Université P. et M. Curie (Paris VI) date de mise à jour: 25/03/2009
Deuxième semestre 2008/2009

Master de sciences et technologies 1ère année - Mention : Mathématiques et applications
Spécialité : Mathématiques Fondamentales

Sixième fascicule : 9/03/2009

4 Corps de Nombres

4.1 Norme, trace, discriminant

Rappelons que tous les anneaux considérés sont commutatifs et unitaires. Sauf mention explicite du contraire on les supposera aussi intègres. Les éléments inversibles (on dit encore *les unités*) d'un anneau A forment un groupe multiplicatif noté $A^\times$. On désigne par K le corps des fractions de A.

Un A–module M est *de type fini* s'il est engendré par une partie finie $\{x_1, \dots, x_m\}$. Cela signifie que tout élément de M peut s'écrire comme combinaison linéaire à coefficients dans A de $x_1, \dots, x_m$:

$$M = \{a_1x_1 + \cdots + a_mx_m \ ; \ (a_1, \dots, a_m) \in A^m\},$$

ce que l'on écrit $M = Ax_1 + \cdots + Ax_m$. Un A–module M est *libre* s'il existe une famille $\{e_i\}_{i\in I}$ d'éléments de M (qu'on appelle *base de M sur A*) telle que tout élément de M s'écrive *de manière unique* comme combinaison linéaire de ces éléments : pour tout $x \in M$ il existe une *unique* famille $\{a_i\}_{i\in I}$ d'éléments de A, de support

$$\{i \in I \ ; \ a_i \neq 0\}$$

fini, telle que

$$x = \sum_{i\in I} a_ie_i.$$

L'unicité signifie que les éléments e_i, $(i \in I)$, sont linéairement indépendants sur A : une relation $\sum_{i\in I} a_ie_i = 0$ avec une famille $\{a_i\}_{i\in I}$ d'éléments de A, de support fini entraîne $a_i = 0$ pour tout $i \in I$. Quand M est un A-module de libre de base $\{e_i\}_{i\in I}$, on peut considérer le K-espace vectoriel V ayant pour base $\{e_i\}_{i\in I}$, il contient M comme sous–A–module.

Un A–module M est libre de type fini si et seulement s'il admet une base $\{e_1, \dots, e_n\}$: tout élément x de M s'écrit de manière unique

$$x = a_1e_1 + \cdots + a_ne_n$$

avec des a_i dans A. L'entier n est la dimension du K-espace vectoriel V engendré par $\{e_1, \dots, e_n\}$, il ne dépend pas du choix de la base. C'est le *rang du A-module libre M*. On étend la définition du rang à un A-module quelconque M en disant que c'est le nombre maximal d'éléments de M linéairement indépendants sur A.

Les *éléments de torsion* d'un A-module M sont les éléments $x \in M$ pour lesquels il existe $a \in A$, $a \neq 0$, tel que $ax = 0$. Ils forment un sous–A–module M_{tors} de M. Un A-module est dit

sans torsion si le seul élément de torsion est 0. Par exemple un A–module libre est sans torsion. Un A-module M est *de torsion* si tout élément de M est de torsion : $M_{\rm tors} = M$.

Exemples. 1. Prenons $A = \mathbf{Z}$. Un $\mathbf{Z}$–module n'est autre qu'un groupe abélien. Un élément est de torsion si et seulement s'il est d'ordre fini dans le groupe. Un $\mathbf{Z}$–module de type fini G a un sous–groupe de torsion $G_{\rm tors}$ fini, un rang $r \geq 0$ fini et G est isomorphe à $G_{\rm tors} \times \mathbf{Z}^r$. Ainsi un groupe fini est de torsion, alors que $\mathbf{Z}^r$ est un $\mathbf{Z}$–module libre de type fini. Des exemples de $\mathbf{Z}$–modules libres de type fini que nous allons étudier sont $\mathbf{Z}$, $\mathbf{Z}[i] = \mathbf{Z} + \mathbf{Z}i$, $\mathbf{Z}[\sqrt{2}]$, $\mathbf{Z}[\sqrt{5}]$, $\mathbf{Z}[\Phi]$ où $\Phi = (1+\sqrt{5})/2$ est le nombre d'or, $\mathbf{Z}[\zeta_n]$ où n est un entier positif et ζ_n une racine primitive n–ième de l'unité.
2. Le sous-anneau de $\mathbf{C}$ engendré par $1/2$ sur $\mathbf{Z}$:

$$\mathbf{Z}[1/2] = \big\{a/2^n \ ; \ a \in \mathbf{Z}, \ n \in \mathbf{Z}_{\geq 0}\big\},$$

constitué des nombres rationnels dont le développement diadique (en base 2) est fini, n'est pas un $\mathbf{Z}$-module de type fini.
3 Soient A un anneau. L'ensemble $A^{(\mathbf{Z}_{\geq 0})}$ formé des suites d'éléments de A de support fini

$$\big(a_0, a_1, \ldots, a_n, \ldots\big) \ , \quad \text{il existe } n_0 \geq 0 \text{ tel que } a_n = 0 \text{ pour } n \geq n_0$$

est un A-module libre dont une base est $\{e_i\}_{i \in \mathbf{Z}_{\geq 0}}$ avec

$$e_i = \big(\delta_{i,0}, \ldots, \delta_{in}, \ldots\big), \qquad \delta_{ij} = \begin{cases} 1 & \text{si } i = j \\ 0 & \text{si } i \neq j. \end{cases}$$

4. Comme $\mathbf{Z}$–module, $\mathbf{Q}$ n'est pas de type fini : une partie libre a au plus un élément. Il est de rang 1 et sans torsion.
5. Le groupe additif $\mathbf{Q}/\mathbf{Z}$ est de torsion, de rang 0 ; il n'est pas de type fini.
6. Soient F est un corps, $A = F[T]$, $K = F(T)$, et $L = K(\sqrt{T})$ un corps de décomposition du polynôme $X^2 - T \in F[X]$. Le sous–anneau $F[\sqrt{T}]$ de L engendré par $\sqrt{T}$ est un A-module libre de type fini.

Soient A un anneau, M un A-module libre de type fini et u un endomorphisme de M. On note ${\rm Tr}(u)$, ${\rm N}(u)$ et $P_u(X)$ la trace, la norme et le polynôme caractéristique de u respectivement. Dans une base $(e_1, \ldots, e_n)$ de M sur A, si $\mathsf{A} = \big(a_{ij}\big)_{1 \leq i,j \leq n}$ désigne la matrice attachée à u, on a

$${\rm Tr}(u) = \sum_{i=1}^{n} a_{ii} \quad \text{et} \quad {\rm N}(u) = \det(\mathsf{A}).$$

D'autre part en désignant par I l'endomorphisme identité de M on a

$$P_u(X) = \det(XI - u) = X^n - {\rm Tr}(u)X^{n-1} + \cdots + (-1)^n {\rm N}(u).$$

Quand u_1 et u_2 sont des endomorphismes de M on a

$${\rm Tr}(u_1 + u_2) = {\rm Tr}(u_1) + {\rm Tr}(u_2) \quad \text{et} \quad {\rm N}(u_1 \circ u_2) = {\rm N}(u_1){\rm N}(u_2).$$

Supposons de plus que M est un anneau - on le notera B. Soit donc B un anneau contenant A qui est un A-module libre de rang fini. Pour $x \in B$ l'application

$$\begin{array}{rccc} [x] : & B & \longrightarrow & B \\ & y & \longmapsto & xy \end{array}$$

est un endomorphisme du A-module B et l'application $x \mapsto [x]$ est un homomorphisme d'anneaux de B dans l'anneau des endomorphismes de B.
La norme, la trace et le polynôme caractéristique de $[x]$ sont appelés *norme*, *trace* et *polynôme caractéristique* de x de B sur A et notés respectivement

$$\mathrm{N}_{B/A}(x), \quad \mathrm{Tr}_{B/A}(x) \quad \text{et} \quad P_{B/A}(x;X).$$

On a donc, pour x et y dans B,

$$\mathrm{N}_{B/A}(xy) = \mathrm{N}_{B/A}(x)\mathrm{N}_{B/A}(y) \tag{4.1}$$

et

$$\mathrm{Tr}_{B/A}(x+y) = \mathrm{Tr}_{B/A}(x) + \mathrm{Tr}_{B/A}(y).$$

La trace $\mathrm{Tr}_{B/A}$ est un homomorphisme de A–modules de B dans A, tandis que la norme induit un homomorphisme du groupe $B^\times$ des unités de B dans le groupe $A^\times$ des unités de A.

On commence par utiliser ces notions quand A et B sont des corps, que l'on note K et L.

Lemme 4.2. *Soit L/K une extension séparable de degré n. Soit N une extension finie de L, normale sur K et soient $\sigma_1, \dots, \sigma_n$ les différents K-isomorphismes de L dans N. Alors pour $\alpha \in L$ on a*

$$\mathrm{Tr}_{L/K}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha), \quad \mathrm{N}_{L/K}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$$

et

$$P_{L/K}(\alpha;X) = \prod_{i=1}^{n} \big(X - \sigma_i(\alpha)\big).$$

Démonstration. Soit d le degré de α sur K et

$$P(X) = X^d + a_1 X^{d-1} + \cdots + a_d \in K[X]$$

son polynôme irréductible sur K. Supposons dans un premier temps que α est un élément primitif de l'extension L/K, c'est-à-dire que $L = K(\alpha)$ ou encore que $d = n$. Quand on prend $\{1, \alpha, \dots, \alpha^{d-1}\}$ comme base de L sur K, la matrice associée à l'endomorphisme $[\alpha]$ est

$$M_\alpha = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_d \\ 1 & 0 & \cdots & 0 & -a_{d-1} \\ 0 & 1 & \cdots & 0 & -a_{d-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_1 \end{pmatrix}.$$

Par conséquent le polynôme caractéristique de $[\alpha]$ est le polynôme irréductible de α sur K. Le fait qu'il s'écrive

$$\prod_{i=1}^{d} \big(X - \sigma_i(\alpha)\big)$$

provient du Théorème 2.19.

Dans le cas général on note $d = [K(\alpha) : K]$ et $m = [L : K(\alpha)]$, de sorte que $n = md$ et on prend une base $(e_1, \ldots, e_m)$ de L sur $K(\alpha)$. Dans la base $\{e_i\alpha^j \, ; 1 \le i \le m, \ 0 \le j < d\}$ de L sur K que l'on ordonne par

$$\big(e_1, e_1\alpha, \ldots, e_1\alpha^{d-1}, e_2, e_2\alpha, \ldots, e_2\alpha^{d-1}, \ldots, e_m, e_m\alpha, \ldots, e_m\alpha^{d-1}\big),$$

la matrice de $[\alpha]$ s'écrit comme un bloc diagonal $\mathrm{diag}\big(M_\alpha, \ldots, M_\alpha\big)$. Donc

$$P_{L/K}(\alpha; X) = P(X)^m,$$

$$\mathrm{Tr}_{L/K}(\alpha) = m\mathrm{Tr}_{K(\alpha)/K}(\alpha), \qquad \mathrm{N}_{L/K}(\alpha) = \big(\mathrm{N}_{K(\alpha)/K}(\alpha)\big)^m.$$

Enfin la suite $(\sigma_1(\alpha), \ldots, \sigma_n(\alpha))$ est formée des d conjugués de α sur K, chacun étant répété m fois. □

Lemme 4.3. *Soit L/K une extension finie séparable. L'application*

$$\begin{array}{ccc} L \times L & \to & K \\ (x, y) & \mapsto & \mathrm{Tr}_{L/K}(xy) \end{array}$$

est une forme bilinéaire symétrique non dégénérée sur L.

Il en résulte que l'application qui à $x \in L$ associe $y \mapsto \mathrm{Tr}_{L/K}(xy)$ est un isomorphisme du K-espace vectoriel L sur son dual $\mathrm{Hom}_K(L, K)$.

Démonstration du lemme 4.3. Que ce soit une forme bilinéaire symétrique est clair. Dire qu'elle est non dégénérée signifie que si $x \in L$ est tel que $\mathrm{Tr}_{L/K}(xy) = 0$ pour tout $y \in L$, alors $x = 0$. Cela résulte du lemme 4.4 suivant. □

Lemme 4.4 (Lemme de Dedekind sur l'indépendance linéaire des caractères)**.** *Soient G un groupe, k un corps, $\sigma_1, \ldots, \sigma_n$ des homomorphisms deux-à-deux distincts de G dans le groupe multiplicatif $k^\times$. Alors $\sigma_1, \ldots, \sigma_n$ sont linéairement indépendants sur k dans l'espace vectoriel k^G.*

Démonstration. On démontre le résultat par récurrence sur n. Pour $n = 1$ il est trivial. Supposons $n \ge 2$. Soient $a_1, \ldots, a_n$ des éléments de k tels que

$$\sum_{i=1}^{n} a_i\sigma_i(x) = 0 \quad \text{pour tout } x \in G.$$

Alors pour tout $x \in G$ et tout $y \in G$ on a

$$\sum_{i=1}^{n} a_i\sigma_i(x)\sigma_i(y) = 0.$$

Comme $\sigma_n \ne \sigma_1$ il existe $y \in G$ tel que $\sigma_n(y) \ne \sigma_1(y)$. En utilisant la relation

$$\sum_{i=2}^{n} a_i\big(\sigma_i(y) - \sigma_1(y)\big)\sigma_i(x) = 0$$

avec l'hypothèse de récurrence, on en déduit $a_n = 0$, puis $a_1 = \ldots = a_n = 0$. □

Remarque. Sous l'hypothèse supplémentaire que la caractéristique de K est soit nulle, soit première avec $[L : K]$, le fait que la forme bilinéaire $(x, y) \mapsto \mathrm{Tr}_{L/K}(xy)$ soit non dégénérée se déduit aussi de la relation

$$\mathrm{Tr}_{L/K}(\alpha^n) + a_1\mathrm{Tr}_{L/K}(\alpha^{n-1}) + \cdots + a_{n-1}\mathrm{Tr}_{L/K}(\alpha) + a_n[L : K] = 0$$

quand le polynôme irréductible de α sur K est $X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n \in K[X]$: comme $a_n \neq 0$, l'un des nombres $\mathrm{Tr}_{L/K}(\alpha^i)$, $(1 \leq i \leq n)$ n'est pas nul.

Définition. Soient $A \subset B$ deux anneaux. On suppose que B est un A-module libre de rang n. On définit une application $D_{B/A} : B^n \to A$ appelée *discriminant de B sur A* par

$$D_{B/A}(x_1, \ldots, x_n) = \det\big(\mathrm{Tr}_{B/A}(x_ix_j)\big)_{1\leq i,j\leq n}.$$

Exemple. Prenons pour$A$ l'anneau $F[T]$ des polynômes en une variable sur un corps F et pour B l'anneau $A[\sqrt{T}]$. Ainsi B est un A–module libre de rang 2, une base étant $\{1, \sqrt{T}\}$. La trace $\mathrm{Tr}_{B/A}$ de 1 est 2, celle de T est $2T$ (en général $\mathrm{Tr}_{B/A}(a) = 2a$ pour $a \in A$) et la trace de $\sqrt{T}$ est 0 (le polynôme $X^2 - T$ a pour racines $\sqrt{T}$ et $-\sqrt{T}$ dont la somme est nulle). Donc $D_{B/A}(1, \sqrt{T}) = 4T$. Noter que si F est de caractéristique 2 alors l'application $D_{B/A}$ est nulle.

Une variante de cet exemple consiste à prendre pour A un corps K et pour B le corps $K(\sqrt{d})$, où d est un élément de K qui n'est pas un carré : le discriminant $D_{B/A}(1, \sqrt{d})$ vaut $4d$.

Lemme 4.5. *Soient $\mathsf{A} = \big(a_{ij}\big)_{1\leq i,j\leq n}$ une matrice $n \times n$ à coefficients dans A. On pose*

$$y_j = \sum_{i=1}^{n} a_{ij}x_i, \quad (1 \leq j \leq n).$$

Alors

$$D_{B/A}(y_1, \ldots, y_n) = (\det \mathsf{A})^2 D_{B/A}(x_1, \ldots, x_n)$$

Démonstration. Cela résulte du fait que l'application $(x, y) \mapsto \mathrm{Tr}_{B/A}(xy)$ est bilinéaire. □

Donc si $x_1, \ldots, x_n$ sont linéairement dépendants sur A, alors $D_{B/A}(x_1, \ldots, x_n) = 0$ (on a supposé A intègre).

Si $\{x_1, \ldots, x_n\}$ et $\{y_1, \ldots, y_n\}$ sont deux bases de B comme A-module, alors la matrice de passage A est inversible, donc $\det \mathsf{A}$ est une unité de A. En particulier l'idéal principal de A engendré par le discriminant $D_{B/A}(x_1, \ldots, x_n)$ d'une base ne dépend pas de la base $\{x_1, \ldots, x_n\}$: on le note $\mathcal{D}_{B/A}$ et on l'appelle *idéal discriminant de B sur A*.

Si $A = \mathbf{Z}$ le déterminant $\det \mathsf{A}$ d'une matrice de passage entre deux bases de B sur $\mathbf{Z}$ est ± 1, donc son carré est $+1$ et le discriminant $D_{B/\mathbf{Z}}(x_1, \ldots, x_n)$ d'une base de B sur $\mathbf{Z}$ ne dépend pas de la base $\{x_1, \ldots, x_n\}$. C'est le *discriminant absolu* de B, que l'on note $\mathcal{D}_B$.

Lemme 4.6. *Soient $A \subset B$ deux anneaux ; on suppose que B est un A-module libre de rang n et que l'idéal $\mathcal{D}_{B/A}$ n'est pas l'idéal $\{0\}$. Soit $(x_1, \ldots, x_n) \in B^n$. Alors $D_{B/A}(x_1, \ldots, x_n)$ engendre l'idéal $\mathcal{D}_{B/A}$ si et seulement si $\{x_1, \ldots, x_n\}$ est une base de B comme A-module.*

L'hypothèse que l'idéal $\mathcal{D}_{B/A}$ n'est pas l'idéal $\{0\}$ est évidemment nécessaire, et nous avons vu un exemple où elle n'est pas satisfaite.

Démonstration. Par définition de l'idéal discriminant $\mathcal{D}_{B/A}$, si $\{x_1,\dots,x_n\}$ est une base de B comme A-module, alors $D_{B/A}(x_1,\dots,x_n)$ est un générateur de l'idéal $\mathcal{D}_{B/A}$

Inversement supposons que $D_{B/A}(x_1,\dots,x_n)$ engendre l'idéal $\mathcal{D}_{B/A}$. Soit $\{e_1,\dots,e_n\}$ une base de B sur A. On écrit $x_i=\sum_{j=1}^n a_{ij}e_j$ $(1\le i\le n)$ et on note $d_x=D_{B/A}(x_1,\dots,x_n)$, $d_e=D_{B/A}(e_1,\dots,e_n)$ et $a=\det(a_{ij})$. D'après le lemme 4.5 on a $d_x=a^2d_e$. Par hypothèse d_x et d_e engendrent le même idéal $\mathcal{D}_{B/A}$. Donc $d_x=ud_e$ avec $u\in A^\times$. Alors $(a^2-u)d_e=0$. Comme l'idéal principal $\mathcal{D}_{B/A}$ contient un élément non nul et que A est intègre, il en résulte que a^2 est inversible, donc que a est aussi une unité de A, donc la matrice (a_{ij}) est inversible, son inverse étant une matrice à coefficients dans A et par conséquent $\{x_1,\dots,x_n\}$ est une base de B sur A.

□

Proposition 4.7. *Soit L/K une extension séparable de degré n, soit N une extension finie de L, normale sur K , $x_1,\dots,x_n$ des éléments de L et soient $\sigma_1,\dots,\sigma_n$ les différents K-isomorphismes de L dans N. Alors*

$$D_{L/K}(x_1,\dots,x_n)=\Big(\det\big(\sigma_h(x_j)\big)_{1\le h,j\le n}\Big)^2.$$

De plus $(x_1,\dots,x_n)$ est une base de L sur K si et seulement si

$$D_{L/K}(x_1,\dots,x_n)\ne 0.$$

Démonstration. On utilise le lemme 4.2 :

$$\mathrm{Tr}_{L/K}(x_ix_j)=\sum_{h=1}^n\sigma_h(x_i)\sigma_h(x_j).$$

Donc

$$D_{L/K}(x_1,\dots,x_n)=\det\big(\mathrm{Tr}_{L/K}(x_ix_j)\big)=\det\big(\sigma_h(x_i)\big)\det\big(\sigma_h(x_j)\big)=\big(\det(\sigma_h(x_j)\big)^2.$$

Pour compléter la démonstration il reste à voir que la matrice $\big(\sigma_h(x_j)\big)$ est régulière. Si $b_1,\dots,b_n$ sont des éléments de N tels que $b_1\sigma_1(x_j)+\cdots+b_n\sigma_n(x_j)=0$ pour $1\le j\le n$, alors $b_1\sigma_1(x)+\cdots+b_n\sigma_n(x)=0$ pour tout $x\in B$ et d'après le lemme 4.4 il en résulte $b_1=\cdots=b_n=0$. □

Soit P un polynôme non nul à coefficients dans un corps K et soit E une extension de K dans laquelle P est complètement décomposé :

$$P(X)=a_0\prod_{i=1}^n(X-x_i),$$

où n est le degré de P, a_0 son coefficient directeur et $x_i\in E$. Nous avons déjà défini le *discriminant de P* par

$$D(P)=a_0^{n(n-1)}\prod_{1\le i<j\le n}(x_i-x_j)^2=(-1)^{n(n-1)/2}a_0^{n(n-1)}\prod_{\substack{1\le i,j\le n,\\ i\ne j}}(x_i-x_j).$$

De la définition on déduit $D(P)=0$ si et seulement si P a au moins une racine multiple. La théorie de Galois § 2.8 montre que $D(P)$ est un élément de K. De la proposition 4.7, on déduit que si $P\in K[X]$ est un polynôme unitaire irréductible de degré n et si $L=K(\alpha)$ est un corps de rupture de P sur K, avec $P(\alpha)=0$, alors

$$D(P)=D_{L/K}(1,\alpha,\dots,\alpha^{n-1}).$$

Exercice. Vérifier que le discriminant du polynôme $aX^2 + bX + c$ est $b^2 - 4ac$ et que celui de $X^3 + pX + q$ est $-4p^3 - 27q^2$.

4.2 Entiers algébriques

Proposition 4.8. *Soient A un anneau intègre, K un corps contenant A et $\alpha \in K$. Les propriétés suivantes sont équivalentes :*
(i) α est racine d'un polynôme unitaire à coefficients dans A.
(ii) Le sous-anneau $A[\alpha]$ de K engendré par α sur A est un A-module de type fini.
(iii) $A[\alpha]$ est contenu dans un sous-anneau de K qui est de type fini comme A-module.

Démonstration. Supposons la propriété *(i)* vérifiée ; soit

$$X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n \in A[X]$$

un polynôme unitaire à coefficients dans A ayant α comme racine. De la relation

$$\alpha^n = -a_1\alpha^{n-1} - \cdots - a_{n-1}\alpha - a_n$$

on déduit par récurrence sur m

$$\alpha^m \in A + A\alpha + \cdots + A\alpha^{n-1} \quad \text{pour tout } m \geq 1,$$

donc $A[\alpha] = A + A\alpha + \cdots + A\alpha^{n-1}$ et par conséquent l'anneau $A[\alpha]$ est un A-module de type fini.

L'implication *(ii)*⇒*(iii)* est triviale.

Supposons la propriété *(iii)* vérifiée. Soit B un sous anneau de K contenant $A[\alpha]$. On suppose que B est un A-module de type fini et on écrit $B = Ax_1 + \cdots + Ax_m$. Pour $1 \leq i \leq m$ le fait que αx_i appartienne à B entraîne qu'il existe des éléments a_{ij} de A $(1 \leq j \leq m)$ tels que

$$\alpha x_i = \sum_{j=1}^{m} a_{ij}x_j.$$

Posons $M = \big(a_{ij}\big)_{1\leq i,j\leq m}$ et soit I la matrice identité $m \times m$. La matrice $\alpha I - M$ est associée à un endomorphisme de K^m dont le noyau contient $(x_1, \ldots, x_m)$. Soit $P \in A[X]$ le déterminant de la matrice $XI - M$. Alors P est un polynôme unitaire qui admet α comme racine. D'où *(i)*.

□

Définition. On dit que $\alpha \in K$ est *entier sur A* s'il vérifie les propriétés équivalentes de la proposition 4.8.

Par exemple si A est un corps k et donc K une extension de k, un élément de K est entier sur k si et seulement s'il est algébrique sur k.

Corollaire 4.9. *L'ensemble des éléments de K entiers sur A est un sous-anneau de K.*

Démonstration. Si α et β sont des éléments de K entiers sur A, alors l'anneau $A[\alpha, \beta]$ est un sous-A-module de type fini de K (un système générateur fini est formé d'éléments $\alpha^i\beta^j$), donc tous ses éléments sont entiers sur A.

□

Définition. L'ensemble des éléments de K qui sont entiers sur A est appelé la *fermeture intégrale de A dans K.*

De la proposition 4.8 on déduit que la relation d'intégralité est transitive :

Corollaire 4.10. *Soient K un corps, A un sous-anneau de K, A_0 la fermeture intégrale de A dans K et B un sous-anneau de A_0 contenant A. Alors la fermeture intégrale de B dans K est A_0.*

Démonstration. Soit B_0 la fermeture intégrale de B dans K. Un élément de A_0 est entier sur A, donc sur B, et par conséquent appartient à B_0. Ainsi $A_0 \subset B_0$. Pour voir l'inclusion dans l'autre sens, on considère un élément x de B_0, il est entier sur B, donc racine d'un polynôme unitaire à coefficients dans B. Soient $b_1, \ldots, b_m$ les coefficients de ce polynôme ; le sous–anneau $A[b_1, \ldots, b_m]$ de B est un A–module de type fini, il en est de même de $A[b_1, \ldots, b_m, x]$, donc par la proposition 4.8 on en déduit que x est entier sur A, ce qui montre $B_0 \subset A_0$. □

Définition. La *clôture intégrale* d'un anneau est la fermeture intégrale de cet anneau dans son corps des fractions.

La clôture intégrale de A est un anneau qui contient A et qui est contenu dans la fermeture intégrale de A dans K, pour tout corps K contenant A.

Définition. Un anneau est dit *intégralement clos* s'il est égal à sa clôture intégrale.

Un anneau factoriel est intégralement clos : en effet, si A est un anneau factoriel de corps des fractions K et si $\alpha \in K$ est racine d'un polynôme unitaire à coefficients dans A :

$$\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0,$$

on écrit $\alpha = p/q$ avec p et q dans A sans facteurs irréductibles communs et de la relation

$$p^n + a_1 p^{n-1} q + \cdots + a_n q^n = 0$$

on déduit que q divise p, donc que q est inversible et $\alpha \in A$.

En particulier un anneau principal est intégralement clos. On en déduit par exemple qu'un nombre rationnel qui est entier sur $\mathbf{Z}$ est dans $\mathbf{Z}$.

L'anneau $\mathbf{Z}[2i] = \mathbf{Z} + 2i\mathbf{Z}$ n'est pas intégralement clos, puisque son corps des fractions $\mathbf{Q}(i)$ contient i, qui est racine du polynôme $X^2 + 1$, donc est entier sur $\mathbf{Z}[2i]$, mais n'appartient pas à $\mathbf{Z}[2i]$.

Définition. On appelle *nombre algébrique* tout nombre complexe qui est algébrique sur $\mathbf{Q}$ et *entier algébrique* tout nombre complexe qui est entier sur $\mathbf{Z}$.

Si α est un nombre algébrique, dont le polynôme irréductible sur $\mathbf{Q}$ est

$$X^n + a_1 X^{n-1} + \cdots + a_n \in \mathbf{Q}[X],$$

l'unique polynôme irréductible de $\mathbf{Z}[X]$ qui s'annule au point α et dont le coefficient directeur soit positif est

$$dX^n + da_1 X^{n-1} + \cdots + da_n \in \mathbf{Z}[X], \tag{4.11}$$

où d est le plus petit commun multiple des dénominateurs des nombres $a_1, \ldots, a_n$. Nous appellerons ce polynôme (4.11) le *polynôme minimal de α sur $\mathbf{Z}$.*

Si α est un entier algébrique, alors les valeurs propres de $[\alpha]$ sont des entiers algébriques, donc le polynôme caractéristique de α sur $\mathbf{Z}$ est à coefficients dans $\mathbf{Z}$; en particulier $\mathrm{N}_{K/\mathbf{Q}}(\alpha)$ et $\mathrm{Tr}_{K/\mathbf{Q}}(\alpha)$ sont dans $\mathbf{Z}$.

Le lemme de Gauss 2.24 montre que pour un nombre algébrique α les conditions suivantes sont équivalentes :
(i) α est entier (sur $\mathbf{Z}$)
(ii) Le polynôme minimal de α sur $\mathbf{Z}$ est unitaire.
(iii) Le polynôme irréductible de α sur $\mathbf{Q}$ a ses coefficients dans $\mathbf{Z}$.
(iv) Le polynôme minimal de α sur $\mathbf{Z}$ coïncide avec son polynôme irréductible sur $\mathbf{Q}$.

Quand on parle du polynôme irréductible ou du polynôme minimal d'un nombre algébrique, on omet souvent de préciser "sur $\mathbf{Q}$" et "sur $\mathbf{Z}$" respectivement.

Le corollaire 4.9 montre que les entiers algébriques forment un sous-anneau de $\mathbf{C}$, dont le corps des fractions est le corps $\overline{\mathbf{Q}}$ des nombres algébriques. Si α est un nombre algébrique, l'ensemble des entiers $d \in \mathbf{Z}$ tels que $d\alpha$ soit entier algébrique est un idéal non nul de $\mathbf{Z}$: il contient le coefficient directeur du polynôme minimal de α sur $\mathbf{Z}$.

Rappelons qu'on appelle *corps de nombres* une extension finie de $\mathbf{Q}$. D'après le théorème de l'élément primitif 2.21, un corps de nombres est un sous-corps de $\mathbf{C}$ de la forme $\mathbf{Q}(\alpha)$ avec α nombre algébrique. Le *degré* d'un corps de nombres est son degré sur $\mathbf{Q}$. Un *corps quadratique* est une extension de $\mathbf{Q}$ de degré 2, un *corps cubique* une extension de $\mathbf{Q}$ de degré 3, un corps *biquadratique* une extension de degré 4...

L'*anneau des entiers* d'un corps de nombres K est l'intersection de K avec l'anneau des entiers algébriques. On le notera $\mathbf{Z}_K$. Le corps des fractions de $\mathbf{Z}_K$ est K. Le Corollaire 4.10 montre que $\mathbf{Z}_K$ est un anneau intégralement clos.

Les éléments inversibles (*unités*) de l'anneau $\mathbf{Z}_K$ forment un groupe multiplicatif $\mathbf{Z}_K^\times$; ce sont les éléments de $\mathbf{Z}_K$ de norme ± 1.

Quand K est un corps de nombres, on utilise des expressions comme "unités de K", "idéaux de K", "discriminant de K" pour parler des unités, des idéaux ou du discriminant de l'anneau des entiers de K.

Définition. Soit α un nombre algébrique. On appelle *norme absolue* de α (resp. *trace absolue* de α) la norme (resp. la trace) $\mathrm{N}_{\mathbf{Q}(\alpha)/\mathbf{Q}}(\alpha)$ (resp. $\mathrm{Tr}_{\mathbf{Q}(\alpha)/\mathbf{Q}}(\alpha)$). On les note respectivement $\mathrm{N}(\alpha)$ et $\mathrm{Tr}(\alpha)$.

Du lemme 4.2 on déduit que si α est un nombre algébrique dont le polynôme irréductible sur $\mathbf{Q}$ est

$$P(X) = X^d + a_1 X^{d-1} + \cdots + a_d \in \mathbf{Q}[X],$$

alors

$$\mathrm{N}(\alpha) = (-1)^d a_d \quad \text{et} \quad \mathrm{Tr}(\alpha) = -a_1.$$

Plus généralement, si K est un corps de nombres de degré n sur $\mathbf{Q}$, α un élément de K, d le degré de α sur $\mathbf{Q}$ et $\alpha_1, \ldots, \alpha_d$ les conjugués de α dans $\mathbf{C}$, alors

$$\mathrm{N}_{K/\mathbf{Q}}(\alpha) = (\alpha_1 \cdots \alpha_d)^{n/d} \quad \text{et} \quad \mathrm{Tr}_{K/\mathbf{Q}}(\alpha) = \frac{n}{d}(\alpha_1 + \cdots + \alpha_d).$$

Soit k un corps quadratique. Il existe un entier $d \in \mathbf{Z}$ sans facteur carré tel que $k = \mathbf{Q}(\sqrt{d})$. Soit α un élément de k, alors α est racine du polynôme $X^2 - X\mathrm{Tr}_{k/\mathbf{Q}}(\alpha) + \mathrm{N}_{k/\mathbf{Q}}(\alpha)$, donc α est entier si et seulement si $\mathrm{Tr}_{k/\mathbf{Q}}(\alpha)$ et $\mathrm{N}_{k/\mathbf{Q}}(\alpha)$ sont dans $\mathbf{Z}$.

Soit $\alpha = x + y\sqrt{d} \in k$, avec x et y dans $\mathbf{Q}$. On a $\mathrm{Tr}_{k/\mathbf{Q}}(\alpha) = 2x$ et $\mathrm{N}_{k/\mathbf{Q}}(\alpha) = x^2 - dy^2$. Si α est entier, alors les nombres $a = 2x$ et $b = x^2 - dy^2$ sont dans $\mathbf{Z}$. Comme d n'est pas divisible par 4, le nombre $c = 2y$ est aussi dans $\mathbf{Z}$. Alors de la relation $a^2 - dc^2 = 4b$ on déduit que soit a et c sont pairs, soit a et c sont impairs et dans ce dernier cas $d \equiv 1 \pmod 4$. Par conséquent l'anneau $\mathbf{Z}_k$ des entiers de k est

$$\mathbf{Z}_k = \begin{cases} \mathbf{Z} + \mathbf{Z}\sqrt{d} & \text{si } d \equiv 2 \text{ ou } 3 \pmod 4 \\ \mathbf{Z} + \mathbf{Z}\dfrac{1+\sqrt{d}}{2} & \text{si } d \equiv 1 \pmod 4. \end{cases}$$

Ainsi $\mathbf{Z}_k = \mathbf{Z} + \mathbf{Z}\alpha$ où α est une des deux racines du polynôme $X^2 - d$ si $d \equiv 2$ ou $3 \pmod 4$, et l'une des deux racines du polynôme $X^2 - X - (d-1)/2$ si $d \equiv 1 \pmod 4$.

Le discriminant D_k de k est le discriminant $D_{\mathbf{Z}_k}$ de l'anneau des entiers de k :

$$D_k = \begin{cases} \det \begin{vmatrix} 2 & 0 \\ 0 & 2d \end{vmatrix} = 4d & \text{si } d \equiv 2 \text{ ou } 3 \pmod 4 \\ \det \begin{vmatrix} 2 & 1 \\ 1 & (1+d)/2 \end{vmatrix} = d & \text{si } d \equiv 1 \pmod 4. \end{cases}$$

Ainsi le discriminant est toujours congru à 0 ou 1 modulo 4 et le corps quadratique s'écrit aussi $k = \mathbf{Q}(\sqrt{D_k})$.

Le groupe des racines de l'unités d'un corps de nombres quadratique k est $\{1, i, -1, -i\}$ si k a pour discriminant -4 — c'est-à-dire $k = \mathbf{Q}(i)$—, c'est $\{1, \varrho, \varrho^2, -1, -\varrho, -\varrho^2\}$ si k a pour discriminant -3, où ϱ est une racine primitive cubique de l'unité (c'est-à-dire pour $k = \mathbf{Q}(\sqrt{-3})$) enfin les seules racines de l'unité dans $\mathbf{Z}_k$ sont $\{\pm 1\}$ sinon.

Quand d est négatif, il est facile de vérifier que le groupe des unités du corps $k = \mathbf{Q}(\sqrt{d})$ est fini : il est composé des racines de l'unité. Nous verrons au § 4.4 que pour $d > 0$ le groupe $\mathbf{Z}_k^\times$ des unités de $\mathbf{Z}_k$ est un $\mathbf{Z}$-module de rang 1.

Proposition 4.12. *Soit K un corps de nombres de degré n. Alors l'anneau des entiers $\mathbf{Z}_K$ de K est un $\mathbf{Z}$-module libre de rang n.*

Démonstration. La conclusion signifie qu'il existe n éléments $e_1, \ldots, e_n$ de $\mathbf{Z}_K$, linéairement indépendants sur $\mathbf{Q}$, tels que

$$\mathbf{Z}_K = \mathbf{Z}e_1 + \cdots + \mathbf{Z}e_n.$$

Soit $f_1, \ldots, f_n$ une base de K sur $\mathbf{Q}$ formée d'éléments de $\mathbf{Z}_K$ (partant d'une base quelconque il suffit de multiplier par un dénominateur pour obtenir une telle base).

La forme bilinéaire $(x, y) \mapsto \mathrm{Tr}_{K/\mathbf{Q}}(xy)$ étant non dégénérée (lemme 4.2), il existe une base $f_1^*, \ldots, f_n^*$ de K sur $\mathbf{Q}$ telle que $\mathrm{Tr}_{K/\mathbf{Q}}(f_i f_j^*) = \delta_{ij}$ (symbole de Kronecker). Soit $a \in \mathbf{Z}$, $a > 0$ tel que af_j^* soit entier algébrique pour $1 \leq j \leq d$.

Pour $x \in K$ on écrit

$$x = x_1 f_1 + \cdots + x_d f_d$$

avec $x_1, \dots, x_d$ dans $\mathbf{Q}$ et on a $\mathrm{Tr}_{K/\mathbf{Q}}(xf_j^*) = x_j$. Maintenant si $x \in \mathbf{Z}_K$ on a $xaf_j^* \in \mathbf{Z}_K$, donc $\mathrm{Tr}_{K/\mathbf{Q}}(xaf_j^*) = ax_j \in \mathbf{Z}$. On en déduit que l'indice du sous–groupe $\mathbf{Z}f_1 + \cdots + \mathbf{Z}f_d$ dans $\mathbf{Z}_K$ divise a. Par conséquent pour tout $x \in \mathbf{Z}_K$ on a

$$ax \in \mathbf{Z}f_1 + \cdots + \mathbf{Z}f_d,$$

ce qui donne

$$\mathbf{Z}f_1 + \cdots + \mathbf{Z}f_d \subset \mathbf{Z}_K \subset \frac{1}{a}\big(\mathbf{Z}f_1 + \cdots + \mathbf{Z}f_d\big).$$

Pour conclure on utilise alors les résultats du § 4.3 suivant sur la structure des modules sur un anneau principal (proposition 4.14).

□

Il résulte de la Proposition 4.12 que tout idéal de $\mathbf{Z}_K$ est un $\mathbf{Z}$–module libre de rang n. Une base de $\mathbf{Z}_K$ comme $\mathbf{Z}$–module est *une base d'entiers de* K, son discriminant ne dépend pas de la base, c'est le *discriminant du corps de nombres* K.

Soient k un corps de nombres et n son degré. D'après le théorème de l'élément primitif 2.21, il existe $\alpha \in k$ tel que $k = \mathbf{Q}(\alpha)$. On décompose le polynôme irréductible $P \in \mathbf{Q}[X]$ de α dans $\mathbf{R}[X]$: soient r_1 le nombre de facteurs irréductibles de degré 1 et r_2 le nombre de facteurs irréductibles de degré 2. Ainsi $r_1 + 2r_2 = n$. Notons $\alpha_1, \dots, \alpha_{r_1}$ les racines réelles de P :

$$P(X) = \prod_{i=1}^{r_1}(X - \alpha_j) \prod_{j=r_1+1}^{r_1+r_2} (X^2 + b_jX + c_j).$$

Pour $r_1 + 1 \le j \le r_1 + r_2$ le polynôme $X^2 + b_jX + c_j$ a deux racines complexes conjuguées, que l'on note α_j et $\alpha_{r_2+j} = \overline{\alpha}_j$. Ainsi la décomposition de P en facteurs irréductibles dans $\mathbf{C}$ est

$$P(X) = \prod_{i=1}^{n}(X - \alpha_j).$$

Il y a n $\mathbf{Q}$-isomorphismes $\sigma_1, \dots, \sigma_n$ de k dans $\mathbf{C}$, qui sont déterminés respectivement par

$$\sigma_j(\alpha) = \alpha_j \quad (1 \le j \le n).$$

On dit que ce sont des *plongements* de k dans $\mathbf{C}$. Pour $1 \le j \le r_1$ l'image $\sigma_j(k)$ de k par σ_j est dans $\mathbf{R}$, tandis que σ_{r_1+j} et $\sigma_{r_1+r_2+j}$ sont complexes conjugués pour $1 \le j \le r_2$. Si τ désigne la conjugaison complexe, qui est un automorphisme involutif ($\tau^2 = 1$) du corps $\mathbf{C}$, on a

$$\tau \circ \sigma_j = \sigma_j \circ \tau = \sigma_j \text{ pour } 1 \le j \le r_1 \text{ et } \tau \circ \sigma_{r_1+j} = \sigma_{r_1+j} \circ \tau = \sigma_{r_1+r_2+j} \text{ pour } 1 \le j \le r_2.$$

On note encore $\overline{\sigma_{r_1+j}} = \tau \circ \sigma_{r_1+j}$.

L'ensemble $\{\sigma_1, \dots, \sigma_{r_1}\}$ des plongements réels et celui $\{\sigma_{r_1+1}, \dots, \sigma_{r_1+2r_2}\}$ des plongements non réels ne dépendent pas du choix de l'élément primitif α. Le *plongement canonique* de k est l'application $\mathbf{Q}$-linéaire injective $\underline{\sigma} : k \to \mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$ définie par

$$\underline{\sigma}(x) = \big(\sigma_1(x), \dots, \sigma_{r_1+r_2}(x)\big).$$

Le seul choix qui ne soit pas intrinsèque est celui entre un plongement non réel et son conjugué. On identifie $\mathbf{C}$ à $\mathbf{R}^2$ par $z = \Re e(z) + i\Im m(z)$ et on note encore $\underline{\sigma}$ l'application $\mathbf{Q}$-linéaire de k dans $\mathbf{R}^n$ qui envoie $x \in k$ sur

$$\Big(\sigma_1(x), \dots, \sigma_{r_1}(x), \Re e\big(\sigma_{r_1+1}(x)\big), \Im m\big(\sigma_{r_1+1}(x)\big), \dots, \Re e\big(\sigma_{r_1+r_2}(x)\big), \Im m\big(\sigma_{r_1+r_2}(x)\big)\Big).$$

Le couple (r_1, r_2) est la *signature* du corps de nombres k. Le degré de k est alors $r_1 + 2r_2$.

Lemme 4.13. *Le signe du discriminant absolu d'un corps de nombres k de signature (r_1, r_2) est $(-1)^{r_2}$.*

Démonstration. . Dans le développement du déterminant de la matrice des $\sigma_i(\alpha_j)$ (cf. proposition 4.7), les nombres réels ont des carrés positifs, les nombres imaginaires purs ont des carrés négatifs et il y en a r_2. Voir [2], Prop. 4.8.11. □

Exercice. Soit T un polynôme unitaire irréductible de degré n de $\mathbf{Z}[X]$ et $K = \mathbf{Q}(\theta)$. On désigne par $D(T)$ le discriminant de T et par D_K celui du corps de nombres K.
a) Montrer que le discriminant de $1, \theta, \dots, \theta^{n-1}$ est $D(T)$.
b) Soit f l'indice de $\mathbf{Z}[\theta]$ dans $\mathbf{Z}_K$. Vérifier $D(T) = D_K f^2$.
`Référence` : [2], § 4.4.

Une famille $(\alpha_1, \dots, \alpha_n)$ de n éléments dans un corps de nombres de degré n est une base d'entiers de K si et seulement si les deux conditions suivantes sont satisfaites :
(i) Les α_i sont entiers
(ii) Le discriminant $D(\alpha_1, \dots, \alpha_n)$ est égal au discriminant de K.

Exercice. Montrer que le discriminant d'un corps de nombres est congru à 0 ou 1 modulo 4
`Indication` : en utilisant la proposition 4.7 développer le déterminant de la matrice des $\sigma_i(\alpha_j)$ et regrouper les termes de signature paire et ceux de signature impaire pour écrire le discriminant sous la forme $(P-N)^2 = (P+N)^2 - 4PN$ et vérifier que $P+N$ et PN sont des entiers.
On suppose que T est un polynôme unitaire irréductible dans $\mathbf{Z}[X]$ de discriminant D qui est

- soit sans facteur carré et congru à 1 modulo 4,
- soit de la forme $4d$ avec d sans facteur carré et congru à 1 modulo 4.

Soit θ une racine de T dans une extension de $\mathbf{Q}$. En déduire que $(1, \theta, \dots, \theta^{n-1})$ est une base d'entiers de $\mathbf{Q}(\theta)$.

4.3 Structure des modules sur les anneaux principaux

Dans la démonstration de la Proposition 4.12, nous avons utilisé un théorème sur la structure des sous-modules d'un module libre de type fini sur un anneau principal. En voici l'énoncé.

Quand A est un anneau (intègre, rappelons-le) et M un A-module, on a déjà défini le *rang de M* comme le nombre maximal ($\leq \infty$) d'éléments de M linéairement indépendants sur A. Quand A est de type fini, le rang r de A est fini, majoré par le nombre minimal de générateurs de A. Par exemple $(\mathbf{Z}/2\mathbf{Z})^s \times \mathbf{Z}^r$ est de rang r, le nombre minimal de générateurs est $r+s$. D'autre part le rang de $\mathbf{Q}$ sur $\mathbf{Z}$ est 1, mais $\mathbf{Q}$ n'est pas de type fini sur $\mathbf{Z}$

Si K est le corps des fractions de A, et si M est un A-module libre, il possède une base, et on peut plonger M dans un K-espace vectoriel V. Dans ce cas le rang de M est le nombre d'éléments d'une base de M comme A-module, et plus généralement le rang d'un sous-module N de M est la dimension du K-espace vectoriel engendré par N dans V.

Proposition 4.14. (Modules sur les anneaux principaux.) *Soit A un anneau principal, soit M un A-module libre de rang m et soit N un sous-A-module de M. Alors N est libre de rang $n \leq m$. De plus il existe une base $\{e_1, \dots, e_m\}$ de M comme A-module et des éléments $a_1, \dots, a_n$ de A tels que $\{a_1e_1, \dots, a_ne_n\}$ soit une base de N sur A et que a_i divise a_{i+1} dans A pour $1 \leq i < n$.*

Les idéaux $a_1A \supset a_2A \supset \cdots \supset a_nA$ de A sont appelés *facteurs invariants* du sous-A-module N de M : ils ne dépendent pas de la base $(a_1, \dots, e_n)$ de M vérifiant les conditions de la proposition 4.14.

Démonstration. Voir [12], § 1.5. □

En écrivant un module de type fini comme un quotient d'un module libre de type fini, on en déduit :

Corollaire 4.15. *Soient A un anneau principal et M un A–module de type fini. Il existe un entier n et des idéaux $a_1A \supset a_2A \supset \cdots \supset a_nA$ de A tels que A soit isomorphe au A–module produit direct $A/a_1A \times A/a_2A \times \cdots \times A/a_nA$.*

Par conséquent un A–module sans torsion est libre, isomorphe à A^n pour un entier $n \geq 0$.

4.4 Unités d'un corps de nombres

Une référence pour cette section est [12].

4.4.1 Énoncé du théorème de Dirichlet

Une *unité algébrique* est un élément inversible de l'anneau des entiers algébriques.

Lemme 4.16. *Pour un entier algébrique α d'un corps de nombres k, les conditions suivantes sont équivalentes*
(i) α est une unité algébrique.
(ii) $\mathrm{N}(\alpha) = \pm 1$.
(iii) $\mathrm{N}_{k/\mathbf{Q}}(\alpha) = \pm 1$.

Démonstration. .
L'équivalence entre (ii) et (iii) est banale, puisque $\mathrm{N}(\alpha) = \mathrm{N}_{\mathbf{Q}(\alpha)/\mathbf{Q}}(\alpha)$ et que

$$\mathrm{N}_{k/\mathbf{Q}}(\alpha) = \big(\mathrm{N}(\alpha)\big)^{[k:\mathbf{Q}(\alpha)]}.$$

Si α est une unité algébrique, d'inverse β, et si k est un corps de nombres contenant α, alors on a d'une part $\mathrm{N}_{k/\mathbf{Q}}(\alpha) \in \mathbf{Z}$ et $\mathrm{N}_{k/\mathbf{Q}}(\beta) \in \mathbf{Z}$ car α et β sont entiers algébriques, et d'autre part $\mathrm{N}_{k/\mathbf{Q}}(\alpha)\mathrm{N}_{k/\mathbf{Q}}(\beta) = \mathrm{N}_{k/\mathbf{Q}}(\alpha\beta) = 1$ car $\alpha\beta = 1$. Donc $\mathrm{N}_{k/\mathbf{Q}}(\alpha)$ est un élément inversible de $\mathbf{Z}$, ce qui montre $(i) \Rightarrow (ii)$.

Enfin si α est un entier algébrique de norme ± 1, son polynôme minimal sur $\mathbf{Z}$ s'écrit

$$X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n \in \mathbf{Z}[X]$$

avec $a_n = \pm 1$, et l'entier algébrique

$$\beta = -a_n(\alpha^{n-1} + a_1\alpha^{n-2} + \cdots + a_{n-1})$$

vérifie $\alpha\beta = a_n^2 = 1$, donc β est l'inverse de α.

□

Notons qu'il existe des *nombres* algébriques de norme ± 1 qui ne sont pas des unités algébriques : un exemple est

$$\frac{-1+i\sqrt{15}}{4}$$

qui est racine du polynôme $2X^2+X+2$.

La structure du groupe des unités $\mathbf{Z}_k^\times$ d'un corps de nombres k est donnée par le *Théorème de Dirichlet* :

Théorème 4.17 (Dirichlet)**.** *Soient k un corps de nombres, n son degré, r_1 le nombre de plongements réels de k et $2r_2$ le nombre de plongements complexes deux-à-deux conjugués complexes. Alors le groupe des unités $\mathbf{Z}_k^\times$ de k est un groupe de type fini et de rang $r = r_1 + r_2 - 1$.*

Exercice. Faire le lien entre le théorème de Dirichlet pour les corps quadratiques réels et l'équation de Pell étudiée au début du cours.

Dire que $\mathbf{Z}_k^\times$ est un groupe abélien de type fini et de rang r signifie que d'une part son groupe de torsion, qui est le groupe $k_{\rm tors}^\times$ des racines de l'unité contenues dans k, est fini, et d'autre part que le quotient $\mathbf{Z}_k/k_{\rm tors}^\times$ est isomorphe à $\mathbf{Z}^r$: il existe r unités $\epsilon_1,\dots,\epsilon_r$ dans $\mathbf{Z}_k^\times$, qui sont linéairement indépendantes dans $\mathbf{Z}_k^\times$ (on dit *multiplicativement indépendantes* puisque la loi est multiplicative), telles que toute unité de k s'écrive de manière unique

$$\zeta\epsilon_1^{a_1}\cdots\epsilon_r^{a_r}$$

avec ζ racine de l'unité et $a_i \in \mathbf{Z}$ $(1 \le i \le r)$. On dit que $(\epsilon_1,\dots,\epsilon_r)$ est un système fondamental d'unités de k si cette propriété est vérifiée, c'est-à-dire si les images de $\epsilon_1,\dots,\epsilon_r$ modulo torsion forment une base du groupe abélien libre $\mathbf{Z}_k^\times/k_{\rm tors}^\times$.

La démonstration du théorème 4.17 nécessite quelques préliminaires sur les sous-groupes de $\mathbf{R}^n$.

4.4.2 Sous-groupes de $\mathbf{R}^n$

Des exemples de sous-groupes de $\mathbf{R}$ sont d'une part

$$\{0\}, \quad \mathbf{Z} \quad \text{et plus généralement } \mathbf{Z}x \text{ pour } x \in \mathbf{R}$$

et d'autre part

$$\mathbf{Z}+\mathbf{Z}\sqrt{2}, \quad \mathbf{Q} \quad \text{et} \quad \mathbf{R}.$$

Les sous-groupes de la première liste sont discrets dans $\mathbf{R}$: un sous-groupe G de $\mathbf{R}^n$ est *discret* si pour tout compact K de $\mathbf{R}^n$, l'intersection $G \cap K$ est finie. Ceux de la deuxième liste sont denses.

On remarquera que l'adhérence d'un sous-groupe de $\mathbf{R}^n$ est encore un sous-groupe de $\mathbf{R}^n$.

Quand G_1 et G_2 sont deux sous-groupes de $\mathbf{R}^{n_1}$ et $\mathbf{R}^{n_2}$ respectivement, le produit $G_1 \times G_2$ est un sous-groupe de $\mathbf{R}^n$ avec $n = n_1 + n_2$.

Nous allons voir que, dans une certaine mesure, ces remarques permettent de décrire tous les sous-groupes de $\mathbf{R}^n$.

Nous commençons par décrire les sous-groupes discrets de $\mathbf{R}^n$.

Lemme 4.18. *Un sous-groupe G de $\mathbf{R}^n$ est discret dans $\mathbf{R}^n$ si et seulement s'il existe un ouvert U de $\mathbf{R}^n$ contenant 0 tel que $G \cap U$ soit discret.*

Démonstration. Si G est discret on peut prendre $U = \mathbf{R}^n$. Inversement, si G n'est pas discret, il existe un élément $z \in \mathbf{R}^n$ qui est un point d'accumulation d'éléments de G : pour tout $\epsilon > 0$ il existe $x \in G$ tel que $0 < |z - x| < \epsilon$ et il existe $y \in G$ tel que $0 < |z - y| < |z - x|$. Alors $0 < |x - y| < 2\epsilon$ et $x - y \in G$, ce qui montre que 0 est point d'accumulation de G.

□

Exercice. 1. Montrer qu'un sous-groupe non discret de $\mathbf{R}$ est partout dense.
2. En déduire la liste des sous-groupes fermés de $\mathbf{R}$.
3. Soit G un sous-groupe de type fini de $\mathbf{R}$. Donner une condition nécessaire et suffisante sur son rang pour que G soit dense dans $\mathbf{R}$.
4. Soit $\theta \in \mathbf{R}$. Donner une condition nécessaire et suffisante sur θ pour que le sous-groupe $\mathbf{Z} + \mathbf{Z}\theta$ soit dense dans $\mathbf{R}$.

Proposition 4.19. *Soit G un sous-groupe discret de $\mathbf{R}^n$. Il existe un entier t dans l'intervalle $0 \leq t \leq n$ et des éléments $e_1, \ldots, e_t$ de G, linéairement indépendants sur $\mathbf{R}$, tels que $G = \mathbf{Z}e_1 + \cdots + \mathbf{Z}e_t$.*

En particulier $e_1, \ldots, e_t$ sont linéairement indépendants sur $\mathbf{Z}$, donc G est libre de rang t. Le nombre t est la dimension du $\mathbf{R}$-sous–espace vectoriel de $\mathbf{R}^n$ engendré par G. La proposition 4.19 montre que dans un sous-groupe discret de $\mathbf{R}^n$, des éléments linéairement indépendants sur $\mathbf{Z}$ sont automatiquement linéairement indépendants sur $\mathbf{R}$.

Définition. Un sous-groupe discret de $\mathbf{R}^n$ de rang maximal n est appelé *réseau* (en anglais *lattice*) de $\mathbf{R}^n$.

Démonstration de la proposition 4.19. Soit $f_1, \ldots, f_t$ une partie de G libre sur $\mathbf{R}$ maximale. C'est une base du sous-espace vectoriel V de $\mathbf{R}^n$ engendré par G. De plus $G' = \mathbf{Z}f_1 + \cdots + \mathbf{Z}f_t$ est un sous-groupe de G. Montrons que G' est d'indice fini dans G.

Soit K un compact de $\mathbf{R}^n$ contenant

$$\{u_1 f_1 + \cdots + u_t f_t \ ; \ 0 \leq u_i < 1 \ (1 \leq i \leq t)\}.$$

Soit $x \in G$. Alors $x \in V$, donc on peut écrire $x = x_1 f_1 + \cdots + x_t f_t$ avec $x_i \in \mathbf{R}$. Soit $m_i = [x_i]$ la partie entière de x_i :

$$m_i \in \mathbf{Z}, \quad 0 \leq x_i - m_i < 1 \qquad (1 \leq i \leq n).$$

Posons $x' = m_1 f_1 + \cdots + m_t f_t$. Alors $x' \in G'$ et $x - x' \in G \cap K$. Comme G est discret, $G \cap K$ est fini. Donc le groupe quotient G/G' est fini et G' est d'indice fini dans G.

Soit s l'ordre de G/G' et soit $f_i' = f_i/s$ $(1 \leq i \leq t)$. On a

$$G' = \mathbf{Z}f_1 + \cdots + \mathbf{Z}f_t \subset G \subset \mathbf{Z}f_1' + \cdots + \mathbf{Z}f_t',$$

ce qui permet de conclure grâce à la proposition 4.14.

□

Théorème 4.20 (Structure des sous-groupes de $\mathbf{R}^n$)**.** *Soit G un sous-groupe de $\mathbf{R}^n$. Il existe un plus grand sous-espace vectoriel V de $\mathbf{R}^n$ sur $\mathbf{R}$ contenu dans l'adhérence de G. Soient d la dimension de V et $d + t$ la dimension de l'espace vectoriel engendré par G sur $\mathbf{R}$. Posons enfin $G' = G \cap V$. Alors il existe un sous-groupe G'' de G, discret de rang t, tel que G soit la somme directe de G' et G''.*

Démonstration. On utilisera la norme euclidienne :

$$\text{pour } \underline{x} = (x_1, \dots, x_n),\ \|\underline{x}\| = \sqrt{\sum_{j=1}^{n} |x_j|^2}.$$

Pour $\varrho > 0$ notons

$$B(0, \varrho) = \{x \in \mathbf{R}^n\ ;\ \|x\| \le \varrho\}$$

la boule euclidienne de rayon ϱ et soit V_ϱ le $\mathbf{R}$-espace vectoriel engendré par $G \cap B(0, \varrho)$ dans $\mathbf{R}^n$. Posons

$$V = \bigcap_{\varrho > 0} V_\varrho.$$

L'application $\varrho \mapsto \dim V_\varrho$ est croissante à valeurs entières ≥ 0, donc il existe $\varrho_0 > 0$ tel que $V = V_\varrho$ pour $0 < \varrho \le \varrho_0$.

Montrons que $G' = G \cap V$ est dense dans V. Soit $\epsilon > 0$ et soit $x \in V$. Posons $\varrho = \min\{\epsilon/d,\ \varrho_0\}$ et soit $\{e_1, \dots, e_d\}$ une base de V sur $\mathbf{R}$ avec $e_i \in G \cap B(0, \varrho)$. On écrit $x = x_1 e_1 + \cdots + x_d e_d$, on pose $m_i = [x_i]$ $(1 \le i \le d)$ et $y = m_1 e_1 + \cdots + m_d e_d$. Alors $y \in G'$ vérifie $\|x - y\| \le \epsilon$.

Soit maintenant W le sous-espace de $\mathbf{R}^n$ engendré par G. Comme il contient V sa dimension est $d + t$ avec $t \ge 0$. Soit V' un supplémentaire de V dans W et soit $p : W \to V'$ la projection de noyau V.

Montrons que $p(G)$ est un sous-groupe discret de V'. Soit $z \in p(G)$ tel que $\|z\| < \epsilon$ avec $\epsilon = \varrho_0/2$. On va montrer que cela entraîne $z = 0$, ce qui permettra de conclure grâce au lemme 4.18. Soit $w \in G$ tel que $z = p(w)$; on a $u = w - z \in V$. Comme G' est dense dans V il existe $w' \in G'$ tel que $\|u - w'\| < \epsilon$. Alors $w - w' \in G$ vérifie $\|w - w'\| < \varrho_0$. Comme $V = V_{\varrho_0}$ il en résulte $w - w' \in V$ et donc $p(w - w') = 0$. Mais $p(w - w') = z$, donc $z = 0$.

Ainsi $p(G)$ est un sous-groupe discret de V' de rang t, donc un réseau de V'. On en prend une base $p(y_1), \dots, p(y_t)$ et on pose $G'' = \mathbf{Z}y_1 + \cdots + \mathbf{Z}y_t$. Ainsi $G = G' \oplus G''$.

Enfin comme G'' est discret, V est le plus grand sous-espace vectoriel de $\mathbf{R}^n$ contenu dans l'adhérence de G.

□

Le théorème 4.20 permet de préciser la structure des sous-groupes fermés de $\mathbf{R}^n$:

Corollaire 4.21. *Soit G un sous-groupe fermé de $\mathbf{R}^n$. Il existe un plus grand sous-espace vectoriel V contenu dans G ; si W est un sous-espace vectoriel de $\mathbf{R}^n$ supplémentaire de V, alors $W \cap G$ est un sous-groupe discret de $\mathbf{R}^n$, et G est somme directe de V et de $W \cap G$.*

Exercice. Soit $\mathbf{x} = (x_1, \dots, x_n) \in \mathbf{R}^n$. On considère le sous-groupe

$$G = \mathbf{Z}^n + \mathbf{Z}\mathbf{x} = \{(a_1 + a_0 x_1, \dots, a_n + a_0 x_n)\ ;\ (a_0, \dots, a_n) \in \mathbf{Z}^{n+1}\}$$

de $\mathbf{R}^n$.
1. Montrer que G est discret dans $\mathbf{R}^n$ si et seulement si $\mathbf{x} \in \mathbf{Q}^n$.
2. En déduire que les conditions suivantes sont équivalentes.
(i) 0 est un point d'accumulation de G
(ii) Pour tout $\epsilon > 0$ il existe des entiers $p_1, \dots, p_n$, q, avec $q > 0$, tels que

$$0 < \max_{1 \le i \le n} |q x_i - p_i| < \epsilon.$$

(iii) L'un au moins des n nombres $x_1, \dots, x_n$ est irrationnel.
3. Montrer que G est dense dans $\mathbf{R}^n$ si et seulement si les nombres $1, x_1, \dots, x_n$ sont linéairement indépendants sur $\mathbf{Q}$.
En déduire que pour tout $(\xi_1, \xi_2) \in \mathbf{R}^2$ et pour tout $\epsilon > 0$ il existe des entiers rationnels p_1, p_2 et q avec

$$|\xi_1 - p_1 - q\sqrt{2}| \le \epsilon \quad \text{et} \quad |\xi_2 - p_2 - q\sqrt{3}| \le \epsilon.$$

Exercice. On appelle *caractère* de $\mathbf{R}^n$ tout homomorphisme continu de $\mathbf{R}^n$ dans $\mathbf{R}/\mathbf{Z}$ (ou dans le groupe multiplicatif $\mathbf{U}$ des nombres complexes de module 1, cela revient au même).
1. Vérifier que tout homomorphisme continu du groupe additif $\mathbf{R}$ dans lui-même est une application $\mathbf{R}$-linéaire, c'est-à-dire de la forme $x \mapsto \lambda x$, pour un $\lambda \in \mathbf{R}$. En déduire d'abord que tout homomorphisme continu du groupe additif $\mathbf{R}$ dans le groupe multiplicatif $\mathbf{R}^\times$ est de la forme $x \mapsto e^{\lambda x}$, ensuite que tout homomorphisme continu du groupe additif $\mathbf{R}$ dans le groupe multiplicatif $\mathbf{U}$ est de la forme $x \mapsto e^{i\lambda x}$. En déduire que tout homomorphisme continu $\chi : \mathbf{R} \to \mathbf{R}/\mathbf{Z}$ se factorise en $\chi = s \circ h$:

$$\begin{array}{ccc} \mathbf{R} & \xrightarrow{\ h\ } & \mathbf{R} \\ & \chi \searrow & \downarrow s \\ & & \mathbf{R}/\mathbf{Z} \end{array}$$

où $s : \mathbf{R} \to \mathbf{R}/\mathbf{Z}$ est la surjection canonique et $h : \mathbf{R} \to \mathbf{R}$ est une application linéaire.
2. Quand u est un élément de $\mathbf{R}^n$, l'application ψ_u de $\mathbf{R}^n$ dans $\mathbf{U}$ donnée par $x \mapsto e^{2i\pi u \cdot x}$ (où $u \cdot x$ est le produit scalaire standard dans $\mathbf{R}^n$) est un caractère de $\mathbf{R}^n$. Vérifier qu'on les obtient tous ainsi. Le noyau de ψ_u est $\{x \in \mathbf{R}^n;\ u \cdot x \in \mathbf{Z}\}$.
3. En déduire que l'application de $\mathrm{Hom}_{\mathbf{R}}(\mathbf{R}^n, \mathbf{R})$ dans le groupe des caractères de $\mathbf{R}^n$ qui, à une forme linéaire φ, associe $\chi_\varphi : x \mapsto e^{2i\pi\varphi(x)}$, est un isomorphisme de groupes. Le noyau de χ_φ est $\varphi^{-1}(\mathbf{Z})$.
4. Soit G un sous-groupe de type fini de $\mathbf{R}^n$. Montrer que les conditions suivantes sont équivalentes.
(i) G est dense dans $\mathbf{R}^n$.
(ii) Pour tout sous-espace vectoriel V de $\mathbf{R}^n$ distinct de $\mathbf{R}^n$, on a

$$\mathrm{rang}_{\mathbf{Z}}(G/G \cap V) > \dim_{\mathbf{R}}(\mathbf{R}^n/V).$$

(iii) Pour tout hyperplan H de $\mathbf{R}^n$, on a $\mathrm{rang}_{\mathbf{Z}}(G/G \cap H) \ge 2$.
(iv) Pour toute forme linéaire non nulle $\varphi : \mathbf{R}^n \longrightarrow \mathbf{R}$ on a $\varphi(G) \not\subset \mathbf{Z}$.
(v) Pour tout caractère non trivial χ de $\mathbf{R}^n$, on a $\chi(G) \ne \{1\}$.
(vi) Choisissons des générateurs $g_1, \dots, g_\ell$ de G sur $\mathbf{Z}$ et écrivons les coordonnées des g_j dans la base canonique de $\mathbf{R}^n$:

$$g_j = (g_{1j}, \dots, g_{nj}), \qquad (1 \le j \le \ell);$$

pour tout $(s_1, \dots, s_\ell)$ dans $\mathbf{Z}^\ell$ distinct de $(0, \dots, 0)$, la matrice

$$\begin{pmatrix} g_{11} & \cdots & g_{1\ell} \\ \vdots & \ddots & \vdots \\ g_{n1} & \cdots & g_{n\ell} \\ s_1 & \cdots & s_\ell \end{pmatrix}$$

est de rang $n+1$.
Montrer aussi que dans le cas $\ell = n+1$, la condition (vi) est équivalente à la suivante :
(vii) Les $n+1$ nombres réels

$$\Delta_h = \det\Big(g_{ij}\Big)_{\substack{1\le i\le n\\ 1\le j\le n+1,\ j\ne h}}, \qquad (1 \le h \le n+1)$$

sont linéairement indépendants sur $\mathbf{Q}$.

Voici une caractérisation des réseaux parmi les sous-groupes discrets d'un sous-espace vectoriel de $\mathbf{R}^n$.

Lemme 4.22. *Soient V un sous-espace vectoriel de $\mathbf{R}^n$ et soit G un sous-groupe discret de $\mathbf{R}^n$ contenu dans V. Pour que G engendre V sur $\mathbf{R}$, il faut et il suffit qu'il existe un ensemble borné B de V tel que*

$$V = \bigcup_{g\in G} (B+g).$$

Démonstration. Si G contient une base $\{e_1,\dots,e_n\}$ de V sur $\mathbf{R}$, alors

$$B = \{x_1e_1 + \cdots + x_ne_n \ ;\ 0 \le x_i < 1 \ (1\le i\le n)\}$$

convient.

Inversement, si G est contenu dans un sous-espace vectoriel V' de V avec $V' \ne V$, et si $p : V \to W$ est la projection de V sur un supplémentaire W de V' dans V, alors pour toute partie B de V on a

$$p\left(\bigcup_{g\in G}(B+g)\right) = p(B).$$

Comme $W = p(V)$ est de dimension ≥ 1, si B est borné, alors $p(B) \ne p(V)$, donc

$$\bigcup_{g\in G}(B+g) \ne V.$$

□

Soit G un réseau de $\mathbf{R}^n$. Pour chaque base $\mathbf{e} = \{e_1,\dots,e_n\}$ de G le parallélogramme

$$P_{\mathbf{e}} = \{x_1e_1 + \cdots + x_ne_n \ ;\ 0 \le x_i < 1 \ (1\le i\le n)\}$$

est un *domaine fondamental* pour G, c'est-à-dire un système complet de représentants des classes modulo G. En écrivant

$$\mathbf{R}^n = \bigcup_{g\in G}(P_{\mathbf{e}}+g) \tag{4.23}$$

on obtient une partition de $\mathbf{R}^n$.

Le passage d'une base de G à une autre se fait avec une matrice de déterminant ± 1, donc la mesure de Lebesgue $\mu(P_{\mathbf{e}})$ de $P_{\mathbf{e}}$ ne dépend pas de $\mathbf{e}$: ce nombre est appelé *le volume* du réseau G et noté $v(G)$.

Voici un exemple des résultats obtenus par Minkowski au XIXème siècle comme application de sa *géométrie des nombres.*

Théorème 4.24 (*Minkowski*)**.** *Soient G un réseau de $\mathbf{R}^n$ et B un sous-ensemble mesurable de $\mathbf{R}^n$. On suppose $\mu(B) > v(G)$. Alors il existe x et y distincts dans B tels que $x - y \in G$.*

Démonstration. Grâce à (4.23) on peut écrire B comme réunion disjointe des $B \cap (P_{\mathbf{e}} + g)$ avec g parcourant G. Alors

$$\mu(B) = \sum_{g \in G} \mu\left(B \cap (P_{\mathbf{e}} + g)\right).$$

Comme la mesure de Lebesque est invariante par translation on a

$$\mu\left(B \cap (P_{\mathbf{e}} + g)\right) = \mu\left((-g + B) \cap P_{\mathbf{e}}\right).$$

Les ensembles $(-g + B) \cap P_{\mathbf{e}}$ sont tous contenus dans $P_{\mathbf{e}}$ et la somme de leurs mesures est $\mu(B) > \mu(P_{\mathbf{e}})$. Donc ils ne sont pas deux-à-deux disjoints (c'est une des versions du *principe des tiroirs de Dirichlet*). Il existe $g \neq g'$ dans G tels que

$$(-g + B) \cap (-g' + B) \neq \emptyset.$$

Soient x et y dans B tels que $-g + x = -g' + y$. Alors $x - y = g - g' \in G \setminus \{0\}$.

□

Corollaire 4.25. *Soit G un réseau de $\mathbf{R}^n$ et soit B un sous-ensemble mesurable de $\mathbf{R}^n$, convexe et symétrique par rapport à l'origine, tel que $\mu(B) > 2^n v(G)$. Alors $B \cap G \neq \{0\}$.*

Démonstration. On applique le théorème 4.24 à l'ensemble

$$B' = \frac{1}{2}B = \{x \in \mathbf{R}^n \ ; \ 2x \in B\}.$$

On a $\mu(B') = 2^{-n}\mu(B) > v(G)$, donc il existe $x \neq y$ dans B' tels que $x - y \in G$. Alors $2x$ et $2y$ sont dans B, et comme B est symétrique $-2y \in B$. Enfin B est convexe, donc $(2x - 2y)/2 = x - y \in G \cap B$.

□

Remarque. Avec les notations du corollaire 4.25, si on suppose que B est une partie compacte de $\mathbf{R}^n$, alors l'inégalité large $\mu(B) \geq 2^n v(G)$ suffit pour obtenir la conclusion. On le voit par exemple en appliquant le corollaire 4.25 à $(1 + \epsilon)B$ avec $\epsilon \to 0$.

4.4.3 Plongements d'un corps de nombres

Proposition 4.26. *L'image de l'anneau des entiers $\mathbf{Z}_k$ de k par le plongement canonique $\underline{\sigma}$ est un réseau de $\mathbf{R}^n$.*

Nous utiliserons plusieurs fois la remarque suivante : la somme des modules des coefficients d'un polynôme

$$(X - \alpha_1) \cdots (X - \alpha_n) \in \mathbf{C}[X]$$

est majorée par

$$(1 + |\alpha_1|) \cdots (1 + |\alpha_n|). \tag{4.27}$$

Démonstration. Si K est un compact de $\mathbf{R}^n$, il existe un nombre réel $C > 0$ tel que tout $(x_1, \dots, x_n) \in K$ vérifie $|x_i| \leq C$ $(1 \leq i \leq n)$. Si $x \in k$ est tel que $\underline{\sigma}(x) \in K$, alors $|\sigma_i(x)| \leq C\sqrt{2}$ pour tout $i = 1, \dots, n$. De (4.27) on déduit que pour $x \in \mathbf{Z}_k \cap \underline{\sigma}^{-1}(K)$ la somme des modules des coefficients du polynôme minimal de x est majorée par $(1 + C\sqrt{2})^n$, donc les polynômes unitaires irréductibles de $\mathbf{Z}[X]$ dont ces x sont racines sont en nombre fini. Ainsi $\underline{\sigma}(\mathbf{Z}_k) \cap K$ est fini, et par conséquent $\underline{\sigma}(\mathbf{Z}_k)$ est un sous-groupe discret de $\mathbf{R}^n$. Comme $\underline{\sigma}$ est un homomorphisme injectif de $\mathbf{Z}$-modules et que $\mathbf{Z}_k$ est de rang n, son image $\underline{\sigma}(\mathbf{Z}_k)$ est un sous-groupe de rang n de $\mathbf{R}^n$.

□

Le calcul du volume de ce réseau se déduit de la proposition suivante :

Proposition 4.28. *Soit M un sous-$\mathbf{Z}$-module libre de k de rang n et soit $x_1, \dots, x_n$ une base de M sur $\mathbf{Z}$. Alors $\underline{\sigma}(M)$ est un réseau de $\mathbf{R}^n$ de volume*

$$v\big(\underline{\sigma}(M)\big) = 2^{-r_2}\big|\det\big(\sigma_i(x_j)\big)\big|.$$

Démonstration. Soit d un entier positif tel que $dx_i \in \mathbf{Z}_k$ pour $1 \leq i \leq n$. Alors $dM \subset \mathbf{Z}_k$. Donc $\underline{\sigma}(dM)$ est un sous-groupe d'indice fini de $\underline{\sigma}(\mathbf{Z}_k)$, et il résulte de la proposition 4.26 que $\underline{\sigma}(dM)$ et $\underline{\sigma}(M)$ sont des réseaux de $\mathbf{R}^n$.

Le volume de $\underline{\sigma}(M)$ est la valeur absolue du déterminant de la matrice $n \times n$ dont la $i$ème colonne est

$$\Big(\sigma_1(x_i), \dots, \sigma_{r_1}(x_i), \Re e\big(\sigma_{r_1+1}(x_i)\big), \Im m\big(\sigma_{r_1+1}(x_i)\big), \dots, \Re e\big(\sigma_{r_1+r_2}(x_i)\big), \Im m\big(\sigma_{r_1+r_2}(x_i)\big)\Big).$$

Par combinaison linéaire des lignes, la valeur absolue de ce déterminant est égale au module du déterminant de la matrice dont la $i$ème colonne est

$$\Big(\sigma_1(x_i), \dots, \sigma_{r_1}(x_i), \sigma_{r_1+1}(x_i), (1/2)\overline{\sigma}_{r_1+1}(x_i), \dots, \sigma_{r_1+r_2}(x_i), (1/2)\overline{\sigma}_{r_1+r_2}(x_i)\Big).$$

□

On en déduit immédiatement :

Corollaire 4.29. *Le volume du réseau $\underline{\sigma}(\mathbf{Z}_k)$ de $\mathbf{R}^n$ est*

$$2^{-r_2}|D_k|^{1/2}$$

où D_k est le discriminant de k.

Le plongement canonique d'un corps de nombres est utile pour étudier la structure additive de l'anneau des entiers. Pour étudier la structure multiplicative on introduit le *plongement logarithmique* λ de k : c'est l'application de $k^\times$ dans $\mathbf{R}^{r_1+r_2}$ qui envoie $x \in k^\times$ sur

$$\lambda(x) = \Big(\log|\sigma_1(x)|, \dots, \log|\sigma_{r_1}(x)|, 2\log|\sigma_{r_1+1}(x)|, \dots, 2\log|\sigma_{r_1+r_2}(x)|\Big).$$

Comme

$$\mathrm{N}_{k/\mathbf{Q}}(x) = \prod_{i=1}^{n} \sigma_i(x),$$

si $s : \mathbf{R}^{r_1+r_2} \to \mathbf{R}$ est l'application $s(t_1, \dots, t_{r_1+r_2}) = t_1 + \cdots + t_{r_1+r_2}$, alors pour $x \in k^\times$ on a $s \circ \lambda(x) = \log |\mathrm{N}_{k/\mathbf{Q}}(x)|$.

En particulier un élément x de $k^\times$ vérifie $|\mathrm{N}_{k/\mathbf{Q}}(x)| = 1$, si et seulement si $\lambda(x)$ appartient à l'hyperplan $H = \ker s$ de $\mathbf{R}^{r_1+r_2}$ d'équation $t_1 + \cdots + t_{r_1+r_2} = 0$.

Grâce au lemme 4.16 on en déduit :

Lemme 4.30. *Soit $x \in \mathbf{Z}_k$, $x \neq 0$. Les trois propriétés suivantes sont équivalentes :*
(i) $x \in \mathbf{Z}_k^\times$
(ii) $\mathrm{N}_{k/\mathbf{Q}}(x) = \pm 1$
(iii) $\lambda(x) \in H$.

Le résultat suivant, dû à Kronecker, nous permettra de déterminer le noyau de la restriction de λ à $\mathbf{Z}_k \setminus \{0\}$:

Lemme 4.31. *Si un entier algébrique non nul α a tous ses conjugués complexes de modules ≤ 1, alors α est une racine de l'unité.*

Démonstration. L'hypothèse sur α et la majoration (4.27) impliquent que la somme des modules des coefficients des polynômes minimaux des nombres α^m, $m \in \mathbf{Z}$, $m \geq 0$, est bornée par $2^{[\mathbf{Q}(\alpha):\mathbf{Q}]}$, indépendamment de m, donc ces nombres α^m forment un ensemble fini : il existe $m \neq m'$ tel que $\alpha^m = \alpha^{m'}$, d'où le lemme 4.31.

□

On déduit du lemme 4.31

$$\mathbf{Z}_k \cap \ker \lambda = k_{\mathrm{tors}}^\times.$$

Comme la fonction d'Euler $\varphi(n)$ tend vers l'infini avec n, le groupe de torsion d'un corps de nombres est fini (donc cyclique).

4.4.4 Théorème de Dirichlet

Le théorème 4.17 de Dirichlet, qui donne la structure du groupe des unités d'un corps de nombres, est une conséquence de l'énoncé plus précis suivant :

Théorème 4.32. *L'image $\lambda(\mathbf{Z}_k)$ de l'anneau des entiers de k par le plongement logarithmique est un réseau de l'hyperplan H.*

La démonstration du théorème 4.32 va utiliser plusieurs lemmes auxiliaires.

Lemme 4.33. *Pour tout compact K de $\mathbf{R}^{r_1+r_2}$ l'ensemble de $\alpha \in \mathbf{Z}_k^\times$ tels que $\lambda(\alpha) \in K$ est fini.*

Démonstration. La majoration (4.27) montre que si K est un compact de $\mathbf{R}^{r_1+r_2}$ les polynômes unitaires irréductibles de $\mathbf{Z}[X]$ dont les éléments de $\lambda^{-1}(K) \cap \mathbf{Z}_k$ sont racines sont en nombre fini. □

Il résulte du lemme 4.33 que $\mathbf{Z}_k^\times$ est un groupe de type fini, produit direct du groupe fini $k_{\mathrm{tors}}^\times$ par un groupe libre de type fini et de rang $r \leq r_1 + r_2 - 1$:

$$\mathbf{Z}_k^\times \simeq k_{\mathrm{tors}}^\times \times \mathbf{Z}^r.$$

Pour compléter la démonstration des théorèmes 4.32 et 4.17 il reste à vérifier que $r = r_1 + r_2 - 1$, c'est-à-dire que $\mathbf{Z}_k^\times$ contient $r_1 + r_2 - 1$ éléments multiplicativement indépendants, ce qui revient encore à dire que $\lambda(\mathbf{Z}_k^\times)$ engendre l'hyperplan H sur $\mathbf{R}$. Pour cela on part d'un élément z de H et on veut montrer qu'il existe un élément de $\lambda(\mathbf{Z}_k^\times)$ à distance bornée de z (pour pouvoir utiliser le lemme 4.22). On construit déjà un élément α de $\mathbf{Z}_k$ tel que $\lambda(\alpha)$ ne soit pas trop loin de z, on majore la valeur absolue de la norme de α en utilisant le fait que $\lambda(\alpha)$ est proche de H, et cela suffit pour approcher $\lambda(\alpha)$, donc z, par un élément de $\lambda(\mathbf{Z}_k^\times)$, grâce au lemme 4.34 que voici.

Lemme 4.34. *Soit $\kappa > 0$. Il existe un sous-ensemble fini Γ de $\mathbf{Z}_k$ tel que tout entier $\alpha \in \mathbf{Z}_k$ vérifiant $|\mathrm{N}_{k/\mathbf{Q}}(\alpha)| \leq \kappa$, puisse s'écrire $\alpha = \epsilon\gamma$ avec $\gamma \in \Gamma$ et $\epsilon \in \mathbf{Z}_k^\times$.*

Démonstration. Le seul élément de $\mathbf{Z}_k$ de norme 0 est 0. Donc si $\kappa < 1$ le résultat est vrai avec $\Gamma = \{0\}$.

Soit m un entier non nul dans l'intervalle $-\kappa \leq m \leq \kappa$. L'anneau $\mathbf{Z}_k/m\mathbf{Z}_k$ est fini ; il n'y a donc qu'un nombre fini d'idéaux de $\mathbf{Z}_k$ qui contiennent $m\mathbf{Z}_k$. Si $\alpha \in \mathbf{Z}_k$ vérifie $\mathrm{N}_{k/\mathbf{Q}}(\alpha) = m$, alors $m \in \alpha\mathbf{Z}_k$.

Ceci montre qu'il n'y a qu'un nombre fini d'idéaux principaux de $\mathbf{Z}_k$ ayant un générateur dont la norme a une valeur absolue $\leq \kappa$. Pour chacun d'eux on choisit un générateur γ et on prend pour Γ l'ensemble de ces γ (sans oublier 0). □

Lemme 4.35. *Il existe une constante $\kappa > 0$ ayant la propriété suivante : si $\lambda_1, \dots \lambda_n$ sont des nombres réels positifs vérifiant $\lambda_1 \cdots \lambda_n = \kappa$ et $\lambda_{r_1+r_2+j} = \lambda_{r_1+j}$ pour $1 \leq j \leq r_2$, alors il existe $\alpha \in \mathbf{Z}_k$ tel que*

$$0 < |\sigma_i(\alpha)| \leq \lambda_i \quad \textit{pour} \quad 1 \leq i \leq n.$$

Démonstration. Soit K le compact de $\mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$ défini par

$$|z_i| \leq \lambda_i \quad \text{pour} \quad 1 \leq i \leq r_1 + r_2.$$

Son volume est

$$\prod_{i=1}^{r_1}(2\lambda_i) \prod_{j=r_1+1}^{r_1+r_2} \pi\lambda_j^2 = 2^{r_1}\pi^{r_2}\kappa.$$

On prend $\kappa > (2/\pi)^{r_2}|D_k|^{1/2}$ de telle sorte que ce volume soit $> 2^{r_1+r_2}|D_k|^{1/2}$. Comme le volume de $\underline{\sigma}(\mathbf{Z}_k)$ est $2^{-r_2}|D_k|^{1/2}$ (lemme 4.29), on a $\mu(K) > 2^n v(\underline{\sigma}(\mathbf{Z}_k))$ et il ne reste plus qu'à appliquer le théorème de Minkowski 4.25.

□

Remarque. Sous les hypothèses du lemme 4.35, l'élément α qui est donné par la conclusion satisfait $1 \leq |\mathrm{N}_{k/\mathbf{Q}}(\alpha)| \leq \kappa$.

Démonstration du théorème 4.32. Soit $(t_1, \dots, t_{r_1+r_2}) \in H$. Posons $n_j = 1$ pour $1 \leq j \leq r_1$, $n_j = 2$ pour $r_1 < j \leq r_1 + r_2$,

$$\lambda_j = \kappa^{1/n} e^{t_j/n_j} \quad (1 \leq j \leq r_1 + r_2)$$

et $\lambda_{r_1+r_2+j} = \lambda_{r_1+j}$ pour $1 \leq j \leq r_2$, où κ est la constante dont l'existence est affirmée dans l'énoncé du lemme 4.35. Alors $\lambda_1 \cdots \lambda_n = \kappa$, donc il existe $\alpha \in \mathbf{Z}_k$ tel que

$$0 < |\sigma_j(\alpha)| \leq \lambda_j \quad \text{pour} \quad 1 \leq j \leq n$$

et $1 \leq |\mathrm{N}_{k/\mathbf{Q}}(\alpha)| \leq \kappa$. Comme $t_1 + \cdots +, t_{r_1+r_2} = 0$ on en déduit, pour $1 \leq j \leq r_1 + r_2$,

$$|\sigma_j(\alpha)| = |\mathrm{N}_{k/\mathbf{Q}}(\alpha)| \prod_{\substack{1\leq i\leq n\\ i\neq j}} |\sigma_i(\alpha)|^{-1} \geq \kappa^{-(n-1)/n} e^{t_j/n_j}.$$

Cela montre qu'il existe une constante κ' telle que, pour tout $(t_1, \ldots, , t_{r_1+r_2}) \in H$, il existe $\alpha \in \mathbf{Z}_k$ vérifiant $|\mathrm{N}_{k/\mathbf{Q}}(\alpha)| \leq \kappa$ et

$$\max_{1\leq j\leq, r_1+r_2} \big|t_j - n_j \log|\sigma_j(\alpha)|\big| \leq \kappa'.$$

On utilise le lemme 4.34 : soit Γ un sous-ensemble fini de $\mathbf{Z}_k$ tel que tout élément $\alpha \in \mathbf{Z}_k$ satisfaisant $|\mathrm{N}_{k/\mathbf{Q}}(\alpha)| \leq \kappa$ s'écrive $\epsilon\gamma$ avec $\epsilon \in \mathbf{Z}_k^\times$ et $\gamma \in \Gamma$. Alors pour tout $t \in H$ il existe $\gamma \in \Gamma$ et $\epsilon \in \mathbf{Z}_k^\times$ tels que

$$\|t - \lambda(\gamma) - \lambda(\epsilon)\| \leq \kappa',$$

ce qui montre que si B désigne la boule de $\mathbf{R}^{r_1+r_2}$ de centre 0 et de rayon

$$R = \kappa' + \max_{\gamma\in\Gamma} \|\lambda(\gamma)\|,$$

on a

$$H \subset \bigcup_{\epsilon\in\mathbf{Z}_k^\times} \big(B + \lambda(\epsilon)\big).$$

Le lemme 4.22 permet de conclure que $\lambda(\mathbf{Z}_k^\times)$ est un réseau de H.

□

Définition. *Un système fondamental d'unités d'un corps de nombres k* est un ensemble de $r = r_1 + r_2 - 1$ unités $\epsilon_1, \ldots, \epsilon_r$ dans $\mathbf{Z}_k^\times$ dont les images modulo $k_{\mathrm{tors}}^\times$ forment une base du groupe $\mathbf{Z}_k^\times / k_{\mathrm{tors}}^\times$.

Cela signifie que toute unité ϵ de k peut s'écrire de manière unique

$$\zeta \epsilon_1^{a_1} \cdots \epsilon_r^{a_r}$$

avec ζ racine de l'unité et $a_j \in \mathbf{Z}$.

Soit $\eta_1, \ldots, \eta_r$ un ensemble de r unités de k. On définit le *régulateur* $R(\eta_1, \ldots, \eta_r)$ de ce système d'unités comme le module du déterminant d'un mineur $r \times r$ de la matrice $(r+1) \times r$ dont les colonnes sont

$$\lambda(\eta_j), \qquad (1 \leq j \leq r).$$

Le fait que la norme de η_j soit ± 1 montre que tous ces mineurs ont le même module. Un système de r unités est indépendant (dans le $\mathbf{Z}$-module $\mathbf{Z}_k^\times$) si et seulement si son régulateur n'est pas nul.

Lemme 4.36. *Soit $\epsilon_1, \ldots, \epsilon_r$ un système fondamental d'unités de k et soit $\eta_1, \ldots, \eta_r$ un système indépendant de r unités de k. Alors le quotient*

$$R(\eta_1, \ldots, \eta_r)/R(\epsilon_1, \ldots, \epsilon_r)$$

est égal à l'indice du sous-groupe de $\mathbf{Z}_k^\times / k_{\mathrm{tors}}^\times$ engendré par les classes de $\eta_1, \ldots, \eta_r$.

Démonstration. Soit E le sous-groupe de $\mathbf{Z}_k^\times$ engendré par $\eta_1, \dots, \eta_r$. D'après la proposition 4.14 qui donne la structure des modules sur les anneaux principaux, il existe une base $x_1, \dots, x_r$ de $\mathbf{Z}_k^\times / k_{\rm tors}^\times$ et des entiers positifs $a_1, \dots, a_r$ tels que $a_1 x_1, \dots, a_r x_r$ soit une base de $E/k_{\rm tors}^\times$. Alors l'indice de $E/k_{\rm tors}^\times$ dans $\mathbf{Z}_k^\times / k_{\rm tors}^\times$ est $a_1 \cdots a_r$, et le quotient des régulateurs aussi.

□

En particulier le régulateur d'un système fondamental d'unités de k est le minimum parmi les régulateurs des systèmes indépendants de r unités de k, il ne dépend donc pas du système fondamental choisi : on l'appelle le *régulateur de* k et on le note R_k. Si $r = 0$ (c'est-à-dire $k = \mathbf{Q}$ ou si k est un corps quadratique imaginaire) on pose $R_k = 1$.

4.5 Idéaux d'un corps de nombres

Petit aperçu historique

L'invention de la notion d'idéal provient des recherches au XIXème siècle sur le *dernier théorème de Fermat* : il s'agissait de démontrer qu'il n'y a pas d'entiers positifs $n \geq 3$, x, y et z satisfaisant $x^n + y^n = z^n$. En supposant n impair et en utilisant l'identité

$$x^n + y^n = (x+y)(x+\zeta y)\cdots(x+\zeta^{n-1}y), \quad \zeta = \zeta_n = e^{2i\pi/n}$$

Kummer a démontré en 1844 que l'énoncé de Fermat est vrai pour un exposant premier $n = p$ pour lequel l'anneau des entiers du corps $\mathbf{Q}(\zeta_p)$ est factoriel ; Dirichlet a alors remarqué que l'existence d'une décomposition en facteurs irréductibles est toujours vraie, mais que l'unicité n'est pas claire. C'est dès 1844 que Kummer a su qu'il n'y avait pas unicité de la décomposition en éléments irréductibles dans l'anneau $\mathbf{Z}[\zeta_{23}]$. Il l'a écrit à Liouville en 1847 (à la suite d'une note de G. Lamé à l'Académie des Sciences le 11 mars 1847), ajoutant qu'il avait trouvé un substitut qui étaient les "nombres idéaux". L'idée est la suivante.

Dans le corps $k = \mathbf{Q}(\sqrt{-5})$ la décomposition en facteurs irréductibles n'est pas unique

$$21 = 3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5}).$$

Kummer affirme qu'il existe des objets qu'il appelle *nombres idéaux* donnant une décomposition unique

$$(21) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$$

qui explique la décomposition précédente :

$$\mathfrak{p}_1\mathfrak{p}_2 = (3), \quad \mathfrak{p}_3\mathfrak{p}_4 = (7), \qquad \mathfrak{p}_1\mathfrak{p}_3 = (1 + 2\sqrt{-5}), \quad \mathfrak{p}_2\mathfrak{p}_4 = (1 - 2\sqrt{-5}).$$

Dedekind a précisé cette construction de nombres idéaux. Si $\mathfrak{a}$ est un nombre idéal, on veut satisfaire les relations, pour a et b dans $\mathbf{Z}_k$,

$$\text{si } \mathfrak{a}|a \text{ et } \mathfrak{a}|b \text{ alors pour tout } \lambda \in \mathbf{Z}_k \text{ et } \mu \in \mathbf{Z}_k \text{ on a } \mathfrak{a}|\lambda a + \mu b.$$

On veut aussi que $\mathfrak{a}$ soit déterminé par $\{a \in \mathbf{Z}_k \ ; \ \mathfrak{a}|a\}$. L'idée est donc de considérer les sous-ensembles $\mathfrak{a}$ de $\mathbf{Z}_k$ qui vérifient la propriété

$$a \in \mathfrak{a},\ b \in \mathfrak{a}, \lambda \in \mathbf{Z}_k,\ \mu \in \mathbf{Z}_k \ \Rightarrow \lambda a + \mu b \in \mathfrak{a}.$$

Ce sont donc les idéaux de $\mathbf{Z}_k$.

Dans l'exemple précédent on prend

$$\mathfrak{p}_1 = (3, 1-\sqrt{-5}), \quad \mathfrak{p}_2 = (3, 1+\sqrt{-5}), \quad \mathfrak{p}_3 = (7, 3-\sqrt{-5}), \quad \mathfrak{p}_4 = (7, 3+\sqrt{-5}).$$

Références : [R], [P], Sk].

4.5.1 Idéaux entiers

Soient K un corps de nombres, $\mathbf{Z}_K$ son anneau d'entiers.

Lemme 4.37. *Soit $\alpha \in \mathbf{Z}_K$. Alors $\mathbf{Z}_K/\alpha\mathbf{Z}_K$ a $|\mathrm{N}_{K/\mathbf{Q}}(\alpha)|$ éléments.*

Démonstration. On utilise la proposition 4.14 : il existe une base $\{e_1, \ldots, e_n\}$ de $\mathbf{Z}_K$ et des entiers $a_1, \ldots, a_n$ tels que $\{a_1e_1, \ldots, a_ne_n\}$ soit une base de l'idéal $\alpha\mathbf{Z}_K$. Soit u l'endomorphisme du $\mathbf{Z}$-module $\mathbf{Z}_K$ qui envoie e_i sur a_ie_i. Son image est $\alpha\mathbf{Z}_K$ et sa matrice dans la base $\{e_1, \ldots, e_n\}$ est la matrice diagonale $\mathrm{diag}(a_1, \ldots, a_n)$, dont le déterminant est $a_1 \cdots a_n = \mathrm{N}(\alpha\mathbf{Z}_K)$. Comme $\{\alpha e_1, \ldots, \alpha e_n\}$ est aussi une base de $\alpha\mathbf{Z}_K$, il existe un automorphisme v du $\mathbf{Z}$-module $\alpha\mathbf{Z}_K$ tel que $v(a_ie_i) = \alpha e_i$. Alors $\det v = \pm 1$; comme $v \circ u$ est la restriction de $[\alpha]$ à $\mathbf{Z}_K$, le déterminant de u est aussi égal à $\pm\mathrm{N}_{K/\mathbf{Q}}(\alpha)$. □

Soit $\mathfrak{a}$ un idéal non nul de $\mathbf{Z}_K$, $\alpha \neq 0$ un élément de $\mathfrak{a}$. Alors $\mathbf{Z}_K\alpha \subset \mathfrak{a}$. Des propositions 4.12 et 4.14 on déduit que $\mathfrak{a}$ est un $\mathbf{Z}$-module libre de rang $n = [K : \mathbf{Q}]$. Par conséquent il existe une base $\{e_1, \ldots, e_n\}$ de $\mathbf{Z}_K$ comme $\mathbf{Z}$-module et des entiers positifs $a_1, \ldots, a_n$ tels que $\{a_1e_1, \ldots, a_ne_n\}$ soit une base de $\mathfrak{a}$ sur $\mathbf{Z}$ et que a_i divise a_{i+1} dans $\mathbf{Z}$ pour $1 \leq i < n$. On en déduit que le quotient $\mathbf{Z}_K/\mathfrak{a}$ est fini avec $a_1 \cdots a_n$ éléments. Le nombre d'éléments de $\mathbf{Z}_K/\mathfrak{a}$ est appelé *norme de* $\mathfrak{a}$ et noté $\mathrm{N}(\mathfrak{a})$.

Le lemme 4.37 montre que la norme d'un idéal principal est égale à la valeur absolue de la norme de K sur $\mathbf{Q}$ d'un générateur.

Si $\mathfrak{a}$ et $\mathfrak{b}$ sont deux idéaux de $\mathbf{Z}_K$ avec $\mathfrak{a} \subset \mathfrak{b}$, alors les surjections canoniques de $\mathbf{Z}_K$ sur les quotients induisent une surjection de $\mathbf{Z}_K/\mathfrak{a}$ sur $\mathbf{Z}_K/\mathfrak{b}$, donc $\mathrm{N}(\mathfrak{b})$ divise $\mathrm{N}(\mathfrak{a})$.

Soient $n = [K : \mathbf{Q}]$ le degré de K et $\underline{\sigma} : K \to \mathbf{R}^n$ son plongement canonique.

Lemme 4.38. *Soit $\mathfrak{a}$ un idéal non nul de $\mathbf{Z}_K$. Alors $\underline{\sigma}(\mathfrak{a})$ est un réseau de $\mathbf{R}^n$ de volume $2^{-r_2}|D_K|^{1/2}\mathrm{N}(\mathfrak{a})$ et le discriminant de $\mathfrak{a}$ est $D_K\mathrm{N}(\mathfrak{a})^2$. .*

Quand r_1 et r_2 sont deux entiers ≥ 0 avec $n = r_1 + 2r_2 \geq 1$ on définit la *constante de Minkowski* $M(r_1, r_2)$ par

$$M(r_1, r_2) = \left(\frac{4}{\pi}\right)^{r_2} \cdot \frac{n!}{n^n}.$$

On écrit encore $M(K)$ au lieu de $M(r_1, r_2)$ quand K est un corps de nombres de degré n ayant r_1 plongements réels et $2r_2$ plongements imaginaires deux-à-deux conjugués.

Nous déduirons ultérieurement (§ 4.5.5) plusieurs conséquences du lemme suivant.

Théorème 4.39. *Soient K un corps de nombres et $\mathfrak{a}$ un idéal non nul de $\mathbf{Z}_K$. Il existe $\alpha \in \mathfrak{a}$ tel que*

$$1 \leq |N_{K/\mathbf{Q}}(\alpha)| \leq M(K)|D_K|^{1/2}\mathrm{N}(\mathfrak{a}).$$

Nous renvoyons au § 4.2 de [12] pour la démonstration.

4.5.2 Idéaux premiers

Soient K un corps de nombres, $\mathbf{Z}_K$ son anneau d'entiers, $\mathfrak{p}$ un idéal premier non nul de $\mathbf{Z}_K$. Si $\alpha \in \mathfrak{p}$ a pour polynôme minimal $X^m + a_1X^{m-1} + \cdots + a_m$ (avec $m = [\mathbf{Q}(\alpha) : \mathbf{Q}]$) alors a_m appartient $\mathfrak{p} \cap \mathbf{Z}$ donc cette intersection n'est pas réduite à 0.

L'injection de $\mathbf{Z}$ dans $\mathbf{Z}_K$ induit une injection de $\mathbf{Z}/\mathfrak{p} \cap \mathbf{Z}$ dans l'anneau $\mathbf{Z}_K/\mathfrak{p}$ qui est intègre, donc $\mathbf{Z}/\mathfrak{p} \cap \mathbf{Z}$ est intègre et l'idéal $\mathfrak{p} \cap \mathbf{Z}$ de $\mathbf{Z}$ est premier non nul.

Rappelons le résultat élémentaire suivant :

Lemme 4.40. *Un anneau fini intègre est un corps.*

Démonstration. Si A est un anneau fini intègre, pour $x \in A \setminus \{0\}$ l'application $y \mapsto xy$ est une injection de A dans A, donc une bijection. □

Si $\mathfrak{p}$ est un idéal premier non nul de $\mathbf{Z}_K$, le corps fini $k = \mathbf{Z}_K/\mathfrak{p}$ est appelé *corps résiduel de* $\mathfrak{p}$. Dans ce cas $\mathbf{Z}/\mathfrak{p} \cap \mathbf{Z}$ est un sous-corps de k, donc le générateur positif de $\mathbf{Z} \cap \mathfrak{p}$ est un nombre premier p qui est appelé *la caractéristique du corps résiduel* k (on dit encore la *caractéristique résiduelle de* $\mathfrak{p}$). La norme de $\mathfrak{p}$ est donc p^f où $f = [k : \mathbf{F}_p]$ est le *degré du corps résiduel*.

Rappelons que le produit $\mathfrak{ab}$ de deux idéaux d'un anneau A est par définition l'idéal de A engendré par les produits ab, a parcourant $\mathfrak{a}$ et b parcourant $\mathfrak{b}$. Ainsi

$$\mathfrak{ab} \subset \mathfrak{a} \cap \mathfrak{b} \subset \mathfrak{a} \subset \mathfrak{a} + \mathfrak{b}.$$

Deux idéaux $\mathfrak{a}$ et $\mathfrak{b}$ de A sont dits *premiers entre eux* si $\mathfrak{a} + \mathfrak{b} = A$. Dans ce cas on a $\mathfrak{ab} = \mathfrak{a} \cap \mathfrak{b}$.

Lemme 4.41. *Soient $\mathfrak{a}$ et $\mathfrak{b}$ deux idéaux non nuls de $\mathbf{Z}_K$. Si $\mathfrak{a} = \mathfrak{ab}$, alors $\mathfrak{b} = \mathbf{Z}_K$.*

Démonstration. Soit $\alpha_1, \ldots, \alpha_n$ une base de l'idéal $\mathfrak{a}$ comme $\mathbf{Z}$-module. Comme $\alpha_i \in \mathfrak{ab}$ pour $1 \le i \le n$, on peut écrire

$$\alpha_i = \sum_{j=1}^{n} \beta_{ij}\alpha_j \quad \text{pour} \quad 1 \le i \le n,$$

avec des coefficients β_{ij} dans $\mathfrak{b}$. Alors la matrice $\big(\beta_{ij}\big)_{1\le i,j\le n} - I$ a un déterminant nul, d'où on déduit en développant $1 \in \mathfrak{b}$.

□

Soient A est un anneau, M un A-module et $\mathfrak{a}$ un idéal de A différent de A. Alors $\mathfrak{a}M$ est un sous-module de M et le quotient $M/\mathfrak{a}M$ est un A-module. Montrons que $M/\mathfrak{a}M$ a une structure naturelle de $A/\mathfrak{a}$-module.

En effet, la structure de A-module du quotient $M/\mathfrak{a}M$ est donnée par un homomorphisme de A-modules

$$\begin{array}{ccc} A & \to & \mathrm{Hom}_A(M/\mathfrak{a}M, M/\mathfrak{a}M) \\ a & \mapsto & (x \mapsto ax) \end{array}$$

dont le noyau contient $\mathfrak{a}$. On en déduit un homomorphisme de A-modules

$$A/\mathfrak{a} \longrightarrow \mathrm{Hom}_A(M/\mathfrak{a}M, M/\mathfrak{a}M)$$

qui confère à $M/\mathfrak{a}M$ la structure de $A/\mathfrak{a}$-module annoncée.

En particulier si $\mathfrak{a}$ est un idéal maximal $\mathfrak{p}$ de A alors $M/\mathfrak{p}M$ a une structure naturelle d'espace vectoriel sur le corps $A/\mathfrak{p}$.

On applique ceci avec $A = \mathbf{Z}_K$.

Lemme 4.42. *Soit $\mathfrak{a}$ un idéal non nul de $\mathbf{Z}_K$ et soit $\mathfrak{p}$ un idéal premier non nul de $\mathbf{Z}_K$. On désigne par k le corps résiduel $\mathbf{Z}_K/\mathfrak{p}$. Alors $\mathfrak{a}/\mathfrak{p}\mathfrak{a}$ est un k-espace vectoriel de dimension ≥ 1.*

Démonstration. Le lemme 4.41 implique $\mathfrak{a} \neq \mathfrak{p}\mathfrak{a}$, donc la dimension de ce k-espace vectoriel est ≥ 1. □

En fait il va résulter de ce qui suit que la dimension de cet espace vectoriel est 1.

Soit $\mathfrak{p}$ un idéal premier non nul de $\mathbf{Z}_K$. En utilisant au choix le lemme 4.41 ou bien le lemme 4.42, on obtient $\mathfrak{p}^m \neq \mathfrak{p}^{m+1}$ pour tout $m \geq 0$. La suite

$$\mathbf{Z}_K \supset \mathfrak{p} \supset \mathfrak{p}^2 \cdots \supset \mathfrak{p}^m \supset \cdots$$

est donc strictement décroissante. D'après le lemme 4.42 le quotient $\mathfrak{p}^m/\mathfrak{p}^{m+1}$ est isomorphe comme $\mathbf{Z}_K$-module à $\mathbf{Z}_K/\mathfrak{p}$; il en résulte que la norme de $\mathfrak{p}^m$ est $\mathrm{N}(\mathfrak{p})^m$.

L'intersection de tous les $\mathfrak{p}^m$ est $\{0\}$: en effet, quand $\mathfrak{b}$ est un idéal de $\mathbf{Z}_K$ distinct de $\mathbf{Z}_K$ et α est un élément non nul de $\mathfrak{b}$, le plus grand entier m tel que $\alpha \in \mathfrak{b}^m$ est borné par la condition que $\mathrm{N}(\mathfrak{b})^m$ divise $\mathrm{N}_{K/\mathbf{Q}}(\alpha)$.

Soit $\mathfrak{a}$ un idéal non nul de $\mathbf{Z}_K$. L'ensemble des entiers $t \geq 0$ tels que $\mathfrak{a} \subset \mathfrak{p}^t$ est non vide (il contient 0) et fini. On désigne par $v_{\mathfrak{p}}(\mathfrak{a})$ le plus grand de ces entiers :

$$\mathfrak{a} \subset \mathfrak{p}^t \quad \text{pour} \quad 0 \leq t \leq v_{\mathfrak{p}}(\mathfrak{a}) \quad \text{et} \quad \mathfrak{a} \not\subset \mathfrak{p}^t \quad \text{pour} \quad t = v_{\mathfrak{p}}(\mathfrak{a}) + 1.$$

On a $v_{\mathfrak{p}}(\mathfrak{a}) > 0$ si et seulement si $\mathfrak{a} \subset \mathfrak{p}$. On a aussi $v_{\mathfrak{p}}(\mathfrak{a}\mathfrak{p}) = v_{\mathfrak{p}}(\mathfrak{a}) + 1$, donc $v_{\mathfrak{p}}(\mathfrak{p}^m) = m$ pour $m \geq 0$. Enfin $v_{\mathfrak{p}}(\mathfrak{p}') = 0$ si $\mathfrak{p}$ et $\mathfrak{p}'$ sont deux idéaux premiers distincts.

Théorème 4.43. *Soit $\mathfrak{a}$ un idéal non nul de $\mathbf{Z}_K$. L'ensemble des idéaux premiers $\mathfrak{p}$ de $\mathbf{Z}_K$ qui contiennent $\mathfrak{a}$ est fini et on a*

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a})},$$

où le produit est étendu à l'ensemble des idéaux premiers non nuls de $\mathbf{Z}_K$.

De plus une telle décomposition est unique : si on a

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{a_{\mathfrak{p}}},$$

où les $a_{\mathfrak{p}}$ sont des entiers rationnels ≥ 0 tous nuls sauf un nombre fini, alors $a_{\mathfrak{p}} = v_{\mathfrak{p}}(\mathfrak{a})$ pour tout $\mathfrak{p}$.

Remarque. Le théorème 4.43 montre que, sous les hypothèses du lemme 4.42, $\mathfrak{a}/\mathfrak{a}\mathfrak{p}$ est de dimension 1 comme espace vectoriel sur $\mathbf{Z}_K/\mathfrak{p}$ car il n'y a pas d'idéal entre $\mathfrak{a}\mathfrak{p}$ et $\mathfrak{a}$.

Pour une démonstration du théorème 4.43, voir par exemple le livre de Samuel.

4.5.3 Idéaux fractionnaires

Soit A un anneau, soit M un A-module et soient N_1 et N_2 deux sous-A-modules de M. On dit que M est somme directe de N_1 et N_2, et on écrit $M = N_1 \oplus N_2$, si l'application $(x_1, x_2) \mapsto x_1 + x_2$ est un isomorphisme de A-modules de $N_1 \times N_2$ sur M. Cela revient à dire que l'on a $M = N_1 + N_2$ et $N_1 \cap N_2 = \{0\}$.

Si $\mathfrak{A}_1$ et $\mathfrak{A}_2$ sont deux idéaux d'un anneau A tels que $\mathfrak{A}_1 + \mathfrak{A}_2 = A$, alors $\mathfrak{A}_1 \cap \mathfrak{A}_2 = \mathfrak{A}_1\mathfrak{A}_2$ et $A/\mathfrak{A}_1\mathfrak{A}_2$ est isomorphe à $A/\mathfrak{A}_1 \times A/\mathfrak{A}_2$.

Nous utiliserons la notion d'anneau *noethérien* que voici.

Proposition 4.44. *Soient A un anneau et M un A-module. Les propriétés suivantes sont équivalentes :*
(i) Toute famille non vide de sous-modules de M admet un élément maximal.
(ii) Toute suite croissante de sous-modules de M est stationnaire à partir d'un certain rang.
(iii) Tout sous-module de M est de type fini.

Démonstration. Voir [12], § 1.4. □

Définition. Quand les conditions de la proposition 4.44 sont satisfaites on dit que M est un *A-module noethérien.* Un anneau est dit *noethérien* s'il est noethérien comme A-module, c'est-à-dire si tout suite croissante d'idéaux

$$\mathfrak{A}_1 \subset \mathfrak{A}_2 \subset \cdots$$

est stationnaire.

De la condition (iii) de la la proposition 4.44 il résulte qu'un anneau principal est noethérien.

Soient A un anneau intègre, K son corps des fractions. Un sous-A-module $\mathfrak{a}$ **non nul** de K est un *idéal fractionnaire de K par rapport à A* s'il vérifie les propriétés équivalentes suivantes :
(i) Il existe $\alpha \in A$, $\alpha \neq 0$ tel que $\alpha\mathfrak{a} \subset A$.
(ii) Il existe $\beta \in K$, $\beta \neq 0$ tel que $\beta\mathfrak{a} \subset A$.

L'équivalence vient du fait que si $\beta\mathfrak{a} \subset A$ avec $\beta \in K^\times$, alors on peut écrire $\beta = \alpha/\gamma$ avec α et γ dans $A \setminus \{0\}$, d'où $\alpha\mathfrak{a} \subset A$.

On dira aussi que $\mathfrak{a}$ est un *idéal fractionnaire de A.*

Lemme 4.45. *Si $\mathfrak{a}_1$ et $\mathfrak{a}_2$ sont des idéaux fractionnaires de A, alors*

$$\mathfrak{a}_1 + \mathfrak{a}_2, \quad \mathfrak{a}_1 \cap \mathfrak{a}_2, \quad \mathfrak{a}_1\mathfrak{a}_2$$

et

$$(\mathfrak{a}_1 : \mathfrak{a}_2) := \{x \in K \ ; \ x\mathfrak{a}_2 \subset \mathfrak{a}_1\}$$

sont des idéaux fractionnaires de A.

Démonstration. Si α_1 et α_2 sont des éléments non nuls de $A \setminus \{0\}$ tels que $\mathfrak{a}_i \subset \alpha_i^{-1}A$ pour $i = 1$ et $i = 2$, alors $\mathfrak{a}_1 + \mathfrak{a}_2$, $\mathfrak{a}_1 \cap \mathfrak{a}_2$ et $\mathfrak{a}_1\mathfrak{a}_2$ sont des sous-A-modules non nuls de K contenus dans $(\alpha_1\alpha_2)^{-1}A$.

Si α_1 est un élément non nul de A tel que $\mathfrak{a}_1 \subset \alpha_1^{-1}A$ et si a_2 est un élément non nul de $\mathfrak{a}_2$, alors pour tout $x \in (\mathfrak{a}_1 : \mathfrak{a}_2)$ on a

$$\alpha_1 a_2 x \in \alpha_1 x\mathfrak{a}_2 \subset \alpha_1\mathfrak{a}_1 \subset A,$$

donc $\alpha_1 a_2(\mathfrak{a}_1 : \mathfrak{a}_2) \subset A$.

Il reste à vérifier que le A-module $(\mathfrak{a}_1 : \mathfrak{a}_2)$ n'est pas nul. Si a_1 est un élément non nul de $\mathfrak{a}_1$ et α_2 un élément non nul de A tel que $\mathfrak{a}_2 \subset \alpha_2^{-1}A$, alors $a_1\alpha_2$ est un élément non nul de $(\mathfrak{a}_1 : \mathfrak{a}_2)$:

$$a_1\alpha_2\mathfrak{a}_2 \subset a_1 A \subset \mathfrak{a}_1.$$

□

On déduit du lemme 4.45 que si $\mathfrak{a}$ est un idéal fractionnaire de A, alors

$$(A : \mathfrak{a}) = \{x \in K \ ; \ x\mathfrak{a} \subset A\} \quad \text{et} \quad (\mathfrak{a} : \mathfrak{a}) = \{x \in K \ ; \ x\mathfrak{a} \subset \mathfrak{a}\}$$

sont des idéaux fractionnaires de A.

Tout sous-A-module de type fini de K non nul est un idéal fractionnaire.

Réciproquement, quand A est un anneau noethérien, tout idéal fractionnaire de A est de type fini : pour $\alpha \in A \setminus \{0\}$ les A-modules $\mathfrak{a}$ et $\alpha\mathfrak{a}$ sont isomorphes. Donc, quand A est noethérien, un idéal fractionnaire n'est autre qu'un sous-A-module non nul de type fini de K. Si $\mathfrak{a}$ admet $\{a_i\}$ comme partie génératrice et si $\mathfrak{b}$ est engendré par $\{b_j\}$, alors $\mathfrak{a}+\mathfrak{b}$ est engendré par $\{a_i\} \cup \{ b_j\}$ et $\mathfrak{ab}$ par $\{a_i b_j\}$.

Quand K est un corps de nombres, un *idéal entier* de K est un idéal de $\mathbf{Z}_K$, c'est-à-dire un idéal fractionnaire de $\mathbf{Z}_K$ contenu dans $\mathbf{Z}_K$.

Proposition 4.46. *Soit $\mathfrak{p}$ un idéal premier non nul de $\mathbf{Z}_K$. Soit*

$$\mathfrak{p}' = \{x \in K \ ; \ x\mathfrak{p} \subset \mathbf{Z}_K\}.$$

Alors $\mathfrak{p}'$ est un idéal fractionnaire de $\mathbf{Z}_K$ qui contient $\mathbf{Z}_K$ et $\mathfrak{p}\mathfrak{p}' = \mathbf{Z}_K$.

Du théorème 4.43 on déduit que les idéaux fractionnaires de $\mathbf{Z}_K$ forment un groupe abélien d'élément neutre $\mathbf{Z}_K = (1)$.

Théorème 4.47. *Soit $\mathfrak{a}$ un idéal fractionnaire de $\mathbf{Z}_K$. Il existe une décomposition unique*

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{a_\mathfrak{p}},$$

où le produit est étendu à l'ensemble des idéaux premiers non nuls de $\mathbf{Z}_K$ et les $a_\mathfrak{p}$ sont des entiers rationnels tels que $\{\mathfrak{p} \ ; \ a_\mathfrak{p} \neq 0\}$ soit fini.

Démonstration. Soit $\alpha \in \mathbf{Z}_K \setminus \{0\}$ tel que $\alpha\mathfrak{a} \subset \mathbf{Z}_K$. On décompose les idéaux entiers $\alpha\mathbf{Z}_K$ et $\alpha\mathfrak{a}$ en produit d'idéaux premiers, on multiplie par les inverses des idéaux premiers apparaissant dans la décomposition de $\alpha\mathbf{Z}_K$ et on trouve la décomposition annoncée de $\mathfrak{a}$. L'unicité résulte de ce qui précède.

□

Soit K un corps de nombres. Le théorème 4.43 montre que la propriété (4.1) de multiplicativité de la norme s'étend aux idéaux de $\mathbf{Z}_K$:

Corollaire 4.48. *Soient $\mathfrak{a}$ et $\mathfrak{b}$ deux idéaux de $\mathbf{Z}_K$. Alors*

$$\mathrm{N}(\mathfrak{ab}) = \mathrm{N}(\mathfrak{a})\mathrm{N}(\mathfrak{b}). \tag{4.49}$$

Démonstration. Grâce au théorème 4.43 il suffit de vérifier la propriété (4.49) quand $\mathfrak{b}$ est un idéal premier. Notons-le $\mathfrak{p}$.

L'homomorphisme canonique

$$\mathbf{Z}_K/\mathfrak{ap} \to \mathbf{Z}_K/\mathfrak{a}$$

est surjectif et a pour noyau $\mathfrak{a}/\mathfrak{ap}$. Le quotient $k = \mathbf{Z}_K/\mathfrak{p}$ est un corps fini (ayant $\mathrm{N}(\mathfrak{p})$ éléments) et $\mathfrak{a}/\mathfrak{ap}$ est un k-espace vectoriel de dimension 1 (car $\mathfrak{p}$ est maximal - cf lemme 4.42 et la remarque

qui suit le théorème 4.43), donc est isomorphe à k. Ainsi $\mathfrak{a}/\mathfrak{a}\mathfrak{p}$ a $\mathrm{N}(\mathfrak{p})$ éléments et par conséquent $\mathbf{Z}_K/\mathfrak{a}\mathfrak{p}$ en a $\mathrm{N}(\mathfrak{a})\mathrm{N}(\mathfrak{p})$.

□

Remarque. Une autre démonstration, due à H.W. Lenstra, est donnée dans [2], Lemma 4.6.8.

Grâce au corollaire 4.48 on peut étendre la définition de la norme aux idéaux fractionnaires. Avec les notations du corollaire 4.47, on pose $v_{\mathfrak{p}}(\mathfrak{a}) = a_{\mathfrak{p}}$ et

$$\mathrm{N}(\mathfrak{a}) = \prod_{\mathfrak{p}} \mathrm{N}(\mathfrak{p})^{a_{\mathfrak{p}}}.$$

La norme d'un idéal fractionnaire principal de $\mathbf{Z}_K$ est égale à la valeur absolue de la norme de K sur $\mathbf{Q}$ d'un générateur : pour tout $\alpha \in K^\times$ on a $\mathrm{N}(\alpha\mathbf{Z}_K) = |\mathrm{N}_{K/\mathbf{Q}}(\alpha)|$.

Le lemme 4.46 signifie que les idéaux premiers non nuls sont inversibles dans le monoïde des idéaux fractionnaires de $\mathbf{Z}_K$. L'inverse $\mathfrak{p}'$ de $\mathfrak{p}$ est aussi noté $\mathfrak{p}^{-1}$:

$$\mathfrak{p}^{-1} = \{x \in K \ ; \ x\mathfrak{p} \subset \mathbf{Z}_K\}.$$

Exercice. Soient $\mathfrak{a}$ un idéal non nul et $\mathfrak{p}$ un idéal premier non nul de $\mathbf{Z}_K$.
1. Montrer qu'il existe $\alpha \in \mathfrak{a}$ tel que $\alpha \notin \mathfrak{a}\mathfrak{p}$.
Montrer qu'il existe un idéal $\mathfrak{b}$ de $\mathbf{Z}_K$ tel que $\mathfrak{a}\mathfrak{b} = \alpha\mathbf{Z}_K$.
Vérifier $\mathfrak{a} = \alpha\mathbf{Z}_K + \mathfrak{a}\mathfrak{p}$.
2. Soient $a_1, \ldots, a_N$ des représentants des classes de $\mathbf{Z}_K$ modulo $\mathfrak{a}$, avec $N = \mathrm{N}(\mathfrak{a})$, et soient $b_1, \ldots, b_M$ des représentants des classes de $\mathbf{Z}_K$ modulo $\mathfrak{p}$, avec $M = \mathrm{N}(\mathfrak{p})$. Vérifier que

$$\{a_i + \alpha b_j\}_{\substack{1 \le i \le N \\ 1 \le j \le M}}$$

est un système complet de représentants des classes de $\mathbf{Z}_K$ modulo $\mathfrak{a}\mathfrak{p}$.

Du théorème 4.43 on déduit, pour $\mathfrak{p}$ idéal premier de $\mathbf{Z}_K$ et $\mathfrak{a}$, $\mathfrak{b}$ idéaux fractionnaires de $\mathbf{Z}_K$:

$$\begin{array}{rcl} v_{\mathfrak{p}}(\mathfrak{a}\mathfrak{b}) & = & v_{\mathfrak{p}}(\mathfrak{a}) + v_{\mathfrak{p}}(\mathfrak{b}), \\ v_{\mathfrak{p}}(\mathfrak{a}+\mathfrak{b}) & = & \min\{v_{\mathfrak{p}}(\mathfrak{a}), v_{\mathfrak{p}}(\mathfrak{b})\}, \\ v_{\mathfrak{p}}(\mathfrak{a}\cap\mathfrak{b}) & = & \max\{v_{\mathfrak{p}}(\mathfrak{a}), v_{\mathfrak{p}}(\mathfrak{b})\}. \end{array}$$

Soit $\mathfrak{p}$ un idéal premier de $\mathbf{Z}_K$. On définit *l'indice de ramification* $e(\mathfrak{p})$ de $\mathfrak{p}$ par $e(\mathfrak{p}) = v_{\mathfrak{p}}(p\mathbf{Z}_K)$ où p désigne la caractéristique résiduelle de $\mathfrak{p}$. Ainsi $e(\mathfrak{p}) \ge 1$.

Soit p un nombre premier et soit $p\mathbf{Z}_K$ l'idéal principal de $\mathbf{Z}_K$ qu'il engendre. Le théorème 4.43 montre qu'il existe une décomposition, unique à l'ordre près des facteurs,

$$p\mathbf{Z}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}, \tag{4.50}$$

où g est un entier ≥ 1, $\mathfrak{p}_1, \ldots, \mathfrak{p}_g$ sont des idéaux premiers de $\mathbf{Z}_K$ deux-à-deux distincts et $e_i \ge 1$ est l'indice de ramification de $\mathfrak{p}_i$ $(1 \le i \le g)$.

Les idéaux $\mathfrak{p}_1, \ldots, \mathfrak{p}_g$ sont précisément les idéaux premiers $\mathfrak{p}$ de $\mathbf{Z}_K$ tels que $\mathfrak{p} \cap \mathbf{Z} = p\mathbf{Z}$. On dit que ce sont les *idéaux premiers de* $\mathbf{Z}_K$ *au dessus de* p. De la décomposition (4.50) on déduit

$$\mathbf{Z}_K/p\mathbf{Z}_K \simeq \mathbf{Z}_K/\mathfrak{p}_1^{e_1} \cdots \mathbf{Z}_K/\mathfrak{p}_g^{e_g}.$$

En notant $n = [K : \mathbf{Q}]$, en désignant par f_i le degré du corps résiduel de $\mathfrak{p}_i$ et en utilisant le corollaire 4.48, on obtient

$$p^n = \mathrm{N}_{K/\mathbf{Q}}(p) = \mathrm{N}(\mathfrak{p}_1)^{e_1} \cdots \mathrm{N}(\mathfrak{p}_g)^{e_g} = p^{e_1 f_1 + \cdots + e_g f_g}.$$

Par conséquent

$$e_1 f_1 + \cdots + e_g f_g = n. \tag{4.51}$$

On dit que $\mathfrak{p}_i$ est *ramifié au dessus de* p si l'exposant e_i est ≥ 2. On dit que p est *ramifié dans* K si l'un des exposants e_i est ≥ 2. On dit encore que p est
- *totalement ramifié dans* K si $e_1 = n$: alors $g = 1$ et $f_1 = 1$
- *totalement décomposé dans* K si $g = n$: alors $e_1 = \cdots = e_n = f_1 = \cdots = f_n = 1$
- *inerte dans* K si $f_1 = n$: alors $g = 1$ et $e_1 = 1$; cela revient à dire que $p\mathbf{Z}_K$ est un idéal premier.

Voici ce qui se passe pour les corps quadratiques

Proposition 4.52. *Soit d un entier sans facteur carré et soit p un nombre premier impair. Dans le corps $K = \mathbf{Q}(\sqrt{d})$, p se décompose de la façon suivante :*
(i) Si p divise d, alors p est ramifié dans K :
$p\mathbf{Z}_K = \mathfrak{p}^2$ *avec* $\mathrm{N}(\mathfrak{p}) = p$.
(ii) Si $\left(\frac{d}{p}\right) = 1$, alors p est décomposé dans K :
$p\mathbf{Z}_K = \mathfrak{p}_1\mathfrak{p}_2$ *avec* $\mathrm{N}(\mathfrak{p}_1) = \mathrm{N}(\mathfrak{p}_1) = p$.
(iii) Si $\left(\frac{d}{p}\right) = -1$, alors p est inerte dans K :
$p\mathbf{Z}_K = \mathfrak{p}$.

Démonstration. Si $d \equiv 2$ ou $3 \pmod 4$, alors $\mathbf{Z}_K = \mathbf{Z}[\sqrt{d}]$. Si $d \equiv 1 \pmod 4$, on a $\mathbf{Z}_K = \mathbf{Z}[(1 + \sqrt{d})/2]$, dans ce dernier cas comme p est un nombre premier impair on peut écrire $\mathbf{Z}_K = \mathbf{Z}[\sqrt{d}] + p\mathbf{Z}_K$. Par conséquent on a toujours

$$\mathbf{Z}_K/p\mathbf{Z}_K = \mathbf{Z}[\sqrt{d}]/p\mathbf{Z}[\sqrt{d}] \simeq \mathbf{Z}[X]/(p, X^2 - d) \simeq \mathbf{F}_p[X]/(X^2 - d).$$

- Le polynôme $X^2 - d$ a une racine double dans $\mathbf{F}_p$ si et seulement si p divise d.
- Il se décompose en deux facteurs linéaires distincts si et seulement si $\left(\frac{d}{p}\right) = 1$.
- Il est irréductible si et seulement si $\left(\frac{d}{p}\right) = -1$. □

Exercice. Soit d un entier sans facteur carré et soit K le corps quadratique $\mathbf{Q}(\sqrt{d})$. Vérifier :
(i) 2 est ramifié dans K si et seulement si $d \equiv 2$ ou $3 \pmod 4$, c'est-à-dire si et seulement si le discriminant de K est pair.
(ii) 2 est décomposé dans K si et seulement si $d \equiv 1 \pmod 8$.
(iii) 2 est inerte dans K si et seulement si $d \equiv 5 \pmod 8$.

4.5.4 Discriminant et ramification

Nous admettrons l'énoncé suivant :

Théorème 4.53. *Soit K un corps de nombres. Les nombres premiers qui se ramifient dans K sont en nombre fini : ce sont les diviseurs premiers du discriminant D_K.*

Exercice. Soit θ un entier algébrique, T le polynôme unitaire irréductible de θ (qui est à coefficients dans $\mathbf{Z}$) et K le corps de nombres $\mathbf{Q}(\theta)$, . On suppose $\mathbf{Z}[\theta] = \mathbf{Z}_K$. Soit p un nombre premier. On décompose le polynôme T en facteurs irréductibles unitaires sur $\mathbf{Z}_p$:

$$T(X) = \prod_{i=1}^{g} T_i(X)^{e_i} \pmod{p}.$$

Soit $\mathfrak{p}_i$ l'idéal engendré par p et $T_i(\theta)$ dans $\mathbf{Z}_K$. Montrer que la décomposition de l'idéal $p\mathbf{Z}_K$ en produit d'idéaux premiers est

$$p\mathbf{Z}_K = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i}$$

et que l'indice résiduel f_i est égal au degré de T_i.
`Référence`. Voir [2], Théorème 4.8.13.

4.5.5 Classes d'idéaux - théorèmes de finitude

Soit K un corps de nombres. Les idéaux fractionnaires de $\mathbf{Z}_K$ forment un groupe multiplicatif. Les idéaux fractionnaires principaux (c'est-à-dire monogènes) forment un sous-groupe, et le quotient est le *groupe* $\mathrm{Cl}(K)$ *des classes d'idéaux de* K. Dire que deux idéaux fractionnaires $\mathfrak{a}$ et $\mathfrak{b}$ sont *équivalents* signifie qu'il existe $\alpha \in K$, $\alpha \neq 0$, tel que $\mathfrak{a} = \alpha\mathfrak{b}$.

Soit $\mathfrak{a}$ un idéal fractionnaire et soit α un élément non nul de $\mathbf{Z}_K$ tel que $\alpha\mathfrak{a}$ soit un idéal entier. Il résulte de la définition que $\mathfrak{a}$ est équivalent à $\alpha\mathfrak{a}$. Donc toute classe d'équivalence contient un idéal entier.

Rappelons que $M(K)$ désigne la constante de Minkowski du corps K (théorème 4.39).

Proposition 4.54. *Toute classe d'idéaux contient un idéal entier* $\mathfrak{a}$ *de norme* $\mathrm{N}(\mathfrak{a}) \leq M(K)|D_K|^{1/2}$.

Démonstration. Si $\mathfrak{a}_1$ est un idéal dans la classe considérée, si α est un élément non nul de $\mathbf{Z}_K$ tel que l'idéal $\mathfrak{a}_2 = \alpha\mathfrak{a}_1^{-1}$ soit entier, en appliquant le théorème 4.39 à $\mathfrak{a}_2$ on trouve un élément $\beta \in \mathfrak{a}_2$ vérifiant $|\mathrm{N}_{K:\mathbf{Q}}(\beta)| \leq M(K)|D_K|^{1/2}\mathrm{N}(\mathfrak{a}_2)$. Alors $\mathfrak{a} = \beta\mathfrak{a}_2^{-1}$ est équivalent à $\mathfrak{a}_1$ et vérifie la propriété requise.

□

Théorème 4.55 (Minkowski)**.** *Le groupe* $\mathrm{Cl}(K)$ *des classes d'idéaux de* K *est fini.*

Le nombre d'éléments de $\mathrm{Cl}(K)$ est le *nombre de classes* du corps K. On le note $h(K)$. Pour tout idéal fractionnaire $\mathfrak{a}$ l'idéal $\mathfrak{a}^{h(K)}$ est principal.

Par conséquent l'anneau $\mathbf{Z}_K$ est principal si et seulement si $h(K) = 1$.

Démonstration du théorème 4.55. La proposition 4.54 montre qu'il suffit de vérifier qu'il n'y a qu'un nombre fini d'idéaux entiers ayant une norme donnée. Soit donc N un entier non nul (seul l'idéal nul a pour norme 0). Soit $\mathfrak{a}$ un idéal entier de norme N. Alors $\mathfrak{a}$ est d'indice N dans $\mathbf{Z}_K$ (lemme 4.37), donc $\mathfrak{a}$ appartient à l'ensemble fini des idéaux de $\mathbf{Z}_K$ qui contiennent N.

□

Le théorème 4.39 donne une minoration du discriminant d'un corps de nombres : comme la norme de l'idéal $(1) = \mathbf{Z}_K$ vaut 1 on a

$$|D_K| \geq M(K)^{-2}. \tag{4.56}$$

On en déduit $|D_K| > 1$ pour $K \neq \mathbf{Q}$, donc il n'y a pas d'extension de $\mathbf{Q}$ autre que $\mathbf{Q}$ qui ne soit pas ramifiée.

La minoration (4.56) montre aussi que $|D_K|$ tend vers l'infini quand le degré n de K sur $\mathbf{Q}$ tend vers l'infini. Nous allons en déduire :

Corollaire 4.57 (*Hermite*)**.** *Il n'y a qu'un nombre fini de sous-corps de* $\mathbf{C}$ *de discriminant donné.*