Le théorème des unités

Mathilde Gerbelli-Gauthier

19 juin 2013

1 Introduction

Le Théorème des unités de Dirichlet est un résultat de théorie algébrique des nombres qui décrit la structure du groupe des unités d'un corps de nombres. Une de ses applications est la caractérisation des solutions à l'équation Diophantienne appellée équation de Pell :

$$x^2 - Dy^2 = 1 \qquad D \text{ est un entier sans facteur carré.}$$

Le problème de trouver des solutions entières à cette équation remonte à l'antiquité, où elles auraient servi à l'approximation de nombres irrationnels [2, XII]. En effet, les couples d'entiers (a, b) satisfaisant l'équiation de Pell permettent d'obtenir des séquences d'approximations rationelles de $\sqrt{D}$ d'une précision remarquable. De plus, toutes ces solutions peuvent être obetenues a partir d'une solution fondamentale (a_0, b_0). Il est possible que Diophante ait lui même été au courant de cette propriété pour certaines valeurs de D, et c'est aussi le cas du mathématicien Indien Brahmegupta [2, XII]. Il fallut cependant attendre les travaux de Lagrange, qui établit complètement le lien entre l'équation de Pell et l'approximation de $\sqrt{D}$ par fractions continues, pour une solution complète [1, 0.1].

Une autre façon d'aborder la recherche des solutions à cette équation appartient à la théorie algébrique des nombres. En effet, comme c'est le cas pour de nombreuses équations Diophantiennes, il est possible de démontrer l'existence ou non de solutions en factorisant le côté gauche de l'équation dans un ensemble de nombres plus grand que $\mathbb{Z}$. Dans le cas de l'équation de Pell, on ajoute $\sqrt{D}$ à $\mathbb{Z}$ et l'équation devient

$$(x + y\sqrt{D})(x - y\sqrt{D}) = 1.$$

La recherche de solutions entières se mue en la recherche d'éléments inversibles dans $\mathbb{Z}[\sqrt{D}]$.

Bien sur, les seuls éléments inversibles de $\mathbb{Z}$ sont ± 1, mais dans les ensembles comme $\mathbb{Z}[\sqrt{D}]$, appelés anneaux d'entiers, la factorisation est plus exotique. Par exemple, le théorème fondamental de l'arithmétique, qui garantit la factorisation unique des entiers en nombres premiers, n'a pas toujours d'équivalent. De plus, cette factorisation n'est unique qu'à l'unité près, ce qui dans $\mathbb{Z}$ n'autorise qu'un changement de signe. Ce n'est pas toujours le cas dans

un anneau d'entiers, comme le montre l'exemple suivant dans $\mathbb{Z}[\sqrt{5}]$:

$$(9 + 4\sqrt{5})(9 - 4\sqrt{5}) = 81 - 5 \cdot 16 = 1.$$

Le nombre $9+4\sqrt{5}$ possède donc un inverse dans $\mathbb{Z}[\sqrt{5}]$, ce qui en fait une unité. Il correspond également à la solution $(9, 4)$ de l'équation de Pell pour $D = 5$, dont on a dit plus haut qu'on pouvait en produire une infinité. Cela laisse à croire qu'il existe des anneaux d'entiers contenant une infinité d'unités. C'est exactement ce qu'a prouvé Dirichlet en 1840 [3, §5].

Théorème (Dirichlet). *Soient K un corps de nombres, r_1 le nombre de plongements réels de K, r_2 son nombre de paires de plongements complexes, et $r = r_1 + r_2 - 1$. Le groupe $\mathcal{O}_K*$ des unités de K est isomorphe à $\mathbb{Z}^r \times G$, où G est un groupe cyclique fini, formé par les racines de l'unité contenues dans K.*

Ce théorème admirable implique que pour tout anneau d'entiers d'un corps de nombres, il existe un *système fondamental d'unités* $(u_1, ..., u_r)$ de rang maximal tel que chaque unité de l'anneau d'entiers s'exprime d'une façon et d'une seule comme

$$\zeta u_1^{e_1} \cdot ... \cdot u_r^{e_r} \qquad \zeta^k = 1 \quad e_i \in \mathbb{Z}.$$

Le résultat permet donc non seulement de caractériser toutes les solutions de l'équation de Pell, mais aussi de déterminer la structure du groupe des unités de n'importe quel corps de nombres. La preuve fait intervenir des éléments d'algèbre et de topologie, et repose sur l'étude de la géométrie des corps de nombres.

2 Préliminaires

2.1 Corps de nombres

Définition Un *corps de nombres* K est une extension de $\mathbb{Q}$ de degré fini n, c'est-à-dire un corps contenant $\mathbb{Q}$ et qui est un $\mathbb{Q}$-espace vectoriel de dimension finie.

Les élements de K sont algébriques sur $\mathbb{Q}$, c'est-à-dire qu'ils satisfont un un polynôme unitaire irréductible à coefficients dans $\mathbb{Q}$, qu'on appelle le *polynôme minimal*.

Définition Un élément de K est *entier* si les coefficients de son polynôme minimal sont dans $\mathbb{Z}$.

L'ensemble des élements entiers de K est un anneau que l'on dénote $\mathcal{O}_K$. On s'intéresse a sa structure multiplicative, et particulièrement aux éléments de $\mathcal{O}_K$ dont l'inverse multiplicatif est aussi un entier.

Définition Les *unités* de K sont les unités de $\mathcal{O}_K$, c'est à dire les éléments qui ont un inverse multiplicatif dans $\mathcal{O}_K$. Elles forment un groupe que l'on dénote $\mathcal{O}_K^*$.

BASES Le corps K est de caractéristique 0 et contient donc une copie de $\mathbb{Q}$; de même $\mathcal{O}_K$ contient une copie de $\mathbb{Z}$. De plus, $\mathcal{O}_K$ est un module libre de rang n sur $\mathbb{Z}$ [4, §2.8]. On appelle $\mathbb{Z}$-*base* de $\mathcal{O}_K$ un système $(x_1, ..., x_n)$ générateur de $\mathcal{O}_K$ comme $\mathbb{Z}$-module.

PROPOSITION 1. *Soit K un corps de nombres, $\mathcal{O}_K$ son anneau des entiers, et $(x_1, ..., x_n)$ une $\mathbb{Z}$-base de $\mathcal{O}_K$. Alors $(x_1, ..., x_n)$ est une base du $\mathbb{Q}$-espace vectoriel K.*

Démonstration. Puisque $(x_1, ..., x_n)$ a la bonne cardinalité pour être une base, il suffit de montrer que les x_i sont linéairement indépendants sur $\mathbb{Q}$. Supposons qu'au contraire on aie $a_1x_1 + ... + a_nx_n = 0$ pour des $a_i \in \mathbb{Q}$, pas tous nuls. Soit l, le plus petit commun multiple des dénominateurs des a_i. Alors $la_1x_1 + ... + la_nx_n = 0$ et les la_i sont dans $\mathbb{Z}$, ce qui contredit que $(x_1, ..., x_n)$ est une $\mathbb{Z}$ base de $\mathcal{O}_K$. □

Soit K un corps de nombre, $x \in K$. L'application $m_x : K \mapsto K$ donnée par $m_x(y) = xy$ est une transformation linéaire du $\mathbb{Q}$-espace vectoriel K. En effet, pour $x, y, z \in K$, $\alpha \in \mathbb{Q}$, a $x(\alpha y) = \alpha(xy)$ et $x(y + z) = xy + xz$. Puisque tout élément non-nul de K a un inverse, la transformation linéaire m_x est toujours inversible.

On peut choisir une base $(e_1, ..., e_n)$ de K et considérer la matrice $M_{e,x}$ de la multiplication par x dans la base e ; ses entrées sont bien sûr dans $\mathbb{Q}$. Si $(e_1, ..., e_n)$ est de surcroît une $\mathbb{Z}$-base de $\mathcal{O}_K$ et que $x \in \mathcal{O}_K$, les entrées de $M_{e,x}$ sont des entiers. En effet, pour tout vecteur e_i de la $\mathbb{Z}-$base, $xe_i \in \mathcal{O}_K$. On peut donc l'écrire

$$xe_i = \sum_{i=1}^{n} a_{ij}e_j \qquad a_{ij} \in \mathbb{Z}.$$

La matrice de la transformation est donc donnée par (a_{ij}) et ses entrées sont dans $\mathbb{Z}$.

DÉFINITION Soit K un corps de nombres, $x \in K$. La *norme* de x, qu'on dénote $N(x)$, est le déterminant de la transformation linéaire m_x.

REMARQUE La norme $N(x)$ est un élement de $\mathbb{Q}$ et est indépendante de la base choisie pour K ; si si $x \in \mathcal{O}_K$, $N(x) \in \mathbb{Z}$. On déduit également que $N(xy) = N(x)N(y)$.

De plus, on peut identifier le polynôme minimal $p_{m_x}(X)$ de la transformation linéaire m_x avec le polynôme minimal $p_x(X)$ du nombre algébrique x. En effet, on sait que les deux sont moniques et irréductibles sur $\mathbb{Q}$, et que $p_x(m_x) = 0$ puisque $p_x(m_x)[1] = p_x(x) = 0$. Cette identification permet de conclure que si d est le degré de p_{m_x}, alors d divise n et $N(x) = (-1)^n a_0^{n/d}$ ou a_0 est le terme constant de p_{m_x}. Cela résulte du fait que dans un corps de nombres, le polynome charactéristique χ_{m_x} (dont le terme constant est le déterminant de m_x) est une puissance du polynôme minimal. Pour plus de détails, voir [4, §2.6].

On note que le terme constant d'un polynôme est le produit de toutes ses racines et que dans le cas de $p(X)$, toutes les racines existent dans $\mathbb{C}$. On obtient donc une nouvelle défintition équivalente de la norme : $N(x)$ est le produit des racines du polynôme minimal dans $\mathbb{C}$, élevées à la puissance n/d.

PROPOSITION 2. *Un élement $x \in \mathcal{O}_K$ est une unité si et seulement si $N(x) = \pm 1$.*

Démonstration. On suppose d'abord que x possède un inverse dans $\mathcal{O}_K$. Puisque la norme est multiplicative, $N(x)N(x^{-1}) = N(1) = 1$, et comme $N(x), N(x^{-1}) \in \mathbb{Z}$, $N(x) = \pm 1$.

Réciproquement, si $N(x) = \pm 1$, le polynôme minmal de x est de la forme $x^n + a_{n-1}x^{n-1} + ... + a_1 x \pm 1$. On a donc $x^n + a_{n-1}x^{n-1} + ... + a_1 x = \mp 1$, et l'élément $\pm(x^{n-1} + a_{n-1}x^{n-2} + ... + a_1)$ est l'inverse de x dans $\mathcal{O}_K$. □

Exemples : corps quadratiques réels [4, §4.6] Les corps de nombres correspondant aux solutions de l'équation de Pell sont les corps quadratiques *réels* de la forme $\mathbb{Q}(\sqrt{D})$ où D est un entier positif sans facteur carré. L'anneau des entiers dépend de la valeur de D modulo 4.

$$\mathcal{O}_{\mathbb{Q}(\sqrt{D})} = \begin{cases} \mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right] & D \equiv 1 \mod 4 \\ \mathbb{Z}[\sqrt{D}] & D \equiv 2, 3 \mod 4 \end{cases}$$

Par exemple, dans le corps quadratique réel $\mathbb{Q}(\sqrt{3})$, l'anneau des entiers est

$$\mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3} \mid a, b \in \mathbb{Z}\}.$$

La norme de l'élément $\alpha = a + b\sqrt{3}$ est donné par $\alpha\bar{\alpha} = a^2 - 3b^2$. On peut voir que l'élément $2 + \sqrt{3}$ est une unité. De plus, l'élement $(2 + \sqrt{3})^2 = 7 + 4\sqrt{3}$ est également une unité, et il en va ainsi pour toutes les puissances positives et négatives de $2 + \sqrt{3}$. On voit ici une illustration du théorème des unités pour les corps quadratiques réels : le groupe $\mathcal{O}_K^*$ est isomorphe à $\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Corps quadratiques imaginaires [4, §4.5] Les unités sont différentes dans un corps quadratique *imaginaire*, où D est négatif. Par exemple, dans $\mathbb{Q}(\sqrt{-3})$:

$$\mathcal{O}_{\mathbb{Q}(\sqrt{-3})} = \mathbb{Z}\left[\frac{1+\sqrt{3}}{2}\right] = \left\{a + b\frac{1+\sqrt{-3}}{2} \mid a, b \in \mathbb{Z}\right\}.$$

Dans ce cas, $N(a + b\frac{1+\sqrt{-3}}{2}) = a^2 + ab + b^2$ et les unités correspondent aux solutions entières de $x^2 + xy + y^2 = \pm 1$. Si x et y sont tous deux du même signe, il n'y a que quatre solutions possibles :

$$(\pm 1, 0) \to \pm 1 \quad (0, \pm 1) \to \frac{\pm(1 + \sqrt{-3})}{2}.$$

Si x et y sont de signes opposés, les seules solutions possibles sont :

$$(1, -1) \to \frac{1 - \sqrt{-3}}{2} \quad (-1, 1) \to \frac{-1 + \sqrt{-3}}{2}.$$

On remarque que toutes les solutions sont des racines sixièmes de l'unité ; cette observation va être confirmée pour les corps quadratiques imaginaires par le théorème des unités.

Corps cubiques Il existe deux structures possible pour le groupe des unités d'un corps cubique. Cela dépend du nombre de racines réeles du polynôme cubique dont on adjoint la racine : il peut avoir trois racines réelles ou une seule [1].

Trois racines dans $\mathbb{R}$ Un exemple d'un tel corps est $\mathbb{Q}(\alpha)$ où α est une racine du polynôme $x^3 + x^2 - 2x - 1$. Dans ce cas, on a

$$\mathcal{O}_{\mathbb{Q}(\alpha)} = \mathbb{Z}[\alpha, \alpha^2 - 2] = \{a + b\alpha + c(\alpha^2 - 2) \mid a, b, c \in \mathbb{Z}\}.$$

Dans cet anneau, en plus de ± 1, on a deux unités fondamentales : $\alpha + 1$ et $\alpha^2 - 1$, et $\mathcal{O}^*_{\mathbb{Q}(\alpha)}$ est donc isomorphe à $\mathbb{Z}^2 \times \mathbb{Z}/2\mathbb{Z}$.

Une seule racine dans $\mathbb{R}$ La seconde classe d'exemples provient des polynômes cubiques ayant une seule racine réelle. Le corps de cubique $\mathbb{Q}(\sqrt[3]{2})$ en est une illustration. L'anneau des entiers est de la forme :

$$\mathcal{O}_{\mathbb{Q}(\sqrt[3]{2})} = \mathbb{Z}[\sqrt[3]{2}, \sqrt[3]{4}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Z}\}.$$

La norme est

$$N(a + b\sqrt[3]{2} + c\sqrt[3]{4}) = a^3 + 2b^3 + 4c^3 - 6abc.$$

L'unique unité fondamentale est $\sqrt[3]{2} - 1$; elle correspond à la solution (-1,1,0) de l'équation $x^3 + 2y^3 + 4z^3 - 6xyz$. Le groupe $\mathcal{O}^*_{\sqrt[3]{-2}}$ est donc isomorphe à $\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Dans les exemples qu'on vient de voir, le sous-groupe de $\mathcal{O}_K$ formé des racines de l'unité était cyclique (d'ordre 2 ou 6). C'est en fait le case dans n'importe quel corps.

Proposition 3. *Soit K un corps, et G, un sous-groupe fini du groupe multiplicatif K^*. Alors G est cyclique.*

Démonstration. Le groupe G est abélien et fini, il est donc isomorphe à $\mathbb{Z}/_{a_1\mathbb{Z}} \times \mathbb{Z}/_{a_2\mathbb{Z}} \times ... \times \mathbb{Z}/_{a_n\mathbb{Z}}$ avec $a_1 \mid a_2 \mid ... \mid a_n$. On en déduit l'existence d'un élement $g = (0, 0, ..., 1)$ d'ordre a_n dans G. D'autre part, $h^{a_n} = 1$ pour tout $h \in G$. Comme K est un corps, le polynnôme $x^{a_n} = 1$ a au plus a_n racines dans K. Donc G contient précisément a_n élements, soient les puissances de g. □

2.2 Réseaux

Les exemples ci-dessus ont illustré une variéte de structures possibles pour le groupe d'unités de $\mathcal{O}_K$. Le constat général va être que dans tous les corps de nombres, les unités sont en nombre aussi grand que le permet la géométrie de $\mathcal{O}_K$. Afin de préciser la notion d'"aussi grand que possible", on va étudier les propriétés géométriques de $\mathcal{O}_K$ quand il est plongé dans $\mathbb{R}^n$ de façon naturelle. Pour ce faire, on va d'abord démontrer quelques résultats

1. Les calculs de cette section ont été réalisés à l'aide de la fonction `bnfclassunit` de PARI.

sur les sous-groupes de $\mathbb{R}^n$ à l'aide d'outis de topologie et d'analyse. Cette section est basée sur [4, §4.1].

DÉFINITION Un sous-groupe G de $\mathbb{R}^n$ est *discret* si pour toute partie compacte B de $\mathbb{R}^n$, l'intersection $B \cap G$ contient un nombre fini d'éléments.

Un exemple de sous-groupe discret de $\mathbb{R}^n$ est $\mathbb{Z}^n$, et la proposition suivante va démontrer que, comme le dit Samuel, c'est a peu près le seul.

PROPOSITION 4. *Soit G, un sous-groupe discret de $\mathbb{R}^n$. Alors G est un $\mathbb{Z}$-module libre engendré par r vecteurs linéairemenet indépendants sur $\mathbb{R}$.*

Démonstration. On choisit un ensemble $(e_1, ..., e_r)$ d'éléments de G qui sont linéairement indépendants, et tels que r soit maximal, et on appelle P le parallélotope fermé de $\mathbb{R}^n$ dont les côtés sont les e_i. P est compact et ne contient donc qu'un nombre fini d'éléments de G. Soit $x \in G$; par la maximalité de r, on peut écrire $x = \sum_i \lambda_i e_i$. On définit ensuite, pour tout $j \in \mathbb{Z}$, l'élément x_j :

$$x_j = jx - \sum_{i=1}^{r} [j\lambda_i] e_i = \sum_{i=1}^{r} (j\lambda_i - [j\lambda_i]) e_i \qquad ([a] \text{ est la partie entière de } a).$$

On voit que $x_j \in P \cap G$ puisque les coefficients sont inférieurs à 1. Etant donné que en particulier

$$x = 1 \cdot x - \sum_i [1 \cdot \lambda_i] e_i + \sum_i [1 \cdot \lambda_i] e_i = x_1 + \sum_i [\lambda_i] e_i.$$

on voit que x est la somme d'élements de $P \cap G$. Comme c'est vrai pour tout x, la finitude de $P \cap G$ implique que G est engendré sur $\mathbb{Z}$ par un nombre fini d'élements. D'autre part, cette finitude montre qu'on a deux entiers j, h tels que

$$x_j = x_h \quad \Rightarrow \quad (j-h)\lambda_i = [j\lambda_i] - [h\lambda_i]$$

Ceci montre que les λ_i sont rationnels. G est donc engendré par un nombre fini d'élements qui sont des combinaisons linéaires des (e_i) à coefficients dans $\mathbb{Q}$. Le groupe G est donc un sous-groupe d'indice fini de $\sum \mathbb{Z} e_i$ qui contient les e_i. C'est donc un $\mathbb{Z}$-module libre de rang r. □

DÉFINITION Soit G un sous-groupe discret de $\mathbb{R}^n$, et r son rang. Si r est maximal, on appelle G est un *réseau*.

DÉFINITION Soit Γ un réseau et $(e_1, ..., e_n)$, une $\mathbb{Z}$-base de Γ. On appelle le parallélotope

$$P_e = \{\sum_{i=1}^{n} \alpha_i e_i \ \mid \ 0 \leq \alpha_i < 1\}$$

le *parallélotope fondamental* de Γ pour la base e.

Le parallélotopte fondamental correspond à un quotient $\mathbb{R}^n/\Gamma$; chaque point de $\mathbb{R}^n$ est donc congru modulo Γ à un unique point de P_e. Le parallélotope fondamental est bien sûr dépendant de la base choisie, mais nous allons maintenant démontrer que son volume ne l'est pas.

PROPOSITION 5. *Le volume de P_e est indépendant de la base choisie pour Γ.*

Démonstration. Soit $(f_1, ..., f_n)$ une autre $\mathbb{Z}$-base de Γ. Chaque f_i s'écrit comme la somme $f_i = \sum_{j=1}^{n} \alpha_{ij} e_j$, où les α_{ij} sont des entiers. Puisque le déterminant d'une transformation linéaire mesure le changement de volume, on a $\mu(P_f) = |\det(\alpha_{ij})|\mu(P_e)$. D'autre part, comme les f_i constituent aussi une $\mathbb{Z}$-base de Γ, la matrice (α_{ij}) possède une inverse dont les entrées sont également des entiers. Il s'ensuit que $\det(\alpha_{ij})$ est inversible dans $\mathbb{Z}$, et donc $\det(\alpha_{ij}) = \pm 1$, ce qui confirme que $\mu(P_e) = \mu(P_f)$. □

Ceci nous permet d'appeller *covolume de* Γ le volume de n'importe lequel des P_e. On le dénote $\mu(\Gamma)$.

2.3 Le plongement canonique

Les résultats de la section précédente nous permettront d'étudier l'anneau des entiers $\mathcal{O}_K$ comme un réseau de $\mathbb{R}^n$. On va maintenant définir les morphismes naturels de K dans $\mathbb{C}$ afin d'avoir une façon canonique d'identifier $\mathcal{O}_K$ à un réseau.

DÉFINITION Soit K un corps de nombres. Un *plongement* est un morphisme d'anneaux injectif $\sigma : K \to \mathbb{C}$.

Soit n le degré de K sur $\mathbb{Q}$. C'est un résultat central de théorie de Galois [4, §2.4] qu'il existe n plongements distincts $\sigma_i : K \hookrightarrow \mathbb{C}$. Ces plongements peuvent être *réels*, c'est à dire qu'ils envoient K dans $\mathbb{R}$; dans le cas contraire on les qualifie de *complexes*. Les plongements complexes viennent par paires. En effet, si $\sigma : K \to \mathbb{C}$ est un plongement, alors son conjugué complexe $\bar{\sigma}$

$$\bar{\sigma} : K \to \mathbb{C} \qquad \bar{\sigma}(x) \mapsto \overline{\sigma(x)}$$

est est également un. On peut donc regrouper les plongements de $K \hookrightarrow \mathbb{C}$ en r_1 plongements réels et $2r_2$ plongements complexes, avec $r_1 + 2r_2 = n$. Ce sont ces entiers qu'on a vus dans l'énoncé du Théorème des unités.

LE PLONGEMENT CANONIQUE [4, §5.1] Soient σ_i, $1 \leq i \leq n$ les n plongements de K. On les numérote de facon à ce que les r_1 premiers soient réels et que pour les $2r_2$ suivants on aie $\sigma_{j+r_2} = \bar{\sigma_j}$. On applique simultanément les $r_1 + r_2$ premiers morphismes pour obtenir le *plongement canonique* de K.

$$\sigma : K \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$$
$$\sigma(x) = (\sigma_1(x), ..., \sigma_{r_1+r_2}(x))$$

Ce plongement induit naturellement un plongement de $\mathcal{O}_K$, dont on verra bientôt que l'image est un sous-groupe discret de $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. Il est donc naturel de considérer son covolume, dont la mesure est un invariant appelé le discriminant du corps de nombres.

DÉFINITION [4, §2.7] Soit $\mathcal{O}_K$ l'anneau des entiers d'un corps de nombres, et $(x_1, ..., x_n)$ une $\mathbb{Z}$-base de $\mathcal{O}_K$ sur $\mathbb{Z}$. Le *discriminant* de $\mathcal{O}_K$ est défini par la formule suivante :

$$d = \det(\sigma_i(x_j))^2.$$

Une conséquence (pas tout a fait directe, voir [4, §2.7]) de cette définition est que le discriminant est un entier, et qu'il est indépendant de la base choisie pour $\mathcal{O}_K$. En effet, un réarrangement des sommes permet de constater que $d = \det(\mathrm{Tr}(x_i x_j))$ ou $\mathrm{Tr}(x)$ est la trace de la matrice $M_{e,x}$ dont les entrées sont des entiers. Finalement, le discriminant est non-nul. En effet, une fois qu'on sait que le discriminant est indépendant de la base choisie pour $\mathcal{O}_K$, on peut conclure que si $d = 0$, alors les plongements σ_i sont linéairement dépendants sur $\mathbb{Q}$. Autrement dit, il existe des coefficients u_i tels que

$$\sum_{i=1}^{n} u_i \sigma_i(x_j) = 0 \quad \text{pour tout } x_j.$$

Or, cette indépendance linéaire est impossible : c'est précisément l'assertion au lemme de Dedekind sur l'indépendance des caractères, un résultat classique que nous nous contenterons de citer, mais dont la preuve se trouve dans [4, §2.7].

PROPOSITION 6. *Soient K un corps de nombres de degré n, $\mathcal{O}_K$ son anneau des entiers et d son discriminant. Alors $\sigma(\mathcal{O}_K)$ est un réseau de $\mathbb{R}^n$ dont le covolume est donné par $\mu(\sigma(\mathcal{O}_K)) = 2^{-r_2}|d|^{\frac{1}{2}}$.*

Démonstration. Soit $(x_1, ..., x_n)$ une $\mathbb{Z}$-base de $\mathcal{O}_K$; on sait qu'il s'agit d'une $\mathbb{Q}$-base de K. Pour x_j fixé, les composantes de $\sigma(x_j)$ dans la base standard de $\mathbb{R}^n$ sont :

$$(\sigma_1(x_j), ..., \sigma_{r_1}(x_j), \Im(\sigma_{r_1+1}(x_j)), \Re(\sigma_{r_1+1}(x_j)), ..., \Im(\sigma_{r_1+r_2}(x_j)), \Re(\sigma_{r_1+r_2}(x_j)).$$

On va calculer la le déterminant D de la matrice dont la j^{e} colonne est le vecteur $\sigma(x_j)$. On utilise les formules

$$\Re(z) = \frac{1}{2}(z + \bar{z}) \quad \Im(z) = \frac{1}{2i}(z - \bar{z})$$

ainsi que la linéarité alternée dans les lignes pour voir que $D = \frac{1}{(2i)^{r_2}} \det(\sigma_i(x_j)) = \frac{1}{(2i)^{r_2}}|d|^{\frac{1}{2}}$. Comme ce déterminant n'est pas nul, on conclut que la matrice est inversible, et donc que les $\sigma(x_j)$ constituent une base de $\mathbb{R}^n$. Le sous-groupe de $\mathbb{R}^n$ qu'ils engendrent est donc un réseau, qu'on dénotera $\sigma(\mathcal{O}_K)$. Il s'ensuit que la matrice $(\sigma_i(x_j))$ correspond à un changement de base, de la base standard de $\mathbb{R}^n$ à la base des $\sigma(x_j)$. Finalement, la propriéte du déterminant comme mesure du changement de volume nous permet de conclure que $\mu(\sigma(\mathcal{O}_K)) = \frac{1}{2^{r_2}}|d|^{\frac{1}{2}}$. □

L'image de $\sigma(\mathcal{O}_K)$ (que nous appellerons ici $\mathcal{O}_K$ par abus de langage) est donc un réseau de $\mathbb{R}^n$. C'est également le cas de ses idéaux principaux. En effet, soit $a \in \mathcal{O}_K$, et (a) l'idéal engendré par a. La multiplication m_a est un isomorphisme de $\mathbb{Z}$-modules entre $\mathcal{O}_K$ et (a). De plus, par le théorème des modules sur les anneaux principaux [4, §1.5], il existe une $\mathbb{Z}$-base $(x_1, ..., x_n)$ de $\mathcal{O}_K$ des entiers $a_1, ..., a_n$ tels que $(a_1x_1, ..., a_nx_n)$ est une $\mathbb{Z}$-base de (a). Le quotient $\mathcal{O}_K/(a)$ est donc un $\mathbb{Z}$-module fini, de la forme $\mathbb{Z}/a_1\mathbb{Z} \times ... \times \mathbb{Z}/a_n\mathbb{Z}$.

Si on retourne à l'idée de $\mathcal{O}_K$ comme réseau et qu'on choisit $(x_1, ..., x_n)$ comme base, on voit que (a) est un sous-réseau de $\mathcal{O}_K$ dans lequel chaque élément x_i de la base a été dilaté d'une longueur a_i. On appelle (a) un sous-réseau d'indice $a_1 \cdot ... \cdot a_n$ de $\mathcal{O}_K$; l'indice de (a) dans $\mathcal{O}_K$ est donc égal à la cardinalité du quotient $\mathcal{O}_K/(a)$. Cet indice correspond également à la dilatation du covolume du réseau $\mathcal{O}_K$ sous l'effet de la multiplication par a. Or, cette multiplication est une transformation linéaire, nous l'avons vu au §2.1 ; son déterminant est $N(x)$. Comme le déterminant d'une transformation linéaire mesure précisément la dilatation du volume du parellélotope engendré par la base, on obtient le résultat suivant.

Proposition 7. *Soit $\mathcal{O}_K$, l'anneau des entiers d'un corps de nombres, $a \in \mathcal{O}_K$, et (a), l'idéal principal engendré par a. Si, $N(a)$ est la norme de a, alors $N(a) = |\mathcal{O}_K/(a)|$.*

On peut donc parler de la norme de l'idéal (a) comme de l'indice de (a) dans $\mathcal{O}_K$ ou de la cardinalité du quotient $\mathcal{O}_K/(a)$. On a le résultat suivant à propos des normes d'idéaux, qui ne sera pas démontré, mais dont la preuve se trouve à [4, §4.3]. Cependant, pour s'en convaincre, on observer que $\mathcal{O}_K$ ne possède qu'un nombre fini de sous-réseaux d'indice m.

Théorème 1. *Soit $\mathcal{O}_K$ l'anneau des entiers d'un corps de nombres. Pour chaque entier $m \in \mathbb{Z}$, il existe un nombre fini d'idéaux principaux de norme m.*

2.4 Théorème de Minkowski

La preuve du théorème des unités reposera sur la propriété qu'a le réseau $\mathcal{O}_K$ qu'une partie assez grande $\mathbb{R}^n$ en contient au moins un élément non-trivial. C'est en gros le propos du théorème suivant et de son corollaire, qu'on peut retrouver au [4, §4.2]. On rapelle les notations : pour une partie mesurable $S \subset \mathbb{R}$, on désigne par $\mu(S)$ désigne sa mesure de Lebesgue. Pour un réseau Γ, on rappelle que $\mu(\Gamma)$ désigne la mesure de son parallélotope fondamental P_e.

Théorème 2 (Minkowski). *Soit Γ un réseau de $\mathbb{R}^n$ et S un sous-ensemble intégrable de $\mathbb{R}^n$ tel que $\mu(S) > \mu(\Gamma)$. Il existe alors deux élements distincts $x, y \in S$ tels que $x - y \in \Gamma$.*

Démonstration. Soit P_e un parallélotope fondamental pour Γ. Par définition de P_e, on a

$$\mathbb{R}^n = \bigcup_{h\in\Gamma} h + P_e \quad \Rightarrow \quad S = \bigcup_{h\in\Gamma} S \cap (h + P_e) \quad \Rightarrow \quad \mu(S) = \sum_{h\in\Gamma} \mu(S \cap (h + P_e)).$$

Puisque la mesure de Lebesgue est invariante par translation, on a $\mu(S\cap(h+P_e)) = \mu((-h+S)\cap P_e)$. On en déduit qu'il existe deux éléments $h_1, h_2 \in \Gamma$, $h_1 \neq h_2$ tels que l'intersection

$$((-h_1 + S) \cap P_e) \cap ((-h_2 + S) \cap P_e)$$

est non-nulle. En effet, puisque $(-h+S)\cap P_e \subseteq P_e$ si tous les $(-h+S)\cap P_e$ étaient deux a deux disjoints, on aurait

$$\mu(S) = \sum_{h\in\Gamma} \mu((-h+S)\cap P_e) \leq \mu(P_e)$$

ce qui contredirait l'hypothèse de départ. Puisque $((-h_1+S)\cap P_e)\cap((-h_2+S)\cap P_e) \neq \emptyset$, il existe $x, y \in S$ tels que $x-h_1 = y-h_2$. Ceci permet de conclure que $x-y = h_1-h_2 \in \Gamma$. □

Corollaire 1. *Soit Γ un réseau de $\mathbb{R}^n$, et S une partie intégrable de $\mathbb{R}^n$ qui soit symétrique par rapport à 0, convexe, et dont le volume satisfait :*

$$\mu(S) > 2^n \mu(\Gamma).$$

Alors S contient un élement non-nul de Γ.

Démonstration. On applique le théorème à la partie $S' = \frac{1}{2}S$ de $\mathbb{R}^n$. En effet :

$$\mu(S') = \frac{1}{2^n}\mu(S) > \mu(\Gamma).$$

On a donc $x, y \in S'$, $x \neq y$ tels que $z = x-y \in \Gamma$. Puisque S est symétrique par rapport à l'origine, on a $2x, -2y \in S$. La convexité de S nous donne :

$$z = \frac{1}{2}(2x+(-2y)) \quad \Rightarrow \quad z \in tx+(1-t)y, \;\; t\in[0,1] \quad \Rightarrow \quad z \in S.$$

□

3 Le théorème des unités

Nous sommes maintenant armés de toutes les notions nécessaires pour démontrer le théorème de unités. Cette section est tirée de [4, §4.4].

Théorème 3 (Dirichlet). *Soient K un corps de nombres, n son degré, r_1 et r_2 les entiers définis au §2.3, et $r = r_1 + r_2 - 1$. Le groupe $\mathcal{O}_K^*$ des unités de K est isomorphe à $\mathbb{Z}^r \times G$, où G est un groupe cyclique fini, formé par les racines de l'unité contenues dans K.*

Démonstration. La première partie de la peuve consiste à démontrer que $\mathcal{O}_K^*$ est un groupe abélien de type fini. Pour ce faire un va considérer la fonction suivante, appelée *plongement logarithmique* :

$$L : \mathcal{O}_K^* \to \mathbb{R}^{r_1+r_2}$$
$$L(x) = (\log|\sigma_1(x)|, ..., \log|\sigma_{r_1+r_2}(x)|)$$

La fonction $L(x)$ est un homomorphisme car $L(xy) = L(x)+L(y)$. Nous montrerons maintenant que son image est un sous-groupe discret de $\mathbb{R}^{r_1+r_2}$.

Soit B, un compact de $\mathbb{R}^{r_1+r_2}$. On veut montrer que le nombre d'unités x telles que $L(x) \in B$ est fini. Puisque B est compact, il est borné et il existe M tel que $\log(\sigma_i(x)) < M$ pour $1 \leq i \leq r_1 + r_2$. Il s'ensuit que si $L(x) \in B$, alors $|\sigma_i(x)| < e^M$. On se souvient que les $\sigma_i(x)$ sont racines dans $\mathbb{C}$ du polynôme minimal de x. Les coefficients de ce polynôme sont donc les fonctions symétriques élémentaires des $\sigma_i(x)$, ce qui implique que ces coefficients aussi sont bornés. Or, puisque $x \in \mathcal{O}_K$, ces coefficients sont dans $\mathbb{Z}$, ce qui fait qu'il n'y en a qu'un nombre fini possible. Comme le degré du polynôme minimal d'un élément de K est borné par n, on n'a qu'un nombre fini possible de polynômes minimaux, et donc de x tels que $L(x) \in B$.

La première conséquence de ce résultat est que le noyau de L est un groupe fini, et donc cyclique par le résultat prouvé au §2.2. La deuxième est que $L(\mathcal{O}_K^*)$ est un sous-groupe discret de $\mathbb{R}^{r_1+r_2}$, et donc isomorphe à $\mathbb{Z}^l$ pour $l \leq r_1 + r_2$. On peut conclure que $\mathcal{O}_K^*$ est un groupe abélien de type fini, donc de la forme $\mathbb{Z}^k \times G$, où G est fini. En fait, puisque $\ker(L)$ est fini et que $\mathrm{Im}(L) \cong \mathbb{Z}^l$, la torsion du $\mathbb{Z}$-module $\mathcal{O}_K^*$ correspond précisément à $\ker(L)$. On déduit donc que la structure de $\mathcal{O}_K^*$ est

$$\mathcal{O}_K^* \cong \mathbb{Z}^k \times \ker(L).$$

Il nous reste à démontrer que $k = r_1 + r_2 - 1$. D'abord, observons que la norme de tout élément $x \in \mathcal{O}_K^*$ est 1, ce qui revient à dire que

$$\prod_{i=1}^{n} \sigma_i(x) = \prod_{i=1}^{r_1} \sigma_i(x) \prod_{j=r_1+1}^{r_2} \sigma_j(x)\overline{\sigma_j(x)} = 1.$$

On observe que $|\sigma_j(x)| = |\overline{\sigma_j(x)}|$, et on applique le logarithme. On voit ansi que pour tout $x \in \mathcal{O}_K^*$,

$$\log|\sigma_1(x)| + ... + \log|\sigma_{r_1}(x)| + 2\log|\sigma_{r_1+1}| + ... + 2\log|\sigma_{r_1+r_2}(x)| = 0.$$

L'image $L(\mathcal{O}_K^*)$ est donc contenue dans un hyperplan W dont l'équation est

$$W = \{(x_1, ..., x_{r_1+r_2}) \mid x_1 + ... + x_{r_1} + 2x_{r_1+1} + ... + 2x_{r_1+r_2} = 0\}$$

ce qui démontre que $k \leq r_1 + r_2 - 1$. Pour démontrer l'inégalité inverse, on va prouver que $L(\mathcal{O}_K^*)$ engendre W comme espace vectoriel. L'idée sera de montrer que pour tout fonctionnel non-nul

$$f : W \to \mathbb{R}$$

il existe une unité u telle que $f(L(u)) \neq 0$. D'abord, comme $W \subset \mathbb{R}^{r+1}$ est un hyperplan, la projection de W sur $\mathbb{R}^r$ est un isomorphisme d'espace vectoriels. Donc pour un fonctionnel f et pour tout $y = (y_1, ..., y_{r+1}) \in W \subset \mathbb{R}^{r+1}$ on peut écrire

$$f(y) = c_1y_1 + ... + c_ry_r \quad c_i \in \mathbb{R}. \tag{3.1}$$

On va maintenant obtenir des entiers $x \in \mathcal{O}_K$ de norme bornée et s'en servir pour démontrer l'existence de u. Soit un entier α tel que $\alpha > \left(\frac{1}{2\pi}\right)^{r_2} |d|^{\frac{1}{2}}$. Si on a un r-tuple $\lambda = (\lambda_1, ..., \lambda_r)$, soit $\lambda_{r+1} \in \mathbb{R}$ qui satisfait

$$\prod_{i=1}^{r_1} \lambda_i \prod_{j=r_1+1}^{r_1+r_2} \lambda_j^2 = \alpha.$$

Le r-tuple $(\lambda_1, ..., \lambda_r)$ est arbitraire pour l'instant, mais on va éventuellement le produire afin de construire une classe d'éléments de $\mathcal{O}_K$ dont les images par $f \circ L$ seront distinctes.
L'étape suivant consiste a construire à partir de α un sous-ensemble $B_\lambda \subset \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ contenant un entier :

$$B_\lambda = \{x = (x_1, ..., x_{r_1}, z_1, ..., z_{r_2}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \ \mid \ |x_i| \leq \lambda_i \ \& \ |z_j| \leq \lambda_j\}.$$

L'ensemble B_λ est convexe et symétrique par rapport à l'origine. De plus, son volume est donné par :

$$\prod_{i=1}^{r_1} 2\lambda_i \prod_{j=r_1+1}^{r_1+r_2} \pi\lambda_j^2 = 2^{r_1}\pi^{r^2}\alpha > 2^{-r_2}|d|^{\frac{1}{2}} = v(\sigma(\mathcal{O}_K)).$$

On peut donc appliquer le Théorème de Minkowski et conclure qu'il existe un entier non-nul $x_\lambda \in \mathcal{O}_K$ tel que $\sigma(x_\lambda) \in B_\lambda$, c'est-à-dire que $|\sigma_i(x_\lambda)| \leq \lambda_i$ pour tout i (on compte deux fois $\sigma_j(x_\lambda)$ car son conjugué complexe a la même norme). Comme la norme de x_λ est un entier, on en déduit les inégalités suivantes :

$$1 \leq |N(x_\lambda)| = \prod_{i=1}^{n} \sigma_i(x_\lambda) \leq \prod_{i=1}^{r_1} \lambda_i \prod_{j=r_1+1}^{r_1+r_2} \lambda_j^2 = \alpha$$

$$|\sigma_i(x_\lambda)| \geq |N(x_\lambda)| \prod_{j \neq i} |\sigma_j(x_\lambda)|^{-1} \geq \prod_{i \neq j} \lambda_j^{-1} \geq \lambda_i^{-1}\alpha$$

$$\Rightarrow \qquad \lambda_i^{-1}\alpha \leq \sigma_i(x_\lambda) \leq \lambda_i.$$

On prend ensuite le logarithme et on réarrange, ce qui donne :

$$0 \leq \log(\lambda_i) - \log|\sigma_i(x_\lambda)| \leq \alpha.$$

On a maintenant affaire à une égalité concernant les coordonées d'un vecteur dans W. On prend donc la somme sur les c_i de (3.1) pour obtenir

$$\left|\sum c_i \log(\lambda_i) - f(L(x_\lambda))\right| \leq \left(\sum c_i\right) \log\alpha.$$

On va utiliser cette borne, ainsi que celle sur la norme de x, pour démontrer l'existence d'une unité u telle que $f(L(u)) \neq 0$. Soit $\beta > (\sum c_i) \log\alpha$. Pour chaque entier $h \in \mathbb{Z}$, on choisit $\lambda(h) = \lambda_1(h), ..., \lambda_r(h)$ tels que

$$\sum c_i\lambda_i(h) = 2\beta h.$$

On applique maintenant à $\lambda(h)$ le procéde expliqué plus haut pour obtenir $x_h = x_\lambda(h) \in \mathcal{O}_K$. L'entier algébrique x_h satisfait par construction les inégalités suivantes :

$$|2\beta_h - f(L(x_h))| = \left|\sum c_i \log(\lambda_i(h)) - f(L(x_h))\right| \leq \left(\sum c_i\right) \log \alpha < \beta$$

$$\Rightarrow (2h-1)\beta < f(L(x_h)) < (2h+1)\beta.$$

La dernière inégalité implique que pour chaque entier $h \in \mathbb{Z}$, $f(L(x_h)) < f(L(x_{h+1}))$ et que les valeurs de $f(L(x_h))$ sont donc toutes distinctes.

On a une infinité de x_h qui prennent tous des valeurs distinctes, mais leur norme est uniformément bornée. En effet, on a vu plus haut que

$$|N(x_h)| = \prod_{i=1}^{n} \sigma_i(x_h) \leq \alpha.$$

Comme on peut identifier la norme d'un élément avec celle de l'idéal principal qu'il engendre, on voit que la norme des idéaux (x_h) est bornée par α. Cependant, on a vu au Théorème 1 qu'il n'y a qu'un nombre fini d'idéaux d'une norme donnée. Comme les normes sont dans $\mathbb{Z}$ et qu'il n'y a qu'un nombre fini d'entiers inférieurs à α, il doit donc exister deux entiers distincts i, j tels que $(x_i) = (x_j)$. Il existe donc une unité $u \in \mathcal{O}_K^\times$ telle que $x_i = ux_j$. Il s'ensuit, puisque L est un logarithme, que $L(u) = L(x_i) - L(x_j)$. On peut appliquer le fonctionnel linéaire f pour conclure que $f(L(u)) = f(L(x_i)) - f(L(x_j)) \neq 0$ puisque les $f(L(x_h))$ sont tous distincts. On a donc démontré que pour n'importe quel fonctionnel f il existe une unité telle que $f(L(u)) \neq 0$, ce qui implique que les unités engendrent W, et que le rang de $\mathcal{O}_K^\times$ est bien $r_1 + r_2 - 1$. □

Références

[1] R. Dedekind, *Theory of Algebraic Integers*, Traduction et introduction de John Stillwell, Cambridge University Press, Cambridge, 1996 (publication initiale en 1877).

[2] L.E. Dickson, *History of the Theory of Numbers*, Vol. II, Chelsea Publ. Co., New York, 1971.

[3] J.S. Milne, *Algebraic Number Theory (v3.03)*, disponible en ligne au www.jmilne.org/math, 2011.

[4] P. Samuel, *Théorie algébrique des nombres*, Hermann, Paris, 1967.