_0} = s^{-1} \left(D(f, s) - \frac{A}{s - \sigma_0} \right) - \frac{\sigma_0^{-1} A}{s}$$

et cette fonction se prolonge donc en une fonction continue sur $\overline{\Pi}_{\sigma_0}$. On déduit du théorème 4.9 que $M_f(e^t) \sim A\sigma_0^{-1} e^{\sigma_0 t}$ en $+\infty$ et donc que $M_f(x) \sim A\sigma_0^{-1} x^{\sigma_0}$ en $+\infty$. □

On peut en déduire le théorème des nombres premiers.

Théorème 4.11. *On a*

$$\psi(x) \sim_{+\infty} x \quad \text{et} \quad \pi(x) \sim_{+\infty} \frac{x}{\log x}.$$

Démonstration. D'après le théorème 2.6, il suffit de prouver que $\psi(x) \sim_{+\infty} x$. On applique alors le théorème 4.10 à la fonction arithmétique Λ. On a déjà remarqué que, pour $s \in \Pi_1$

$$D(\Lambda, s) = -\frac{\zeta'(s)}{\zeta(s)}.$$

Comme la fonction ζ est méromorphe sur $\mathbb{C}$, ne possède pas de zéro sur la droite $\mathrm{Re}(s) = 1$ et possède un unique pôle simple en $s = 1$, on en conclut que la fonction $-\frac{\zeta'}{\zeta}$ possède un unique pôle sur $\overline{\Pi}_1$, il s'agit d'un pôle en $s = 1$, qui est simple et de résidu 1. Autrement dit la fonction holomorphe $s \mapsto D(\Lambda, s) - \frac{1}{s-1}$ se prolonge en une fonction continue sur $\overline{\Pi}_1$. En appliquant le théorème 4.10, on en conclut que

$$M_\Lambda(x) = \psi(x) \sim_{+\infty} x.$$

□

4.1.8 Démonstration du théorème d'Ikehara

Nous allons à présent démontrer le théorème 4.9. Commençons par choisir une fonction K de $\mathbb{R}$ dans $[0,+\infty[$ intégrable et dont la transformée de Fourier est à support compact. Pour montrer qu'une telle fonction existe, partons de k définie par

$$k(x) = \begin{cases} 0 & \text{si } x \notin [-1,1] \\ 1-|x| & \text{si } x \in [-1,1] \end{cases}$$

La fonction k est alors continue et à support compact. Calculons sa transformée de Fourier. Si $x \in \mathbb{R} \setminus \{0\}$, on a

$$\begin{aligned} \widehat{k}(x) = \int_{\mathbb{R}} k(t)e^{-2\pi ixt}\,dt &= \int_0^1 (1-t)e^{-2\pi ixt}\,dt + \int_{-1}^0 (1+t)e^{-2\pi ixt}\,dt \\ &= 2\int_0^1 (1-t)\cos(2\pi xt)\,dt \\ &= 2\int_0^1 \frac{\sin(2\pi xt)}{2\pi x}\,dt = \left[-\frac{2\cos(2\pi xt)}{(2\pi x)^2}\right]_0^1 \\ &= \frac{1}{2\pi^2x^2}(1-\cos(2\pi x)) = \frac{\sin^2(\pi x)}{(\pi x)^2}. \end{aligned}$$

Par continuité de $\widehat{k}$, on a alors $\widehat{k}(0) = 1$. Comme $\widehat{k}$ est intégrable, la formule d'inversion de Fourier et la parité de $\widehat{k}$ impliquent que $k = \widehat{\widehat{k}}$, on peut donc choisir $K = \widehat{k}$. Pour $\lambda > 0$, on pose alors

$$K_\lambda = \lambda K(\lambda \cdot).$$

Remarquons que, pour $x \in \mathbb{R}$,

$$\widehat{K_\lambda}(x) = \lambda \int_{\mathbb{R}} K(\lambda t)e^{2\pi ixt}\,dt = \widehat{K}(\lambda^{-1}x)$$

et donc que $\widehat{K_\lambda}$ est à support dans $[-\lambda,\lambda]$

Lemme. *Soit $H : [0,+\infty[\to [0,+\infty[$ une fonction continue telle que $\int_0^{+\infty} H(t)e^{-st}\,dt$ converge pour tout $s \in \Pi_0$ et telle qu'il existe $A > 0$ pour lequel la fonction*

$$s \mapsto \int_0^{+\infty} H(t)e^{-st}\,dt - \frac{A}{s}$$

se prolonge par continuité sur $\overline{\Pi}_0$. Alors, pour tout $\lambda > 0$, le produit de convolution $H * K_\lambda$ est défini et

$$\forall \lambda > 0, \quad \lim_{x \to +\infty} (H * K_\lambda)(x) = A.$$

Démonstration. Soit H une fonction vérifiant les hypothèses du lemme. Pour $\sigma > 0$ et $t \geqslant 0$, posons $H_\sigma(t) = H(t)e^{-\sigma t}$, $G_\sigma(t) = H_\sigma(t) - Ae^{-\sigma t}$ et on pose $H_\sigma(t) = G_\sigma(t) = 0$

pour $t < 0$. Les fonctions H_σ et G_σ sont alors intégrables et leurs transformées de Fourier valent, pour $x \in \mathbb{R}$

$$\widehat{H_\sigma}(x) = \int_0^{+\infty} h(t)e^{-(\sigma+2\pi ix)t}\,dt, \quad \widehat{G_\sigma}(x) = \int_0^{+\infty} h(t)e^{-(\sigma+2\pi ix)t}\,dt - \frac{A}{\sigma+2\pi ix}.$$

Pour $\lambda > 0$, la fonction $G_\sigma * K_\lambda$ est intégrable et sa transformée de Fourier vaut $\widehat{G_\sigma}\widehat{K_\lambda}$. Cette dernière, étant continue à support compact, est intégrable et la formule d'inversion de Fourier nous donne

$$\forall x \in \mathbb{R}, \quad (G_\sigma * K_\lambda)(x) = \int_{-\lambda}^{\lambda} \widehat{G_\sigma}(t)\widehat{K_\lambda}(t)e^{2\pi ixt}\,dt.$$

Pour $t \in \mathbb{R}$, posons alors $g(t)$ la valeur en it du prolongement continue de la fonction $s \mapsto \int_0^{+\infty} h(t)e^{-st}\,dt - \frac{A}{s}$. Par compacité de $[0,1] \times [-\lambda, \lambda]$, on en conclut que

$$\forall x \in \mathbb{R}, \quad \lim_{\sigma\to 0}(H_\sigma * K_\lambda)(x) = \int_{-\lambda}^{\lambda} g(t)\widehat{K_\lambda}(t)e^{2\pi ixt}\,dt. \tag{4.2}$$

Par ailleurs, pour $x \in \mathbb{R}$, on a

$$\lim_{\sigma\to 0}(H_\sigma * K_\lambda)(x) = \lim_{\sigma\to 0}\int_0^{+\infty} H(t)e^{-\sigma t}K_\lambda(x-t)\,dt = \int_0^{+\infty} H(t)K_\lambda(x-t)\,dt$$

d'après le théorème de convergence monotone. Comme pour les mêmes raisons,

$$\lim_{\sigma\to 0}\int_0^{+\infty} e^{-\sigma t}K_\lambda(x-t)\,dt = \int_0^{+\infty} K_\lambda(x-t) = \int_{-\infty}^{x} K_\lambda(t)\,dt < +\infty$$

on déduit de (4.2) que la convolution $H * K_\lambda$ est bien définie et que

$$\forall \lambda > 0,\ \forall x \in \mathbb{R}, \quad (H * K_\lambda)(x) = A\int_0^{+\infty} K_\lambda(t)\,dt + \int_{-\lambda}^{\lambda} g(t)\widehat{K_\lambda}(t)e^{2\pi ixt}\,dt.$$

On déduit alors du lemme de Riemann-Lebesgue que

$$\forall \lambda > 0, \quad \lim_{x\to+\infty}(H * K_\lambda)(x) = A\int_{\mathbb{R}} K_\lambda(t)\,dt = A\int_{\mathbb{R}} K(t)\,dt = A\widehat{K}(0) = A. \qquad \square$$

Preuve du théorème 4.9. Soit h une fonction vérifiant les hypothèses du théorème 4.9. La fonction H définie par $H(t) = h(t)e^{-\sigma_0 t}$ vérifie alors les hypothèses du lemme 4.1.8. On en déduit que, pour tout $\lambda > 0$,

$$A = \lim_{x\to+\infty}\int_0^{+\infty} h(t)e^{-\sigma_0 t}K_\lambda(x-t)\,dt = \lim_{x\to+\infty}\int_{-\infty}^{x} K_\lambda(t)h(x-t)e^{-\sigma_0(x-t)}\,dt.$$

Par ailleurs, pour tous $x \leqslant y$, on a

$$H(y) = h(y)e^{-\sigma_0 y} \geqslant h(x)e^{-\sigma_0 y} = H(x)e^{\sigma_0(x-y)}.$$

Ainsi

$$\begin{aligned}\forall\lambda>0,\,\forall a>0,\quad A &\geqslant \limsup_{x\to+\infty}\int_{-a}^{a} K_\lambda(t)H(x-t)\,dt\\ &\geqslant \limsup_{x\to+\infty}\int_{-a}^{a} K_\lambda(t)H(x-a)e^{\sigma_0(t-a)}\,dt\\ &\geqslant \limsup_{x\to+\infty} H(x-a)e^{-2\sigma_0 a}\int_{-a}^{a} K_\lambda(t)\,dt.\end{aligned}$$

On en déduit

$$\limsup_{x\to+\infty} H(x) \leqslant A\frac{e^{2\sigma_0 a}}{\int_{-a}^{a} K_\lambda(t)\,dt} = A\frac{e^{2\sigma_0 a}}{\int_{-\lambda a}^{\lambda a} K(t)\,dt}.$$

En prenant $a=\lambda^{-\frac{1}{2}}$ et faisant tendre λ vers $+\infty$, on obtient

$$\limsup_{x\to+\infty} H(x) \leqslant A.$$

Comme h, et donc H est continue par morceaux, cette inégalité implique H est bornée sur $[0,+\infty[$. Soit $C>0$ tel que $H(t)\leqslant C$ pour tout $t\geqslant 0$. De même, on a

$$\begin{aligned}\forall\lambda>0,\,\forall a>0,\quad \int_{-a}^{a} K_\lambda(t)H(x-t)\,dt &\leqslant \int_{-a}^{a} H(x+a)e^{\sigma_0(a+t)}K_\lambda(t)\,dt\\ &\leqslant H(x+a)e^{2\sigma_0 a}\int_{-a}^{a} K_\lambda(t)\,dt\end{aligned}$$

et donc

$$\begin{aligned}\forall\lambda>0,\,\forall a>0,\quad \liminf_{x\to+\infty} H(x) &\geqslant e^{-2\sigma_0 a}\int_{-a}^{a} H(x-t)K_\lambda(t)\,dt\\ &\geqslant e^{-2\sigma_0 a}\int_{\mathbb{R}} H(x-t)K_\lambda(t)\,dt - Ce^{-2\sigma_0 a}\int_{\mathbb{R}\setminus[-a,a]} K_\lambda(t)\,dt\\ &\geqslant e^{-2\sigma_0 a}\int_{\mathbb{R}} H(x-t)K_\lambda(t)\,dt - Ce^{-2\sigma_0 a}\int_{\mathbb{R}\setminus[-\lambda a,\lambda a]} K(t)\,dt.\end{aligned}$$

En faisant tendre λ vers $+\infty$, on en déduit

$$\forall a>0,\quad \liminf_{x\to+\infty} H(x) \geqslant Ae^{-2\sigma_0 a}$$

et donc $\liminf_{x\to+\infty} H(x)\geqslant A$. Finalement on a

$$A\leqslant \liminf_{x\to+\infty} H(x) \leqslant \limsup_{x\to+\infty} H(x)\leqslant A$$

et donc $\lim_{x\to+\infty} H(x)=A$ d'où le résultat. □

4.2 Le théorème de Dirichlet

4.2.1 Fonctions L de Dirichlet

Soit χ un caractère de Dirichlet de module $N \in \mathbb{N}^*$. On appelle *fonction L de Dirichlet* associée à χ la série de Dirichlet

$$L(\chi, s) = \sum_{n \geqslant 1} \frac{\chi(n)}{n^s} (= D(\chi, s)).$$

Comme $|\chi(n)| \leqslant 1$ pour tout $n \in \mathbb{Z}$, on a $\sigma_a(\chi) \leqslant 1$. Comme la fonction χ est complètement multiplicative, et que $\chi(p) = 0$ si $p \mid N$, on a

$$\forall s \in \Pi_1, \quad L(\chi, s) = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1} = \prod_{p \nmid N} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}.$$

Considérons le cas particulier où $\chi = \chi_0$ est le caractère trivial modulo N. On a alors

$$L(\chi_0, s) = \prod_{p \nmid N} \left(1 - \frac{1}{p^s}\right)^{-1} = \zeta(s) \prod_{p \mid N} \left(1 - \frac{1}{p^s}\right).$$

En particulier on en déduit que la fonction $L(\chi_0, -)$ se prolonge méromorphiquement à $\mathbb{C}$ avec un unique pôle en $s = 1$, ce pôle est simple de résidu $\prod_{p|N}(1 - \frac{1}{p}) = \frac{\varphi(N)}{N}$. Comme par ailleurs,

$$\sum_{n \geqslant 1} \left| \frac{\chi(n)}{n^s} \right| = L(\chi_0, \mathrm{Re}(s)),$$

on en déduit que l'abscisse de convergence absolue de toute fonction L de Dirichlet est en fait égale à 1.

Supposons désormais que $\chi \neq \chi_0$. Pour tout $n \geqslant 1$, on a

$$M_\chi(n) = \sum_{k=1}^{n} \chi(k) = \sum_{k=1}^{q-1} \underbrace{\left(\sum_{i=kN+1}^{(k+1)N} \chi(i) \right)}_{=0} + \sum_{i=1}^{r} \chi(i)$$

où $n = qN + r$ avec $0 < r \leqslant N$. On en déduit en particulier que

$$\forall n \geqslant 1, \quad |M_\chi(n)| \leqslant N.$$

Le procédé de sommation par parties nous donne alors

$$\sum_{k=1}^{n} \frac{\chi(k)}{k^s} = \frac{M_\chi(n)}{n^s} + s \int_1^n \frac{M_\chi(t)}{t^{s+1}}\, dt.$$

Comme la fonction M_χ est bornée, on en conclut que cette série converge pour $\mathrm{Re}(s) > 0$. Ainsi $\sigma_c(\chi) \leqslant 0$. Cependant la suite $(\chi(n)n^{-s})_{n \geqslant 1}$ ne converge pas pour $\mathrm{Re}(s) < 0$, on a donc $\sigma_c(\chi) = 0$. On a donc prouvé le résultat suivant.

Théorème 4.12. *Soit χ un caractère de Dirichlet de module N.*

(i) Si $\chi = \chi_0$, la fonction L associé à χ_0 se prolonge en une fonction méromorphe sur $\mathbb{C}$ ayant un unique pôle, simple, en $s = 1$.

(ii) Si $\chi \neq \chi_0$, la fonction L associée à χ se prolonge en une fonction holomorphe sur Π_0.

Remarque. On peut en fait montrer que la fonction L d'un caractère $\chi \neq \chi_0$ se prolonge en une fonction holomorphe sur $\mathbb{C}$ tout entier et que cette fonction admet une équation fonctionnelle similaire à celle de la fonction ζ mais nous n'utiliserons pas ce résultat dans la suite.

4.2.2 Énoncé du théorème

Soit $N \in \mathbb{N}^*$ et soit $a \in \mathbb{Z}$ un entier. On peut se demander s'il existe une infinité de nombres premiers p tels que $p \equiv a\,[N]$. Une condition nécessaire pour cela est que $a \wedge N = 1$. Il est remarquable que c'est condition est en fait suffisante.

Nous fixons désormais $a \in \mathbb{Z}$ tel que $a \wedge N = 1$ et posons, pour $x \in \mathbb{R}$,

$$\pi(x; N, a) = \mathrm{Card}\{p \leqslant x \mid p \equiv a\,[N]\}.$$

Théorème 4.13. *(i)* $\lim_{x \to +\infty} \pi(x; N, a) = +\infty$ *(Dirichlet, 1830).*

(ii) On a

$$\pi(x; N, a) \sim_{+\infty} \frac{1}{\varphi(N)} \frac{x}{\log x}.$$

4.2.3 Démonstration

Nous allons suivre une stratégie proche de la stratégie de démonstration du théorème des nombres premiers. Nous commençons donc par introduire un analogue de la fonction ψ de Tchebychev. Pour $x \in \mathbb{R}$, on pose

$$\psi(x; N, a) = \sum_{\substack{n \leqslant x \\ n \equiv a\,[N]}} \Lambda(n).$$

Un raisonnement analogue à celui du théorème 2.6 montre qu'il est équivalent de prouver

$$\psi(x; N, a) \sim_{+\infty} \frac{1}{\varphi(N)} x. \tag{4.3}$$

Par ailleurs, comme la fonction χ est complètement multiplicative, on a

$$e = \chi e = \chi(\mathbb{1} * \mu) = (\chi) * (\chi\mu)$$

de sorte que l'inverse de χ pour la composition arithmétique est la fonction arithmétique $\chi\mu$. De plus $\chi\Lambda = (\chi \log) * (\chi\mu)$, on en déduit

$$\forall s \in \Pi_1, \quad -\frac{L'(\chi, s)}{L(\chi, s)} = \sum_{n \geqslant 1} \frac{\Lambda(n)\chi(n)}{n^s} = D(\chi\Lambda, s).$$

Rappelons que, d'après le théorème 3.20, on a, puisque $a \wedge N = 1$,

$$\frac{1}{\varphi(N)} \sum_{\chi\,[N]} \overline{\chi(a)}\chi(n) = \begin{cases} 1 & \text{si } n \equiv a\,[N] \\ 0 & \text{sinon.} \end{cases}$$

Posons alors

$$f(n) = \begin{cases} \Lambda(n) & \text{si } n \equiv a\,[N] \\ 0 & \text{sinon.} \end{cases}$$

On en déduit que

$$\forall s \in \Pi_1, \quad D(f, s) = -\frac{1}{\varphi(N)} \sum_{\chi\,[N]} \overline{\chi(a)} \frac{L'(\chi, s)}{L(\chi, s)}.$$

Comme la fonction sommatoire de la fonction arithmétique f est exactement la fonction $\psi(-; N, a)$, le théorème d'Ikehara 4.10 suggère qu'il devrait être utile d'étudier le comportement des fonctions L de Dirichlet sur la droite d'équation $\mathrm{Re}(s) = 1$. Posons, pour $s \in \Pi_1$,

$$\begin{aligned} g(s) &= D(f, s) - \frac{1}{\varphi(N)} \frac{1}{s-1} \\ &= \frac{1}{\varphi(N)} \left(-\frac{L'(\chi_0, s)}{L(\chi_0, s)} - \frac{1}{s-1} \right) - \frac{1}{\varphi(N)} \sum_{\chi \neq \chi_0} \overline{\chi(a)} \frac{L'(\chi, s)}{L(\chi, s)}. \end{aligned}$$

On sait déjà que la fonction $L(\chi_0, -)$ a un pôle simple en $\mathrm{Re}(s) = 1$. De plus, pour $\mathrm{Re}(s) = 1$, on a

$$L(\chi_0, s) = \zeta(s) \prod_{p \mid N} \left(1 - \frac{1}{p^s}\right).$$

On déduit donc du théorème 4.8 que la fonction $L(\chi_0, -)$ ne s'annule pas sur la droite d'équation $\mathrm{Re}(s) = 1$. On en déduit que la fonction $s \mapsto -\frac{L'(\chi_0, s)}{L(\chi_0, s)} - \frac{1}{s-1}$ se prolonge en une fonction continue sur $\overline{\Pi}_1$.

Si l'on prouve que chaque fonction $L(\chi, -)$ avec $\chi \neq \chi_0$ ne s'annule pas sur $\overline{\Pi}_1$, on en conclut que la fonction g se prolonge en une fonction continue sur $\overline{\Pi}_1$. On déduit alors l'équivalent 4.3 du théorème d'Ikehara.

On sait déjà que si $\mathrm{Re}(s) > 1$, on a $e = \chi * (\chi\mu)$ et donc, $L(\chi, s)L(\chi\mu, s) = 1$, de sorte que $L(\chi, s) \neq 1$. L'équivalent (4.3), et le théorème 4.13, sont alors conséquences du résultat suivant, qu'il nous reste à démontrer.

Théorème 4.14. *Soit $\chi \neq \chi_0$ un caractère de Dirichlet modulo N. Alors*

$$\forall t \in \mathbb{R}, \quad L(1 + it) \neq 0.$$

4.2.4 Non annulation des fonctions L sur la droite $\mathrm{Re}(s) = 1$

Nous allons, dans un premier temps, suivre la même stratégie que pour la fonction zeta. Soit χ un caractère de Dirichlet non trivial de module N. Posons, pour $\sigma > 1$ et $t \in \mathbb{R}$,

$$h(\sigma, t) = L(\chi_0, \sigma)^3 L(\chi, \sigma + it)^4 L(\chi^2, \sigma + 2it).$$

On a alors

$$\log|h(\sigma,t)| = -3\sum_p \log\left|1 - \frac{\chi_0(p)}{p^\sigma}\right| - 4\sum_p \log\left|1 - \frac{\chi(p)}{p^{\sigma+it}}\right| - \sum_p \log\left|1 - \frac{\chi^2(p)}{p^{\sigma+2it}}\right|.$$

On a $\chi_0(p) = \chi(p) = 0$ si $p \mid N$, et, pour $p \nmid N$, $\chi_0(p) = 1$ et $\chi(p) = e^{i\theta_p}$ pour un certain $\theta_p \in \mathbb{R}$. On obtient

$$\log|h(\sigma,t)| = \sum_{p\nmid N}\sum_{n\geqslant 1} \frac{1}{np^{n\sigma}}(3 + 4\cos(n(\theta_p - t\log p)) + \cos(2n(\theta_p - t\log p))) \geqslant 0.$$

On en déduit que $|h(\sigma, t)| \geqslant 1$ pour tous $\sigma > 1$ et $t \in \mathbb{R}$.

Supposons par l'absurde que $L(\chi, 1 + it) = 0$. Soit r l'ordre d'annulation de $L(\chi, -)$ en $1 + it$. On a alors

$$L(\chi_0, \sigma)^3 L(\chi, \sigma + it)^4 \sim_{\sigma\to 1} c(\sigma - 1)^{4r-3}$$

pour un certain $c \neq 0$. Si $t \neq 0$ ou si $\chi^2 \neq \chi_0$, on sait que la fonciton $L(\chi^2, -)$ n'a pas de pôle en $1 + it$ et on en déduit $\lim_{\sigma\to 1} h(\sigma, t) = 0$, ce qui est absurde.

Ce raisonnement ne nous permet malheureusement pas de conclure lorsque $t = 0$ et $\chi^2 = \chi_0$. Il faut donc traiter à part le cas des caractères de Dirichlet quadratiques.

Fixons donc χ un caractère de Dirichlet modulo N tel que $\chi^2 = \chi_0$ et $\chi \neq \chi_0$. Pour $s \in \Pi_1$, on pose

$$F(s) = \frac{\zeta(s)L(\chi, s)}{\zeta(2s)} = \sum_{n\geqslant 1} \frac{a(n)}{n^s}.$$

Il s'agit d'une série de Dirichlet dont on note $a(n)$ le $n$ième coefficient. On peut écrire

$$\begin{aligned} F(s) &= \prod_p \frac{1 - p^{-2s}}{(1 - p^{-s})(1 - \chi(p)p^{-s})} = \prod_p \frac{1 + p^{-s}}{1 - \chi(p)p^{-s}} \\ &= \prod_p \left(\sum_{k\geqslant 0}(1 + p^{-s})\frac{\chi(p)^k}{p^{ks}}\right) = \prod_p \left(1 + \sum_{k\geqslant 1} \frac{\chi(p)^{k-1} + \chi(p)^k}{p^{ks}}\right). \end{aligned}$$

Ainsi F est la série de Dirichlet associée à la fonction arithmétique multiplicative a définie par

$$a(p^k) = \begin{cases} 1 & \text{si } p^k = 1 \\ \chi(p)^{k-1}(1 + \chi(p)) & \text{sinon.} \end{cases}$$

Comme $\chi(p) \in \{0, 1, -1\}$ pour tout p, on en conclut que $a(p^k) \geqslant 0$ et donc $a(n) \geqslant 0$ pour tout $n \geqslant 1$. Remarquons de plus que la fonction F est méromophe sur Π_0 et que $\zeta(2s) \neq 0$ pour $\mathrm{Re}(s) \geqslant \frac{1}{2}$. Ainsi le seul pôle éventuel de F sur $\Pi_{\frac{1}{2}}$ est le pôle de ζ en $s = 1$. On en déduit que $L(\chi, 1) = 0$ si et seulement si la fonction F est holomorphe sur $\Pi_{\frac{1}{2}}$.

Lemme (Lemme de Landau)**.** *Soit a une fonction arithmétique à valeurs positives. Alors $\sigma_c(a) = \sigma_a(a)$ et la fonction $D(a, -)$ ne se prolonge pas sur en une fonction holomorphe sur un voisinage de $\sigma = \sigma_c(a)$.*

Utilisons ce lemme pour conclure. Si $L(\chi, 1) = 0$, alors la fonction F est holomorphe sur $\Pi_{\frac{1}{2}}$. Comme il s'agit d'une série de Dirichlet d'une fonction arithmétique positive, on déduit du lemme de Landau que son abscisse de convergence $\sigma_c(a)$ est $\leqslant \frac{1}{2}$. En particulier,

$$\forall x \in \left]\frac{1}{2}, 1\right[, \quad F(x) = \sum_{n \geqslant 1} \frac{a(n)}{n^x} \geqslant a(0) = 1.$$

Cependant ni ζ ni $L(\chi, -)$ n'ont de pôle en $\frac{1}{2}$, contrairement à $s \mapsto \zeta(2s)$. On en conclut que $F(\frac{1}{2}) = 0$, ce qui est absurde. On a donc $L(\chi, 1) \neq 0$.

Preuve du lemme de Landau. Posons $\sigma = \sigma_c(a) = \sigma_a(a)$. Supposons par l'absurde qu'il existe un voisinage U de σ sur lequel $F = D(a, -)$ se prolonge en une fonction holomorphe. Soient $x > \sigma$ et $R > x - \sigma$ tels que la boule ouverte $B(x, R)$ de centre x et de rayon R soit contenue dans U et contienne σ (on peut choisir une boule $B(x, r)$ contenue dans U et poser $x = \sigma + \frac{r}{4}$, $R = \frac{r}{2}$). La série entière $\sum_{k \geqslant 0} \frac{F^{(k)}(x)}{k!} X^k$ possède donc un rayon de convergence $\geqslant R$. Par ailleurs, comme $x > \sigma$, on a

$$F^{(k)}(x) = \sum_{n \geqslant 1} (-\log n)^k \frac{a(n)}{n^x}.$$

On obtient donc, pour $x - R < y < \sigma$,

$$\begin{aligned} F(y) &= \sum_{k \geqslant 0} \frac{F^{(k)}(x)}{k!} (y - x)^k = \sum_{k \geqslant 0} \sum_{n \geqslant 1} (-1)^k (\log n)^k \frac{a(n)}{k! n^x} (y - x)^k \\ &= \sum_{k \geqslant 0} \sum_{n \geqslant 1} \underbrace{(\log n)^k \frac{a(n)}{k! n^x} (x - y)^k}_{\geqslant 0} = \sum_{n \geqslant 1} \frac{a(n)}{n^x} \sum_{k \geqslant 0} (\log n)^k \frac{(x - y)^k}{k!} \\ &= \sum_{n \geqslant 1} \frac{a(n)}{n^x} n^{x - y} = \sum_{n \geqslant 1} \frac{a(n)}{n^y}. \end{aligned}$$

Ainsi la série $\sum_{n \geqslant 1} \frac{a(n)}{n^y}$ est convergente de sorte que $\sigma \leqslant y$, ce qui est absurde. □

Chapitre 5

Théorie algébrique des nombres

5.1 Entiers algébriques

5.1.1 Rappels de théorie des corps (sous-corps de $\mathbb{C}$)

Soit K un sous-corps de $\mathbb{C}$. Un élément $\alpha \in \mathbb{C}$ est dit *algébrique sur* K s'il existe un polynôme $P \in K[X]$ non nul tel que $P(\alpha) = 0$. Il existe alors un unique polynôme unitaire P de degré minimal vérifiant $P(\alpha) = 0$. On l'appelle le *polynôme minimal de* α *sur* K et on le note $\pi_{\alpha,K}$. Le degré de $\pi_{\alpha,K}$ est alors appelé le *degré* de α sur K et est noté $\deg_K \alpha$. On a de plus la propriété suivante : si $P \in K[X]$, pour que $P(\alpha) = 0$ il faut et il suffit que $\pi_{\alpha,K}$ divise P. On en déduit que $\pi_{\alpha,K}$ est l'unique polynôme unitaire irréductible de $K[X]$ annulant α.

Lorsque α est algébrique sur $\mathbb{Q}$, on dit parfois simplement que α est un nombre algébrique. On note alors $\pi_\alpha = \pi_{\alpha,\mathbb{Q}}$ et $\deg \alpha = \deg_{\mathbb{Q}} \alpha$.

Si L est un sous-corps de $\mathbb{C}$ contenant K et de dimension finie sur K, on note $[L : K]$ l'entier $\dim_K L$. Rappelons que si $K \subset L \subset M$ sont des sous-corps de $\mathbb{C}$ tels que M est de dimension finie sur L et L de dimension finie sur K, alors $[M : K] = [M : L][L : K]$. Plus précisément, si $(e_1, \ldots, e_r)$ est une base de L sur K et $(f_1, \ldots, f_s)$ est une base de M sur L, alors la famille $(e_i f_j)_{\substack{1 \leqslant i \leqslant r \\ 1 \leqslant j \leqslant s}}$ est une base de M sur K.

Soit $\alpha \in \mathbb{C}$ et soit K un sous-corps de $\mathbb{C}$. Le nombre $\alpha \in \mathbb{C}$ est algébrique sur K si et seulement si il existe un sous-corps L de $\mathbb{C}$ contenant α et K et de dimension finie sur K et tel que $\alpha \in L$. On note $K(\alpha)$ le plus petit sous-corps de $\mathbb{C}$ contenant K et α. Ainsi α est algébrique sur K si et seulement si $K(\alpha)$ est de dimension finie sur K. Si α est algébrique sur K, alors la famille $(1, \alpha, \alpha^2, \ldots, \alpha^{d-1})$ est une base de $K(\alpha)$ sur K et $d = \deg_K \alpha = \deg \pi_{\alpha,K}$. On en déduit que l'ensemble des nombres algébriques sur K est un sous-corps de $\mathbb{C}$. On note $\overline{\mathbb{Q}}$ l'ensemble des nombres algébriques (sous-entendu sur $\mathbb{Q}$). C'est donc un sous-corps de $\mathbb{C}$.

Soit K un sous-corps de $\mathbb{C}$. Un sous-corps L de $\mathbb{C}$ contenant K est dit *algébrique sur*

K si tous ses éléments sont algébriques sur K. Un sous-corps de $\mathbb{C}$ est dit *algébrique* s'il est algébrique sur $\mathbb{Q}$. Un sous-corps algébrique de $\mathbb{C}$ n'est pas toujours de dimension finie sur $\mathbb{Q}$. Par exemple le sous-corps $\overline{\mathbb{Q}}$ est algébrique, mais est de dimension infinie sur $\mathbb{Q}$.

5.1.2 Définition des entiers algébriques

Soit $\alpha \in \mathbb{C}$. On dit que α est un *entier algébrique* s'il existe $P \in \mathbb{Z}[X]$, *unitaire*, tel que $P(\alpha) = 0$.

Exemple. Le nombre $\sqrt{2}$ est un entier algébrique car il est annulé par le polynôme unitaire $X^2 - 2 \in \mathbb{Z}[X]$. Nous démontrerons un peu plus loin que le nombre $\alpha = \frac{1}{2}\sqrt{7}$ est algébrique mais n'est pas un entier algébrique. En effet il est annulé par le polynôme $4X^2 - 7 \in \mathbb{Z}[X]$. Comme ce polynôme n'est pas unitaire, on ne peut pas en conclure que α est un entier algébrique.

Nous pouvons parler d'éléments entiers dans une situation bien plus générale. Soit A un anneau commutatif et soir R un anneau contenant A. On dit qu'un élément $x \in R$ est *entier sur* A s'il existe un polynôme $P \in A[X]$, unitaire, tel que $P(x) = 0$. Un entier algébrique correspond à la situation où $A = \mathbb{Z}$ et $R = \mathbb{C}$: c'est un élément de $\mathbb{C}$ qui est entier sur l'anneau $\mathbb{Z}$.

Théorème 5.1. *Soit $x \in R$. Les assertions suivantes sont équivalentes :*

(i) l'élément x est entier sur A ;

(ii) la sous-A-algèbre $A[x]$ de R engendrée par x est un A-module de type fini ;

(iii) il existe une sous-A-algèbre $B \subset R$ telle que $x \in B$ et qui est un A-module de type fini.

Démonstration. Prouvons l'assertion $(i) \Rightarrow (ii)$. Supposons donc que x est entier sur A. Il existe alors un polynôme unitaire $P(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_0 \in A[X]$ tel que $P(x) = 0$. Soit M le sous-A-module de R engendré par les éléments $1, x, \ldots, x^{d-1}$, c'est-à-dire $M = \sum_{i=0}^{d-1} Ax^i$. C'est un sous-$A$-module de type fini de R puisqu'il est engendré *comme A-module* par une famille finie. On sait de plus que

$$x^d = -\sum_{i=0}^{d-1} a_i x^i \in M.$$

On prouve alors par récurrence sur $n \geqslant d$ que $x^n \in M$ pour tout entier $n \geqslant d$. Ainsi $A[x] \subset M$. L'inclusion réciproque $M \subset A[x]$ est immédiate. Ainsi $A[x]$ est bien un A-module de type fini.

L'implication $(ii) \Rightarrow (iii)$ est immédiate, il suffit de choisir $B = A[x]$.

Prouvons l'implication $(iii) \Rightarrow (i)$. On suppose qu'il existe $B \subset R$ une sous-A-algèbre contenant x qui est de plus un A-module de type fini. Soit $(e_1, \ldots, e_n)$ une famille génératrice de B comme A-module. Comme B est en particulier un sous-anneau

de R, on a $xB \subset B$. Ainsi, pour tout $1 \leqslant i \leqslant n$, il existe des éléments $m_{i,1}, \ldots, m_{i,n} \in A$ tels que

$$xe_i = \sum_{j=1}^{n} m_{i,j} e_j. \tag{5.1}$$

Soit M la matrice $M = (m_{i,j})_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant n}}$. La relation (5.1) implique que la matrice $xI_n - M$ annule le vecteur de B^n de coordonnées $(e_1, \ldots, e_n)$, c'est-à-dire :

$$(xI_n - M) \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} = 0.$$

Rappelons que la formule de Cramer, valable dans l'anneau $\mathcal{M}_n(B)$, nous donne

$$\det(xI_n - M) I_n = {}^t \operatorname{Com}(xI_n - M)(xI_n - M).$$

On en déduit que, pour tout $1 \leqslant i \leqslant n$, on a $\det(xI_n - M)e_i = 0$. Comme les éléments $e_1, \ldots, e_n$ engendrent B comme A-module, il existe des éléments $a_1, \ldots, a_n$ dans A tels que $1 = a_1 e_1 + \cdots + a_n e_n$. On en déduit que

$$\det(xI_n - M) = \det(xI_n - M)1 = 0.$$

Ainsi le polynôme caractéristique de M annule x. C'est un polynôme unitaire de $A[X]$, on en déduit que x est entier sur A. □

Corollaire. *L'ensemble des éléments de R qui sont entiers sur A forment un sous-anneau de R.*

Démonstration. Soient α et β deux éléments de R qui sont entiers sur A. Il suffit de prouver que $\alpha + \beta$, $\alpha - \beta$ et $\alpha\beta$ sont entiers sur A. Comme α est entier sur A, on déduit du théorème 5.1 que $A[\alpha] \subset R$ est un A-module de type fini. De plus β est entier sur A, il est donc en particulier entier sur l'anneau $A[\alpha]$. Ainsi le sous-anneau $A[\alpha, \beta] = A[\alpha][\beta]$ de R est un $A[\alpha]$-module de type fini. Comme $A[\alpha]$ est un A-module de type fini, on en déduit que $A[\alpha, \beta]$ est un A-module de type fini. Finalement $B = A[\alpha, \beta]$ est une sous-algèbre de R, qui est un A-module de type fini et qui contient $\alpha + \beta$, $\alpha - \beta$ et $\alpha\beta$. Le théorème 5.1 implique alors que ces trois éléments sont entiers sur A. □

Exemple. Les nombres complexes $\sqrt{2} + \sqrt{3}$, $i\sqrt[3]{5} + \sqrt{7}$ sont des exemples d'entiers algébriques.

Un sous-corps de $\mathbb{C}$ qui est de dimension finie sur $\mathbb{Q}$ est appelé un *corps de nombres*. L'ensemble des éléments d'un corps de nombres K qui sont entiers sur $\mathbb{Z}$ est un sous-anneau de K que l'on note $\mathcal{O}_K$ et que l'on appelle *anneau des entiers de K*.

Exemple. L'anneau des entiers de $\mathbb{Q}$ et l'anneau $\mathbb{Z}$. En effet, on a démontré au cours du chapitre 1 que si $x \in \mathbb{Q}$ est annulé par un polynôme unitaire $P \in \mathbb{Z}[X]$, alors $x \in \mathbb{Z}$.

On dispose également d'une caractérisation des entiers algébriques en terme de polynôme minimal.

Théorème 5.2. *Soit $\alpha \in \overline{\mathbb{Q}}$ un nombre algébrique. Soit $\pi_\alpha \in \mathbb{Q}[X]$ son polynôme minimal. Pour que α soit un entier algébrique, il faut et il suffit que $\pi_\alpha \in \mathbb{Z}[X]$.*

Démonstration. Si $\pi_\alpha \in \mathbb{Z}[X]$, alors α est un entier algébrique puisque π_α est unitaire et annule α. Réciproquement supposons que α est un entier algébrique. Il existe alors un polynôme unitaire $P \in \mathbb{Z}[X]$ annulant α. Ceci implique que le polynôme π_α divise le polynôme P dans $\mathbb{Q}[X]$. Comme $P \in \mathbb{Z}[X]$, il existe un entier $m \in \mathbb{N}^*$ tel que $m\pi_\alpha \in \mathbb{Z}[X]$ et $m\pi_\alpha$ divise P dans $\mathbb{Z}[X]$. En particulier le coefficient dominant de $m\pi_\alpha$ divise le coefficient dominant de P. Or le coefficient dominant de $m\pi_\alpha$ est m puisque π_α est unitaire et celui de P est 1. On en conclut que $m = 1$ et donc que $\pi_\alpha \in \mathbb{Z}[X]$. □

Corollaire. *Soit $\alpha \in \overline{\mathbb{Q}}$ un nombre algébrique. Si α est un entier algébrique, alors les conjugués de α sont des entiers algébriques.*

Démonstration. En effet, si α est un entier algébrique, son polynôme minimal π_α est un polynôme unitaire de $\mathbb{Z}[X]$. Les conjugués de α sont alors par définition les racines de π_α, qui sont évidemment des entiers algébriques. □

Plus généralement, on peut démontrer le résultat suivant.

Théorème 5.3. *Soient $K \subset L$ deux corps de nombres. Soit $x \in L$. Alors $x \in \mathcal{O}_L$ si et seulement si $\pi_{x,K} \in \mathcal{O}_K[X]$.*

Démonstration. Une direction est immédiate : si $\pi_{x,K} \in \mathcal{O}_K[X]$, alors x est annulé par un polynôme unitaire de $\mathcal{O}_K[X]$ et donc $x \in \mathcal{O}_L$. Réciproquement si $x \in \mathcal{O}_L$, il existe un polynôme unitaire $P \in \mathcal{O}_K[X]$ annulant x. En particulier $\pi_{x,K}$ divise P dans $K[X]$. On en conclut que les racines de $\pi_{x,K}$ sont des racines de P, tous les conjugués de x sur K sont donc des entiers algébriques. Les relations coefficients-racines montrent alors que les coefficients de $\pi_{x,K}$ sont des entiers algébriques, donc des éléments de $\mathcal{O}_K$. Ainsi $\pi_{x,K} \in \mathcal{O}_K[X]$. □

5.1.3 Entiers algébriques quadratiques

Un corps de nombres K est dit *quadratique* si $[K : \mathbb{Q}] = 2$. Soit K un corps de nombres quadratique et soit $\alpha \in K \setminus \mathbb{Q}$. La famille $(1, \alpha)$ est alors libre sur $\mathbb{Q}$ et est donc une $\mathbb{Q}$-base de K. On en déduit que $K = \mathbb{Q}(\alpha)$ et donc que $\deg \alpha = 2$. Le polynôme minimal π_α de α sur $\mathbb{Q}$ est donc de la forme $X^2 + a_1X + a_2 \in \mathbb{Q}[X]$. En multipliant ce polynôme par le ppcm des dénominateurs de a_1 et a_2 on obtient un polynôme $aX^2 + bX + c \in \mathbb{Z}[X]$ annulant α. On en déduit que $\alpha = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$, de sorte que $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{d})$ où $d = b^2 - 4ac \in \mathbb{Z}$. On peut encore écrire $d = m^2 d_1$ où $m \in \mathbb{N}^*$ et $d_1 \in \mathbb{Z}$ est un entier sans diviseur carré. On a alors $K = \mathbb{Q}(\sqrt{d_1})$. Remarquons que,

puisque $\mathbb{Q} \subsetneq K$, on a $d_1 \notin \{0,1\}$. Ainsi un corps de nombres quadratique est de la forme $\mathbb{Q}(\sqrt{d})$ où $d \in \mathbb{Z} \smallsetminus \{0,1\}$ est sans diviseur carré, c'est-à-dire tel que $v_p(d) \in \{0,1\}$ pour tout nombre premier p.

Théorème 5.4. *Soit $d \in \mathbb{Z} \smallsetminus \{0,1\}$ sans diviseur carré et soit $K = \mathbb{Q}(\sqrt{d})$. Alors l'anneau des entiers de K est de la forme*

$$\mathcal{O}_K = \mathbb{Z}[\alpha] = \{a + b\alpha \mid (a,b) \in \mathbb{Z}^2\}$$

avec

$$\alpha = \begin{cases} \sqrt{d} & \text{si } d \equiv 2 \text{ ou } 3\,[4], \\ \frac{1+\sqrt{d}}{2} & \text{si } d \equiv 1\,[4]. \end{cases}$$

Démonstration. Soit $x = a + b\sqrt{d} \in K$ où $(a,b) \in \mathbb{Q}^2$. Déterminons une condition nécessaire pour que $x \in \mathcal{O}_K$. Posons $\overline{x} = a - b\sqrt{d}$. Comme $\overline{x}$ est un conjugué de x, le corollaire 5.1.2 implique qu'il s'agit d'un entier algébrique. Par ailleurs le polynôme $P(X) = (X-x)(X-\overline{x}) = X^2 - (x+\overline{x})X + x\overline{x}$ est à coefficients dans $\mathbb{Q}$. De plus ses coefficients $x + \overline{x}$ et $x\overline{x}$ sont également des entiers algébriques. Comme les seuls entiers algébriques de $\mathbb{Q}$ sont les éléments de $\mathbb{Z}$, on en déduit donc que

$$x + \overline{x} \in \mathbb{Z}, \quad x\overline{x} \in \mathbb{Z}.$$

On a donc $2a \in \mathbb{Z}$ et $a^2 - db^2 \in \mathbb{Z}$. Posons $a_1 = 2a \in \mathbb{Z}$ de sorte que $a_1^2 - 4db^2 \in 4\mathbb{Z}$. On en déduit que $4db^2 \in \mathbb{Z}$. Soit p un nombre premier. On déduit de cette relation la relation

$$v_p(4) + v_p(d) + 2v_p(b) \geqslant 0$$

Comme d est sans diviseur carré, on a $v_p(d) \in \{0,1\}$ de sorte que, si $p \neq 2$, on a $v_p(b) \geqslant 0$ et, si $p = 2$, $v_2(b) \geqslant -1$. On en déduit la relation $2b \in \mathbb{Z}$. Posons donc $b_1 = 2b$. La relation $a_1^2 - db_1^2 \in 4\mathbb{Z}$ et le fait que d est sans diviseur carré implique que 2 divise a_1 si et seulement si 2 divise b_1.

On en déduit que si 2 ne divise pas a_1, alors 2 ne divise pas b_1 et on obtient donc $\overline{d} = \overline{a_1}^2\overline{b_1}^{-2}$ dans $\mathbb{Z}/4\mathbb{Z}$. En particulier d est un carré modulo 4. Comme d est sans diviseur carré, on a $\overline{d} \neq \overline{0}$ et donc $d \equiv 1\,[4]$. Ainsi si d est congru à 2 ou 3, modulo 4, les entiers a_1 et b_1 sont tous deux pairs et donc $(a,b) \in \mathbb{Z}^2$. En particulier $x \in \mathbb{Z}[\sqrt{d}]$. Si $d \equiv 1\,[4]$, alors a_1 et b_1 ne sont pas nécessairement pairs mais ont nécessairement la même parité. On en déduit que $(a,b) \in (2^{-1}\mathbb{Z})^2$ avec $a - b \in \mathbb{Z}$. En particulier $x \in \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$.

Réciproquement, posons $\alpha = \frac{1+\sqrt{d}}{2}$ si $d \equiv 1\,[4]$, et $\alpha = \sqrt{d}$ dans le cas contraire. Il nous reste à vérifier que les éléments de $\mathbb{Z}[\alpha]$ sont bien des entiers algébriques. D'après le corollaire au théorème 5.1, il est suffisant de vérifier que α est un entier algébrique. Le nombre $\sqrt{d}$ est toujours un entier algébrique puisqu'il est annulé par le polynôme unitaire $X^2 - d \in \mathbb{Z}[X]$. Le polynôme minimal du nombre $\frac{1+\sqrt{d}}{2}$ est le polynôme

$$\left(X - \frac{1+\sqrt{d}}{2}\right)\left(X - \frac{1-\sqrt{d}}{2}\right) = X^2 - X + \frac{1-d}{4}.$$

Ce polynôme est dans $\mathbb{Z}[X]$ si et seulement si $d \equiv 1\,[4]$, donc $\frac{1+\sqrt{d}}{2}$ est un entier algébrique si et seulement si $d \equiv 1\,[4]$. □

Exemple. Les nombres $\frac{1+\sqrt{5}}{2}$ et $\frac{1+i\sqrt{7}}{2}$ sont des entiers algébriques, mais ce n'est pas le cas de $\frac{1+\sqrt{3}}{2}$.

5.1.4 Discriminant d'un corps de nombres

Soient $K \subset L$ deux corps de nombres. Si $\alpha \in L$, on note m_α l'application K-linéaire

$$m_\alpha : \begin{array}{ccc} L & \longrightarrow & L \\ x & \longmapsto & \alpha x \end{array}.$$

On définit alors des éléments de K par les formules

$$\mathrm{Tr}_{L/K}(\alpha) \coloneqq \mathrm{Tr}(m_\alpha), \quad N_{L/K}(\alpha) \coloneqq \det(m_\alpha).$$

Ce sont des éléments de K que l'on appelle respectivement *trace* et *norme* de α relativement à L/K. Si α et β sont des éléments de L, on a $m_{\alpha+\beta} = m_\alpha + m_\beta$ et $m_{\alpha\beta} = m_\alpha \circ m_\beta$. Ainsi

$$\mathrm{Tr}_{L/K}(\alpha+\beta) = \mathrm{Tr}_{L/K}(\alpha) + \mathrm{Tr}_{L/K}(\beta), \quad N_{L/K}(\alpha\beta) = N_{L/K}(\alpha)N_{L/K}(\beta).$$

De plus si $\alpha \in K$ et $\beta \in L$, on a $m_{\alpha\beta} = \alpha m_\beta$ de sorte que

$$\mathrm{Tr}_{L/K}(\alpha\beta) = \alpha\,\mathrm{Tr}_{L/K}(\beta), \quad N_{L/K}(\alpha\beta) = \alpha^{[L:K]} N_{L/K}(\beta).$$

De façon plus générale, on peut définir $\chi_{L/K,\alpha}(X) \coloneqq \chi_{m_\alpha}(X)$ le *polynôme caractéristique de* m_α. On a alors

$$\chi_{L/K,\alpha}(X) = X^{[L:K]} + a_{[L:K]-1}X^{[L:K]-1} + \cdots + a_1 X + a_0$$

avec $a_{[L:K]-1} = -\,\mathrm{Tr}_{L/K}(\alpha)$ et $a_0 = (-1)^{[L:K]} N_{L/K}(\alpha)$.

Si $(\alpha_1, \ldots, \alpha_n) \in L^n$ est une famille de $n = [L : K]$ éléments de L, on appelle *discriminant* de la famille $(\alpha_1, \ldots, \alpha_n)$ l'élément

$$\Delta_{L/K}(\alpha_1, \ldots, \alpha_n) = \det((\mathrm{Tr}_{L/K}(\alpha_i\alpha_j))_{\substack{1\leqslant i\leqslant n \\ 1\leqslant j\leqslant n}}).$$

Exemple. Considérons le cas où $K = \mathbb{Q}$ et $L = \mathbb{Q}(\sqrt{d})$ avec $d \in \mathbb{Z}$ non carré. Si $\alpha = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ avec $(a, b) \in \mathbb{Q}^2$, alors la matrice de l'endomorphisme m_α dans la base $(1, \sqrt{d})$ de $\mathbb{Q}(\sqrt{d})$ est $\left(\begin{smallmatrix} a & db \\ b & a \end{smallmatrix}\right)$. Ainsi on a

$$\mathrm{Tr}_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(a + b\sqrt{d}) = 2a, \quad N_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(a + b\sqrt{d}) = a^2 - db^2.$$

De plus,

$$\Delta_{L/K}(1, \sqrt{d}) = \det \begin{pmatrix} 2 & 0 \\ 0 & 2d \end{pmatrix} = 4d.$$

Théorème 5.5. *Soient $K \subset L$ deux corps de nombres. Posons $n = [L : K]$ et fixons $(\alpha_1, \dots, \alpha_n) \in L^n$. Pour que la famille $(\alpha_1, \dots, \alpha_n)$ soit une base de L comme K-espace vectoriel, il faut et il suffit que $\Delta_{L/K}(\alpha_1, \dots, \alpha_n) \neq 0$.*

Démonstration. Soit M la matrice $(\mathrm{Tr}_{L/K}(\alpha_i\alpha_j))_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant n}} \in \mathcal{M}_n(K)$. Si $(\alpha_1, \dots, \alpha_n)$ n'est pas une base de L sur K, il existe un n-uplet $(\lambda_1, \dots, \lambda_n) \in K^n$ non nul tel que $\sum_{i=1}^n \lambda_i\alpha_i = 0$. En particulier, pour $1 \leqslant j \leqslant n$, on a $\mathrm{Tr}_{L/K}(\alpha_j \sum_{i=1}^n \lambda_i\alpha_i) = 0$. On en déduit que le vecteur de K^n de coordonnées $(\lambda_1, \dots, \lambda_n)$ est dans le noyau de M. On en déduit que $\det(M) = 0$ et donc que $\Delta_{L/K}(\alpha_1, \dots, \alpha_n) = 0$.

Réciproquement supposons que $\det(M) = 0$. Supposons par l'absurde que $(\alpha_1, \dots, \alpha_n)$ est une base de L sur K. Comme $\det(M) = 0$, il existe un n-uplet non nul $(\lambda_1, \dots, \lambda_n) \in K^n$ tel que

$$M \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} = 0.$$

Ainsi, si $x = \sum_{i=1}^n \lambda_i\alpha_i$, on a $\mathrm{Tr}(\alpha_j x) = 0$ pour tout $1 \leqslant j \leqslant n$. Comme $(\alpha_1, \dots, \alpha_n)$ est une base de L sur K, on en déduit que pour tout $y \in L$, on a $\mathrm{Tr}_{L/K}(yx) = 0$. Comme le n-uplet $(\lambda_1, \dots, \lambda_n)$ est non nul, on a $x \neq 0$. Comme de plus L est un sous-corps de $\mathbb{C}$, on a $x^{-1} \in L$ et donc $\mathrm{Tr}(x^{-1}x) = 0$. Or $\mathrm{Tr}_{L/K}(x^{-1}x) = \mathrm{Tr}_{L/K}(1) = [L : K]$. C'est absurde. Ainsi la famille $(\alpha_1, \dots, \alpha_n)$ n'est pas une base de L sur K. □

Supposons que $\underline{\alpha} = (\alpha_1, \dots, \alpha_n)$ est une base de L sur K et que $\underline{\beta} = (\beta_1, \dots, \beta_n)$ en est une autre. Soit $P \in \mathrm{GL}_n(K)$ la matrice de passage de $\underline{\alpha}$ à $\underline{\beta}$, c'est-à-dire $P = (p_{i,j})_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant n}}$ avec

$$\beta_j = \sum_{i=1}^n p_{i,j}\alpha_i.$$

La matrice $M = (\mathrm{Tr}_{L/K}(\alpha_i\alpha_j))_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant n}}$ est la matrice de la forme bilinéaire symétrique $(x, y) \mapsto \mathrm{Tr}_{L/K}(xy)$ dans la base $\underline{\alpha}$. On a donc une égalité de matrices de $\mathcal{M}_n(K)$:

$$(\mathrm{Tr}_{L/K}(\beta_i\beta_j))_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant n}} = {}^tP(\mathrm{Tr}_{L/K}(\alpha_i\alpha_j))_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant n}}P$$

de sorte que

$$\Delta_{L/K}(\beta_1, \dots, \beta_n) = \det(P)^2\Delta_{L/K}(\alpha_1, \dots, \alpha_n).$$

Théorème 5.6. *Soient $K \subset L$ deux corps de nombres. Si $x \in \mathcal{O}_L$, alors $\mathrm{Tr}_{L/K}(x) \in \mathcal{O}_K$ et $N_{L/K}(x) \in \mathcal{O}_K$. Plus généralement $\chi_{L/K,x}(X) \in \mathcal{O}_K[X]$. De plus, si $(\alpha_1, \dots, \alpha_n)$ est une base du K-espace vectoriel L incluse dans $\mathcal{O}_L$, alors $\Delta_{L/K}(\alpha_1, \dots, \alpha_n) \in \mathcal{O}_K$.*

Démonstration. Tous les énoncés sont directement conséquences de l'observation suivante : si $x \in \mathcal{O}_L$, alors $\chi_{L/K,x}(X) \in \mathcal{O}_K[X]$. Prouvons-la. Soit $K(x) \subset L$ le sous-corps

de L engendré par K et x. On a donc une inclusion de corps de nombres $K \subset K(x) \subset L$. Soit $r = [L : K(x)]$ et soit $(e_1, \dots, e_r)$ une base de L vu comme $K(x)$-espace vectoriel. Posons $d = \deg_K(x)$. On a alors $n = dr$. Chaque $K(x)$-droite $K(x)e_i$ est stable par multiplication par x, donc par l'endomorphisme K-linéaire m_x.

Notons $\pi_{x,K}(X) \in K[X]$ le polynôme minimal de x sur K. On a $\pi_{x,K}(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_0$. Le sous-espace $K(x)$ de L est stable par m_x et la matrice de $m_x|_{K(x)}$ dans la base $(1, x, x^2, \dots, x^{d-1})$ est alors la matrice

$$M_x = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \ddots & 0 & -a_1 \\ 0 & 1 & 0 & \ddots & -a_2 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 & -a_{d-1} \end{pmatrix}.$$

On en conclut que la matrice de m_x dans la base $(e_1, xe_1, \dots, x^{d-1}e_1, e_2, xe_2, \dots, x^{d-1}e_r)$ est la matrice par blocs

$$\begin{pmatrix} M_x & 0_d & \cdots & 0_d \\ 0_d & M_x & \ddots & 0_d \\ \vdots & \ddots & \ddots & \vdots \\ 0_d & \cdots & 0_d & M_x \end{pmatrix}.$$

Ainsi $\chi_{L/K,x}(X) = \chi_{K(x)/K,x}(X)^r = \pi_{x,K}(X)^r$. Si $x \in \mathcal{O}_L$, ses conjugués sur K sont aussi des entiers algébriques. Ainsi les racines de $\pi_{x,K}$ sont des entiers algébriques. Les relations entre coefficients et racines d'un polynôme montrent que les coefficients de $\pi_{x,K}$ sont également des entiers algébriques. Comme par ailleurs ce sont des éléments de K, on en conclut que $\pi_{x,K} \in \mathcal{O}_K[X]$. Ainsi on a également $\chi_{L/K,x}(X) = \pi_{x,K}(X)^r \in \mathcal{O}_K[X]$. □

Théorème 5.7. *Soit K un corps de nombres. L'anneau des entiers $\mathcal{O}_K$ est alors un $\mathbb{Z}$-module libre de rang $[K : \mathbb{Q}]$. De plus, si $(\alpha_1, \dots, \alpha_n)$ est une base du $\mathbb{Z}$-module libre $\mathcal{O}_K$, le discriminant $\Delta_{K/\mathbb{Q}}(\alpha_1, \dots, \alpha_n)$ est indépendant du choix de la base $(\alpha_1, \dots, \alpha_n)$. On le note $\Delta_{\mathcal{O}_K/\mathbb{Z}}$.*

Démonstration. Montrons dans un premier temps que $\mathcal{O}_K$ contient une base de K vu comme $\mathbb{Q}$-espace vectoriel. Posons $n = [K : \mathbb{Q}]$ et fixons $(\alpha_1, \dots, \alpha_n)$ une base de K vu comme $\mathbb{Q}$-espace vectoriel. Remarquons que si $\alpha \in K$, il existe $d \in \mathbb{Q}^\times$ tel que $d\alpha \in \mathcal{O}_K$. En effet soit $P \in \mathbb{Q}[X]$ unitaire tel que $P(\alpha) = 0$. Posons $P(X) = X^m + a_{m-1}X^{m-1} + \cdots + a_0$ et choisissons $d \in \mathbb{Z}$ non nul tel que $da_i \in \mathbb{Z}$ pour tout $0 \leqslant i \leqslant d-1$. Alors $d\alpha$ est racine du polynôme

$$d^m P(d^{-1}X) = X^m + a_{m-1}dX^{m-1} + \cdots + a_1 d^{m-1}X + a_0 d^m \in \mathbb{Z}[X].$$

Ainsi $d\alpha$ est annulé par un polynôme unitaire de $\mathbb{Z}[X]$ et est donc un élément de $\mathcal{O}_K$. Il existe donc $d \in \mathbb{Z}$ non nul et suffisamment grand pour que $d\alpha_i \in \mathcal{O}_K$ pour tout $1 \leqslant i \leqslant n$, ce qui implique que $\mathcal{O}_K$ contient une base de K sur $\mathbb{Q}$.

Fixons donc $(\alpha_1, \dots, \alpha_n)$ une base de K sur $\mathbb{Q}$ dont les éléments appartiennent à $\mathcal{O}_K$. Posons $M = \sum_{i=1}^n \mathbb{Z}\alpha_i$. Comme la famille $(\alpha_1, \dots, \alpha_n)$ est $\mathbb{Q}$-libre, on a $M = \bigoplus_{i=1}^n \mathbb{Z}\alpha_i$. De plus, la forme ($\mathbb{Q}$-)bilinéaire $(x, y) \mapsto \mathrm{Tr}_{K/\mathbb{Q}}(xy)$ est non dégénérée. Il existe donc une famille $(\beta_1, \dots, \beta_n)$ de K^n telle que

$$\forall 1 \leqslant i \leqslant n,\ \forall 1 \leqslant j \leqslant n, \quad \mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i \beta_j) = \delta_{i,j}. \tag{5.2}$$

On en déduit en particulier que la famille $(\beta_1, \dots, \beta_n)$ est aussi une base du $\mathbb{Q}$-espace vectoriel K. Si $x \in \mathcal{O}_K$, on peut donc écrire

$$x = \sum_{i=1}^n \lambda_i \beta_i$$

avec $(\lambda_1, \dots, \lambda_n) \in \mathbb{Q}^n$. La relation (5.2) implique alors que

$$\forall 1 \leqslant i \leqslant n, \quad \lambda_i = \mathrm{Tr}_{K/\mathbb{Q}}(x\alpha_i).$$

Comme $x \in \mathcal{O}_K$ et $\alpha_i \in \mathcal{O}_K$, on a $x\alpha_i \in \mathcal{O}_K$ et donc $\mathrm{Tr}_{K/\mathbb{Q}}(x\alpha_i) \in \mathbb{Z}$ de sorte que $\lambda_i \in \mathbb{Z}$. Ainsi

$$\mathcal{O}_K \subset \bigoplus_{i=1}^n \mathbb{Z}\beta_i.$$

On en déduit que $\mathcal{O}_K$ est un sous-groupe d'un groupe abélien libre de rang fini n. Le théorème de structure des groupes abéliens finis implique que $\mathcal{O}_K$ est aussi un groupe abélien libre de rang fini $n' \leqslant n$. Cependant $\mathcal{O}_K$ contient le groupe abélien libre $\bigoplus_{i=1}^n \mathbb{Z}\alpha_i$ qui est de rang n. Ainsi $n \leqslant n' \leqslant n$ et donc $n = n'$, c'est-à-dire que $\mathcal{O}_K$ est de rang $n = [K : \mathbb{Q}]$.

Soit maintenant $\underline{\alpha} = (\alpha_1, \dots, \alpha_n)$ et $\underline{\beta} = (\beta_1, \dots, \beta_n)$ deux bases du $\mathbb{Z}$-module libre $\mathcal{O}_K$. On a donc

$$\Delta_{K/\mathbb{Q}}(\alpha_1, \dots, \alpha_n) \in \mathbb{Z}, \quad \Delta_{K/\mathbb{Q}}(\beta_1, \dots, \beta_n) \in \mathbb{Z}.$$

De plus soit $P \in \mathcal{M}_n(\mathbb{Z})$ la matrice de passage de $\underline{\alpha}$ à $\underline{\beta}$. Comme $\underline{\alpha}$ et $\underline{\beta}$ sont deux bases du même $\mathbb{Z}$-module, on a $P^{-1} \in \mathcal{M}_n(\mathbb{Z})$ et donc $P \in \mathrm{GL}_n(\mathbb{Z})$. Ainsi $\det(P) \in \mathbb{Z}^\times = \{\pm 1\}$, donc $\det(P)^2 = 1$. On a donc une égalité $\Delta_{K/\mathbb{Q}}(\alpha_1, \dots, \alpha_n) = \Delta_{K/\mathbb{Q}}(\beta_1, \dots, \beta_n)$. □

Remarque. Au cours de la démonstration du théorème 5.7, on a montré que si $x \in K$, il existe $d \in \mathbb{N}^*$ tel que $dx \in \mathcal{O}_K$. Ceci montre en particulier que K est le corps des fractions de l'anneau intègre $\mathcal{O}_K$. Ceci généralise le fait que $\mathbb{Q}$ est le corps des fractions de l'anneau $\mathbb{Z}$.

Exemple. Soit $x \in \mathbb{C}$ une racine du polynôme $X^3 - X + 1$. Ils 'agit d'un polynôme irréductible de $\mathbb{Q}[X]$ car il est de degré 3 et n'a pas de racine dans $\mathbb{Q}$ (on peut vérifier par exemple que ± 1 ne sont pas des racines). Ainsi $X^3 - X + 1$ est le polynôme minimal de π_x de x sur $\mathbb{Q}$. Posons $K = \mathbb{Q}(x)$. On a donc $\deg x = 3$ et $[K : \mathbb{Q}] = 3$. On en déduit également que

$$\chi_{K/\mathbb{Q},x}(X) = \pi_x(X) = X^3 - X + 1$$

et donc $\mathrm{Tr}_{K/\mathbb{Q}}(x) = 0$. On a également $\mathrm{Tr}_{K/\mathbb{Q}}(x^3) = \mathrm{Tr}_{K/\mathbb{Q}}(x-1) = -3$ et

$$\mathrm{Tr}_{K/\mathbb{Q}}(x^4) = \mathrm{Tr}_{K/\mathbb{Q}}(x(x-1)) = \mathrm{Tr}_{K/\mathbb{Q}}(x^2).$$

Ainsi

$$\begin{aligned}\Delta_{K/\mathbb{Q}}(1,x,x^2) &= \det\begin{pmatrix} 3 & 0 & \mathrm{Tr}_{K/\mathbb{Q}}(x^2) \\ 0 & \mathrm{Tr}_{K/\mathbb{Q}}(x^2) & -3 \\ \mathrm{Tr}_{K/\mathbb{Q}}(x^2) & -3 & \mathrm{Tr}_{K/\mathbb{Q}}(x^2)\end{pmatrix} \\ &= 3(\mathrm{Tr}_{K/\mathbb{Q}}(x^2) - 9) - \mathrm{Tr}_{K/\mathbb{Q}}(x^2)^3.\end{aligned}$$

Il faut donc pouvoir calculer $\mathrm{Tr}_{K/\mathbb{Q}}(x^2)$. Posons $y = x^2$. On a alors

$$\begin{aligned}y^3 = x^6 = (x^3)^2 = (x-1)^2 = y + 1 - 2x\ ; \\ y^2 = x^4 = x(x-1) = y - x.\end{aligned}$$

L'élément y vérifie donc la relation

$$y^3 - 2y^2 + y - 1 = 0.$$

Ce polynôme est encore irréductible dans $\mathbb{Q}[X]$, c'est donc le polynôme minimal de y sur $\mathbb{Q}$, on en déduit que $\chi_{K/\mathbb{Q},y} = \pi_y = X^3 - 2X^2 + X - 1$ et donc que $\mathrm{Tr}_{K/\mathbb{Q}}(x^2) = \mathrm{Tr}_{K/\mathbb{Q}}(y) = 2$. Au final

$$\Delta_{K/\mathbb{Q}}(1,x,x^2) = -15 - 8 = -23.$$

On peut mettre à profit ce calcul de discriminant pour déterminer l'anneau des entiers de K. En effet, comme x est un entier algébrique, on a $\mathbb{Z}[x] \subset \mathcal{O}_K$. De plus $\underline{\alpha} = (1, x, x^2)$ est une base du $\mathbb{Z}$-module $\mathbb{Z}[x]$. Soit $\underline{\beta} = (\beta_1, \beta_2, \beta_3)$ une base du $\mathbb{Z}$-module $\mathcal{O}_K$ et soit $P = P_{\underline{\beta},\underline{\alpha}}$ la matrice de passage de $\underline{\beta}$ à $\underline{\alpha}$. On a alors

$$\Delta_{K/\mathbb{Q}}(\underline{\alpha}) = \det(P)^2 \Delta_{K/\mathbb{Q}}(\underline{\beta}).$$

Mais $\Delta_{K/\mathbb{Q}}(\underline{\alpha}) = -23$ et $\Delta_{K/\mathbb{Q}}(\underline{\beta}) \in \mathbb{Z}$. Comme $P \in \mathcal{M}_3(\mathbb{Z})$, le nombre $\det(P)^2$ est un carré de $\mathbb{Z}$. Comme 23 est premier, on a nécessairement $\det(P) \in \{\pm 1\}$, c'est-à-dire $\mathcal{O}_K = \mathbb{Z}[x]$. Ainsi l'anneau des entiers de $K = \mathbb{Q}(x)$ est l'anneau $\mathbb{Z}[x]$.

5.2 Idéaux et anneaux de Dedekind

5.2.1 Exemple

Considérons le corps de nombres quadratique $K = \mathbb{Q}(\sqrt{-2}) = \mathbb{Q}(i\sqrt{2})$. D'après le théorème 5.4, son anneau d'entiers est le sous-anneau $A = \mathcal{O}_K = \mathbb{Z}[i\sqrt{2}]$.

Proposition. *L'anneau A est principal. De plus $A^\times = \{\pm 1\}$.*

Démonstration. Commençons par déterminer le groupe des inversibles $A^\times$. Il est clair que 1 et -1 sont des éléments inversibles. Réciproquement soit $x \in A^\times$. On peut écrire $x = a+bi\sqrt{2}$ avec $(a,b) \in \mathbb{Z}^2$. D'après le théorème 5.6, on a $N_{K/\mathbb{Q}}(x) \in \mathbb{Z}$. De même $x^{-1} \in A$, donc $N_{K/\mathbb{Q}}(x^{-1}) \in \mathbb{Z}$. Comme par ailleurs $N_{K/\mathbb{Q}}(x)N_{K/\mathbb{Q}}(x^{-1}) = N_{K/\mathbb{Q}}(xx^{-1}) = 1$, on a $N_{K/\mathbb{Q}}(x) \in \mathbb{Z}^\times = \{\pm 1\}$. Comme $N_{K/\mathbb{Q}}(x) = (a+bi\sqrt{2})(a-bi\sqrt{2}) = a^2+5b^2 > 0$, on en déduit que $a^2 + 5b^2 = 1$. Comme $(a,b) \in \mathbb{Z}^2$, on a nécessairement $b = 0$ et $a \in \{\pm 1\}$ donc $x \in \{\pm 1\}$.

Démontrons maintenant que A est principal. L'anneau A est en fait un cas particulier d'anneau euclidien. Soit I un idéal non nul de A. L'ensemble $\{N_{K/\mathbb{Q}}(x) \mid x \in I \smallsetminus \{0\}\}$ est une partie non vide de $\mathbb{N}^*$. Il existe donc $x \in I$ tel que

$$N_{K/\mathbb{Q}}(x) = \min\{N_{K/\mathbb{Q}}(y) \mid y \in I \smallsetminus \{0\}\}.$$

Soit $y \in I$ et considérons l'élément $\frac{y}{x} \in K$. On peut écrire $\frac{y}{x} = r + si\sqrt{2}$ avec $(r,s) \in \mathbb{Q}^2$. Soient $(a',b') \in \mathbb{Z}^2$ tels que $|a'-r| \leqslant \frac{1}{2}$ et $|b'-s| \leqslant \frac{1}{2}$. Alors

$$N_{K/\mathbb{Q}}(yx^{-1} - (a'+b'i\sqrt{2})) \leqslant \frac{1}{4} + \frac{1}{2} < 1.$$

On en conclut que $N_{K/\mathbb{Q}}(y - x(a'+b'i\sqrt{2})) < N_{K/\mathbb{Q}}(x)$. Par minimalité de $N_{K/\mathbb{Q}}(x)$, et puisque $y - x(a'+b'i\sqrt{2}) \in I$, on en conclut que $y = x(a'+b'i\sqrt{2})$, c'est-à-dire $y \in (x)$. Donc $I = (x)$ et A est bien un anneau principal. □

Voici une application de ce résultat. On recherche l'ensemble des couples d'entiers $(x,y) \in \mathbb{Z}^2$ satisfaisant l'équation

$$x^2 + 2 = y^3.$$

Supposons que (x,y) est une telle solution. On peut réécrire cette équation sous la forme

$$(x + i\sqrt{2})(x - i\sqrt{2}) = y^3.$$

Comme A est un anneau principal, si on arrive à prouver que les éléments $x + i\sqrt{2}$ et $x-i\sqrt{2}$ sont premiers entre eux, ils doivent tous deux être des cubes de A, éventuellement multipliés par un élément inversible. Soit donc $d = (x + i\sqrt{2}) \wedge (x - i\sqrt{2})$ leur pgcd. On a en particulier $d|2i\sqrt{2}$ et $d|2x$. Le nombre $p \coloneqq i\sqrt{2}$ est un élément irréductible de A. Admettons le pour le moment et démontrons le plus tard. On a donc $d|2i\sqrt{2} = -p^3$. Donc si d n'est pas inversible dans A, on doit avoir $p|d$. Mais comme d divise $x + i\sqrt{2} = x + p$, on doit avoir $p|x$. Ainsi $p^2 = -2$ divise x^2 dans A. Ceci implique que $\frac{x^2}{2} \in A \cap \mathbb{Q} = \mathbb{Z}$, donc 2 divise x^2 dans $\mathbb{Z}$. Comme 2 est un nombre premier, on en conclut que 2 divise x dans $\mathbb{Z}$, c'est-à-dire que x est pair. Ainsi y^3 doit être pair et donc y également. On peut en conclure que $2^3|y^3$ et $2^2|x^2$, et donc que $2^2|2 = y^3 - x^2$, ce qui est absurde. Ainsi d est inversible dans A : $x + i\sqrt{2}$ et $x - i\sqrt{2}$ sont premiers entre eux dans A.

Comme A est principal, il est factoriel, on en conclut qu'il existe $z \in A$ et $\gamma \in A^\times$ tels que $x + i\sqrt{2} = \gamma z^3$. Il existe donc $(a,b) \in \mathbb{Z}^2$ tels que

$$x + i\sqrt{2} = \pm(a + bi\sqrt{2})^3.$$

En développant cette relation on obtient

$$\begin{cases} x = \pm(a^3 - 6ab^2) \\ 1 = \pm(3a^2b - 2b^3) \end{cases}$$

ce qui implique $b = \pm 1$ et $3a^2 - 2 = \pm 1$. Ainsi on a nécessairement $a = \pm 1$ et donc $x \in \{\pm 5\}$. Les seules solutions de l'équations sont donc $(x, y) = (5, 3)$ et $(x, y) = (-5, 3)$ (on vérifie facilement que ce sont bien des solutions).

Il nous reste à démontrer l'irréductibilité de $i\sqrt{2}$ dans A. Supposons que $i\sqrt{2} = \alpha\beta$ avec α et β dans A. En appliquant la norme, on obtient $2 = N_{K/\mathbb{Q}}(\alpha)N_{K/\mathbb{Q}}(\beta)$ qui est une relation entre éléments de $\mathbb{Z}$. Ainsi $N_{K/\mathbb{Q}}(\alpha) \in \{1, 2\}$. Si $N_{K/\mathbb{Q}}(\alpha) = 2$, alors $N_{K/\mathbb{Q}}(\beta) = 1$ et $\beta \in A^\times$. Si $N_{K/\mathbb{Q}}(\alpha) = 1$, alors $\alpha \in A^\times$, ce qui prouve bien que $\alpha \in A^\times$ ou $\beta \in A^\times$ donc que $i\sqrt{2}$ est irréductible dans A.

Le point essentiel de cette étude repose sur la factorialité de l'anneau d'entiers $\mathbb{Z}[i\sqrt{2}]$. On est bien sûr tenté d'appliquer cette méthode à d'autres équations diophantiennes, par exemple

$$z^n = x^n + y^n = (x + y)(x + y\zeta) \cdots (x + y\zeta^{n-1}), \quad \zeta = e^{\frac{2\pi i}{n}}.$$

Malheureusement les anneaux d'entiers de corps de nombres ne sont pas factoriels en général. En voici un exemple.

Proposition. *Soit $K = \mathbb{Q}(i\sqrt{5})$. L'anneau $\mathcal{O}_K$ n'est pas factoriel.*

Démonstration. D'après le théorème 5.4, on a $\mathcal{O}_K = \mathbb{Z}[i\sqrt{5}]$ puisque $-5 \equiv 3\,[4]$. Montrons dans un premier temps que le nombre 2 est irréducible dans $\mathcal{O}_K$. Si $2 = \alpha\beta$ avec $\alpha, \beta \in \mathcal{O}_K$, alors $4 = N_{K/\mathbb{Q}}(\alpha)N_{K/\mathbb{Q}}(\beta)$. Or

$$2 \notin N_{K/\mathbb{Q}}(\mathcal{O}_K) = \{a^2 + 5b^2 \mid (a, b) \in \mathbb{Z}^2\}.$$

On a donc $N_{K/\mathbb{Q}}(\alpha) \in \{1, 4\}$. Si $N_{K/\mathbb{Q}}(\alpha) = 1$, alors α est inversible dans $\mathcal{O}_K$. Sinon $N_{K/\mathbb{Q}}(\alpha) = 4$ et $N_{K/\mathbb{Q}}(\beta) = 1$, donc β est inversible dans $\mathcal{O}_K$. Ceci implique que 2 est un élément irréductible de l'anneau $\mathcal{O}_K$. Le même raisonnement permet de montrer que les éléments 3, $1 + i\sqrt{5}$ et $1 - i\sqrt{5}$ sont irréductibles dans $\mathcal{O}_K$. Or on peut écrire

$$6 = 2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5}).$$

Si l'anneau $\mathcal{O}_K$ était factoriel, l'unicité de la décomposition en produit d'irréductibles devrait impliquer que 2 est égal à $1 + i\sqrt{5}$ ou $1 - i\sqrt{5}$ à un élément inversible près. On vérifie, comme pour l'anneau $\mathbb{Z}[i\sqrt{2}]$, que $\mathbb{Z}[i\sqrt{5}]^\times = \{\pm 1\}$ de sorte que l'on devrait avoir $2 = \pm(1 + i\sqrt{5})$ ou $2 = \pm(1 - i\sqrt{5})$. Aucune de ces inégalités n'est vérifiée, donc l'anneau $\mathcal{O}_K$ n'est pas factoriel. □

5.2.2 Anneaux de Dedekind

Soit K un corps de nombres. Commençons par collecter quelques propriétés des idéaux de son anneau d'entiers $\mathcal{O}_K$.

Lemme. *Soit I un idéal non nul de $\mathcal{O}_K$. Alors $I \cap \mathbb{Z} \neq \{0\}$.*

Démonstration. Soit $x \in I$ un élément non nul. Comme x est un entier algébrique. Soit $P(X) = \pi_x(X) \in \mathbb{Z}[X]$ le polynôme minimal de x (c'est a priori un élément de $\mathbb{Q}[X]$ mais il est dans $\mathbb{Z}[X]$ puisque x est un entier algébrique). Posons $P(X) = X^d + \cdots + a_0 \in \mathbb{Z}[X]$. Comme $P(X)$ est irréductible dans $\mathbb{Q}[X]$, on a nécessairement $a_0 \neq 0$. Par ailleurs

$$a_0 = -x^d - \sum_{i=1}^{d-1} a_i x^i \in I \cap \mathbb{Z}. \qquad \square$$

Proposition. *Soit $I \subset \mathcal{O}_K$ un idéal non nul de $\mathcal{O}_K$. Alors, pour la loi d'addition, I est un groupe abélien libre de rang $[K : \mathbb{Q}]$ et l'anneau quotient $\mathcal{O}_K/I$ est fini.*

Démonstration. Le groupe additif I est un sous-groupe de $\mathcal{O}_K$. D'après le théorème 5.7, le groupe $\mathcal{O}_K$ est libre de rang $[K : \mathbb{Q}]$. Ainsi I est un groupe abélien libre de rang inférieur à $[K : \mathbb{Q}]$. Par ailleurs le théorème de structure des groupes abéliens de type fini nous donne l'existence d'une $\mathbb{Z}$-base $(e_1, \ldots, e_n)$ de $\mathcal{O}_K$ et d'entiers $d_1 | d_2 | \cdots | d_n$ tels que

$$\mathcal{O}_K = \bigoplus_{i=1}^{n} \mathbb{Z} e_i, \quad I = \bigoplus_{i=1}^{n} \mathbb{Z} d_i e_i.$$

Soit $d \in I \cap \mathbb{Z}$ avec $d \neq 0$ dont l'existence est assurée par le lemme ci-dessus. On a alors $d\mathcal{O}_K \subset I$ et $d\mathcal{O}_K$ est isomorphe à $\mathcal{O}_K$ en tant que groupe abélien. C'est donc un groupe abélien libre de rang $[K : \mathbb{Q}]$. Ainsi le rang de I est supérieur ou égal à $[K : \mathbb{Q}]$ donc I est un groupe abélien libre de rang $[K : \mathbb{Q}]$. On en déduit que $d_i \neq 0$ pour $1 \leqslant i \leqslant n$ et donc que

$$\mathcal{O}_K/I \simeq \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_n\mathbb{Z}.$$

En particulier $\mathcal{O}_K/I$ est un anneau fini. $\square$

Nous allons en déduire une propriété importante des idéaux premiers de l'anneau $\mathcal{O}_K$.

Théorème 5.8. *Soit K un corps de nombres. Tout idéal premier non nul de $\mathcal{O}_K$ est un idéal maximal de $\mathcal{O}_K$.*

Démonstration. Soit $\mathfrak{p}$ un idéal premier non nul de $\mathcal{O}_K$. La proposition ci-dessus montre que $\mathcal{O}_K/\mathfrak{p}$ est un anneau fini. Comme de plus $\mathfrak{p}$ est un idéal premier, c'est un anneau

intègre. Or tout anneau intègre et fini est nécessairement un corps. En effet soit $a \in \mathcal{O}_K/\mathfrak{p} \setminus \{0\}$. On peut considérer le morphisme de groupes (pour la loi d'addition)

$$\begin{array}{ccc} \mathcal{O}_K/\mathfrak{p} & \longrightarrow & \mathcal{O}_K/\mathfrak{p} \\ x & \longmapsto & ax \end{array}$$

Comme $\mathcal{O}_K/\mathfrak{p}$ est intègre, ce morphisme de groupes abéliens est injectif. Mais comme $\mathcal{O}_K/\mathfrak{p}$ est fini, ce morphisme est aussi bijectif. Il existe donc $b \in \mathcal{O}_K/\mathfrak{p}$ tel que $ab = 1$. Ainsi $\mathcal{O}_K/\mathfrak{p}$ est un corps et donc $\mathfrak{p}$ est un idéal maximal. □

Un anneau A est dit *intégralement clos* si A est intègre et si tout élément de son corps des fractions $\operatorname{Frac} A$ qui est entier sur A est un élément de A.

Exemple. L'anneau $\mathbb{Z}$ est intégralement clos : tout élément de $\mathbb{Q}$ qui est racine d'un polynôme unitaire de $\mathbb{Z}[X]$ est déjà dans $\mathbb{Z}$. Plus généralement, le même raisonnement montre que tout anneau factoriel est intégralement clos.

Exemple. Soit $d \in \mathbb{Z}$ tel que $d \equiv 1\,[4]$ qui n'est pas un carré. L'anneau $\mathbb{Z}[\sqrt{d}]$ n'est pas intégralement clos. En effet $\mathbb{Q}(\sqrt{d})$ est le corps des fractions de l'anneau $\mathbb{Z}[\sqrt{d}]$. De plus, on a vu au cours de la démonstration du théorème 5.4 que $\frac{1+\sqrt{d}}{2}$ est entier sur $\mathbb{Z}$, donc sur $\mathbb{Z}[\sqrt{d}]$, mais $\frac{1+\sqrt{d}}{2} \notin \mathbb{Z}[\sqrt{d}]$.

Proposition. *Soit K un corps de nombres. L'anneau de ses entiers $\mathcal{O}_K$ est intégralement clos.*

Démonstration. On a déjà vu que K est le corps des fractions de $\mathcal{O}_K$. Soit $x \in K$ un élément qui est entier sur $\mathcal{O}_K$. D'après le théorème 5.1, l'anneau $\mathcal{O}_K[x]$ est un $\mathcal{O}_K$-module de type fini. Comme $\mathcal{O}_K$ est un $\mathbb{Z}$-module de type fini, on en conclut que $\mathcal{O}_K[x]$ est un $\mathbb{Z}$-module de type fini. Comme $\mathbb{Z}[x] \subset \mathcal{O}_K[x]$, l'anneau $\mathbb{Z}[x]$ est un $\mathbb{Z}$-module de type fini, donc x est entier sur $\mathbb{Z}$ et donc $x \in \mathcal{O}_K$. □

Exemple. L'anneau $\mathbb{Z}[i\sqrt{5}]$ est un exemple d'anneau intégralement clos mais qui n'est pas factoriel.

Enfin, on rappelle qu'un anneau A est dit *noethérien* si tout idéal de A est de type fini. On a montré dans la proposition ci-dessus que tout idéal de l'anneau des entiers d'un corps de nombres est de type fini. Ainsi les anneaux d'entiers de corps de nombres sont des anneaux noethériens.

Définition. *Un anneau commutatif A est un* anneau de Dedekind *s'il est noethérien, intégralement clos et si tout idéal premier non nul de A est maximal.*

Le théorème suivant résume une partie des résultats démontrés dans cette partie.

Théorème 5.9. *Soit K un corps de nombres. L'anneau de ses entiers $\mathcal{O}_K$ est un anneau de Dedekind.*

Dans la suite, nous montrerons que les anneaux de Dedekind ont des propriétés très semblables à celles des anneaux factoriels, à condition de remplacer les éléments de l'anneau par ses idéaux, et les éléments irréductibles par les idéaux premiers non nuls (donc maximaux).

5.2.3 Idéaux fractionnaires

Soit A un anneau de Dedekind et soit K son corps de fractions. Un *idéal fractionnaire* de A est un sous-A-module $I \subset K$ tel qu'il existe $x \in A \setminus \{0\}$ tel que $xI \subset A$. En particulier un idéal de A est un idéal fractionnaire (on peut prendre $x = 1$).

Exemple. Soit $A = \mathbb{Z}$. C'est un anneau de Dedekind puisque c'est l'anneau des entiers du corps de nombres $\mathbb{Q}$. Si $r \in \mathbb{Q} \setminus \{0\}$ le sous-$\mathbb{Z}$-module $I \coloneqq \mathbb{Z}r = \{ar \mid a \in \mathbb{Z}\}$ est un idéal fractionnaire de $\mathbb{Z}$. En effet, en écrivant $r = \frac{p}{q}$ avec p et q entier, on a $qI = \mathbb{Z}p$ qui est bien inclus dans $\mathbb{Z}$.

Remarquons que si I est un idéal fractionnaire de A et si $x \in A$ est tel que $xI \subset A$, alors xI est un idéal de A.

Si I et J sont deux idéaux fractionnaires de A, on peut définir leur *somme* en posant

$$I + J \coloneqq \{x + y \mid (x, y) \in I \times J\}.$$

On vérifie facilement que c'est encore un idéal fractionnaire de A. On peut également définir le *produit* de I et J en posant

$$IJ \coloneqq \left\{ \sum_{i=1}^{n} x_i y_i \mid n \in \mathbb{N}^*,\ x_i \in I,\ y_i \in J \right\}.$$

On vérifie facilement que c'est également un idéal fractionnaire de A.

Un idéal fractionnaire I est dit *principal* s'il existe $x \in K$ tel que

$$I = (x) \coloneqq \{ax \mid a \in A\}.$$

Pour tout élément $x \in K \setminus \{0\}$, l'ensemble (x) est un idéal fractionnaire de A. De plus si x et y sont deux éléments de K, on a $(x) = (y)$ si et seulement si il existe $u \in A^\times$ tel que $y = ux$.

Un idéal fractionnaire I de A est dit *inversible* s'il existe un idéal fractionnaire J tel que $IJ = A$ (A est l'idéal trivial de A, engendré par 1).

5.2.4 Quelques résultats généraux sur les idéaux premiers

Cette partie contient quelques résultats techniques concernant les idéaux premiers qui nous serviront plus tard.

Rappelons que, dans $\mathbb{Z}$, un entier b divise un entier a si et seulement si l'idéal (b) contient l'idéal (a). C'est-à-dire

$$b|a \Leftrightarrow (a) \subset (b).$$

De façon plus générale, dans un anneau quelconque, si I et J sont deux idéaux, il faut penser à la relation $I \subset J$ comme « J divise I ».

Dans ce contexte, le lemme ci-dessous doit être pensé comme une version très générale du Lemme de Gauss sur la divisibilité dans $\mathbb{Z}$.

Lemme. *Soit A un anneau. Soit $\mathfrak{p}$ un idéal premier de A. Si $\mathfrak{p}$ contient un produit $\mathfrak{p}_1 \cdots \mathfrak{p}_r$, alors il existe $1 \leqslant i \leqslant r$ tel que $\mathfrak{p}_i \subset \mathfrak{p}$.*

Démonstration. Supposons par l'absurde que pour tout $1 \leqslant i \leqslant r$, il existe $x_i \in \mathfrak{p}_i \smallsetminus \mathfrak{p}$. Comme $\mathfrak{p}$ est un idéal premier, on a $\prod_{i=1}^r x_i \notin \mathfrak{p}$. Cependant $\prod_{i=1}^r x_i \in \mathfrak{p}_1 \cdots \mathfrak{p}_r$. Ceci contredit l'inclusion $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subset \mathfrak{p}$. On en déduit bien qu'il existe $1 \leqslant i \leqslant r$ tel que $\mathfrak{p}_\mathrm{i} \subset \mathfrak{p}$. □

Lemme. *Soit A un anneau noethérien. Tout idéal de A contient un produit fini d'idéaux premiers. Si de plus A est intègre, tout idéal non nul de A contient un produit fini d'idéaux premiers non nuls de A.*

Démonstration. Notons E l'ensemble des idéaux de A qui ne contiennent aucun produit fini d'idéaux premiers de A. On veut montrer que $E = \emptyset$. Supposons par l'absurde que $E \neq \emptyset$. Soit $I \in E$. En particulier I n'est pas premier. Il existe donc deux éléments x et y dans $A \smallsetminus I$ tels que $xy \in I$. Posons $I_1 = I + (x)$ et $I_2 = I + (y)$. Alors soit I_1 soit I_2 est un élément de E. En effet, dans le cas contraire, il existerait des idéaux premiers $\mathfrak{p}_1, \ldots, \mathfrak{p}_r, \mathfrak{q}_1, \ldots, \mathfrak{q}_s$ tels que $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subset I_1$ et $\mathfrak{q}_1 \cdots \mathfrak{q}_s \subset I_2$. Alors, comme $xy \in I$,

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \mathfrak{q}_1 \cdots \mathfrak{q}_s \subset I_1 I_2 \subset I$$

ce qui contredit $I \in E$. Ainsi $I_1 \in E$ ou $I_2 \in E$. On peut donc construire une suite strictement croissante d'idéaux $(I_n)_{n \geqslant 0}$ telle que $I_n \in E$, strictement croissante signifie $I_n \subsetneq I_{n+1}$ pour tout $n \geqslant 0$. Or un anneau noethérien ne peut contenir de suite strictement croissante d'idéaux. En effet si $(I_n)_{n \geqslant 0}$ est une telle suite, l'ensemble $\bigcup_{n \geqslant 0} I_n$ est un idéal de A et, puisque A est noethérien, est donc de type fini. Soient $x_1, \ldots, x_t$ des générateurs de cet idéal. Il existe $N \geqslant 0$ tel que $x_1, \ldots, x_t \in I_N$, c'est-à-dire $I_N = \bigcup_{n \geqslant 0} I_n$, donc $I_n = I_N$ pour $n \geqslant N$. Ceci contredit la croissance stricte de la suite. Finalement $E \neq \emptyset$ contredit le caractère noethérien de A, donc $E = \emptyset$.

Le même raisonnement montre que si A est intègre et noethérien, un idéal non nul contient un produit fini d'idéaux premiers non nuls. □

Lemme (Lemme de Krull)**.** *Soit A un anneau commutatif et soit $I \subset A$ un idéal non trivial ($I \neq A$). Alors il existe un idéal maximal $\mathfrak{m}$ contenant I.*

Démonstration. Donnons la preuve dans le cas particulier où A est noethérien, seul cas dans lequel nous utiliserons ce résultat. Supposons par l'absurde qu'il n'existe pas d'idéal maximal contenant I. On peut alors construire par récurrence une suite $(I_n)_{n\geqslant 0}$ telle que $I_0 = I$ et $I_n \subsetneq I_{n+1} \subsetneq A$. L'existence d'une telle suite contredit alors le caractère noethérien de A. La démonstration du cas général nécessite l'usage de l'axiome du choix. □

5.2.5 Décomposition des idéaux dans un anneau de Dedekind

Nous allons démontrer ici que les anneaux de Dedekind ont des propriétés similaires à certaines propriétés des anneaux factoriels, à condition de remplacer les éléments de l'anneau par ses idéaux.

Commençons par prouver que tout idéal premier non nul $\mathfrak{p}$ (ou idéal maximal) d'un anneau de Dedekind A est inversible. Rappelons que cela signifie qu'il existe un idéal fractionnaire $\mathfrak{q}$ tel que $\mathfrak{pq} = A$.

Théorème 5.10. *Soit A un anneau de Dedekind. Tout idéal premier non nul $\mathfrak{p}$ de A est inversible.*

Démonstration. Soit K le corps des fractions de A. On cherche donc à construire un idéal fractionnaire $\mathfrak{p}^{-1} \subset K$ tel que $\mathfrak{pp}^{-1} = A$. Remarquons déjà que si $\mathfrak{p}^{-1}$ existe alors $\mathfrak{p}^{-1}$ est contenu dans $\{x \in K \mid x\mathfrak{p} \subset A\}$. Commençons donc par considérer cet ensemble, que nous notons $\mathfrak{p}'$:

$$\mathfrak{p}' = \{x \in K \mid x\mathfrak{p} \subset A\}.$$

Il est facile de vérifier que $\mathfrak{p}'$ est un sous-A-module de K. Montrons que c'est en réalité un idéal fractionnaire de A. En effet, comme $\mathfrak{p}$ est non nul, on peut choisir $d \in \mathfrak{p} \setminus \{0\}$. Alors, par définition de $\mathfrak{p}'$, on a $d\mathfrak{p}' \subset A$. Ceci montre que $\mathfrak{p}'$ est un idéal fractionnaire de A.

Montrons à présent que $\mathfrak{pp}' = A$. Ce qui est clair, c'est que $\mathfrak{pp}' \subset A$ par définition de $\mathfrak{p}'$. De plus $\mathfrak{pp}'$ est un idéal fractionnaire de A qui est contenu dans A, c'est donc un idéal de A. De plus, il est clair que $A \subset \mathfrak{p}'$. On en déduit donc que $\mathfrak{p}A = \mathfrak{p} \subset \mathfrak{pp}'$. On a donc une inclusion d'idéaux de A :

$$\mathfrak{p} \subset \mathfrak{pp}' \subset A.$$

Utilisons à présent le fait que A est un anneau de Dedekind : on sait que $\mathfrak{p}$ est premier non nul, donc un idéal maximal de A. Ceci implique que $\mathfrak{pp}' = \mathfrak{p}$ ou $\mathfrak{pp}' = A$. Dans le deuxième cas, on a gagné. Il faut donc exclure le premier cas. Nous aurons besoin d'un lemme qui sera réutilisé plus tard.

Lemme. *Soit $\mathfrak{a}$ un idéal fractionnaire non nul d'un anneau de Dedekind A. Si $x \in K$, où K désigne le corps des fractions de A, est tel que $x\mathfrak{a} \subset \mathfrak{a}$, alors $x \in A$.*

Démonstration. Soit $d \in A \smallsetminus \{0\}$ tel que $d\mathfrak{a} \subset A$. Alors $x(d\mathfrak{a}) \subset d\mathfrak{a}$ et $d\mathfrak{a}$ est un idéal non nul de A. Quitte à remplacer $\mathfrak{a}$ par $d\mathfrak{a}$, on peut donc supposer que $\mathfrak{a}$ est un idéal de A, ce que l'on fait. On a $x\mathfrak{a} \subset \mathfrak{a}$ et donc, par une récurrence immédiate, $x^n\mathfrak{a} \subset \mathfrak{a}$ pour tout entier $n \geqslant 0$. On en conclut que si $P \in \mathbb{Z}[X]$, alors $P(x)\mathfrak{a} \subset \mathfrak{a}$. Ainsi, pour tout $y \in A[x]$, on a $y\mathfrak{a} \subset \mathfrak{a}$. Rappelons de plus que $\mathfrak{a}$ est non nul, il existe donc $b \in \mathfrak{a} \smallsetminus \{0\}$. Ainsi pour tout $y \in A[x]$, on a

$$y(b) \subset y\mathfrak{a} \subset \mathfrak{a} \subset A.$$

Ainsi $bA[x] \subset A$ et on vérifie facilement que $bA[x]$ est un idéal de A. Comme A est un anneau de Dedekind, il est en particulier noethérien et $bA[x]$ est donc un A-module de type fini. Ceci implique que $A[x] = b^{-1}(bA[x])$ est également un A-module de type fini. On déduit alors du théorème 5.1 que x est entier sur A. L'élément x est donc un élément de K qui est entier sur A. Comme A est un anneau de Dedekind, il est intégralement clos, on a donc $x \in A$. □

Supposons donc, par l'absurde, que $\mathfrak{p}\mathfrak{p}' = \mathfrak{p}$. Soit $x \in \mathfrak{p}'$. Comme $\mathfrak{p}\mathfrak{p}' = \mathfrak{p}$, on a $x\mathfrak{p} \subset \mathfrak{p}$ et donc, d'après le lemme ci-dessus, $x \in A$. Ainsi on a prouvé que $\mathfrak{p}' \subset A$. Comme par ailleurs on a déjà vu que $A \subset \mathfrak{p}'$, on en conclut que $\mathfrak{p}' = A$. En d'autres termes, on a « simplifié par $\mathfrak{p}$ » dans l'égalité $\mathfrak{p}\mathfrak{p}' = \mathfrak{p}$, mais comme on vient de le voir, c'est une opération qui est loin d'être automatique !

Nous ne sommes pas encore arrivés à une contradiction. Continuons. Soit $a \in \mathfrak{p} \smallsetminus \{0\}$. Comme l'anneau A est noethérien et intègre, l'idéal non nul (a) contient un produit fini d'idéaux premiers non nuls $\mathfrak{p}_1 \cdots \mathfrak{p}_r$. Supposons que r est minimal parmi l'ensemble des entiers n tels que (a) contient un produit de n idéaux premiers non nuls. On a des inclusions

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \subset (a) \subset \mathfrak{p}.$$

Comme $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ et $\mathfrak{p}$ sont des idéaux premiers, il existe $1 \leqslant i \leqslant r$ tel que $\mathfrak{p}_i \subset \mathfrak{p}$. Mais A est un anneau de Dedekind, donc $\mathfrak{p}_i$ est un idéal maximal ! Comme $\mathfrak{p} \neq A$ (puisque $\mathfrak{p}$ est premier), on a $\mathfrak{p} = \mathfrak{p}_i$. Quitte à réordonner les indices $1 \leqslant i \leqslant r$, et par commutativité de A, on peut supposer que $i = 1$. Posons $I = \mathfrak{p}_2 \cdots \mathfrak{p}_r$. On a donc $\mathfrak{p}I \subset (a)$ et, par minimalité de r, $I \not\subset (a)$. Soit donc $b \in I \smallsetminus (a)$. Alors, puisque $\mathfrak{p}I \subset (a)$, on a $b\mathfrak{p} \subset (a)$. Ainsi $\frac{b}{a}\mathfrak{p} \subset A$. Par définition de $\mathfrak{p}'$, on en déduit que $\frac{b}{a} \in \mathfrak{p}' = A$ et donc $a|b$ dans A, ou encore $b \in (a)$. C'est une contradiction. □

Remarque. Soit $\mathfrak{p}$ un idéal premier non nul d'un anneau de Dedekind A. Si $\mathfrak{p}'$ est un idéal fractionnaire tel que $\mathfrak{p}\mathfrak{p}' = A$, alors $\mathfrak{p}'$ est unique. On le note donc $\mathfrak{p}^{-1}$ et on l'appelle *inverse* de A. En effet si $\mathfrak{p}\mathfrak{p}' = \mathfrak{p}\mathfrak{p}''$, on a alors

$$\underbrace{\mathfrak{p}'\mathfrak{p}}_{=A}\,\mathfrak{p}' = \underbrace{\mathfrak{p}'\mathfrak{p}}_{=A}\,\mathfrak{p}'' \Rightarrow \mathfrak{p}' = \mathfrak{p}''.$$

Si $n \in \mathbb{Z}$, on pose donc

$$\mathfrak{p}^n = \begin{cases} \mathfrak{p}^n & \text{si } n > 0; \\ (\mathfrak{p}^{-1})^{-n} & \text{si } n < 0; \\ A & \text{si } n = 0. \end{cases}$$

Voici le théorème fondamental concernant la multiplication dans les anneaux de Dedekind.

Théorème 5.11. *Soit A un anneau de Dedekind. Notons $\mathcal{P}$ l'ensemble des idéaux premiers non nuls de A. Si I est un idéal fractionnaire non nul de A, il existe une unique famille presque nulle $(n_\mathfrak{p})_{\mathfrak{p}\in\mathcal{P}}$ d'éléments de $\mathbb{Z}$ (c'est-à-dire $n_\mathfrak{p} = 0$ sauf pour un nombre fini de $\mathfrak{p}$) telle que*

$$I = \prod_{\mathfrak{p}\in\mathcal{P}} \mathfrak{p}^{n_\mathfrak{p}} = \underbrace{\mathfrak{p}_1 \cdots \mathfrak{p}_1}_{n_{\mathfrak{p}_1}} \underbrace{\mathfrak{p}_2 \cdots \mathfrak{p}_2}_{n_{\mathfrak{p}_2}} \cdots \underbrace{\mathfrak{p}_r \cdots \mathfrak{p}_r}_{n_{\mathfrak{p}_r}}.$$

De plus, si $I \subset A$, alors tous les $n_\mathfrak{p}$ sont dans $\mathbb{N}$.

Démonstration. Commençons par démontrer l'existence de la décomposition. Soit $\mathfrak{a}$ un idéal fractionnaire non nul de A. On peut supposer que $\mathfrak{a}$ est un idéal de A. En effet, dans le cas général on peut trouver $d \in A \setminus \{0\}$ tel que $d\mathfrak{a} \subset A$. Alors, si $d\mathfrak{a}$ et (d) se décomposent en produits d'idéaux premiers

$$d\mathfrak{a} = \prod_{\mathfrak{p}\in\mathcal{P}} \mathfrak{p}^{n_\mathfrak{p}}, \quad (d) = \prod_{\mathfrak{p}\in\mathcal{P}} \mathfrak{p}^{m_\mathfrak{p}},$$

il en est de même de $\mathfrak{a}$ puisque

$$\mathfrak{a} = (d^{-1})(d\mathfrak{a}) = \prod_{\mathfrak{p}\in\mathcal{P}} \mathfrak{p}^{n_\mathfrak{p}-m_\mathfrak{p}}.$$

On est donc ramener à prouver que si $\mathfrak{a}$ est un idéal non nul de A, il existe des idéaux premiers non nuls $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ tels que $\mathfrak{a} = \mathfrak{p}_1 \ldots \mathfrak{p}_n$. Notons E l'ensemble des idéaux non nuls de A qui ne vérifient pas cette propriété. On veut montrer que $E = \emptyset$. Supposons donc E non vide. Soit $\mathfrak{a} \in E$. En particulier $\mathfrak{a}$ n'est pas un idéal maximal de A. D'après le Lemme de Krull, il existe un idéal maximal $\mathfrak{m}$, donc premier, tel que $\mathfrak{a} \subset \mathfrak{m}$. D'après le théorème 5.10, on a $\mathfrak{m}^{-1}\mathfrak{a} \subset A$. Donc $\mathfrak{m}^{-1}\mathfrak{a}$ est un idéal de A. On a également l'inclusion $\mathfrak{m}\mathfrak{a} \subset \mathfrak{a}$. En multipliant les deux côtés de cette inclusion par l'idéal fractionnaire $\mathfrak{m}^{-1}$, on obtient $\mathfrak{a} \subset \mathfrak{m}^{-1}\mathfrak{a}$. Montrons que cette inclusion est stricte.

Supposons par l'absurde que $\mathfrak{a} = \mathfrak{a}\mathfrak{m}^{-1}$. Le lemme utilisé dans la preuve du théorème 5.10 montre alors que $\mathfrak{m}^{-1} \subset A$. Comme, clairement, $A \subset \mathfrak{m}^{-1}$, on a $A = \mathfrak{m}^{-1}$ et donc $A = \mathfrak{m}$ en utilisant encore une fois le théorème 5.10. C'est absurde. On a donc

$$\mathfrak{a} \subsetneq \mathfrak{m}^{-1}\mathfrak{a} \subset A.$$

Montrons enfin que $\mathfrak{b} := \mathfrak{m}^{-1}\mathfrak{a}$ est un élément de E. Si on peut écrire $\mathfrak{b} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ avec $\mathfrak{p}_i$ premiers non nuls, alors, par définition de $\mathfrak{m}^{-1}$, on a $\mathfrak{a} = \mathfrak{m}\mathfrak{p}_1 \cdots \mathfrak{p}_r$, ce qui contredit $\mathfrak{a} \in E$. En continuant ce processus, on peut créer une suite strictement croissante d'éléments de E, ce qui contredit le caractère noethérien de A.

Prouvons à présent l'unicité de la décomposition. Supposons que l'on ait une égalité de la forme

$$\prod_{\mathfrak{p}\in\mathcal{P}} \mathfrak{p}^{n_\mathfrak{p}} = \prod_{\mathfrak{p}\in\mathcal{P}} \mathfrak{p}^{m_\mathfrak{p}}$$

avec des entiers relatifs $n_\mathfrak{p}$ et $m_\mathfrak{p}$ presque tous nuls. On déduit du théorème 5.10 une égalité

$$\prod_{\mathfrak{p}\in\mathcal{P}} \mathfrak{p}^{n_\mathfrak{p}-m_\mathfrak{p}} = A.$$

Supposons par l'absurde qu'il existe au moins un idéal premier $\mathfrak{p}$ tel que $n_\mathfrak{p} - m_\mathfrak{p} \neq 0$. Quitte à multiplier cette égalité par une puissance convenable des idéaux $\mathfrak{p}$ tels que $n_\mathfrak{p} - m_\mathfrak{p} < 0$, on est ramené à une situation

$$\mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_r^{n_r} = \mathfrak{q}_1^{m_1} \cdots \mathfrak{q}_s^{m_s}$$

où $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ et $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$ sont des idéaux premiers non nuls *deux à deux distincts* et $n_1, \ldots, n_r$, $m_1, \ldots, m_s$ des entiers > 0. Alors

$$\mathfrak{p}_1 \supset \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_r^{n_r} = \mathfrak{q}_1^{m_1} \cdots \mathfrak{q}_s^{m_s}.$$

Il existe donc $1 \leqslant j \leqslant s$ tel que $\mathfrak{p}_1 \supset \mathfrak{q}_j$. Comme $\mathfrak{q}_j$ est un idéal premier non nul et que A est un anneau de Dedekind, l'idéal $\mathfrak{q}_j$ est maximal et donc $\mathfrak{p}_1 = \mathfrak{q}_j$, c'est une contradiction. □

Exemple. Nous avons déjà remarqué que l'anneau $A = \mathbb{Z}[i\sqrt{5}]$ est un anneau de Dedekind qui n'est pas factoriel. Appliquons le théorème 5.11 à la factorisation de certains idéaux. Prenons l'exemple de l'idéal principal $\mathfrak{a} = (2)$ engendré par l'élément 2. On cherche une décomposition $(2) = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ où les $\mathfrak{p}_i$ sont des idéaux premiers non nuls de A. Remarquons que l'on a alors $(2) \subset \mathfrak{p}_i$ pour tout $1 \leqslant i \leqslant r$. Il faut donc commencer par déterminer quels idéaux premiers de A contiennent (2). Or, dans un anneau quelconque A, les idéaux de A contenant un idéal I sont en bijection avec les idéaux de A/I. Il faut donc, dans notre cas, determiner l'anneau $A/\mathfrak{a} = \mathbb{Z}[i\sqrt{5}]/(2)$.

Pour cela, on peut commencer par remarquer que $\mathbb{Z}[i\sqrt{5}]$ est isomorphe à l'anneau $\mathbb{Z}[X]/(X^2+5)$. En effet, par définition de $\mathbb{Z}[i\sqrt{5}]$, il existe un (unique) morphisme d'anneaux *surjectif* $\mathbb{Z}[X] \to \mathbb{Z}[i\sqrt{5}]$ envoyant X sur $i\sqrt{5}$. L'utilisation de la division euclidienne dans $\mathbb{Z}[X]$ par X^2+5 (possible car X^2+5 est unitaire) montre assez facilement que le noyau de ce morphisme est l'idéal principal (X^2+5). D'où l'isomorphisme recherché.

On peut à présent décrire plus facilement le quotient $\mathbb{Z}[i\sqrt{5}]/(2)$:

$$\mathbb{Z}[i\sqrt{5}]/(2) \simeq \mathbb{Z}[X]/((X^2+5)+(2)) = \mathbb{Z}[X]/(X^2+5, 2) \simeq \mathbb{F}_2[X]/(X^2+\overline{5})$$

où $X^2+\overline{5}$ est l'image de X^2+5 dans $\mathbb{F}_2[X]$. Or, dans $\mathbb{F}_2[X]$, on a

$$X^2+\overline{5} = X^2+\overline{1} = (X+\overline{1})^2.$$

Ainsi, $\mathbb{Z}[i\sqrt{5}]/(2) \simeq \mathbb{F}_2[X]/(X+1)^2$. On remarque premièrement que $\mathbb{Z}[i\sqrt{5}]/(2)$ n'est pas intègre, donc que l'idéal (2) n'est pas premier dans $\mathbb{Z}[i\sqrt{5}]$. Par ailleurs, l'anneau $\mathbb{F}_2[X]/(X+1)^2$ possède un unique idéal premier : l'idéal engendré par $(X+1)$ (en effet, comme $\mathbb{F}_2[X]$ est principal, les idéaux premiers de $\mathbb{F}_2[X]/(X+1)^2$ sont en bijection avec les idéaux premiers de $\mathbb{F}_2[X]$ contenant $(X+1)^2$, c'est-à-dire avec les élément irréductibles de $\mathbb{F}_2[X]$ divisant $(X+1)^2$). Il y a donc un unique idéal premier de $\mathbb{Z}[i\sqrt{5}]$ contenant (2), c'est l'image inverse $\mathfrak{p}$ dans $\mathbb{Z}[i\sqrt{5}]$ de l'idéal $(X+1)$ de $\mathbb{F}_2[X]/(X+1)^2 \simeq \mathbb{Z}[i\sqrt{5}]/(2)$. Cette image inverse est donc $\mathfrak{p} = (2, 1+i\sqrt{5})$. Il existe donc $n \geqslant 1$ tel que $(2) = \mathfrak{p}^n$. Comme $(X+1)^2 = 0$ dans $\mathbb{F}_2[X]/(X+1)^2$, on a $\mathfrak{p}^2 \subset (2)$. Comme par ailleurs $(2) \subsetneq \mathfrak{p}$ (puisque (2) n'est pas premier), on a finalement $(2) = \mathfrak{p}^2$. On peut aussi vérifier directement que $(2, 1+i\sqrt{5})^2 = (2)$ (exercice).

Décomposons à présent l'idéal (3) dans $\mathbb{Z}[i\sqrt{5}]$. Le même raisonnement que ci-dessus montre que

$$\mathbb{Z}[i\sqrt{5}]/(3) \simeq \mathbb{F}_3[X]/(X-1)(X+1).$$

Ainsi (3) n'est pas premier et (3) est contenu dans exactement deux idéaux maximaux de $\mathbb{Z}[i\sqrt{5}]$: $\mathfrak{p}_1 = (3, 1+i\sqrt{5})$ et $\mathfrak{p}_2 = (3, -1+i\sqrt{5})$. On vérifie alors que $(3) = \mathfrak{p}_1\mathfrak{p}_2$.

Décomposons $\mathfrak{a} = (11)$ dans $\mathbb{Z}[i\sqrt{5}]$. Cette fois-ci, on a

$$\mathbb{Z}[i\sqrt{5}]/(11) \simeq \mathbb{F}_{11}[X]/(X^2+5).$$

Il faut donc décomposer l'idéal X^2+5 en produit d'irréductibles dans l'anneau principal $\mathbb{F}_{11}[X]$. Le polynôme X^2+5 étant de degré 2, il est irréductible dans $\mathbb{F}_{11}[X]$ si et seulement si il possède une racine dans $\mathbb{F}_{11}$. Il possède une racine dans $\mathbb{F}_{11}[X]$ si et seulement si -5 est un carré dans $\mathbb{F}_{11}$. On peut utiliser la loi de réciprocité quadratique pour tester ceci (ou faire directement la liste des carrés de $\mathbb{F}_{11}$) :

$$\left(\frac{-5}{11}\right) = -\left(\frac{5}{11}\right) = -\left(\frac{11}{5}\right) = -\left(\frac{1}{5}\right) = -1.$$

Donc X^2+5 est irréductible dans $\mathbb{F}_{11}$, ceci implique que $\mathbb{Z}[i\sqrt{5}]/(11)$ est un anneau intègre et que l'idéal (11) est déjà premier dans $\mathbb{Z}[i\sqrt{5}]$.

Remarque. Soit A un anneau de Dedekind et soit $\mathfrak{a}$ un idéal fractionnaire non nul de A. On peut décomposer $\mathfrak{a}$ en produit d'idéaux premier non nuls :

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_\mathfrak{p}}.$$

Il découle du théorème 5.11 que $\mathfrak{a} \subset A$ si et seulement si, pour tout $\mathfrak{p}$, on a $n_\mathfrak{p} \geqslant 0$.

De façon générale, si $\mathfrak{a}$ est un idéal fractionnaire non nul de A et $\mathfrak{p}$ un idéal premier non nul de A, on note $v_\mathfrak{p}(\mathfrak{a}) \in \mathbb{Z}$ la puissance de l'idéal $\mathfrak{p}$ dans la décomposition de $\mathfrak{a}$. On a donc

$$\mathfrak{a} = \prod_{\mathfrak{p} \in \mathcal{P}} \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{a})}$$

et $\mathfrak{a} \subset A \Leftrightarrow \forall \mathfrak{p} \in \mathcal{P},\ v_\mathfrak{p}(\mathfrak{a}) \geqslant 0$.

Si $\mathfrak{a}$ et $\mathfrak{b}$ sont deux idéaux non nuls d'un anneau de Dedekind. On dit que $\mathfrak{b}$ *divise* $\mathfrak{a}$ s'il existe un idéal $\mathfrak{c}$ tel que $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$.

Corollaire. *Soient $\mathfrak{a}$ et $\mathfrak{b}$ deux idéaux non nuls d'un anneau de Dedekind A. Alors $\mathfrak{b}$ divise $\mathfrak{a}$ si et seulement si $\mathfrak{b} \supset \mathfrak{a}$.*

Démonstration. Le sens $\mathfrak{a} = \mathfrak{b}\mathfrak{c} \Rightarrow \mathfrak{b} \supset \mathfrak{a}$ est immédiat. Il faut prouver l'autre implication. Supposons donc que $\mathfrak{b} \supset \mathfrak{a}$. On a alors

$$\mathfrak{a} = \prod_{\mathfrak{p} \in \mathcal{P}} \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{a})}, \quad \mathfrak{b} = \prod_{\mathfrak{p} \in \mathcal{P}} \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{b})}.$$

En multipliant l'inclusion $\mathfrak{b} \supset \mathfrak{a}$ par $\mathfrak{b}^{-1}$, on obtient

$$A \supset \prod_{\mathfrak{p} \in \mathcal{P}} \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{a}) - v_\mathfrak{p}(\mathfrak{b})}$$

ce qui implique bien $v_\mathfrak{p}(\mathfrak{a}) \geqslant v_\mathfrak{p}(\mathfrak{b})$ pour tout idéal premier non nul $\mathfrak{p}$. On peut alors poser

$$\mathfrak{c} = \prod_{\mathfrak{p} \in \mathcal{P}} \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{a}) - v_\mathfrak{p}(\mathfrak{b})}. \qquad \square$$

5.3 Groupe des classes d'idéaux

5.3.1 Définitions

Soit A un anneau de Dedekind. On note $I(A)$ l'ensemble des idéaux fractionnaires non nuls de A. Il s'agit d'un groupe abélien pour la multiplication des idéaux fractionnaires. Son élément neutre est l'idéal trivial A. Pour vérifier que $I(A)$ est bien un groupe, le point délicat est de vérifier que tout élément possède un inverse. L'existence de cet inverse est assurée par les théorèmes 5.10 et 5.11.

Plus précisément, le théorème 5.11 montre que $I(A)$ est un groupe abélien libre dont une base est donnée par l'ensemble $\mathcal{P}$ des idéaux premiers non nuls de A. Autrement dit l'application suivante est un isomorphisme de groupes :

$$\begin{array}{ccc} I(A) & \longrightarrow & \bigoplus_{\mathfrak{p} \in \mathcal{P}} \mathbb{Z} \\ \mathfrak{a} & \longmapsto & v_\mathfrak{p}(\mathfrak{a}). \end{array}$$

On note $P(A)$ le sous-groupe de $I(A)$ constitué des idéaux principaux (vérifier que c'est bien un sous-groupe) et on note $\mathrm{Cl}(A) \coloneqq I(A)/P(A)$ le groupe quotient. On appelle $\mathrm{Cl}(A)$ le *groupe des classes d'idéaux* de A.

On peut encore décrire le groupe $\mathrm{Cl}(A)$ comme le quotient de l'ensemble $I(A)$ par la relation d'équivalence suivante :

$$I \sim J \Leftrightarrow \exists \alpha \in K^\times,\ J = \alpha I.$$

Les éléments de $\mathrm{Cl}(A)$ sont appelés les *classes d'idéaux* de A, ce sont en effet les classes d'équivalence pour la relation ci-dessus. Le lemme ci-dessous montre que toute classe d'équivalence contient un idéal de A (et pas uniquement un idéal fractionnaire).

Lemme. *Soit $c \in \mathrm{Cl}(A)$. Alors il existe un idéal $\mathfrak{a} \subset A$ tel que $\mathfrak{a} \in c$.*

Démonstration. Soit $\mathfrak{b} \in c$ un idéal fractionnaire de la classe c. Alors il existe $d \in A \setminus \{0\}$ tel que $d\mathfrak{b} \subset A$. On peut donc choisir $\mathrm{a} = d\mathfrak{b}$ puisque $\mathfrak{a}$ et $\mathfrak{b}$ sont clairement dans la même classe. □

Remarque. Soit A un anneau de Dedekind. L'anneau A est principal si et seulement si tous ses idéaux sont principaux, c'est-à-dire si et seulement si tous ses idéaux sont dans la même classe. Ainsi le groupe $\mathrm{Cl}(A)$ est trivial, ie $\mathrm{Cl}(A) = \{e\}$, si et seulement si l'anneau A est principal. Le groupe $\mathrm{Cl}(A)$ mesure donc le défaut de principalité de l'anneau A.

Exemple. D'après la remarque ci-dessus, on a donc

$$\mathrm{Cl}(\mathbb{Z}) = \mathrm{Cl}(\mathbb{Z}[i]) = \mathrm{Cl}(\mathbb{Z}[i\sqrt{2}]) = \{e\}.$$

En revanche $\mathrm{Cl}(\mathbb{Z}[i\sqrt{5}])$ est un groupe non trivial. Nous le calculerons plus tard.

5.3.2 Le cas particulier des corps de nombres

Théorème 5.12. *Soit K un corps de nombres. Alors le groupe $\mathrm{Cl}(\mathcal{O}_K)$ est un groupe abélien* fini.

Le cardinal h_K du groupe $\mathrm{Cl}(\mathcal{O}_K)$ est appelé *nombre de classes* du corps K. En général, c'est un nombre assez délicat à calculer.

Remarque. Il existe des anneaux de Dedekind dont le groupe de classes est infini. Le théorème 5.12 est donc particulier aux anneaux d'entiers de corps de nombres.

Afin de démontrer le théorème 5.12, nous aurons besoin du lemme suivant qui est une variation sur le thème du principe des tiroirs de Dirichlet.

Lemme. *Il existe un entier $M \geqslant 1$, ne dépendant que de K, tel que pour tout $\alpha \in \mathcal{O}_K$ et tout $\beta \in \mathcal{O}_K \smallsetminus \{0\}$, il existe $1 \leqslant t \leqslant M$ entier et $\omega \in \mathcal{O}_K$ tels que*

$$|N_{K/\mathbb{Q}}(t\alpha - \omega\beta)| < |N_{K/\mathbb{Q}}(\beta)|.$$

Démonstration. Posons $\gamma = \frac{\alpha}{\beta} \in K$. On recherche donc un entier t et un élément $\omega \in \mathcal{O}_K$ tels que $|N_{K/\mathbb{Q}}(t\gamma - \omega)| < 1$. Rappelons que d'après le théorème 5.7, l'anneau $\mathcal{O}_K$ est un $\mathbb{Z}$-module libre de rang $n = [K : \mathbb{Q}]$. On peut donc trouver une famille $(\omega_1, \dots, \omega_n) \in \mathcal{O}_K^n$ telle que $\mathcal{O}_K = \mathbb{Z}\omega_1 \oplus \cdots \oplus \mathbb{Z}\omega_n$. Comme K est le corps des fractions de $\mathcal{O}_K$, la famille $(\omega_1, \dots, \omega_n)$ est également une base du $\mathbb{Q}$-espace vectoriel K. Posons alors $\gamma = \sum_{i=1}^n \gamma_i\omega_i$, $\gamma_i \in \mathbb{Q}$. Considérons l'application

$$f : \begin{array}{ccc} \mathbb{Q}^n & \longrightarrow & \mathbb{Q} \\ (x_1, \dots, x_n) & \longmapsto & N_{K/\mathbb{Q}}(x_1\omega_1 + \cdots + x_n\omega_n). \end{array}$$

Rappelons que

$$N_{K/\mathbb{Q}}(x_1\omega_1 + \cdots + x_n\omega_n) = \det(m_{x_1\omega_1 + \cdots + x_n\omega_n}) = \det(x_1 m_{\omega_1} + \cdots + x_n m_{\omega_n}).$$

Comme $\det : \mathcal{M}_n(\mathbb{Q}) \to \mathbb{Q}$ est un polynôme homogène de degré n, on en conclut que l'application f est un polynôme homogène de degré n en les variables $x_1, \dots, x_n$. Il existe donc des éléments $a_{(i_1,\dots,i_n)} \in \mathbb{Q}$ tels que

$$\forall (x_1, \dots, x_n) \in \mathbb{Q}^n, \quad f(x_1, \dots, x_n) = \sum_{\substack{(i_1,\dots,i_n) \in \mathbb{N}^n \\ i_1 + \cdots + i_n = n}} a_{(i_1,\dots,i_n)} x_1^{i_1} \cdots x_n^{i_n}.$$

En posant $C = \max |a_{(i_1,\dots,i_n)}| \operatorname{Card}\{(i_1, \dots, i_n) \in \mathbb{N}^n \mid i_1 + \cdots + i_n = n\}$, on obtient

$$\forall (x_1, \dots, x_n) \in \mathbb{Q}^n, \quad |f(x_1, \dots, x_n)| \leqslant C(\max |x_i|)^n.$$

Rappelons que l'on est parti de l'élément $\gamma = \sum_{i=1}^n \gamma_i\omega_i \in K$. Posons alors, pour $1 \leqslant i \leqslant n$, $\gamma_i = \lfloor \gamma_i \rfloor + \{\gamma_i\}$ avec $\lfloor \gamma_i \rfloor \in \mathbb{N}$ et $0 \leqslant \{\gamma_i\} < 1$. On définit

$$\lfloor \gamma \rfloor \coloneqq \sum_{i=1}^n \lfloor \gamma_i \rfloor \omega_i \in \mathcal{O}_K, \quad \{\gamma\} \coloneqq \sum_{i=1}^n \{\gamma_i\}\omega_i \in K.$$

Enfin, plongeons K dans $\mathbb{R}^n$ au moyen du morphisme, injectif, de groupes suivant :

$$\phi : \begin{array}{ccc} K & \longrightarrow & \mathbb{R}^n \\ \sum_{i=1}^n x_i\omega_i & \longmapsto & (x_1, \dots, x_n). \end{array}$$

On a alors $\phi(\{\gamma\}) \in [0, 1[^n$. Fixons un entier $m > C^{\frac{1}{n}}$ et posons $M \coloneqq m^n$. On peut découper le cube $[0, 1[^n$ en m^n « petits » cubes de côté $\frac{1}{m}$:

$$[0, 1[^n = \coprod_{0 \leqslant a_i < m} \prod_{i=1}^n \left[\frac{a_i}{m}, \frac{a_i + 1}{m} \right[.$$

Considérons les $M+1$-points $\phi(\{k\gamma\}) \in [0,1[^n$ pour $1 \leqslant k \leqslant M+1$. Ils se répartissent dans la partition de $[0,1[^n$ en M petits cubes. Au moins deux d'entre eux doivent donc appartenir au même petit cube. Il existe donc $1 \leqslant k_\gamma < \ell_\gamma \leqslant M+1$ tels que $\phi(\{k_\gamma\gamma\})$ et $\phi(\{\ell_\gamma\gamma\})$ appartiennent au même petit cube. Posons $t = \ell_\gamma - k_\gamma$ et $t\gamma = \omega + \delta$ avec $\omega \coloneqq \lfloor \ell_\gamma\gamma \rfloor - \lfloor k_\gamma\gamma \rfloor$, $\delta \coloneqq \{\ell_\gamma\gamma\} - \{k_\gamma\gamma\}$. On a donc $\omega \in \mathcal{O}_K$ et $\delta = \sum_{i=1}^n \delta_i\omega_i$ avec $|\delta_i| < \frac{1}{m}$ d'où $|N_{K/\mathbb{Q}}(\delta)| \leqslant Cm^{-n} < 1$. Remarquons que t est un entier $1 \leqslant t \leqslant M$ et que M ne dépend pas des éléments α et β choisis au départ. □

Nous pouvons à présent démontrer le théorème 5.12. Le début de la preuve ressemble beaucoup à la démonstration de la proposition de la partie 5.2.1. Sauf qu'ici le raisonnement n'aboutit pas au caractère principal de l'anneau $\mathcal{O}_K$ mais à la finitude du groupe de classes. C'est assez logique si on pense à la finitude du groupe de classes comme un énoncé nous disant que $\mathcal{O}_K$ n'est pas principal mais *presque*...

Démonstration du théorème 5.12. Soit I un idéal non nul de $\mathcal{O}_K$. On choisit un élément $\beta \in I \smallsetminus \{0\}$ tel que $|N_{K/\mathbb{Q}}(\beta)|$ soit minimal. Soit $\alpha \in I$. D'après le lemme, il existe un entier M (indépendant de α) un entier et $1 \leqslant t_\alpha \leqslant M$ tel que $|N_{K/\mathbb{Q}}(t_\alpha\alpha - \omega\beta)| < |N_{K/\mathbb{Q}}(\beta)|$ où $\omega \in \mathcal{O}_K$. Or $t_\alpha\alpha - \omega\beta \in I$. Ainsi par minimalité de $|N_{K/\mathbb{Q}}(\beta)|$ on doit avoir $t_\alpha\alpha - \omega\beta = 0$, c'est-à-dire $t_\alpha\alpha \in (\beta)$. Comme t_α divise $M!$, on a $M!\alpha \in (\beta)$. On en déduit que, pour tout $\alpha \in I$, on a $M!\alpha \in (\beta)$. Ainsi $M!I \subset (\beta)$. Posons donc $J \coloneqq (\beta)I^{-1}$. C'est un idéal fractionnaire de $\mathcal{O}_K$ et $J \sim I^{-1}$ par définition. De plus, on a $(\beta) \subset I$ donc $J \subset \mathcal{O}_K$ et on vient de montrer que $M! \in J$. Notons $\overline{J}$ l'image de J dans l'anneau quotient $\mathcal{O}_K/(M!)$ par l'application quotient $\pi : \mathcal{O}_K \to \mathcal{O}_K/(M!)$. Comme $(M!) \subset J$, on a $J = \pi^{-1}(\overline{J})$. Comme l'anneau $\mathcal{O}_K/(M!)$ est *fini*, on en déduit qu'il n'y a qu'un nombre fini de possibilités pour J : le nombre d'idéaux de $\mathcal{O}_K$ contenant $M!$ est fini. Or toute classe $c \in \mathrm{Cl}(\mathcal{O}_K)$ possède un élément de la forme J^{-1} où J est un idéal de $\mathcal{O}_K$ contenant $M!$. On en conclut que $\mathrm{Cl}(\mathcal{O}_K)$ est un ensemble fini. □

5.3.3 Norme d'un idéal dans un corps de nombres

Soit K un corps de nombres et soit $I \subset \mathcal{O}_K$ un idéal non nul. Alors l'ensemble $\mathcal{O}_K/I$ est fini. On pose alors $N(I) \coloneqq \mathrm{Card}\,\mathcal{O}_K/I$. C'est un entier appelé *norme* de l'idéal I.

On veut prouver que la norme est multiplicative.

Commençons par une caractérisation de la norme en fonction du discriminant. On rappelle qu'un idéal non nul $I \subset \mathcal{O}_K$ est un $\mathbb{Z}$-module libre de rang $n = [K : \mathbb{Q}]$.

Lemme. *Soit I un idéal non nul de $\mathcal{O}_K$ et soit $(\omega_1, \ldots, \omega_n)$ une base du $\mathbb{Z}$-module I. On a alors*

$$\Delta_{K/\mathbb{Q}}(\omega_1, \ldots, \omega_n) = N(I)^2\Delta_{\mathcal{O}_K/\mathbb{Z}}.$$

Démonstration. On a déjà vu que $\Delta_{\mathcal{O}_K/\mathbb{Z}}$ est le discriminant d'une $\mathbb{Z}$-base de $\mathcal{O}_K$ et ne dépend pas du choix de cette $\mathbb{Z}$-base. Pour la même raison, le nombre $\Delta_{K/\mathbb{Q}}(\omega_1, \ldots, \omega_n)$ ne dépend que de I et pas du choix de la base $(\omega_1, \ldots, \omega_n)$. Le théorème de structure

des $\mathbb{Z}$-modules libres de type fini nous assure donc l'existence d'une $\mathbb{Z}$-base $(e_1, \dots, e_n)$ de $\mathcal{O}_K$ et d'entiers $d_1|d_2|\cdots|d_n$ tels que $(d_1e_1, \dots, d_ne_n)$ est une base de I. On a alors

$$\Delta_{K/\mathbb{Q}}(\omega_1, \dots, \omega_n) = \Delta_{\mathcal{O}_K/\mathbb{Z}} \det(D)^2$$

où D est la matrice diagonale de diagonale $(d_1, d_2, \dots, d_n)$. Ainsi $\det(D) = \prod_{i=1}^n d_i$. Par ailleurs

$$\mathcal{O}_K/I \simeq \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_n\mathbb{Z}$$

donc $\det(D) = N(I)$. □

Vérifions maintenant que cette définition est compatible avec la définition de la norme d'un élément de $\mathcal{O}_K$.

Lemme. *Si $I = (a)$, $a \in \mathcal{O}_K$, est un idéal principal, alors $N(I) = |N_{K/\mathbb{Q}}(a)|$.*

Démonstration. Fixons $(\omega_1, \dots, \omega_n)$ une $\mathbb{Z}$-base de $\mathcal{O}_K$. C'est en particulier une base du $\mathbb{Q}$-espace vectoriel K. Soit M_a la matrice de l'endomorphisme m_a dans cette base. Remarquons que la famille $(a\omega_1, \dots, a\omega_n)$ est alors une $\mathbb{Z}$-base de $I = (a)$ et que M_a est la matrice de passage de la base $(\omega_1, \dots, \omega_n)$ à la base $(a\omega_1, \dots, a\omega_n)$. Attention M_a n'est pas une matrice diagonale si $a \notin \mathbb{Z}$! On en déduit une égalité de matrices

$$(\mathrm{Tr}(a\omega_i a\omega_j))_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant n}} = {}^tM_a(\mathrm{Tr}(\omega_i\omega_j))_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant n}} M_a.$$

Ainsi $\Delta_{K/\mathbb{Q}}(a\omega_1, \dots, a\omega_n) = (\det M_a)^2 \Delta_{\mathcal{O}_K/\mathbb{Z}}$ et donc, d'après le lemme précédent, $N(I)^2 = (\det M_a)^2 = N_{K/\mathbb{Q}}(a)^2$. On en déduit que $N(I) = |N_{K/\mathbb{Q}}(a)|$. □

On peut enfin prouver la propriété de multiplicativité de la norme.

Théorème 5.13. *Soient I et J deux idéaux de $\mathcal{O}_K$. On a alors $N(IJ) = N(I)N(J)$.*

Démonstration. Si l'un des deux idéaux est nul, l'égalité est évidente. On suppose donc $I \neq 0$ et $J \neq 0$. En utilisant le théorème 5.11, on voit qu'il suffit de prouver que $N(I\mathfrak{p}) = N(I)N(\mathfrak{p})$ pour tout idéal I non nul et tout idéal premier non nul $\mathfrak{p}$. Comme $I\mathfrak{p} \subset I \subset \mathcal{O}_K$ et que le groupe quotient $\mathcal{O}_K/I\mathfrak{p}$ est fini le groupe quotient $I/I\mathfrak{p}$ est fini. On a donc une égalité

$$N(I\mathfrak{p}) = \mathrm{Card}\, \mathcal{O}_K/I\mathfrak{p} = (\mathrm{Card}\, \mathcal{O}_K/I)(\mathrm{Card}\, I/I\mathfrak{p}).$$

Il faut donc prouver que $\mathrm{Card}\, I/I\mathfrak{p} = \mathrm{Card}\, \mathcal{O}_K/\mathfrak{p}$. Par unicité de la décomposition d'un idéal en produit d'idéaux premiers, on a $I\mathfrak{p} \subsetneq I$. On peut donc choisir, et fixer, un élément $a \in I \smallsetminus I\mathfrak{p}$. Considérons l'application suivante

$$\theta : \begin{array}{ccc} \mathcal{O}_K & \longrightarrow & I/I\mathfrak{p} \\ x & \longmapsto & ax + I\mathfrak{p} \end{array}.$$

Il s'agit d'un morphisme de $\mathcal{O}_K$-modules.

L'application θ est surjective. En effet son image est un sous-$\mathcal{O}_K$-module de $I/I\mathfrak{p}$. L'image réciproque J de ce sous-module par l'application quotient $I \to I/I\mathfrak{p}$ est donc un sous-$\mathcal{O}_K$-module de I, c'est-à-dire un idéal de $\mathcal{O}_K$ contenu I et contenant $I\mathfrak{p}$. On a donc une inclusion d'idéaux

$$I\mathfrak{p} \subset J \subset I.$$

Comme $a \notin I\mathfrak{p}$, on a $\theta(1) = a + I\mathfrak{p} \neq I\mathfrak{p}$ dans $I/I\mathfrak{p}$. Ainsi $I\mathfrak{p} \subsetneq J$. On en déduit que $\mathfrak{p} \subsetneq JI^{-1} \subset \mathcal{O}_K$. Comme $\mathfrak{p}$ est un idéal maximal de $\mathcal{O}_K$, on a $JI^{-1} = \mathcal{O}_K$ et donc $I = J$. Ceci prouve la surjectivité de θ.

Calculons $\operatorname{Ker}\theta$. Son noyau $\operatorname{Ker}\theta$ est un sous-$\mathcal{O}_K$-module de $\mathcal{O}_K$ c'est-à-dire un idéal de $\mathcal{O}_K$. De plus les éléments de $\mathfrak{p}$ sont dans le noyau de $\operatorname{Ker}\theta$. On a donc $\mathfrak{p} \subset \operatorname{Ker}\theta$. Comme de plus $\mathfrak{p}$ est un idéal maximal de $\mathcal{O}_K$, on a $\operatorname{Ker}\theta = \mathcal{O}_K$ ou $\operatorname{Ker}\theta = \mathfrak{p}$. Or on a vu plus haut que $1 \notin \operatorname{Ker}\theta$, donc $\operatorname{Ker}\theta = \mathfrak{p}$. Ainsi l'application θ induit un isomorphisme de $\mathcal{O}_K$-modules finis

$$\mathcal{O}_K/\mathfrak{p} \simeq I/I\mathfrak{p}.$$

On en conclut que $\operatorname{Card}\mathcal{O}_K/\mathfrak{p} = \operatorname{Card} I/I\mathfrak{p}$. □

Corollaire. *Soit I un idéal de $\mathcal{O}_K$ tel que $N(I)$ est premier. Alors l'idéal I est un idéal premier non nul de $\mathcal{O}_K$.*

Démonstration. Soit $I = I_1I_2$ une décomposition de I en produit de deux idéaux. Alors $N(I) = N(I_1)N(I_2)$ et $N(I)$ est un nombre premier. On a donc $N(I_1) = 1$ ou $N(I_2) = 1$, c'est-à-dire $I_1 = \mathcal{O}_K$ ou $I_2 = \mathcal{O}_K$. □

Corollaire. *Soient $I_1 \subset I_2$ deux idéaux de $\mathcal{O}_K$. On a $N(I_1) = N(I_2)$ si et seulement si $I_1 = I_2$.*

Démonstration. En effet, comme $I_1 \subset I_2$, on a $I_1 = I_2I_3$ où I_3 et un idéal de $\mathcal{O}_K$. Alors $N(I_1) = N(I_2)$ implique $N(I_3) = 1$ et donc $I_3 = \mathcal{O}_K$, d'où $I_1 = I_2$. □

Corollaire. *Soit $a \in \mathcal{O}_K$. Alors $a \in \mathcal{O}_K^\times$ si et seulement si $|N_{K/\mathbb{Q}}(a)| = 1$.*

Chapitre 6

Formes quadratiques binaires

6.1 Classes de formes quadratiques

6.1.1 Définition

Une *forme quadratique binaire* est un polynôme homogène de degré 2 à coefficients dans $\mathbb{Z}$: $q(X,Y) \in \mathbb{Z}[X,Y]$. On peut donc écrire de façon unique

$$q(X,Y) = aX^2 + bXY + cY^2, \quad (a,b,c) \in \mathbb{Z}^3.$$

On adoptera la notation $[a,b,c]$ pour désigner la forme ci-dessus.

Une forme quadratique binaire $[a,b,c]$ est dite *primitive* si $\mathrm{PGCD}(a,b,c) = 1$ ou encore si $[a,b,c]$ n'est pas de la forme nq pour un entier $n \geqslant 2$ et une forme quadratique binaire q.

Soit $n \in \mathbb{Z}$ un entier et soit q une forme quadratique binaire. On dit que la forme q *représente* n s'il existe $(x,y) \in \mathbb{Z}^2 \smallsetminus \{(0,0)\}$ tel que $q(x,y) = n$. On dit que q *représente primitivement* n si on peut choisit $(x,y) \in \mathbb{Z}^2$ tel que $q(x,y) = n$ et $\mathrm{PGCD}(x,y) = 1$.

Exemple. La forme $[1,0,5]$ ne représente pas 2 mais représente primitivement 6.

Le *discriminant* d'une forme quadratique $[a,b,c]$ est l'entier $\mathrm{Disc}(q) \coloneqq b^2 - 4ac$. Un entier ne peut être un discriminant que s'il est congru à 0 ou 1 modulo 4.

Théorème 6.1. *Soit $[a,b,c]$ une forme quadratique binaire de discriminant D. Alors pour que $[a,b,c]$ représente 0 il faut et il suffit que D soit un carré dans $\mathbb{Z}$ ou encore que $[a,b,c]$ soit le produit de deux formes linéaires. Si de plus $D \leqslant 0$, les entiers représentés par $[a,b,c]$ sont tous de même signe.*

Démonstration. Commençons par étudier le cas où $a = 0$. Dans ce cas la forme $q = [a,b,c]$ s'écrit $q(X,Y) = Y(bX + cY)$. Il est clair qu'elle représente 0 et que son discriminant $D = b^2$ est un carré. Enfin $D \leqslant 0$ si et seulement si $b = 0$ si et seulement si q est de signe constant sur $\mathbb{Z}^2$.

On peut donc supposer que $a \neq 0$. On peut alors écrire, pour $(x, y) \in \mathbb{Z}^2$,

$$q(x,y) = a\left(\left(x + \frac{b}{2a}y\right)^2 - \frac{b^2}{4a^2}y^2 + \frac{c}{a}y^2\right).$$

De sorte que

$$\forall (x,y) \in \mathbb{Z}^2, \quad 4aq(x,y) = (2ax + by)^2 - Dy^2. \tag{6.1}$$

On en déduit que si q représente 0, alors D est un carré dans $\mathbb{Q}$, donc est un carré dans $\mathbb{Z}$ puisque $D \in \mathbb{Z}$. Si tel est le cas posons $D = \delta^2$ avec $\delta \in \mathbb{Z}$. On peut donc écrire

$$4aq(x,y) = (2ax + (b-\delta)y)(2ax + (b+\delta)y)$$

Ainsi $4aq$ se factorise comme le produit de deux polynômes homogènes de degré 1 de $\mathbb{Z}[X, Y]$. De plus $4a$ divise $(b-\delta)(b+\delta) = 4ac$. Ainsi $b-\delta$ et $b+\delta$ sont tous deux pairs et on peut écrire $a = \alpha\beta$ avec $(\alpha, \beta) \in \mathbb{Z}^2$, $\alpha | b-\delta$ et $\beta | b+\delta$ de sorte que

$$q(X,Y) = \left(\frac{2a}{2\alpha} + \frac{b-\delta}{2\alpha}y\right)\left(\frac{2a}{2\beta}x + \frac{b+\delta}{2\beta}y\right).$$

Par ailleurs si q se factorise comme produit de deux polynômes homogènes de degré 1 de $\mathbb{Z}[X, Y]$, q représente 0 puisqu'un polynôme homogène de degré 1 de $\mathbb{Z}[X, Y]$ s'annule sur des éléments non nuls de $\mathbb{Z}^2$. Toutes les équivalences sont donc démontrées.

Il reste à vérifier que $D \leqslant 0$ si et seulement si les entiers représentés par $[a, b, c]$ sont tous de même signe. On peut encore supposer $a \neq 0$. Si $D \leqslant 0$, on déduit de l'égalité (6.1) que $aq(x, y) \geqslant 0$ pour tout $(x, y) \in \mathbb{Z}^2$. Ainsi le signe de $q(x, y)$ est constant lorsque (x, y) parcourt $\mathbb{Z}^2$. Si $D > 0$, il suffit d'observer que $4aq(1, 0) > 0$ et $4aq(-b, 2a) < 0$. □

Soit D le discriminant d'une forme quadratique binaire q. Supposons que $D < 0$. On dit que q est *définie positive* si elle prend des valeurs positives et *définie négative* dans le cas inverse.

6.1.2 Relation d'équivalence

Soit q une forme quadratique binaire. Soit u et v deux éléments de Z^2. L'application $(x, y) \mapsto q(xu + yv)$ est alors une autre forme quadratique binaire. Plus précisément si $u = \left(\begin{smallmatrix}\alpha\\ \gamma\end{smallmatrix}\right)$ et $v = \left(\begin{smallmatrix}\beta\\ \delta\end{smallmatrix}\right)$, alors

$$\forall (x,y) \in \mathbb{Z}^2, \quad q(xu + yv) = q(\alpha x + \beta y, \gamma x + \delta y).$$

Cette égalité peut encore se reformuler en utilisant la matrice P de la base (u, v) dans la base canonique de $\mathbb{Z}^2$. On a alors $P = \left(\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right)$ et $q(xu+yv) = q\left(P\left(\begin{smallmatrix}x\\ y\end{smallmatrix}\right)\right)$. On note $q \cdot P$ la forme quadratique binaire ainsi obtenue.

La *matrice* de la forme quadratique binaire $q = [a, b, c]$ est définie comme la matrice

$$\mathrm{Mat}(q) \coloneqq \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}$$

de sorte que

$$q(X, Y) = (X, Y)\,\mathrm{Mat}(q)\begin{pmatrix} X \\ Y \end{pmatrix}.$$

On en déduit la formule $\mathrm{Mat}(q \cdot P) = {}^tP\,\mathrm{Mat}(q)P$.

Remarquons que $\mathrm{Disc}(q) = -4 \det \mathrm{Mat}(q)$. On en déduit immédiatement la formule

$$\mathrm{Disc}(q \cdot P) = \det(P)^2\,\mathrm{Disc}(q).$$

On dit que deux formes quadratiques q et q' sont *équivalentes*, et on note $q \sim q'$, si il existe $P \in \mathrm{GL}_2(\mathbb{Z})$ tel que $q' = q \cdot P$. On dit que q et q' sont *proprement équivalentes*, et on note $q \overset{+}{\sim} q'$, si $q' = q \cdot P$ avec $P \in \mathrm{SL}_2(\mathbb{Z})$.

Remarquons que si $q \sim q'$, alors $\mathrm{Disc}(q) = \mathrm{Disc}(q')$.

La loi $(q, P) \mapsto q \cdot P$ définit une action (à droite) du groupe $\mathrm{GL}_2(\mathbb{Z})$ sur l'ensemble des formes quadratiques binaires. Deux formes sont équivalentes si et seulement si elles sont dans une même orbite pour cette action. On en déduit que la relation $\sim$ est une relation d'équivalence. De même deux formes sont proprement équivalentes si et seulement si elles sont dans une même orbite de $\mathrm{SL}_2(\mathbb{Z})$ pour cette action, ce qui prouve que $\overset{+}{\sim}$ est aussi une relation d'équivalence, plus fine que $\sim$.

Le principal intérêt de la notion de formes équivalentes est que deux formes équivalentes représentent les mêmes entiers. Ainsi, si on s'intéresse aux entiers représentés par une forme, on peut la remplacer par n'importe quel autre forme qui lui est équivalente.

En utilisant la matrice $P = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, on obtient

$$\forall (a, b, c) \in \mathbb{Z}^3, \quad [a, b, c] \sim [a, -b, c].$$

La proposition suivante montre comment certaines opérations élémentaires permettent de bouger dans une classe d'équivalence propre.

Proposition. *En utilisant les matrices* $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ *et* $\left(\begin{smallmatrix} 1 & -1 \\ 0 & 1 \end{smallmatrix}\right)$, *on obtient*

$$\begin{aligned} \forall (a, b, c) \in \mathbb{Z}^3, \quad [a, b, c] &\overset{+}{\sim} [c, -b, a] \\ &\overset{+}{\sim} [a, b + 2a, c + b + a] \\ &\overset{+}{\sim} [a, b - 2a, c - b + a]. \end{aligned} \tag{6.2}$$

Exemple. Par exemple, on peut facilement trouver une forme quadratique proprement équivalente à $q(X, Y) = 5X^2 + 6XY + 2Y^2$ au moyen de ces opérations élémentaires :

$$[5, 6, 2] \overset{+}{\sim} [2, -6, 5] \overset{+}{\sim} [2, -2, 1] \overset{+}{\sim} [1, 2, 2] \overset{+}{\sim} [1, 0, 1].$$

Remarque. Si $q \sim q'$, alors q est primitive si et seulement si q' est primitive. En effet, comme $\sim$ est une relation d'équivalence il suffit de montrer que si $P \in \mathrm{GL}_2(\mathbb{Z})$ et si $q \cdot P$ est primitive alors q est primitive. En effet si $q = nq''$ avec un entier $n \geqslant 2$ et q'' quadratique binaire, alors $q' = q \cdot P = n(q'' \cdot P)$.

Si $n \in \mathbb{Z}$ est représenté par une forme quadratique binaire q, on recherche désormais des formes proprement équivalentes à q d'une forme particulièrement simple.

Théorème 6.2. *Soit $n \in \mathbb{Z} \smallsetminus \{0\}$. Alors n est primitivement représenté par une forme quadratique binaire q si et seulement si q est proprement équivalente à une forme $[n, b, c]$ avec $-|n| < b \leqslant |n|$.*

Démonstration. Si $q = [n, b, c]$, alors $q(1, 0) = n$. Ainsi n est primitivement représenté par q et par toute forme qui lui est proprement équivalente.

Réciproquement supposons qu'il existe q et $(x, y) \in \mathbb{Z}^2$ tels que $x \wedge y = 1$ et $q(x, y) = n$. D'après le théorème de Bezout, il existe $(v, w) \in \mathbb{Z}^2$ tel que $xw - yv = 1$. Posons $P = \left(\begin{smallmatrix} x & v \\ y & w \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. On a alors $q \cdot P = [n, b', c']$ avec $b', c' \in \mathbb{Z}$ puisque $q \cdot P(1, 0) = n$. Effectuons la division euclidienne de b' par $2|n|$. On a alors $b' = b + k|n|$ avec $-|n| < b \leqslant |n|$. En appliquant successivement les relations élémentaires (6.2), on obtient $[n, b', c'] \overset{+}{\sim} [n, b, c]$ pour un certain entier $c \in \mathbb{Z}$. □

Corollaire. *Soit p un nombre premier et soit $D \in \mathbb{Z}$. Alors p est représenté par au plus une classe d'équivalence de discriminant D.*

Démonstration. L'entier p est premier, donc si $p = q(x, y)$ avec $(x, y) \in \mathbb{Z}^2$, on a nécessairement $x \wedge y = 1$. Si p est représenté par deux formes q et q', on déduit du théorème 6.2 qu'il existe des entiers b, b', c, c' avec $-p < b, b' \leqslant p$ tels que $q \overset{+}{\sim} [p, b, c]$ et $q' \overset{+}{\sim} [p, b', c']$. En utilisant les relations (6.2), on voit que, quitte à remplacer $\overset{+}{\sim}$ par $\sim$, on peut même supposer $0 \leqslant b, b' \leqslant p$. On a de plus $b^2 - 4pc = D = (b')^2 - 4pc'$. On en déduit que $b^2 \equiv (b')^2 \,[4p]$ et donc que $b \equiv \pm b' \,[p]$. Comme $0 \leqslant b, b' \leqslant p$, on a $b = b'$ ou $b' = p - b$. Ce dernier cas est exclus si p est impair car b et b' doivent avoir la même parité. Si $p = 2$, on a également $b' \neq 2 - b$ car les carrés de 0, 1 et 2 sont distincts modulo $8 = 4p$. Ainsi $b = b'$ et $c = c'$ puisque $b^2 - 4c = (b')^2 - 4c'$. On en déduit que $q \sim q'$. □

6.1.3 Classes d'équivalence

Théorème 6.3. *Soit $D \in \mathbb{Z}$ un entier qui n'est pas un carré. Il n'existe qu'un nombre fini de classes d'équivalence propre (et donc de classe d'équivalence) de discriminant D.*

Pour démontrer ce théorème, nous allons utiliser un procédé de réduction appelé réduction de Lagrange. C'est l'objet du lemme suivant.

Lemme. *Soit $D \in \mathbb{Z}$ un entier qui n'est pas un carré. Toute forme quadratique binaire de discriminant D est proprement équivalente à une forme $[a,b,c]$ avec $-|a| < b \leqslant |a| \leqslant |c|$. On a alors $1 \leqslant |a| \leqslant \sqrt{\frac{|D|}{3}}$.*

Démonstration. Soit q une forme quadratique binaire de discriminant D. Choisissons $(x,y) \in \mathbb{Z}^2$ tel que

$$|q(x,y)| = \min\{|q(x',y')| \ \mid (x',y') \in \mathbb{Z}^2 \smallsetminus \{(0,0)\}\}.$$

Posons $a = q(x,y)$. Remarquons dans un premier temps que $x \wedge y = 1$. En effet si $d = x \wedge y > 1$, on peut écrire $x = dx'$, $y = dy'$ et $|q(x,y)| = d|q(x',y')| > |q(x',y')|$, ce qui est absurde. Le théorème 6.2 montre alors que q est proprement équivalente à une forme $[a,b,c]$ avec $-|a| < b \leqslant |a|$. Comme D n'est pas un carré, on doit avoir $c \neq 0$. Comme c est représenté par $[a,b,c]$, on a donc $|a| \leqslant |c|$ par définition de (x,y).

La dernière inégalité se prouve en remarquant que

$$4|a|^2 \leqslant 4|a||c| = |b^2 - D| \leqslant |b|^2 + |D| \leqslant |a|^2 + |D|.$$

Ainsi $|a| \leqslant \sqrt{\frac{|D|}{3}}$. □

On peut à présent prouver le théorème 6.3.

Démonstration du théorème 6.3. D'après le lemme, toute classe d'équivalence propre de discriminant D contient une forme $[a,b,c]$ telle que $|b| \leqslant |a| \leqslant |c|$ et $|a| \leqslant \sqrt{\frac{|D|}{3}}$. Il y a donc un nombre fini de possibilités pour a, b et c donc un nombre fini de classes d'équivalence propre. □

Soit $D \in \mathbb{Z}$ un entier non carré. On note $\mathrm{Cl}(D)$ l'ensemble des classes d'équivalence propre de formes quadratiques binaires de discriminant D et $\mathcal{P}(D) \subset \mathrm{Cl}(D)$ l'ensemble des classes d'équivalence propre de discriminant D qui sont primitives.

Théorème 6.4. *Soit D un entier non carré. Alors*

$$\mathrm{Card}\ \mathrm{Cl}(D) = \sum_{\substack{g \geqslant 1 \\ g^2 | D}} \mathrm{Card}\, \mathcal{P}\left(\frac{D}{g^2}\right).$$

Démonstration. Supposons que $[a,b,c] \overset{+}{\sim} [a',b',c']$. On a alors $\mathrm{PGCD}(a,b,c) = \mathrm{PGCD}(a',b',c')$. En effet, si $q = [a,b,c]$ et $d = \mathrm{PGCD}(a,b,c)$, alors d est le plus grand entier n tel que $q = nq'$ pour une forme quadratique binaire q'.

On peut donc partitioner l'ensemble $\mathrm{Cl}(D)$ en parties constituées de classes ayant le même pgcd. Remarquons par ailleurs que si $\mathrm{PGCD}(a,b,c) = g$, alors $[a,b,c] = gq$ pour

une forme quadratique binaire primitive q. Dans ce cas le discriminant de q est $\frac{D}{g^2}$. On en déduit une bijection

$$\mathcal{P}\left(\frac{D}{g^2}\right) \simeq \{\overline{[a,b,c]} \in \mathrm{Cl}(D) \mid \mathrm{PGCD}(a,b,c) = g\}$$

donnée par $q \mapsto gq$. □

6.1.4 Nombre de classes d'équivalence dans le cas défini

On fixe désormais un entier D qui n'est pas un carré et tel que $D < 0$. On note $\mathrm{Cl}_+(D) \subset \mathrm{Cl}(D)$ (resp. $\mathcal{P}_+(D) \subset \mathcal{P}(D)$) l'ensemble des classes d'équivalence propre (resp. primitives) qui sont de plus définies positives. On pose alors

$$h(D) \coloneqq \mathrm{Card}\, \mathcal{P}_+(D).$$

Remarquons qu'une forme quadratique binaire$[a,b,c]$ de discriminant $D < 0$ est définie positive si et seulement si $a > 0$.

On peut déterminer l'entier $h(D)$ en dénombrant les formes quadratiques binaire dites *réduites*. Une forme quadratique binaire $[a,b,c]$ de discriminant D est dite *réduite* si

$$-a < b \leqslant a \leqslant c \quad \text{et si } b \geqslant 0 \text{ lorsque } a = c.$$

Théorème 6.5. *Toute forme quadratique binaire définie positive de discriminant D est proprement équivalente à une unique forme réduite.*

L'entier $h(D)$ est donc égal au nombre de formes quadratiques primitives réduites définies positives de discriminant D.

Démonstration. Montrons dans un premier temps l'existence d'une telle forme. D'après le théorème 6.2, une forme quadratique binaire q de discriminant D est proprement équivalente à une forme $[a,b,c]$ avec $-|a| < b \leqslant |a| \leqslant |c|$. Comme q est définie positive, on a nécessairement $a > 0$ et $c > 0$. Si $a < c$, $[a,b,c]$ est réduite. Sinon, $a = c$ et $[a,b,c] \overset{+}{\sim} [a,-b,a]$, donc on peut supposer $b \geqslant 0$, c'est-à-dire $[a,b,a]$ réduite.

Montrons à présent l'unicité. Nous allons utilise le lemme suivant.

Lemme. *Soit $q = [a,b,c]$ une forme réduite de discriminant D avec $D < 0$. Alors a est le plus petit entier naturel non nul représenté par q. De plus si $a < c$, c est le plus petit entier non nul représenté primitivement par q et différent de a. L'équation $a = q(x,y)$ a exactement deux solutions si et seulement si $a < c$. Enfin, si $a < c$, l'équation $c = q(x,y)$ a exactement deux solutions primitives, sauf si $b = a$.*

Démonstration. Rappelons l'égalité (6.1)

$$4aq(x,y) = (2ax + by)^2 - Dy^2.$$

Si $|y| \geqslant 2$, on en déduit $aq(x,y) \geqslant -D = 4ac - b^2$. Comme $b^2 \leqslant a^2 \leqslant ac$, on a $4ac - b^2 \geqslant 3ac$ et donc $q(x,y) \geqslant 3c > c$ puisque $c > 0$. On en déduit que si $q(x,y) = a$ ou $q(x,y) = c$, on a nécessairement $|y| \leqslant 1$.

Si $y = 0$, on a $q(x,0) = ax^2$.

Par ailleurs $q(x,-1) = q(-x,1)$, il suffit donc d'étudier le cas $y = 1$. De plus $|2ax + b| \geqslant |b|$ avec égalité si $x = 0$ ou $b = a$ et $x = -1$. Ainsi

$$\forall x \in \mathbb{Z}, \quad q(x,1) \geqslant \frac{b^2 - D}{4a} = c$$

avec égalité si et seulement si $x = 0$ ou $b = a$ et $x = -1$.

Pour conclure :

— a est bien le plus entier non nul représenté par q. Si $c > a$, $(\pm 1, 0)$ sont les seules solutions de l'équation $a = q(x,y)$;

— les seuls entiers entiers $a < m < c$ représentés par q sont de la forme $n^2 a$ et les seules solutions de $n^2 a = q(x,y)$ sont alors $(\pm n, 0)$. Ces entiers m ne sont donc pas représentés primitivement par q. Ainsi, si $c > a$ l'entier c est le plus petit entier $> a$ représenté primitivement par q.

— Si $q(x,y) = c$, avec $y \neq 0$, on a $y = \pm 1$. Si $c > a$, l'équation a exactement deux solutions $(0, \pm 1)$, sauf si $b = a$. □

On peut achever la preuve du théorème. Supposons que $[a,b,c] \overset{+}{\sim} [a',b',c']$ sont deux formes réduites proprement équivalentes de discriminant D. Le lemme donne une caractérisation de a qui est indépendante de la forme choisie dans une classe d'équivalence propre. On en déduit que $a = a'$. Comme $c = a$ si et seulement si $a = q(x,y)$ a strictement plus de deux solutions, on en conclut que

$$a < c \Leftrightarrow a' < c'.$$

De plus, si $a < c$, le lemme nous donne une caractérisation de c en terme des entiers représentés primitivement par $[a,b,c]$. On en conclut que $c = c'$. On a donc

$$b^2 - 4ac = D = (b')^2 - 4a'c'$$

donc $b' = \pm b$.

Si $a = c$, et donc $a' = c'$, on doit avoir $b \geqslant 0$ et $b' \geqslant 0$, donc $b = b'$. Supposons donc $a < c$ (et donc $a' < c'$).

Posons $q = [a,b,c]$ et $q' = [a',b',c']$. Le lemme implique que $b = a$ si et seulement si l'équation $c = q(x,y)$ strictement plus de deux solutions primitives. Donc $b = a$ si et seulement si l'équation $c' = q'(x,y)$ strictement plus de deux solutions primitives. Ainsi $b = a$ si et seulement si $b' = a'$. Si $b = a$, on a donc $b = a = a' = b'$. On peut donc supposer que $b \neq a$, et donc que $b' \neq a'$.

On a alors $q' = q \cdot P$ pour une matrice $P \in \mathrm{SL}_2(\mathbb{Z})$ et on peut écrire $q'(x,y) = q(xu+yv)$ où u et v sont les deux vecteurs colonnes de P. Or $q(u) = a' = a$. Donc d'après le lemme, $u = \pm \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$. De même $q(v) = c' = c$ donc $v = \pm \left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right)$. Ainsi $P = \left(\begin{smallmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{smallmatrix}\right)$. Mais comme de plus $\det P = 1$, on a $P = \pm I_2$ et donc $q = q'$. Ceci achève la preuve de l'unicité. □

Exemple. Utilisons ce résultat pour calculer $h(-20)$. Il s'agit de faire la liste des formes quadratiques $q = [a,b,c]$, primitives et réduites, telles que $b^2 - 4ac = -20$. On sait que, d'après le lemme de la partie 6.1.3,

$$|a| \leqslant \sqrt{\frac{-D}{3}} < 3.$$

Ainsi $a \in \{1,2\}$. De plus $b^2 - 4ac = -20$ donc b est pair.

— Si $a = 1$, on a $b \in \{0,1\}$. Comme b est pair $b = 0$ et $c = 5$.

— Si $a = 2$, on a $b \in \{-1,0,1,2\}$. Comme b est pair, $b \in \{0,2\}$. On a donc $b = 0$ et $-8c = -20$ qui n'a pas de solution ou $b = 2$ et $4 - 8c = -20$ c'est-à-dire $c = 3$. Les deux formes $[1,0,5]$ et $[2,2,3]$ sont réduites et primitives, on a donc $h(-20) = 2$.

On montre de même que $h(-4) = h(-3) = 1$ (exercice).

6.2 Formule du nombre de classes

6.2.1 Le symbole de Kronecker

Soit $D < 0$ un entier tel que D est congru à 0 ou 1 modulo 4. Nous allons définir un caractère de Dirichlet qui étend le symbole de Legendre au cas où le dénominateur peut être pair.

Théorème 6.6. *Il existe un unique caractère de Dirichlet χ_D d'ordre 2 modulo $|D|$ vérifiant la propriété suivante : si p est premier et si $p \nmid D$, alors $\chi_D(p) = 1$ si et seulement si D est un carré modulo $4p$. On a de plus $\chi_D(-1) = -1$.*

Démonstration. Commençons par prouver l'unicité. Comme χ_D est un caractère de Dirichlet modulo $|D|$, il est déterminé par ses valeurs sur les nombres premiers p ne divisant pas D. L'unicité en découle facilement.

Prouvons donc l'existence de χ_D. Commençons par le cas où D est pair. Alors $D = -2^e D'$ avec $e \geqslant 2$ et $D' \geqslant 1$ impair. Pour $n \geqslant 1$ premier à D, donc impair, posons

$$\chi_D(n) \coloneqq \left(\frac{D}{n}\right)$$

le symbole de Jacobi modulo n. Si $p \nmid D$, on a $\chi_D(p) = \left(\frac{D}{p}\right)$. Ainsi

$$\chi_D(p) = 1 \Leftrightarrow D \text{ est un carré modulo } p \Leftrightarrow D \text{ est un carré modulo } 4p$$

en conséquence du théorème des restes et du fait que $p \neq 2$. Vérifions que l'on a défini une fonction $|D|$-périodique sur les nombres premiers à D. La loi de réciprocité quadratique pour le symbole de Jacobi nous donne en effet (puisque n est impair si n est premier à D) :

$$\begin{aligned}\chi_D(n) &= \left(\frac{-1}{n}\right)\left(\frac{2}{n}\right)^e\left(\frac{D'}{n}\right)\\ &= (-1)^{\frac{n-1}{2}}(-1)^{e\frac{n^2-1}{8}}(-1)^{\frac{n-1}{2}\frac{D'-1}{2}}\left(\frac{n}{D'}\right).\end{aligned}$$

Les trois premiers termes sont 8-périodiques et le dernier est D'-périodique. La fonction χ_D et donc $8D'$-périodique sur l'ensemble des entiers $n \geqslant 1$ premiers à D. Remarquons que dans le cas particulier où $e = 2$, on a

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

Comme les deux premiers termes sont 4-périodiques, la fonction χ_D est cette fois-ci $4D'$-périodique. Ainsi, quelque soit la valeur de $e \geqslant 2$, la fonction χ_D est $2^eD' = |D|$-périodique sur l'ensemble $\mathbb{N}^*$. Elle se prolonge donc de façon unique en un caractère de Dirichlet modulo $|D|$. De plus

$$\chi_D(-1) = -(-1)^{-\frac{D'-1}{2}}\left(\frac{-1}{D'}\right) = -(-1)^{\frac{D'-1}{2}}\left(\frac{-1}{D'}\right) = -1.$$

Considérons maintenant le cas où D est impair. Posons, pour $n \in \mathbb{Z}$,

$$\chi_D(n) = \left(\frac{n}{|D|}\right).$$

Il s'agit, clairement cette fois, d'une fonction $|D|$-périodique. Vérifions qu'elle a les propriétés voulues. Si $p \nmid D$ est premier et impair, on a, en utilisant le fait que $|D| = -D \equiv 3\,[4]$,

$$\chi_D(p) = \left(\frac{p}{|D|}\right) = \left(\frac{-1}{p}\right)\left(\frac{|D|}{p}\right) = \left(\frac{D}{p}\right).$$

Donc $\chi_D(p) = 1$ si et seulement si D est un carré modulo p, c'est-à-dire si et seulement si D est un carré modulo $4p$.

De plus, on a $\chi_D(2) = 1$ si et seulement si $|D|$ est congru à 1 ou -1 modulo 8. Comme on sait de plus que $|D| \equiv 3\,[4]$, on a $\chi_D(2) = 1$ si et seulement si $|D| \equiv -1\,[8]$, c'est-à-dire $D \equiv 1\,[8]$. Donc $\chi_D(2) = 1$ si et seulement si D est un carré modulo 8 (toujours en utilisant que $D \equiv 1\,[4]$). De plus

$$\chi_D(-1) = \left(\frac{-1}{|D|}\right) = (-1)^{\frac{|D|-1}{2}} = -1. \qquad \square$$

Le caractère χ_D s'appelle le *symbole de Kronecker* modulo D.

Remarque. Au cours de la preuve du théorème 6.6, on a vu la formule suivante pour le symbole de Kronecker : pour $n \geqslant 1$ et $\mathrm{PGCD}(n, D) = 1$,

$$\chi_D(n) = \begin{cases} (\frac{D}{n}) & \text{si } 2 \mid D; \\ (\frac{n}{|D|}) & \text{si } 2 \nmid D. \end{cases}$$

Si $k \in \mathbb{N}^*$ et si q est une forme quadratique binaire, on pose

$$\Psi(k, q) = \mathrm{Card}\{(x, y) \in \mathbb{Z}^2 \mid q(x, y) = k\}.$$

Soient $q_1, \ldots, q_{h(D)}$ une famille de formes quadratiques binaires représentant les classes d'équivalence propre primitives de discriminant D. Posons alors

$$\Psi(k) \coloneqq \sum_{i=1}^{h(D)} \Psi(k, q_i).$$

Le reste de cette partie sera consacré à la démonstration du résultat suivant :

Théorème 6.7. *Soit $D < 0$ un entier congru à 0 ou 1 modulo 4. Soit $k \in \mathbb{N}^*$ tel que $\mathrm{PGCD}(k, D) = 1$. On a alors*

$$\Psi(k) = w \sum_{\substack{n \geqslant 1 \\ n \mid k}} \chi_D(n)$$

avec

$$w = \begin{cases} 6 & \textit{si } D = -3 \\ 4 & \textit{si } D = -4 \\ 2 & \textit{sinon.} \end{cases}$$

Exemple. On a $h(-3) = 1$. Soit p un nombre premier différent de 3. On a alors $\Psi(p) = 6(1 + \chi_{-3}(p))$. Comme $\chi_{-3}(p) = (\frac{p}{3})$, on en conclut que si q est une forme quadratique binaire primitive de discriminant -3, l'équation $q(x, y) = p$ a des solutions si et seulement si $p \equiv 1\,[3]$. Si elle a des solutions, elle en a exactement 12. Nous avions déjà vu un cas particulier de ce résultat lorsque $q(X, Y) = X^2 - XY + Y^2$.

On a $h(-20) = 2$. Soit p un nombre premier différent de 2 et 5. On a alors $\Psi(p) = 2(1 + \chi_{-20}(p))$. On a $\chi_{-20}(p) = (\frac{-5}{p}) = (-1)^{\frac{p-1}{2}}(\frac{p}{5})$. Par exemple 13 n'est pas représenté par une forme quadratique binaire de discriminant -20. Par contre 7 est représenté par une telle forme. Cependant comme il y a deux classes, on en conclut que 7 est représenté soit par $[1, 0, 5]$ soit par $[2, 2, 3]$.

6.2.2 Stabilisateur d'une forme quadratique

Soit q une forme quadratique binaire. On note Γ_q le sous-groupe de $\mathrm{SL}_2(\mathbb{Z})$ défini par

$$\Gamma_q \coloneqq \{P \in \mathrm{SL}_2(\mathbb{Z}) \mid q \cdot P = q\}.$$

Théorème 6.8. *Soit q une forme quadratique binaire primitive de discriminant $D < 0$. On a $\Gamma_q = \{\pm I_2\}$ si $D \notin \{-4, -3\}$. Si $D = -4$, on a $\Gamma_q \simeq \mathbb{Z}/4\mathbb{Z}$ et si $D = -3$, $\Gamma_q \simeq \mathbb{Z}/6\mathbb{Z}$.*

Démonstration. Si $q \overset{+}{\sim} q'$, on a $q' = q \cdot P$ pour une matrice $P \in \mathrm{SL}_2(\mathbb{Z})$ et on vérifie que $\Gamma_{q'} = P^{-1}\Gamma_q P$. Le théorème 6.5 montre donc qu'il suffit de traiter le cas d'une forme q qui est réduite. On suppose donc que $q = [a, b, c]$ est réduite. Soit (e_1, e_2) la base canonique de $\mathbb{Z}^2$. On a donc $q(e_1) = a$. Si $\theta \in \Gamma_q$, on a $q(\theta(e_1)) = a$. Ainsi si $a < c$, on doit avoir $\theta(e_1) = \pm e_1$. Ceci implique que θ est une matrice de la forme $\pm \left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right)$ pour un entier $h \in \mathbb{Z}$. On sait de plus que ${}^t\theta \,\mathrm{Mat}(q)\theta = \mathrm{Mat}(q)$. Un simple calcul donne donc

$$\begin{pmatrix} a & \frac{b+2ah}{2} \\ \frac{b+2ah}{2} & c + bh + h^2 \end{pmatrix} = \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}.$$

Ainsi on doit avoir $ah = 0$, donc $h = 0$. Finalement $\theta = \pm I_2$.

Il reste donc à traiter le cas où $a = c$ et $b \geqslant 0$. Si $a = c = b$, comme q est supposée primitive, on a $q = [1, 1, 1]$ et donc $D = -3$. Un calcul direct montre que

$$\Gamma_q = \left\{ \pm I_2, \pm \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \pm \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix} \right\}$$

et que ce groupe est cyclique d'ordre 6. On peut donc supposer que $0 \leqslant b < a = c$. Rappelons que $q(x, y) = a$ si et seulement si $y = 0$ et $x = \pm 1$ ou $y = \pm 1$ et $x = 0$. Ainsi $\theta(e_1) = \pm e_1$ et $\theta = \pm I_2$ ou $\theta(e_1) = \pm e_2$. De même $\theta(e_2) \in\in \{\pm e_1, \pm e_2\}$. Comme θ est inversible et de déterminant 1, θ échange les sous-groupes $\mathbb{Z}e_1$ et $\mathbb{Z}e_2$, donc

$$\theta \in \left\{ \pm I_2, \pm \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\}$$

et on en conclut que Γ_q est un sous-groupe d'un groupe cyclique d'ordre 4 contenant $\{\pm I_1\}$. Donc Γ_q est réduit à $\{\pm I_2\}$ ou cyclique d'ordre 4. Supposons Γ_q cyclique d'ordre 4. Alors Γ_q contient la matrice $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ et la relation

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & a \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & a \end{pmatrix}$$

implique $b = -b$ donc $b = 0$. Comme q est primitive, on a $q = [1, 0, 1]$ et $D = -4$. Réciproquement, on vérifie que les seules formes quadratiques primitives réduites de discriminant -3 et -4 sont respectivement $[1, 1, 1]$ et $[1, 0, 1]$ qui ont des groupes d'automorphismes cycliques d'ordres 6 et 4. □

6.2.3 Démonstration du théorème 6.7

On fixe désormais un entier $D < 0$ congru à 0 ou 1 modulo 4.

Soit q une forme quadratique binaire définie positive. On peut définir un produit scalaire sur $\mathbb{R}^2$ en posant

$$\langle x, y\rangle_q \coloneqq q(x+y) - q(x) - q(y).$$

Ce produit scalaire prend des valeurs entières sur $\mathbb{Z}^2$ et $\langle x, x\rangle_q = 2q(x)$ pour tout $x \in \mathbb{Z}^2$.

Soit (x, y) une solution primitive de l'équation $q(x, y) = k$. Il existe alors un couple $(r, s) \in \mathbb{Z}^2$ tel que $xs - yr = 1$. On pose alors

$$\nu_q(x, y) = \left\langle \begin{pmatrix} x \\ y \end{pmatrix}, \begin{pmatrix} r \\ s \end{pmatrix} \right\rangle_q [2k].$$

La classe $\nu_q(x, y) \in \mathbb{Z}/2k\mathbb{Z}$ ne dépend pas du choix de (r, s). En effet si (r', s') est un autre choix, il existe $m \in \mathbb{Z}$ tel que $(r', s') = (r, s) + m(x, y)$. On a alors

$$\left\langle \begin{pmatrix} x \\ y \end{pmatrix}, \begin{pmatrix} r' \\ s' \end{pmatrix} \right\rangle_q = \left\langle \begin{pmatrix} x \\ y \end{pmatrix}, \begin{pmatrix} r \\ s \end{pmatrix} \right\rangle_q + 2mq(x, y) \equiv \left\langle \begin{pmatrix} x \\ y \end{pmatrix}, \begin{pmatrix} r \\ s \end{pmatrix} \right\rangle_q [2k].$$

Lemme. *Soient q et q' deux formes de discriminant D. Soient (x, y) et (x', y') des éléments de $\mathbb{Z}$ tels que $\mathrm{PGCD}(x, y) = \mathrm{PGCD}(x', y') = 1$ et $q(x, y) = k = q'(x', y')$. Supposons que $\nu_q(x, y) = \nu_{q'}(x', y')$. Alors il existe une matrice $P \in \mathrm{SL}_2(\mathbb{Z})$ telle que $\left(\begin{smallmatrix} x' \\ y' \end{smallmatrix}\right) = P \left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right)$ et $q' \cdot P = q$. En particulier $q \overset{+}{\sim} q'$.*

Démonstration. Choisissons donc des couples (r, s) et (r', s') de $\mathbb{Z}^2$ tels que $xs - yr = x's' - y'r' = 1$. Quitte à modifier (r, s) par un multiple de (x, y), on peut même supposer que

$$\left\langle \begin{pmatrix} x \\ y \end{pmatrix}, \begin{pmatrix} r \\ s \end{pmatrix} \right\rangle_q = \left\langle \begin{pmatrix} x' \\ y' \end{pmatrix}, \begin{pmatrix} r' \\ s' \end{pmatrix} \right\rangle_{q'}.$$

Posons alors la matrice

$$P = \begin{pmatrix} x' & r' \\ y' & s' \end{pmatrix} \begin{pmatrix} x & r \\ y & s \end{pmatrix}^{-1} \in \mathrm{SL}_2(\mathbb{Z}).$$

On a alors

$$P \begin{pmatrix} x & r \\ y & s \end{pmatrix} = \begin{pmatrix} x' & r' \\ y' & s' \end{pmatrix}.$$

Mais alors $q' \cdot P(x, y) = q'(x', y') = k = q(x, y)$. De même

$$\left\langle \begin{pmatrix} x \\ y \end{pmatrix}, \begin{pmatrix} r \\ s \end{pmatrix} \right\rangle_{q' \cdot P} = \left\langle \begin{pmatrix} x' \\ y' \end{pmatrix}, \begin{pmatrix} r' \\ s' \end{pmatrix} \right\rangle_{q'} = \left\langle \begin{pmatrix} x \\ y \end{pmatrix}, \begin{pmatrix} r \\ s \end{pmatrix} \right\rangle_q$$

et

$$D = \left\langle \begin{pmatrix} x \\ y \end{pmatrix}, \begin{pmatrix} r \\ s \end{pmatrix} \right\rangle_q^2 - 4q \begin{pmatrix} x \\ y \end{pmatrix} q \begin{pmatrix} r \\ s \end{pmatrix} = \left\langle \begin{pmatrix} x' \\ y' \end{pmatrix}, \begin{pmatrix} r' \\ s' \end{pmatrix} \right\rangle_{q'}^2 - 4q' \begin{pmatrix} x' \\ y' \end{pmatrix} q' \begin{pmatrix} r' \\ s' \end{pmatrix}$$

montre que $q\binom{r}{s} = q'\binom{r'}{s'}$. Ainsi $\langle\cdot,\cdot\rangle_q$ et $\langle\cdot,\cdot\rangle_{q'\cdot P}$ sont deux produits scalaires qui coïncident sur une base de $\mathbb{Z}^2$, ils sont donc égaux et on en conclut que $q' \cdot P = q$, et donc que $q' \overset{+}{\sim} q$. □

Lemme. *Soit q une forme primitive de discriminant D. Posons $w = \operatorname{Card}\Gamma_q$. Soit $(x_0, y_0) \in \mathbb{Z}^2$ tel que $q(x_0, y_0) = k$. Alors l'équation $q(x, y) = k$ a exactement w solutions primitives (x, y) vérifiant $\nu_q(x, y) = \nu_q(x_0, y_0)$.*

Démonstration. Soit (x_1, y_1) une autre solution primitive de l'équation $q(x, y) = k$. D'après le lemme 6.2.3, il existe $P \in \mathrm{SL}_2(\mathbb{Z})$ telle que $\binom{x_1}{y_1} = P\binom{x_0}{y_0}$ et telle que $q \cdot P = q$. On a donc $P \in \Gamma_q$. Comme toute matrice de Γ_q est conjuguée à une matrice de rotation, les éléments de Γ_q n'ont pas de point fixe non nul dans $\mathbb{Z}^2$. Ainsi les orbites de Γ_q dans $\mathbb{Z}^2$ ne contenant pas $(0, 0)$ sont de cardinal w. Comme l'ensemble des solutions primitives de $q(x, y) = k$ est une telle orbite, on en déduit le résultat. □

Remarquons que si deux entiers n_1 et n_2 sont congrus modulo $2k$, alors leurs carrés sont congrus modulo $4k$. En effet si $2k|n_1 - n_2$, alors n_1 et n_2 ont la même parité, donc $2|n_1 + n_2$ et $4k|n_1^2 - n_2^2$. L'application $n \mapsto n^2$ se factorise donc en une application $\mathbb{Z}/2k\mathbb{Z} \to \mathbb{Z}/4k\mathbb{Z}$.

Lemme. *Soit $k \geqslant 1$ un entier premier à D. Soit $\nu \in \mathbb{Z}/2k\mathbb{Z}$. Il existe une forme quadratique binaire primitive q de discriminant D et une solution primitive (x, y) à l'équation $q(x, y) = k$ vérifiant $\nu_q(x, y) = \nu$ si et seulement si*

$$\nu^2 \equiv D\,[4k].$$

Ce lemme implique en particulier qu'un entier k premier à D est représenté primitivement par une forme quadratique primitive de discriminant D si et seulement si D est un carré modulo $4k$.

Démonstration. Commençons par vérifier que la condition est nécessaire. Supposons que $k = q(x, y)$ avec $\mathrm{PGCD}(x, y) = 1$. Soient $u = \binom{x}{y}$ et $v = \binom{r}{s}$ tels que $xs - yr = 1$, c'est-à-dire $\det(u, v) = 1$. En écrivant la matrice de q dans la base (u, v), on voit que

$$D = \langle u, v\rangle_q^2 - 4q(u)q(v) = \langle u, v\rangle_q^2 - 4kq(v)$$

donc $\nu_q(x, y)^2 = D$ dans $\mathbb{Z}/4k\mathbb{Z}$.

Il s'agit également d'une condition suffisante. Supposons que $\nu^2 \equiv D\,[4k]$. On peut donc écrire $D = \nu^2 - 4kc$ pour un certain $c \in \mathbb{Z}$. La forme $q = [k, \nu, c]$ est alors de discriminant D. Elle représente primitivement k et, comme $\mathrm{PGCD}(k, D) = 1$, on a $\mathrm{PGCD}(k, \nu) = 1$, donc $[k, \nu, c]$ est primitve. □

Lemme. *Soit $k \geqslant 1$ un entier premier à D. Le nombre de solutions dans $\mathbb{Z}/2k\mathbb{Z}$ à la congruence*

$$x^2 \equiv D\,[4k]$$

vaut $\sum_{\substack{m\geqslant 1\\ m|k}} \chi_D(m)\mu(m)^2$.

Démonstration. Posons $k = 2^e \prod_{i=1}^r p_i^{e_i}$ où les p_i sont des nombres premiers impairs deux à deux distincts. Comme $\mathrm{PGCD}(k, D) = 1$, on a $p_i \nmid D$. Le théorème des restes nous donne

$$x^2 \equiv D\,[4k] \Leftrightarrow \begin{cases} x^2 \equiv D\,[2^{e+2}] \\ \forall i = 1, \ldots, r,\ x^2 \equiv D\,[p_i^{e_i}]. \end{cases}$$

Comme p_i est un impair, on a un isomorphisme de groupes

$$\begin{array}{ccc} (\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times & \xrightarrow{\sim} & (\mathbb{Z}/p_i\mathbb{Z})^\times \times \mathbb{Z}/p_i^{e_i-1}\mathbb{Z} \\ x & \longmapsto & (x_1, x_2) \end{array},$$

où $x \mapsto x_1$ est la réduction modulo p_i. Soit (D_1, D_2) l'image de $D\,[p_i^{e_i}]$ par cet isomorphisme. Comme $p_i^{e_i-1}$ est impair, on voit que le nombre de solutions à l'équation $x^2 = (D\,[p_i^{e_i}])$ est égal au nombre de solutions à l'équation $x^2 = D_1$ dans $(\mathbb{Z}/p_i\mathbb{Z})^\times$. Comme D_1 est la réduction de D modulo p_i, il suffit donc de considérer le cas où $e_i = 1$. Comme $\mathbb{Z}/p_i\mathbb{Z}$ est un corps de caractéristique première à 2, le cardinal de cet ensemble vaut 2 si D est un carré modulo p_i et 0 sinon. On a donc

$$\mathrm{Card}\{x \in (\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times \mid x^2 = (D\,[p_i^{e_i}])\} = \left(1 + \left(\frac{D}{p_i}\right)\right).$$

Supposons que $e \geqslant 1$, c'est-à-dire k pair. Dans ce cas D est impair. Le groupe $(\mathbb{Z}/2^{2+e})^\times$ n'est pas cyclique mais isomorphe au groupe produit $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^e\mathbb{Z})$. On a cette fois des isomorphismes

$$\begin{array}{ccc} \{\pm 1\} \times \mathbb{Z}/2^e\mathbb{Z} & \xrightarrow{\sim} & (\mathbb{Z}/2^{e+2}\mathbb{Z})^\times \\ (x, y) & \longmapsto & x5^y \\ \{\pm 1\} \times \mathbb{Z}/2^{e-1}\mathbb{Z} & \xrightarrow{\sim} & (\mathbb{Z}/2^{e+1}\mathbb{Z})^\times \\ (x, y) & \longmapsto & x5^y \end{array}$$

Posons $(D\,[2^{e+2}]) = x5^y$ avec $x \in \{\pm 1\}$ et $y \in \mathbb{Z}/2^e\mathbb{Z}$. Le nombre de $z \in (\mathbb{Z}/2^{e+1}\mathbb{Z})^\times$ tels que $z^2 = (D\,[2^{e+2}])$ est donc égal au nombre de couples $(x', y') \in \{\pm 1\} \times \mathbb{Z}/2^{e-1}\mathbb{Z}$ tels que $x'^2 = x$ et $2y' \equiv y\,[2^e]$. Une condition nécessaire et suffisante pour que l'équation ait des solutions est donc que $x = 1$ et y est pair, c'est-à-dire si et seulement si D est un carré modulo 8. Alors y' est uniquement déterminé par y et x' peut prendre deux valeurs. Ainsi

$$\mathrm{Card}\{x \in (\mathbb{Z}/2^{e+1}\mathbb{Z})^\times \mid x^2 \equiv D\,[2^{e+2}]\} = (1 + \chi_D(2)).$$

Si k est impair, il est clair que l'application $\nu \mapsto \nu^2$ induit une bijection

$$\{x \in \mathbb{Z}/2\mathbb{Z} \mid x \equiv D\,[2]\} \simeq \{x \in \mathbb{Z}/4\mathbb{Z} \mid x \equiv D\,[4]\}.$$

Dans ce cas le nombre $\mathrm{Card}\{x \in (\mathbb{Z}/2\mathbb{Z}) \mid x^2 \equiv D\,[4]\}$ vaut toujours 1.

Finalement, on a

$$\mathrm{Card}\{x \in (\mathbb{Z}/2k)^\times \mid x^2 \equiv D\,[4k]\} = \prod_{p|k}(1+\chi_D(p)).$$

En remarquant que $\mu(m)^2 = 1$ si m est sans diviseur carré et 0 sinon, on a bien

$$\prod_{p|k}(1+\chi_D(p)) = \sum_{m|k}\chi_D(m)\mu(m)^2. \qquad \square$$

Nous pouvons à présent démontrer le théorème 6.7.

Démonstration du théorème 6.7. Soit $\nu \in \mathbb{Z}/2k\mathbb{Z}$ tel que $\nu^2 \equiv D\,[4k]$. D'après le lemme 6.2.3, il existe $1 \leqslant i \leqslant h(D)$ et $(x,y) \in \mathbb{Z}^2$ tels que $\mathrm{PGCD}(x,y) = 1$, $q_i(x,y) = k$ et $\nu_{q_i}(x,y) = \nu$. D'après le lemme 6.2.3, il existe un unique $1 \leqslant i \leqslant h(D)$ vérifiant ces propriétés. Enfin, d'après le lemme 6.2.3, le nombre de couples (x,y) vérifiant ces propriétés est exactement w. Soit donc $\varphi(k,q_i)$ le nombre de solutions primitives à l'équation $q_i(x,y) = k$ et soit $\varphi(k) = \sum_{i=1}^{h(D)}\varphi(k,q_i)$. On a donc

$$\varphi(k) = \sum_{\substack{\nu\in\mathbb{Z}/2k\mathbb{Z}\\ \nu^2\equiv D\,[4k]}} w = w\sum_{m|k}\chi_D(m)\mu(m)^2$$

où la dernière égalité est conséquence du lemme 6.2.3.

Plus généralement soit (x,y) une solution de l'équation $q(x,y) = k$ et soit $g = \mathrm{PGCD}(x,y)$. Alors $(x,y) = g(x',y')$ et $k = g^2q(x',y')$ avec $\mathrm{PGCD}(x',y') = 1$. On en déduit que

$$\begin{aligned}\Psi(k) &= \sum_{\substack{g\geqslant 1\\ g^2|k}}\varphi\left(\frac{k}{g^2}\right) = w\sum_{\substack{g\geqslant 1\\ g^2|k}}\sum_{m|\frac{k}{g^2}}\chi_D(m)\mu(m)^2\\ &= w\sum_{\substack{g\geqslant 1\\ g^2|k}}\sum_{m|\frac{k}{g^2}}\chi_D(mg^2)\mu(m)^2.\end{aligned}$$

Comme tout diviseur de k s'écrit de façon unique sous la forme g^2m avec m sans diviseur carré, on en déduit que

$$\Psi(k) = w\sum_{m|k}\chi_D(m). \qquad \square$$

6.2.4 La formule analytique du nombre de classes

Soit $D < 0$ un entier congru à 0 ou 1 modulo 4.

Le caractère de Dirichlet χ_D est non trivial. L'abscisse de convergence de la série de Dirichlet $L(\chi_D, s)$ est donc 0. On a démontré au chapitre 4 que $L(\chi_D, 1) \neq 0$. Nous allons à présent donner une formule exacte pour la valeur $L(\chi_D, 1)$.

Lemme. *On a*

$$\lim_{x\to+\infty}\frac{1}{x}\sum_{\substack{k\leqslant x\\ k\wedge D=1}}\sum_{\substack{n\geqslant 1\\ n|k}}\chi_D(n)=\frac{\varphi(|D|)}{|D|}L(1,\chi_D).$$

Démonstration. Posons $A(x,D,n)=\mathrm{Card}\{k\leqslant\frac{x}{n}\mid k\wedge D=1\}$. Alors

$$\frac{1}{x}\sum_{\substack{k\leqslant x\\ k\wedge D=1}}\sum_{n|k}\chi_D(n)=\frac{1}{x}\sum_{n\leqslant x}\chi_D(n)\sum_{\substack{k\leqslant\frac{x}{n}\\ k\wedge D=1}}1=\frac{1}{x}\sum_{n}\chi_D(n)A(x,D,n)$$

(remarquons que $A(x,D,n)=0$ si $n>x$).

Nous allons montrer que la série de fonctions $\sum_{n\geqslant 1}\chi_D(n)\frac{A(x,D,n)}{x}$ est uniformément convergente sur $[1,+\infty[$. La convergence uniforme se prouve par un procédé de sommation par parties. Pour tout $M\geqslant 1$, on a (en notant $S_n=\sum_{m=1}^{n}\chi_D(m)$) :

$$\begin{aligned}\left|\sum_{n\geqslant M}\chi_D(n)\frac{A(x,D,n)}{x}\right|&=\left|\sum_{n\geqslant M}(S_n-S_{n-1})\frac{A(x,D,n)}{x}\right|\\&=\left|\sum_{n\geqslant M}S_n\left(\frac{A(x,D,n)}{x}-\frac{A(x,D,n+1)}{x}\right)-S_{M-1}\frac{A(x,D,M)}{x}\right|\\&\leqslant 2|D|\frac{A(x,D,M)}{x}\leqslant 2|D|\frac{1}{M}.\end{aligned}$$

car la fonction $n\mapsto\frac{A(x,D,n)}{x}$ est décroissante et $|S_n|\leqslant|D|$ pour tout $n\geqslant 1$ vu que χ_D est un caractère de Dirichlet non trivial modulo $|D|$.

Remarquons alors que $\lim_{x\to+\infty}\frac{1}{x}A(x,D,n)=\frac{\varphi(|D|)}{|D|}\frac{1}{n}$. □

Lemme. *Soit $D<0$ un entier congru à 0 ou 1 modulo 4. Soit $q=[a,b,c]$ une forme quadratique binaire primitive de discriminant D. On a alors*

$$\mathrm{Card}\{(x,y)\in(\mathbb{Z}/|D|\mathbb{Z})^2\mid q(x,y)\in(\mathbb{Z}/|D|\mathbb{Z})^\times\}=|D|\varphi(|D|).$$

Démonstration. On se ramène facilement au cas où n est de la forme p^e avec p un nombre premier. Il faut donc prouver que

$$\{(x,y)\in(\mathbb{Z}/p^e\mathbb{Z})^2\mid q(x,y)\in(\mathbb{Z}/p^e\mathbb{Z})^\times\}=p^{e-1}(p-1)p^e$$

où p est un nombre premier divisant D. Remarquons que

$$\begin{aligned}&\{(x,y)\in(\mathbb{Z}/p^e\mathbb{Z})^2\mid q(x,y)\in(\mathbb{Z}/p^e\mathbb{Z})^\times\}\\&\qquad=\{(x,y)\in(\mathbb{Z}/p^e\mathbb{Z})^2\mid(q(x,y)\,[p])\in(\mathbb{Z}/p\mathbb{Z})^\times\}.\end{aligned}$$

Un couple (x,y) est dans cet ensemble si est seulement sa réduction modulo p vérifie $q(x,y)\in(\mathbb{Z}/p\mathbb{Z})^\times$. Il suffit donc de prouver le cas où $e=1$.

Si $p|D$, on a $p|b^2-4ac$. Comme $\mathrm{PGCD}(a,b,c)=1$, quitte à échanger a et c, on peut supposer que p ne divise pas a. Comme souvent, il convient de séparer le cas où $p=2$ et le cas où p est impair.

— Si $p>2$, on a (dans $\mathbb{Z}/p\mathbb{Z}$) :

$$q(x,y)\neq 0 \Leftrightarrow aq(x,y)\neq 0 \Leftrightarrow (2ax+by)^2-Dy^2\neq 0 \Leftrightarrow (2ax+by)\neq 0.$$

L'équation $2ax+by=0$ définit une droite de $(\mathbb{Z}/p\mathbb{Z})^2$, son complémentaire est donc de cardinal $p^2-p=p(p-1)$.

— Si $p=2$, comme $2|D$, ona $2|b$. Alors $q(x,y)\neq 0$ si et seulement si $ax^2+cy^2\neq 0$. Comme $a\neq 0$, on vérifie facilement qu'il y a exactement deux couples (x,y) dans $(\mathbb{Z}/2\mathbb{Z})^2$ tel que $ax^2+cy^2\neq 0$ (selon la parité de c). □

Lemme. *Soit $q=[a,b,c]$ une forme quadratique binaire primitive de discriminant D. On a alors*

$$H(x,q) \coloneqq \sum_{\substack{k\leqslant x\\ k\wedge D=1}} \Psi(k,q) \sim_{x\to+\infty} \frac{2\pi}{\sqrt{|D|}}\frac{\varphi(|D|)}{|D|}x.$$

Démonstration. Soit $(x_0,y_0)\in\mathbb{Z}^2$ tel que $q(x_0,y_0)\notin |D|\mathbb{Z}$ et posons

$$H(t,q,x_0,y_0) \coloneqq \mathrm{Card}\{(x,y)\equiv(x_0,y_0)\,[|D|] \mid q(x,y)\leqslant t\}.$$

On a

$$H(t,q,x_0,y_0)=\mathrm{Card}((x_0,y_0)+|D|\mathbb{Z}^2)\cap\sqrt{t}\mathcal{E}$$

où $\mathcal{E}$ est l'ellipse

$$\mathcal{E}\coloneqq\{(x,y)\in\mathbb{R}^2 \mid q(x,y)\leqslant 1\}.$$

L'aire de cette ellipse est $\mathrm{Vol}(\mathcal{E})=\frac{2\pi}{\sqrt{|D|}}$. On déduit alors de la Proposition de la partie 6.2.5 que

$$H(t,q,x_0,y_0)\sim_{t\to+\infty}\frac{2\pi}{\sqrt{|D|}|D|^2}t.$$

Comme $H(t,q)$ est la somme des $H(t,q,x_0,y_0)$ où (x_0,y_0) parcourt une famille de représentants de l'ensemble

$$\{(x,y)\in(\mathbb{Z}/|D|\mathbb{Z})^2 \mid (q(x,y)\mathrm{mod}\,|D|)\neq 0\}$$

on en déduit (à l'aide du lemme 6.2.4) le résultat. □

On peut finalement en déduire la *formule analytique du nombre de classes* :

Théorème 6.9. *On a*

$$h(D)=\frac{w\sqrt{|D|}}{2\pi}L(\chi_D,1).$$

Démonstration. Soient $q_1, \dots, q_{h(D)}$ des représentants des classes d'équivalence propre de formes quadratiques binaires de discriminant D. On a alors

$$\sum_{i=1}^{h(D)} H(x, q_i) = \sum_{\substack{k \leqslant x \\ k \wedge D = 1}} \psi(k) = w \sum_{\substack{k \leqslant x \\ k \wedge D = 1}} \sum_{n|k} \chi_D(n).$$

Ainsi on a

$$\frac{1}{x} \sum_{i=1}^{h(D)} H(x, q_i) \sim_{x \to +\infty} \frac{2\pi}{\sqrt{|D|}} \frac{\varphi(|D|)}{|D|} h(D) \sim w \frac{\varphi(|D|)}{|D|} L(\chi_D, 1).$$

Ainsi $h(D) = \frac{w\sqrt{|D|}}{2\pi} L(\chi_D, 1)$. □

Corollaire. *On a* $L(\chi_D, 1) > 0$.

Exemple. Considérons le cas où $D = -4$. Alors

$$\chi_{-4}(n) = \begin{cases} 1 & \text{si } n \equiv 1\,[4] \\ -1 & \text{si } n \equiv 3\,[4] \\ 0 & \text{sinon.} \end{cases}$$

On a par ailleurs déjà calculé $h(-4) = 1$. On en déduit que

$$L(\chi_{-4,1}) = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \dots = \frac{\pi}{4}.$$

6.2.5 Un résultat sur les réseaux de $\mathbb{R}^n$

Dans tout ce qui suit, pour un réel $\lambda > 0$, on note $\overline{B(0, \lambda)}$ la boule fermée de centre 0 et de rayon λ de $\mathbb{R}^n$ muni de la distance euclidienne :

$$\overline{B(0, \lambda)} \coloneqq \{x \in \mathbb{R}^n \mid ||x|| \leqslant \lambda\}.$$

On appelle *réseau* de $\mathbb{R}^n$ un sous-groupe additif de $\mathbb{R}^n$ engendré par une base de $\mathbb{R}^n$. Un réseau Λ est donc un sous-groupe $\Lambda = \mathbb{Z}e_1 \oplus \dots \oplus \mathbb{Z}e_n$ de $\mathbb{R}^n$ où $(e_1, \dots, e_n)$ est une base de $\mathbb{R}^n$. Une *maille élémentaire* d'un réseau Λ est une partie de $\mathbb{R}^n$ de la forme

$$M = \prod_{i=1}^{n} [0, 1[\, e_i.$$

On a alors une partition de $\mathbb{R}^n$ donnée par

$$\mathbb{R}^n = \coprod_{x \in \Lambda} (x + M).$$

Il y a beaucoup de choix possibles de base $(e_1, \dots, e_n)$ donnant lieu au même réseau. Cependant le volume de la maille M ne dépend pas du choix de la base $(e_1, \dots, e_n)$. En effet si $(e'_1, \dots, e'_n)$ est une autre base du $\mathbb{Z}$-module Λ, il existe une matrice $P \in \mathrm{GL}_n(\mathbb{Z})$ telle que $Pe_i = e'_i$ pour tout $1 \leqslant i \leqslant n$. Posons $M' = \prod_{i=1}^n [0,1[\, e_i$. On a alors

$$\mathrm{Vol}(M') = |\det(e'_1, \dots, e'_n)| = |\det(P)||\det(e_1, \dots, e_n)| = \mathrm{Vol}(M).$$

Le nombre réel $\mathrm{Vol}(M)$, qui ne dépend donc que de Λ, est appelé *volume* du réseau Λ et noté $\mathrm{Vol}(\Lambda)$.

Soit $x_0 \in \mathbb{R}^n$. Si $\lambda > 0$, on pose

$$N(\lambda) \coloneqq \mathrm{Card}((x_0 + \Lambda) \cap \overline{B(0,\lambda)}).$$

Lemme. *On a un équivalent, lorsque $\lambda \to +\infty$,*

$$N(\lambda) \sim \lambda^n \frac{\mathrm{Vol}(\overline{B(0,1)})}{\mathrm{Vol}(\Lambda)}.$$

Démonstration. Soit M une maille élémentaire du réseau Λ. Soit

$$d \coloneqq \sup\{||x - y|| \mid x, y \in M\}$$

le diamètre de la partie M. Posons

$$A(\lambda) \coloneqq \{x \in (x_0 + \Lambda) \cap \overline{B(0, \lambda - d)}\}$$
$$B(\lambda) \coloneqq \{x \in (x_0 + \Lambda) \cap \overline{B(0, \lambda + d)}\}.$$

Remarquons que si $x \in A(\lambda)$, on a $x + M \subset \overline{B(0,\lambda)}$. Réciproquement si $y \in \overline{B(0,\lambda)}$, il existe $x \in B(\lambda)$ tel que $y \in x + M$. Ainsi

$$\coprod_{x \in\ A(\lambda)} (x + M) \subset \overline{B(0,\lambda)} \subset \coprod_{x \in B(\lambda)} (x + M).$$

On en déduit que, pour tout $\lambda > 0$,

$$\mathrm{Card}(A(\lambda))\,\mathrm{Vol}(M) \leqslant \mathrm{Vol}(\overline{B(0,\lambda)}) \leqslant \mathrm{Card}(B(\lambda))\,\mathrm{Vol}(M).$$

Par ailleurs, on a $\mathrm{Vol}(\overline{B(0,\lambda)}) = \lambda^n\,\mathrm{Vol}(\overline{B(0,1)})$. Ainsi, en remarquant que $N(\lambda) = \mathrm{Card}\,A(\lambda + d) = \mathrm{Card}\,B(\lambda - d)$, on a

$$(\lambda - d)^n\,\mathrm{Vol}(\overline{B(0,1)}) \leqslant N(\lambda)\,\mathrm{Vol}(M) \leqslant (\lambda + d)^n\,\mathrm{Vol}(\overline{B(0,1)}).$$

On en déduit l'équivalent recherché. □

Nous n'utiliserons en fait que le cas particulier où $n = 2$.

Soit $\mathcal{E} \subset \mathbb{R}^2$ une ellipse de centre 0. Il existe alors une dilatation $h \in \mathrm{GL}_2(\mathbb{R})$ tel que $h(\mathcal{E}) = \overline{B(0,1)}$. Soit Λ un réseau de $\mathbb{R}^2$. Le sous-groupe $h(\Lambda)$ est alors un autre réseau de $\mathbb{R}^2$ et on a $\mathrm{Vol}(h(\Lambda)) = |\det(h)|\,\mathrm{Vol}(\Lambda)$ et $\mathrm{Vol}(\mathcal{E}) = |\det h|^{-1}\pi$. Ainsi

$$\mathrm{Vol}(h(\Lambda)) = \frac{\pi}{\mathrm{Vol}(\mathcal{E})}\,\mathrm{Vol}(\Lambda).$$

On en déduit que, pour $x_0 \in \mathbb{R}^2$, on a

$$\mathrm{Card}((x_0 + \Lambda) \cap \lambda\mathcal{E}) \sim_{\lambda\to+\infty} \lambda^2 \frac{\mathrm{Vol}(\mathcal{E})}{\mathrm{Vol}(\Lambda)}.$$

Dans le cas particulier où $\Lambda = m\mathbb{Z}^2$ pour un entier $m \geqslant 1$, on a le résultat suivant :

Proposition. *Soit $x_0 \in \mathbb{R}^2$ et soit $\mathcal{E}$ une ellipse de $\mathbb{R}^2$ centrée en 0. On a*

$$\mathrm{Card}((x_0 + m\mathbb{Z}^2) \cap \lambda\mathcal{E}) \sim_{\lambda\to+\infty} \lambda^2 \frac{\mathrm{Vol}(\mathcal{E})}{m^2}.$$

6.3 Lien avec les groupes de classes des corps quadratiques

Soit $d \in \mathbb{Z}$ un entier sans diviseur carré et différent de 1. On pose $K = \mathbb{Q}(\sqrt{d})$. On rappelle que K est un corps quadratique et que $\mathcal{O}_K = \mathbb{Z}[\alpha]$ où

$$\alpha = \begin{cases} \sqrt{d} & \text{si } d \equiv 2 \text{ ou } 3\,[4] \\ \frac{1+\sqrt{d}}{2} & \text{si } d \equiv 1\,[4]. \end{cases}$$

On a calculé que

$$\Delta_{\mathcal{O}_K/\mathbb{Z}} = \begin{cases} 4d & \text{si } d \equiv 2 \text{ ou } 3\,[4] \\ d & \text{si } d \equiv 1\,[4]. \end{cases}$$

On appelle donc *discriminant fondamental* un entier $D \in \mathbb{Z} \smallsetminus \{1, 4\}$ tel que $D \equiv 1\,[4]$ et D est sans diviseur carré ou $D = 4d$ où d est un entier congru à 2 ou 3 modulo 4 sans diviseur carré. Les discriminants fondamentaux sont donc très exactement les discriminants des extensions quadratiques de $\mathbb{Q}$.

Théorème 6.10. *Soit $D < 0$ un discriminant fondamental. Posons $K = \mathbb{Q}(\sqrt{D})$. Alors $h(D) = h_K$. Autrement dit le nombre de classes d'équivalence propre de formes quadratiques binaires primitives définies positives de discriminant D est égal au nombre de classes de diviseurs dans $\mathcal{O}_K$.*

Avant de prouver ce théorème, effectuons quelques constructions. On fixe un discriminant fondamental $D < 0$.

On choisit $\sqrt{D}$ de sorte que $\operatorname{Im}\sqrt{D} > 0$, c'est-à-dire tel que $\sqrt{D} = i\sqrt{-D}$. Soit I un idéal non nul de $\mathcal{O}_K$. Alors I est un $\mathbb{Z}$-module libre de rang 2, on peut donc l'écrire sous la forme $I = \mathbb{Z}\alpha_1 \oplus \mathbb{Z}\alpha_2$ où (α_1, α_2) est une $\mathbb{Q}$-base de K sur $\mathbb{Q}$. Comme $K \not\subset \mathbb{R}$, une base de K sur $\mathbb{Q}$ est en particulier une base de $\mathbb{C}$ sur $\mathbb{R}$. On a donc $\mathbb{R}\alpha_1 \neq \mathbb{R}\alpha_2$ dans $\mathbb{C}$. On en conclut que

$$\alpha_1\overline{\alpha_2} - \alpha_2\overline{\alpha_1} \notin \mathbb{R}.$$

On dit que la base (α_1, α_2) est *directe* si $\operatorname{Im}(\alpha_1\overline{\alpha_2} - \alpha_2\overline{\alpha_1}) > 0$. Remarquons que si la base (α_1, α_2) n'est pas directe, alors la base (α_2, α_1) est directe.

Notons

$$\mathcal{S} \coloneqq \{(\alpha_1, \alpha_2) \in K^2 \mid \mathbb{Z}\alpha_1 \oplus \mathbb{Z}\alpha_2 \text{ est un idéal non nul de } \mathcal{O}_K \text{ et } (\alpha_1, \alpha_2) \text{ est directe}\}.$$

Si $\alpha = (\alpha_1, \alpha_2) \in \mathcal{S}$, on note I_α l'idéal $\mathbb{Z}\alpha_1 \oplus \mathbb{Z}\alpha_2$ et on pose, pour $(x, y) \in \mathbb{Z}^2$,

$$q_\alpha(x, y) \coloneqq \frac{N_{K/\mathbb{Q}}(x\alpha_1 + y\alpha_2)}{N(I_\alpha)} = \frac{|x\alpha_1 + y\alpha_2|^2}{N(I_\alpha)}.$$

Nous allons en fait prouver le résultat suivant :

Proposition. *(i) Pour tout $\alpha \in \mathcal{S}$, la fonction q_α est une forme quadratique binaire primitive définie positive de discriminant D.*

(ii) Pour α et β dans $\mathcal{S}$, on a $q_\alpha \overset{+}{\sim} q_\beta$ si et seulement si les idéaux I_α et I_β sont dans la même classe.

(iii) L'application $\alpha \mapsto q_\alpha$ induit une bijection entre les ensembles $\mathrm{Cl}(\mathcal{O}_K)$ et $\mathcal{P}_+(D)$.

(iv) Soit $\alpha \in \mathcal{S}$ et soit $c \in \mathrm{Cl}(\mathcal{O}_K)$. L'ensemble des entiers représentés par q_α est l'ensemble des normes d'idéaux appartenant à la classe c^{-1}.

Démonstration. Commençons par prouver (i). Un calcul direct montre que

$$\forall (x, y) \in \mathbb{Z}^2, \quad q_\alpha(x, y) = \frac{x^2 N_{K/\mathbb{Q}}(\alpha_1) + y^2 N_{K/\mathbb{Q}}(\alpha_2) + xy(\alpha_1\overline{\alpha_2} + \alpha_2\overline{\alpha_1})}{N(I_\alpha)}.$$

Comme I_α est un idéal de $\mathcal{O}_K$, les nombres α_1 et α_2 sont des entiers de K, on a donc $N_{K/\mathbb{Q}}(\alpha_1), N_{K/\mathbb{Q}}(\alpha_2) \in \mathbb{Z}$ et $\alpha_1\overline{\alpha_2} + \alpha_2\overline{\alpha_1} \in \mathbb{Q} \cap \mathcal{O}_K = \mathbb{Z}$. Pour montrer que q_α est une forme quadratique binaire, il suffit de vérifier :

$$q_\alpha(1, 0) \in \mathbb{Z}, \quad q_\alpha(0, 1) \in \mathbb{Z}, \quad q_\alpha(1, 1) \in \mathbb{Z}.$$

On aura en effet $q_\alpha = [q_\alpha(1,0), q_\alpha(1,1) - q_\alpha(1,0) - q_\alpha(0,1), q_\alpha(0,1)]$. Comme $\alpha_1 \in I_\alpha$, on a $(\alpha_1) \subset I_\alpha$ et donc $N(I_\alpha) \mid N((\alpha_1)) = N_{K/\mathbb{Q}}(\alpha_1)$. Donc

$$q_\alpha(1, 0) = \frac{N_{K/\mathbb{Q}}(\alpha_1)}{N(I_\alpha)} \in \mathbb{Z}.$$

De même, $q_\alpha(0, 1) \in \mathbb{Z}$. Comme de plus $\alpha_1 + \alpha_2 \in I_\alpha$, on a de même $q_\alpha(1, 1) \in \mathbb{Z}$. Ainsi q_α est bien une forme quadratique binaire. Comme l'extensions $K/\mathbb{Q}$ est quadratique

imaginaire, on a $N_{K/\mathbb{Q}}(x) = x\overline{x} \geqslant 0$ pour tout $x \in K$ avec égalité si et seulement si $x = 0$. Ainsi q_α est définie positive (voir l'exercice 3 du TD5 pour la première égalité).

Calculons le discriminant de q_α. On a

$$\begin{aligned}\mathrm{Disc}(q_\alpha) &= N(I_\alpha)^{-2}((\alpha_1\overline{\alpha_2} + \alpha_2\overline{\alpha_1})^2 - 4N_{K/\mathbb{Q}}(\alpha_1)N_{K/\mathbb{Q}}(\alpha_2)) = N(I_\alpha)^{-2}(\alpha_1\overline{\alpha_2} - \alpha_2\overline{\alpha_1})^2 \\ &= N(I_\alpha)^{-2}\begin{vmatrix}\alpha_1 & \alpha_2 \\ \overline{\alpha_1} & \overline{\alpha_2}\end{vmatrix}^2 = N(I_\alpha)^{-2}\Delta_{K/\mathbb{Q}}(\alpha_1, \alpha_2).\end{aligned}$$

Or on a déjà vu que

$$\Delta_{K/\mathbb{Q}}(\alpha_1, \alpha_2) = N(I_\alpha)^2\Delta_{\mathcal{O}_K/\mathbb{Z}}$$

de sorte que $\mathrm{Disc}(q_\alpha) = \Delta_{\mathcal{O}_K/\mathbb{Z}} = D$. Il reste à vérifier que la forme q_α est primitive. Supposons que $q_\alpha = nq'$ avec q' une forme quadratique binaire. Alors $\mathrm{Disc}(q_\alpha) = n^2\,\mathrm{Disc}(q')$, ainsi n^2 divise $\mathrm{Disc}(q_\alpha) = D$. Or D est sans facteur carré sauf si $D = 4d$ avec d sans facteur carré et d congru à 2 ou 3 modulo 4. Ainsi $n = 1$ ou $n = 2$ et $\mathrm{Disc}(q') = d$. Le deuxième cas est impossible car un discriminant de forme quadratique est toujours congru à 0 ou 1 modulo 4. On en conclut que $n = 1$ et donc que q_α est primitive.

Prouvons (ii). Soient $\alpha = (\alpha_1, \alpha_2)$ et $\beta = (\beta_1, \beta_2)$ deux éléments de $\mathcal{S}$. Supposons dans un premier temps que $I_\alpha = I_\beta$. Alors il existe une matrice $P \in \mathrm{GL}_2(\mathbb{Z})$ telle que

$$\begin{pmatrix}\beta_1 \\ \beta_2\end{pmatrix} = P\begin{pmatrix}\alpha_1 \\ \alpha_2\end{pmatrix}.$$

Comme P est à coefficients entiers, on en déduit que

$$\begin{pmatrix}\beta_1 & \overline{\beta_1} \\ \beta_2 & \overline{\beta_2}\end{pmatrix} = P\begin{pmatrix}\alpha_1 & \overline{\alpha_1} \\ \alpha_2 & \overline{\alpha_2}\end{pmatrix}.$$

En considérant les déterminants, on obtient

$$\mathrm{Im}(\beta_1\overline{\beta_2} - \beta_2\overline{\beta_1}) = \det(P)\,\mathrm{Im}(\alpha_1\overline{\alpha_2} - \alpha_2\overline{\alpha_1}).$$

Ainsi $\det(P) > 0$ et $P \in \mathrm{SL}_2(\mathbb{Z})$. Il est clair que $q_\beta \cdot P = q_\alpha$ et donc $q_\beta \overset{+}{\sim} q_\alpha$.

Supposons désormais que $I_\alpha \sim I_\beta$. Il existe alors c_1 et c_2 dans $\mathcal{O}_K \smallsetminus \{0\}$ tels que $c_1I_\alpha = c_2I_\beta$. On en déduit que $q_{c_1\alpha} \overset{+}{\sim} q_{c_2\beta}$. Par ailleurs

$$\begin{aligned}\forall (x, y) \in \mathbb{Z}^2, \quad q_{c_1\alpha}(x, y) &= \frac{N_{K/\mathbb{Q}}(xc_1\alpha_1 + yc_1\alpha_2)}{N(c_1I_\alpha)} \\ &= \frac{N_{K/\mathbb{Q}}(c_1)}{N_{K/\mathbb{Q}}(c_1)}\frac{N_{K/\mathbb{Q}}(x\alpha_1 + y\alpha_2)}{N(I_\alpha)} = q_\alpha(x, y)\end{aligned}$$

et donc $q_{c_1\alpha} = q_\alpha$, d'où $q_\alpha \overset{+}{\sim} q_\beta$.

Réciproquement supposons que $q_\alpha \overset{+}{\sim} q_\beta$. Soit $P \in \mathrm{SL}_2(\mathbb{Z})$ telle que $q_\beta = q_\alpha \cdot P$.

On peut donc écrire

$$\forall (x,y)\in\mathbb{Z}^2,\quad q_\alpha(x,y)=\frac{N_{K/\mathbb{Q}}(\alpha_2)}{N(I_\alpha)}N_{K/\mathbb{Q}}\left(\frac{\alpha_1}{\alpha_2}x+y\right).$$

Posons $P=\left(\begin{smallmatrix}p & q\\ r & s\end{smallmatrix}\right)$. On a alors

$$q_\beta(x,y)=q_\alpha(px+qy,rx+sy)$$

et donc

$$\begin{aligned}\frac{N_{K/\mathbb{Q}}(\beta_2)}{N(I_\beta)}N_{K/\mathbb{Q}}\left(\frac{\beta_1}{\beta_2}x+y\right)&=N_{K/\mathbb{Q}}\left(\frac{\alpha_1}{\alpha_2}(px+qy)+(rx+sy)\right)\\&=N_{K/\mathbb{Q}}\left(x(p\frac{\alpha_1}{\alpha_2}+r)+(q\frac{\alpha_1}{\alpha_2}+s)y\right)\\&=\star N_{K/\mathbb{Q}}\left(x\frac{(p\frac{\alpha_1}{\alpha_2}+r)}{(q\frac{\alpha_1}{\alpha_2}+s)}+y\right)\end{aligned}$$

Nous allons utiliser le lemme suivant.

Lemme. *Soient τ et τ' deux éléments de $\mathbb{C}$ tels que $\operatorname{Im}\tau>0$ et $\operatorname{Im}\tau'>0$. Si les deux formes quadratiques q et q' définies par $(x,y)\mapsto|x\tau+y|^2$ et $(x,y)\mapsto|x\tau'+y|^2$ sont proportionnelles sur $\mathbb{Z}^2$. Alors $\tau=\tau'$.*

Démonstration. L'évaluation de ces deux formes en $(0,1)$ montrent qu'elles sont égales. En développant les deux formes, on remarque que $|\tau|=|\tau'|$ et $\operatorname{Re}\tau=\operatorname{Re}\tau'$. Ainsi $\operatorname{Im}\tau=\pm\operatorname{Im}\tau'$ donc $\operatorname{Im}\tau=\operatorname{Im}\tau'$. □

Comme $\det(P)=1$, un calcul simple montre que

$$\operatorname{Im}\frac{p\alpha_1+q\alpha_2}{r\alpha_1+s\alpha_2}=\frac{|\alpha_2|^2}{|r\alpha_1+s\alpha_2|^2}\operatorname{Im}\frac{\alpha_1}{\alpha_2}>0.$$

On en déduit que $\frac{\beta_1}{\beta_2}=\frac{p\alpha_1+q\alpha_2}{r\alpha_1+s\alpha_2}$. Ainsi

$$\begin{aligned}\mathbb{Z}\beta_1+\mathbb{Z}\beta_2&=\beta_2(\mathbb{Z}\frac{\beta_1}{\beta_2}+\mathbb{Z})\\&=\frac{\beta_2}{r\alpha_1+s\alpha_2}(\mathbb{Z}(p\alpha_1+q\alpha_2)+\mathbb{Z}(r\alpha_1+s\alpha_2))\\&=\frac{\beta_2}{r\alpha_1+s\alpha_2}(\mathbb{Z}\alpha_1+\mathbb{Z}\alpha_2)\end{aligned}$$

car $\left(\begin{smallmatrix}p & q\\ r & s\end{smallmatrix}\right)\in\mathrm{SL}_2(\mathbb{Z})$. On a donc $I_\alpha\sim I_\beta$.

Prouvons (iii). Le (ii) montre que l'application $\alpha\mapsto q_\alpha$ induit une application injective de $\mathrm{Cl}(\mathcal{O}_K)$ vers $\mathcal{P}_+(D)$. Il reste à prouver que cette application est surjective. Soit donc $q=[a,b,c]$ une forme quadratique binaire primitive de discriminant D. On a

$$\forall (x,y)\in\mathbb{Z}^2,\quad 4aq(x,y)=(2ax+by)^2-Dy^2=N_{K/\mathbb{Q}}(2ax+by+i\sqrt{-D}y).$$

Posons alors $\alpha_1 = 2a$ et $\alpha_2 = b - i\sqrt{-D}$. On a alors

$$\alpha_1\overline{\alpha_2} - \alpha_2\overline{\alpha_1} \in i\,]0, +\infty[$$

donc $\alpha \coloneqq (\alpha_1, \alpha_2)$ est une base directe de K sur $\mathbb{Q}$. Supposons pour le moment que $I_\alpha \coloneqq \mathbb{Z}\alpha_1 \oplus \mathbb{Z}\alpha_2$ est un idéal de $\mathcal{O}_K$. On a alors

$$\Delta_{K/\mathbb{Q}}(\alpha_1, \alpha_2) = \begin{vmatrix} 2a & 2a \\ b - i\sqrt{-D} & b + i\sqrt{-D} \end{vmatrix}^2 = (4ai\sqrt{-D})^2 = D(4a)^2.$$

Comme $\Delta_{\mathcal{O}_K/\mathbb{Z}} = D$, on a bien $N(I_\alpha) = 4a$ et donc $q = q_\alpha$.

Il reste à vérifier que I_α est bien un idéal de $\mathcal{O}_K$. Commençons par le cas où $D \equiv 0\,[4]$, c'est-à-dire $D = 4d$ avec d congru à 2 ou 3 modulo 4. On a alors $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$. Il faut prouver que I_α est stable par multiplication par les éléments de $\mathcal{O}_K$. Comme I_α est déjà un sous-groupe additif de $\mathcal{O}_K$, il suffit de prouver que $\sqrt{d}I_\alpha \subset I_\alpha$. Montrer que $\sqrt{d}\alpha_1 \in I_\alpha$ et $\sqrt{d}\alpha_2 \in I_\alpha$. On a alors

$$\begin{aligned} \frac{\sqrt{D}}{2}(b - \sqrt{D}) = \frac{\sqrt{D}}{2}b - \frac{D}{2} &= \frac{b}{2}(\sqrt{D} - b) + \frac{b^2}{2} - \frac{D}{2} \\ &= \frac{b}{2}(\sqrt{D} - b) + 2ac \in \mathbb{Z}2a \oplus \mathbb{Z}(\sqrt{D} - b) = I_\alpha \end{aligned}$$

En effet, D est pair, donc b est pair. De même

$$\frac{\sqrt{D}}{2}2a = a\sqrt{D} = a(\sqrt{D} - b) + ab = a(\sqrt{D} - b) + 2a\frac{b}{2} \in I_\alpha.$$

Considérons le cas où $D \equiv 1\,[4]$ et $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{D}}{2}]$. On a

$$\begin{aligned} \frac{1 + \sqrt{D}}{2}(b - \sqrt{D}) = \frac{b}{2} - \frac{D}{2} + (\frac{b}{2} - \frac{1}{2})\sqrt{D} &= \frac{b-1}{2}(\sqrt{D} - b) + \frac{b(b-1)}{2} + \frac{b-D}{2} \\ &= \frac{b-1}{2}(\sqrt{D} - b) + \frac{b^2 - D}{2} = \frac{b-1}{2}(\sqrt{D} - b) + 2ac. \end{aligned}$$

On a gagné car b est impair cette fois-ci. Enfin :

$$\frac{1 + \sqrt{D}}{2}2a = a(1 + \sqrt{D}) = a + a(\sqrt{D} - b) + ab = a(\sqrt{D} - b) + \frac{b+1}{2}2a \in I_\alpha.$$

Il reste à prouver (iv). Soit $(x, y) \in \mathbb{Z}^2$ et posons $\xi = x\alpha_1 + y\alpha_2$. On a $(\xi) \subset I_\alpha$. Posons alors $J_\xi = (\xi)I_\alpha^{-1}$ qui est un idéal de $\mathcal{O}_K$. Alors $J_\xi \in c^{-1}$ et $N(J_\xi) = q_\alpha(x, y)$. Réciproquement supposons que $J \in c^{-1}$. Alors, il existe a et b dans $\mathcal{O}_K \smallsetminus \{0\}$ tels que $aJ = bI_\alpha^{-1}$ et donc $JI_\alpha = (\xi)$ où $\xi = ba^{-1}$. Ainsi $\xi \in I_\alpha J \subset I_\alpha$ et $N(J) = \frac{N_{K/\mathbb{Q}}(\xi)}{N(I_\alpha)} = q_\alpha(x, y)$ où $\xi = x\alpha_1 + y\alpha_2$. □

Remarque. Ce résultat nous donne un procédé très efficace pour vérifier si deux idéaux de $\mathcal{O}_K$ sont équivalents. Il suffit de calculer les formes quadratiques associées, de déterminer les formes réduites qui leur sont proprement équivalentes et de vérifier que ces formes sont égales.

Corollaire. *Toute classe d'idéal de $\mathcal{O}_K$ contient un idéal de norme $\leqslant \sqrt{\frac{|D|}{3}}$.*

Exemple. Donnons l'exemple du corps $K = \mathbb{Q}(i\sqrt{5})$. Son anneau d'entiers est $\mathcal{O}_K = \mathbb{Z}[i\sqrt{5}]$ et son discriminant est $D = -20$. On a déjà calculé que $h(-20) = 2$. Ainsi le groupe des classes de l'anneau $\mathcal{O}_K$ est de cardinal 2 et donc isomorphe à $\mathbb{Z}/2\mathbb{Z}$. Donnons un exemple d'idéal non principal de l'anneau $\mathcal{O}_K$. Rappelons qu'il existe deux formes quadratiques primitives réduites de discriminant -20 : $q_1 = [1, 0, 5]$ et $q_2 = [2, 2, 3]$. Remarquons que l'idéal trivial est l'idéal I_α avec $\alpha = (i\sqrt{5}, 1)$. Ainsi

$$q_\alpha(x, y) = N_{K/\mathbb{Q}}(xi\sqrt{5} + y) = y^2 + 5x^2$$

donc $q_\alpha = [5, 0, 1] \overset{+}{\sim} q_1$. Ainsi la classe d'équivalence propre de $q_1 = [1, 0, 5]$ est la classe des idéaux principaux. Il suffit donc de donner un idéal I_β tel que q_β soit proprement équivalente à $[2, 2, 3]$. Considérons par exemple l'idéal $I = (2, 1 + i\sqrt{5})$. Remarquons que $I = \mathbb{Z}2 + \mathbb{Z}(1 + i\sqrt{5})$ (attention ce n'est pas complètement évident, un petit calcul s'impose). On a donc $I = I_\beta$ avec $\beta = (1 + i\sqrt{5}, 2)$ et $N(I) = 2$. Alors

$$q_\beta(x, y) = \frac{1}{2}|x + 2y + yi\sqrt{5}|^2 = \frac{1}{2}((x + 2y)^2 + 5x^2) = 3x^2 + 2xy + 2y^2.$$

Alors

$$q_\beta = [3, 2, 2] \overset{+}{\sim} [2, -2, 3] \overset{+}{\sim} [2, 2, 3].$$

Ainsi l'idéal I n'est pas principal.