Cours de Théorie des Nombres, option M1, 2018-2019 Université de Bordeaux

Qing Liu

Table des matières

Chapitre 1

Rappels et compléments d'algèbre commutative.

Tous les anneaux considérés dans ce cours sont commutatifs unitaires. Les homomorphismes d'anneaux $A \to B$ envoient 1_A sur 1_B par définition.

1.1 Anneaux et modules noethériens

Soit A un anneau (commutatif unitaire).

Définition 1.1.1 Un A-module M est de *type fini* s'il est engendré par une famille finie. Il est *noethérien* si tous ses sous-modules sont de type fini. En particulier M lui-même est de type fini. On dira que A est *noethérien* s'il est noethérien en tant que A-module (équivalent : tout idéal est de type fini).

Concrètement, M est de type fini s'il existe $x_1, \ldots, x_n \in M$ tels que M soit engendré par les x_i. Cela revient à dire que tout $x \in M$ s'écrit comme $x = a_1x_1 + \cdots + a_nx_n$ pour certains $a_1, \ldots, a_n \in A$. Quand cela est le cas, on écrit aussi

$$M = Ax_1 + \cdots + Ax_n.$$

Exemple 1.1.2

1. Un corps est toujours noethérien. Un espace vectoriel sur un corps K est noethérien si et seulement s'il est de dimension finie.
2. L'anneau $\mathbb{Z}$ (ou plus généralement un anneau principal) est noethérien puisque tout idéal est principal.
3. $\mathbb{Q}$ est un anneau noethérien, mais comme $\mathbb{Z}$-module il n'est pas noethérien.
4. L'anneau des polynômes à coefficients dans un corps et à une infinité de variables n'est pas noethérien.
5. L'ensemble des fonctions (resp. fonctions continues ; resp. fonctions C^∞) de $\mathbb{R}$ dans $\mathbb{R}$ est un anneau non noethérien.

La proposition suivante nécessite l'axiome du choix.

Proposition 1.1.3. *Les propriétés suivantes sont équivalentes :*

(i) *M est noethérien ;*

(ii) *toute suite croissante de sous-modules de M est stationnaire ;*

(iii) *tout ensemble non vide de sous-modules de M admet un élément maximal (pour l'inclusion).*

Démonstration. (i) $\Rightarrow$ (ii). La réunion est un sous-module, de type fini, donc égal à un des sous-modules.

(ii) $\Rightarrow$ (iii) Soit F un tel ensemble. S'il n'a pas d'élément maximal, alors on peut construire une suite strictement croissante infinie avec des sous-modules appartenant à F.

(iii) $\Rightarrow$ (i). Soit N un sous-module. Soit F l'ensemble des sous-modules de N de type fini. Alors F est non vide car il contient $\{0\}$. Soit N_0 un élément maximal de F. Pour tout $x \in N$, $N_0 + xA \in F$, donc $x \in N_0$ et $N = N_0$ est de type fini. □

En restant dans les axiomatiques ZF (sans l'axiome du choix donc), (i) n'implique pas (iii). Il est alors possible de définir les modules noethériens avec la propriété (iii) qui est plus forte que (i). Avec cette définition, les énoncés de ce paragraphe restent vrais. Les anneaux qu'on rencontrera dans ce cours sont noethériens dans le sens fort (iii).

Proposition 1.1.4. *La classe des A-modules noethériens est stable par sous-module, quotient, extension (suite exacte) et somme directe finie.*

Démonstration. Pour $M \oplus N$: utiliser la projection dans N. □

Corollaire 1.1.5. *Soit A un anneau noethérien. Alors M est noethérien si et seulement si M est de type fini.*

Le théorème suivant ne sera pas montré en cours.

Theorem 1.1.6. (Théorème de Transfert de Hilbert) *Si A est noethérien, alors l'anneau des polynômes $A[X]$ est noethérien.*

Démonstration. Soit I un idéal de $A[X]$. Pour tout $d \geq 0$, posons

$$J_d = \{a \in A \mid \exists\ F(X) = aX^d + a_{d-1}X^{d-1} + ... + a_0 \in I\}.$$

C'est l'ensemble des coefficients dominants des polynômes de degré d dans I union $\{0\}$. C'est un idéal de A et on a $J_d \subseteq J_{d+1}$ pour tout $d \geq 0$. On a donc une suite croissante d'idéaux dans A. D'après la proposition 1.1.3, la suite est stationnaire et donc il existe $N \geq 0$ tel que $J_d = J_{d+1}$ pour tout $d \geq N$. Pour tout $d \leq N$, on prend un *système de générateurs* $\{a_{d,1}, ..., a_{d,m_d}\}$ de J_d (c'est-à-dire que J_d est engendré par $\{a_{d,1}, ..., a_{d,m_d}\}$). Pour tout $j \leq m_d$, on fixe un élément

$$F_{d,j}(X) = a_{d,j}X^d + \{\text{termes de degré} \leq d-1\} \in I.$$

Montrons que I est engendré par l'ensemble $S = \{F_{d,j}(X) \mid 0 \leq d \leq N, 1 \leq j \leq m_d\}$. Ce qui impliquera que I est de type fini et donc que $A[X]$ est noethérien.

Soit I' l'idéal de $A[X]$ engendré par S. Alors $I' \subseteq I$ car $S \subseteq I$. Supposons que $I \neq I'$ et montrons qu'il y a une contradiction. Soit $P(X) = aX^d + ... + a_0 \in I \setminus I'$ de degré d minimal parmi les polynômes de $I \setminus I'$. On a $a \in J_d$. Supposons d'abord $d \leq N$. Alors $J_d = J_N$. Il existe donc $c_{N,1}, ..., c_{N,m_N} \in A$ tels que $a = \sum_{1 \leq j \leq m_d} c_{N,j} a_{N,j}$. Considérons

$$Q(X) := P(X) - \sum_{1 \leq j \leq m_N} c_{N,j} F_{N,j}(X) X^{d-N}.$$

Alors $Q(X) \in I \setminus I'$, $\deg Q(X) < d$. Impossible.

Supposons maintenant $d < N$. Comme pour J_N, il existe $c_{d,1}, ..., c_{d,m_d}$ tels que $a = \sum_{1 \leq j \leq m_d} c_{d,j} a_{d,j}$. Considérons

$$Q(X) := P(X) - \sum_{1 \leq j \leq m_d} c_{d,j} F_{d,j}(X).$$

Alors $Q(X) \in I \setminus I'$, $\deg Q(X) \leq d-1$. On a de nouveau une contradiction. □

Définition 1.1.7 Soit A un anneau. Une *A-algèbre* est un anneau B muni d'un homomorphisme d'anneaux $\phi : A \to B$.

Les exemples typiques sont les anneaux quotients de A, les anneaux de polynômes à coefficients dans A (la structure d'algèbre est donnée par $a \mapsto a$ polynôme constant), et les anneaux quotients de ces derniers. Tout anneau B contenant A comme sous-anneau est naturelement une A-algèbre.

Une extension de corps L/K correspond à une K-algèbre L qui est un corps, l'homomorphisme $K \to L$ qui définit la structure étant l'inclusion.

Soient $\phi : A \to B$ et $\psi : A \to C$ des A-algèbres. Un *homomorphisme de A-algèbres* $f : B \to C$ est un homomorphisme d'anneaux tel que $f \circ \phi = \psi$. Lorsque ϕ, ψ sont des inclusions, cela veut dire que $f|_A$ est égal à l'identité.

Soit $\phi : A \to B$ une A-algèbre. On a alors naturellement une structure de A-module sur B en posant pour la multiplication externe $a \star b = \phi(a)b$ pour tout $a \in A$ et pour tout $b \in B$. Une *A-algèbre finie* est une A-algèbre qui est de type fini en tant que A-module (avec la structure décrite ci-avant). On dit que B est une *A-algèbre de type fini* si B est isomorphe, en tant que A-algèbre, à un quotient d'un anneau de polynômes $A[T_1, \ldots, T_n]$.

Soit

$$F(T_1, \ldots, T_n) = \sum_{\nu \in \mathbb{N}^n} a_v T_1^{\nu_1} \cdots T_n^{\nu_n} \in A[T_1, \ldots, T_n].$$

Soient $b_1, \ldots, b_n \in B$. On note

$$F(b_1, \ldots, b_n) = \sum_{\nu \in \mathbb{N}^n} \phi(a_v) b_1^{\nu_1} \cdots b_n^{\nu_n} \in B.$$

C'est une "expression polynomiale" en les $b_1, \ldots, b_n$. On note $A[b_1, \ldots, b_n]$ l'ensemble de ces expressions polynomiales quand $F(T_1, \ldots, T_n)$ parcourt l'ensemble

$A[T_1, \ldots, T_n]$. C'est une sous-A-algèbre de B. Avec cette notation, on a B finie sur A s'il existe $b_1, \ldots, b_n \in B$ tels que

$$B = Ab_1 + \cdots + Ab_n.$$

Tandis que B est de type fini sur A s'il existe $b_1, \ldots, b_n \in B$ tels que

$$B = A[b_1, \ldots, b_n].$$

Ce qui est une condition plus faible qu'être finie.

Exemple 1.1.8 Tout anneau admet une unique structure de $\mathbb{Z}$-algèbre.

Corollaire 1.1.9. *Si A est noethérien (par exemple si c'est un corps ou un anneau principal), alors toute A-algèbre de type fini est un anneau noethérien.*

Exemple 1.1.10 L'anneau des polynômes $A[T]$ est naturellement une A-algèbre, de type fini par définition, mais pas finie. En effet, si $A[T]$ était engendré par $P_1(T), \ldots, P_n(T)$ en tant que A-module, alors tout élément de $A[T]$ serait de la forme $\sum_{1 \leq i \leq n} a_i P_i(T)$ avec $a_i \in A$, et serait de degré $\leq \max_i\{P_i(T)\}$. Absurde.

Exemple 1.1.11 Soit $P(T) = T^d + a_{d-1}T^{d-1} + \cdots + a_1 T + a_0 \in A[T]$. Alors $B = A[T]/(P(T)A[T])$ est une A-algèbre finie. En effet en utilisant la division euclidienne par $P(T)$ dans $A[T]$, ce qui est possible car $P(T)$ est unitaire, on voit que B est engendré comme A-module par la famille $\{1, t, \ldots, t^{d-1}\}$ où $t \in B$ est la classe de T modulo $P(T)A[T]$.

Exercice 1.1.12 Soit $F(T) = a_d T^d + a_{d-1}T^{d-1} + \cdots + a_1 T + a_0 A[T]$ un polynôme. Supposons que $B = A[T]/(F(T)A[T])$ soit fini sur A. Notons t la classe de T dans l'anneau quotient B.

1. Montrer qu'il existe $n > 0$ tel que $\{1, t, \ldots, t^{n-1}\}$ soit une famille génératrice de B comme A-module. En déduire qu'il existe un polynôme unitaire $P(T) \in A[T]$ de degré n tel que $P(t) = 0$.
2. Supposons de plus que A est intègre. Montrer que $F(T)$ est unitaire.

Soit B une A-algèbre et soit M un B-module. Alors M a naturellement une structure de A-module. Le produit externe étant défini par $a \times x = \phi(a)x$ si $\phi : A \to B$ définit la structure de A-algèbre sur B.

Proposition 1.1.13. *(Transitivité) Soit B une A-algèbre finie et soit M un B-module de type de fini. Alors M, en tant que A-module, est de type fini. En particulière, une algèbre finie sur B est une algèbre finie sur A.*

Démonstration. Soit $M = \sum_{1 \leq i \leq n} Bx_i$ et $B = \sum_{1 \leq j \leq m} Ab_j$. Alors

$$M = \sum_{1 \leq i \leq n; 1 \leq j \leq m} A(b_j x_i).$$

□

Corollaire 1.1.14. *Sous les hypothèses de la proposition, toute B-algèbre finie est aussi une A-algèbre finie.*

1.2 Modules sur un anneau principal

Rappelons qu'un anneau A est *principal* s'il est intègre, et si tout idéal de A est engendré par un élément. En général on convient implicitement que A *n'est pas un corps.* Exemples usuels : $\mathbb{Z}$, $K[x]$, $\mathbb{Z}[i]$. On en verra quelques autres. Mais parmi les anneaux d'entiers, il n'en existe pas beaucoup. Une façon de montrer qu'un anneau A est principal est de montrer qu'il est *euclidien*, c'est-à-dire qu'on a une division euclidienne sur l'anneau (c'est le cas des trois exemples précédents). Mais un anneau principal n'est pas nécessairement euclidien.

Les modules sur un anneau sont des généralisations des espaces vectoriels sur un corps. Mais contrairement aux espaces vectoriels, un module n'admet pas nécessairement une base. Par exemple $\mathbb{Z}/2\mathbb{Z}$ vu comme $\mathbb{Z}$-module est non nul, mais n'a aucune famille libre (tout vecteur x est "tué par 2" : $2x = 0$). Cependant, sur un anneau principal, la structure des modules est particulièrement simple. Soit A un anneau principal. Soit M un A-module. L'ensemble

$$M_t = \cup_{a\in A, a\neq 0}\{x \in M \ \mid \ ax = 0\}$$

est un sous-module de A, appelé la *torsion* de M. Si $A = \mathbb{Z}$, cela correspond aux éléments d'ordre fini dans le groupe abélien M. On dit que M est *sans torsion* si $M_t = \{0\}$. Les deux théorèmes qui suivent ont été vus au semestre d'automne.

Theorem 1.2.1. *Supposons A principal. Soit M un module de type fini sur A. Alors M/M_t est libre de rang fini, M_t est de type fini, et M est isomorphe (non canoniquement) à la somme directe*

$$M \simeq (M/M_t) \oplus M_t.$$

En particulier, M est libre si et seulement s'il est sans torsion sur A.

Theorem 1.2.2. (Base adaptée) *Soit M un module libre de rang fini m sur A. Soit N un sous-module de M. Alors N est libre de rang $n \leq m$. De plus il existe une base $\{e_1, \ldots, e_s, \ldots e_m\}$ de M et des éléments $a_1, \ldots, a_n \in A$ non nuls tels que*

$$N = \oplus_{1\leq i\leq n} a_i e_i A, \quad a_1 \mid a_2 \mid \cdots \mid a_n.$$

La suite décroissante des idéaux $a_1A \supseteq \cdots \supseteq a_nA$ est unique.

Remarque 1.2.3 Le théorème dit qu'un sous-module $N \subseteq M$ possède toujours une base de la forme $\{a_1e_1, \ldots, a_me_m\}$ pour un choix convenable des e_i. En revanche il est faux en générale qu'une base de N se complète en une base de M de cette façon, même à homothétie près. Prenons par exemple $M = \mathbb{Z}^3$ avec la base canonique $\epsilon_1, \epsilon_2, \epsilon_3$. Soit N le sous-module de M engendré par $f_1 := \epsilon_1, f_2 := \epsilon_1 + 2\epsilon_2 + 2\epsilon_3$. Ces derniers forment une base de N. Mais il n'existe pas de base e_1, e_2, e_3 de M et des $a_i \in \mathbb{Z}$ tels que $f_1 = a_1e_1, f_2 = a_2e_2$. C'est-à-dire qu'on ne peut pas imposer une base de N dans le théorème.

1.3 Rappel sur le lemme de Gauss dans les anneaux factoriels

On se donne un anneau factoriel A, de corps de fractions K.

Proposition 1.3.1. (Lemme de Gauss) *Soit A factoriel de corps des fractions K.*

(1) *Soient $F, G \in A[X]$ non nuls. Alors*

$$\mathrm{cont}(F(X)G(X)) = \mathrm{cont}(F(X))\mathrm{cont}(G(X))$$

(à association près).

(2) *Soit $f(X) \in K[X]$ non nul. Alors* $\mathrm{cont}(f(X)) \in K^*$ *est défini à multiplication par une unité de A près, et* $\mathrm{cont}(fg) = \mathrm{cont}(f)\mathrm{cont}(g)$.

(3) *Si $f(X) \in K[X]$ est unitaire, alors*

$$\mathrm{cont}(f(X)) \in A^{-1} := \{1/a \mid a \in A \setminus \{0\}\},$$

et on a $\mathrm{cont}(f(X)) = 1$ *si et seulement si $f(X) \in A[X]$.*

(4) *L'anneau $A[X]$ est factoriel. Ses éléments irréductibles sont les irréductibles de A et les polynômes $F(X) \in A[X]$ non constants irréductibles dans $K[X]$ et de contenu* 1.

Démonstration. (3) Attention, le contenu d'un polynôme est défini à multiplication par un élément inversible de A près. On écrit

$$f(X) = X^n + \frac{a_{n-1}}{a}X^{n-1} + \cdots + \frac{a_1}{a}X + \frac{a_0}{a}$$

avec $a, a_i \in A$ et $a \neq 0$. Alors

$$\mathrm{cont}(f) = \frac{\mathrm{cont}(af)}{a} = \frac{\mathrm{pgcd}\{a, a_{n-1}, \ldots, a_0\}}{a}.$$

Donc $1/\mathrm{cont}(f) \in A$. Si $\mathrm{cont}(f) = 1$, alors $\mathrm{pgcd}\{a, a_{n-1}, \ldots, a_0\} = a$, donc $a \mid a_i$ pour tout i et $f(X) \in A[X]$.

□

Chapitre 2

Extensions entières

2.1 Éléments entiers

Soient A un anneau intègre, sous-anneau d'un anneau intègre B. On peut donc considérer B comme une A-algèbre.

Définition 2.1.1 On dit qu'un élément $b \in B$ est *entier sur* A s'il existe un polynôme **unitaire** $P(X) \in A[X]$ tel que $P(b) = 0$. Autrement dit, s'il existe $a_0, ..., a_{d-1} \in A$ $(d \geq 1)$ tels que

$$b^d + a_{d-1}b^{d-1} + \cdots + a_0 = 0.$$

L'équation ci-dessus définit une *relation entière* de b sur A. Tout élément de A est entier sur A. On dit que B *est entier sur* A si tous ses éléments sont entiers sur A. On dira aussi que B est une *extension entière de* A.

Exemple 2.1.2 Les éléments $\sqrt{2}, i = \sqrt{-1}, \sqrt{2} + i, (\sqrt{5} + 1)/2$ sont entiers sur $\mathbb{Z}$: ce sont des zéros respectivement des polynômes

$$X^2 - 2,\ X^2 + 1,\ X^4 - 2X^2 + 9,\ X^2 - X - 1 \in \mathbb{Z}[X].$$

Par contre $\sqrt{2}/2 = 1/\sqrt{2}$ n'est pas entier sur $\mathbb{Z}$. Cela se montre directement en considérant une relation entière sur $\mathbb{Z}$. Voir aussi 2.1.4.

Lorsque A, B sont des corps, les éléments entiers sont les éléments algébriques. Mais lorsque A n'est pas un corps, il ne suffit pas que b soit zéro d'un polynôme non nul, car on ne peut pas rendre unitaire un polynôme non nul en divisant par le coefficient dominant.

Tout élément de B entier sur A est algébrique sur $\mathrm{Frac}(A)$. Réciproquement, quels sont les éléments de $\mathrm{Frac}(B)$ entiers sur A ?

Proposition 2.1.3. *Soit A un anneau factoriel de corps de fractions K. Soit L/K une extension de corps. Alors $b \in L$ est entier sur A si et seulement si son polynôme minimal $m(X)$ appartient à $A[X]$.*

Démonstration. Supposons que $b \in L$ soit entier sur A. Il existe un polynôme unitaire $F(X) \in A[X]$ qui annule b. On a $F(X) = m(X)g(X)$ pour un certain $g(X) \in K[X]$ unitaire. Or $\mathrm{cont}(m(X)), \mathrm{cont}(g(X)) \in A^{-1}$ et leur produit vaut 1, donc $\mathrm{cont}(m(X)) = 1$ et $m(X) \in A[X]$ (proposition 1.3.1(3)).

La réciproque est immédiate. □

Exemple 2.1.4 Le polynôme minimal de $\sqrt{2}/2$ est $X^2 - 1/4 \notin \mathbb{Z}[X]$. Donc $\sqrt{2}/2$ n'est pas entier sur $\mathbb{Z}$.

Exercice 2.1.5 Trouver l'ensemble des éléments entiers sur $\mathbb{Z}$ dans $\mathbb{Q}[\sqrt{d}]$ où $d \in \mathbb{Z}$ est sans facteur carré (c'est $\mathbb{Z}[(\sqrt{d}+1)/2]$ ou $\mathbb{Z}[\sqrt{d}]$ selon que $d \equiv 1 \mod 4$ ou non).

On sait que dans les extensions de corps, les éléments algébriques sont stables par addition et multiplication. Nous allons montrer la même propriété pour les éléments entiers.

Proposition 2.1.6. *Soient $A \subseteq B$ des anneaux intègres. Soit $b \in B$. Les conditions suivantes sont équivalentes :*

(i) *b est entier sur A ;*

(ii) *La sous-A-algèbre*

$$A[b] := \{F(b) \mid F(X) \in A[X]\}$$

de B est finie sur A ;

(iii) *Il existe un sous-A-module $M \neq 0$ de B de type fini sur A et stable par la multiplication par b.*

Démonstration. (i) $\Longrightarrow$ (ii). Soit $P(X) \in A[X]$ un polynôme unitaire que annule b. Par division euclidienne par $P(X)$, on est ramené à ne considérer que les $F(b)$ avec $\deg F(X) \leq d := \deg P(X)$. Donc $A[b]$ est engendré par $\{1, b, \ldots, b^{d-1}\}$.

(ii) $\Longrightarrow$ (iii). Prendre $E = A[b]$.

(iii) $\Longrightarrow$ (i). Soient $x_1, \ldots, x_n$ une famille génératrice de E en tant que A-module. Il existe une matrice $N = (a_{ij})_{1 \leq i,j \leq n} \in M_n(A)$ telle que

$$b.(x_1, \ldots, x_n)^t = N.(x_1, \ldots, x_n)^t.$$

Donc

$$D.(x_1, \ldots, x_n)^t = 0$$

où $D = bI_n - N \in M_n(B)$. Il suit que

$$^t\mathrm{com}(D).D.(x_1, \ldots, x_n)^t = 0$$

pour la comatrice de D (vues dans $M_n(\mathrm{Frac}(B))$, voir aussi §2.3.1). Donc $\det D \in A$ satisfait $(\det D)x = 0$ pour tout $x \in E$. Comme $E \neq 0$ et B est un anneau intègre, on en déduit que $\det D = 0$. Autrement dit, le polynôme caractéristique de D, élément de $\mathrm{Frac}(A)[T]$, s'annule en b. Mais ce polynôme caractéristique est unitaire et, par sa construction, est à coefficients dans A. Il suit que b est entier sur A. □

Remarque 2.1.7 L'équivalence entre (i) et (ii) ci-dessus est vraie pour toute A-algèbre B, sans hypothèse d'intégrité. Mais on a alors besoin d'une version de Cayley-Hamilton pour les modules sur un anneau quelconque. D'autre part, cette équivalence peut se démontrer directement sans passer par (iii). En effet si $A[b]$ est de type fini comme A-module, engendré par $P_1(b), \ldots, P_r(b)$, alors $A[b]$ est engendré par $1, b, \ldots, b^\delta$ comme A-module, où $\delta = \max_i\{\deg P_i(X)\}$. En écrivant $b^{\delta+1}$ comme une combinaison linéaire des puissances inférieures on voit que b est entier sur A.

L'utilité de (iii) est essentiellement pour le corollaire suivant quand A n'est pas noethérien.

Corollaire 2.1.8. *Soit $A \subseteq B$ comme avant. Si B est fini sur A, alors il est entier sur A.*

Démonstration. Cela résulte de 2.1.6(iii) en prenant $M = B$. □

Corollaire 2.1.9. *Soient $A \subseteq B \subseteq C$ des anneaux intègres.*

(1) *Soient $b_1, \ldots, b_n \in B$ entiers sur A. Alors*

$$A[b_1, \ldots, b_n] := \{F(b_1, \ldots, b_n) \mid F(X_1, \ldots, X_n) \in A[X_1, \ldots, X_n]\}$$

est fini (donc entier) sur A.

(2) *L'ensemble B_0 des éléments de B entiers sur A forment une sous-A-algèbre entière de B.*

(3) (Transitivité) *Supposons C entier sur B et B entier sur A. Alors C est entier sur A.*

Démonstration. (1) On a $A[b_1]$ fini sur A. Comme b_n est entier sur A donc entier sur $A[b_1, \ldots, b_{n-1}]$, on a $A[b_1, \ldots, b_n]$ fini sur $A[b_1, \ldots, b_{n-1}]$. On conclut par récurrence sur n en utilisant le corollaire 1.1.14.

(2) Résulte de (1). En effet il est clair que $A \subseteq B_0$. Si $b_1, b_2 \in B$, alors $b_1 + b_2, b_1 b_2 \in A[b_1, b_2]$ sont entiers sur A, donc appartiennent à B_0.

(3) Si $c \in C$ est entier sur B, on a une relation entière

$$c^n + b_{n-1}c^{n-1} + \cdots + b_0 = 0, \quad b_i \in B.$$

Alors c est entier sur $A[b_0, \ldots, b_{n-1}]$, donc $A[b_0, \ldots, b_{n-1}, c]$ est fini sur A et c est entier sur A. □

Exemple 2.1.10 Les nombres $\sqrt{2}, \sqrt{3}$ sont évidemment entiers sur $\mathbb{Z}$. Mais $\sqrt{2} + \sqrt{3}$ aussi, ce qui est moins évident *a priori*.

Exercice 2.1.11 Une preuve plus directe de 2.1.9. Soit $b \in B$ (B intègre) entier sur A. Soit $P(X) \in A[X]$ un polynôme unitaire qui s'annule en b.

1. Soient $\beta_1, \ldots, \beta_n \in \Omega$ les racines de $P(X)$ dans une clôture algébrique Ω de $K = \mathrm{Frac}(A)$. Alors $s_1(\beta_1, \ldots, \beta_n), \ldots, s_n(\beta_1, \ldots, \beta_n)$, où les $s_1, \ldots, s_n$ sont les polynômes symétriques élémentaires, appartiennent à A.

2. En déduire que pour tout $F(X_1, \ldots, X_n) \in A[X_1, \ldots, X_n]$ symétrique, $F(\beta_1, \ldots, \beta_n) \in A$.
3. Soit $H(X_1, \ldots, X_n) \in A[X_1, \ldots, X_n]$ et considérons

$$f(T) = \prod_{\sigma \in S_n} (T - H(\beta_{\sigma(1)}, \ldots, \beta_{\sigma(n)})) \in \Omega[T].$$

Montrer que les coefficients de $f(T)$ sont de polynômes symétriques en les $\beta_1, \ldots, \beta_n$. En déduire que $f(T) \in A[T]$ et que $H(\beta_1, \ldots, \beta_n)$ est entier sur A.

Définition 2.1.12 Soient K le corps des fractions de A, L/K une extension de corps. On appelle *clôture intégrale de A dans L* l'ensemble des éléments de L entiers sur A.C'est un sous-anneau de L contenant A et entier sur A.

Définition 2.1.13 Soit L un corps de nombres (extension finie de $\mathbb{Q}$). La clôture intégrale de $\mathbb{Z}$ dans L est appelée *l'anneau des entiers de L* et notée, dans ce cours, $\mathcal{O}_L$.

Exemple 2.1.14
1. L'anneau des entiers de $\mathbb{Z}$ est $\mathbb{Z}$ lui-même. En effet si $r \in \mathbb{Q}$ est entier sur $\mathbb{Z}$, comme son polynôme minimal sur $\mathbb{Q}$ est $X - r$, on a $r \in \mathbb{Z}$ par la proposition 2.1.3.
2. Soit $L = \mathbb{Q}[i]$ avec $i^2 = -1$. Si $x + yi \in \mathbb{Q}[i]$ est entier sur $\mathbb{Z}$, son polynôme minimal $X^2 - 2xX + (x^2 + y^2)$ doit appartenir à $\mathbb{Z}[X]$. Donc x et par suite y appartiennent à $\frac{1}{2}\mathbb{Z}$. On écrit $x = k/2, y = \ell/2$ avec $k, \ell \in \mathbb{Z}$. Alors $k^2 + \ell^2 \in 4\mathbb{Z}$. Cela implique que l'un des k, ℓ est pair, et aussi que l'autre est pair, donc $x, y \in \mathbb{Z}$. Inversement $\mathbb{Z}[i]$ est fini sur $\mathbb{Z}$ donc ses éléments sont entiers sur $\mathbb{Z}$. On voit ainsi que $\mathcal{O}_L = \mathbb{Z}[i]$ l'anneau des entiers de Gauss.

Définition 2.1.15 On dit qu'un anneau intègre A est *intégralement clos* si sa clôture intégrale dans $\mathrm{Frac}(A)$ est égale est à A lui-même.

Exemple 2.1.16 L'anneau $A := \mathbb{Z}[\sqrt{5}]$ n'est pas intégralement clos. En effet, $(1 + \sqrt{5})/2 \in \mathrm{Frac}(A)$ est entier sur $\mathbb{Z}$, donc entier sur A, mais il n'appartient pas à A.

Proposition 2.1.17. *Soit L une extension de* $\mathrm{Frac}(A)$*. Alors la clôture intégrale de A dans L est un anneau intégralement clos.*

Démonstration. Soit B la clôture intégrale de A dans L. Soit $c \in \mathrm{Frac}(B) \subseteq L$ entier sur B. Alors c est entier sur A d'après 2.1.9(3). Donc $c \in B$. □

Proposition 2.1.18. *Tout anneau factoriel (en particulier tout anneau principal) est intégralement clos.*

Démonstration. Soit $x \in K$ un élément entier sur A et non nul. On écrit $x = u/v$ avec u, v premiers entre eux. Soit une relation entière

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0, \quad a_i \in A.$$

Alors

$$u^n + a_{n-1}v(u^{n-1} + \cdots + a_0 v^{n-1}) = 0.$$

Si p est un diviseur premier de v, alors $p \mid u^n$, donc $p \mid u$. Ce qui est contraire à l'hypothèse u, v premiers entre eux. Il suit que v n'a pas de diviseur premier et donc $v \in A^*$. D'où $x \in A$. □

Remarque 2.1.19 Il existe des anneaux intégralement clos qui ne sont pas factoriels. C'est le cas par exemple de l'anneau $\mathbb{Q}[x, y, z]/(xy - z^2)$. Un anneau des entiers d'un corps de nombres $\mathcal{O}_L$ n'est presque jamais factoriel. On peut montrer qu'il est factoriel si et seulement s'il est principal. Ce qui est rarement vrai.

Nous avons une généralisation de la proposition 2.1.3 :

Proposition 2.1.20. *Soit A un anneau intégralement clos. Soient L/K une extension algébrique et $b \in L$ de polynôme minimal $m_b(X) \in K[X]$. Alors b est entier sur A si et seulement si $m_b(X) \in A[X]$.*

Démonstration. Supposons b entier sur A. Soient $b_1, \ldots, b_n$ les racines de $m_b(X)$ dans une clôture algébrique Ω de K. Pour tout $i \leq n$, par l'unicité du corps de rupture, il existe un K-ismorphisme $\sigma : K[b] \to K[b_i]$ qui envoie b sur b_i. Cet isomorphisme transforme une relation entière de b sur A en une relation entière de b_i sur A. Donc b_i est aussi entier sur A. Il suit de 2.1.9(2) que les coefficients $m_b(X) = \prod_i (X - b_i) \in K[X]$ sont entiers sur A, donc appartiennent à A. □

2.2 Norme, trace, discriminant

Dans ce paragraphe nous allons associer des invariants à des éléments entiers et aux extensions entières libres. Le but est de définir des invariants des corps de nombres qui permettent de les classifier.

2.2.1 Interlude sur les polynômes symétriques

Soient K un corps et $n \geq 1$. Un polynôme $P(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]$ est dit *symétrique* s'il est invariant par permutation des variables :

$$P(X_{\tau(1)}, \ldots, X_{\tau(n)}) = P(X_1, \ldots, X_n), \quad \text{pour tout } \tau \in S_n$$

(groupe symétrique). Par exemples, pour tout $1 \leq i \leq n$, les polynômes

$$s_i(X_1, \ldots, X_n) = \sum_{1 \leq j_1 < j_2 < \ldots < j_i \leq n} X_{j_1} \ldots X_{j_i}$$

sont symétriques et appelés les polynômes symétriques élémentaires.

Théorème 2.2.1. *L'ensemble des polynômes symétriques dans $K[X_1, \ldots, X_n]$ est égal à la sous-K-algèbre $K[s_1(X_1, \ldots, X_n), \ldots, s_n(X_1, \ldots, X_n)]$. Autrement dit, tout polynôme symétrique est une combinaison K-linéaire de produits de polynômes symétriques élémentaires.*

Sur un corps de caractéristique nulle, l'anneau des polynômes symétrique est également engendré par les polynômes de Newton $\sum_{1 \leq k \leq n} T_k^i$, $i = 1, 2, ..., n$.

Proposition 2.2.2. *Dans $K[X_1, \ldots, X_n][Y]$, on a*

$$\prod_{1 \leq i \leq n} (Y - X_i) = Y^n - s_1 Y^{n-1} + \cdots + (-1)^k s_k Y^{n-k} + (-1)^n s_n$$

(où il faut comprendre $s_i(X_1, \ldots, X_n)$ pour s_i.)

Corollaire 2.2.3 (Relations entre racines et coefficients)**.** *Soit*

$$P(X) = X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \in K[X].$$

Soient $x_1, \ldots, x_n$ les racines de $P(X)$ dans une clôture algébrique de K, comptées avec multiplicité. Alors

$$s_i(x_1, \ldots, x_n) = (-1)^i a_{n-i}, \quad i = 1, \ldots, n.$$

En particulier, $x_1 + \cdots + x_n = -a_{n-1}$ et $x_1 \cdots x_n = (-1)^n a_0$.

2.2.2 Le cas des extensions finies de corps

Dans ce sous-paragraphe et le suivant, nous allons donner des formules aussi simples que possibles pour le calcul de la trace et de la norme.

Proposition 2.2.4. *Soient L/K une extension finie, $x \in L$ et*

$$m_x(X) = X^n + a_{n-1} X^{n-1} + \cdots + a_0 \in K[X]$$

son polynôme minimal. Alors

(1)

$$\mathrm{Tr}_{K[x]/K}(x) = -a_{n-1}, \quad \mathrm{N}_{K[x]/K}(x) = (-1)^n a_0.$$

(2)

$$\mathrm{Tr}_{L/K}(x) = [L : K[x]] \mathrm{Tr}_{K[x]/K}(x), \quad \mathrm{N}_{L/K}(x) = \mathrm{N}_{K[x]/K}(x)^{[L:K[x]]}.$$

Démonstration. (1) La matrice de l'application K-linéaire $K[x] \to K[x]$ multiplication par x, dans la base $\{1, x, \ldots, x^{n-1}\}$, est la matrice compagnon de $m_x(X)$

$$M = \begin{pmatrix} 0 & 0 & 0 & ... & -a_0 \\ 1 & 0 & 0 & ... & -a_1 \\ \vdots & \vdots & \vdots & \vdots & \\ 0 & . & ... & 1 & -a_{n-1} \end{pmatrix}$$

Cela permet de conclure que $\mathrm{Tr}_{K[x]/K}(x) = \mathrm{Tr}(M) = -a_{n-1}$, $\mathrm{N}_{K[x]/K}(x) = \det(M) = (-1)^{n+1}(-a_0) = (-1)^n a_0$.

(2) Soit $e_1, \ldots, e_m$ une base de $L/K[x]$. Comme $\{1, x, \ldots, x^{n-1}\}$ est une base de $K[x]/K$, on obtient une base

$$\{e_1, xe_1, \ldots, x^{n-1}e_1\} \cup \{e_2, xe_2, \ldots, x^{n-1}e_2\} \cup \cdots \cup \{e_m, xe_m, \ldots, x^{n-1}e_m\}$$

de L/K. La matrice dans cette base de la multiplication par x dans L est la matrice diagonale par blocs

$$\begin{pmatrix} M & 0 & 0 & ... & 0 \\ 0 & M & 0 & ... & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & . & . & ... & M \end{pmatrix}$$

Cela implique immédiatement (2). □

Remarque 2.2.5 (Transitivité des traces et normes) La proposition 2.2.4 est un cas particulier du résultat suivant. Soient L/F, F/K des extensions finies de corps. Soit $x \in L$, alors on a

$$\mathrm{Tr}_{L/K}(x) = \mathrm{Tr}_{F/K}(\mathrm{Tr}_{L/F}(x)), \quad \mathrm{N}_{L/K}(x) = \mathrm{N}_{F/K}(\mathrm{N}_{L/F}(x)).$$

L'égalité sur les traces se démontre relativement aisément. Pour la norme, c'est une autre paire de manches. Voir Bourbaki : Algèbre 1, III, §9, n°4, Prop 6.

Définition 2.2.6 Soit $x \in L$ algébrique sur K. On fixe une clôture algébrique $\bar{K}$. Un *conjugué de* x dans $\bar{K}$ est une racine dans $\bar{K}$ du polynôme minimal $m_x(X) \in K[X]$. Un élément $y \in \bar{K}$ est un conjugué de x si et seulement s'il existe $K[x] \to \bar{K}$ qui envoie x sur y.

Corollaire 2.2.7. *Soient $x_1, \ldots, x_n$ les conjugués de x dans $\bar{K}$ (comptés avec multiplicité). Alors*

$$\mathrm{Tr}_{K[x]/K}(x) = x_1 + \cdots + x_n, \quad \mathrm{N}_{K[x]/K}(x) = x_1 x_2 \cdots x_n.$$

Cela résulte de la proposition 2.2.4 et des relations entre les racines et les coefficients de $m_x(X)$.

Exemple 2.2.8 Soit $K = \mathbb{Q}$, $p \geq 3$ premier et $L = \mathbb{Q}[\zeta_p]$ un corps cyclotomique, où $\zeta_p \in \mathbb{C}$ est une racine primitive p-ième de l'unité. Le polynôme minimal de ζ_p sur $\mathbb{Q}$ est

$$(X^p - 1)/(X - 1) = X^{p-1} + \cdots + X + 1.$$

Ce dernier est aussi le polynôme minimal de ζ_p^ℓ pour tous $1 \leq \ell \leq p-1$. Donc $\mathrm{Tr}_{L/\mathbb{Q}}(\zeta_p^\ell) = -1$. D'où une formule générale pour tous les éléments de L :

$$\mathrm{Tr}_{L/\mathbb{Q}}\Big(\sum_{0 \leq \ell \leq p-2} a_\ell \zeta_p^\ell\Big) = (p-1)a_0 - \sum_{1 \leq \ell \leq p-2} a_\ell.$$

Contrairement à la trace, la norme est en général moins aisée à calculer. On a $\mathrm{N}_{L/\mathbb{Q}}(\zeta) = (-1)^{p-1} = 1$. Le polynôme minimal de $\zeta_p - 1$ est

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

Donc $\mathrm{N}_{L/\mathbb{Q}}(\zeta_p - 1) = p$. On peut calculer similairement $\mathrm{N}_{L/\mathbb{Q}}(a\zeta_p + b)$ pour tous nombres rationnels $a, b \in \mathbb{Q}$.

2.2.3 Le cas des extensions séparables

On fixe un corps K et une clôture algébrique $\bar{K}$. Rappelons qu'un élément algébrique $x \in L$ est *séparable* sur K si son polynôme minimal est séparable (i.e. sans racine multiple dans $\bar{K}$). Une extension finie est dite séparable si tous ses éléments sont séparables. On sait que x séparable implique que $K[x]$ séparable. Sur un corps de caractéristique nulle, toute extension algébrique est séparable. Si L/F et F/K sont des extensions finies, alors L/K est séparable si et seulement si L/F et F/K sont séparables.

Soit L/K une extension finie. Les K-isomorphismes de L dans $\bar{K}$ s'appellent les *plongements de L dans $\bar{K}$*. On note $\mathrm{Isom}_K(L, \bar{K})$ l'ensemble de ces plongements. Rappelons aussi :

Theorem 2.2.9. *Soit L/K une extension finie.*

(1) *Si F/L est une extension finie, alors la restriction*

$$\mathrm{Isom}_K(F, \bar{K}) \to \mathrm{Isom}_K(L, \bar{K})$$

est une application surjective. Autrement dit, tout $\tau \in \mathrm{Isom}_K(L, \bar{K})$ s'étend (ou se relève) en un $\sigma \in \mathrm{Isom}_K(F, \bar{K})$.

(2) *Supposons de plus que L/K est séparable de degré n.*

   (a) (Théorème de l'élément primitif) Il existe $\theta \in L$ tel que $L = K[\theta]$.

   (b) Il existe exactement n plongements de L dans $\bar{K}$, et on a une bijection

$$\mathrm{Isom}_K(L, \bar{K}) \to \{\theta_1, \ldots, \theta_n\}, \quad \tau \mapsto \tau(\theta)$$

   avec l'ensemble $\theta_1, \ldots, \theta_n$ des conjugués de θ dans $\bar{K}$.

Lemme 2.2.10. *Soient F/K une extension finie galoisienne et L/K une sous-extension. Considérons la restriction*

$$r : \mathrm{Gal}(F/K) = \mathrm{Isom}_K(F, \bar{K}) \to \mathrm{Isom}_K(L, \bar{K}).$$

Alors pour tout $\tau \in \mathrm{Isom}_K(L, \bar{K})$, $r^{-1}(\tau)$ est de cardinal $[F : L]$.

Démonstration. On sait que r est surjective par 2.2.9(3). Si $\sigma_1, \sigma_2 \in \mathrm{Gal}(F/K)$, on a $r(\sigma_1) = r(\sigma_2)$ si et seulement si $(\sigma_1^{-1}\sigma_2)|_L = \mathrm{Id}_L$, ou de façon équivalente, $\sigma_1^{-1}\sigma_2 \in \mathrm{Gal}(F/L)$. Il suit que $r^{-1}(\tau)$ est en bijection avec $\mathrm{Gal}(F/L)$ qui a $[F : L]$ éléments. □

Theorem 2.2.11. *Soit L/K une extension séparable de degré n. Alors pour tout $x \in L$, on a*

$$\mathrm{Tr}_{L/K}(x) = \sum_{\tau \in \mathrm{Isom}_K(L,\bar{K})} \tau(x), \quad \mathrm{N}_{L/K}(x) = \prod_{\tau \in \mathrm{Isom}_K(L,\bar{K})} \tau(x).$$

Démonstration. Supposons d'abord L/K galoisienne. On a

$$\sum_{\sigma \in \mathrm{Gal}(L/K)} \sigma(x) = \sum_{\tau \in \mathrm{Isom}_K(K[x],\bar{K})} \Big(\sum_{\sigma|_{K[x]}=\tau} \sigma(x) \Big) =$$

$$= \sum_{\tau \in \mathrm{Isom}_K(K[x],\bar{K})} [L : K[x]]\tau(x) = [L : K[x]]\mathrm{Tr}_{K[x]/K}(x) = \mathrm{Tr}_{L/K}(x)$$

d'après 2.2.10, 2.2.7 et 2.2.4(2).

Dans le cas général, on considère la clôture galoisienne F/K de L/K. Soit $x \in L$. Alors

$$\sum_{\sigma \in \mathrm{Gal}(F/K)} \sigma(x) = [F : L] \sum_{\tau \in \mathrm{Isom}_K(L,\bar{K})} \tau(x)$$

en utilisant 2.2.10. De plus, d'après le cas galoisien, on a

$$\sum_{\sigma \in \mathrm{Gal}(F/K)} \sigma(x) = \mathrm{Tr}_{F/K}(x) = [F : K[x]]\mathrm{Tr}_{K[x]/K}(x)$$

et, par (2.2.4(2)),

$$\mathrm{Tr}_{L/K}(x) = [L : K[x]]\mathrm{Tr}_{K[x]/K}(x).$$

Il suit que

$$\mathrm{Tr}_{L/K}(x) = \mathrm{Tr}_{F/K}(x)/[F : L] = \sum_{\tau \in \mathrm{Isom}_K(L,\bar{K})} \tau(x).$$

L'égalité sur la norme se montre de la même façon. □

2.2.4 Discriminant

On fixe un corps K. Soit

$$\varphi : V \times V \to K$$

une forme bilinéaire symétrique sur un K-espace vectoriel V de dimension finie. Pour toute base $\varepsilon = \{e_1, \ldots, e_n\}$ de V, on définit le discriminant

$$\mathrm{disc}(\varphi, \varepsilon) = \det(\mathrm{Mat}(\varphi, \varepsilon) := \det(\varphi(e_i, e_j)) \in K.$$

On a φ non-dégénérée si et seulement si $\mathrm{disc}(\varphi, \varepsilon) \neq 0$. Si ε' est une famille de n vecteurs dans V, on a une matrice de passage U qui décrit les coordonnées de ε' dans la base ε. Alors

$$\mathrm{Mat}(\varphi, \varepsilon') = U.\mathrm{Mat}(\varphi, \varepsilon).{}^tU.$$

Par conséquent,

$$\mathrm{disc}(\varphi, \varepsilon') = \det(U)^2 \mathrm{disc}(\varphi, \varepsilon). \tag{2.1}$$

Supposons que φ soit non-dégénérée, donc $\mathrm{disc}(\varphi, \varepsilon) \in K^*$. De l'égalité ci-dessus on déduit alors deux informations. D'abord, la famille ε' est une base si et seulement si $\det(\varphi(e'_i, e'_j)) \in K^*$, et que si c'est le cas, alors $\mathrm{disc}(\varphi, \varepsilon')$ diffère de $\mathrm{disc}(\varphi, \epsilon)$ par un facteur multiplicatif qui est un carré de K^*. En particulier, si $K \subseteq \mathbb{R}$, alors le signe de $\mathrm{disc}(\varphi, \varepsilon)$ est indépendant du choix de la base.

Nous allons maintenant considérer une forme bilinéaire très concrète. Soit L/K une extension finie. On a une forme bilinéaire symétrique canonique

$$\mathrm{Tr}_{L/K} : L \times L \to K, \quad (x, y) \mapsto \mathrm{Tr}_{L/K}(xy).$$

Pour toute base ε de L/K, on pose

$$D_{L/K}(\varepsilon) = \mathrm{disc}(\mathrm{Tr}_{L/K}, \varepsilon) \in K.$$

Remarque 2.2.12 La forme bilinéaire $\mathrm{Tr}_{L/K}(\cdot, \cdot)$ induit une application K-linéaire $L \to L^\vee$ (le dual comme K-espace vectoriel), définie par $x \mapsto \mathrm{Tr}_{L/K}(x, \cdot)$. Le forme est non-dégénérée si et seulement si $L \to L^\vee$ est injective. Soit $x \in L$ non nul. Alors x appartient au noyau de $L \to L^\vee$ si et seulement si et seulement si $\mathrm{Tr}_{L/K}(xy) = 0$ pour tout $y \in L$. Ce qui revient à $\mathrm{Tr}_{L/K}(z) = 0$ pour tout $z \in L$. Donc si $\mathrm{car}(K) = 0$ ou si $\mathrm{car}(K) = p > 0$ est premier à $[L : K]$, alors car $\mathrm{Tr}_{L/K}(1) = [L : K] \neq 0 \in K$ et la forme bilinéaire trace est non-dégénérée.

Nous allons voir plus bas (théorème 2.2.14 (2)) que cette forme est non-dégénérée dès que L/K est séparable. On peut montrer que cette condition est aussi nécessaire pour la non-dégénérescence.

L'ensemble $\mathrm{App}(X, \bar{K})$ des applications d'un ensemble X donné dans $\bar{K}$ est naturellement un espace vectoriel sur $\bar{K}$. Lorsque $X = L$, on a le résultat suivant.

Lemme 2.2.13. (Dedekind) *Soit L/K une extension finie. Soient $\sigma_1, ..., \sigma_n \in \mathrm{Isom}_K(L, \bar{K})$ deux à deux distincts. Soient $\lambda_1, \ldots, \lambda_n$ des éléments de $\bar{K}$ tels que*

$$\sum_{1 \leq i \leq n} \lambda_i \sigma_i(x) = 0, \quad \forall x \in L.$$

Alors $\lambda_i = 0$ pour tout $i \leq n$. Autrement dit, la famille des σ_i est libre dans $\mathrm{App}(L, \bar{K})$.

Démonstration. Raisonnons par l'absurde. On peut supposer qu'il existe des $\lambda_1, \ldots, \lambda_m$ dans $\bar{K}$, non tous nuls, tels que $\sum_{1 \leq i \leq m} \lambda_i \sigma_i = 0$ et que m soit minimal pour cette propriété. Cela entraine que $\lambda_i \neq 0$ pour tout $i \leq m$. Fixons $y \in L$. Pour tout $x \in L$, on a

$$\sum_{1 \leq i \leq m} \lambda_i \sigma_1(y) \sigma_i(x) = 0, \qquad \sum_{1 \leq i \leq m} \lambda_i \sigma_i(y) \sigma_i(x) = 0$$

(car $\sigma_i(y)\sigma_i(x) = \sigma_i(yx)$). Donc

$$\sum_{2\leq i\leq m} \lambda_i(\sigma_1(y) - \sigma_i(y))\sigma_i(x) = 0.$$

Il suit de la minimalité de m que $\sigma_1(y) - \sigma_i(y) = 0$ pour tout $i \leq m$ et tout $y \in L$. Donc $m = 1$. Mais alors $\lambda_1 = 0$. Absurde. □

Theorem 2.2.14. *Soit L/K une extension finie séparable. Soit $\varepsilon = \{\varepsilon_i\}_{1\leq i\leq n}$ une base de L en tant que K-espace vectoriel et notons $\{\sigma_1, \ldots, \sigma_n\}$ les éléments de* $\mathrm{Isom}_K(L, \bar{K})$. *On a*

(1) $D_{L/K}(\varepsilon) = (\det(\sigma_i(\varepsilon_j))_{i,j})^2$ *et*

(2) $D_{L/K}(\varepsilon) \neq 0$. *Autrement dit, la forme trace* $\mathrm{Tr}_{L/K}$ *est non-dégénérée.*

Démonstration. (1) Soit $\{\sigma_1, \ldots, \sigma_n\}$ les plongements de L dans $\bar{K}$. On a

$$\mathrm{Tr}(\varepsilon_i\varepsilon_j) = \sum_{1\leq k\leq n} \sigma_k(\varepsilon_i\varepsilon_j) = \sum_{1\leq k\leq n} \sigma_k(\varepsilon_i)\sigma_k(\varepsilon_j).$$

Si $M = (\sigma_k(\varepsilon_i))_{k,i} \in M_{n\times n}(\bar{K})$, alors $(\mathrm{Tr}(\varepsilon_i\varepsilon_j))_{i,j} = M^t.M$. Ce qui implique (1).

(2) Si $D_{L/K} = 0$, alors les vecteurs ligne de la matrice M ci-dessus sont liées. Comme ε est une base de L/K, il existe $\lambda_1, \ldots, \lambda_n \in \bar{K}$, non tous nuls, tels que $\sum_{i\leq n} \lambda_i\sigma_i = 0$. Ce qui contredit le lemme de Dedekind ci-dessus. □

Remarque 2.2.15 En général $\det(\sigma_i(\varepsilon_j))_{i,j} \notin K$ même si son carré appartient à K^*.

Corollaire 2.2.16. *Soient $x_1, \ldots, x_n \in L$. Alors* $\det(\mathrm{Tr}(x_ix_j))_{i,j} \neq 0$ *si et seulement si $\{x_1, \ldots, x_n\}$ est une base de L/K.*

Nous allons donner des moyens de calculer concrètement le discriminant pour certains types de bases.

Définition 2.2.17 Soit $P(X) \in K[X]$ un polynôme unitaire de degré n. Soient $\alpha_1, \ldots, \alpha_n$ ses racines dans une clôture algébrique de K (comptées avec leurs multiplicités). Alors le *discriminant de $P(X)$* est

$$\mathrm{disc}(P) = \prod_{1\leq i<j\leq n} (\alpha_i - \alpha_j)^2 = (-1)^{n(n-1)/2} \prod_{1\leq i\neq j\leq n} (\alpha_i - \alpha_j).$$

C'est une fonction symétrique des racines de $P(X)$, donc $\mathrm{disc}(P) \in K$ par le théorème fondamental des polynômes symétriques (théorème 2.2.1). De plus, $\mathrm{disc}(P) \neq 0$ si et seulement si $P(X)$ est séparable.

Lemme 2.2.18. *Soit $P(X) \in K[X]$ comme ci-dessus. Alors*

$$\mathrm{disc}(P) = (-1)^{n(n-1)/2} \prod_{1\leq i\leq n} P'(\alpha_i).$$

Preuve: On a $P'(X) = \sum_{1\leq i\leq n} \prod_{j\neq i}(X-\alpha_j)$. Donc $P'(\alpha_i) = \prod_{j\neq i}(\alpha_i - \alpha_j)$. D'où

$$\prod_i P'(\alpha_i) = \prod_{1\leq i,j\leq n, i\neq j} (\alpha_i - \alpha_j) = (-1)^{n(n-1)/2}\mathrm{disc}(P).$$

Exemple 2.2.19 Le discriminant de $X^2 + aX + b$ est $a^2 - 4b$. En effet, $(\alpha_1 - \alpha_2)^2 = (\alpha_1 + \alpha_2)^2 - 4\alpha_1\alpha_2 = (-a)^2 - 4b$.

Exemple 2.2.20 Soit K un corps de caractéristique nulle et Soit $P(X) = X^n - 1 \in K[X]$. Soit $\mathbb{\mu}_n \subset \bar{K}$ l'ensemble des racines n-ièmes de 1. Alors $P'(\zeta) = n\zeta^{n-1}$ pour tout $\zeta \in \mathbb{\mu}_n$. Donc

$$(-1)^{n(n-1)/2}\mathrm{disc}(X^n - 1) = \prod_{\zeta\in\mathbb{\mu}_n} (n\zeta^{n-1}) = n^n(\prod_{\zeta\in\mathbb{\mu}_n} \zeta^{n-1}) = (-1)^{n^2-1}n^n$$

et $\mathrm{disc}(X^n - 1) = (-1)^{(n^2+n-2)/2}n^n$.

Exemple 2.2.21 Soit $P(X) = X^n + aX + b \in K[X]$ un polynôme. Alors

$$\mathrm{disc}(P(X)) = (-1)^{n(n-1)/2}(n^n b^{n-1} + (-1)^{n-1}(n-1)^{n-1}a^n).$$

On retrouve les formules connues pour $n = 2, 3$. Montrons cette formule. Le cas $a = 0$ se traite comme dans l'exemple précédent. Supposons donc $a \neq 0$.

Notons que si $P(X) = \prod_{1\leq i\leq n}(X-\alpha_i)$ est sa décomposition dans une clôture algébrique de K, alors pour $t \in K^*, b \in K$, on a

$$P(t^{-1}X - t^{-1}b) = \prod_{1\leq i\leq n} ((t^{-1}X - t^{-1}b) - \alpha_i)$$

et donc que

$$t^n P(t^{-1}X - t^{-1}b) = \prod_{1\leq i\leq n} (X - (t\alpha_i + b)).$$

En évaluant en $X = 0$, on obtient

$$\prod_i (t\alpha_i + b) = (-1)^n t^n P(-t^{-1}b). \tag{2.2}$$

On a

$$P'(\alpha_i) = n\alpha_i^{n-1} + a = \alpha_i^{-1}(n(-a\alpha_i - b) + a\alpha_i) = -\alpha_i^{-1}((n-1)a\alpha_i + b)$$

et donc

$$\prod_i P'(\alpha_i) = (-1)^n(\prod_i \alpha_i)^{-1} \prod_i ((n-1)a\alpha_i + b).$$

La formule désirée résulte alors du lemme 2.2.18 et de l'égalité (2.2) ci-dessus.

Proposition 2.2.22. *Soit $L = K[\alpha]$ une extension séparable. Soit $m_\alpha(X)$ le polynôme minimal de α. Alors $\varepsilon := \{1, \alpha, \ldots, \alpha^{n-1}\}$ est une base de L/K et on a*

$$D_{L/K}(\varepsilon) = \mathrm{disc}(m_\alpha(X)) = (-1)^{n(n-1)/2}\mathrm{N}_{L/K}(m'_\alpha(\alpha)).$$

Démonstration. La première égalité résulte du théorème 2.2.14(1) et de Vandermonde. La seconde égalité résulte du lemme précédent et du théorème 2.2.11. □

2.2.5 Plongements réels et imaginaires

Soit L un corps de nombres. Par l'égalité (2.1), le signe du discriminant $D_{L/\mathbb{Q}}(\varepsilon)$ est indépendant de la base ε. Nous allons déterminer ce signe.

Définition 2.2.23 Un plongement $\sigma \in \mathrm{Isom}_{\mathbb{Q}}(L, \overline{\mathbb{Q}})$ est dit *réel* si $\sigma(L) \subset \mathbb{R}$, et *imaginaire* sinon. On dit que L est *totalement réel* si tous les plongements sont réels et *totalement imaginaire* si tous les plongements sont imaginaires.

Proposition 2.2.24. *Soit $n = [L : \mathbb{Q}]$. Soient r_1 (resp. r_2') le nombre de plongements réels (resp. imaginairs). Si $L = \mathbb{Q}[\alpha]$, alors r_1 est le nombre de racines réelles du polynôme minimal $m_\alpha(X)$, et $r_2' = 2r_2$ est le nombre de racines imaginaires (non réelles) avec $r_2 \in \mathbb{N}$. Et on a*

$$n = r_1 + 2r_2.$$

Démonstration. Soit σ un plongement. Alors $\sigma(\alpha)$ est une racine de $m_\alpha(X)$ et $\sigma(L) = \mathbb{Q}[\sigma(\alpha)]$. Donc σ est réel si et seulement si $\sigma(\alpha) \in \mathbb{R}$. On compte ensuite le nombre de racines réelles et imaginaires de $m_\alpha(X)$. □

Notons que les nombres r_1, r_2 sont invariants par isomorphismes de $\mathbb{Q}$-extensions.

Exemple 2.2.25
1. $\mathbb{Q}[i]$ est totalement imaginaire ; $\mathbb{Q}[\sqrt{2}]$ est totalement réel.
2. Si $n \geq 3$, alors $\mathbb{Q}[\zeta_n]$ est totalement imaginaire.
3. Soit $L = \mathbb{Q}[\alpha]$, où α est une racine d'un polynôme $X^3 + aX + b \in \mathbb{Q}[X]$ supposé irréductible. Un plongement σ est déterminé par $\sigma(\alpha)$. Il y en a un qui est réel et deux qui sont imaginaires ou bien trois réels. Si le discriminant $-(4a^3 + 27b^2) > 0$, on sait que les trois racines sont réelles, et donc que L est totalement réel. Si le discriminant est < 0, la formule de Cardan montre qu'il existe une racine rélle et deux imaginaires, donc $r_1 = r_2 = 1$.

Exercice 2.2.26 Si $L/\mathbb{Q}$ est galoisien, alors L est totalement réel ou totalement imaginaire.

Proposition 2.2.27. *Le signe de $D_{L/\mathbb{Q}}(\varepsilon)$ est $(-1)^{r_2}$.*

Démonstration. Écrivons $L = \mathbb{Q}[\alpha]$. Soient

$$\alpha_1, \ldots, \alpha_{r_1}, \alpha_{r_1+1}, \bar{\alpha}_{r_1+1}, \ldots, \alpha_{r_1+r_2}, \bar{\alpha}_{r_1+r_2}$$

les racines du polynôme minimal $m(X)$ de α, ordonnées de cette manière. On a

$$\mathrm{disc}(m(X)) = c^2 \prod_{1 \leq i \leq r_2} (\alpha_{r_1+i} - \bar{\alpha}_{r_1+i})^2$$

avec un $c \in \mathbb{R}^*$. En effet,

$$\alpha_i - \alpha_j \in \mathbb{R}, \quad \text{si } 1 \leq i < j \leq r_1$$

$$(\alpha_i - \alpha_{r_1+j})(\alpha_i - \bar{\alpha}_{r_1+j}) \in \mathbb{R}, \quad \text{si } i \leq r_1, j \leq r_2$$

et

$$(\alpha_{r_1+i} - \alpha_{r_1+j})(\bar{\alpha}_{r_1+i} - \bar{\alpha}_{r_1+j}),\ (\alpha_{r_1+i} - \bar{\alpha}_{r_1+j})(\bar{\alpha}_{r_1+i} - \alpha_{r_1+j}) \in \mathbb{R}$$

si $1 \leq i < j \leq r_2$.

Or $(\alpha_{r_1+i} - \bar{\alpha}_{r_1+i})^2 \in \mathbb{R}$ est strictement négatif. Donc le signe du discriminant $D_{L/K}(\{1, \alpha, \ldots, \alpha^{n-1}\})$ est $(-1)^{r_2}$. Cela reste vrai pour toute base de $L/\mathbb{Q}$ par le théorème 2.2.14 (1). □

2.3 Applications aux extensions entières

Soit A un anneau intègre, B la clôture intégrale de A dans une extension L de $K = \mathrm{Frac}(A)$. Nous allons étudier la structure de B comme A-module (surtout quand L/K est séparable).

2.3.1 Généralités d'algèbre linéaire

Soit A un anneau (commutatif unitaire) et $M \in M_n(A)$ une matrice carrée d'ordre n à coefficients dans A. On définit

$$\mathrm{Tr}(M) = \sum_{1 \leq i \leq n} a_{ii} \in A, \quad \det M = \sum_{\gamma \in S_n} \varepsilon(\gamma) a_{\gamma(1)1} \cdots a_{\gamma(n)n} \in A$$

où S_n désigne le groupe symétrique de n éléments. Une fois le déterminant défini, on peut définir la comatrice $\mathrm{com}(M)$.

Soit $\varphi : A \to B$ un homomorphisme d'anneaux. Alors on a un homomorphisme d'anneaux (non-commutatifs !) $\tilde{\varphi} : M_n(A) \to M_n(B)$ défini par $\tilde{\varphi} : (a_{ij})_{i,j} \mapsto (\varphi(a_{ij}))_{i,j}$ Il est alors clair que $\mathrm{Tr}(\tilde{\varphi}(M)) = \varphi(\mathrm{Tr}(M))$ et que $\det(\tilde{\varphi}(M)) = \varphi(\det(M))$. De plus $\tilde{\varphi}(\mathrm{com}(M)) = \mathrm{com}(\tilde{\varphi}(M))$.

Proposition 2.3.1. *Soit A un anneau Soient $M, N \in M_n(A)$.*

(1) *Pour tout $a \in A$, on a $\mathrm{Tr}(aM + N) = a\mathrm{Tr}(M) + \mathrm{Tr}(N)$.*

(2) *On a $\det(MN) = \det(M)\det(N)$ et*

$$M.{}^t\mathrm{com}(M) = {}^t\mathrm{com}(M).M = \det(M) I_n.$$

(3) *Une matrice $U \in M_n(A)$ est inversible si et seulement si $\det(U) \in A^*$.*

(4) *Si $U \in M_n(A)$ est inversible, alors*

$$\det(UMU^{-1}) = \det M, \quad \mathrm{Tr}(UMU^{-1}) = \mathrm{Tr}(M).$$

Démonstration. (1) est une vérification directe. (2) Cela peut se vérifier directement à la main. Une autre méthode est de se ramener au cas connu des matrices à coefficients dans un corps. Considérons l'anneau $R = \mathbb{Z}[S_{ij}, T_{ij}]_{1 \leq i,j \leq n}$ des polynômes à $2n^2$ variables. Écrivons $M = (a_{ij})$ et $N = (b_{ij})$. Soit $\varphi : R \to A$

l'homomorphisme d'anneaux défini par $\varphi(S_{ij}) = a_{ij}$ et $\varphi(T_{ij}) = b_{ij}$. Soit $\tilde{M} = (S_{ij})_{i,j}, \tilde{N} = (T_{ij})_{i,j} \in M_n(R)$. Alors $\tilde{\varphi}(\tilde{M}) = M, \tilde{\varphi}(\tilde{N}) = N$. Pour vérifier les égalités de (2), il suffit de les vérifiers pour les matrices $\tilde{M}, \tilde{N}$ dans $M_n(R)$. Or R est un sous-anneau de son corps des fractions $\mathrm{Frac}(R)$. Les égalités désirées sont valides dans $M_n(\mathrm{Frac}(R))$, donc valides dans $M_n(R) \subseteq M_n(\mathrm{Frac}(R))$.

(3) Utiliser la comatrice.

(4) La formule sur le déterminant résulte de (2). Pour la trace, on procède comme dans (2). □

Corollaire 2.3.2. *Si M est libre de rang fini sur A, alors* Tr *et* det *sont définis pour les endomorphismes linéaires de M.*

Définition 2.3.3 Soient $A \subseteq B$ des anneaux intègres avec B libre de rang $n \geq 1$ sur A. Pour tout $b \in B$, la multiplication par b sur B, notée $[b]$ est un endomorphisme linéaire de B. On définit $\mathrm{Tr}_{B/A}(b)$ et $\mathrm{N}_{B/A}(b)$ comme étant $\mathrm{Tr}([b])$ et $\det([b])$ respectivement. Il faut noter que la définition dépend de B/A.

Exemple 2.3.4

1. $\mathrm{Tr}_{B/A}(a) = na, \mathrm{N}_{B/A}(a) = a^n$ pour tout $a \in A$.
2. Si $A = \mathbb{Z}$ et $B = \mathbb{Z}[i]$. Pour tous $k, \ell \in \mathbb{Z}$, $\mathrm{Tr}_{B/A}(k + \ell i) = 2k$, $\mathrm{N}_{B/A}(k + \ell i) = k^2 + \ell^2$ (on utilise la base $\{1, i\}$ de B sur A.

2.3.2 Finitude de la clôture intégrale

Proposition 2.3.5. *Soient A un anneau intègre, L une extension algébrique de $K = \mathrm{Frac}(A)$.*

(1) *Soit C la clôture intégrale de A dans L. Alors*

$$L = \left\{ \frac{c}{a} \;\middle|\; a \in A \setminus \{0\}, x \in C \right\}.$$

En particulier $L = \mathrm{Frac}(C)$.

(2) *Soit $A \subseteq B \subseteq L$ avec B anneau libre de rang n sur A et $L = \mathrm{Frac}(B)$. Alors $n = [L : K]$. De plus toute famille libre à n éléments de B (en tant que A-module) est une base de L comme K-espace vectoriel.*

Démonstration. (1) Soit $\beta \in L$. Soit

$$\beta^n + t_{n-1}\beta^{n-1} + \cdots + t_0 = 0, \quad t_i \in K$$

une relation algébrique de β sur K. Soit $a \in A$ non nul tel que $at_i \in A$ pour tout $i \leq n-1$ (un dénominateur commun des t_i). Alors $c := a\beta \in B$ et $\beta = c/a$.

(2) Soit $\alpha \in L$. Montrons d'abord que α peut s'écrire comme une fraction avec dénominateur dans A. On a $\alpha = c/b$ avec $b, c \in B$ et $b \neq 0$. Soit

$$b^m + a_{m-1}b^{m-1} + \cdots + a_1 b + a_0 = 0, \quad a_i \in A$$

une relation entière de degré m minimal. Alors $a_0 \neq 0$. Il suit que

$$\frac{c}{b} = \frac{c(-a_1 - \cdots - a_{m-1}b^{m-2} - b^{m-1})}{a_0}$$

est une fraction avec dénominateur dans A et numérateur dans B.

Soit $b_1, \dots, b_n$ une base de B sur A. Il suit immédiatement de ce qui précède que pour tout $\alpha \in L$, il existe $a \in A$ non nul et $a_1, \dots, a_n \in A$ tels que $a\alpha = \sum_{1 \leq i \leq m} a_i b_i$ et donc

$$\alpha = \sum_{1 \leq i \leq m} (a_i a^{-1}) b_i, \quad a_i a^{-1} \in K.$$

Donc $\{b_1, \dots, b_n\}$ est une famille génératrice de L/K. Elle est libre sur K car toute relation linéaire entre les b_i sur K induit une relation linéaire sur A en multipliant par un dénominateur commun des coefficients. Donc les b_i forment une base de L/K. Toute famille libre à n éléments de B est libre dans L/K comme on vient de voir. Elle est donc une base de L/K. □

Corollaire 2.3.6. *Sous les hypothèses de 2.3.5(3), pour tout $b \in B$, on a*

$$\mathrm{Tr}_{L/K}(b) = \mathrm{Tr}_{B/A}(b), \quad \mathrm{N}_{L/K}(b) = \mathrm{N}_{B/A}(b).$$

Démonstration. Soit $b_1, \dots, b_n$ une base de B sur A. D'après la proposition 2.3.5 ci-dessus, c'est aussi une base de L sur K. Les endomorphismes $[b]_B$ et B et $[b]_L$ de L ont la même matrice dans la base des b_i. Donc ils ont la même trace et le même déterminant. □

Le corollaire ci-dessus exige que B soit libre sur A. Cependant lorsque A est intégralement clos, on peut relaxer cette condition.

Proposition 2.3.7. *Soit A un anneau intégralement clos. Soit B la clôture intégrale de A dans L. Alors pour tout $b \in B$, $\mathrm{Tr}_{L/K}(b), \mathrm{N}_{L/K}(b) \in A$. De plus, $b \in B^*$ si et seulement si $\mathrm{N}_{L/K}(b) \in A^*$.*

Démonstration. La première partie résulte de la proposition 2.1.20. Supposons $b \in B^*$, d'inverse $c \in B$. Alors $\mathrm{N}_{L/K}(b), \mathrm{N}_{L/K}(c) \in A$ avec $\mathrm{N}_{L/K}(b)\mathrm{N}_{L/K}(c) = \mathrm{N}_{L/K}(bc) = 1$. Donc $\mathrm{N}_{L/K}(b) \in A^*$.

Inversement, supposons $\mathrm{N}_{L/K}(b) \in A^*$. Soit

$$X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in A[X]$$

le polynôme minimal de b sur K. Alors $a_0 = (-1)^n \mathrm{N}_{L/K}(b) \in A^*$ et la relation

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

implique que $b \in B^*$. □

Exemple 2.3.8 Les unités de $\mathbb{Z}[i]$ sont $\pm 1, \pm i$. En revanche, les unités d'une extension entière aussi simple que $\mathbb{Z}[\sqrt{2}]$ sont déjà plus compliquées à déterminées : il faut résoudre une équation de Pell-Fermat : $x^2 - 2y^2 = \pm 1$. On y reviendra au chapitre 5 (exemple 5.1.6).

Theorem 2.3.9. *Soit A un anneau intègre, noethérien et intégralement clos, soit L/K une extension finie séparable et soit B la clôture intégrale de A dans L. Alors B est finie sur A. En particulier, B est noethérien.*

Démonstration. Par 2.3.5, il existe une base $e_1, \dots, e_n$ de L/K constituée d'éléments $e_i \in B$. Par 2.2.14, la forme trace $\mathrm{Tr}_{L/K}$ est non-dégénrée. Il existe donc une base duale $e_1^\vee, \dots, e_n^\vee \in L$:

$$\mathrm{Tr}_{L/K}(e_i e_j^\vee) = \delta_{ij}, \quad 1 \leq i, j \leq n.$$

(En général, $e_i^\vee \notin B$.) Pour tout $b \in B$, il existe $\lambda_1, \dots, \lambda_n \in K$ tels que $b = \lambda_1 e_1^\vee + \cdots + \lambda_n e_n^\vee$. Donc $\lambda_j = \mathrm{Tr}_{L/K}(be_j) \in A$ (proposition 2.3.7). Donc

$$B \subseteq Ae_1^\vee + \cdots Ae_n^\vee.$$

Le membre de droite est un A-module de type fini. Comme A est noethérien, ce module est noethérien, donc B B est de type fini comme A-module (par suite c'est un A-module noethérien).

Tout idéal de B est un sous-A-module de B, donc de type fini sur A et *a fortiori* de type fini sur B. Ce qui implique que B est un anneau noethérien. □

Remarque 2.3.10 Le théorème 2.3.9 est faux sans l'hypothèse L/K séparable ou sans l'hypothèse A intégralement clos.

Corollaire 2.3.11. *Soit L un corps de nombres. Alors l'anneau des entiers $\mathcal{O}_L$ (2.1.13) de L est noethérien, intégralement clos, libre de rang $[L : \mathbb{Q}]$ sur $\mathbb{Z}$.*

2.3.3 Discriminant des extensions entières

Définition 2.3.12 Soit L un corps de nombres. Une base de $\mathcal{O}_L$ sur $\mathbb{Z}$ est appelée une *base d'entiers* de L.

Tout comme les bases des espaces vectoriels, les bases d'entiers sont extrêmement utiles pour l'étude des anneaux d'entiers. Étant donné L, comment trouver une base d'entiers ? Dans ce qui suit, nous verrons quelques conditions suffisantes pour qu'une famille soit une base.

Soit B un anneau intègre, libre de rang n sur un sous-anneau A. Soit ε une base de B. Posons

$$D_{B/A}(\varepsilon) = \det(\mathrm{Tr}_{B/A}(\varepsilon_i \varepsilon_j))_{i,j}.$$

Si ε' est une famille de n éléments dans B, et si $U \in M_n(A)$ est la matrice des coordonnées des ε'_i dans ε, alors comme pour les extensions de corps, on a

$$D_{B/A}(\varepsilon') = (\det U)^2 D_{B/A}(\varepsilon)$$

(où $D_{B/A}(\varepsilon')$ est défini de même façon que $D_{B/A}(\varepsilon)$). Si $D_{B/A}(\varepsilon) \neq 0$, alors ε' est une base de B si et seulement si $\det U \in A^*$.

Remarque 2.3.13 Sous les hypothèses ci-dessous, ε est aussi une base de $L := \mathrm{Frac}(B)$ sur K (2.3.5(3)). Pour tout élément $b \in B$, $\mathrm{Tr}_{B/A}(b) = \mathrm{Tr}_{L/K}(b)$ (corollaire 2.3.6) et donc $D_{L/K}(\varepsilon) = D_{B/A}(\varepsilon)$. En particulier, $D_{B/A}(\varepsilon) \neq 0$ si L/K est séparable.

Corollaire 2.3.14. *Soit L un corps de nombres. Alors $D_{\mathcal{O}_L/\mathbb{Z}}(\varepsilon) \in \mathbb{Z}$ est indépendant du choix d'une base ε.*

L'entier $D_{\mathcal{O}_L/\mathbb{Z}} := D_{\mathcal{O}_L/\mathbb{Z}}(\varepsilon)$ s'appelle le *discriminant* de L. Il est invariant par $\mathbb{Q}$-isomorphismes. On le note parfois $D_{L/\mathbb{Q}}$ ou même d_L dans les moments de grande paresse.

Proposition 2.3.15. *Soit L un corps de nombres. Soit $\underline{b} = \{b_1, \ldots, b_n\}$ une famille de $n = [L : \mathbb{Q}]$ éléments de $\mathcal{O}_L$. Si $D_{L/\mathbb{Q}}(\underline{b}) \in \mathbb{Z}$ est non nul, sans facteur carré, alors $\underline{b}$ est une base de $\mathcal{O}_L$ sur $\mathbb{Z}$.*

Démonstration. En effet, si $U \in M_n(\mathbb{Z})$ est la matrice qui exprime $\underline{b}$ en fonction d'une base ε, on a

$$D_{\mathcal{O}_L/\mathbb{Z}}(\underline{b}) = \det(U)^2 D_{\mathcal{O}_L/\mathbb{Z}}.$$

Donc $\det(U) = \pm 1$ et U est inversible dans $M_n(\mathbb{Z})$. □

Exemple 2.3.16 Soit d un entier relatif sans facteur carré et différent de 1. Soit $L = \mathbb{Q}[\sqrt{d}]$. Si $d \equiv 1 \mod 4$. On écrit $d = 4m + 1$. Soit $\alpha = (\sqrt{d} - 1)/2$. Le polynôme minimal de α sur $\mathbb{Q}$ est $X^2 + X - m$. Il suit que $D_{\mathcal{O}_L/\mathbb{Z}}(\{1, \alpha\}) = \mathrm{disc}(X^2 + X - m) = d$ est sans facteur carré. Donc $\mathcal{O}_L = \mathbb{Z}[\alpha]$ et $D_{\mathcal{O}_L/\mathbb{Z}} = d$.

Exemple 2.3.17 Soit $L = \mathbb{Q}[\alpha]$ avec $\alpha \in \mathbb{C}$ une racine de $X^5 - X - 1$ (dont on prouve l'irréductibilité directement en partant d'une décomposition $(X^2 + aX + b)(X^3 - aX^2 + cX - b)$ dans $\mathbb{Z}[X]$). Soit $\underline{b} = \{1, \alpha, \ldots, \alpha^4\}$. Alors $D_{L/\mathbb{Q}}(\underline{b}) = (-1)^{10}\mathrm{disc}(X^5 - X - 1) = 19.151$ (exemple 2.2.21 ou utiliser le logiciel pari, commande `poldisc` sous `gp`). Cela montrer que $\underline{b}$ est une base de $\mathcal{O}_L$ et donc aussi $\mathcal{O}_L = \mathbb{Z}[\alpha]$.

Exemple 2.3.18 Soit $A = \mathbb{Z}$, $B = \mathbb{Z}[\zeta_p]$ avec $p > 2$ premier. Considérons la base $\varepsilon = \{1, \zeta_p, \ldots, \zeta_p^{p-2}\}$ de B sur A. Alors

$$D_{B/\mathbb{Z}}(\varepsilon) = (-1)^{(p-1)(p-2)/2} N_{\mathbb{Q}[\zeta_p]/\mathbb{Q}}(\Phi_p'(\zeta_p)).$$

On a $(X - 1)\Phi_p(X) = X^p - 1$, donc

$$(X - 1)\Phi_p'(X) + \Phi_p(X) = pX^{p-1}$$

et

$$\Phi_p'(\zeta_p) = p\frac{\zeta_p^{p-1}}{\zeta_p - 1}, \quad N_{\mathbb{Q}[\zeta_p]/\mathbb{Q}}(\Phi_p'(\zeta_p)) = p^{p-1}\frac{1}{p} = p^{p-2}$$

(exemple 2.2.8). Notons que $p - 2$ étant impair et $(p - 1)/2 \in \mathbb{N}$, le signe de $D_{\mathbb{Q}[\zeta_p]/\mathbb{Q}}$ est $(-1)^{(p-1)/2}$. Par ailleurs, tous les conjugués de ζ_p sont des nombres

imaginaires. Donc $\mathbb{Q}[\zeta_p]$ est totalement imaginaire, de degré $(p-1)/2$ sur $\mathbb{Q}$. Cela confirme la proposition 2.2.27.

On montrera (proposition 5.2.7) que $\mathbb{Z}[\zeta_p]$ est égal à l'anneau des entiers de $\mathbb{Q}[\zeta_p]$. Il suit que

$$D_{\mathcal{O}_L/\mathbb{Z}} = (-1)^{(p-1)/2} p^{p-2}$$

si $L = \mathbb{Q}[\zeta_p]$.

Le cas complémentaire à l'exemple 2.3.16, c'est-à-dire le cas de $\mathbb{Q}[\sqrt{d}]$ avec $d \equiv 2, 3 \mod 4$ sera traité avec la proposition qui suit.

Proposition 2.3.19. (Stickelberger) *Soit L un corps de nombres. Alors on a $D_{\mathcal{O}_L/\mathbb{Z}} \equiv 0$ ou $1 \mod 4$.*

Démonstration. Soit $\varepsilon_1, \ldots, \varepsilon_n$ une base de $\mathcal{O}_L$ sur $\mathbb{Z}$. Soient $\sigma_1, \ldots, \sigma_n$ les éléments de $\mathrm{Isom}_{\mathbb{Q}}(L, \bar{\mathbb{Q}})$. Notons N la clôture galoisienne de L dans $\mathbb{Q}$. Alors $D_{\mathcal{O}_L/\mathbb{Z}} = (\det M)^2$ où $M = (\sigma_i(\varepsilon_j))_{i,j} \in M_n(N)$. On peut écrire $\det M = P - I$ où P est la somme des termes (lorsque l'on développe le déterminant, voir le début du §2.3.1) correspondant aux permutations de signature 1 et I les autres. Concrètement,

$$P = \sum_{\gamma \in A_n} \prod_{1 \le i \le n} \sigma_{\gamma(i)}(\varepsilon_i), \quad I = \sum_{\gamma \in S_n^-} \prod_{1 \le i \le n} \sigma_{\gamma(i)}(\varepsilon_i).$$

où S_n^- désigne les permutations de signature -1. Alors

$$(\det M)^2 = (P - I)^2 = (P + I)^2 - 4PI.$$

Il suffit de montrer que $P + I, PI \in \mathbb{Z}$, ou même que $P + I, PI \in \mathbb{Q}$ car ce sont des éléments de $\mathcal{O}_N$ et on a $\mathcal{O}_N \cap \mathbb{Q} = \mathbb{Z}$.

Pour tout $\tau \in \mathrm{Gal}(N/\mathbb{Q})$, l'application

$$\mathrm{Isom}_{\mathbb{Q}}(L, \bar{\mathbb{Q}}) \to \mathrm{Isom}_{\mathbb{Q}}(L, \bar{\mathbb{Q}}), \quad \sigma \mapsto \tau \circ \sigma$$

est une bijection. Fixons $\tau \in \mathrm{Gal}(N/\mathbb{Q})$. Il existe donc $\gamma_\tau \in \mathcal{S}_n$, dépendant de τ, tel que $\tau\sigma_i = \sigma_{\gamma_\tau(i)}$ pour tout $i \le n$. Alors ou bien $\tau(P) = P, \tau(I) = I$ (si $\gamma_\tau \in S_n$ est de signature 1), ou bien $\tau(P) = I, \tau(I) = P$ (si γ_τ est de signature -1). En effet,

$$\tau(P) = \sum_{\gamma \in A_n} \prod_{1 \le i \le n} \sigma_{\gamma_\tau \circ \gamma}(\varepsilon_i) = \sum_{\gamma' \in \gamma_\tau A_n} \prod_{1 \le i \le n} \sigma_{\gamma'}(\varepsilon_i)$$

et

$$\tau(I) = \sum_{\gamma' \in \gamma_\tau S_n^-} \prod_{1 \le i \le n} \sigma_{\gamma'}(\varepsilon_i).$$

Dans les deux cas, $P + I, PI$ sont invariants par τ. Ils appartiennent donc à $\mathbb{Q}$. □

Corollaire 2.3.20. *Si $[L : \mathbb{Q}] = n$ et si une famille de n éléments dans $\mathcal{O}_L$ a son discriminant égal à $4d$ avec d un entier non nul sans facteur carré et $d \equiv 2, 3 \mod 4$, alors cette famille est une base de $\mathcal{O}_L$.*

Démonstration. Sinon, le discriminant de cette famille est égal à $a^2 D_{\mathcal{O}_L/\mathbb{Z}}$ pour un carré $a^2 > 1$. Donc $a = 2$ et $D_{\mathcal{O}_L/\mathbb{Z}} = d$. Ce qui est impossible d'après Stickelberger. □

Exemple 2.3.21 Si $d \neq 0$ est un entier sans facteur carré, congru à 2 ou 3 mod 4, et $L = \mathbb{Q}[\sqrt{d}]$, on a

$$D_{\mathcal{O}_L/\mathbb{Z}}(\{1, \sqrt{d}\}) = 4d.$$

Donc $\mathcal{O}_L = \mathbb{Z}[\sqrt{d}]$. Cela peut cependant se montrer par un calcul simple. Notons que toute extension quadratique de $\mathbb{Q}$ est de la forme $\mathbb{Q}[\sqrt{d}]$ pour un entier $d \neq 0$ sans facteur carré.

En général c'est une question difficile de trouver une base d'entier d'un anneau d'entiers. Pour des calculs concrèts, on peut utiliser par exemple le logiciel `pari` ou `Sage`.

Chapitre 3

Anneaux de Dedekind

Les anneaux de Dedekind sont des généralisations des anneaux d'entiers de corps de nombres. Cette notion est plus souple que celle des anneaux d'entiers. Elle inclut en particulier les localisations des anneaux d'entiers. Elle inclut aussi des anneaux qui proviennent de la géométrie algébrique. Il est souvent plus agréable de travailler dans ce cadre plus général.

3.1 Décomposition des idéaux

3.1.1 Anneaux de Dedekind, définition et exemples

Définition 3.1.1 Un anneau intègre A est un *anneau de Dedekind* s'il est

1. noethérien et intégralement clos,
2. *de dimension de Krull* 1 : les idéaux premiers non nuls de A sont maximaux et A n'est pas un corps (ce qui équivaut à l'existence d'un idéal maximal non nul).

Exemple 3.1.2 Tout anneau principal A qui n'est pas un corps (*e.g.* $\mathbb{Z}$) est un anneau de Dedekind. En effet, tout idéal premier non nul est engendré par un élément irréductible f. Si $fA \subseteq I = f'A$, alors $f' \mid f$, donc f' est inversible ou associé à f, donc $I = A$ ou fA. Ce qui montre que fA est maximal.

La proposition suivante donne une méthode générale pour construire des anneaux de Dedekind.

Proposition 3.1.3. *Soient A un anneau de Dedekind, L une extension finie séparable de A et B la clôture intégale de A dans L. Alors B est un anneau de Dedekind. En particulier, les anneaux d'entiers sont des anneaux de Dedekind.*

De plus pour tout idéal maximal $\mathfrak{q}$ de B, l'intersection $\mathfrak{q} \cap A$ est un idéal maximal de A.

Démonstration. Par construction, B est intégralement clos. On a vu dans 2.3.9 que B est noethérien et fini sur A. Soit $\mathfrak{q}$ un idéal premier non nul de B. Alors

$\mathfrak{p} := \mathfrak{q} \cap A$ est un idéal premier de A. Montrons qu'il est non nul. Soit $b \in \mathfrak{q}$ non nul. Il vérifie une relation entière

$$b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0 = 0$$

avec $a_i \in A$. On peut supposer $a_0 \neq 0$ car sinon on peut simplier l'égalité par b et en obtenir une nouvelle de degré $n-1$. Il suit alors que $a_0 \in \mathfrak{q} \cap A$ et est non nul. Par suite $\mathfrak{p}$ est un idéal maximal de A. L'homomorphisme canonique $A/\mathfrak{p} \to B/\mathfrak{q}$ est injectif et fini, et fait donc de $B/\mathfrak{q}$ un anneau intègre fini sur un corps. C'est donc un corps (voir le lemme ci-après), et $\mathfrak{q}$ est maximal.

Il reste à montrer que B n'est pas un corps. Comme A n'en est pas un, il existe $a \in A$ non nul et non inversible. Si B était un corps, alors $1/a \in B$ et serait entier sur A, donc $1/a \in A$ puisque A est intégralement clos et donc $a \in A^*$, contradiction. □

Lemme 3.1.4. *Soit C un anneau intègre contenant un corps K. Supposons que C soit de dimension finie en tant que K-espace vectoriel. Alors C est un corps.*

Démonstration. Soit $c \in C$ non nul. Alors l'application $[c] : C \to C$, $x \mapsto cx$ est K-linéaire et injective, c'est donc un isomorphisme. L'antécédent de 1_C par cette application est l'inverse de c. Donc C est un corps. □

Corollaire 3.1.5. *L'anneau d'entiers $\mathcal{O}_L$ d'un corps de nombres est un anneau de Dedekind.*

La classe des anneaux principaux qui ne sont pas des corps est contenue dans celle des anneaux de Dedekind. Nous allons voir que cette inclusion est stricte.

Exemple 3.1.6 Soit $L = \mathbb{Q}[\sqrt{-5}]$. Montrons que 2 est irréductible mais pas premier dans $\mathcal{O}_L$. Comme $-5 \equiv 3 \mod 4$, on a $\mathcal{O}_L = \mathbb{Z}[\sqrt{-5}]$ (exemple 2.3.21). Montrons que 2 est un élément irréductible de $\mathcal{O}_L$. Soit

$$2 = (a + b\sqrt{-5})(c + d\sqrt{-5}), \quad a, b, c, d \in \mathbb{Z}.$$

En prenant la norme sur $\mathbb{Z}$, on obtient

$$4 = (a^2 + 5b^2)(c^2 + 5d^2).$$

Comme $5 > 1$, on a $b = d = 0$ et $2 = \pm ac$. Il suit que $a + b\sqrt{-5}$ ou $c + d\sqrt{-5}$ est égal à ± 1 et est inversible. Cela montre que 2 est irréductible dans $\mathcal{O}_L$. On a

$$(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6 \in 2\mathcal{O}_L,$$

mais $1 + \sqrt{-5},\ 1 - \sqrt{-5} \notin 2\mathcal{O}_L = 2\mathbb{Z} + 2\mathbb{Z}[\sqrt{-5}]$. Donc $2\mathcal{O}_L$ n'est pas un idéal premier et 2 n'est pas premier. On conclut que $\mathcal{O}_L$ n'est pas factoriel, et donc *a fortiori* pas principal.

Exemple 3.1.7 Il existe des exemples d'anneaux de Dedekind qui proviennent de la géométrie algébrique. Si $P(X, Y) \in \mathbb{C}[X, Y]$ est un polynôme irréductible tel que $P, \partial P/\partial X$ et $\partial P/\partial Y$ n'ont pas de zéro commun dans $\mathbb{C}^2$, alors on peut montrer que l'anneau quotient $\mathbb{C}[X, Y]/P(X, Y)\mathbb{C}[X, Y]$ est un anneau de Dedekind.

Exercice 3.1.8 Soit $f(X) \in \mathbb{C}[X]$ un polynôme non constant et sans racine multiple. Montrer que $\mathbb{C}[X,Y]/P(X,Y)\mathbb{C}[X,Y]$, où $P(X,Y) = Y^2 - f(X)$, est un anneau de Dedekind.

3.1.2 Idéaux fractionnaires

Rappelons que dans un anneau A, on définit le produit de deux idéaux I, J comme étant l'ensemble des sommes finies d'éléments de la forme xy avec $x \in I, y \in J$. C'est l'idéal de A engendré par les xy, $x \in I, y \in J$. En général IJ est strictement plus grand que cet ensemble des xy. Mais si $I = aA$, alors $IJ = \{ay \mid y \in J\}$.

Nous allons montrer que dans un anneau de Dedekind, tout idéal non nul s'écrit comme un produit d'idéaux premiers, de façon unique à permutation près, exactement comme tout entier strictement positif s'écrit comme un produit de nombres premiers.

Un outil technique de base pour la preuve est la théorie des « idéaux fractionnaires ». L'ensemble des idéaux de A forme un « monoide » commutatif unitaire avec A comme élément neutre. Le seul élément ayant un inverse est A lui-même. Ce monoide est donc très d'être un groupe. Cependant, à l'instar de $\mathbb{N}$, en élargissant ce monoide aux idéaux fractionnaires, on obtient un groupe si A est un anneau de Dedekind.

Définition 3.1.9 Soient A un anneau noethérien intègre. Soit $K = \mathrm{Frac}(A)$. Un *idéal fractionnaire* de A est un sous-A-module non nul M de K de type fini.

Exemple 3.1.10
1. Il suit de la définition que les idéaux fractionnaires contenus dans A sont exactement les idéaux non nuls de A.
2. Soit $\alpha \in K^*$, soit I un idéal non nul de A. Alors $\alpha I := \{\alpha x \mid x \in I\}$ est un idéal fractionnaire. Les idéaux fractionnaires de la forme αA sont appelés *idéaux fractionnaires principaux.*

Proposition 3.1.11. *Soit M un sous-A-module de K. Les propriétés suivantes sont équivalentes.*

(i) *M est un idéal fractionnaire ;*

(ii) *il existe $\alpha \in K^*$ et un idéal I de A tels que $M = \alpha I$;*

(iii) *il existe $\alpha \in K^*$ tel que $M \subseteq \alpha A$.*

Démonstration. (i) $\Longrightarrow$ (ii). Soient $x_1, x_2, \ldots, x_n \in K$ des générateurs du A-module M. Il existe $a \in A$ non nul tel que $ax_i \in A$ pour tout $i \leq n$. Il suit que $I := aM \subseteq A$. C'est un sous-A-module de A, donc un idéal, et on a $M = a^{-1}I$.

(ii) implique trivialement (iii). Enfin (iii) implique (i) car αA est un A-module de type fini. Comme A est noethérien, cela implique que M est de type fini. □

Définition 3.1.12 Soient M, N deux idéaux fractionnaires. On définit le produit MN comme étant le sous-A-module de K engendré par les éléments xy

avec $x \in M, y \in N$. Si $M = \alpha I$ et $N = \beta J$, alors $MN = (\alpha\beta)IJ$ est aussi un idéal fractionnaire. On a $(\alpha A)(\beta A) = (\alpha\beta)A$.

Si M, N sont des idéaux de A, cette définition coincide avec celle des produits d'idéaux.

Si $\alpha \in K^*$, on note $\alpha M = \{\alpha x \mid x \in M\}$ le produit des idéaux fractionnaires αA et M.

ATTENTION : en général l'ensemble des xy est strictement plus petit que MN.

Exemple 3.1.13 Tout idéal fractionnaire M de $\mathbb{Z}$ est de la forme $M = r\mathbb{Z}$ pour un nombre rationnel $r \in \mathbb{Q}$ non nul.

On note $I(A)$ l'ensemble des idéaux frationnaires de A. Le produit des idéaux fractionnaires est clairement commutatif et associatif, avec l'idéal A comme élément neutre. Nous allons montrer que le produit fait de $I(A)$ un groupe commutatif. Pour tout idéal fractionnaire, notons

$$M^{-1} := \{x \in K \mid xM \subseteq A\}.$$

C'est un idéal fractionnaire car c'est un sous-A-module de K et si $M \subseteq \alpha A$, alors $M^{-1} \subseteq \alpha^{-1}A$. Ce sera l'inverse de M pour le produit dans $I(A)$.

Lemme 3.1.14. *Soient A un anneau noethérien et I un idéal non nul de A.*

(1) *Alors I contient un produit $\mathfrak{p}_1 \cdots \mathfrak{p}_n$ d'idéaux premiers non nuls (non nécessairement distincts).*

(2) *Si A est un anneau de Dedekind, alors tout idéal maximal de A contenant I est égal à un des $\mathfrak{p}_i$ ci-dessus.*

Démonstration. (1) Considérons l'ensemble $\mathcal{S}$ des idéaux non nuls de A ne vérifiant pas la propriété énoncée et supposons cet ensemble non vide. Comme A est noethérien, cet ensemble admet un élément maximal (pour l'inclusion) I. Par définition de $\mathcal{S}$, I n'est pas premier. Il existe donc $a, b \in A \setminus I$ tels que $ab \in I$. Considérons les idéaux $I + aA, I + bA$ de A. Ils contiennent strictement I. Par la maximalité de I dans $\mathcal{S}$, ces idéaux n'appartiennent pas à $\mathcal{S}$. On a donc

$$I + aA \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_n, \quad I + bA \supseteq \mathfrak{q}_1 \cdots \mathfrak{q}_m$$

avec des idéaux premiers non nuls $\mathfrak{p}_i, \mathfrak{q}_j$. Il suit que

$$\mathfrak{p}_1 \cdots \mathfrak{p}_n \mathfrak{q}_1 \cdots \mathfrak{q}_m \subseteq (I + aA)(I + bA) \subseteq I.$$

Contradiction avec l'hypothèse $I \in \mathcal{S}$. Donc $\mathcal{S} = \emptyset$.

(2) Soit $\mathfrak{p}$ est un idéal maximal contenant I. Supposons qu'aucun des $\mathfrak{p}_i$ ne soit contenu dans $\mathfrak{p}$. On choisis alors un $a_i \in \mathfrak{p}_i \setminus \mathfrak{p}$ pour chaque $i \leq n$. Le produit $a_1 \cdots a_n \in \mathfrak{p}_1 \cdots \mathfrak{p}_n \subseteq \mathfrak{p}$, impossible car $\mathfrak{p}$ est premier. Suppsons donc que $\mathfrak{p}$ contienne $\mathfrak{p}_{i_0}$, alors ils sont égaux puisque $\mathfrak{p}_{i_0}$ est automatiquement maximal, A étant un anneau de Dedekind. □

Lemme 3.1.15. *Soit $\mathfrak{p}$ un idéal maximal de A. Alors dans $I(A)$ on a $\mathfrak{p}^{-1}\mathfrak{p} = A$.*

Démonstration. Montrons d'abord qu'il existe $x \in \mathfrak{p}^{-1} \setminus A$. Soit $a \in \mathfrak{p} \setminus \{0\}$ tel que $\mathfrak{p} \neq aA$ (remplacer a par a^2 si $\mathfrak{p} = aA$). On a une inclusion

$$\mathfrak{p}_1 \cdots \mathfrak{p}_n \subseteq aA \subset \mathfrak{p}$$

avec des idéaux maximaux $\mathfrak{p}_i$ par le lemme 3.1.14 ci-dessus et on peut supposer que n est le plus petit possible. On a $n \geq 2$ car $aA \neq \mathfrak{p}$. Par le même lemme, on peut supposer que $\mathfrak{p}_n = \mathfrak{p}$. Par la minimalité de n, il existe $b \in \mathfrak{p}_1 \cdots \mathfrak{p}_{n-1}$ et $b \notin aA$. Il suit que $x := b/a \notin A$. Mais $x\mathfrak{p} \subseteq a^{-1}\mathfrak{p}_1 \cdots \mathfrak{p}_n \subseteq A$, donc $x \in \mathfrak{p}^{-1} \setminus A$.

Par définition $\mathfrak{p}^{-1}\mathfrak{p}$ est un idéal fractionnaire contenu dans A. C'est donc un idéal de A. S'il n'est pas égal à A, il est contenu dans un idéal maximal $\mathfrak{p}' \supseteq \mathfrak{p}^{-1}\mathfrak{p} \supseteq \mathfrak{p}$. Donc $\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p}' = \mathfrak{p}$. En particulier $x\mathfrak{p} \subseteq \mathfrak{p}$. Il suit de la proposition 2.1.6(iii) que $x \in K$ est entier sur A, donc $x \in A$. Contradiction. □

3.1.3 Théorème de décomposition des idéaux

Dans un anneau principal, tout élément non nul se décompose de manière unique comme produit d'éléments irréductibles. Donc tout idéal non nul se décompose comme produit d'idéaux maximaux. Cette dernière propriété est plus faible que la décomposition des éléments, mais elle se généralise aux anneaux de Dedekind.

Theorem 3.1.16. *Soit A un anneau de Dedekind. Soit I un idéal non nul de A. Alors il existe des idéaux maximaux deux à deux distincts $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ et des entiers $r_1, \ldots, r_s \geq 1$ tels que*

$$I = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_s^{r_s}$$

(si $I = A$, on convient que A est le produit d'idéaux maximaux indexé par un ensemble vide). Une telle décomposition est unique à permutation près. Les $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ sont exactement les idéaux premiers de A contenant I.

Démonstration. Montrons d'abord l'existence. Il suffit de montrer que I est un produit d'idéaux maximaux. On écrit $\mathfrak{p}_1 \cdots \mathfrak{p}_n \subseteq I$ comme avant et on raisonne par récurrence sur n (les $\mathfrak{p}_i$ ne sont pas nécessairement distincts). Si $n = 1$, alors $I = \mathfrak{p}_1$ ou A et il n'y a rien à démontrer. Si $n \geq 2$, on peut supposer que $I \subseteq \mathfrak{p}_n$ et on a alors $\mathfrak{p}_1 \cdots \mathfrak{p}_{n-1} \subseteq \mathfrak{p}_n^{-1} I \subseteq A$. Par récurrence $\mathfrak{p}_n^{-1} I$ est un produit d'ideaux maximaux $\mathfrak{q}_1 \cdots \mathfrak{q}_m$, il suit que $I = \mathfrak{p}_n \mathfrak{p}_n^{-1} I = \mathfrak{p}_n \mathfrak{q}_1 \cdots \mathfrak{q}_m$.

Lorsque l'on a une décomposition $I = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_s^{r_s}$ comme dans le théorème, chaque $\mathfrak{p}_i$ contient I. Inversement si $\mathfrak{p}$ est un idéal maximal contenant I, par le lemme 3.1.14, $\mathfrak{p}$ est égal à un des $\mathfrak{p}_i$. Cela implique déjà l'unicité de l'ensemble des idéaux maximaux qui interviennent dans la décomposition de I. Le reste de l'unicité se démontre par une récurrence sur $r_1 + \cdots + r_s$ en utilisant le lemme ci-dessus qui permet de "simplifier" par un idéal maximal dans un produit d'idéaux maximaux. □

Exemple 3.1.17 Si A est principal dans le théorème, on prend un générateur a de I, on le décompose en produit $a = \prod_i p_i^{r_i}$ avec des des éléments irréductibles p_i deux à deux non-associés. On alors

$$I = \prod_i (p_i A)^{r_i}$$

est la décomposition recherchée.

Exemple 3.1.18 Revenons à l'exemple 3.1.6. Donc $n \geq 5$ sans facteur carré, $n \equiv 1 \mod 4$ et $L = \mathbb{Q}[\sqrt{-n}]$. On a vu que l'idéal $2\mathcal{O}_L$ n'était pas premier. Quelle est sa factorisation en produit d'idéaux maximaux ? Notons $\theta = \sqrt{-n}$. Alors $\mathcal{O}_L = \mathbb{Z}[\theta]$. Soit $\mathfrak{p}_2 = (2, 1+\theta)$. Montrons que c'est un idéal maximal et que $2\mathcal{O}_L = \mathfrak{p}_2^2$.

D'abord, tout élément de $\mathcal{O}_L$ est équivalent, modulo $\mathfrak{p}_2$, à 0 ou 1. Cela implique immédiatement que $\mathcal{O}_L/\mathfrak{p}_2$ est isomorphe à $\mathbb{F}_2$, donc $\mathfrak{p}_2$ est maximal. L'idéal $\mathfrak{p}_2^2$ est engendré par $4, 2(1+\theta), (1+\theta)^2$. On a

$$(1+\theta)^2 = 2\theta + 1 - n \in 2\mathcal{O}_L.$$

Donc $\mathfrak{p}_2^2 \subseteq 2\mathcal{O}_L$. De plus, si on écrit $n = 4m+1$, on a

$$-2 = (1+\theta)^2 - 2(\theta+1) + 4m \in \mathfrak{p}_2^2.$$

Donc $2\mathcal{O}_L = \mathfrak{p}_2^2$.

Considérons maintenant la décomposition de $3\mathcal{O}_L$. On va prendre $n = 5$. Modulo 3, on a $X^2 + 5 = (X+1)(X-1)$. Considérons $\mathfrak{p}_{3,1} = (3, \theta - 1)$ et $\mathfrak{p}_{3,2} = (3, \theta + 1)$. Ce sont des idéaux maximaux comme on le voit pour $\mathfrak{p}_2$. Ils sont distincts car sinon ils contiendraient 3 et $2 = (\theta+1) - (\theta-1)$ et donc 1. Ils contiennent 3, donc $3\mathcal{O}_L$. Par ailleurs, si un idéal maximal $\mathfrak{p}$ de $\mathcal{O}_K$ contient 3, il contient $6 = (\theta-1)(\theta+1)$, donc il contient aussi $\theta - 1$ ou $\theta + 1$. Il suit que $\mathfrak{p}$ est égal à $\mathfrak{p}_{3,1}$ ou $\mathfrak{p}_{3,2}$. Le théorème de decomposition dit que $3\mathcal{O}_L = \mathfrak{p}_{3,1}^{r_1}\mathfrak{p}_{3,2}^{r_2}$ avec $r_1, r_2 \geq 1$. Comme $\mathfrak{p}_{3,1}\mathfrak{p}_{3,2} = (9, 3(\theta-1), 3(\theta+1), \theta^2-1) \subseteq 3\mathcal{O}_L$, on trouve

$$3\mathcal{O}_L = \mathfrak{p}_{3,1}\mathfrak{p}_{3,2}.$$

Enfin un dernier exemple avec $11\mathcal{O}_L$ (toujour avec $n = 5$). On a $\mathcal{O}_L/11\mathcal{O}_L = \mathbb{Z}[X]/(11, X^2+5) = \mathbb{F}_{11}[X]/(X^2+5)$ est un corps car X^2+5 est irréductible dans $F_{11}[X]$. Donc la décomposition de $11\mathcal{O}_L$ est juste égale à l'idéal lui-même.

Revenons brièvement aux idéaux fractionnaires.

Corollaire 3.1.19. *L'ensemble $I(A)$ des idéaux fractionnaires de A muni du produit un groupe commutatif.*

Démonstration. Cela résulte immédiatement du théorème et du lemme 3.1.15. □

Exercice 3.1.20 Montrer que l'inverse de M dans $I(A)$ est égal à M^{-1}.

Exercice 3.1.21 Montrer que tout idéal fractionnaire M de A possède une décomposition unique

$$M = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_n^{r_n}$$

avec $r_i \in \mathbb{Z} \setminus \{0\}$ et que $M \subseteq A$ si et seulement si $r_i > 0$ pour tout i.

Remarque 3.1.22 Pour un anneau intègre A en général, on peut définir similairement l'ensemble des idéaux fractionnaires avec une loi de multiplication commutative et associative. On peut montrer que si cet ensemble est un groupe, alors A est nécessairement un corps ou un anneau de Dedekind.

Remarque 3.1.23 La structure du groupe des idéaux fractionnaires est très simple. C'est le groupe abélien libre engendré par l'ensemble des idéaux maximaux de A. Par exemple, l'ensemble des idéaux maximaux d'un anneau d'entiers est dénombrable, donc $I(\mathcal{O}_L) \simeq I(\mathbb{Z})$ pour tout corps de nombres L. On ne peut donc pas tirer énormément d'informations sur A à partir de $I(A)$.

Définition 3.1.24 L'ensemble des idéaux fractionnaires principaux (ceux de la forme αA, pour un $\alpha \in K^*$) est un sous-groupe du groupe $I(A)$. Le groupe quotient est appelé le *groupe des classes* de A. On le note $\mathrm{Cl}(A)$.

Proposition 3.1.25. *On a* $\mathrm{Cl}(A) = \{1\}$ *si et seulement si* A *est principal.*

Démonstration. Si A est principal, tout idéal fractionnaire est principal par la proposition 3.1.11. Inversement, supposons $\mathrm{Cl}(A) = \{1\}$. Soit I un idéal non nul de A. Alors il existe $x \in K^*$ tel que $I = xA$. On a $x = x.1 \in I$, donc $x \in A$ et I est un idéal principal. Ce qui prouve que A est principal. □

Définition 3.1.26 Soit L un corps de nombres, on appelle $\mathrm{Cl}(\mathcal{O}_L)$ *le groupe des classes* de L, et on le note (par abus de notation !) $\mathrm{Cl}(L)$. On verra que ce groupe est fini. Son cardinal, noté h_L ou $h(L)$, est appelé le *nombre de classes* de L. C'est un invariant important de l'extension L. Mais on verra qu'il n'est pas toujours facile à déterminer, même pour les extensions quadratiques !

Exemple 3.1.27 Soit $d > 0$ sans facteur carré et soit $L = \mathbb{Q}[\sqrt{-d}]$ (*cf.* exemple 3.1.6). On connait les valeurs de d pour lesquel h_L vaut 1 :

$$1, 2, 3, 7, 11, 19, 43, 67, 163.$$

Ceux pour lesquel h_L vaut 2 :

$$5, 6, 10, 13, 15, 22, 35, 37, 51, 58, 91, 115, 123, 187, 235, 267, 403, 427.$$

On sait que h_L tend vers l'infini avec d. En revanche, on conjecture que $h_{\mathbb{Q}[\sqrt{d}]}$ vaut 1 pour une infinité de d.

3.1.4 Génération des idéaux d'un anneau de Dedekind

Nous allons montrer que les anneaux locaux de Dedekind sont principaux et que tout idéal dans un anneau de Dedekind est engendré par au plus 2 éléments.

Un anneau est *local* s'il a un unique idéal maximal. Voir § 3.2 pour plus d'informations.

Proposition 3.1.28. *Soit A un anneau de Dedekind local. Alors A est principal.*

Démonstration. Soit $\mathfrak{p}$ l'idéal maximal de A. On a $\mathfrak{p} \neq \mathfrak{p}^2$ (sinon on obtient $A = \mathfrak{p}$ en multipliant par $\mathfrak{p}^{-1}$). Soit $t \in \mathfrak{p} \setminus \mathfrak{p}^2$. Alors la décomposition de tA en produit d'idéaux maximaux est $tA = \mathfrak{p}$. Soit I un idéal non nul de A, alors il existe $m \geq 0$ tel que $I = \mathfrak{p}^m = t^m A$. Donc A est principal. □

Définition 3.1.29 Deux idéaux I, J d'un anneau A sont dits *premiers entre eux* si $I + J = A$. Cela revient à dire qu'il n'existe aucun idéal maximal de A contenant à la fois I et J.

Lemme 3.1.30. *Soit A un anneau.*

(1) *Deux idéaux maximaux distincts dans A sont toujours premiers entre eux.*

(2) *Si $J_1, \ldots, J_q$ sont des idéaux premiers à I, alors $J_1 \cdots J_q$ est premier à I.*

(3) *Soient I, J premiers entre eux. Soient $m, n \geq 1$. Alors I^m et J^n sont premiers entre eux.*

Démonstration. (1) Si I, J sont maximaux et distincts, alors $I + J$ est un idéal qui contient strictement I, donc égal à A.

(2) Soient $1 = \alpha_i + \beta_i$ avec $\alpha_i \in I$ et $\beta_i \in J_i$ pour tout $i \leq q$. Le produit de ces q égalités montre que $1 \in I + \prod_{i \leq n} J_i$.

(3) Utiliser deux fois (2). □

Theorem 3.1.31 (Théorème des restes chinois)**.** *Soit A un anneau. Considérons des idéaux $I_1, \ldots, I_n$ de A deux à deux premiers entre eux. Alors*

(1) *On a $\cap_{1 \leq i \leq n} I_i = \prod_{1 \leq i \leq n} I_i$.*

(2) *L'homomorphisme d'anneaux canonique $A \to \prod_{1 \leq i \leq n} A/I_i$ est surjectif, et induit un isomorphisme*

$$A/\prod_{1 \leq i \leq n} I_i \simeq \prod_i A/I_i.$$

.

Démonstration. On se ramène à $n = 2$ grâce au lemme ci-dessus. Soient deux idéaux I, J premiers entre eux. Soit $1 = \alpha + \beta$ avec $\alpha \in I$ et $\beta \in J$. Pour tout $x \in I \cap J$, on a $x = x\alpha + x\beta \in IJ + IJ = IJ$. D'où $I \cap J \subseteq IJ$. L'inclusion inverse est évidente. Ce qui montre (1).

Pour tous $a, b \in A$, on a $a - b = (a - b)\alpha + (a - b)\beta$, donc

$$a + (b - a)\alpha = b + (a - b)\beta \in (a + I) \cap (b + J).$$

Cela montre la surjectivité de $A \to A/I \times A/J$. Le théorème de factorisation des homomorphismes d'anneaux implique (2). □

Lemme 3.1.32. *Soit A un anneau de Dedekind. Soit $\mathfrak{p}$ un idéal maximal et $t \in \mathfrak{p} \setminus \mathfrak{p}^2$. Fixons $n \geq 2$. Alors tout idéal de $A/\mathfrak{p}^n$ est engendré par une puissance de $\bar{t}$, la classe de t dans $A/\mathfrak{p}^n$.*

Démonstration. En effet, dans la décomposition de tA, $\mathfrak{p}$ apparaît avec l'exposant 1 : $tA = \mathfrak{p}I$ avec I premier à $\mathfrak{p}$ (car produit d'idéaux maximaux distincts de $\mathfrak{p}$), donc premier à $\mathfrak{p}^{n-1}$. Soient $x_0 \in \mathfrak{p}^{n-1}$ et $y_0 \in I$ tels que $x_0 + y_0 = 1$. Pour tout $x \in \mathfrak{p}$, on a $x = xx_0 + xy_0 \in \mathfrak{p}^n + tA$. Il suit que $\mathfrak{p} = tA + \mathfrak{p}^n$. Pour tout $m \geq 1$, on a alors $\mathfrak{p}^m = t^m A + \mathfrak{p}^n$. Si $J' \subseteq A/\mathfrak{p}^n$ est un idéal, son image réciproque J dans A est un idéal de A contenant $\mathfrak{p}^n$, il est donc égal à $\mathfrak{p}^m$ pour un $0 \leq m \leq n$. Il suit que $J' = \mathfrak{p}^m/\mathfrak{p}^n = \bar{t}^m A/\mathfrak{p}^n$. □

Lemme 3.1.33. *Soit A un anneau de Dedekind. Soit I un idéal non nul de A. Alors tout idéal de A/I est engendré par un élément.*

Démonstration. Soit $I = \prod_i \mathfrak{p}_i^{r_i}$ avec des idéaux maximaux 2 à 2 distincts et $r_i \geq 1$. Alors $A/I \simeq \prod_i A/\mathfrak{p}_i^{r_i}$ par le théorème 3.1.31. Tout idéal de $A/\mathfrak{p}_i^{r_i}$ étant monogène 3.1.32, il en est de même pour A/I. □

Corollaire 3.1.34. *Soit A un anneau de Dedekind. Alors tout idéal I de A est engendré par au plus 2 éléments.*

Démonstration. On peut supposer $I \neq 0$. Soit $a \in I$ non nul. Alors l'idéal I/aA de A/aA est engendré par un élément $\bar{b}$ avec $b \in I$. Il suit que $I = aA + bA$. □

3.2 Étude locale

Soit A un anneau de Dedekind de corps de fractions K. Sa structure devient plus simple par localisation (c'est-à-dire en ajoutant des dénominateurs à A). Typiquement, la localisation par rapport à un idéal maximal conduit à un anneau de valuation discrète.

3.2.1 Localisation

Ce sous-paragraphe regroupe quelques généralités sur la localisation. La plupart d'entre elles ont été vue en TD, nous n'y reviendrons donc pas. Nous passons directement à la proposition 3.2.12 et son corollaire 3.2.13.

On supposera dans cette section que A est un anneau intègre. On note K son corps des fractions. La localisation est un procédé qui génère des A-algèbres, et qui permet entre autres d'étudier "isolément" les idéaux premiers de A.

L'exemple le plus simple de localisation est le corps des fractions K lui-même. On voit que ce procédé fabrique un anneau ayant une structure plus simple que l'anneau de départ.

Définition 3.2.1 Une *partie multiplicative* S de A est un sous-ensemble non vide stable par multiplication. Par commodité on demandera aussi que $1 \in S$ et $0 \notin S$.

Exemple 3.2.2 $S = A \setminus \{0\}$, ou plus généralement, $A \setminus \mathfrak{p}$ pour un idéal premier $\mathfrak{p}$ de A ; $\{f^n | n \geq 1\}$ pour un élément donné $f \in A$.

Définition 3.2.3 On pose

$$S^{-1}A = \{a/s \in K \mid a \in A, s \in S\}.$$

On l'appelle la *localisation de* A par rapport à S. On voit immédiatement que c'est un sous-anneau de K contenant A. L'inclusion $A \subseteq S^{-1}A$ fait de ce dernier une A-algèbre. De plus, $\mathrm{Frac}(S^{-1}A) = K$.

Exemple 3.2.4 Si $\mathfrak{p}$ est un idéal premier de A, on note $A_\mathfrak{p}$ la localisation de A par rapport à $A \setminus \mathfrak{p}$. En particulier, $K = A_{\{0\}}$. Si $f \in A$, on note A_f la localisation de A par rapport à $\{f^n \mid n \geq 0\}$. La localisation $\mathbb{Z}_{10}$ est l'anneau des nombres décimaux.

Soit I un idéal de A. On note $S^{-1}I$ l'ensemble $\{a/s \mid a \in I, s \in S\}$. C'est un idéal de $S^{-1}A$, égal à l'idéal de $S^{-1}A$ engendré par la partie $I \subset S^{-1}A$. On note cet idéal aussi par $I(S^{-1}A)$.

Proposition 3.2.5. *Si A est noethérien, alors il en est de même pour $S^{-1}A$.*

Démonstration. Soit J un idéal de $S^{-1}A$. Alors $I := J \cap A$ est un idéal de A, donc engendré par $x_1, \ldots, x_n \in I$. Ce sont aussi des éléments de J puisque $I \subseteq J$. Pour tout $x = \alpha/s \in J$, on a $\alpha = sx \in J \cap A = I$. Donc $\alpha = \sum_i a_i x_i$ avec $a_i \in A$ et $x = \sum_i (a_i/s)x_i$. Ce qui montre que $x_1, \ldots, x_n$ engendrent J en tant que $S^{-1}A$-module. Donc J est de type fini et $S^{-1}A$ est noethérien. □

Proposition 3.2.6. *Soit S une partie multiplicative de A. Les correspondances*

$$\mathfrak{q} \mapsto \mathfrak{q} \cap A, \quad \mathfrak{p} \mapsto S^{-1}\mathfrak{p}$$

établissent une bijection (réciproque l'une de l'autre) de l'ensemble des idéaux premiers de $S^{-1}A$ avec l'ensemble des idéaux premiers de A ne rencontrant pas S.

Démonstration. Notons d'abord que si $\mathfrak{q}$ est un idéal premier de $A_\mathfrak{p}$, $\mathfrak{q} \cap A$ est un idéal premier de A (l'image réciproque par un homomorphisme d'anneaux d'un idéal premier est un idéal premier). De plus $(\mathfrak{q} \cap A) \cap S = \emptyset$ car sinon, si s est dans l'intersection, on a $s \in \mathfrak{q}$ et $s \in (S^{-1}A)^*$, Ce qui impliquerait que $\mathfrak{q} = S^{-1}A$, et ce n'est pas un idéal premier !

Inversement, si $\mathfrak{p}$ est un idéal premier de A avec $\mathfrak{p} \cap S = \emptyset$, montrons que $S^{-1}\mathfrak{p}$ est premier dans $S^{-1}A$. C'est un idéal propre car $1 = \alpha/s$ avec $\alpha \in \mathfrak{p}$, $s \in S$ implierait que $\alpha = s \in \mathfrak{p} \cap S$. Ensuite, si $\alpha_1/s_1 \times \alpha_2/s_2 \in S^{-1}\mathfrak{p}$, alors $\alpha_1\alpha_2 \in \mathfrak{p}$, donc, par exemple $\alpha_1 \in \mathfrak{p}$. Il suit que $\alpha_1/s_1 \in S^{-1}\mathfrak{p}$.

Il reste à montrer que $(S^{-1}\mathfrak{p}) \cap A = \mathfrak{p}$ et $S^{-1}(\mathfrak{q} \cap A) = \mathfrak{q}$ pour $\mathfrak{p}, \mathfrak{q}$ comme dans l'énoncé. On a clairement $\mathfrak{p} \subseteq (S^{-1}\mathfrak{p}) \cap A$ et $S^{-1}(\mathfrak{q} \cap A) \subseteq \mathfrak{q}$.

Soit $a = \alpha/s \in (S^{-1}\mathfrak{p}) \cap A$. Alors $sa = \alpha \in \mathfrak{p}$. Comme $s \notin \mathfrak{p}$ puisque $S \cap \mathfrak{p}$ est vide, on a $a \in \mathfrak{p}$. Donc $(S^{-1}A) \cap \mathfrak{p} \subseteq \mathfrak{p}$ et on a l'égalité. Soit $x = \alpha/s \in \mathfrak{q}$. Alors $\alpha = sx \in \mathfrak{q} \cap A$ et $x = \alpha/s \in S^{-1}(\mathfrak{q} \cap A)$. Ce qui montre l'inclusion $\mathfrak{q} \subseteq S^{-1}(\mathfrak{q} \cap A)$ et donc l'égalité. □

Corollaire 3.2.7. *Avec les notations de la propostion ci-dessus, si de plus* $\mathfrak{p}$ *est un idéal maximal de* A*, alors* $S^{-1}\mathfrak{p}$ *est un idéal maximal de* $S^{-1}A$*.*

Démonstration. Si $\mathfrak{p}$ est maximal, et si $S^{-1}\mathfrak{p}$ est contenu dans un idéal maximal $\mathfrak{q}$ de $S^{-1}A$, alors $\mathfrak{p} = \mathfrak{q} \cap A$, et donc $S^{-1}\mathfrak{p} = \mathfrak{q}$ est un idéal maximal. □

Définition 3.2.8 On dit qu'un anneau A est *local* s'il admet un unique idéal maximal. Par exemple, un corps est un anneau local. L'idéal maximal d'un anneau local contient tous les idéaux premiers.

Exercice 3.2.9 Un anneau A est local si et seulement si $A \setminus A^*$ est un idéal. Ce sera alors l'idéal maximal de A. Si I est un idéal de A, alors $A \setminus I = A^*$ si et seulement si I est l'unique idéal maximal de A.

Exemple 3.2.10 L'anneau $\mathbb{Z}$ n'est pas local.

Exemple 3.2.11 Soit A un anneau intègre. Soit $\mathfrak{p}$ un idéal premier de A. Alors $A_\mathfrak{p}$ est un anneau local, d'idéal maximal $S^{-1}\mathfrak{p}$, où $S = A \setminus \mathfrak{p}$. En effet par la proposition 3.2.6, $S^{-1}\mathfrak{p}$ est un idéal premier puisque $\mathfrak{p} \cap S = \emptyset$. De plus, les idéaux premiers de $A_\mathfrak{p}$ sont de la forme $S^{-1}\mathfrak{p}'$ avec $\mathfrak{p}' \cap S = \emptyset$ donc $\mathfrak{p}' \subseteq A \setminus S = \mathfrak{p}$ et $S^{-1}\mathfrak{p}'$ est contenu dans $S^{-1}\mathfrak{p}$.

Cet exemple est fondamental. À partir de $\mathfrak{p}$, on a construit un anneau dont les idéaux premiers correspondent à ceux de A contenus dans $\mathfrak{p}$. Ce qui simplifie considérablement la structure du nouvel anneau.

Il existe une explication du terme « local » provenant de la géométrie algébrique.

Proposition 3.2.12. *Soit* A *un anneau intègre et intégralement clos, alors* $S^{-1}A$ *est intégralement clos.*

Démonstration. Soit $x \in \mathrm{Frac}(S^{-1}A) = \mathrm{Frac}(A) = K$ un élément entier sur $S^{-1}A$. On a une relation entière

$$x^n + (a_{n-1}/s_{n-1})x^{n-1} + \cdots + (a_0/s_0) = 0, \quad a_i \in A, s_i \in S.$$

En prenant $s = s_0 s_1 \cdots s_{n-1}$, on obtient une relation entière de sx sur A, donc $sx \in A$ et $x \in S^{-1}A$. Autrement dit, $S^{-1}A$ est intégralement clos. □

Proposition 3.2.13. *Si* A *est un anneau de Dedekind, alors* $S^{-1}A$ *est soit un corps, soit un anneau de Dedekind.*

Démonstration. D'après ce qui précède, $S^{-1}A$ est intègre, intégralment close et noethérien. Enfin, tout idéal premier de $S^{-1}A$ est de la forme $S^{-1}\mathfrak{p}$ avec $\mathfrak{p}$ idéal premier de A. Comme $\mathfrak{p}$ est nul ou maximal, il en est de même pour $S^{-1}\mathfrak{p}$ d'après 3.2.6. Si $S^{-1}A$ n'est pas un corps, c'est alors un anneau de Dedekind. □

Un point intéressant avec la localisation est qu'elle permet de rendre un idéal principal en ajoutant juste un dénominateur.

Proposition 3.2.14. *Soient A un anneau de Dedekind, $\mathfrak{p}$ un idéal maximal et $t \in \mathfrak{p} \setminus \mathfrak{p}^2$. Alors il existe $s \in A \setminus \mathfrak{p}$ tel que $s\mathfrak{p} \subseteq tA \subseteq \mathfrak{p}$.*

Démonstration. La décomposition de tA fait apparaître $tA = \mathfrak{p}^r I_0$ avec I_0 produit d'idéaux maximaux différents de $\mathfrak{p}$ (donc premier à $\mathfrak{p}$), et $r \geq 1$. On a $r = 1$ car $t \notin \mathfrak{p}^2$. Soit $s \in I_0 \setminus \mathfrak{p}$ (il existe car I_0 est premier à $\mathfrak{p}$). Il suit que $\mathfrak{p} = tI_0^{-1} \subseteq t(s^{-1}A)$ et que $s\mathfrak{p} \subseteq tA$. □

Exercice 3.2.15 Trouver une partie multiplicative S de $\mathbb{Z}$, différente de $\mathbb{Z}\setminus\{0\}$, telle que $S^{-1}\mathbb{Z} = \mathbb{Q}$.

Exercice 3.2.16 Si A est principal (resp. factoriel), montrer que $S^{-1}A$ est principal (resp. factoriel).

3.2.2 Anneaux de valuation discrète

Nous avons vu que les anneaux de Dedekind locaux sont principaux (proposition 3.1.28). Une façon de construire de tels anneaux est donnée par les valuations discrètes.

Définition 3.2.17 Soit K un corps. Une *valuation discrète* sur K est une application $v : K^* \to \mathbb{Z}$ (et on conviendra souvent que v s'étend sur K en posant $v(0) = +\infty$) telle que pour tous $a, b \in K^*$

1. $v(ab) = v(a) + v(b)$ (c'est un homomorphisme de groupes) ; en particuler $v(1) = 0$.
2. $v(a + b) \geq \min\{v(a), v(b)\}$ (si $a + b = 0$, il n'y a pas de condition).

On dit que la valuation est *non triviale* si $v(K^*) \neq \{0\}$ et qu'elle est *normalisée* si $v(K^*) = \mathbb{Z}$ (en général c'est un sous-groupe non nul de $\mathbb{Z}$, donc de la forme $d\mathbb{Z}$). Nous n'utiliserons que les valuations non triviales dans ce cours.

Exemple 3.2.18 Soit p un nombre premier. On a une *valuation p-adique* sur $\mathbb{Q}$, définie comme suit. Tout nombre rationnel x non nul s'écrit de façon unique a/b avec $a, b \in \mathbb{Z}$ premiers entre eux et $b > 0$. On décompose $a = p^r u$, $b = p^s v$ avec $r, s \in \mathbb{N}$ et u, v premiers à p. Alors la valuation p-adique $v_p(x)$ est égale à $v_p(a) - v_p(b) = r - s$. On a $x = p^{v_p(x)} c/d$ avec $c, d \in \mathbb{Z}$ premiers à p.

Un corps K muni d'une valuation discrète non triviale v est appelé un *corps de valuation discrète*. L'ensemble

$$\mathcal{O}_v := \{a \in K^* \mid v(a) \geq 0\} \cup \{0\}.$$

est un sous-anneau de K, appelé un *anneau de valuation discrète*, ou l'*anneau de valuation de* (K, v). Le sous-ensemble

$$\mathfrak{m}_v := \{a \in K^* \mid v(a) > 0\} \cup \{0\}$$

est un idéal de $\mathcal{O}_v$.

Proposition 3.2.19. *Un anneau A est un anneau de valuation discrète si et seulement si c'est un anneau de Dedekind local. Son idéal maximal est alors $\mathfrak{m}_v$.*

Démonstration. Supposons que A est un anneau de valuation discrète. Si $a \in A \setminus \mathfrak{m}_v$, alors $v(1/a) = -v(a) = 0$, donc $1/a \in A$ et $a \in A^*$. Ce qui montre que A est local d'idéal maximal m_v. Soit I un idéal non nul de A. Soit $x_0 \in I$ de valuation minimale. Alors pour tout $x \in I$, $v(x/x_0) \geq 0$, donc $x/x_0 \in A$ et $I = x_0A$. Ce qui prouve que A est principal. La valuation étant non triviale, il existe $a \in K$ non nul avec $v(a) > 0$. Donc $a \in A$ et $1/a \notin A$ et A n'est pas un corps.

Inversement, soit A un anneau de Dedekind local. Il est alors principal (3.1.28). Soit t un générateur de l'idéal maximal $\mathfrak{m}$ de A. Comme A est un anneau factoriel, t est un élément premier et pour tout $a \in A$ non nul, il existe un unique $n \geq 0$ tel que $a = t^n u$ avec $u \in A \setminus tA = A^*$. On pose $v(a) = n$. Cela définit une application $A \setminus \{0\} \to \mathbb{N}$ qui est multiplicative et qui s'étend en une valuation discrète non triviale sur $K = \mathrm{Frac}(A)$ (les détails sont à vérifier laissés aux). □

La proposition suivante est un principe local-global (si une certaine propriété est vraie en localisant en tous les idéaux maximaux, alors elle est vraie globalement).

Proposition 3.2.20. *Soient I, J deux idéaux dans un anneau intègre A. Si $IA_\mathfrak{m} \subseteq JA_\mathfrak{m}$ pour tout idéal maximal $\mathfrak{m}$ de A, alors $I \subseteq J$.*

Démonstration. Soit $\beta \in I$ et considérons

$$H = \{a \in A \mid a\beta \in J\}.$$

C'est un idéal de A. On veut montrer que $H = A$, ce qui impliquera que $1 \in H$ et donc que $\beta \in J$. Si H est un idéal propre, il est contenu dans un idéal maximal $\mathfrak{m}$ de A. Comme $IA_\mathfrak{m} \subseteq JA_\mathfrak{m}$ par hypothèse, il existe $\alpha \in J$, $s \in A \setminus \mathfrak{m}$ tels que $\beta = \alpha/s$. Donc $s\beta \in J$ et $s \in H \subseteq \mathfrak{m}$. Mais $s \notin \mathfrak{m}$. Contradiction. □

Theorem 3.2.21. *Soit A un anneau intègre noethérien qui n'est pas un corps. Alors A est un anneau de Dedekind si et seulement si pour tout idéal maximal $\mathfrak{m}$ de A, la localisation $A_\mathfrak{m}$ est un anneau de valuation discrète.*

Démonstration. Supposons vérifiée la propriété sur les localisations $A_\mathfrak{m}$. Soit $x = a/b \in K = \mathrm{Frac}(A)$ (avec $a, b \in A$) entier sur A. Alors pour tout idéal maximal $\mathfrak{m}$ de A, $x \in \mathrm{Frac}(A_\mathfrak{m})$ est entier sur $A_\mathfrak{m}$. Ce qui montre que $x \in A_\mathfrak{m}$. Donc $aA_\mathfrak{m} \subseteq bA_m$ pour tout idéal maximal $\mathfrak{m}$. La proposition 3.2.20 montre alors que $aA \subseteq bA$, donc $a \in bA$ et $x \in A$. Ce qui montre que A est intégralement clos.

Soit $\mathfrak{p}$ un idéal premier non nul de A. Soit $\mathfrak{m}$ un idéal maximal de A contenant $\mathfrak{p}$. Alors $\mathfrak{p}A_\mathfrak{m}$ est un idéal premier non nul de $A_\mathfrak{m}$ (proposition 3.2.6), donc égal à $\mathfrak{m}A_\mathfrak{m}$. Il suit que $\mathfrak{p} = \mathfrak{m}$ (*loc. cit.*) et $\mathfrak{p}$ est maximal. On a donc montré que A est un anneau de Dedekind.

Inversement, si A est un anneau de Dedekind, alors $A_\mathfrak{m}$ est un anneau de Dedekind local (3.2.13). On peut donc appliquer la proposition 3.1.28. □

Remarque 3.2.22 Soit $\mathfrak{p}$ un idéal maximal de A, on peut définir une sorte d'évaluation $v_\mathfrak{p}$ en $\mathfrak{p}$ sur l'ensemble des idéaux fractionnaires de A de la façon suivante. Soit I un idéal non nul de A. Si $\mathfrak{p}$ ne contient pas I, on pose $v_\mathfrak{p}(I) = 0$. Sinon, on pose $v_\mathfrak{p}(I) = r$ l'exposant de $\mathfrak{p}$ dans la décomposition de I. Ceci définit une application multiplicative de l'ensemble des idéaux non nuls de A dans $\mathbb{Z}$. Elle s'étend en un homomorphisme de groupes $v_\mathfrak{p} : I(A) \to \mathbb{Z}$.

Exercice 3.2.23 Soient I, J deux idéaux non nuls de A. Montrer que $I \subseteq J$ si et seulement is $v_\mathfrak{p}(I) \geq v_\mathfrak{p}(J)$ pour tous idéaux maximaux $\mathfrak{p}$ de A.

3.3 Ramification

Dans l'exemple 3.1.18 nous avons vu que le nombre premier $2 \in \mathbb{Z}$ n'est plus un élément premier dans l'anneau des entiers d'une extension quadratique L. Autrement dit, l'idéal $2\mathcal{O}_L \subseteq \mathcal{O}_L$ engendré par l'idéal maximal $2\mathbb{Z} \subset \mathbb{Z}$ n'est plus maximal. Ce type de phénomène s'appelle la ramification, et c'est l'analogue de la notion de ramification pour les applications entre des variétés topologiques ou complexes (comme l'application conforme $\mathbb{C} \to \mathbb{C}$, $z \mapsto z^2$).

3.3.1 Ramification et décomposition

Soit $A \subseteq B$ une extension d'anneaux de Dedekind, soient $\mathfrak{p}$ (resp. $\mathfrak{q}$) un idéal maximal de A (resp. de B) tels que $\mathfrak{p} \subseteq \mathfrak{q}$. Alors l'idéal $\mathfrak{p}B$ de B engendré par le sous-ensemble $\mathfrak{p}$ de B est non nul et se décompose donc en $\mathfrak{p}B = \mathfrak{q}^e I$ avec $\mathfrak{q}$ premier à I. Comme $\mathfrak{q} \cap A$ est un idéal premier contenant $\mathfrak{p}$, ils sont égaux. Le corps $A/\mathfrak{p}$ (resp. $B/\mathfrak{q}$) s'appelle le *corps résiduel* de A en $\mathfrak{p}$ (resp. de B en $\mathfrak{q}$). L'inclusion $\mathfrak{p} \subseteq \mathfrak{q}$ induit canoniquement une extension de corps $A/\mathfrak{p} \to B/\mathfrak{q}$.

Définition 3.3.1 Dans la situation ci-dessus, on appelle l'entier $e \geq 1$ l'*indice de ramification* de $A \subseteq B$ en $\mathfrak{q}$ et $A/\mathfrak{p} \to B/\mathfrak{q}$ l'*extension résiduelle* en $\mathfrak{q}$. On dit que $A \subseteq B$ est *non-ramifié en* $\mathfrak{q}$ si $e = 1$ et si l'extension résiduelle est finie et séparable. Notons que la dernière condition est automatiquement satisfaite pour les extensions $\mathbb{Z} \subseteq \mathcal{O}_L$ d'anneaux d'entiers de corps de nombres. En effet, les corps résiduels sont alors des corps finis, et toute extension finie d'un corps fini est séparable.

Pour un $\mathfrak{p}$ fixé, si $A \subseteq B$ est non-ramifié en tous les $\mathfrak{q} \subseteq \mathfrak{p}$, on dit que l'extension est *non-ramifiée au-dessus de* $\mathfrak{p}$. Lorsque $A = \mathbb{Z}$ et $B = \mathcal{O}_L$. On dira par abus de langage que $L/\mathbb{Q}$ est non-ramifiée au-dessus de p.

Exemple 3.3.2

1. Dans l'exemple 3.1.18 avec $L = \mathbb{Q}[\sqrt{-5}]$, l'indice de ramification de $\mathbb{Z} \subset \mathcal{O}_L$ en $\mathfrak{p}_2$ est égal à 2, avec une extension résiduelle triviale. Les indices de ramification en $\mathfrak{p}_{3,1}$ et $\mathfrak{p}_{3,2}$ sont égaux à 1 avec extensions résiduelles triviales. Donc $L/\mathbb{Q}$ est non-ramifiée au-dessus de 3. De même les calculs de l'exemple montrent que $L/\mathbb{Q}$ est non-ramifiée au-dessus de 11. En fait elle est non-ramifiée au-dessus de tout premier $p \neq 2, 5$.

2. Soit $P(z) \in \mathbb{C}[z]$ un polynôme non constant. Considérons

$$A := \mathbb{C}[t] \subseteq B := \mathbb{C}[z], \quad \text{où } t = P(z).$$

Soit $\mathfrak{p}$ un idéal maximal de A, alors il existe $\lambda \in \mathbb{C}$ tel que $\mathfrak{p} = (t-\lambda)\mathbb{C}[t]$. Tout idéal maximal $\mathfrak{q}$ de B contenant $\mathfrak{p}B$ est de la forme $\mathfrak{q} = (z-\mu)\mathbb{C}[z]$ avec $P(\mu) - \lambda = 0$ (exercice). Alors l'indice de ramification en $\mathfrak{q}$ est l'ordre d'annulation de $P(X) - \lambda \in \mathbb{C}[X]$ en μ et l'extension résiduelle est triviale. Notons que la somme des indices de ramification en les idéaux maximaux $\mathfrak{q} \subseteq B$ contenant $\mathfrak{p}$ est alors égale au

$$\deg(P(X) - \lambda) = \deg P(X) = [\mathbb{C}(z) : \mathbb{C}(t)].$$

Ceci se généralise en théorème 3.3.9.

Nous allons maintenant préparer la preuve du théorème 3.3.9. On fixe $A \subseteq B$ une extension finie d'anneaux de Dedekind. Soit $\mathfrak{p}$ un idéal maximal de A et $\mathfrak{q}$ un idéal maximal de B contenant $\mathfrak{p}$. On note $f = [B/\mathfrak{q} : A/\mathfrak{p}]$.

Lemme 3.3.3. *Pour tout $r \geq 0$, on a un isomorphisme de B-modules $B/\mathfrak{q} \to \mathfrak{q}^r/\mathfrak{q}^{r+1}$.*

Démonstration. Soit $\pi \in \mathfrak{q} \setminus \mathfrak{q}^2$. L'homomorphisme B-linéaire $B \to \mathfrak{q}^r, b \mapsto b\pi^r$ induit un homomorphisme B-linéaire $B/\mathfrak{q} \to \mathfrak{q}^r/\mathfrak{q}^{r+1}$. Il existe $s \in B \setminus \mathfrak{q}$ tel que $s\mathfrak{p}^i \subseteq \pi^i B$ pour tout $i \leq r+1$ (proposition 3.2.14). Si $\pi^r b \in \mathfrak{q}^{r+1}$, alors $s\pi^r b \in \pi^{r+1}B$, donc $sb \in \pi B \subseteq \mathfrak{q}$ et $b \in \mathfrak{q}$. D'où l'injectivité. Soit $b \in \mathfrak{q}^r$. On a $sb = \pi^r b'$. Il existe $s' \in B \setminus \mathfrak{q}$ tel que $ss' \in 1 + \mathfrak{q}$ car $\mathfrak{q} + sB = B$. Cela implique la surjectivité. □

Lemme 3.3.4. *Soient R un anneau, I un idéal de R et M un R-module. Supposons que $IM = 0$ (i.e., $ax = 0$ pour tout $a \in I$ et pour tout $x \in M$). Alors M est naturellement un R/I-module.*

Démonstration. Il suffit de définir la loi de produit externe. Pour toute classe $\bar{a} \in R/I$ et $x \in M$, on pose $\bar{a} * x = ax$. Si $\bar{a} = \bar{a'}$, alors $a - a' \in I$ et $ax = a'x$. Donc le produit externe est bien défini. Il est trivial de montrer que les axiomes d'un module sur R/I sont vérifiés. □

Corollaire 3.3.5. *Si $r \leq e$, alors $B/\mathfrak{q}^r$ est un $A/\mathfrak{p}$-espace vectoriel de dimension fr.*

Démonstration. Notons que $\mathfrak{p} \subseteq \mathfrak{q}^e \subseteq \mathfrak{q}^r$, donc $B/\mathfrak{q}^r$ est naturellement un espace vectoriel sur $A/\mathfrak{p}$ d'après le lemme ci-dessus. Si $r \geq 1$, on a une suite exacte d'espaces vectoriels sur $A/\mathfrak{p}$:

$$0 \to \mathfrak{q}^{r-1}/\mathfrak{q}^r \to B/\mathfrak{q}^r \to B/\mathfrak{q}^{r-1} \to 0.$$

D'où $\dim_{A/\mathfrak{p}} B/\mathfrak{q}^r = \dim_{A/\mathfrak{p}} B/\mathfrak{q}^{r-1} + \dim_{A/\mathfrak{p}} B/\mathfrak{q}$ en utilisant le lemme 3.3.3 ci-dessus. Cela implique immédiatement le corollaire par récurrence sur r. □

Fixons $\mathfrak{p}$ et considérons la décomposition de l'idéal $\mathfrak{p}B$ de B :

$$\mathfrak{p}B = \prod_{1\leq i\leq m} \mathfrak{q}_i^{e_i}.$$

Notons $f_i = [B/\mathfrak{q}_i : A/\mathfrak{p}]$.

Proposition 3.3.6. *On a*

$$\dim_{A/\mathfrak{p}}(B/\mathfrak{p}B) = \sum_{1\leq i\leq m} e_i f_i.$$

Démonstration. D'après le théorème des restes chinois 3.1.31, on a un isomorphisme canonique

$$B/\mathfrak{p}B \simeq \prod_{1\leq i\leq m} B/\mathfrak{q}_i^{e_i}.$$

C'est un isomorphisme d'anneaux, mais aussi de B-modules (par construction), et donc de A-modules. Comme tous les modules en présence sont annulés par $\mathfrak{p}$, c'est aussi un isomorphisme de $A/\mathfrak{p}$-espaces vectoriels. Il suffit alors d'appliquer le corollaire 3.3.5 ci-dessus. □

Nous allons maintenant comparer $\dim_{A/\mathfrak{p}} B/\mathfrak{p}B$ avec le degré de l'extension $\mathrm{Frac}(B)/\mathrm{Frac}(A)$. Pour cela, nous supposons que B est la clôture intégrale de A dans une extension finie séparable L de $K = \mathrm{Frac}(A)$ (proposition 3.1.3), de sorte que B soit de type fini comme A-module (2.3.9). Nous allons alors montrer que $\dim_{A/\mathfrak{p}} B/\mathfrak{p}B = [L : K]$. Nous commençons avec une forme très générale du célèbre lemme de Nakayama.

Lemme 3.3.7 (Lemme de Nakayama)**.** *Soient R un anneau, I un idéal de R et M un R-module de type fini. Si $M = IM$, alors il existe $\alpha \in I$ tel que $(1+\alpha)M = 0$.*

Démonstration. Soit $\{x_1, \ldots, x_n\}$ un système de générateurs de M sur R. Il existe une matrice D à coefficients dans I telle que

$${}^t(x_1, \ldots, x_n) = D \cdot {}^t(x_1, \ldots, x_n).$$

Donc $(1_n - D)^t(x_1, \ldots, x_n) = 0$. En multipliant par la comatrice de $1_n - D$ on obtient $\det(1_n - D) \cdot {}^t(x_1, \ldots, x_n) = 0$. Soit $a = \det(1_n - D) = 1 + \alpha \in 1 + I$, alors $ax_i = 0$ pour tout $i \leq n$, donc $aM = 0$. □

Corollaire 3.3.8. *Soient $b_1, \cdots, b_n \in B$ dont les images dans $B/\mathfrak{p}B$ forment une base de $A/\mathfrak{p}$-espace vectoriel. Alors ils forment une base de L/K.*

Démonstration. (1) Indépendance linéaire. Soit $\sum_{1\leq j\leq n} a_j b_b = 0$ avec $a_j \in K$. On veut montrer que les a_j sont tous nuls. En chassant les dénominateurs, on peut supposer que $a_j \in A$. Supposons que les a_j ne sont pas tous nuls. Alors il existe $r \geq 0$ tel que $a_j \in \mathfrak{p}^r$ pour tous $j \leq n$, et que l'un des a_j, disons a_1, n'appartient pas à $\mathfrak{p}^{r+1}$.

Soit $t \in \mathfrak{p} \setminus \mathfrak{p}^2$. Soit $s \in A \setminus \mathfrak{p}$ tel que $s\mathfrak{p}^r \subseteq t^r A$ (proposition 3.2.14). Alors $\sum_j (sa_j t^{-r}) b_j = 0$ avec $sa_j t^{-r} \in A$. En passant dans $B/\mathfrak{p}B$, on obtient $sa_j t^{-r} \in \mathfrak{p}$. En particulier $sa_1 \in t^r \mathfrak{p} \subseteq \mathfrak{q}^{r+1}$. Soit $a' \in A$ tel que $1 = sa' + x$ avec $x \in \mathfrak{q}$, alors $a_1 = (sa' + x)a_1 \in \mathfrak{p}^{r+1}$. Contradiction.

(2) Génération. Soit $N = \sum_{1 \leq j \leq n} Ab_j \subseteq B$. Soit $M = B/N$ (quotient de A-modules). Comme $B \subseteq N + \mathfrak{p}B$ par l'hypothèse sur les b_j, on a $M = \mathfrak{p}M$. Il suit du lemme de Nakayam qu'il existe $\alpha \in \mathfrak{p}$ tel que $(1+\alpha)M = 0$. Autrement dit, comme $1 + \alpha \neq 0$, on a $B \subseteq (1+\alpha)^{-1} N \subseteq \sum_{1 \leq j \leq n} Kb_j$. En appliquant la proposition 2.3.5(1) avec $C = B$, on obtient $L \subseteq \sum_{1 \leq j \leq n} Kb_j$. Les $b_1, \cdots, b_n$ forment bien une base de L sur K. □

Theorem 3.3.9. *Soit A un anneau de Dedekind de corps de fractions K, soit B la clôture intégrale de A dans une extension finie séparable L/K. Pour tout idéal maximal $\mathfrak{p}$ de A, on a une décomposition*

$$\mathfrak{p}B = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_n^{e_n} \tag{3.1}$$

où $\mathfrak{q}_1, \ldots, \mathfrak{q}_n$ sont les idéaux maximaux de B contenant $\mathfrak{p}$, deux à deux distincts et où e_i est l'indice de ramification de $A \subseteq B$ en $\mathfrak{q}_i$. De plus, on a l'égalité

$$[L : K] = \sum_{1 \leq i \leq n} e_i f_i \tag{3.2}$$

où f_i est le degré de l'extension résiduelle de $A/\mathfrak{p} \subseteq B/\mathfrak{q}_i$.

Démonstration. Cela résulte de la proposition 3.3.6 et du corollaire 3.3.8. □

Proposition 3.3.10 (Cas galoisien)**.** *Conservons les notations du théorème 3.3.9 et supposons l'extension L/K galoisienne. Alors $e_i = e_j$ et $f_i = f_j$ pour tous $i, j \leq n$.*

Démonstration. Pour tout $\sigma \in G := \mathrm{Gal}(L/K)$, $\sigma(\mathfrak{q}_i)$ est un idéal maximal de B contenant $\sigma(\mathfrak{p}) = \mathfrak{p}$. Donc G opère sur l'ensemble des $\mathfrak{q}_i$. Montrons que l'action est transitive. Supposons par exemple que $\sigma(\mathfrak{q}_2) \neq \mathfrak{q}_1$ pour tout $\sigma \in G$. Soit

$$x \in \mathfrak{q}_1 \setminus \cup_{\sigma \in G} \sigma(\mathfrak{q}_2).$$

Un tel x existe par le théorème des restes chinois 3.1.31 (prendre un antécédent de $(0, 1, \ldots, 1)$ par $B \to \prod_i B/\mathfrak{q}_i$). Alors

$$\prod_{\sigma \in G} \sigma(x) = N_{L/K}(x) \in A \cap \mathfrak{q}_1 = \mathfrak{p} \subseteq \mathfrak{q}_2.$$

Donc un des conjugués de x appartient à $\mathfrak{q}_2$. Contradiction. Ce qui montre la transivitivé de l'action.

Fixons $r \leq n$. Soit $\sigma \in G$ tel que $\sigma(\mathfrak{q}_1) = \mathfrak{q}_r$. Comme $\mathfrak{p}B = \sigma(\mathfrak{p}B) = \prod \sigma(\mathfrak{q}_i)^{e_i}$, il suit de l'unicité de la décomposition que $e_1 = e_r$. De plus, σ induit un isomorphisme de A-modules $B/\mathfrak{q}_1 \to B/\sigma(\mathfrak{q}_1) = B/\mathfrak{q}_r$ qui est *a fiortiori* un isomorphisme de $(A/\mathfrak{p})$-espaces vectoriels. Donc $f_1 = f_r$. □

Nous allons donner une méthode concrète pour calculer les invariants e et f dans un cas particulier (extensions monogènes).

Proposition 3.3.11 (Cas monogène)**.** *Soient A, B comme ci-dessus. Supposons $B = A[\theta]$ pour un certain $\theta \in B$. Soit $H(X) \in A[X]$ le polynôme minimal de θ. Fixons un idéal maximal $\mathfrak{p}$ de A, et notons $k(\mathfrak{p}) = A/\mathfrak{p}$. Soit $\bar{H}(X)$ la classe de $H(X)$ dans $k(\mathfrak{p})[X]$. Considérons la factorisation*

$$\bar{H}(X) = \prod_{1 \leq i \leq n} h_i(X)^{r_i}, \quad r_i \geq 1$$

avec les $h_i(X) \in k(\mathfrak{p})[X]$ unitaires irréductibles et deux à deux distincts. Soit $H_i(X) \in A[X]$ un polynôme unitaire dont l'image dans $k(\mathfrak{p})[X]$ est égale à $h_i(X)$. Alors les propriétés suivantes sont vraies.

(1) *On a un isomorphisme d'anneaux $A[X]/(H(X)) \simeq B$.*

(2) *Soit $\mathfrak{q}_i = H_i(\theta)B + \mathfrak{p}B$. Alors c'est un idéal maximal de B contenant $\mathfrak{p}$ avec $B/\mathfrak{q}_i \simeq k(\mathfrak{p})[X]/(h_i(X))$.*

(3) *Les $\mathfrak{q}_1, \ldots, \mathfrak{q}_n$ sont deux à deux distincts et sont exactement les idéaux maximaux de B contenant $\mathfrak{p}$.*

(4) *On a $e_i = r_i$, $f_i = \deg h_i(X)$.*

(5) *La décomposition de $\mathfrak{p}B$ est donnée par*

$$\mathfrak{p}B = \prod_{1 \leq i \leq n} \mathfrak{q}_i^{r_i}.$$

Démonstration. (1) Par hypothèse l'homomorphisme de A-algèbres $A[X] \to B$ défini par $F(X) \mapsto F(\theta)$ est surjectif. Déterminons son noyau. Soit $F(X) \in A[X]$ tel que $F(\theta) = 0$. Comme $H(X) \in A[X]$ est unitaire, on peut effectuer une division euclidienn dans $A[X]$:

$$F(X) = H(X)Q(X) + R(X), \quad \deg R(X) < \deg H(X).$$

Il suit que $R(\theta) = 0$, donc $R(X) = 0$ puisque $H(X)$ est le polynôme minimal de θ sur K. Donc $F(X) \in H(X)A[X]$ et le noyau en question est égal à $H(X)A[X]$. Ce qui prouve (1).

(2) Rappelons que si $I \subseteq J \subseteq R$ sont des idéaux dans un anneau R, alors on a un isomorphisme canonique $R/J \simeq (R/I)/(J/I)$.

On a

$$B/\mathfrak{q}_i \simeq A[X]/(H(X), H_i(X), \mathfrak{p}) \simeq k(\mathfrak{p})[X]/(h_i(X))$$

est un corps. Donc $\mathfrak{q}_i$ est un idéal maximal de B contenant $\mathfrak{p}$ et $k(\mathfrak{q}_i) \simeq k(\mathfrak{p})[X]/(h_i(X))$ est une extension de $k(\mathfrak{p})$ de degré $f_i = \deg h_i(X)$.

(3) Soient $i \neq j \leq n$, montrons que $\mathfrak{q}_i \neq \mathfrak{q}_j$. En effet, comme $h_i(X), h_j(X)$ sont premiers entre eux, il existe $g_i(X), g_j(X) \in k(\mathfrak{p})[X]$ tels que $g_i h_i + g_j h_j = 1$. Si $G_i(X), G_j(X) \in A[X]$ sont des polynômes qui s'envoient sur $g_i(X), g_j(X)$ dans $k(\mathfrak{p})[X]$, alors

$$G_i(X)H_i(X) + G_j(X)H_j(X) = 1 + S(X), \quad S(X) \in \mathfrak{p}[X]$$

($\mathfrak{p}[X]$ est l'ensemble des polynômes à coefficients dans $\mathfrak{p}$). Si $\mathfrak{q}_i = \mathfrak{q}_j$, alors

$$1 + S(\theta) = G_i(\theta)H_i(\theta) + G_j(\theta)H_j(\theta) \in \mathfrak{q}_i + \mathfrak{q}_j = \mathfrak{q}_i.$$

Or $1 + S(\theta) \in 1 + \mathfrak{p}B \subseteq 1 + \mathfrak{q}_i$ est dans le complémentaire de $\mathfrak{q}_i$. Contradiction.

Il reste à montrer que tout idéal maximal $\mathfrak{q}$ de B contenant $\mathfrak{p}B$ est égal à un des $\mathfrak{q}_i$. Similairement à ce qui précède, on a

$$H(X) = \prod_{1\leq i\leq n} H_i(X)^{r_i} + R(X), \quad R(X) \in \mathfrak{p}[X]$$

avec un $R(X) \in \mathfrak{p}[X]$. Il suit que

$$0 = H(\theta) = \prod_{1\leq i\leq n} H_i(\theta)^{r_i} + R(\theta), \quad R(\theta) \in \mathfrak{p}B. \tag{3.3}$$

Donc $\prod_i H_i(\theta)^{r_i} \in \mathfrak{q}$. Par suite, $H_i(\theta) \in \mathfrak{q}$ pour un certain $i \leq n$. Cela entraîne que $\mathfrak{q}_i \subseteq \mathfrak{q}$, donc $\mathfrak{q}_i = \mathfrak{q}$ puisqu'il est maximal.

(4)-(5) L'équation (3.3) ci-dessus implique que

$$\prod_{i\leq n} H_i(\theta)^{r_i} = -R(\theta) \in \mathfrak{p}B.$$

Il suit que $\prod_i \mathfrak{q}_i^{r_i} \subseteq (\prod_i H_i(\theta)^{r_i}, \mathfrak{p}B) \subseteq \mathfrak{p}B = \prod_i \mathfrak{q}_i^{e_i}$. L'exercice 3.2.23 montre que $r_i \geq e_i$ pour tous $i \leq n$. Par ailleurs, on a

$$\sum_{i\leq n} r_i f_i = \deg \overline{H}(X) = \deg H(X) = [L : K]$$

car $H(X)$ est le polynôme minimal de θ sur K et que $L = K[\theta]$ (Proposition 2.3.5). D'après le théorème 3.3.9 on a

$$\sum_i e_i f_i = \sum_i r_i f_i.$$

Comme $r_i \geq e_i$ et $f_i \geq 1$ pour tout i, on a $r_i = e_i$ pour tout $i \leq n$. □

Exemple 3.3.12 Soit $d \neq 1$ un entier sans facteur carré et $\equiv 2, 3 \mod 4$. Considérons $L = \mathbb{Q}[\sqrt{d}]$. On a $\mathcal{O}_L = \mathbb{Z}[\sqrt{d}] = \mathbb{Z}[X]/(X^2 - d)$ (exemple 2.3.21). En un premier $p > 2$ ne divisant pas d, on a

$$\mathcal{O}_L/p\mathcal{O}_L = \mathbb{F}_p[X]/(X^2 + \bar{d})$$

est soit un corps, auquel cas il y a un seul premier dans $\mathcal{O}_L$ au-dessus de p et on a $e = 1$, $f = 2$; soit produit de deux copies de $\mathbb{F}_p$ et il y a deux premiers au-dessus de p avec $e_i = f_i = 1$. Dans les deux cas, L est non-ramifié au-dessus de p.

En $p = 2$, on a $\mathcal{O}_L/p\mathcal{O}_L = \mathbb{F}_p[X]/(X + 1)^2$ ou $\mathbb{F}_p[X]/(X^2)$. Donc $s = 1$, et on a $e = 2$, $f = 1$. Il suit que $2\mathcal{O}_L = \mathfrak{q}^2$ comme dans l'exemple 3.1.18.

En $p > 2$ divisant d, on a $\mathcal{O}_L/p\mathcal{O}_L = \mathbb{F}_p[X]/(X^2)$. Donc situation similaire à 2 : un seul premier au-dessus de p avec $e = 2$ et $f = 1$.

Pour $p > 2$ et premier à d, $X^2 - d$ est soit irréductible, soit produit de deux facteurs linéaires premiers entre eux. Donc $s = 1$ ou 2. Si $s = 1$, on a $e = 1$ et $f = 2$. Si $s = 2$, on a $e_1 = e_2 = f_1 = f_2 = 1$.

En résumé, les nombres premiers ramifiés dans l'extension L sont 2 et les diviseurs premiers de d. Par ailleurs, le discriminant $D_{\mathcal{O}_L/\mathbb{Z}} = 4d$. Donc les nombres premiers ramifiés sont ceux qui divisent $D_{\mathcal{O}_L/\mathbb{Z}}$. Ceci n'est pas un hasard comme on va voir un peu plus loin.

Exemple 3.3.13 Soit $L = \mathbb{Q}[\alpha]$ engendrée par une racine $\alpha \in \mathbb{C}$ de $H(X) = X^5 - X - 1$. On a vu (2.3.17) que $\mathcal{O}_L = \mathbb{Z}[\alpha]$. Dans $\mathbb{F}_2$, on a la décomposition $X^5 - X - 1 = (X^2 + X + 1)(X^3 + X^2 + 1)$ en facteurs irréductibles. Donc au-dessus de $2\mathbb{Z}$, on a $s = 2$, $e_1 = 1$, $f_1 = 2$ et $e_2 = 1$, $f_2 = 3$. Cela implique d'ailleurs que $L/\mathbb{Q}$ n'est pas galoisienne d'après la proposition 3.3.10.

3.3.2 Ramification et discriminant

Nous allons donner un résultat qui généralise l'exemple 3.3.12 concernant la ramification.

Theorem 3.3.14. *Supposons B libre sur A avec une base ε. Alors $A \to B$ est ramifié au-dessus de $\mathfrak{p}$ si et seulement si $\mathfrak{p}$ contient $D_{B/A}(\varepsilon)$. En particulier, si $\mathrm{Frac}(B)/\mathrm{Frac}(A)$ est une extension séparable, alors $A \to B$ est ramifié seulement au-dessus d'un nombre fini de $\mathfrak{p}$.*

Démonstration. Nous démontrons ce théorème dans le cas où $B = A[\theta]$ est monogène sur A comme dans la proposition 3.3.11. Nous gardons les notations de cette proposition. Comme le discriminant est indépendant du choix d'une base de B sur A à multiplication par des inversibles de A près, il suffit de montrer le théorème avec la base $\{1, \theta, \ldots, \theta^{d-1}\}$ où $d = \deg H(X)$. Notons $K = \mathrm{Frac}(A)$ et $L = \mathrm{Frac}(B) = K[X]/(H(X)) = K[\theta]$. Alors $D := D_{B/A}(\varepsilon) = D_{L/K}(\varepsilon) = \mathrm{disc}(H(X))$. Dire que l'extension B/A est non-ramifiée au-dessus de $\mathfrak{p}$ est équivalent à $r_i = 1$ et les $h_i(X)$ séparables. Comme ceux-ci sont premiers entre eux, c'est encore équivalent à $\overline{H}(X)$ séparable, c'est-à-dire que $\mathrm{disc}(\overline{H}(X)) \neq 0$. Or $\mathrm{disc}(\overline{H}(X)) = \overline{\mathrm{disc}(H(X))} \in A/\mathfrak{p}$. Cela implique le théorème. Lorsque l'extension $\mathrm{Frac}(B)/\mathrm{Frac}(A)$ est séparable, comme c'est le corps de rupture de $H(X)$, on a $\mathrm{disc}(H(X)) \neq 0$ et il n'y a qu'un nombre fini d'idéaux maximaux de A qui contiennent $\mathrm{disc}(H(X))$. □

Remarque 3.3.15 On verra que $\mathbb{Z}$ n'admet aucune extension non triviale non-ramifiée au-dessus de tout nombre premier (corollaire 4.2.16). Autrement dit $\mathbb{Z}$ est une sorte d'espace simplement connexe. Il en est de même pour l'anneau $\mathbb{C}[X]$, cela résulte du fait que l'espace topologique $\mathbb{C}$ est simplement connexe.

En revanche, si k est un corps de caractéristique $p > 0$, l'extension finie non triviale $A = k[t] \subset B = k[y]$ avec $t = y^p - y$ est non-ramifiée au-dessus de tout idéal maximal de A.

Chapitre 4

Groupe des classes des corps de nombres

Le groupe des classes d'un anneau de Dedekind A est un groupe commutatif qui mesure en quelque sorte le défaut de A à être principal. Il est trivial si et seulement si A est principal, cf. proposition 3.1.25. Plus précisément, si I est un idéal non nul de A, et si sa classe dans $\mathrm{Cl}(A)$ est d'ordre fini égal à e, alors I^e est un idéal principal. Dans ce chapitre nous étudions le groupe des classes de l'anneau des entiers d'un corps de nombres. Nous montrons notamment que ce groupe est fini (4.1.8) et donnons aussi une borne en termes de certains invariants du corps de nombres (4.2.10).

4.1 Finitude du groupe des classes

Pour évaluer la taille de $\mathrm{Cl}(A)$ lorsque A est un anneau d'entiers, on va montrer que tout idéal fractionnaire est équivalent à un idéal de petite norme.

4.1.1 Norme absolue

Proposition 4.1.1 (et définition)**.** *Soit L un corps de nombres. Soit I un idéal non nul de $\mathcal{O}_L$. Alors l'anneau quotient $\mathcal{O}_L/I$ est fini. Son cardinal est appelé* la norme de I *et est noté $N(I)$.*

Démonstration. Considérons l'idéal $I \cap \mathbb{Z}$ de $\mathbb{Z}$, il est principal, égal à $d\mathbb{Z}$ pour un certain $d \geq 0$. Soit $b \in I$ non nul. Son polynôme minimal sur $\mathbb{Q}$ appartient à $\mathbb{Z}[X]$, et le terme constant a_0 est non nul. Comme $a_0 \in I \cap \mathbb{Z}$, on a $d \neq 0$. Comme $d \in I$, on a $d\mathcal{O}_L \subseteq I$.

On a une application surjective $\mathbb{Z}$-linéaire $\mathbb{Z}^n \to \mathcal{O}_L$, d'où une application surjective $\mathbb{Z}^n/d\mathbb{Z}^n \to \mathcal{O}_L/d\mathcal{O}_L$. Comme le membre de gauche est fini (il a d^n éléments), celui de droite aussi. Or $\mathcal{O}_L/I$ est un quotient de $\mathcal{O}_L/d\mathcal{O}_L$, il est donc fini. □

Exemple 4.1.2 Lorsque $L = \mathbb{Q}$, on a $I = k\mathbb{Z}$ et $N(I) = |k|$.

Lemme 4.1.3. *Soit $\mathfrak{q}$ un idéal maximal de $\mathcal{O}_L$, soit p le générateur premier de l'idéal maximal $\mathfrak{q} \cap Z = p\mathbb{Z}$ et notons $f_\mathfrak{q} = [\mathcal{O}_L/\mathfrak{q} : \mathbb{Z}/p\mathbb{Z}]$. Alors $N(\mathfrak{q}) = p^{f_\mathfrak{q}}$, et $N(\mathfrak{q}^r) = N(\mathfrak{q})^r$ pour tout $r \geq 0$ (par convention $\mathfrak{q}^0 = \mathcal{O}_L$).*

Démonstration. En effet, pour tout $r \geq 1$, le noyau de la surjection canonique $\mathcal{O}_L/\mathfrak{q}^r \to \mathcal{O}_L/\mathfrak{q}^{r-1}$ est égal $\mathfrak{q}^r/\mathfrak{q}^{r-1} \simeq \mathcal{O}_L/\mathfrak{q}$ (lemme 3.3.3) qui est de cardinal p^f. Cela implique immédiatement le résultat recherché. □

Proposition 4.1.4. *Soit L un corps de nombre.*

(1) *Soit I un idéal non nul de $\mathcal{O}_L$ et soit*

$$I = \prod_i \mathfrak{q}_i^{r_i}$$

sa décomposition en product d'idéaux maximaux. Soit $p_i \in \mathbb{N}$ tel que $\mathfrak{q}_i \cap \mathbb{Z} = p_i\mathbb{Z}$ et soit $f_i = [\mathcal{O}_L/\mathfrak{q}_i : \mathbb{Z}/p_i\mathbb{Z}]$. Alors

$$N(I) = \prod_i p_i^{f_i r_i}.$$

(2) *Si $I, J \subseteq \mathcal{O}_L$ sont non nuls, alors $N(IJ) = N(I)N(J)$.*

Démonstration. (1) En regroupant les $\mathfrak{q}_i$, on peut les supposer deux à deux distincts. Le théorème des restes chinois 3.1.31 implique que $\mathcal{O}_L/I \simeq \prod_i \mathcal{O}_L/\mathfrak{q}_i^{r_i}$, donc

$$|\mathcal{O}_L/I| = \prod_i |\mathcal{O}_L/\mathfrak{q}_i^{r_i}| = \prod_i N(\mathfrak{q}_i^{r_i}).$$

On conclut par le lemme qui précède.

(2) Quitte à admettre des exposants nuls, on peut écrire

$$I = \prod_i \mathfrak{q}_i^{r_i}, \quad J = \prod_i \mathfrak{q}_i^{s_i}.$$

Donc $IJ = \prod_i \mathfrak{q}_i^{r_i+s_i}$. L'égalité $N(IJ) = N(I)N(J)$ est alors une conséquence immédiate de (1). □

Proposition 4.1.5. *Soit L un corps de nombres, soit $\alpha \in \mathcal{O}_L$ non nul. Alors $N(\alpha\mathcal{O}_L) = |N_{L/\mathbb{Q}}(\alpha)|$.*

Démonstration. Le $\mathbb{Z}$-module $\mathcal{O}_L$ est libre de rang $n := [L : \mathbb{Q}]$. Il existe une base $\{e_1, \ldots, e_n\}$ de $\mathcal{O}_L$ comme $\mathbb{Z}$-module et $a_1, \ldots, a_n \in \mathbb{Z}$ des entiers non nuls tels que $\{a_1e_1, \ldots, a_ne_n\}$ soit une base de $\alpha\mathcal{O}_L$ (théorème de la base adaptée 1.2.2). Or $\{\alpha e_1, \ldots, \alpha e_n\}$ est aussi une base de $\alpha\mathcal{O}_L$ sur $\mathbb{Z}$, il existe donc une matrice inversible $U \in \mathrm{GL}_n(\mathbb{Z})$ telle que $(\alpha e_1, \ldots, \alpha e_n)^t = U \cdot (a_1e_1, \ldots, a_ne_n)^t$. Soit M la matrice de l'application $[\alpha] : \mathcal{O}_L \to \mathcal{O}_L$ (multiplcation par α). Alors $M = UD$

où D est la matrice diagonale dont les éléments diagonaux sont $a_1, \ldots, a_n$. Par conséquent,

$$|N_{L/\mathbb{Q}}(\alpha)| = |\det M| = |\det U||\prod_i a_i| = \prod_i |a_i|.$$

D'autre part $N(\alpha\mathcal{O}_L) = |\mathcal{O}_L/\alpha\mathcal{O}_L| = |\prod_i \mathbb{Z}/a_i\mathbb{Z}| = |\prod_i a_i|$. D'où la proposition. □

4.1.2 Application au groupe des classes

La norme absolue est une mesure sur l'ensemble des idéaux non nuls de $\mathcal{O}_L$. Le lemme suivant dit que l'espace des idéaux est discret.

Lemme 4.1.6. *Fixons un corps de nombres L. Soit $c > 0$ un nombre réel. Alors l'ensemble des idéaux non nuls J de $\mathcal{O}_L$ tels que $N(J) \leq c$ est fini.*

Démonstration. Soit $J = \prod_i \mathfrak{q}_i^{r_i}$ la factorisationc avec $r_i \geq 1$ et $N(J) \leq c$. Soit $p_i\mathbb{Z} = \mathfrak{q}_i \cap \mathbb{Z}$. Alors $N(J) = \prod_i p_i^{r_i f_i} \leq c$. Donc $p_i \leq c$ et $r_i \leq c$. Comme il n'y a qu'un nombre fini de $\mathfrak{q}_i$ contenant $p_i\mathcal{O}_L$ avec p_i fixé, on voit que les ensembles des $\mathfrak{q}_i$ et des r_i qui interviennent dans la factorisation des J de $N(J) \leq c$ sont finis. Il n'y a donc qu'un nombre fini de J avec $N(J) \leq c$. □

Lemme 4.1.7. *Soit L un corps de nombres. Alors il existe une constante réelle $c > 0$ avec la propriété suivante : pour tout idéal fractionnaire M de $\mathcal{O}_L$, il existe $\alpha \in K^*$ et un idéal non nul J de $\mathcal{O}_L$ tels que $M = \alpha J$ et $N(J) \leq c$.*

Démonstration. On va montrer le lemme en trois étapes. Soit $n = [L : \mathbb{Q}]$ et fixons une base $e_1, \ldots, e_n$ de $\mathcal{O}_L$ sur $\mathbb{Z}$. C'est aussi une base de L sur $\mathbb{Q}$.

(A) *Il existe une constante $c > 0$ telle que pour tout $(a_1, \ldots, a_n) \in \mathbb{Q}^n$, on ait*

$$|N_{L/\mathbb{Q}}(\sum_i a_i e_i)| \leq c \max_i\{|a_i|^n\}. \tag{4.1}$$

En effet, fixons une base $\{e_1, \ldots, e_n\}$ de l'espace vectoriel $L/\mathbb{Q}$. L'application $[x] : L \to L$ multiplication par $x = \sum_i t_i e_i$ vérifie $[x] = \sum_i t_i[e_i]$, donc sa matrice dans une base de $L/\mathbb{Q}$ s'écrit $\mathrm{Mat}([x]) = \sum_i t_i \mathrm{Mat}([e_i])$. C'est une matrice à coefficients dans $\mathbb{Q}[t_1, \ldots, t_n]$, donc de déterminant

$$N_{L/\mathbb{Q}}(x) = \det[x] = P(t_1, \ldots, t_n) \in \mathbb{Q}[t_1, \ldots, t_n].$$

Il existe une constante réelle $c > 0$ telle que

$$|P(t_1, \cdots, t_n)| \leq c, \quad \forall (t_1, \ldots, t_n) \in [0, 1]^n.$$

Pour tout $(a_1, \cdots, a_n) \in \mathbb{Q}^n$ non nul, on prend $a \in \mathbb{Q}$ tel que $|a| = \max_i\{|a_i|\}$. Alors

$$N_{L/\mathbb{Q}}(\sum_i a_i e_i) = a^n N_{L/\mathbb{Q}}(\sum_i (a_i/a) e_i) = a^n P(a_1/a, \ldots, a_n/a).$$

D'où $|N_{L/\mathbb{Q}}(\sum_i a_i e_i)| \leq c \max_i\{|a_i|^n\}$.

(B) *Pour tout idéal non nul J de $\mathcal{O}_L$, il existe un $\alpha \in J$ non nul tel que* $|N_{L/\mathbb{Q}}(\alpha)| \leq cN(J)$. Considérons l'ensemble

$$E = \left\{ \sum_i a_i e_i \in \mathcal{O}_L \mid a_i \in \mathbb{Z}, 0 \leq a_i \leq N(J)^{1/n} \right\}.$$

Alors

$$|E| = ([N(J)^{1/n}] + 1)^n > N(J).$$

Donc il existe $x, y \in E$ distincts ayant la même image dans $\mathcal{O}_L/J$ (ce dernier a $N(J)$ éléments). Leur différence $\alpha \in \mathcal{O}_L$ vérifie

$$|N_{L/\mathbb{Q}}(\alpha)| \leq cN(J)$$

car les coordonnées de α dans la base e_i appartiennent à $[-N(J)^{1/n}, N(J)^{1/n}]$.

(C) *Preuve du lemme.* L'idéal fractionnaire M est équivalent à un idéal non nul J' de $\mathcal{O}_L$ (proposition 3.1.11). Par (B), il existe $\alpha \in J'$ non nul tel que $|N_{L/\mathbb{Q}}(\alpha)| \leq cN(J')$. Soit $J = \alpha J'^{-1} \subseteq \mathcal{O}_L$. On a $\alpha\mathcal{O}_L = J'J$, donc $N(\alpha\mathcal{O}_L) = N(J')N(J)$. Il résulte de la proposition 4.1.5 que $N(J) = |N_{L/\mathbb{Q}}(\alpha)|N(J')^{-1} \leq c$. Comme M est équivalent à J'^{-1} donc à J, le lemme est prouvé. □

Theorem 4.1.8. *Soit L un corps de nombres. Alors* $\mathrm{Cl}(\mathcal{O}_L)$ *est fini.*

Démonstration. D'après le lemme 4.1.7 ci-dessus, il existe une constante $c > 0$ telle que tout idéal fractionnaire soit équivalent à un idéal non nul J de norme $N(J) \leq c$. Mais il n'existe qu'un nombre fini de tels J d'après le lemme 4.1.6. Donc $\mathrm{Cl}(\mathcal{O}_L)$ est fini. □

Corollaire 4.1.9. *Soit c une constante donnée par le lemme 4.1.7. Alors* $\mathrm{Cl}(\mathcal{O}_L)$ *est engendré par les classes des idéaux maximaux $\mathfrak{q}$ avec $N(\mathfrak{q}) \leq c$. De plus, ces idéaux maximaux vérifient $\mathfrak{q} \cap \mathbb{Z} = p\mathbb{Z}$ avec $p^{f_\mathfrak{q}} \leq c$ où $f_\mathfrak{q}$ est le degré de l'extension résiduelle $\mathbb{Z} \to \mathcal{O}_L$ en $\mathfrak{q}$.*

Exemple 4.1.10 Soit $L = \mathbb{Q}[\sqrt{2}]$. Alors $\{1, \sqrt{2}\}$ est une base de $\mathcal{O}_L$ sur $\mathbb{Z}$ et la constante $c = 2$ convient pour lemme 4.1.7. Pour déterminer $\mathrm{Cl}(\mathcal{O}_L)$, on doit donc chercher les $\mathfrak{q}$ au-dessus de $p = 2$. On a $\mathcal{O}_L = \mathbb{Z}[\sqrt{2}] \simeq \mathbb{Z}[X]/(X^2 - 2)$. Comme $X^2 - 2 \equiv X^2 \mod 2$, on a $2\mathcal{O}_L = \mathfrak{q}_2^2$ avec $\mathfrak{q}_2 = (2, \sqrt{2}) = \sqrt{2}\mathcal{O}_L$ (proposition 3.3.11). Donc $\mathfrak{q}_2$ est principal et $\mathrm{Cl}(\mathcal{O}_L) = 1$. Par suite $\mathbb{Z}[\sqrt{2}]$ est un anneau principal. En fait il est facile de montrer que c'est même un anneau euclidien.

Exemple 4.1.11 Soit $L = \mathbb{Q}[\sqrt{-5}]$. On a $\mathcal{O}_L = \mathbb{Z}[\sqrt{-5}]$ car $-5 \equiv 3 \mod 4$. On voit que $c = 6$ convient car

$$|N_{L/\mathbb{Q}}(a_1 + a_2\sqrt{-5})| = |a_1^2 + 5a_2^2| \leq 6 \max\{|a_1|^2, |a_2|^2\}.$$

Il faut considérer les décompositions des idéaux $2\mathcal{O}_L, 3\mathcal{O}_L$ et $5\mathcal{O}_L$. On a $X^2+5 = (X+1)^2 \in \mathbb{F}_2[X]$, $X^2+5 = (X-1)(X+1) \in \mathbb{F}_3[X]$ et $X^2-5 = X^2 \in \mathbb{F}_5[X]$. Donc

$$2\mathcal{O}_L = \mathfrak{q}_2^2, \quad 3\mathcal{O}_L = \mathfrak{q}_{3,1}\mathfrak{q}_{3,2}, \quad 5\mathcal{O}_L = \mathfrak{q}_5^2$$

avec $\mathfrak{q}_2 = (2, \sqrt{-5}+1)$, $\mathfrak{q}_{3,1} = (3, \sqrt{-5}+1)$, $\mathfrak{q}_{3,2} = (3, \sqrt{-5}-1)$, et $\mathfrak{q}_5 = (5, \sqrt{-5}) = \sqrt{-5}\mathcal{O}_L$. Il suit que $\mathrm{Cl}(\mathcal{O}_L)$ est engendré par les classes de $\mathfrak{q}_2 = (2, 1+\sqrt{-5})$ et de $\mathfrak{q}_3 := \mathfrak{q}_{3,1}$ (noter que $3\mathcal{O}_L = \mathfrak{q}_{3,1}\mathfrak{q}_{3,2}$, donc la classe de $\mathfrak{q}_{3,2}$ est égale à l'inverse de la classe de $\mathfrak{q}_3$ dans $\mathrm{Cl}(\mathcal{O}_L)$).

On a $1+\sqrt{-5} \in \mathfrak{q}_2 \cap \mathfrak{q}_3 = \mathfrak{q}_2\mathfrak{q}_3$ et $N(1+\sqrt{-5}) = 6 = N(\mathfrak{q}_2\mathfrak{q}_3)$. Donc $(1+\sqrt{-5})\mathcal{O}_L = \mathfrak{q}_2\mathfrak{q}_3$ et $\mathrm{Cl}(\mathcal{O}_L)$ est engendré par la classe de $\mathfrak{q}_2$ qui est d'ordre 1 ou 2 (puisque $2\mathcal{O}_L = \mathfrak{q}_2^2$).

Montrons que $\mathfrak{q}_2$ n'est pas principal. S'il était engendré par $a+b\sqrt{-5}$, alors $2 = N(\mathfrak{q}_2) = N(a+b\sqrt{-5}) = a^2+5b^2$. Ce qui n'a pas de solution avec $a, b \in \mathbb{Z}$. Nous concluons que $\mathrm{Cl}(\mathcal{O}_L)$ est un groupe d'ordre 2 engendré par la classe de $\mathfrak{q}_2$. Comme corollaire, pour tout idéal J de $\mathcal{O}_L$, J^2 est principal.

Remarque 4.1.12 En dehors des anneaux d'entiers d'un corps de nombres, il y a d'autres cas où la finitude est valide : si A est un anneau de Dedekind qui est fini sur un anneau de polynômes $F[X]$ à coefficients dans un corps fini F, alors on peut montrer que $\mathrm{Cl}(A)$ est fini.

Mais en général le groupe des classes d'un anneau de Dedekind n'est pas fini. On peut en donner des contre-exemples avec des courbes elliptiques E sur $\mathbb{C}$. Il s'agit d'anneaux du type

$$A = \mathbb{C}[X,Y]/(Y^2 + X^3 + aX + b)$$

avec $a, b \in \mathbb{C}$ fixés et vérifiant $4a^3 + 27b^2 \neq 0$. On peut montrer que A est un anneau de Dedekind (exercice) et que $\mathrm{Cl}(A)$ a toujours des éléments d'ordre infini (en utilisant des outils de géométrie algébrique).

4.2 Borne de Minkowski

Le théorème de finitude 4.1.8, s'il est suffisant pour l'aspect théorique, ne permet pas de déterminer le groupe des classes de façon efficace. Le corollaire 4.1.9 fournit une methode plus concrète, mais la constante c n'est pas toujours aisée à trouver ni optimale. Dans ce paragraphe, nous allons présenter une nette amélioration par la borne de Minkowski (théorème 4.2.10). La méthode de Minkowski (lemme 4.2.5) est à l'origine d'une branche de théorie des nombres appelée la géométrie des nombres.

4.2.1 Rudiments sur les réseaux

Dans toute cette partie, on fixe un entier $n \geq 1$ et on note $V = \mathbb{R}^n$ et $\{e_1, \ldots, e_n\}$ sa base canonique.

Définition 4.2.1 Un *réseau* dans V est un sous-$\mathbb{Z}$-module libre Λ de V, de rang n et contenant une base vectorielle de V. De façon équivalente, Λ est un sous-$\mathbb{Z}$-module de V engendré par une base de V.

Par exemple, $\mathbb{Z}^2$ est un réseau dans $\mathbb{R}^2$, mais $\mathbb{Z}(1,0) + \mathbb{Z}(\sqrt{2},0)$, bien que libre de rang 2 sur $\mathbb{Z}$, n'est pas un réseau.

Remarque 4.2.2 Tout réseau Λ de V est *discret* : c'est-à-dire que pour tout point $v \in \Lambda$, il existe un voisinage ouvert Ω de v dans V tel que $\Omega \cap \Lambda = \{v\}$. En effet, par translation, il suffit de montrer cette propriété pour $v = 0 \in V$. Soit $\varepsilon_1, \ldots, \varepsilon_n$ une base de Λ (en tant que $\mathbb{Z}$-module), donc une base vectorielle de V. Par l'équivalence des normes sur V, il existe une constant $\delta > 0$ telle que

$$||\sum_i x_i \varepsilon_i||_e \geq \delta \max_i\{|x_i|\}$$

où $||.||_e$ désigne la norme euclidienne. On obtient le résultat désiré en prenant $\Omega = \{x \in V \mid ||x||_e < \delta\}$.

Si Λ est un réseau avec une base $\underline{\varepsilon} = \{\varepsilon_1, \ldots, \varepsilon_n\}$, on définit un *domaine fondamental* (dépendant du choix d'une base)

$$F(\Lambda, \underline{\varepsilon}) = \left\{ \sum_{1 \leq i \leq n} x_i \varepsilon_i \mid x_i \in \mathbb{R}, 0 \leq x_i < 1 \right\} \subset V.$$

Notons qu'un domaine fondamental induit une partition de V :

$$V = \coprod_{\lambda \in \Lambda} (F(\Lambda, \underline{\varepsilon}) + \lambda),$$

et chaque morceau $F(\Lambda, \underline{\varepsilon}) + \lambda$ contient un et un seul vecteur de Λ.

Lemme 4.2.3. *Avec les notations ci-dessus, on a les propriétés suivantes.*

(1) *L'ensemble $F(\Lambda, \underline{\varepsilon})$ est mesurable, son volume est égal à $|\det M|$ où M est la matrice des ε_i dans la base orthonormée $\{e_1, \ldots, e_n\}$ de V.*

(2) *Le volume $v(F(\Lambda), \underline{\varepsilon})$ ne dépend pas du choix d'une base $\underline{\varepsilon}$ de Λ.*

Démonstration. (1) Soit

$$T : \mathbb{R}^n \to V, \quad (x_1, \ldots, x_n) \mapsto \sum_i x_i \varepsilon_i.$$

C'est un isomorphisme $\mathbb{R}$-linéaire et on a $T([0,1[^n) = F(\Lambda, \underline{\varepsilon})$. Le volume du domaine fondamental est donné par

$$\int_{F(\Lambda, \underline{\varepsilon})} dy_1 \ldots dy_n = \int_{[0,1[^n} |\det T| dx_1 \ldots dx_n = |\det T|$$

(changement de variables). Or M est aussi la matrice de l'endomorphisme T dans la base canonique, donc le volume de $F(\Lambda, \underline{\varepsilon})$ est égal à $|\det M|$.

(2) Si on change la base $\underline{\varepsilon}$ en $\underline{\varepsilon}'$, le quotient $\det T / \det T'$ est égal au déterminant de la matrice de passage qui vaut ± 1. Donc $|\det T| = |\det T'|$. □

Définition 4.2.4 On notera $\mathrm{vol}(\Lambda)$ le volume de $F(\Lambda, \underline{\varepsilon})$. C'est le *volume du réseau* Λ. Il est indépendant du choix d'une base de Λ.

Lemme 4.2.5 (Minkowski)**.** *Soit Δ une partie convexe compacte de V, symétrique par rapport à l'origine ($v \in \Delta \Longrightarrow -v \in \Delta$). Supposons* $\mathrm{vol}(\Delta) \geq 2^n \mathrm{vol}(\Lambda)$. *Alors $\Lambda \cap \Delta \neq \{0\}$.*

Démonstration. Fixons un domaine fondamental $F := F(\Lambda, \underline{\varepsilon})$. On suppose d'abord $\mathrm{vol}(\Delta) > 2^n \mathrm{vol}(\Lambda)$. Posons

$$\Delta/2 = \{x/2;\ x \in \Delta\}.$$

Elle a pour volume $\mathrm{vol}(\Delta/2) = \mathrm{vol}(\Delta)/2^n > \mathrm{vol}(\Lambda)$ et se découpe en une réunion disjointe

$$\Delta/2 = \coprod_{\lambda \in \Lambda} [(F + \lambda) \cap \Delta/2].$$

Il suit que

$$\mathrm{vol}(\Delta/2) = \sum_{\lambda \in \Lambda} \mathrm{vol}((F + \lambda) \cap \Delta/2) = \sum_{\lambda \in \Lambda} \mathrm{vol}\left(F \cap (\Delta/2 - \lambda)\right).$$

Par conséquent, si les parties $\Delta/2 - \lambda$, $\lambda \in \Lambda$, étaient deux à deux disjointes, comme $F \cap (\Delta/2 - \lambda) \subseteq F$, on aurait $\mathrm{vol}(\Delta/2) \leq \mathrm{vol}(F) = \mathrm{vol}(\Lambda)$, ce qui est contraire à l'hypothèse. Il existe donc $\lambda, \mu \in \Lambda$ distincts tels que $(\Delta/2 - \lambda) \cap (\Delta/2 - \mu) \neq \emptyset$. Donc il existe $x, y \in \Delta$ tels que $x/2 - \lambda = y/2 - \mu$, et donc

$$\lambda - \mu = (x - y)/2.$$

Or Δ est symétrique et convexe, $-y \in \Delta$ et $(x - y)/2 \in \Delta$. Donc $\lambda - \mu \in \Lambda \cap \Delta$ et est non nul.

Supposons maintenant $\mathrm{vol}(\Delta) = 2^n \mathrm{vol}(\Lambda)$. Soit $m > 0$ un entier. Alors on peut appliquer le résultat qu'on vient de montrer à $(1 + 1/m)\Delta$ car ce dernier est convexe, symétrique par rapport à l'origine, et son volume vérifie

$$\mathrm{vol}((1 + 1/m)\Delta) = (1 + 1/m)^n \mathrm{vol}(\Delta) > 2^n \mathrm{vol}(\Lambda).$$

Donc $(1 + 1/m)\Delta \cap \Lambda$ contient au moins deux points. Comme Λ est discret (remarque 4.2.2) et que $(1+1/m)\Delta$ est compact, cette intersection est un espace topologique compact et discret, donc fini (voir aussi lemme 5.2.3). Quand m croit vers l'infini, les

$$(1 + 1/m)\Delta \cap \Lambda$$

sont des ensembles décroissants, finis (avec au moins deux éléments), donc stationnaires. Leur intersection est égale $\Delta \cap \Lambda$ et contient au moins deux éléments, en particulier un élément différent de 0. □

Exercice 4.2.6 Soit p un nombre premier $\equiv 1 \mod 4$. On veut montrer que p est somme de deux carrés.

1. Montrer qu'il existe $u \in \mathbb{F}_p^*$ d'ordre 4.
2. Soit $\varphi : \mathbb{Z}^2 \to \mathbb{F}_p$, $(x, y) \mapsto \overline{(x - uy)}$. Montrer que $\Lambda := \ker \varphi$ est un réseau dans $\mathbb{R}^2$, de volume p.
3. Soit $\Delta \subset \mathbb{R}^2$ le disque fermé centré en l'origine et de rayon $r = \sqrt{3p/2}$. Montrer qu'il existe $a, b \in \Lambda$ tels que $0 < a^2 + b^2 < 3p/2$.
4. Montrer que $a^2+b^2 = p$ (montrer que $a^2+b^2 \in p\mathbb{N}$ en utilisant la définition de Λ). Cela se démontre également avec l'anneau des entiers de Gauss $\mathbb{Z}[i]$.

4.2.2 Applications aux corps de nombres

On fixe un corps de nombres L de degré $n = [L : \mathbb{Q}]$, de *discriminant* $d_L := D_{\mathcal{O}_L/\mathbb{Z}}$ (voir 2.3.14). Soient $r_1, 2r_2$ les nombres de plongements réels et imaginaires (définition 2.2.23). On sait que $n = r_1 + 2r_2$ (proposition 2.2.24).

Soient $\sigma_1, \ldots, \sigma_{r_1}$ les plongements réels et $\sigma_{r_1+1}, \bar{\sigma}_{r_1+1}, \ldots, \sigma_{r_1+r_2}, \bar{\sigma}_{r_1+r_2}$ Les plongements imaginaires. On a alors un homomorphisme d'anneaux injectif et $\mathbb{Q}$-linéaire

$$\rho : L \to V := \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}, \quad x \mapsto (\sigma_1(x), \ldots, \sigma_{r_1}(x), \sigma_{r_1+1}(x), \ldots, \sigma_{r_1+r_2}(x)).$$

On considère V comme un espace vectoriel sur $\mathbb{R}$ (de dimension n) en utilisant l'identification de $\mathbb{C}$ avec $\mathbb{R}^2$: $x + iy \mapsto (x, y)$.

Lemme 4.2.7. *Soit J un idéal non nul de $\mathcal{O}_L$. Alors $\rho(J)$ est un réseau dans V, de volume*

$$\mathrm{vol}(\rho(J)) = 2^{-r_2} N(J) |d_L|^{1/2}.$$

Démonstration. L'idéal J est un $\mathbb{Z}$-module de type fini et sans torsion, donc libre de rang fini. Comme $\mathcal{O}_L/J$ est fini (proposition 4.1.1), J a le même $\mathbb{Z}$-rang que $\mathcal{O}_L$ (utiliser le théorème des bases adaptées 1.2.2), c'est-à-dire n. Soit $\varepsilon_1, \ldots, \varepsilon_n$ une base de J sur $\mathbb{Z}$. Soit M la matrice des $\rho(\varepsilon_i)$ dans la base canonique de V. On va montrer que

$$|\det M| = 2^{-r_2} N(J) |d_L|^{1/2}.$$

En particulier on aura $\det M \neq 0$, ce qui montrera que $\rho(\varepsilon_1), \ldots, \rho(\varepsilon_n)$ est libre sur $\mathbb{R}$ et donc que $\rho(J)$ est un réseau dans V dont le volume est comme prédit (lemme 4.2.3 et définition 4.2.4).

Considérons les vecteurs lignes de la matrice M : pour $i \leq r_1$,

$$L_i = (\sigma_i(\varepsilon_1), \ldots, \sigma_i(\varepsilon_n)) \in V$$

et pour $r_1 + 1 \leq j \leq r_1 + r_2$,

$$L'_j = (\mathrm{Re}(\sigma_j(\varepsilon_1)), \ldots, \mathrm{Re}(\sigma_j(\varepsilon_n)))$$

$$L''_j = (\mathrm{Im}(\sigma_j(\varepsilon_1)), \ldots, \mathrm{Im}(\sigma_j(\varepsilon_n))).$$

Le déterminant de M ne change pas si, pour tout $j \geq r_1 + 1$, on remplace L'_j par

$$L_j := L'_j + \sqrt{-1} L''_j = (\sigma_j(\varepsilon_1), \ldots, \sigma_j(\varepsilon_n)).$$

Maintenant dans la nouvelle matrice, on remplace L''_j par

$$\bar{L}_j = L_j - 2\sqrt{-1}L''_j = (\bar{\sigma}_j(\varepsilon_1), \dots, \bar{\sigma}_j(\varepsilon_n)).$$

On obtient alors une nouvelle matrice D avec $\det D = (-2\sqrt{-1})^{r_2} \det M$. Par ailleurs, l'ensemble $\mathrm{Isom}_{\mathbb{Q}}(L, \bar{\mathbb{Q}})$ des plongements de L dans $\bar{\mathbb{Q}}$ est égal à

$$\{\sigma_1, \dots, \sigma_{r_1+r_2}, \bar{\sigma}_{r+1}, \dots, \bar{\sigma}_{r_1+r_2}\},$$

et la matrice D est celle qui permet de calculer le discriminant

$$D_{\mathcal{O}_L/\mathbb{Z}}(\underline{\varepsilon}) = (\det D)^2$$

(théorème 2.2.14 et remarque 2.3.13). Il suit que $|\det M| = 2^{-r_2}|D_{\mathcal{O}_L/\mathbb{Z}}(\underline{\varepsilon})|^{1/2}$. Il ne reste plus qu'à comparer $D_{\mathcal{O}_L/\mathbb{Z}}(\underline{\varepsilon})$ avec d_L.

Le théorème des bases adaptées 1.2.2 dit qu'il existe une base $\varepsilon'_1, \dots, \varepsilon'_n$ de $\mathcal{O}_L$ sur $\mathbb{Z}$ et des $a_1, \dots, a_n \in \mathbb{Z}$ non nuls tels que $a_1\varepsilon'_1, \dots, a_n\varepsilon'_n$ soit une base de J. Il suit que

$$D_{\mathcal{O}_L/\mathbb{Z}}(\underline{\varepsilon}) = D_{\mathcal{O}_L/\mathbb{Z}}(\{a_1\varepsilon'_1, \dots, a_n\varepsilon'_n\}) = (a_1 \dots a_n)^2 D_{\mathcal{O}_L/\mathbb{Z}}(\underline{\varepsilon'}).$$

Par ailleurs, $\mathcal{O}_L/J \simeq \oplus_{1\leq i\leq n}\mathbb{Z}/a_i\mathbb{Z}$, donc $N(J) = |a_1 \dots a_n|$. D'où

$$D_{\mathcal{O}_L/\mathbb{Z}}(\underline{\varepsilon}) = N(J)^2 d_L.$$

Ce qui achève la démonstration. □

Lemme 4.2.8. *Soit $V = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ comme ci-dessus. Pour tout nombre réel $t > 0$, on pose*

$$\Delta_t = \left\{ (x_1, \dots, x_{r_1}, z_1, \dots, z_{r_2}) \in V \;\middle|\; \sum_i |x_i| + 2\sum_j |z_j| \leq t \right\}.$$

C'est une partie convexe compacte de V, symétrique par rapport à l'origine. Son volume vaut

$$\mathrm{vol}(\Delta_t) = 2^{r_1}(\pi/2)^{r_2} t^n/n!.$$

Démonstration. Seul le calcul du volume est non trivial. On se ramène par homothétie à $t = 1$. Ensuite il y a un calcul explicit assez long. Le résultat est admis. [1] □

Lemme 4.2.9. (Inégalité arithmético-géométrique) *Soient $x_1, \dots, x_n \geq 0$ des nombres réels. Alors*

$$(x_1 \dots x_n)^{1/n} \leq \frac{x_1 + \dots + x_n}{n}.$$

1. On peut trouver une preuve dans Pierre Samuel : Théorie algébrique des nombres, pp 79-80, ou James Milne : Algebraic Number Theory (en ligne), Lemma 4.22.

Démonstration. On passe au logarithme. L'inégalité est alors une conséquence immédiate de la concavité de la fonction $\ln x$. □

Nous pouvons maintenant démontrer le théorème qui donne une majoration explicite de la constante c qui apparait dans le lemme 4.1.7.

Theorem 4.2.10. *Soit L un corps de nombres de degré n. Soit*

$$C_L = \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n}$$

la constante de Minkowski *de L. Alors tout idéal fractionnaire de $\mathcal{O}_L$ est équivalent à un idéal J' de norme*

$$N(J') \leq C_L |d_L|^{1/2}.$$

Démonstration. Soit M un idéal fractionnaire. Alors M^{-1} est équivalent à un idéal non nul $J \subseteq \mathcal{O}_L$. On conserve les notations du lemme 4.2.8 ci-dessus et on choisit t de sorte que

$$\mathrm{vol}(\Delta_t) = 2^n \mathrm{vol}(\rho(J)).$$

D'après les lemmes 4.2.7 et 4.2.8, cette égalité équivaut à

$$t^n = (4/\pi)^{r_2} n! N(J) |d_L|^{1/2} = n^n N(J) C_L |d_L|^{1/2}.$$

Fixons t avec cette condition. D'après le lemme 4.2.5, il existe $\alpha \in J$ non nul tel que $\rho(\alpha) \in \Delta_t$, c'est-à-dire que

$$|\sigma_1(\alpha)| + \cdots + |\sigma_{r_1}(\alpha)| + 2|\sigma_{r_1+1}(\alpha)| + \cdots + 2|\sigma_{r_1+r_2}(\alpha)| \leq t.$$

Par l'inégalité arithmético-géométrique 4.2.9, on a

$$|\sigma_1(\alpha)| \cdots |\sigma_{r_1}(\alpha)| . |\sigma_{r_1+1}(\alpha)|^2 \cdots |\sigma_{r_1+r_2}(\alpha)|^2 \leq (t/n)^n = t^n/n^n.$$

Or le membre de gauche est égal à $|N_{L/\mathbb{Q}}(\alpha)|$ (théorème 2.2.11) et celui de droite est égal à $N(J) C_L |d_L|^{1/2}$ par le choix de t. Par suite, $|N_{L/\mathbb{Q}}(\alpha)| \leq N(J) C_L |d_L|^{1/2}$. Il suit que

$$N(\alpha J^{-1}) \leq C_L |d_L|^{1/2}$$

avec $\alpha J^{-1} \subseteq \mathcal{O}_L$ équivalent à M. □

Remarque 4.2.11 Comme pour le corollaire 4.1.9, le théorème dit que le groupe des classes $\mathrm{Cl}(\mathcal{O}_L)$ est engendré par les classes des idéaux maximaux $\mathfrak{q}$ vérifiant $N(\mathfrak{q}) \leq C_L |d_L|^{1/2}$. Soit $p\mathbb{Z} = \mathfrak{q} \cap \mathbb{Z}$, alors l'inégalité veut dire $p^f \leq C_L |d_L|^{1/2}$, où $f = f_{\mathfrak{q}/p\mathbb{Z}}$. Donc les idéaux $\mathfrak{q}$ sont à chercher parmi les idéaux maximaux au-dessus des premiers p tels que $p^f \leq C_L |d_L|^{1/2}$.

Exemple 4.2.12 Soit $L = \mathbb{Q}[\sqrt{-5}]$. On a $-5 \equiv 3 \mod 4$, donc $d_L = -20$ (exemple 2.3.21). On a

$$C_L|d_L|^{1/2} = (4/\pi)(2!/2^2)\sqrt{20} = 2,8...$$

Il suit que $\mathrm{Cl}(\mathcal{O}_L)$ est engendré par les classes des idéaux de norme $\leq 2,8$, donc de norme ≤ 2. On est ainsi passé de $c = 6$ de l'exemple 4.1.11 à $c = 2$. La dernière partie de 4.1.11 montre que $\mathrm{Cl}(\mathcal{O}_L)$ est engendré par la classe de $\mathfrak{q}$ et que $h_L = 2$.

Exemple 4.2.13 Considérons $L = \mathbb{Q}[\alpha]$ où α est une racine de $X^3 - X - 1$. Ce polynôme est irréductible dans $\mathbb{F}_2[X]$, donc irréductible sur $\mathbb{Q}$. Son discriminant vaut -23 et est sans facteur carré. Il suit que $d_L = D_{\mathcal{O}_L/\mathbb{Z}}(\{1, \alpha, \alpha^2\}) = -23 < 0$ (proposition 2.3.15). Comme $r_1 + 2r_2 = 3$, on a $r_2 = 1$ (proposition 2.2.27). Donc

$$C_L|d_L|^{1/2} = (4/\pi)(3!/27)\sqrt{23} = 1.35... < 2.$$

Tout idéal fractionnaire de $\mathcal{O}_L$ est équivalent à un idéal non nul J de $\mathcal{O}_L$ avec $N(J) < 2$, donc $N(J) = 1$ et $J = \mathcal{O}_L$. Par conséquent $h_L = 1$.

Exemple 4.2.14 Soit $L = \mathbb{Q}[\sqrt{-19}]$. On va montrer que $h_L = 1$. Donc $\mathcal{O}_L$ est un anneau principal. On sait par ailleurs (5.1.5) qu'il n'est pas euclidien. Comme $-19 \equiv 1 \mod 4$, on a $\mathcal{O}_L = \mathbb{Z}[\alpha]$ où $\alpha = (1 + \sqrt{-19})/2$ est racine du polynôme $X^2 - X + 5 \in \mathbb{Z}[X]$. On a donc $d_L = -19$ et

$$C_L|d_L|^{1/2} = (4/\pi)(2!/2^2)\sqrt{19} = 2,77... < 3$$

Comme $X^2 - X + 5 \equiv X^2 + X + 1 \mod 2$ est irréductible dans $\mathbb{F}_2[X]$, $2\mathcal{O}_L$ est maximal et est principal. Donc $h_L = 1$.

Exemple 4.2.15 Soit $L = \mathbb{Q}[\sqrt{-163}]$. On va montrer que $h_L = 1$. On a $-163 \equiv 1 \mod 4$. Donc $d_L = -163$. Il faut considérer les premiers

$$p \leq C_L\sqrt{163} = 2\sqrt{163}/\pi = 8,12...,$$

donc $p = 2, 3, 5$ ou 7. On a $\mathcal{O}_L = \mathbb{Z}[\alpha]$ avec le polynôme minimal de α égal à $X^2 + X + 41$. On vérifie que ce polynôme n'a pas de racine dans $\mathbb{F}_p$ pour $p \leq 7$. Il suit que tout $\mathfrak{q}$ au-dessus de $p \leq 7$ est principal, engendré par p. Donc $\mathcal{O}_L$ est principal.

Corollaire 4.2.16. *Soit L un corps de nombres de degré n.*

(1) *On a $|d_L| \geq \pi^n/4$.*

(2) *(Hermite-Minkowski) Si $L/\mathbb{Q}$ est non-ramifiée, alors $L = \mathbb{Q}$.*

Démonstration. (1) On peut supposer $n \geq 2$. D'après 4.2.10(1) il existe $\alpha \in \mathcal{O}_L$ non nul tel que $1 \leq |N_{L/\mathbb{Q}}(\alpha)| \leq C_L|d_L|^{1/2}$. Donc

$$|d_L| \geq (\pi/4)^{2r_2} n^{2n}/(n!)^2 \geq a_n := (\pi/4)^n n^{2n}/(n!)^2.$$

On a $a_2 = \pi^2/4$ et $a_{n+1}/a_n = (\pi/4)(1+1/n)^{2n}$. Or $(1+1/n)^n = 1+1+... \geq 2$ par la formule du binôme. Donc $(1+1/n)^{2n} \geq 4$. D'où $a_{n+1}/a_n \geq \pi$ et

$$a_n \geq (\pi^2/4)\pi^{n-2} = \pi^n/4.$$

(2) Il suit de (1) que si $n \geq 2$, $|d_L| \geq 3$. Donc $|d_L| = 1$ (ce qui équivaut à $L/\mathbb{Q}$ non-ramifiée, théorème 3.3.14) implique que $n = 1$ et $L = \mathbb{Q}$. □

Remarque 4.2.17 Quand $n = [L : \mathbb{Q}]$ tend vers l'infini, la formule de Stirling dit que $n!/n^n \simeq \sqrt{2\pi}\sqrt{n}e^{-n}$.

Exemple 4.2.18 L'extension $L := \mathbb{Q}[\sqrt{-1}, \sqrt{-5}]$ de $K := \mathbb{Q}[\sqrt{-5}]$ est non-ramifiée. En effet, $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$, et $\alpha := (\sqrt{-1} + \sqrt{-5})/2 \in L$ est zéro du polynôme $X^2 - \sqrt{-5}X - 1 \in \mathcal{O}_K[X]$ et le discriminant de L/K dans la base $\{1, \alpha\}$ vaut $\mathrm{disc}(X^2 - \sqrt{-5}X - 1) = -1$.

Exercice 4.2.19 Montrer que $\mathbb{Q}[\sqrt{-3}]$ est l'unique extension de $\mathbb{Q}$ avec $|d_L| = 3$.

Exercice 4.2.20 Calculer h_L pour $L = \mathbb{Q}[\sqrt{-6}]$ et trouver un générateur du groupe des classes.

Exercice 4.2.21 Soit L un corps de nombres.

1. Soit $\mathfrak{q}$ un maximal dont la classe dans $\mathrm{Cl}(\mathcal{O}_L)$ est d'ordre $m \geq 1$. Montrer qu'il existe une extension F/L de degré m telle que $\mathfrak{q}\mathcal{O}_F$ soit principal.
2. Montrer qu'il existe une extension finie H/L telle que pour tout idéal I de $\mathcal{O}_L$, $I\mathcal{O}_H$ est principal. En prenant la clôture galoisienne, on peut même supposer H galoisienne sur K.

Exercice 4.2.22 Soit $L = \mathbb{Q}[\sqrt{7}]$.

1. Montrer que $L/\mathbb{Q}$ est ramifiée au-dessus de 2 et que $2\mathcal{O}_L = \mathfrak{q}^2$ avec $\mathfrak{q}$ maximal. Calculer $N(\mathfrak{q})$ et trouver un générateur de $\mathfrak{q}$.
2. Montrer que $\mathcal{O}_L$ est principal.

Chapitre 5

Les unités des anneaux d'entiers

Dans l'étude d'un anneau d'entiers ou plus généralement d'un anneau de Dedekind A, nous nous sommes intéressés jusqu'à présent aux idéaux. Il y a un autre object important que ne voient pas les idéaux, ce sont les *unités*, c'est-à-dire les éléments inversibles de l'anneau. Les unités de A forment un groupe commutatif, appelé le *groupe des unités*, et que nous noterons $U(A)$.

Ce chapitre est consacré au théorème de Dirichlet qui décrit la structure de ces groupes dans le cas des anneaux d'entiers d'un corps de nombres.

5.1 Quelques exemples

Exemple 5.1.1 Le cas le plus simple : $U(\mathbb{Z}) = \{\pm 1\}$.

Proposition 5.1.2. *Soit L un corps de nombres. Soit $\alpha \in \mathcal{O}_L$. Alors $\alpha \in U(\mathcal{O}_L)$ si et seulement si $N_{L/\mathbb{Q}}(\alpha) = \pm 1$.*

Démonstration. Si α est inversible dans $\mathcal{O}_L$, alors $N_{L/\mathbb{Q}}(\alpha)$ est inversible dans $\mathbb{Z}$, donc égal à ± 1. Inversement, supposons que $N_{L/\mathbb{Q}}(\alpha) = \pm 1$. Soient $K = \mathbb{Q}[\alpha]$ et $d = [L : K]$. Alors

$$N_{L/\mathbb{Q}}(\alpha) = N_{K/\mathbb{Q}}(N_{L/K}(\alpha)) = N_{K/\mathbb{Q}}(\alpha^d) = N_{K/\mathbb{Q}}(\alpha)^d$$

et on en déduit que $N_{K/\mathbb{Q}}(\alpha) = \pm 1$. Le polynôme minimal de α

$$m_\alpha(X) = X^m + a_{m-1}X^{m-1} + \cdots + a_1 X + a_0 \in \mathbb{Q}[X]$$

est à coefficients dans $\mathbb{Z}$ (proposition 2.1.20) et $a_0 = (-1)^m N_{K/\mathbb{Q}}(\alpha)$ (proposition 2.2.4). Comme $\alpha(\alpha^{n-1} + \cdots + a_1) = \pm 1$, on voit que α est inversible dans $\mathbb{Z}[\alpha]$, donc inversible dans $\mathcal{O}_L$. □

Exemple 5.1.3 Notons $\mathbb{\mu}(L)$ l'ensemble des éléments de L qui sont des racines de l'unité. Alors $\mathbb{\mu}(L) \subseteq U(\mathcal{O}_L)$. En effet si $\zeta^k = 1$ pour un entier $k \geq 1$, alors ζ est entier sur $\mathbb{Z}$, donc appartient à $\mathcal{O}_L$. De plus $\zeta^{-1} \in L$ est aussi une racine de l'unité, donc appartient à $\mathcal{O}_L$, d'où $\mathbb{\mu}(L) \subseteq U(\mathcal{O}_L)$.

Exemple 5.1.4 (*Unités quadratiques imaginaires*) Soit $d > 0$ un entier sans facteur carré. Soit $L = \mathbb{Q}[\sqrt{-d}]$.

1. Supposons $d \equiv 1$ ou $2 \mod 4$. Alors $\mathcal{O}_L = \mathbb{Z}[\sqrt{-d}]$. Soient $a, b \in \mathbb{Z}$. Alors $N_{L/\mathbb{Q}}(a + b\sqrt{-d}) = a^2 + b^2 d$. On cherche $(a, b) \in \mathbb{Z}^2$ tels que $a^2 + b^2 d = 1$.
   (a) Si $d = 1$, les solutions sont $(\pm 1, 0)$ et $(0, \pm 1)$. Donc $U(\mathbb{Z}[\sqrt{-1}]) = \{\pm 1, \pm\sqrt{-1}\}$.
   (b) Si $d \geq 2$, alors $U(\mathcal{O}_L) = \{\pm 1\}$.
2. Supposons $d \equiv 3 \mod 4$. Alors $\mathcal{O}_L = \mathbb{Z}[\alpha]$ où $\alpha = (1 + \sqrt{-d})/2$. Si $a, b \in \mathbb{Z}$, on a

$$N_{L/\mathbb{Q}}(a + b\alpha) = a^2 + ab + b^2(d + 1)/4 = (a + b/2)^2 + b^2 d/4 \geq 0.$$

   Les seules solutions pour $N_{L/\mathbb{Q}}(a + b\alpha) = \pm 1$ sont, lorsque $d > 3$, $a = \pm 1$ et $b = 0$. Donc $U(\mathcal{O}_L) = \pm 1$. Pour $d = 3$, on trouve des solutions supplémentaires : $U(\mathcal{O}_L) = \{\pm 1, \pm(1 \pm \sqrt{-3})/2 = \pm e^{\pm 2i\pi/3}\}$.

En résumé, $U(\mathcal{O}_L) = \mathbb{\mu}(L)$ pour les extensions quadratiques imaginaires.

Remarque 5.1.5 (Pas fait en cours) Soit A un anneau euclidien avec un stathme

$$v : A \to \mathbb{N} \cup \{+\infty\}.$$

Alors il existe $\alpha \in A \setminus (\{0\} \cup A^*)$ tel que la surjection canonique $A \to A/\alpha A$ induise une application surjective $A^* \cup \{0\} \to A/\alpha A$. Il suffit pour cela de prendre $\alpha \in A \setminus (\{0\} \cup A^*)$ avec $v(\alpha)$ minimal : pour tout $a \in A$, on a $a = \alpha q + r$ avec $q, r \in A$ et $v(r) < v(\alpha)$. Donc $r = 0$ ou $r \in A^*$ et on a $a \equiv r \mod \alpha$.

Cette propriété permet de montrer que $\mathcal{O}_L = \mathbb{Z}[(-1 + \sqrt{-19})/2]$ n'est pas euclidien. En effet, $\mathcal{O}_L^* = \{\pm 1\}$. Si $\mathcal{O}_L$ est euclidien, il existe $\alpha \in \mathcal{O}_L$ non nul et non inversible tel que $\mathcal{O}_L/\alpha\mathcal{O}_L$ possède au plus 3 éléments. C'est donc un corps, isomorphe à $\mathbb{F}_2$ ou $\mathbb{F}_3$ et $\alpha\mathcal{O}_L$ est un idéal maximal de $\mathcal{O}_L$ au-dessus de 2 ou 3. En particulier $\alpha\mathcal{O}_L$ contient $2\mathcal{O}_L$ ou $3\mathcal{O}_L$. Or on a vu que $\mathcal{O}_L = \mathbb{Z}[X]/(X^2 + X + 5)$ (exemple 4.2.14) et $\mathcal{O}_L/2\mathcal{O}_L, \mathcal{O}_L/3\mathcal{O}_L$ sont des corps (car $X^2 + X + 5$ est irréductible dans $\mathbb{F}_2$ et $\mathbb{F}_3$), isomorphe à $\mathbb{F}_4$ et $\mathbb{F}_9$. Donc $\alpha\mathcal{O}_L = 2\mathcal{O}_L$ ou $3\mathcal{O}_L$ avec $|\mathcal{O}_L/\alpha\mathcal{O}_L| \geq 4$. Contradiction.

Exemple 5.1.6 Si la situation des extensions quadratiques imaginaires est très limpide, le cas réel est plus... complexe et plus intéressant. Considérons $L = \mathbb{Q}[\sqrt{2}]$. On a $\mathcal{O}_L = \mathbb{Z}[\sqrt{2}]$. Il faut donc chercher $a, b \in \mathbb{Z}$ tels que

$$a^2 - 2b^2 = \pm 1. \tag{5.1}$$

C'est une *équation de Pell-Fermat*. Elle est équivalente à $N_{L/\mathbb{Q}}(a + b\sqrt{2}) = \pm 1$.

On a $\alpha_0 = 1 + \sqrt{2}$ qui est de norme $N_{L/\mathbb{Q}}(\alpha_0) = -1$. C'est donc une unité de $\mathbb{Z}[\sqrt{2}]$ et on a

$$\{\pm\alpha_0^k \mid k \in \mathbb{Z}\} \subseteq U := U(\mathbb{Z}[\sqrt{2}]).$$

Montrons qu'on a ainsi toutes les unités de $\mathcal{O}_L$. Montrons que $U \cap]1, \alpha_0[= \emptyset$. Soit $\alpha = a + b\sqrt{2}$ une unité dans cet intervalle ouvert. Alors

$$\sqrt{2} - 1 = \alpha_0^{-1} < \alpha^{-1} < 1.$$

En additionnant avec $1 < \alpha < 1 + \sqrt{2}$, on trouve $\sqrt{2} < \alpha^{-1} + \alpha < 2 + \sqrt{2}$. Comme $N_{L/\mathbb{Q}}(\alpha) = \pm 1$, on trouve $\alpha + \alpha^{-1} = 2a$ ou $2b\sqrt{2}$. On trouve facilement une contradiction en retournant à ces deux inégalités.

Soit maintenant $\alpha \in U$ une unité > 1. Il existe un entier $k \geq 0$ tel que $\alpha_0^k \leq \alpha < \alpha_0^{k+1}$. Alors $\alpha\alpha_0^{-k} \in U \cap [1, \alpha_0[$. D'après ce qui précède, $\alpha/\alpha_0^{-k} = 1$ et $\alpha \in \alpha_0^{\mathbb{Z}}$. Pour une unité générale $\alpha \in U$, les $\pm\alpha^{\pm 1}$ sont des unités et l'une d'elles est ≥ 1. Il suit que

$$U(\mathbb{Z}[\sqrt{2}]) = \{\pm\alpha_0^{\mathbb{Z}}\} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}.$$

Ceci est en fait le cas général des corps quadratiques réels.

On a en même temps trouvé les solutions de l'équation (5.1). Pour tout $k \in \mathbb{Z}$, on écrit $(1 + \sqrt{2})^k = a_k + b_k\sqrt{2}$ avec $a_k, b_k \in \mathbb{Z}$. Alors les solutions sont $\{\pm(a_k, b_k) \mid k \in \mathbb{Z}\}$. Comme $N_{L/\mathbb{Q}}(1 + \sqrt{2}) = -1$, les solutions de l'équation avec second membre égal à -1 (resp. 1) sont les $\pm(a_k, b_k)$, avec k impairs (resp. pairs).

Exercice 5.1.7 Soit $m \in \mathbb{Z}$. On veut étudier les solutions de l'équation

$$a^2 - 2b^2 = m$$

avec $a, b \in \mathbb{Z}$.

1. Supposons qu'il existe une solution (a_0, b_0). Montrer que l'ensemble de toutes les solutions est constitué des $\pm(a_k, b_k) \in \mathbb{Z}^2$, k parcourant les entiers relatifs pairs, avec

$$(a_0 + b_0\sqrt{2})(1 + \sqrt{2})^k = a_k + b_k\sqrt{2}.$$

2. Montrer que $a^2 - 2b^2 = m$ a une solution si et seulement si $a^2 - 2b^2 = -m$ en a une (utiliser $1 + \sqrt{2}$).
3. Il peut arriver que l'équation n'ait pas de solution du tout. Montrer que c'est le cas pour $m = 3$. (Raisonner modulo 3).

Exercice 5.1.8 Soient A un anneau de Dedekind, B la clôture intégrale de A dans une extension finie séparable L de $K = \mathrm{Frac}(A)$. Soit $b \in B$. Montrer que $b \in B^*$ si et seulement si $N_{L/K}(b) \in A^*$.

5.2 Théorème des unités de Dirichlet

On note $\mathbb{\mu}_n(\mathbb{C}) = \{z \in \mathbb{C} \mid z^n = 1\}$ pour tout $n \geq 1$. Pour tout corps de nombres L, on note $\mathbb{\mu}_n(L) = \mathbb{\mu}_n(\mathbb{C}) \cap L$ et $\mathbb{\mu}(L) = \cup_{n\geq 1}\mathbb{\mu}_n(L)$ l'ensemble des racines de l'unité dans L.

Les éléments d'ordre fini dans un groupe commutatif forment un sous-groupe appelé le sous-groupe de torsion. Le but de cette section est de montrer le théorème suivant :

Theorem 5.2.1. (Dirichlet) *Soit L un corps de nombres de degré n, soient $r_1, 2r_2$ les nombres de plongements réels et imaginaires de L.*

(1) *Le sous-groupe de torsion de $U(\mathcal{O}_L)$, égal à $\mathbb{\mu}(L)$, est fini et et cyclique.*

(2) *Le groupe quotient $U(\mathcal{O}_L)/\mathbb{\mu}(L)$ est libre de rang $r_1 + r_2 - 1$ et on a donc un isomorphisme (non canonique)*

$$U(\mathcal{O}_L) \simeq \mathbb{\mu}(L) \times \mathbb{Z}^{r_1+r_2-1}.$$

Corollaire 5.2.2. *Le groupe $U(\mathcal{O}_L)$ est fini si et seulement si $L = \mathbb{Q}$ ou si c'est une extension quadratique imaginaire de $\mathbb{Q}$.*

Pour la preuve du théorème, nous allons procéder en plusieurs étapes. Rappelons (4.2.2) qu'un sous-groupe discret d'un espace vectoriel $H \simeq \mathbb{R}^m$ est un sous-groupe G tel que pour tout $x \in G$, il existe U_x ouvert de H avec $U_x \cap G = \{x\}$. Il suffit que cela soit vrai pour $0 \in G$ car $U_0 + x$ est un voisinage ouvert de x dont l'intersection avec G se réduit à $\{x\}$. Commençons avec un résultat sur la structure des sous-groupes discrets.

Lemme 5.2.3. *Soit H un $\mathbb{R}$-espace vectoriel de dimension finie m. Soit G un sous-groupe discret de H.*

(1) *Le sous-ensemble G est fermé dans H. Soit P une partie compacte de H, alors $P \cap G$ est fini.*

(2) *Le groupe G est un $\mathbb{Z}$-module libre engendré par $r \leq m = \dim H$ vecteurs libres dans $\mathbb{R}$.*

(3) *S'il existe une partie bornée M dans H telle que*

$$H = G + M := \{g + x \mid g \in G, x \in M\},$$

alors G est de rang m.

Démonstration. (1) Soit U_0 un voisinage ouvert de $0 \in G$ tel que $G \cap U_0 = \{0\}$. Alors $(U_0 + g) \cap G = \{g\}$ pour tout $g \in G$. Si $(g_n)_n$ est une suite convergente avec $g_n \in G$. Alors c'est une suite de Cauchy. Donc il existe $N \geq 1$ tel que $g_n - g_N \in U_0 \cap G = \{0\}$ pour tout $n \geq N$. Par suite $(g_n)_n$ est stationnaire et sa limite appartient à G. Donc G est fermé.

On a un recouvrement ouvert de P

$$P \subset (H \setminus G) \cup \cup_{g\in G}(U_0 + g)$$

dont, par hypothèse de compacité, on peut extraire un recouvrement fini

$$P \subset (H \setminus G) \cup \cup_{1 \leq i \leq q} (U_0 + g_i).$$

Il suit que $P \cap G = \{g_1, \ldots, g_q\}$ est fini.

(2) Soient $e_1, \ldots, e_r \in G$ des vecteurs libres dans H avec r maximal. Montrons que G est engendré (comme $\mathbb{Z}$-module) par r éléments (mais pas nécessairement par $e_1, \ldots, e_r$). Posons

$$P = \{ \sum_{1 \leq i \leq r} x_i e_i \mid 0 \leq x_i \leq 1\}.$$

C'est l'image de $[0,1]^r$ par l'application continue

$$\mathbb{R}^r \to H, \quad (x_i)_i \mapsto \sum_i x_i e_i,$$

c'est donc un espace compact. Donc $P \cap G$ est fini. Soit $\alpha \in G$. On peut écrire

$$\alpha = \sum_{1 \leq i \leq r} x_i e_i, \quad x_i \in \mathbb{R}.$$

On a

$$\alpha = (\sum_{1 \leq i \leq r} [x_i] e_i) + \sum_{1 \leq i \leq r} (x_i - [x_i]) e_i \in \sum_i \mathbb{Z} e_i + P \cap G.$$

Donc G est engendré par $\{e_1, \ldots, e_r\} \cup (P \cap G)$. C'est donc un $\mathbb{Z}$-module de type fini, sans torsion, donc libre. Comme $G/(\sum_{1 \leq i \leq r} \mathbb{Z} e_i)$ est fini, on voit que G est de rang r par le théorème des bases adaptées 1.2.2.

(3) On peut supposer M fermé, donc compact. Soit H_0 le sous-espace vectoriel de H engendré par G. La surjection canonique $H \to H/H_0$ induit une application continue surjective $M \to H/H_0$ par l'hypothèse $H \subseteq G + M$. Donc l'espace vectoriel réel H/H_0 est compact, ce qui l'oblige à être nul. □

Pour étudier les unités de $\mathcal{O}_L$, on va d'abord plonger L^* dans un hyperplan de $\mathbb{R}^{r_1+r_2}$. On reprend les notations

$$\mathrm{Isom}_{\mathbb{Q}}(L, \bar{\mathbb{Q}}) = \{\sigma_1, \ldots, \sigma_{r_1}, \sigma_{r_1+1}, \bar{\sigma}_{r_1+1}, \ldots, \sigma_{r_1+r_2}, \bar{\sigma}_{r_1+r_2}\}$$

pour les plongements réels et imaginaires de L. Considérons $\ell : L^* \to \mathbb{R}^{r_1+r_2}$ définie par

$$x \mapsto (\ln|\sigma_1(x)|, \ldots, \ln|\sigma_{r_1}(x)|, \ln|\sigma_{r_1+1}(x)|, \ldots, \ln|\sigma_{r_1+r_2}(x)|).$$

C'est la version logarithmique de l'application ρ définie en 4.2.2. Elle est bien définie car $\sigma_j(x) \neq 0$ pour $x \in L^*$ et c'est clairement un homomorphisme de groupes.

Notons $U = U(\mathcal{O}_L)$. Le lemme suivant précise la structure de $\ell(U)$ et du quotient de U/U_{tors}.

Lemme 5.2.4. *Conservons les notations ci-dessus.*

(1) *Pour toute partie bornée $B \subset \mathbb{R}^{r_1+r_2}$, $\ell^{-1}(B) \cap U$ est fini. En particulier $\ell(U)$ est un sous groupe discret, libre de rang fini.*

(2) *Le noyau de ℓ est égal à $\mathbb{\mu}(L)$ et c'est un groupe fini cyclique.*

Démonstration. (1) Soit B une partie bornée de $\mathbb{R}^{r_1+r_2}$. Il existe $c > 0$ tel que

$$|\sigma_i(\alpha)| \leq c, \quad \forall i, \ \forall \alpha \in \ell^{-1}(B).$$

Il existe donc $c' > 0$ qui majore les valeurs absolues de toutes les fonctions symétriques en une partie des $\sigma(\alpha)$, $\sigma \in \mathrm{Isom}_{\mathbb{Q}}(L, \bar{\mathbb{Q}})$. Il suit que le polynôme minimal $m_\alpha(X)$ de α est à coefficients bornés par c'. Si de plus $\alpha \in U \subset \mathcal{O}_L$, on a $m_\alpha(X) \in \mathbb{Z}[X]$. Or il n'existe qu'un nombre fini de polynômes dans $\mathbb{Z}[X]$ de degré $\leq n$ et à coefficients bornés par c'. Donc $\mathcal{O}_L \cap \ell^{-1}(B)$, et *a fortiori* $U \cap \ell^{-1}(B)$, est fini. Par suite $\ell(U)$ a une intersection finie avec toute partie bornée de $\mathbb{R}^{r_1+r_2}$. Cela implique immédiatement que $\ell(U)$ est discret. Par le lemme 5.2.3, $\ell(U)$ est libre de rang fini sur $\mathbb{Z}$.

(2) En prenant $B = \{0\}$ dans (1), on obtient que $\ker \ell \cap U$ est un sous-groupe fini de L^*, ses éléments sont donc d'ordre fini pour la multiplication dans L^* et ces sont donc des racines de l'unité [1]. Inversement, si $\zeta \in \mathbb{\mu}(L)$, avec $\zeta^d = 1$. Alors $d \ln |\sigma_i(\zeta)| = 0$, donc $\ln |\sigma_i(\zeta)| = 0$ et $\zeta \in \ker \ell$. Par ailleurs, $\zeta \in \mathcal{O}_L^*$ puisque son inverse, ζ^{d-1}, appartient à $\mathcal{O}_L$. Enfin, $\mathbb{\mu}(L)$ étant fini, d'ordre disons N, est contenu dans $\mathbb{\mu}_N(\mathbb{C})$, l'ensemble des racines N-ièmes de l'unité dans $\mathbb{C}$. Ce dernier étant cyclique, $\mathbb{\mu}(L)$ aussi. □

Démonstration. (du théorème 5.2.1) Notons encore $U = U(\mathcal{O}_L)$. Il est claire que $\mathbb{\mu}(L) \subseteq U_{\mathrm{tors}}$. Réciproquement, tout élément d'ordre fini dans U est une racine de l'unité et appartient donc à $\mathbb{\mu}(L)$. Par le lemme précédent, il ne reste qu'à montrer que le sous-groupe discret $\ell(U)$ de $\mathbb{R}^{r_1+r_2}$ est de rang $r_1 + r_2 - 1$. Pour tout $\alpha \in U$, on a

$$\sum_{1 \leq i \leq r_1} \ln |\sigma_i(\alpha)| + 2 \sum_{1 \leq j \leq r_2} \ln |\sigma_j(\alpha)| = \ln |N_{L/\mathbb{Q}}(\alpha)| = 0.$$

Donc $\ell(U)$ est contenu dans l'hyperplan

$$H := \{(t_1, \ldots, t_{r_1+r_2}) \in \mathbb{R}^{r_1+r_2} \mid t_1 + \cdots + t_{r_1} + 2t_{r_1+1} + \cdots + 2t_{r_1+r_2} = 0\}$$

de $\mathbb{R}^{r_1+r_2}$. Il suit que $\ell(U)$ est de rang $\leq r_1 + r_2 - 1$. L'inégalité inverse est plus délicate. Nous allons construire une partie bornée M de H telle que $H = \cup_{u \in U}(M + \ell(U))$ et appliquer le lemme 5.2.3(3).

Notation : Si X, Y sont deux sous-ensembles de l'anneau produit $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$, on note XY l'ensemble des produits xy avec $x \in X$ et $y \in Y$.

1. On vient de montrer le théorème de Kronecker : si un nombre algébrique $z \in \mathbb{C}$ est tel que tous ses conjugués sont de module 1, alors z est une racine de l'unité !

L'application ℓ est la restriction à U de la composition de

$$\rho : L^* \to (\mathbb{R}^*)^{r_1} \times (\mathbb{C}^*)^{r_2}$$

(4.2.2) et de l'application surjective

$$\theta : (\mathbb{R}^*)^{r_1} \times (\mathbb{C}^*)^{r_2} \twoheadrightarrow \mathbb{R}^{r_1+r_2}$$

$$\theta(x,z) = (\ln|x_1|, \ldots, \ln|x_{r_1}|, \ln|z_{r_1+1}|, \ldots, \ln|z_{r_1+r_2}|)$$

qui est un homomorphisme de groupes surjectif et continu. Notons que $\rho(U) \subseteq \theta^{-1}(H)$. Il suffit donc de trouver une partie T de $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ telle que $\theta(\theta^{-1}(H) \cap T)$ soit bornée et que $\theta^{-1}(H) \subseteq \rho(U)T$ (on prendra alors $M = \theta(\theta^{-1}(H) \cap T)$).

Soit $\delta > 0$ un nombre réel, qu'on choisira assez grand (on précisera plus tard). Posons

$$X_\delta = \{(x,z) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \mid |x_i| \leq \delta,\ |z_{r_1+j}| \leq \delta\}$$

et

$$Z_\delta = \{\rho(\alpha^{-1}) \mid \alpha \in \mathcal{O}_L, \alpha \neq 0,\ |\mathrm{N}_{L/\mathbb{Q}}(\alpha)| \leq \delta^n\}.X_\delta.$$

On veut montrer que $\theta^{-1}(H) \subseteq Z_\delta$ pour δ suffisamment grand. Montrons que

$$\delta^n \geq 2^{n-r_1}\pi^{-r_2}\mathrm{vol}(\rho(\mathcal{O}_L))$$

suffit. Soit $y \in \theta^{-1}(H)$. Posons

$$Y_y := y^{-1}.X_\delta = \{(x,z) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \mid |x_i| \leq |y_i^{-1}|\delta,\ |z_{r_1+j}| \leq |y_{r_1+j}|^{-1}\delta\}.$$

C'est une partie convexe compacte symétrique de $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ de volume

$$\mathrm{vol}(Y_y) = \prod_{1\leq i\leq r_1}(2\delta|y_i|^{-1}) \prod_{1\leq j\leq r_2}(\pi(\delta|y_{r_1+j}|^{-1})^2) = 2^{r_1}\pi^{r_2}\delta^n \geq 2^n\mathrm{vol}(\rho(\mathcal{O}_L))$$

(on utilise l'hypothèse $\theta(y) \in H$ dans l'égalité du milieu). Par le lemme 4.2.5, $\rho(\mathcal{O}_L) \cap Y_y \neq \{0\}$. Soit $\alpha \in \mathcal{O}_L$ tel que $\rho(\alpha) \in \rho(\mathcal{O}_L) \cap Y_y \setminus \{0\}$. Alors $\alpha \neq 0$ et on $|\sigma_i(\alpha)| \leq |y_i|^{-1}\delta$ si $i \leq r_1$, et $|\sigma_{r_1+j}(\alpha)| \leq |y_{r_1+j}|^{-1}\delta$ si $j \leq r_2$. En tenant compte de l'hypothèse $y \in \theta^{-1}(H)$, on conclut que $|N_{L/\mathbb{Q}}(\alpha)| \leq \delta^n$. Cela implique donc que $y \in \rho(\alpha^{-1}).X_\delta$. D'où $\theta^{-1}(H) \subseteq Z_\delta$.

Étudions maintenant Z_δ. L'ensemble des idéaux principaux non nuls de $\mathcal{O}_L$ de norme $\leq \delta^n$ est fini (lemme 4.1.6). Soit $\{\alpha_1\mathcal{O}_L, \ldots, \alpha_m\mathcal{O}_L\}$ cet ensemble. Alors pour tout $\alpha \in \mathcal{O}_L$ non nul de norme $|N_{L/\mathbb{Q}}(\alpha)| \leq \delta^n$, α est le multiple d'un α_q by une unité de $\mathcal{O}_L$. Cela implique que

$$Z_\delta = \rho(U).(\cup_{1\leq q\leq m}\rho(\alpha_q^{-1}).X_\delta).$$

Notons

$$T = \cup_{1\leq q\leq m}\rho(\alpha_q^{-1}).X_\delta.$$

C'est une partie bornée de $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. Il reste à montrer que $\theta(\theta^{-1}(H) \cap T)$ est bornée. On a T contenu dans un X_R avec $R > 1$. Si $(x,z) \in \theta^{-1}(H) \cap T$, alors $R \geq |x_i| \geq R^{-n+1}$ et $R \geq |z_{r_1+j}| \geq R^{-n+1}$. Donc $\theta(\theta^{-1}(H) \cap T)$ est bornée. Ce qui achève la démonstration. □

Définition 5.2.5 Une famille de $r_1 + r_2 - 1$ éléments dans $U(\mathcal{O}_L)$ qui forment une base dans le quotient libre de $U(\mathcal{O}_L)$ est appelée un *système d'unités fondamentales*. Un tel système induit un isomorphism $U(\mathcal{O}_L) \simeq \mathbb{\mu}(L) \times \mathbb{Z}^{r_1+r_2-1}$. Une *unité fondamentale* est un élément de $U(\mathcal{O}_L)$ qui peut se compléter en un système d'unités fondamentales.

Exemple 5.2.6 Revenons aux corps quadratiques réels $L = \mathbb{Q}[\sqrt{d}]$. Si $\alpha = u+v\sqrt{d}$ $(u, v \in \mathbb{Q})$ est une unité fondamentale, alors $-\alpha, \pm\alpha^{-1}$ aussi. L'ensemble de ces quatre unités est égal à

$$\{u + v\sqrt{d}, -u - v\sqrt{d}, u - v\sqrt{d}, -u + v\sqrt{d}\}$$

(on a $(u + v\sqrt{d})^{-1} = (u - v\sqrt{d})N_{L/\mathbb{Q}}(\alpha)^{-1}$). Soit $\alpha_0 = a + b\sqrt{d}$ le maximum de cet ensemble d'unités. Alors nécessairement $a, b > 0$ et $\alpha_0 > 1$. Conclusion : il existe une unité fondamentale $\alpha_0 = a + b\sqrt{d} > 1$. Il est clair qu'elle est alors la plus petite des unités > 1. Celles-ci sont de la forme $(a + b\sqrt{d})^n = a_n + b_n\sqrt{d}$ avec $n \geq 1$ et $a_n, b_n \in \mathbb{Q}$.

Supposons $d \equiv 2, 3 \mod 4$. Alors $a, b, a_n, b_n \in \mathbb{N}$ et il est facile de voir que a_n, b_n sont des suites croissantes. En particulier, $b_n \geq b$. Donc b est le plus petit entier naturel tel que $db^2 = \square + 1$ ou $\square - 1$. Ainsi, une unité fondamentale de $\mathbb{Q}[\sqrt{7}]$ est donnée par $8 + 3\sqrt{7}$.

Quelques autres exemples : $4 + \sqrt{15}$, $170 + 39\sqrt{19}$ sont les unités fondamentales respectives des corps $\mathbb{Q}[\sqrt{15}], \mathbb{Q}[\sqrt{19}]$. Pour $L = \mathbb{Q}[\sqrt{13}]$, on trouve par une méthode similaire $(3 + \sqrt{13})/2$. Avec le logiciel pari, utiliser la command `quadunit(d)` où d est le discriminant de l'extension quadratique réelle concernée.

Nous terminons par l'étude des unités des extensions cyclotomiques. Soit $m \geq 3$. Une *extension cyclotomique* est une extension de $\mathbb{Q}$ engendré par une racine de l'unité ζ_m d'ordre $m \geq 3$. Pour simplifier, nous nous restreignons au cas $m = p > 2$ premier. Notons ζ une racine primitive p-ième de l'unité, $L = \mathbb{Q}[\zeta]$ et $L^+ = \mathbb{Q}[(\zeta + \zeta^{-1})/2]$. La proposition suivante rassemble les résultats qui seront utilisés dans la section suivante.

Proposition 5.2.7. *Avec les notations ci-dessus, les propriétés suivantes sont vraies.*

(1) *On a* $\mathcal{O}_L = \mathbb{Z}[\zeta]$.

(2) $\mathbb{\mu}(L) = \pm\langle\zeta\rangle = \{\pm\zeta^k \mid k \in \mathbb{Z}\} = \langle -\zeta\rangle$.

(3) $L^+ = L^{\langle c\rangle}$ *où* c *est la conjugaison complexe.*

(4) $U(\mathcal{O}_L) = \langle\zeta\rangle U(\mathcal{O}_{L^+})$.

(5) *Pour tout* $\alpha \in \mathcal{O}_L$, *on a* $\alpha^p \in \mathbb{Z} + p\mathcal{O}_L$.

Démonstration. (1) TD.

(2) Si $\lambda \in \mathbb{\mu}(L)$ est d'ordre N, alors $\lambda\zeta$ est d'ordre $m := \mathrm{ppcm}(N, p)$ et on a $\mathbb{Q}[\lambda\zeta] \subseteq \mathbb{Q}[\zeta]$. Ce qui implique que $\varphi(m) \mid \varphi(p)$. En écrivant $m = p^r m'$ avec p

premier à m', on trouve facilement que $r = 1$ et $m' = 1$ ou 2, donc λ ou $-\lambda$ est une puissance de ζ.

(3) Comme ζ est racine du polynôme

$$X^2 - (\zeta + \zeta^{-1})X + 1 \in L^+[X],$$

on voit que $[L : L^+] \leq 2$. On a l'égalité car ζ est imaginaire et $L^+ \subseteq \mathbb{R}$. La conjugaison complexe c préserve L et est égale à l'identité sur L^+, c'est donc le générateur du groupe de Galois de L/L^+.

(4) Fait en TD.

(5) Soit $\alpha \in \mathcal{O}_L$. Alors $\alpha = \sum_{0 \leq i \leq p-2} a_i \zeta^i$ avec $a_i \in \mathbb{Z}$. Dans tout anneau commutatif A, on a $(x + y)^p \in x^p + y^p + pA$. Donc

$$\alpha^p \in a_0^p + a_1^p + \cdots + a_{p-2}^p + p\mathcal{O}_L \subseteq \mathbb{Z} + p\mathcal{O}_L.$$

□

Lemme 5.2.8. *Pour tous $i, j \in \mathbb{Z}$ premiers à p, on a $(\zeta^i - 1)/(\zeta^j - 1) \in U(\mathcal{O}_L)$.*

Démonstration. Comme ζ^j est un générateur du groupe des racines p-ièmes de l'unité, on a $\zeta^i = (\zeta^j)^m$ pour un $m \geq 1$. Alors

$$\frac{\zeta^i - 1}{\zeta^j - 1} = (\zeta^j)^{m-1} + \cdots + (\zeta^j) + 1 \in \mathcal{O}_L.$$

Par symétrie, $(\zeta^j - 1)/(\zeta^i - 1) \in \mathcal{O}_L$. Donc $(\zeta^i - 1)/(\zeta^j - 1) \in U(\mathcal{O}_L)$. □

Remarque 5.2.9 Le sous-groupe U' de $U(\mathcal{O}_L)$ engendré par les unités ci-dessus s'appelle le groupe des unités cyclotomiques. Le théorème des unités de Dirichlet dit que $U(\mathcal{O}_L)/\mathbb{\mu}(L)$ est libre de rang $(p-3)/2$. Pour $q = 2, \ldots, p-1$, notons $u_q = (\zeta^q - 1)/(\zeta - 1)$. On a $u_{p-q} = -\zeta^{-q} u_q$. Donc U' est engendré par les u_q pour $2 \leq q \leq (p-1)/2$. On peut montrer que U' est d'indice fini dans $U(\mathcal{O}_L)$.

5.3 Premier cas du théorème de Fermat

Soit $n \geq 3$. Le théorème de Fermat stipule que l'équation

$$x^n + y^n = z^n$$

n'a pas de solution avec des entiers naturels x, y, z strictement positifs (de façon équivalente, pas de solution dans $\mathbb{Z}$ avec $xyz \neq 0$). Noter que pour $n = 1, 2$, il existe une infinité de solutions. Fermat a prouvé ce théorème pour $n = 4$. Il suffit alors de montrer le théorème pour $n = p > 2$ nombre premier. Ce qui a été fait par Andrew Wiles en 1994. Dix ans avant, Gerd Faltings avait prouvé une conjecture de Mordell, impliquant en particulier que l'équation de Fermat n'avait qu'un nombre fini de solutions (avec x, y, z premiers entre eux).

Dans cette section, nous montrons une solution partielle lorsque p est un nombre premier "régulier" (5.3.2). On fixe un nombre premier $p > 2$ dans la suite. Soit $L = \mathbb{Q}[\zeta]$ où ζ est une racine primitive p-ième de l'unité.

Theorem 5.3.1. *Soit $p > 2$ un nombre premier. Supposons que p ne divise pas le nombre de classes h_p de $\mathbb{Q}[\zeta]$. Alors il n'existe pas de solution de*

$$x^p + y^p + z^p = 0$$

*avec x, y, z des entiers relatifs premiers à p (*premier cas du théorème de Fermat*).*

Démonstration. Supposons le contraire et prenons une solution (x, y, z) avec $p \not| xyz$.

(0) Premières réductions. On peut bien sûr supposer $\text{pgcd}\{x, y, z\} = 1$. Cela entraîne que x, y, z sont deux à deux premiers entre eux. Si $p = 3$, comme dans $\mathbb{Z}/9\mathbb{Z}$ les cubes non nuls sont 1 et -1, mais que la somme de deux de ces nombres n'est jamais égale à ± 1, on voit que $x^3 + y^3 + z^3 \equiv 0$ n'a pas de solution non nulle dans $\mathbb{Z}/9\mathbb{Z}$. Il suit que $p \neq 3$ et donc $p \geq 5$.

Si $x \equiv y \equiv z \mod p$, alors $3z^p \equiv 0$ et donc $p \mid 3z$. Contraire à l'hypothèse. Donc quitte à permuter x, y, z si nécessaire on peut supposer que $x \not\equiv y \mod p$.

Soit $\zeta \in \mathbb{C}$ une racine primitive p-ième de l'unité. Soit $L = \mathbb{Q}[\zeta]$. On a

$$-z^p = \prod_{0 \leq i \leq p-1} (x + \zeta^i y). \tag{5.2}$$

(1) Montrons que $x + \zeta^i y$ *et* $x + \zeta^j y$ *sont premiers entre eux* (dans le sens où ils engendrent l'idéal unité de $\mathcal{O}_L$) si $i \neq j$. En effet, supposons qu'ils appartiennent tous les deux à un même idéal maximal $\mathfrak{q}$ de $\mathcal{O}_L$. Alors

$$y\zeta^i(\zeta^{j-i} - 1) \in \mathfrak{q}.$$

Si $y \in \mathfrak{q}$, alors $x \in \mathfrak{q}$ et donc $x, y \in \mathfrak{q} \cap \mathbb{Z} = \ell\mathbb{Z}$ pour un nombre premier ℓ. Absurde. Donc $y \notin \mathfrak{q}$. Comme ζ est une unité, on a $\zeta^{j-i} - 1 \in \mathfrak{q}$ et donc

$$p = \text{N}_{L/\mathbb{Q}}(\zeta^{j-i} - 1) \in \mathfrak{q} \cap \mathbb{Z}.$$

On a $\zeta^i - 1 = ((\zeta^i - 1)/(\zeta^{j-i} - 1))(\zeta^{j-i} - 1) \in \mathfrak{q}$ (lemme 5.2.8) et

$$x + y = (x + \zeta^i y) - (\zeta^i - 1)y \in \mathfrak{q} \cap \mathbb{Z} = p\mathbb{Z},$$

ce qui implique que

$$-z^p = x^p + y^p \equiv x + y \equiv 0 \mod p.$$

Ce qui est contraire à l'hypothèse p premier à xyz.

(2) Montrons que

$$x + \zeta y \equiv a\zeta^r v \mod p\mathcal{O}_L \tag{5.3}$$

avec $a \in \mathbb{Z}$, $0 \leq r \leq p-1$ et $v \in U(\mathcal{O}_{L^+})$. En effet, la décomposition (5.2) en termes de produit d'idéaux maximaux implique que

$$(x + \zeta y)\mathcal{O}_L = J^p$$

pour un certain idéal J de $\mathcal{O}_L$. Dans le groupe des classes de L, J^p est donc trivial. Or par hypothèse, h_p est premier à p. Donc J est déjà trivial dans le groupe des classes : $J = \alpha\mathcal{O}_L$ pour un certain $\alpha \in \mathcal{O}_L$ non nul et

$$x + \zeta y = u\alpha^p, \quad u \in U(\mathcal{O}_L).$$

On conclut avec 5.2.7 (4) et 5.2.7 (1).

(3) Fin de la preuve. On applique la conjugaison complexe à l'égalité (5.3) :

$$x + \zeta^{-1} y \equiv a\zeta^{-r} v \mod p$$

(ici $\mod p$ veut dire modulo l'idéal $p\mathcal{O}_L \subset \mathcal{O}_L$). Cela implique que

$$x\zeta^{p-r} + y\zeta^{p+1-r} - x\zeta^r - y\zeta^{r-1} \equiv 0 \mod p$$

et donc

$$y\zeta^{p-r} + x\zeta^{p-r-1} - x\zeta^{r-1} - y\zeta^{r-2} \equiv 0 \mod p.$$

On va conclure par un examen cas par cas suivant la valeur de $0 \leq r \leq p-1$.

- Supposons $2 \leq r \leq p-1$ et $r \neq (p+1)/2$. Les exposants de ζ qui apparaissent sont compris entre 0 et $p-2$ et sont deux à deux distincts. Comme $\{1, \zeta, \ldots, \zeta^{p-2}\}$ est une base de $\mathbb{Z}[\zeta]$ sur $\mathbb{Z}$, cela implique que $p \mid x, y$. Absurde.
- Supposons $r = (p+1)/2$. Alors

  $$(y - x)\zeta^{(p-1)/2} + (x - y)\zeta^{(p-3)/2} \equiv 0 \mod p.$$

  Le même raisonnement que ci-dessus montre que $x - y \equiv 0 \mod p$. Contraire à l'hypothèse faite dans L'étape (0).
- Si $r = 0$, alors $y\zeta^2 - y \equiv 0 \mod p$, donc $p \mid y$. Contraire à l'hypothèse.
- Si $r = 1$, alors $x - x\zeta^2 \equiv 0 \mod p$ et $p \mid x$. Impossible. □

Définition 5.3.2 On dit qu'un nombre premier $p > 2$ est *régulier* si p ne divise pas h_p.

Remarque 5.3.3 On montre que pour p régulier, l'équation de Fermat n'a pas non plus de solution dans le second cas (où p divise x, y ou z), cf. L. Washington, Introduction to cyclotomic fields, Theorem 9.3.

On sait que $h_p = 1$ si et seulement si $p \leq 19$. Le nombre premier 23 est régulier car on montre que $h_{23} = 3$. On ne sait pas s'il existe une infinité de nombres premiers réguliers. Par contre, on sait qu'il existe une infinité de nombres premiers irréguliers. Le plus petit d'entre eux est 37. En fait $h_{29} = 8, h_{31} = 9$ et $h_{37} = 37$.

Chapitre 6

Aspect analytique, fonctions L

6.1 Fonction zêta de Riemann

La fonction zêta de Riemann est la fonction à variable complexe

$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s}, \quad \Re(s) > 1.$$

6.1.1 Prolongement méromorphe en $\Re(s) > 0$

Lemme 6.1.1. *On a les propriétés suivantes :*

(1) *Soit $(f_n)_n$ une suite de fonctions holomorphes sur un ouvert U de $\mathbb{C}$. Si la série $\sum_n f_n$ converge uniformément sur tout compact de U, alors $\sum_n f_n$ est holomorphe sur U.*

(2) *La série $\zeta(s)$ converge absolument pour $\Re(s) > 1$ et est ainsi une fonction holomorphe en s sur cette région de $\mathbb{C}$.*

(3) (Euler, 1749)
$$\zeta(s) = \prod_p (1 - p^{-s})^{-1}, \quad \Re(s) > 1$$
où le produit porte sur tous les nombres premiers p.

Démonstration. (1) Bien connu.

(2) Soit $c > 1$ et $x = \Re(s) \geq c$. Alors $|n^{-s}| = n^{-x} \leq n^{-c}$. Donc la série $\zeta(s)$ converge uniformément sur $\Re(s) \geq c$. Comme tout compact de $\Re(s) > 1$ est contenu dans un fermé de type $\Re(s) \geq c$ pour un certain $c > 1$, (1) implique que $\zeta(s)$ est holomorphe.

(3) Pour tout $m \geq 1$, on a

$$\prod_{p \leq m} (1 - p^{-s})^{-1} = \prod_{p \leq m} (1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \dots) = \sum_{(\text{fact. premiers de } n) \leq m} \frac{1}{n^s}.$$

Comme $\sum_n n^{-s}$ converge absolument, le membre de gauche converge vers la somme portant sur tous les n, c'est-à-dire $\zeta(s)$. □

Lemme 6.1.2. *Soit $\sum_n u_n$ une série complexe absolument convergente telle que $1+u_n \neq 0$ pour tout n, alors le produit infini $\prod_n(1+u_n)$ converge vers une limite non nulle.*

Démonstration. Que le produit infini converge est classique. On peut par exemple appliquer le logarithme au produits partiels finis. Pour montrer que la limite est non nulle, il suffit de montrer que le produit infini $\prod_n(1+u_n)^{-1}$ converge. Quitte à enlever un nombre fini de termes, on peut supposer que $|u_n| \leq 1/2$. On a

$$\frac{1}{1+u_n} = 1 - \frac{u_n}{1+u_n}$$

et

$$|\frac{u_n}{1+u_n}| \leq \frac{|u_n|}{1-|u_n|} \leq 2|u_n|.$$

Donc la série $\sum_n(u_n/(1+u_n))$ converge absolument, il suit que le produit infini $\prod_n((1+u_n)^{-1})$ converge. □

Proposition 6.1.3. *La fonction analytique $\zeta(s)$ ne s'annule pas en $\Re(s) > 1$ et se prolonge en une fonction méromorphe sur $\{s \in \mathbb{C} \mid \Re(s) > 0\}$, avec un unique pôle en 1, de résidu 1. Plus précisément,*

$$\Re(s) > 0 : \quad \zeta(s) = \frac{1}{s-1} + \textit{une fonction holomorphe.}$$

Démonstration. (1) Numérotons les nombres premiers en ordre croissant $p_1 < p_2 < \cdots < p_n < \cdots$. Alors $p_n > n$ et la série $\sum_n p_n^{-s}$ converge absolument si $\Re(s) > 1$. D'après le lemme ci-dessus, le produit infini $\prod_n(1-p_n^{-s})^{-1}$ converge vers une limite non nulle. Or cette limite est égale à $\zeta(s)$. Donc $\zeta(s)$ n'a pas de zéro en $\Re(s) > 1$.

Montrons maintenant le prolongement sur $\Re(s) > 0$. Pour $\Re(s) > 1$, on a

$$\frac{1}{s-1} = \int_1^{+\infty} t^{-s}dt.$$

Donc

$$\zeta(s) - \frac{1}{s-1} = \sum_{n\geq 1} \int_n^{n+1} (n^{-s} - t^{-s})dt = \sum_{n\geq 1} g_n(s).$$

Il suffit de montrer que le membre de droite se prolonge en une fonction holomorphe sur $\Re(s) > 0$.

Comme $g_n(s)$ est une fonction holomorphe sur $\mathbb{C}$, il suffit de montrer que la série de fonctions $\sum_n g_n(s)$ converge uniformément sur tout compact $K \subset \{s \in \mathbb{C} \mid \Re(s) > 0\}$ (lemme 6.1.1 (1)). Il existe $c, C > 0$ tels que $\Re(s) \geq c$ et $|s| \leq C$ sur K. On a $|g_n(s)| \leq \sup_{t\in[n,n+1]} |n^{-s} - t^{-s}|$. Par l'inégalité des

accroissements finis (valable pour les fonctions à valeurs complexes), et comme $d(t^{-s})/dt = -st^{-s-1}$, on a

$$|n^{-s} - t^{-s}| \leq \frac{C}{n^{c+1}}$$

car pour $t \in [n, n+1]$ et s comme ci-dessus, on a $|st^{-s-1}| \leq Cn^{-c-1}$. Ce qui prouve la convergence absolue, donc uniforme, sur K. □

6.1.2 Fonction Gamma

On définit la fonction Gamma pour $\Re(s) > 0$

$$\Gamma(s) = \int_0^{+\infty} t^{s-1} e^{-t} dt.$$

C'est une fonction holomorphe sur $\Re(s) > 0$. Une intégration par parties donne la relation (équation fonctionnelle) pour $\Re(s) > 0$:

$$s\Gamma(s) = \Gamma(s+1). \tag{6.1}$$

Comme $\Gamma(1) = \int_0^{+\infty} \exp(-t)dt = 1$, cette relation implique que

$$\Gamma(n) = (n-1)!, \quad n \geq 1.$$

La relation (6.1) permet aussi de prolonger Γ en une fonction méromorphe sur $\mathbb{C}$: si $0 \geq \Re(s) > -1$, on pose $\Gamma(s) = \Gamma(s+1)/s$. De même pour $\Re(s) > -2$, on prolonge $\Gamma(s)$ par $\Gamma(s+1)/s$ en utilisant le prolongement précédent et ainsi de suite. La fonction méromorphe sur $\mathbb{C}$ ainsi obtenue satisfait encore l'équation fonctionnelle ci-dessus.

En résumé, $\Gamma(s)$ est une fonction méromorphe sur $\mathbb{C}$ dont les pôles (tous simples) sont $0, -1, -2, \ldots$ avec résidu $(-1)^n/n!$ en $s = -n$.

Proposition 6.1.4. *On a*

$$\Gamma(s)\Gamma(1-s) = \frac{\pi}{\sin(\pi s)} \tag{6.2}$$

En particulier, $\Gamma(s)$ *n'a pas de zéro dans* $\mathbb{C}$ *et* $\Gamma(1/2) = \sqrt{\pi}$. *De plus*

$$\Gamma(s) = 2^{s-1}\Gamma\left(\frac{s}{2}\right)\Gamma\left(\frac{s+1}{2}\right)\pi^{-1/2}. \tag{6.3}$$

Démonstration. (Esquisse) On considère la fonction méromorphe

$$f(s) = \Gamma(s)\Gamma(1-s)\sin(\pi s).$$

Elle est holomorphe sur $\mathbb{C}$ car les pôles possibles sont simples et se situent aux entiers et ceux-ci sont des zéros de $\sin(\pi s)$. On montre qu'elle est bornée donc constante égale à $f(0)$. Quand s tends vers 0, on a $\Gamma(s) \sim 1/s$ et $\Gamma(1-s) \sim$

$\Gamma(1) = 1$. Donc $f(0) = \pi$. Cela montre la première formule. Comme conséquence, si Γ s'annule en un $s_0 \in \mathbb{C}$, alors $1 - s_0$ est un pôle de Γ, donc $s_0 \in \mathbb{N}_{>0}$. Mais alors $\Gamma(s_0) = (s_0 - 1)! \neq 0$, contradiction. Enfin, en prenant $s = 1/2$ dans l'égalité (6.2), on trouve $\Gamma(1/2)^2 = \pi$. Mais $\Gamma(1/2) \in \mathbb{R}_{>0}$ par sa définition intégrale, donc $\Gamma(1/2) = \sqrt{\pi}$.

Pour la deuxième formule, on considère

$$g(s) = 2^s \Gamma\left(\frac{s}{2}\right) \Gamma\left(\frac{s+1}{2}\right) \Gamma(s)^{-1}$$

qui est holomorphe sur $\mathbb{C}$ et on montre qu'elle est bornée, donc constante égale à $g(0) = 2\Gamma(1/2) = 2\sqrt{\pi}$. □

6.1.3 Travaux de Riemann

Theorem 6.1.5 (Riemann, 1859)**.** *La fonction $\zeta(s)$ satisfait les propriétés suivantes.*

(1) (Prolongement méromorphe) *La fonction $\zeta(s)$ se prolonge en une fonction méromorphe sur $\mathbb{C}$, avec un unique pôle en $s = 1$.*

(2) (Équation fonctionnelle) *On a l'égalité des fonctions méromorphes sur $\mathbb{C}$:*

$$\pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \pi^{-(1-s)/2}\Gamma\left(\frac{1-s}{2}\right)\zeta(1-s).$$

Démonstration. (1) On va montrer que sur $\Re(s) > 1$, $\zeta(s)\Gamma(s) = I(s)/(e^{2i\pi s} - 1)$ pour une certaine fonction $I(s)$ holomorphe sur $\mathbb{C}$. Soient $\Re(s) > 1$ et $n \geq 1$. Alors

$$\frac{\Gamma(s)}{n^s} = \int_0^{+\infty} t^{s-1} e^{-nt} dt$$

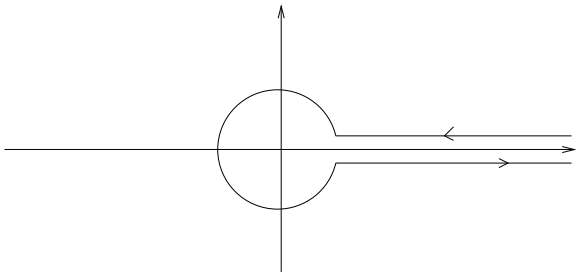
par changement de variables. En sommant sur n, on obtient

$$\Gamma(s)\zeta(s) = \int_0^{+\infty} \frac{t^{s-1}}{e^t - 1} dt.$$

On fixe une détermination du logarithme sur $\mathbb{C} \setminus \mathbb{R}_+ : \Im(\ln z) \in]0, 2\pi[$, et sorte que pour tout $s \in \mathbb{C}$, $z^{s-1} = \exp((s-1)\ln z)$ soit une fonction holomorphe sur $\mathbb{C} \setminus \mathbb{R}_+$. On intègre

$$I(s) := \int_{H_{r,\epsilon}} \frac{z^{s-1}}{e^z - 1} dz$$

le long du chemin $H_{r,\epsilon}$:



où l'arc du cercle est de rayon $r \in]0, 2\pi[$ et où les demi-droites horizontales sont situées à $\Im(z) = \pm\epsilon$. Quand r et $\epsilon \in]0, r[$ varient, on reste dans une région où la fonction que l'on intègre est holomorphe, donc l'intégrale $I(s)$ est indépendante de r, ϵ et est holomorphe en s sur $\mathbb{C}$. On calcule l'intégrale en trois morceaux et on fait tendre ϵ vers 0 :

$$I(s) = \int_{|z|=r} \frac{z^{s-1}}{e^z - 1} dz + (e^{2i\pi(s-1)} - 1) \int_r^{+\infty} \frac{t^{s-1}}{e^t - 1} dt.$$

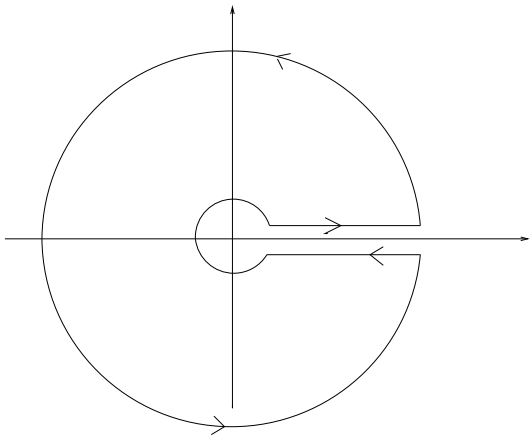
Noter que la première partie est un $O(r^{\Re(s)-1})$. Donc en faisant tendre r vers 0, on trouve que pour tout $\Re(s) > 1$, on a

$$(e^{2i\pi s} - 1)\Gamma(s)\zeta(s) = I(s). \tag{6.4}$$

Ce qui montre que $\zeta(s)$ se prolonge en une fonction méromorphe sur $\mathbb{C}$. Noter que l'égalité (6.4) est alors valable sur $\mathbb{C}$. Si s est un pôle de ζ avec $\Re(s) \leq 0$, on a $(e^{2i\pi s} - 1)\Gamma(s) = 0$, donc $s = -n$ avec $n \in \mathbb{N}$. Comme $e^{2i\pi s} - 1$ a un zéro simple en $-n$, ce n'est pas possible. Donc $\zeta(s)$ n'a pas de pôle avec $\Re(s) \leq 0$. Combiné avec la proposition 6.1.3, on trouve que $s = 1$ est l'unique pôle de $\zeta(s)$.

(2) On doit comparer deux fonctions méromorphes dont on connait les pôles. Il suffit de montrer l'égalité sur l'ouvert $\Re(s) < 0$. Soient $\Re(s) < 0$ et $k \geq 1$. Le théorème des résidus donne

$$\frac{1}{2i\pi} \int_{C_{k,\epsilon}} \frac{z^{s-1}}{e^z - 1} dz = \sum_{1 \leq |n| \leq k} (2i\pi n)^{s-1} \tag{6.5}$$



où le petit cercle est de rayon $r \in]0, 2\pi[$ et le grand de rayon $(2k+1)\pi$. Les deux segments horizontaux sont de partie imaginaire $= \pm\epsilon$. Comme $(-1)^{s-1} = e^{(s-1)i\pi} = -e^{i\pi s}$, le membre de droite dans l'égalité (6.5) ci-dessus est égal à $(2i\pi)^{s-1} \sum_{1\leq|n|\leq k} n^{s-1} = (2i\pi)^{s-1}(1-e^{i\pi s}) \sum_{1\leq n\leq k} n^{s-1}$. Quand $k \to +\infty$ il tend vers $(2i\pi)^{s-1}(1-e^{i\pi s})\zeta(1-s)$ (noter que $\Re(s) < 0$). Quand $k \to +\infty$, l'intégrale dans l'égalité (6.5) est proche de la somme de $-I(s)$ avec l'intégrale curviligne le long du grand cercle $|z| = (2k+1)\pi$. Cette dernière est un $O(k^{\Re(s)-1})$ car $|e^z - 1|$ est minorée par une constante $c > 0$ indépendante de k (on peut prendre $c = 1 - e^{-\pi/2}$ en distinguant les cas $|\Re(z)| \geq \pi/2$ et $|\Re(z)| \leq \pi/2$.) On trouve donc

$$-\frac{1}{2i\pi} I(s) = (2i\pi)^{s-1}(1-e^{i\pi s})\zeta(1-s).$$

En combinant avec l'égalité (6.4), on trouve

$$(2\pi)^s \zeta(1-s) = 2\Gamma(s)\zeta(s)\cos(\pi s/2).$$

L'équation fonctionnelle s'obtient en appliquant les formules de la proposition 6.1.4. □

Corollaire 6.1.6. *Les zéros de $\zeta(s)$ vérifient $s = -2, -4, -6, ...$ (appelés zéros triviaux) ou $0 \leq \Re(s) \leq 1$.*

Démonstration. Utiliser l'équation fonctionnelle et la proposition 6.1.3. □

Hypothèse de Riemann : les zéros non triviaux de $\zeta(s)$ sont tous situés sur la droite $\Re(s) = 1/2$.

Remarque 6.1.7 On peut montrer que pour tout $n \geq 1$:

$$\zeta(2n) = -\frac{(2i\pi)^{2n}}{2(2n)!} B_{2n}$$

où les $B_m \in \mathbb{Q}$ sont les *nombres de Bernoulli* déterminés par la relation

$$\frac{x}{e^x - 1} = \sum_{m \geq 0} B_m \frac{x^m}{m!}.$$

En revanche, les valeurs de $\zeta(s)$ aux entiers naturels impairs > 1 sont encore inconnues. Un célèbre théorème d'Apéry (1978) dit que $\zeta(3)$ est irrationnel. On sait (Rivoal, 2000) qu'il existe une infinité de $\zeta(2n+1)$ irrationnels. On sait aussi que l'un des nombres $\zeta(5), \zeta(7), \zeta(9), \zeta(11)$ est irrationnel (Zudilin, 2001).

6.1.4 Théorème des nombres premiers

La localisation des zéros de $\zeta(s)$ est cruciale pour estimer la répartition des nombres premiers. Soit

$$\pi(x) = \text{Card}\{p \text{ premiers} \mid p \leq x\}$$

la fonction de comptage des nombres premiers. Gauss et Legendre (vers 1790) ont conjecturé que $\pi(x)$ était équivalente à $x/\ln x$ quand x tend vers $+\infty$:

$$\pi(x) = \frac{x}{\ln x} + o(\frac{x}{\ln x}). \tag{6.6}$$

Il se trouve que $\pi(x)$ est mieux approché par la "fonction d'écart logarithmique intégral"

$$\text{Li}(x) := \int_2^x \frac{1}{\ln t} dt$$

que $x/\ln x$.

Theorem 6.1.8. (Hadamard, de la Vallée Poussin 1896) *Il existe une constante $c > 0$ telle que*

$$\pi(x) = \int_2^x \frac{dt}{\ln t} + O(x \exp(-c(\ln x)^{1/2}))$$

quand x tend vers $+\infty$.

Une forme plus faible mais plus explicte

$$\pi(x) = \frac{x}{\ln x} + O(x(\ln x)^{-2}).$$

La meilleure approximation connue actuellement est

$$\pi(x) = \text{Li}(x) + O\left(x \exp(-c(\ln x)^{3/5}/\ln(\ln x)^{1/5})\right)$$

(Korobov, Vinogradov).

Remarque 6.1.9 On peut montrer que l'hypothèse de Riemann est équivalente à l'approximation

$$\pi(x) = \text{Li}(x) + O(x^{1/2} \ln x)$$

et que cette approximation est optimale (1/2 ne peut pas être remplacé par un exposant plus petit).

Remarque 6.1.10 Le théorème de Hadamard-de la Vallée Poussin est plus fort que le théorème des nombres premiers proprement dit (équivalence (6.6)). Il existe maintenant des preuves tout-à-fait accessibles de ce dernier. Voir par exemple la présentation par D. Zagier de la preuve de D.J. Newman en 1980 (`http://minilien.fr/a0lzdl`).

Exercice 6.1.11 Montrer que sur $]0, +\infty[$, la fonction

$$\ln|\ln x| + \ln x + \sum_{n\geq 2} \frac{(\ln x)^n}{n.n!}$$

est une primitive de $1/\ln x$. En déduire que $\mathrm{Li}(x) \sim x/\ln x$.

6.2 Fonctions L de Dirichlet

Il existe différentes généralisations de la fonction zêta de Riemann. Nous évoquerons les séries de Dirichlet et les fonctions zêta de Dedekind.

6.2.1 Caractères de Dirichlet

Un *caractère* en général est un homomorphisme d'un groupe fini vers $\mathbb{C}^*$.

Lemme 6.2.1. *Soit G un groupe fini abélien.*

(1) *L'ensemble $\widehat{G}$ des caractères de G a une structure naturelle de groupe abélien fini, isomorphe (non canoniquement) à G.*

(2) *L'application "évaluation"*

$$G \to \widehat{(\widehat{G})}, \quad g \mapsto (\chi \mapsto \chi(g))$$

est isomorphisme de groupes.

(3) (Relation d'orthogonalité) *Soit $g \in G$. Alors*

$$\sum_{\chi\in\widehat{G}} \chi(g) = \begin{cases} \mathrm{Card}(G) & si \quad g = 1 \\ 0 & sinon. \end{cases}$$

(4) *Si $\chi \neq 1$, alors*

$$\sum_{g\in G} \chi(g) = 0.$$

Démonstration. (1) La structure de groupe est donnée par

$$(\chi_1\chi_2)(a) = \chi_1(a)\chi_2(a).$$

Si on écrit $G = \prod_i C_i$ comme un produit direct de groupes cycliques C_i, alors on a

$$\widehat{G} \simeq \prod_i \widehat{C}_i,$$

et il suffit de montrer l'énoncé pour un groupe cyclique $G \simeq \mathbb{Z}/n\mathbb{Z}$. Dans ce cas-là, $\widehat{G}$ est isomorphe au groupe $\mathbb{\mu}_n(\mathbb{C})$ des racines (non-nécessairement primitifs) n-ième de l'unité dans $\mathbb{C}$. Donc $\widehat{G}$ est cyclique d'ordre n et isomorphe (non canoniquement) à G.

(2) L'application évaluation est clairement un homomorphisme de groupe. On voit qu'elle est injective en écrivant G comme un produit direct de sous-groupes cycliques. Elle est donc un isomorphisme par comparaison de cardinalités.

(3) La relation est évidente si $g = 1$. Supposons $g \neq 1$. Par (2), il existe $\chi_1 \in \widehat{G}$ tel que $\chi_1(g) \neq 1$. On multiplie la somme $\Sigma := \Sigma_\chi \chi(g)$ par $\chi_1(g)$ et on obtient $\chi_1(g).\Sigma = \Sigma$. Donc $\Sigma = 0$.

(4) On identifie G à $\widehat{\widehat{G}}$ par (2) et applique (3) (au groupe $\widehat{G}$). □

Définition 6.2.2 Soit $m \geq 1$ un entier. Un *caractère de Dirichlet* modulo m est un homomorphisme de groupes

$$\chi : (\mathbb{Z}/m\mathbb{Z})^* \to \mathbb{C}^*,$$

c'est-à-dire un caractère du groupe $(\mathbb{Z}/m\mathbb{Z})^*$.

Un caractère de Dirichlet χ induit canoniquement en une application $\overline{\chi} : \mathbb{Z} \to \mathbb{C}$ par $\overline{\chi}(a) = 0$ si $(a, m) \neq 1$ et $\overline{\chi}(a) = \chi(\tilde{a})$ sinon (où $\tilde{a}$ est la classe de a modulo m). On a

$$\overline{\chi}(a + m) = \overline{\chi}(a), \quad \overline{\chi}(ab) = \overline{\chi}(a)\overline{\chi}(b), \quad a, b \in \mathbb{Z}.$$

On note souvent par abus de notation l'application $\overline{\chi}$ encore par χ. De toutes façons, la notation $\overline{\chi}$ n'est pas très heureuse à cause de la possibilité de confusion avec la conjugaison complexe...

6.2.2 Non nullité de $L(1, \chi)$

Définition 6.2.3 Le caractère trivial χ_0 est défini par $\chi_0(a) = 1$ si $(a, m) = 1$ et $\chi_0(a) = 0$ sinon. La série

$$L(s, \chi) = \sum_{n \geq 1} \frac{\chi(n)}{n^s}$$

est appelée la *fonction L de Dirichlet* associée à χ. On retrouve (presque) la fonction zêta de Riemann avec $m = 1$ et $\chi = \chi_0$. Comme $|\chi(n)| = 0$ ou 1, la série converge uniformément sur tout compact de $\{\Re(s) > 1\}$, et définit une fonction holomorphe sur cet ouvert de $\mathbb{C}$.

On sait que la série $\sum_n n^{-1}$ diverge, alors que $\sum_n (-1)^n n^{-1}$ converge. Le lemme suivant est une sorte de généralisation des séries alternées.

Lemme 6.2.4. *Soit $(z_n)_n$ une suite de nombres complexes.*

(1) (Sommation d'Abel) *Soit* $f : [1, +\infty[\to \mathbb{C}$ *une fonction* C^1. *Posons* $A(t) = \sum_{n \leq t} z_n$. *Alors pour tout* $x \geq 1$, *on a*

$$\sum_{1 \leq n \leq x} z_n f(n) = A(x)f(x) - \int_1^x A(t)f'(t)dt.$$

(2) *Soit* $r \in \mathbb{R}$. *On suppose que* $|A(t)|t^{-r}$ *est bornée (par une constante* c*) quand* t *tend vers* $+\infty$. *Alors la série* $\sum_{n \geq 1} z_n n^{-s}$ *définit une fonction holomorphe sur* $\Re(s) > r$.

Démonstration. (1) La fonction $A(x)$ est une fonction en escalier et on vérifie immédiatement que l'égalité à montrer se ramène à $x = m$ un entier naturel. On a

$$\int_1^m A(t)f'(t)dt = \sum_{k=1}^{m-1} \int_k^{k+1} A(t)f'(t)dt = \sum_{k=1}^{m-1} (\sum_{n=1}^{k} z_n(f(k+1) - f(k)))$$

$$= \sum_{n=1}^{m-1} \sum_{k=n}^{m-1} z_n(f(k+1) - f(k)) = \sum_{n=1}^{m-1} z_n(f(m) - f(n)).$$

Donc

$$\int_1^m A(t)f'(t)dt + \sum_{n=1}^{m} z_n f(n) = \sum_{n=1}^{m} z_n f(m) = A(m)f(m).$$

(2) On a

$$\sum_{m \leq n \leq k} z_n n^{-s} = A(k)/k^s - A(m)/m^s + s \int_m^k A(t)/t^{s+1}dt$$

le terme de droite en valeur absolue est majoré par

$$(2c + |s|c/\delta)m^{-\delta}, \quad \delta = \Re(s) - r.$$

D'où la convergence uniforme sur tout compact de $\Re(s) > r$ et l'holomorphie de $\sum_{n \geq 1} z_n n^{-s}$ sur cette région. □

Proposition 6.2.5. *Soit* χ *un caractère modulo* m.

(1) *Pour* $\Re(s) > 1$, *on a*

$$L(s, \chi) = \prod_p (1 - \chi(p)p^{-s})^{-1}.$$

En particulier $L(s, \chi) \neq 0$ *si* $\Re(s) > 1$.

(2) *Si* $\chi = \chi_0$ *le caractère trivial modulo* m. *Alors*

$$L(s, \chi_0) = \zeta(s) \prod_{p|m} (1 - p^{-s}), \quad \Re(s) > 1.$$

Elle se prolonge en une fonction méromorphe sur $\mathbb{C}$, *avec un unique pôle en* 1, *de résidu* $\varphi(m)/m$.

(3) *Supposons $\chi \neq \chi_0$. Alors $L(s,\chi)$ converge uniformément sur tout compact de $\Re(s) > 0$. En particulier $L(s,\chi)$ est holomorphe sur $\Re(s) > 0$.*

Démonstration. (1) se montre comme 6.1.1 (3). (2) découle de (1), car $\chi_0(p) = 1$ si $(p,m) = 1$ et $\chi_0(p) = 0$ si $p|m$, et du théorème 6.1.5(1). Le résidu de $L(s,\chi_0)$ en 1 est égal à $\prod_{p|m}((p-1)/p) = \varphi(m)/m$.

(3) Pour tout $t \geq 1$, posons $A(t) = \sum_{1\leq n\leq t} \chi(n)$. Pour tout $k \in \mathbb{Z}$,

$$\sum_{k\leq i\leq m+k} \chi(i) = \sum_{0\leq a\leq m-1,\ (a,m)=1} \chi(a) = 0$$

d'après le lemme 6.2.1 (4). Il suit que $|A(t)| \leq \varphi(m)$ en écrivant $t = mr + t'$, $r \in \mathbb{N}$, $t' \in [0,m]$. On peut alors appliquer le lemme 6.2.4 (2). □

Remarque 6.2.6 Tout comme la fonction ζ, la fonction $L(s,\chi)$ admet un prolongement méromorphe (holomorphe sous certains hypothèses sur χ : primitif et non trivial) sur $\mathbb{C}$ et une équation fonctionnelle. On connaît ses zéros en $\Re(s) < 0$. Voir § **??**.

GRH (Hypothèse de Riemann Généralisée) : Les zéros de $L(s,\chi)$ situés dans $0 \leq \Re(s) \leq 1$ sont de $\Re(s) = 1/2$.

Lemme 6.2.7. *Soit $a \in (\mathbb{Z}/m\mathbb{Z})^*$ d'ordre d. Alors*

$$\prod_{\chi}(1 - \chi(a)T) = (1 - T^d)^{\varphi(m)/d} \in \mathbb{C}[T].$$

Démonstration. Soit H le groupe des caractères modulo m. Alors a correspond à un caractère $a^* : \chi \mapsto \chi(a)$ de H. C'est un élément d'ordre d dans $\widehat{H} \simeq (\mathbb{Z}/m\mathbb{Z})^*$ (c'est l'isomorphisme canonique de 6.2.1(2) avec $G = (\mathbb{Z}/m\mathbb{Z})^*$). Il suit facilement que a^* est un homomorphisme surjectif de H dans $\mathbb{\mu}_d(\mathbb{C})$. Donc

$$\prod_{\chi\in H}(1 - a^*(\chi)T) = \prod_{w\in\mathbb{\mu}_d(\mathbb{C})}\ \prod_{a^*(\chi)=w}(1 - wT) = \prod_{w\in\mathbb{\mu}_d(\mathbb{C})}(1 - wT)^{\varphi(m)/d}.$$

Or

$$\prod_{w\in\mathbb{\mu}_d(\mathbb{C})}(1 - wT) = T^{-d}\prod_{w}(T^{-1} - w) = T^{-d}((T^{-1})^d - 1) = 1 - T^d,$$

et le lemme est démontré. □

Lemme 6.2.8. *Soit $(a_n)_{n\geq 1}$ une suite de nombres réels positifs ou nuls. On suppose que la série $\sum_{n\geq 1} a_n n^{-s}$ converge et définit une fonction holomorphe $g(s)$ sur $\Re(s) > 1$. Supposons de plus que $g(s)$ s'étend en une fonction holomorphe sur $\Re(s) > 0$. Alors la série $\sum_{n\geq 1} a_n n^{-t}$ converge vers $g(t)$ pour tout $t > 0$.*

Démonstration. Soit $b_k = (-1)^k g^{(k)}(2)/k!$. On a

$$g(s) = \sum_{k\geq 0} b_k (2-s)^k$$

dans un voisinage ouvert de 2. Mais $g(s)$ est holomorphe, donc développable en série entière sur tout le disque disque ouvert $\{s \in \mathbb{C} \mid |s-2| < 2\}$. Il suit que l'égalité ci-dessus vaut pour tout s dans ce disque.

Soit $t \in]0,2[$. On a

$$g(t) = \sum_{k\geq 0} b_k (2-t)^k = \sum_{k\geq 0} \left(\sum_{n\geq 1} a_n \frac{(\ln n)^k}{k!} n^{-2} \right) (2-t)^k.$$

C'est une série sommable à termes positifs ou nuls, on peut donc permuter les signes somme

$$g(t) = \sum_{n\geq 1} \left(\sum_{k\geq 0} \frac{(\ln n)^k}{k!} (2-t)^k \right) a_n n^{-2} = \sum_{n\geq 1} a_n n^{-t}.$$

□

Theorem 6.2.9. *Soit χ un caractère modulo m. Alors $L(1,\chi) \neq 0$.*

Démonstration. Considérons le produit fini sur tous les caractères modulo m :

$$\zeta_m(s) := \prod_{\chi} L(s,\chi).$$

C'est une fonction holomorphe sur $\{\Re(s) > 0\} \setminus \{1\}$. Comme les $L(s,\chi)$ sont holomorphes dans un voisinage de $s = 1$ si $\chi \neq \chi_0$ et que $L(s,\chi_0)$ a un pôle simple en 1, il suffit de montrer que $\zeta_m(s)$ a un pôle en $s = 1$. Supposons le contraire. Alors $\zeta_m(s)$ est holomorphe sur $\Re(s) > 0$.

Pour tout $p \nmid m$, notons $d(p)$ l'ordre de p dans $(\mathbb{Z}/m\mathbb{Z})^*$. Alors pour tout $\Re(s) > 1$, en utilisant 6.2.7, on a

$$\zeta_m(s) = \prod_{p\nmid m} \prod_{\chi} (1 - \chi(p)p^{-s})^{-1} = \prod_{p\nmid m} \left(\frac{1}{1-p^{-d(p)s}} \right)^{\varphi(m)/d(p)}.$$

C'est une série de la forme $\sum_{n\geq 1} a_n n^{-s}$ avec $a_n \in \mathbb{R}_+$. Par le lemme 6.2.8, cette série converge pour tout $t > 0$ et donc

$$\zeta_m(t) = \prod_{p\nmid m} \left(\frac{1}{1-p^{-d(p)t}} \right)^{\varphi(m)/d(p)} = \sum_{n\geq 1} a_n n^{-t}$$

(cf. lemme 6.2.10). Notons que

$$\left(\frac{1}{1-p^{-d(p)t}} \right)^{\varphi(m)/d(p)} = (1 + p^{-d(p)t} + p^{-2d(p)t} + \cdots)^{\varphi(m)/d(p)}$$

$$\geq 1 + p^{-\varphi(m)t} + p^{-2\varphi(m)t} + \cdots = (1 - p^{-\varphi(m)t})^{-1}.$$

Donc pour tout $t > 1/\varphi(m)$,

$$\zeta_m(t) \geq \prod_{p \nmid m} (1 - p^{-\varphi(m)t})^{-1} = L(\varphi(m)t, \chi_0).$$

Mais le membre de droite tend vers $+\infty$ quand t tend vers $1/\varphi(m)$. Contradiction. □

Lemme 6.2.10. *Considérons pour tout nombre premier p, une suite de nombres complexes $(a_{p^k})_{k\geq 1}$. On pose $b_1 = 1$ et pour tout $n \geq 2$*

$$b_n = a_{p_1^{r_1}} \cdots a_{p_\ell{}^{r_\ell}}, \quad \text{si } n = p_1^{r_1} \cdots p_\ell{}^{r_\ell}.$$

Soit $s \in \mathbb{C}$ tel que la série $\sum_{n\geq 1} b_n n^{-s}$ converge absolument. Alors le produit infini

$$\prod_p (1 + \sum_{k\geq 1} a_{p^k} p^{-ks})$$

existe et est égal à $\sum_{n\geq 1} b_n n^{-s}$.

Démonstration. Pour tout p, la série $1 + \sum_{k\geq 1} a_{p^k} n^{-ks}$ est une série extraite de $\sum_n b_n n^{-s}$, donc est absolument convergente. Soit $N \geq 2$, le produit partiel

$$\prod_{p\leq N} (1 + \sum_{k\geq 1} a_{p^k} p^{-ks})$$

est la somme des $b_n n^{-s}$ pour les n dont les facteurs premiers sont $\leq N$. Cela impliquement facilement le lemme. □

6.2.3 Théorème de la progression arithmétique

On a $\mathbb{Z}[i] = \mathbb{Z}[X]/(X^2+1)$. On a vu que l'extension $\mathbb{Z} \to \mathbb{Z}[i]$ est décomposée au-dessus d'un nombre premier $p > 2$ si $X^2 + 1 \in \mathbb{F}_p[X]$ est scindée. Elle est inerte sinon. Une question naturelle est de savoir s'il existe beaucoup de p pour lesquels l'extension est décomposée au-dessus de p. Cette question est équivalente à trouver les nombres premiers $p \equiv 1 \mod 4$.

Plus généralement, soient $m, a \geq 1$ des entiers naturels (par exemple $m = 4$ et $a = 1$). On cherche les nombres premiers dans les termes de la progression arithmétique

$$\{a + mn \mid n \in \mathbb{N}\},$$

autrement dit, les nombres premiers congrus à a modulo m. Il faut bien sûr supposer a, m premiers entre eux pour qu'il en existe. Mais même avec l'hypothèse $(a, m) = 1$, il n'est pas évident qu'il existe *un* nombre premier $\equiv a \mod m$.

Theorem 6.2.11. (Dirichlet) *Soient m, a des entiers premiers entre eux. Alors l'ensemble*

$$A = \{p \text{ premiers} \mid p \equiv a \mod m\}$$

est infini.

Nous avons besoin de quelques résultats préliminaires à la démontration du théorème.

Lemme 6.2.12. *Soit χ un caractère modulo m. Soit*

$$f_\chi(t) = \sum_p \chi(p)/p^t$$

pour $t \in]1, +\infty[$.

(1) *On a*

$$\sum_{k\geq 2,\ p} p^{-kt} \leq 1.$$

Lorsque $t \to 1^+$, on a

$$\sum_p p^{-t} \sim \ln(\frac{1}{t-1}).$$

(2) *Si $\chi = \chi_0$ le caractère trivial, alors*

$$f_\chi(t) \sim \ln(\frac{1}{t-1}), \quad t \to 1^+$$

(3) *Si $\chi \neq \chi_0$, alors $f_\chi(t)$ est bornée dans un voisinage de 1.*

Démonstration. (1) On a pour tout $t > 1$

$$\sum_p \sum_{k\geq 2} p^{-kt} = \sum_p 1/(p^t(p^t-1)) \leq \sum_p 1/(p(p-1)) \leq \sum_{n\geq 2} 1/(n(n-1)) = 1.$$

D'autre part,

$$\ln(\zeta(t)) = -\sum_p (\ln(1-p^{-t})) = \sum_p \left(\sum_{k\geq 1} 1/(kp^{kt}) \right) = \sum_p p^{-t} + \Psi(t)$$

avec $\Psi(t) = \sum_{p,k\geq 2} p^{-kt}/k$ qui prend ses valeurs dans $[0,1]$. Le corollaire résulte alors du fait que $\zeta(t) = 1/(t-1) + O(1)$ dans un voisinage de 1.

(2) On a $f_{\chi_0}(t) = \sum_p p^{-t} - \sum_{p|m} p^{-t}$. L'équivalence désirée résulte de (1).

(3) Soit ln le logarithme qui est continue sur $\mathbb{C} \setminus \mathbb{R}_{\leq 0}$ (les arguments appartiennent à $]-\pi, \pi[$). On a $\ln(1+z) = \sum_{k\geq 1} (-1)^k z^k/k$ si $|z| < 1$. On applique ce logarithme à 6.2.5 (1),

$$\ln L(s,\chi) = -\sum_p \ln(1-\chi(p)p^{-s}) = \sum_{k,p} (\chi(p)^k p^{-ks})/k = f_\chi(s) + F_\chi(s)$$

avec

$$|F_\chi(s)| = |\sum_{p,k\geq 2} \chi(p)^k/kp^{ks}| \leq \sum_{p,k\geq 2} 1/p^{kt} \leq 1$$

si $t = \Re(s)$ d'après (1). Comme $L(t,\chi)$ converge vers $L(1,\chi) \neq 0$ (théorème 6.2.9), on voit que $f_\chi(t)$ reste bornée dans un voisinage de 1. □

Démonstration. (du théorème 6.2.11) Nous allons étudier les variations de la fonction

$$g(s) = \sum_{p \in A} p^{-t}$$

(pour $t > 1$) lorsque t tend vers 1. On a

$$\sum_{\chi} \chi(a)^{-1} f_\chi(t) = \sum_{\chi} \chi(a)^{-1} \sum_{p} \chi(p) p^{-t} = \sum_{p} \left(\sum_{\chi} \chi(a)^{-1} \chi(p) \right) p^{-t}.$$

En appliquant le lemme 6.2.1 (3), on trouve que le dernier membre est égal à $\sum_{p \equiv a \mod m} \varphi(m) p^{-t} = \varphi(m) g(t)$. Il suit que

$$\varphi(m) g(t) = \sum_{\chi} \chi(a)^{-1} f_\chi(t) = f_{\chi_0}(t) + \sum_{\chi \neq \chi_0} \chi(a)^{-1} f_\chi(t).$$

Il suit du lemme 6.2.12 que $g(t) \to \infty$ lorsque $t \to 1$. En particulier, A n'est pas fini. □

Remarque 6.2.13 On peut montrer (théorème de Siegel-Walfisz) que la répartition des nombres premiers suivant leurs classes modulo m est uniforme :

$$\mathrm{Card}\{p \text{ premiers} \mid p \leq x,\ p \equiv a \mod m\} \sim \frac{1}{\varphi(m)} \mathrm{Li}(x).$$

6.3 Fonction zêta de Dedekind

On fixe un corps de nombres K. Rappelons que $\mathcal{O}_K$ désigne l'anneau des entiers de K. La fonction zêta de Dedekind de K est la fonction à variable complexe s :

$$\zeta_K(s) = \sum_{I \subseteq \mathcal{O}_K} \frac{1}{N(I)^s} \tag{6.7}$$

où la somme porte sur l'ensemble des idéaux non nuls I de $\mathcal{O}_K$ et où $N(I) = \mathrm{Card}(\mathcal{O}_K/I)$ (4.1.1). Quand $K = \mathbb{Q}$, on retrouve la fonction zêta de Riemann. Pour tout $n \geq 1$, soit j_n le nombre d'idéaux I de $\mathcal{O}_K$ de norme $N(I) = n$. C'est un nombre fini d'après 4.1.6. On a

$$\zeta_K(s) = \sum_{n \geq 1} \frac{j_n}{n^s}.$$

Lemme 6.3.1. *Soit K un corps de nombres.*

(1) *La série (6.7) converge uniformément sur tout compact de $\{\Re(s) > 1\}$ et définit ainsi une fonction holomorphe sur $\{\Re(s) > 1\}$.*

(2) *Si $\Re(s) > 1$, on a le* produit eulérien

$$\zeta_K(s) = \prod_{\mathfrak{q}} (1 - N(\mathfrak{q})^{-s})^{-1}$$

où $\mathfrak{q}$ parcourt les idéaux maximaux de $\mathcal{O}_K$. En particulier $\zeta_K(s) \neq 0$.

Démonstration. On peut montrer que $\sum_{n\leq t} j_n$ est un $O(t)$, ce qui implique (1) par 6.2.4 (2). Nous donnons ici une preuve différente.

Si $\mathfrak{q}$ est un idéal maximal de $\mathcal{O}_K$, on a $\mathfrak{q}\cap\mathbb{Z} = p\mathbb{Z}$ pour un nombre premier p. On note $f_\mathfrak{q}$ le degré $[\mathcal{O}_K/\mathfrak{q} : \mathbb{Z}/p\mathbb{Z}]$. On sait que $N(\mathfrak{q}) = p^{f_\mathfrak{q}}$ par définition. Soit $t > 1$ un nombre réel. Pour tout $N \geq 1$, on a

$$\prod_{\mathfrak{q}, N(\mathfrak{q})\leq N} \frac{1}{1-N(\mathfrak{q})^{-t}} \leq \prod_{p\leq N} \prod_{\mathfrak{q}\cap\mathbb{Z}=p\mathbb{Z}} \frac{1}{(1-p^{-tf_\mathfrak{q}})} \leq \prod_{p\leq N} \prod_{\mathfrak{q}\cap\mathbb{Z}=p\mathbb{Z}} \frac{1}{(1-p^{-t})}$$

(La première inégalité n'est en général pas une égalité car dans le produit du milieu, on a admis éventuellement des facteurs indexés par $N(\mathfrak{q}) > p$ et que ces facteurs sont > 1). Comme il existe au plus $d := [K : \mathbb{Q}]$ idéaux premiers $\mathfrak{q}$ au-dessus de p, le terme de droite est majoré par

$$\prod_{p\leq N} (\frac{1}{1-p^{-t}})^d \leq \zeta(t)^d.$$

Cela implique que le produit infini $\prod_\mathfrak{q}(1-N(\mathfrak{q})^{-t})^{-1}$ converge quand $t > 1$.

Maintenant tout idéal I de $N(I) \leq N$ se décompose comme $I = \mathfrak{q}_1^{r_1}\cdots\mathfrak{q}_m^{r_m}$ avec $N(\mathfrak{q}_i) \leq N$. Donc si $t > 1$, on a

$$\sum_{N(I)\leq N} N(I)^{-t} \leq \prod_{N(\mathfrak{q})\leq N} \sum_{n\geq 1} 1/N(\mathfrak{q}^n)^{-t} = \prod_{N(\mathfrak{q})\leq N} \frac{1}{1-N(\mathfrak{q})^{-t}} \leq \zeta(t)^d$$

et la série à termes positifs $\sum_I N(I)^{-t}$ converge.

Soit $\delta > 0$ et $\Re(s) \geq 1+\delta$. Pour tout $N > 1$, on a

$$\sum_{N(I)\geq N} |N(I)^{-s}| \leq \sum_{N(I)\geq N} N(I)^{-(1+\delta)},$$

ce qui implique la convergence uniforme sur $\{\Re(s) \geq 1+\delta\}$. D'où (1). La propriété (2) résulte d'une variante du lemme 6.2.10 où les entiers n sont remplacés par des idéaux de $\mathcal{O}_K$ et les nombres premiers par des idéaux maximaux. □

Theorem 6.3.2. *Soit K un corps de nombres.*

(1) *La fonction $\zeta_K(s)$ se prolonge en une fonction méromorphe sur $\mathbb{C}$ avec un unique pôle simple en $s = 1$.*

(2) *Le résidu en $s = 1$ de $\zeta_K(s)$ est égal à*

$$\lim_{s\to 1}(s-1)\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2}}{|\mathbb{\mu}(K)||d_K|^{1/2}} h_K R_K.$$

où $r_1, 2r_2$ sont les nombres de plongements réels et imaginaires, h_K est le nombre de classes, et R_K le régulateur (6.3.3).

(3)

$$\lim_{s\to 0} \frac{\zeta_K(s)}{s^{r_1+r_2-1}} = -\frac{h_K R_K}{|\mathbb{\mu}(K)|}.$$

(4) *On a aussi une équation fonctionnelle.*

(5) *Zéros triviaux : les entiers strictement négatifs pairs sont des zéros d'ordre* $r_1 + r_2$*, les entiers strictement négatifs impairs sont des zéros d'ordre* r_2 *(si* $r_2 > 0$*). Les autres zéros de* $\zeta_K(s)$ *sont dans* $0 \leq \Re(s) \leq 1$.

Définition 6.3.3 Soient $t = r_1 + r_2 - 1$ et $u_1, \ldots, u_t$ une famille d'unités fondamentales de sorte que $\ell(u_1), \ldots, \ell(u_t)$ soit une base du réseau $\ell(U)$ dans $H \subset \mathbb{R}^{t+1}$. Le *régulateur* de L est le volume du réseau $\ell(U)$ dans H, c'est-à-dire le nombre

$$R_L = |\det(\ell(u_1), \ldots, \ell(u_t))| \in \mathbb{R}.$$

Il est indépendant du choix de la famille des u_i (noter que la matrice qui intervient ci-dessus est d'ordre $(t+1) \times t$, on peut supprimer n'importe laquelle des lignes parce que ces vecteurs colonnes se trouvent dans l'hyperplan H).

Bibliographie

[1] D. Marcus, *Number Fields*, Springer Verlag, 1977.

[2] J. Milne, *Algebraic Number Theory*, `http://www.jmilne.org/math/CourseNotes/ANT.pdf`

[3] J. Neukirch, *Algebraic number theory*, Springer Verlag, 1999.

[4] S. Patterson, *An introduction to the theory of the Riemann zeta-function*, Cambridge University Press, 1988.

[5] P. Samuel, *Théorie algébrique des nombres*, Hermann, 1967.

[6] L. Washington, *Introduction to cyclotomic fields*, Springer Verlag, 1982.

Index