Université P. et M. Curie (Paris VI),
Deuxième semestre 2006/2007

Michel Waldschmidt
date de mise à jour: 27/03/2007

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

Mention : Mathématiques et applications
MO11 : Théorie des nombres (12 ECTS)

Troisième partie : Arithmétique des Corps de Nombres

Fascicule 6 : section 3.4 (12 pages)

3.4 Unités d'un corps de nombres

3.4.1 Énoncé du théorème de Dirichlet

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

Lemme 3.14. *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

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

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 $2X^2 + X + 2$.

Soient k un corps de nombres et n son degré. D'après le théorème de l'élément primitif 1.21, 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 :

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

Pour $r_1 + 1 \leq j \leq r_1 + r_2$ le polynôme $X^2 + b_j X + c_j$ 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

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

Pour $1 \leq j \leq r_1$ 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 $1 \leq j \leq r_2$. 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 $z = \Re(z) + i\Im(z)$ et on note encore $\underline{\sigma}$ l'application $\mathbf{Q}$-linéaire de k dans $\mathbf{R}^n$ qui envoie $x \in k$ sur

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

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

Théorème 3.15. *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 $r = r_1 + r_2 - 1$.*

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 $k_{\text{tors}}^\times$ des racines de l'unité contenues dans k, est fini, et d'autre part que le quotient $\mathbf{Z}_k/k_{\text{tors}}^\times$ 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 $a_i \in \mathbf{Z}$ $(1 \leq i \leq r)$. 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 $\mathbf{Z}_k^\times/k_{\text{tors}}^\times$.

La démonstration du théorème 3.15 nécessite quelques préliminaires sur les sous-groupes de $\mathbf{R}^n$.

3.4.2 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 3.16. *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 $0 < |x - y| < 2\epsilon$, 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 3.17. *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 3.17 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 3.17. 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 3.13.

□

Théorème 3.18 (Structure des sous-groupes de $\mathbf{R}^n$). *Soit G un sous-groupe additif 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 discret G'' de G, discret de rang t, tel que G soit la somme directe de G' et G''.*

Démonstration. Pour $\varrho > 0$ notons

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

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 $0 < \varrho \leq \varrho_0$.

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 $\{e_1, \ldots, e_d\}$ 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 $m_i = [x_i]$ $(1 \leq i \leq d)$ et $y = m_1 e_1 + \cdots + m_d e_d$. Alors $y \in G'$ vérifie $\|x - y\| \leq \epsilon$.

Soit maintenant W le sous-espace de $\mathbf{R}^n$ engendré par G. Comme il contient V sa dimension est $d + t$ avec $t \geq 0$. 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'. Sinon il existerait $z \in p(G)$ tel que $0 < \|z\| < \epsilon$ avec $\epsilon = \varrho_0/2$. 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 $\|w - w'\| < \varrho_0$ et $p(w - w') = z \neq 0$, ce qui signifie que $w - w' \in G$ vérifie $w - w' \notin V$ et contredit le fait que $V = V_{\varrho_0}$.

Alors $p(G)$ est un sous-groupe discret de V' de rang t, donc un réseau de V'. On en prend une base $p(y_1), \ldots, p(y_t)$ 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 3.18 permet de préciser la structure des sous-groupes fermés de $\mathbf{R}^n$:

Corollaire 3.19. *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 $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbf{R}^n$. On considère le sous-groupe

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

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 $p_1, \ldots, p_n$, q, avec $q > 0$, tels que

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

(iii) L'un au moins des n nombres $x_1, \ldots, x_n$ est irrationnel.
3. Montrer que G est dense dans $\mathbf{R}^n$ si et seulement si les nombres $1, x_1, \ldots, x_n$ 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

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

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 $\mathrm{rang}_{\mathbf{Z}}(G/G\cap H)\geq 2$.
(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 $\chi(G)\neq\{1\}$.
(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 $\mathbf{R}^n$:

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

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

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

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 3.20. *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

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

convient.

Inversement, si G est contenu dans un sous-espace vectoriel V' de V avec $V'\neq V$, 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 $p(B)\neq p(V)$, donc

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

□

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

$$P_{\mathbf{e}} = \{x_1 e_1 + \cdots + x_n e_n \ ; \ 0 \leq x_i < 1 \ (1 \leq i \leq n)\}$$

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

$$\mathbf{R}^n = \bigcup_{g \in G} (P_{\mathbf{e}} + g) \tag{3.21}$$

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 3.22 (*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 (3.21) 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 3.23. *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 3.22 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 3.23, 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 3.23 à $(1 + \epsilon)B$ avec $\epsilon \to 0$.

3.4.3 Plongements d'un corps de nombres

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

$$(1+|\alpha_1|)\cdots(1+|\alpha_n|). \tag{3.24}$$

Proposition 3.25. *L'image de l'anneau des entiers $\mathbf{Z}_k$ de k par le plongement canonique $\underline{\sigma}$ est un réseau de $\mathbf{R}^n$.*

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 (3.24) 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 3.26. *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 3.25 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

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

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 3.27. *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 3.14 on en déduit :

Lemme 3.28. *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 3.29. *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 (3.24) 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 3.29.

□

On déduit du lemme 3.29

$$\mathbf{Z}_k \cap \ker \lambda = k^\times_{\mathrm{tors}}.$$

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).

3.4.4 Théorème de Dirichlet

Le théorème 3.15 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 3.30. *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 3.30 va utiliser plusieurs lemmes auxiliaires.

Lemme 3.31. *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 (3.24) 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 3.31 que $\mathbf{Z}_k^\times$ est un groupe de type fini, produit direct du groupe fini $k_{\text{tors}}^\times$ par un groupe libre de type fini et de rang $r \leq r_1 + r_2 - 1$:

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

Pour compléter la démonstration des théorèmes 3.30 et 3.15 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 3.20). 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 3.32 que voici.

Lemme 3.32. *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 3.33. *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 3.27), on a $\mu(K) > 2^n v(\underline{\sigma}(\mathbf{Z}_k))$ et il ne reste plus qu'à appliquer le théorème de Minkowski 3.23.

□

Remarque. Sous les hypothèses du lemme 3.33, l'élément α qui est donné par la conclusion satisfait $1 \leq |\mathrm{N}_{k/\mathbf{Q}}(\alpha)| \leq \kappa$.

Démonstration du théorème 3.30. 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 3.33. 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 $(t_1, \dots, , t_{r_1+r_2}) \in H$, 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 3.32 : 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 3.20 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 $\epsilon_1, \dots, \epsilon_r$ 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 $\eta_1, \dots, \eta_r$ un ensemble de r unités de k. On définit le *régulateur* $R(\eta_1, \dots, \eta_r)$ 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 3.34. *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 $\mathbf{Z}_k^\times/k_{\text{tors}}^\times$ engendré par les classes de $\eta_1, \ldots, \eta_r$.

Démonstration. Soit E le sous-groupe de $\mathbf{Z}_k^\times$ engendré par $\eta_1, \ldots, \eta_r$. D'après la proposition 3.13 qui donne la structure des modules sur les anneaux principaux, il existe une base $x_1, \ldots, x_r$ de $\mathbf{Z}_k^\times/k_{\text{tors}}^\times$ et des entiers positifs $a_1, \ldots, a_r$ tels que $a_1x_1, \ldots, a_rx_r$ soit une base de $E/k_{\text{tors}}^\times$. Alors l'indice de $E/k_{\text{tors}}^\times$ dans $\mathbf{Z}_k^\times/k_{\text{tors}}^\times$ 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 $R_k = 1$.