VI
La géométrie des nombres et le groupe des unités

1. Le théorème des unités

Soit K un corps de nombres. Rappelons qu'on note désormais $\mathcal{O}_K$ l'anneau des entiers de K. On note d le degré de K sur $\mathbf{Q}$ et r_1 (resp. r_2) le nombre de places réelles de K (resp. de places complexes non réelles à conjugaison près). On note $\mathcal{D}_K$ le discriminant absolu de K.

Le groupe $\mathcal{O}_K^*$ des éléments inversibles de l'anneau $\mathcal{O}_K$ est le *groupe des unités* de K.

THÉORÈME 1. — *Le groupe $\mathcal{O}_K^*$ est isomorphe au produit d'un groupe cyclique par $\mathbf{Z}^{r_1+r_2-1}$.*

Le théorème 1 est le *théorème des unités* de Dirichlet. Sa démonstration repose sur la théorie de Minkowski.

Il en résulte que les seuls corps de nombres possédant un nombre fini d'unités sont le corps des nombres rationnels et les corps quadratiques imaginaires.

2. Le théorème d'Hermite

C'est le théorème suivant. Il est antérieur au théorème de Minkowski.

THÉORÈME 2. — *Il n'y a qu'un nombre fini (à isomorphisme prs) de corps de nombres de discriminant absolu donné.*

Démonstration. — D'après le corollaire 4 du théorème V-2, il suffit de démontrer qu'il n'y a qu'un nombre fini de corps K de degré d et discriminant $\mathcal{D}_K$ donnés. On peut supposer qu'on a $d > 1$. On peut également supposer que r_1 et r_2 sont donnés.

Lemme 1. — *Soient M un nombre réel > 0 et d un entier > 0. Les entiers algébriques dont tous les conjugés sont majorés en valeur absolue par M n'engendrent qu'un nombre fini de corps de nombres de degré d.*

Démonstration. — Soit K un tel corps de nombres. Soit x un entier algébrique qui l'engendre tel que $|\sigma_i(x)| \leq M$ $(1 \leq i \leq d)$. Le polynôme minimal de x est donné par la formule

$$\prod_i (X - \sigma_i(x)) \in \mathbf{Z}[X].$$

Les coefficients de ce polynôme sont des nombres entiers bornés en termes de d et M puisque les $\sigma_i(x)$ sont bornés en fonctions de M et que ce polynôme est de degré d. Il n'y a qu'un nombre fini de possibilités pour un tel polynôme, puisqu'il n'y qu'un nombre fini de possibilités pour chacun des d coefficients, et donc un nombre fini de possibilités pour $\mathbf{Q}(x) = K$.

Pour obtenir le théorème 1 il suffit de démontrer que K est engendré par un entier algébrique dont les conjugués sont bornés par des nombres ne dépendant que de r_1, r_2 et $\mathcal{D}_K$.

Démontrons-le lorsque K possède au moins une place réelle (*i.e.* $r_1 \geq 1$). Considérons le sous-ensemble X de $\mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$ formé par les éléments $(x_1, ..., x_{r_1}, z_{r_1+1}, ..., z_{r_1+r_2})$ tels que $|x_1| \leq 2^d (\frac{\pi}{2})^{-r_2} \mathcal{D}_K^{1/2}$, $|x_i| \leq \frac{1}{2}$ $(1 < i \leq r_1)$ et $|z_i| \leq \frac{1}{2}$ $(r_1 < i \leq r_1 + r_2)$. C'est un ensemble borné, convexe, symétrique par rapport à l'origine et de volume donné par la formule

$$\mathrm{vol}(X) = 2^{d-r_2+1} \mathcal{D}_K^{1/2} > 2^{d-r_2} \mathcal{D}_K^{1/2}.$$

D'après les propositions V-3 et V-5, il existe $x \in \mathcal{O}_K - \{0\}$ tel que $v_K(x) \in X$. Les conjugués de x sont majorés en valeur absolue par des quantités ne dépendant que de r_1, r_2 et $\mathcal{D}$.

Lemme 2. — *On a* $K = \mathbf{Q}(x)$.
Démonstration. — Il suffit de démontrer qu'on a $\sigma_1(x) \neq \sigma_i(x)$ pour tout $i \neq 1$. En effet le groupe $\mathrm{Gal}(L/\mathbf{Q})$ (où $L/\mathbf{Q}$ est une extension galoisienne qui contient K, voir la leçon VII) permute transitivement les conjugués de x. Le stabilisateur de x dans $\mathrm{Gal}(L/\mathbf{Q})$ est égal à $\mathrm{Gal}(L/\mathbf{Q}(x))$. Ce dernier est égal à $\mathrm{Gal}(L/K)$ si et seulement si $K = \mathbf{Q}(x)$. Si on a $K \neq \mathbf{Q}(x)$, il existe donc $\tau \in \mathrm{Gal}(L/\mathbf{Q}) - \mathrm{Gal}(L/K)$ tel que $\tau(x) = x$. On a alors $\sigma_1(\tau(x)) = \sigma_1(x)$. De plus $\sigma_1 \circ \tau$ et σ_1 définissent des plongements distincts de K dans L puisque $\tau \notin \mathrm{Gal}(L/K)$.

On a $|\sigma_i(x)| \leq \frac{1}{2}$ lorsque $i \neq 1$. Par ailleurs on a $\mathrm{N}_K(x) \in \mathbf{Z}$ puisque x est un entier algébrique. On a

$$|\mathrm{N}_K(x)| = \prod_i |\sigma_i(x)| > 1.$$

On a donc, pour $i \neq 1$,

$$|\sigma_1(x)| \geq 2^{r_1+2r_2-1} > 1 > 1/2 \geq |\sigma_i(x)|.$$

Cela entraîne la relation $\sigma_1(x) \neq \sigma_i(x)$ pour tout $i \neq 1$.

Lorsque K ne possède pas de plongement réel, on peut adapter la démonstration ci-dessus. On considère le sous-ensemble Y de $\mathbf{C}^{r_2}$ formé par les éléments $(z_1, ..., z_{r_2})$ vérifiant $|z_1 - \bar{z}_1| \leq 2^d \frac{8}{\pi} (\frac{\pi}{2})^{-r_2} |\mathcal{D}_K|^{1/2}$, $|z_1 + \bar{z}_1| \leq \frac{1}{2}$ et $|z_i| \leq \frac{1}{2}$ pour $i \neq 1$. C'est aussi un ensemble borné, convexe, symétrique par rapport à l'origine et de volume $\mathrm{vol}(Y)$ vérifiant

$$\mathrm{vol}(Y) > 2^{d-r_2} |\mathcal{D}_K|^{1/2}.$$

Il existe donc $y \in \mathcal{O}_K - \{0\}$ tel que $v_K(y) \in Y$.

Lemme 3. — *On a* $K = \mathbf{Q}(y)$.
Démonstration. — En adaptant les arguments du lemme 2 on obtient qu'on a $|\sigma_1(y)| = |\bar{\sigma}_1(y)| \geq 1$. Par conséquent on a $\sigma_1(y) \neq \sigma_i(y)$ et $\sigma_1(y) \neq \bar{\sigma}_i(y)$ pour tout $i \neq 1$. Il reste à montrer qu'on a $\sigma_1(y) \neq \bar{\sigma}_1(y)$, c'est-à-dire $\sigma_1(y)$ non réel. Cela résulte des conditions $|\sigma_1(y) + \bar{\sigma}_1(y)| \leq \frac{1}{2}$ et $|\sigma_1(y)| = |\bar{\sigma}_1(y)| \geq 1$ qui ne peuvent être satisfaites par deux nombres réels égaux.

3. Démonstration du théorème des unités

Commençons par caractériser les unités de K parmi les entiers de K.

Proposition 1. — *Soit K un corps de nombres. Les unités de K coïncident avec les entiers de K de norme* 1 *ou* -1.
Démonstration. — Soit x une unité de K. Les nombres rationnels $\mathrm{N}_{K/\mathbf{Q}}(x)$ et $\mathrm{N}_{K/\mathbf{Q}}(x^{-1})$ sont des entiers inverses l'un de l'autre. On a donc $\mathrm{N}_{K/\mathbf{Q}}(x) \in \{-1, 1\}$.

Soit $x \in \mathcal{O}_K$ de norme égale à 1 ou -1. On a $x^n + a_{n-1}x^{n-1} + ... + a_1 x + \epsilon = 0$ avec $\epsilon \in \{-1, 1\}$ et avec $a_i \in \mathbf{Z}$ ($i \in \{1, 2, ..., n-1\}$). La quantité

$$y = -\epsilon(x^{n-1} + a_{n-1}x^{n-2} + ... + a_1)$$

est un entier algébrique. On a $xy = 1$ si bien que x est une unité de K.

L'application $K^* \longrightarrow \mathbf{R}^{r_1+r_2}$ qui à x associe $L(x) = (\log(|\sigma_1(x)|), ..., \log(|\sigma_{r_1+r_2}(x)|))$ est un homomorphisme de groupes (relativement à la multiplication et à l'addition respectivement) qu'on appelle le *plongement logarithmique* de K^*.

Lemme 4. — *L'image réciproque dans $\mathcal{O}_K$ par L d'un ensemble compact est un ensemble fini (autrement dit L restreint à $\mathcal{O}_K$ est une application propre).*
Démonstration. — Soit C un sous ensemble compact de $\mathbf{R}^{r_1+r_2}$. Il existe des nombre réels strictement positifs α et β tels que pour tout $x \in L^{-1}(C)$ on ait $\alpha < |\sigma_i(x)| < \beta$ pour toute place σ_i de K dans $\mathbf{C}$. Les fonction symétriques élémentaires de degré $\leq d$ en les $\sigma_i(x)$ sont donc bornées en valeur absolue. Le polynôme minimal de x est à coefficients dans $\mathbf{Z}$ et ces coefficients sont donnés par les fonctions symétriques élémentaires de degré $\leq d$ en les $\sigma_i(x)$. Il appartient donc à un ensemble fini ne dépendant que de α, β et d. L'entier algébrique x appartient à l'ensemble fini des racines de tels polynômes. On en déduit que l'ensemble $L^{-1}(C)$ est fini.

Donnons quelques conséquences du lemme 4.

Lemme 5. — *L'ensemble des unités contenues dans le noyau de L constitue un groupe cyclique.*
Démonstration. — C'est un groupe fini G d'après le lemme 4 puisque c'est l'image réciproque de $\{0\}$ qui est un ensemble fini et donc compact. Tout élément de G est donc d'ordre fini. C'est donc une racine de l'unité. Le groupe G est donc un sous-groupe fini du groupe cyclique des racines n-ièmes de l'unité pour n approprié (par exemple l'exposant du groupe G). C'est donc un groupe cyclique.

Lemme 6. — *L'image par L de $\mathcal{O}_K^*$ est un sous-groupe discret de l'hyperplan H de $\mathbf{R}^{r_1+r_2}$ formé par les éléments $(x_1, ..., x_{r_1+r_2})$ vérifiant*

$$x_1 + ... + x_{r_1} + 2x_{r_1+1} + ... + 2x_{r_1+r_2} = 0.$$

Démonstration. — Soit $x \in \mathcal{O}_K^*$. On a $|\mathrm{N}_{K/\mathbf{Q}}(x)| = 1$ et donc $\log(|\mathrm{N}_{K/\mathbf{Q}}(x)|) = 0$. Par ailleurs on a

$$\log(|\mathrm{N}_{K/\mathbf{Q}}(x)| = \log(|\sigma_1(x)|) + ... + \log(|\sigma_{r_1}(x)|) + 2\log(|\sigma_{r_1+r_2}(x)|) + ... + 2\log(|\sigma_{r_1+r_2}(x)|).$$

On a donc $L(\mathcal{O}_K^*) \subset H$.

Le fait que $L(\mathcal{O}_K^*)$ soit un sous-groupe discret résulte directement du lemme 4.

Corollaire . — *Le groupe $L(\mathcal{O}_K^*)$ est engendré par au plus $r_1 + r_2 - 1$ éléments.*
Démonstration. — En effet un sous-groupe discret d'un espace vectoriel réel de dimension n est engendré par au plus n éléments. Par application à H, ce fait on obtient le résultat.

Pour démontrer le théorème des unités, il reste à établir le résultat suivant.

Proposition 2. — *Le groupe $L(\mathcal{O}_K^*)$ contient $r_1 + r_2 - 1$ éléments $\mathbf{Z}$-linéairement indépendants.*
Démonstration. — Soit f une forme linéaire non nulle sur H. Prolongeons-la en une forme linéaire sur $\mathbf{R}^{r_1+r_2}$ nulle sur $\{0\}^{r_1+r_2-1} \times \mathbf{R}$. Un tel prolongement existe et est unique. On va démontrer qu'il existe une unité x de $\mathcal{O}_K$ telle que $f(L(x)) \neq 0$, ce qui suffit à démontrer l'indépendance linéaire cherchée.

Pour cela il suffit de trouver deux entiers x_1 et x_2 tels que $f(L(x_1)) \neq f(L(x_2))$ et $x_1\mathcal{O}_K = x_2\mathcal{O}_K$. Cette existence est établie si on peut trouver une infinité d'entiers de $\mathcal{O}_K$ d'images distinctes par $f \circ L$ et de norme bornée puisqu'il n'existe qu'un nombre fini d'idéaux de $\mathcal{O}_K$ de norme bornée (proposition V-3).

Soit α un nombre réel vérifiant

$$\alpha > 2^{d-r_1}(\frac{1}{2\pi})^{r_2}|\mathcal{D}_K|^{1/2}.$$

Pour chaque entier $k \geq 0$ on va trouver un élément $x_k \in \mathcal{O}_K$ tel que $\mathrm{N}_{K/\mathbf{Q}}(x_k) \leq \alpha$ et tel que les images des x_k par $f \circ L$ soient deux à deux distinctes.

Soit β un nombre réel $> \log(\alpha)\,||f||_1$, où on a posé

$$||f||_1 = \max_{|x_1|\leq 1,...,|x_{r_1+r_2}|\leq 1}|f(x_1, ..., x_{r_1+r_2})|.$$

Soit k un entier > 0. Soit $\Lambda_k = (\log(\lambda_1), ..., \log(\lambda_{r_1+r_2})) \in \mathbf{R}^{r_1+r_2}$ vérifiant les égalités

$$f(\Lambda_k) = 2\beta k \qquad \text{et} \qquad \prod_{i=1}^{r_1}\lambda_i \prod_{i=r_1+1}^{r_1+r_2}\lambda_i^2 = \alpha.$$

Notons X_k le sous-ensemble de l'espace $\mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$ constitué par les $(r_1 + r_2)$-uplets $(x_1, ..., x_{r_1}, z_{r_1+1}, ..., z_{r_1+r_2})$ vérifiant $|x_i| \leq \lambda_i$ et $|z_i| \leq \lambda_i$. C'est un ensemble compact, convexe, symétrique par rapport à 0 et de volume

$$\mathrm{vol}(X_k) = \prod_{i=1}^{r_1} 2|\lambda_i| \prod_{i=r_1+1}^{r_1+r_2} \pi|\lambda_i|^2 = 2^{r_1}\pi^{r_2}\alpha > 2^d 2^{-r_2}|\mathcal{D}_K|^{1/2}.$$

En comparant ce volume à celui du réseau $v_K(\mathcal{O}_K)$, on établit l'existence, grâce à la proposition V-5 (appliquée à $X = X_k$ et $L = v(\mathcal{O}_K)$), d'un élément non nul $x_k \in v_K(\mathcal{O}_K) \cap X_k$. Soit $a_k \in \mathcal{O}_K$ tel que $v_K(a_k) = x_k$. On alors

$$1 \leq |\mathrm{N}_{K/\mathbf{Q}}(a_k)| = \prod_i |\sigma_i(a_k)| \leq \prod_{i=1}^{r_1} \lambda_i \prod_{i=r_1+1}^{r_1+r_2} \lambda_i^2 = \alpha.$$

De plus on a

$$\frac{\lambda_i}{\alpha} \leq \prod_{j\neq i} \lambda_j^{-1} \leq \mathrm{N}_{K/\mathbf{Q}}(a_k) \prod_{j\neq i} |\sigma_j(a_k)|^{-1} \leq \sigma_i(a_k)| \leq \lambda_i.$$

On a donc

$$0 \leq \log(\lambda_i) - \log(\sigma_i(a_k)) \leq \log(\alpha).$$

Or $(\log(\lambda_i) - \log(|\sigma_i(a_k)|)$ est la i-ième coordonnée de $(\Lambda_k - L(a_k))$. On en déduit les relations

$$|f(L(a_k)) - 2\beta k| = |f(L(a_k)) - f(\Lambda_k)| = f(L(a_k) - \Lambda_k) \leq ||f||_1 \log(\alpha) < \beta,$$

car on a, pour k réel > 0,

$$\max_{|x_1|\leq k,...,|x_{r_1+r_2}|\leq k} f(x_1, ..., x_{r_1+r_2}) = k||f||_1.$$

Cela entraîne

$$... < f(L(a_{k-1})) < (2k-1)\beta < f(L(a_k)) < (2k+1)\beta < f(L(a_{k+1})) < ...$$

Les $f(L(a_k))$ sont donc deux à deux distincts et les x_k sont de norme $\leq \alpha$. Cela termine la démonstration de la proposition 2.

Le théorème des unités résulte de la proposition 2, du lemme 7 et du lemme 8 puisqu'on a établi l'existence d'une suite exacte :

$$0 \longrightarrow U_K \longrightarrow \mathcal{O}_K^* \longrightarrow L(\mathcal{O}_K^*) \longrightarrow 0,$$

où U_K est le sous-groupe cyclique de $\mathcal{O}_K^*$ formé par les racines de l'unité de K, et $L(\mathcal{O}_K^*)$ est un groupe isomorphe à $\mathbf{Z}^{r_1+r_2-1}$.

Remarques. — On formulera un énoncé en termes d'idèles qui contient simultanément le théorème des unités et la finitude du nombre de classes.

Le lemme 6 n'est pas contenu dans le théorème des unités. C'est un énoncé dont on aura besoin lors de notre étude des idèles.

Les racines de l'unité de K sont en nombre fini d'après le lemme 5. Ce n'était pas un résultat évident *a priori*. En effet on peut trouver des anneaux de Dedekind qui possèdent une infinité de racines de l'unité. Ce nombre fini de racine de l'unité est, comme le nombre de classe, un invariant important du corps K.

Parmi les unités on a la caractérisation suivante des racines de l'unité dans K : Ce sont les élément de K dont toutes les valeurs absolues (*i.e.* archimédiennes et non archimédiennes) sont égales à 1. Cela n'était pas *a priori* évident et résulte des lemmes 4 et 5.

Soit $(u_1, ..., u_{r_1+r_2-1})$ un système de générateurs de $L(\mathcal{O}_K^*)$. Une image réciproque par L de cet élément est un *système fondamental d'unités* de $\mathcal{O}_K^*$. Le volume du réseau $L(\mathcal{O}_K^*)$ de H est le *régulateur* du corps K. Il interviendra, ainsi que le nombre de classes, le théorème des unités, le nombres de racines de l'unité dans la formule du nombre de classes. De façon plus précise, si on pose $u_i = (\log|(\sigma_1(x_i))|, ..., \log|(\sigma_{r_1+r_2}(x_i))|)$, le régulateur est donné par la formule

$$|\det{}_{1\leq i,j\leq r_1+r_2-1}(\log(|\sigma_j(x_i)|)|.$$

Remarque . — Le régulateur n'est pas en général un nombre algébrique puisqu'il est construit à partir de logarithmes.

4. Les S-unités

Voici une autre caractérisation des unités de K : Ce sont les éléments de K^* sur lesquels toutes les valuations discrètes de K s'annulent.

Relachons cette condition de la façon suivante. Soit S un ensemble de valeurs absolues normalisées de K contenant l'ensemble S_∞ des valeurs absolues archimédiennes de K (qui sont au nombre de $r_1 + r_2$ car elles coïncident avec les places complexes à conjugaison près).

les valeurs absolues archimédiennes. Rappelons qu'on normalise les places réelles en considérant la valeur absolue usuelle dans $\mathbf{R}$ et qu'on normalise les places complexes en considérant le carré du module. Le groupe K_S des *S-unités* de K est l'ensemble des éléments x de K^* qui vérifient $|x|_v = 1$ pour tout $|.|_v \notin S$. Il contient le groupe des unités.

Notons S_∞ l'ensemble des valeurs absolues archimédiennes de K (qui sont au nombre de r_1+r_2 car elles coïncident avec les places complexes à conjugaison près). Les valuations de K définissent des homonorphismes de groupes $K_S \longrightarrow \mathbf{Z}$. En considérant toutes les valuations associées aux valeurs absolues de $S - S_\infty$, on en déduit l'existence d'une suite exacte

$$1 \longrightarrow \mathcal{O}_K^* \longrightarrow K_S \longrightarrow \mathbf{Z}^{(S-S_\infty)} \longrightarrow 0.$$

Il en résulte, en combinant avec le théorème des unités, que K_S est isomorphe au produit d'un groupe cyclique et de $\mathbf{Z}^{|S|-1|}$. Considérons l'application $\Lambda_S : K_S \longrightarrow \mathbf{R}^{(S)}$ qui à x associe $(\log(|x|_v))_{v\in S}$. Soit T un sous-ensemble de S. Considérons la surjection canonique $\pi_T : \mathbf{R}^{(S)} \longrightarrow \mathbf{R}^{(T)}$; On a $\pi_{S_\infty} \circ \Lambda_S = \Lambda$.

L'homomorphisme Λ_S jouit de propriété analogues à celles établies pour Λ dans la section précédente.

PROPOSITION 3. — *Le noyau de Λ_S est constitué par les racines de l'unité de K. L'image de Λ_S est contenue dans l'hyperplan $\pi_{S_\infty}^{-1}(H)$ de $\mathbf{R}^{(S)}$. Le groupe $\Lambda_S(K_S)$ est un sous-groupe discret de $\mathbf{R}^{(S)}$ isomorphe à $\mathbf{Z}^{|S|-1}$.*

Démonstration. — La première assertion est une conséquence du lemme 5, puisque le noyau de Λ_S est contenu dans le noyau de Λ et puisque les valeurs absolues non archimédiennes des racines de l'unité valent toutes 1.

La deuxième assertion résulte de l'identité $\pi_{S_\infty} \circ \Lambda_S = \Lambda$.

La troisième assertion résulte du fait que $\pi_{S-S_\infty} \circ \Lambda_S(K_S)$ est un réseau de $\mathbf{R}^{(S-S_\infty)}$ (la projection sur chaque composante est isomorphe à $\mathbf{Z}$) et du lemme 6.