CHAPITRE 6

Finitude du nombre des classes d'idéaux d'un anneau de nombres

Dans ce chapitre, nous poursuivons notre étude de l'arithmétique des anneaux de nombres algébriques comme $\mathcal{O}_K$ ou $\mathbb{Z}[\alpha]$ avec $\alpha \in \overline{\mathbb{Z}}$. L'exemple des entiers quadratiques imaginaires nous a montré que ces anneaux ont une forte tendance à ne pas être factoriels ou principaux. [1] Nous étudions ici en général leur défaut de principalité, en introduisant la notion centrale de classes d'idéaux dans un anneau. Le résultat principal est alors que l'ensemble de ces classes est toujours fini, ce qui n'est pas sans rappeler la finitude des classes de formes de discriminant donné. Suivant Minkowski, nous verrons que la géométrie des nombres fournit un algorithme efficace pour déterminer cet ensemble de classes, en particulier pour montrer qu'un anneau de nombres est principal.

Références : Le chapitre IV paragraphes 2 et 3 du livre de Samuel. Le chapitre 12 du livre de Ireland et Rosen.

1. L'ensemble des classes d'idéaux d'un anneau intègre

Soit A un anneau intègre de corps de fractions K. Si I est un idéal de A et si $x \in K$, on note

$$xI = \{xa, a \in I\} \subset K.$$

Une partie de K de cette forme est appelée [2] *idéal fractionnaire de* K. C'est un sous-groupe additif de K stable par multiplication par tout élément de A. En particulier, xI est un idéal de A si de plus $xI \subset A$. C'est notamment le cas si $x \in A$.

Définition 6.1. *Deux idéaux I et J de A sont dits* équivalents*, et l'on note $I \sim J$, s'il existe $x, y \in A$ non nuls tels que $xI = yJ$, ou ce qui revient au même s'il existe $z \in K^\times$ tel que $zI = J$. C'est une relation d'équivalence sur l'ensemble des idéaux non nuls de A dont on note* $\mathrm{Cl}(A)$ *l'ensemble des classes.*

La vérification que c'est une relation d'équivalence est immédiate. On note $[I]$ la classe dans $\mathrm{Cl}(A)$ de l'idéal non nul I de A. L'ensemble $\mathrm{Cl}(A)$ mesure le défaut de principalité de l'anneau A :

Proposition 6.2. *Un idéal non nul I de A est principal si, et seulement si, on a $I \sim A$. En particulier,* $\mathrm{Cl}(A)$ *est de cardinal* 1 *si, et seulement si, A est principal.*

1. En fait, pour ces anneaux il est équivalent d'être factoriel et principal. Cela provient de l'exercice 7.5 combiné au théorème 6.15 (i).

2. Bien que couramment adoptée, c'est une très mauvaise terminologie car en général ce ne sont pas des ideaux de K (dont les seuls idéaux 0 et K, puisque c'est un corps).

Démonstration — On a bien sûr $xA \sim A$ pour tout $x \in A$ non nul. Réciproquement, soit I un idéal de A et $z \in K^*$ tels que $I = zA$. On a $z \cdot 1 \in I \subset A$, et donc I est principal. □

L'ensemble $\mathrm{Cl}(A)$ est muni d'une loi de composition interne intéressante qu'elle hérite du produit des idéaux que nous décrivons maintenant.

Définition 6.3. *Si I et J sont deux idéaux de A. On note IJ l'idéal de A engendré par les éléments de la forme xy avec $x \in I$ et $y \in J$.*

Évidemment, on a $(a)(b) = (ab)$ pour tout $a, b \in A$. Plus généralement, si $I = (a_1, \ldots, a_n)$ et si $J = (b_1, \ldots, b_m)$, alors IJ est l'idéal engendré par les nm éléments $a_i b_j$. L'anneau A étant commutatif par hypothèse, on a $IJ = JI$. Le produit des idéaux est associatifs : $(HI)J = H(IJ)$ est simplement l'idéal engendré par les $xyz = x(yz) = (xy)z$ avec $x \in H$, $y \in I$ et $z \in J$. On définit plus généralement le produit $I_1 \cdots I_n$ de $n \geq 2$ idéaux de A par la relation récursive $I_1 \cdots I_n = (I_1 \cdots I_{n-1})I_n$. Si I, I', J, J' sont des idéaux de A, on constate enfin que les relations $I \sim I'$ et $J \sim J'$ entraînent $IJ \sim I'J'$. Nous avons donc vérifié la proposition suivante.

Proposition 6.4. *La multiplication des idéaux induit une loi de composition sur* $\mathrm{Cl}(A)$*. Cette loi est commutative et associative. La classe de A, i.e. celle des idéaux principaux, en est un élément neutre.*

Ce qui manque en général à $\mathrm{Cl}(A)$ pour être un groupe (muni de cette loi) est donc l'inversibilité de ses éléments. Remarquons qu'il est équivalent de dire que la classe de l'idéal non nul I est inversible et de dire qu'il existe un idéal non nul J de A tel que IJ est principal. Un tel idéal I sera dit simplement inversible.

2. Finitude du nombre des classes d'idéaux

Commençons par une définition importante.

Définition 6.5. *Un ordre du corps de nombres K est un sous-anneau $A \subset \mathcal{O}_K$ contenant une $\mathbb{Q}$-base de K.*

Par exemple, si $\alpha \in \overline{\mathbb{Z}}$ alors $\mathbb{Z}[\alpha]$ est un ordre de $\mathbb{Q}(\alpha)$. De plus, $\mathcal{O}_K$ est également un ordre de K (Lemme 5.19). L'intêret de cette notion pour nous est essentiellement d'englober ces deux cas importants. Notre objectif principal dans ce chapitre est de démontrer le théorème suivant.

Théorème 6.6. (Finitude du nombre des classes) *Si A est un ordre du corps de nombres K, alors* $\mathrm{Cl}(A)$ *est fini.*

Il s'avère que bien qu'un tel A n'est pas toujours principal comme nous l'avons déjà vu, il n'en est pas très loin. En effet, la proposition suivante affirme que tout idéal de I contient un idéal principal qui est très gros, à savoir d'indice dans I inférieur à une constante ne dépendant que de A :

Proposition 6.7. *Soit A un ordre du corps de nombres K. Il existe un entier $C \geq 1$ tel que pour tout idéal I de A, il existe un élément $x \in I$ tel que $|I/Ax| \leq C$.*

Vérifions que cela entraîne le théorème. En effet, soit I un idéal non nul de A, et soit $x \in I$ comme dans l'énoncé de la proposition (en particulier, on a $x \neq 0$ car I est infini). Si N désigne le cardinal du groupe abélien fini I/Ax, alors N annule I/Ax d'après Lagrange, c'est-à-dire $NI \subset Ax$. On constate donc que

$$NA \subset \frac{N}{x} I \subset A$$

(l'inclusion de gauche vient de ce que $x \in I$, donc $N = \frac{N}{x} x \in \frac{N}{x} I$). En particulier, $J = \frac{N}{x} I$ est un idéal de A qui est équivalent à I, car $xJ = NI$, et qui est compris entre NA et A. Rappelons que $N \leq C$ d'après la proposition. Il ne reste donc qu'à vérifier que pour tout entier $N \geq 1$ il n'existe qu'un nombre fini d'idéaux de A contenant N. Cela se déduit par exemple du lemme suivant.

Lemme 6.8. *Pour tout entier $N \geq 1$, l'anneau A/NA est fini, et a $N^{[K:\mathbb{Q}]}$ éléments.*

Démonstration — En effet, le groupe additif de A admet une $\mathbb{Z}$-base $e_1, \ldots, e_n$ à $n = [K : \mathbb{Q}]$ éléments. Nous l'avons déjà vu si $A = \mathbb{Z}[\alpha]$ (Proposition 5.24) où $A = \mathcal{O}_K$ (existence de $\mathbb{Z}$-bases de $\mathcal{O}_K$) et nous le démontrerons pour tout A au théorème 6.15. Soit $e_1, \ldots, e_n \in A$ une telle base. On constate alors que $NA = \oplus_{i=1}^{n} N\mathbb{Z}e_i$, puis que l'ensemble quotient A/NA a exactement N^n éléments. [3] □

Cela termine la démonstration de la finitude du nombre de classes à partir de la proposition 6.7. Observons au passage que nous avons démontré le corollaire suivant.

Corollaire-Définition 6.9. *Soit A un ordre d'un corps de nombres. On note $C(A)$ le plus petit entier C satisfaisant la proposition 6.7. Tout idéal non nul de A est équivalent à un idéal de A contenant un entier N tel que $1 \leq N \leq C(A)$.*

Il ne reste donc qu'à vérifier la proposition 6.7. Elle pourrait se démontrer à l'aide du principe des tiroirs en étudiant le défaut d'euclidianité de A, nous renvoyons à l'exercice 6.13 pour cette approche. L'inconvénient de cette méthode est qu'elle fournit une majoration de $C(A)$ assez mauvaise (bien qu'explicite) qui rend son utilisation peu commode. Dans un paragraphe suivant, nous la déduirons plutôt de la géométrie des nombres, qui donnera un renseignement nettement plus precis et fondamental dans l'optique du calcul effectif de $\mathrm{Cl}(A)$ dans les exemples.

3. Digression : idéaux contenant un nombre premier

Avant de se concentrer sur la preuve de la proposition 6.7, qui nous occupera par la suite jusqu'à la fin du chapitre, remarquons qu'il nous faudra de plus, pour déterminer des représentants de $\mathrm{Cl}(A)$, être capable de déterminer les idéaux de A contenant un entier $N \geq 2$ donné. Ces idéaux sont chacun l'image réciproque d'un idéal de l'anneau fini A/NA, et peuvent donc tous être énumérés en théorie si A est explicite. Lorsque N est premier et A est monogène, on dispose de la recette suivante.

3. Mieux le groupe additif A/NA est isomorphe à $(\mathbb{Z}/N\mathbb{Z})^n$. Attention, il s'agit seulement d'un isomorphisme additif, et l'anneau quotient A/NA n'est pas en général isomorphe à l'anneau produit $(\mathbb{Z}/N\mathbb{Z})^n$.

Proposition 6.10. *Soient $\alpha \in \overline{\mathbb{Z}}$, $A = \mathbb{Z}[\alpha]$, p un nombre premier et $P = \overline{\Pi}_{\alpha,\mathbb{Q}} \in (\mathbb{Z}/p\mathbb{Z})[X]$ la réduction modulo p du polynôme minimal de α sur $\mathbb{Q}$.*

(i) Si $Q \in (\mathbb{Z}/p\mathbb{Z})[X]$ est un diviseur de P, et si $\widetilde{Q} \in \mathbb{Z}[X]$ est un polynôme tel que $\widetilde{Q} \bmod p = Q$, alors $\mathrm{I}(Q) := pA + \widetilde{Q}(\alpha)A$ est un idéal de A contenant p qui ne dépend pas du choix de $\widetilde{Q}$.

(ii) L'application $Q \mapsto \mathrm{I}(Q)$ est une bijection entre facteurs unitaires de P et idéaux de A contenant p ; elle satisfait $Q|Q' \Leftrightarrow \mathrm{I}(Q') \subset \mathrm{I}(Q)$.

(iii) L'anneau $A/\mathrm{I}(Q)$ est isomorphe à $(\mathbb{Z}/p\mathbb{Z})[X]/(Q)$. En particulier, on a

$$|A/\mathrm{I}(Q)| = p^{\deg(Q)}.$$

Ce résultat jouera un rôle important dans les applications. Considérons par exemple $\alpha = \sqrt{-5}$, de sorte que $\Pi_{\alpha,\mathbb{Q}} = X^2 + 5$, et cherchons les idéaux de $A = \mathbb{Z}[\alpha]$ contenant 2. On a $X^2 + 5 \equiv (X + 1)^2 \bmod 2$, les idéaux de $\mathbb{Z}[\alpha]$ contenant 2 sont donc $2A$, $2A + (\alpha + 1)A$ et A. De même, comme $X^2 + 5 \equiv (X - 1)(X + 1) \bmod 3$, les idéaux de A contenant 3 sont $3A$, A, $3A + (\alpha - 1)A$ et $3A + (\alpha + 1)A$. Enfin, si -5 n'est pas un carré modulo p, les idéaux de A contenant p sont simplement A et pA.

Démonstration — Il est clair que $pA + \widetilde{Q}(\alpha)A$ est un idéal de A contenant p. Si $\widetilde{Q}', \widetilde{Q} \in \mathbb{Z}[X]$ sont congrus modulo $p\mathbb{Z}[X]$ alors $\widetilde{Q}'(\alpha) - \widetilde{Q}(\alpha) \in p\mathbb{Z}[\alpha] = pA$ et donc les idéaux $pA + \widetilde{Q}(\alpha)A$ et $pA + \widetilde{Q}'(\alpha)A$ sont les mêmes, ce qui démontre le (i).

Avant de démontrer le (ii) faisons quelques rappels généraux. Soit A un anneau commutatif unitaire.

(a) Soit I un idéal de A. L'application $J \mapsto J/I$ est une bijection entre l'ensemble ordonné (pour l'inclusion) des idéaux de A contenant I et celui des idéaux de A/I, la bijection inverse étant l'application $I' \mapsto \{x \in A, x + I \in I'\}$.

(b) Si $I \subset J$ sont deux idéaux de A, la surjection canonique $A/I \to A/J$ a pour noyau I/J et induit donc un isomorphisme d'anneaux $(A/I)/(I/J) \xrightarrow{\sim} A/J$.

(c) En particulier, si I' et J' sont des idéaux de A, le (ii) appliqué aux idéaux $I = I'$ et $J = I' + J'$ montre que l'application naturelle $A/I' \to A/(I' + J')$ induit un isomorphisme canonique $(A/I')/((I' + J')/I') \xrightarrow{\sim} A/(I' + J')$.

Nous cherchons à appliquer le (a) à $A = \mathbb{Z}[\alpha]$ et $I = pA$, et il faut donc étudier l'anneau A/pA dans ce cas. Nous allons démontrer qu'il existe un isomorphisme canonique

$$A/pA \xrightarrow{\sim} (\mathbb{Z}/p\mathbb{Z})[X]/(P).$$

Il s'agit d'une vérification relativement formelle, mais instructive !, que nous allons justifier lourdement.

Soient B l'anneau $\mathbb{Z}[X]$, $I = \Pi_{x,\mathbb{Q}}B$ et $J = pB$. Soit $\varphi : B \to A$ la surjection canonique $Q \mapsto Q(\alpha)$. On sait que φ induit un isomorphisme $\varphi' : B/I \xrightarrow{\sim} A$, d'après la proposition 5.24. D'autre part, on a clairement les égalités $\varphi(I + J) = \varphi(pB) =$

$p\varphi(B) = pA$. Autrement dit, φ' induit une bijection $(J+I)/I \xrightarrow{\sim} pA$, puis par passage aux quotients un isomorphisme

$$\varphi'' : (B/I)/((I+J)/I) \xrightarrow{\sim} A/pA.$$

D'autre part, le (c) des rappels ci-dessus montre que l'anneau de gauche de cet isomorphisme s'identifie naturellement à $B/(I+J)$, soit encore à $(B/J)/((I+J)/J)$, en appliquant encore le (c) en échangeant les rôles de I et J. Considérons d'autre part la surjection canonique $\psi : B \to (\mathbb{Z}/p\mathbb{Z})[X]$, $Q \mapsto \overline{Q} := Q \bmod p$. Elle est de noyau $J = pB$ et induit donc un isomorphisme $\psi' : B/J \xrightarrow{\sim} (\mathbb{Z}/p\mathbb{Z})[X]$. On a de plus clairement les égalités $\psi(I+J) = \psi(I) = (P)$, de sorte que ψ' induit une bijection $(J+I)/J \xrightarrow{\sim} (P)$, puis un isomorphisme

$$\psi'' : (B/J)/((I+J)/J) \xrightarrow{\sim} (\mathbb{Z}/p\mathbb{Z})[X]/(P).$$

Au final, on a détaillé une suite d'isomorphismes canoniques

$$(\mathbb{Z}/p\mathbb{Z})[X]/(P) \underset{\psi''}{\xleftarrow{\sim}} (B/J)/((I+J)/J) \underset{\text{can}}{\xrightarrow{\sim}} B/(I+J) \underset{\text{can}}{\xleftarrow{\sim}} (B/I)/((I+J)/I) \underset{\varphi''}{\xrightarrow{\sim}} A/pA.$$

Concrètement, l'isomorphisme $A/pA \xrightarrow{\sim} (\mathbb{Z}/p\mathbb{Z})[X]/(P)$ qui s'en déduit est l'unique morphisme d'anneaux envoyant, pour tout $Q \in \mathbb{Z}[X]$, l'élément $Q(\alpha) \bmod pA$ vers $\overline{Q}(X) \bmod P$. Cet isomorphisme envoie en particulier l'idéal $\mathrm{I}(Q)/pA$ sur (Q). Cela démontre le (iii) de la proposition, car $((\mathbb{Z}/p\mathbb{Z})[X]/(P))/(Q) \xrightarrow{\sim} (\mathbb{Z}/p\mathbb{Z})[X]/(Q)$ si $Q|P$, d'après le point (b) du rappel appliqué aux idéaux $(P) \subset (Q)$ de $(\mathbb{Z}/p\mathbb{Z})[X]$.

Démontrons maintenant le point (ii) de la proposition. Par la caractérisation des idéaux d'un quotient rappelée au (a) ci-dessus l'ensemble ordonné des idéaux de $k[X]/(P)$, où k est un corps et $P \in k[X]$, est en bijection naturelle avec celui des idéaux de $k[X]$ contenant P. Par principalité de $k[X]$, les idéaux de $k[X]$ contenant P sont les (Q) avec $Q \in k[X]$ divisant P, le générateur Q étant même unique s'il est choisi unitaire, et de plus $(Q) \subset (Q')$ si et seulement si $Q'|Q$. Le point (ii) de la proposition résulte donc du fait que l'isomorphisme $A/pA \xrightarrow{\sim} (\mathbb{Z}/p\mathbb{Z})[X]/(P)$ décrit plus haut envoie $\mathrm{I}(Q)/pA$ sur (Q).

□

4. Réalisation géométrique de $\mathcal{O}_K$: le plongement canonique

Fixons K un corps de nombres. Nous allons commencer par montrer comment réaliser $\mathcal{O}_K$ de manière naturelle comme un réseau d'un certain espace vectoriel réel de dimension $n = [K : \mathbb{Q}]$. Cela nous permettra non seulement de mieux comprendre sa structure, par exemple de retrouver l'existence de bases entières, mais aussi de lui appliquer la géométrie des nombres de Minkowski, d'où l'on tirera notamment la proposition 6.7.

Le premier exemple est le cas de $\mathbb{Z}$, qui est naturellement un réseau de $\mathbb{R}$. Un second exemple est celui des corps quadratiques imaginaires $K = \mathbb{Q}(\sqrt{d})$ avec d un rationnel < 0. En effet, on a vu que $\mathcal{O}_K$ est de la forme $\mathbb{Z} + \mathbb{Z}\alpha$ avec $\alpha \notin \mathbb{R}$: c'est en particulier un réseau de $\mathbb{C}$ (identifié à $\mathbb{R}^2$). Cette observation a par ailleurs été très utile à la compréhension des anneaux d'entiers quadratiques imaginaires.

Considérons maintenant le cas $K = \mathbb{Q}(\sqrt{2})$, pour lequel on a vu que $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}] = \mathbb{Z} + \mathbb{Z}\sqrt{2}$. On constate que $K \subset \mathbb{R}$, mais $\mathbb{Z} + \mathbb{Z}\sqrt{2}$ n'est pas discret dans

$\mathbb{R}$. En effet, sinon ce serait un réseau, donc de la forme $a\mathbb{Z}$ pour un réel $a > 0$. Mais les conditions $1 \in a\mathbb{Z}$ et $\sqrt{2} \in a\mathbb{Z}$ entraînent par quotient que $\sqrt{2} \in \mathbb{Q}$ ce qui est absurde. Il n'est pas difficile de vérifier qu'un sous-groupe de $\mathbb{R}$ qui n'est pas discret est en fait dense, de sorte que $\mathbb{Z}[\sqrt{2}]$ est en fait dense dans $\mathbb{R}$, ce qui n'est pas très commode pour visualiser ses éléments. On peut rétablir le caractère discret en considérant les deux plongements de $\mathbb{Q}(\sqrt{2})$ dans $\mathbb{R}$, à savoir l'identité et $a + b\sqrt{2} \mapsto a - b\sqrt{2}$. En effet, considérons l'application

$$\iota : \mathbb{Q}(\sqrt{2}) \longrightarrow \mathbb{R}^2, a + b\sqrt{2} \mapsto (a + b\sqrt{2}, a - b\sqrt{2}),$$

a, b désignant ici des nombres rationnels. Cette application est injective et $\mathbb{Q}$-linéaire. Alors $\iota(\mathbb{Z} + \mathbb{Z}\sqrt{2}) = \mathbb{Z}\iota(1) + \mathbb{Z}\iota(\sqrt{2})$. Mais $\iota(1) = (1, 1)$ et $\iota(\sqrt{2}) = (\sqrt{2}, -\sqrt{2})$ sont non proportionnels dans $\mathbb{R}^2$, donc une $\mathbb{R}$-base, et $\iota(\mathbb{Z}[\sqrt{2}])$ est un réseau de $\mathbb{R}^2$. On peut donc voir via l'isomorphisme de groupes ι l'anneau $\mathbb{Z}[\sqrt{2}]$ comme un réseau de $\mathbb{R}^2$. Cette construction s'étend verbatim à tous les $\mathbb{Q}(\sqrt{d})$ avec $d > 0$.

Notons que si $d < 0$, il ne faut pas considérer les deux plongements complexes de $\mathbb{Q}(\sqrt{d})$ mais bien un seul. Par exemple, l'image de $\mathbb{Z}[i] \to \mathbb{C} \times \mathbb{C}$ par l'application $z \mapsto (z, \overline{z})$ est bien un sous-groupe discret mais ce n'est pas un réseau : il est engendré par 2 éléments dans un espace vectoriel réel de dimension 4.

Ces constructions se généralisent comme suit. On considère l'ensemble $\Sigma(K)$ des $n = [K : \mathbb{Q}]$ plongements de K dans $\mathbb{C}$. Si $\sigma \in \Sigma(K)$, on définit son conjugué complexe $\overline{\sigma} : x \mapsto \overline{\sigma(x)}$ ($z \mapsto \overline{z}$ désignant la conjugaison complexe dans $\mathbb{C}$), c'est encore un élément de $\Sigma(K)$. Par définition, l'application $\sigma \mapsto \overline{\sigma}$ est une involution de $\Sigma(K)$. Les points fixes de cette involution, disons Σ_1, sont les *plongements réels de* K, c'est-à-dire les $\sigma \in \Sigma(K)$ tels que $\sigma(K) \subset \mathbb{R}$. Par exemple, si $K = \mathbb{Q}(x)$ avec $x \in \overline{\mathbb{Q}}$ les plongements réels de K sont en bijection naturelle avec les conjugués de x qui sont des nombres réels (Lemme 5.9). Les plongements non réels venant par paires conjuguées, il sera commode de choisir une partie $\Sigma_2 \subset \Sigma(K) \backslash \Sigma_1$ telle que

$$\Sigma(K) = \Sigma_1 \coprod \Sigma_2 \coprod \overline{\Sigma}_2.$$

Il n'y a pas de choix de Σ_2 plus naturel que les autres a priori, et chacun ferait l'affaire dans la construction qui suit. Il sera même commode d'ordonner les éléments de Σ_1 et Σ_2. On pose traditionnellement

$$r_1(K) = |\Sigma_1|, \;\; r_2(K) = |\Sigma_2|$$

et on notera même $r_1 = r_1(K)$ et $r_2 = r_2(K)$ dans ce qui suit pour alléger les notations. On numérote enfin $\Sigma_1 = \{\sigma_1, \ldots, \sigma_{r_1}\}$ et $\Sigma_2 = \{\sigma_{r_1+1}, \ldots, \sigma_{r_1+r_2}\}$. On a $|\Sigma(K)| = n = r_1 + 2r_2$ (Lemme 5.9).

Définition 6.11. *Le plongement canonique de K est l'application $\iota : K \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ définie par*

$$\iota(x) = (\sigma_i(x))_{i=1,\ldots,r_1+r_2}.$$

C'est une application $\mathbb{Q}$-linéaire injective.

Notons que la $\mathbb{Q}$-linéarité de ι découle de celle des $\sigma \in \Sigma(K)$, ainsi que l'injectivité (une coordonnée suffirait d'ailleurs !). L'observation importante de ce paragraphe est alors la suivante.

Théorème 6.12. *$\iota(\mathcal{O}_K)$ est un réseau de $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$.*

Dans la suite, nous identifions $\mathbb{C}$ à $\mathbb{R}^2$ au moyen de la $\mathbb{R}$-base $1, i$. Cela nous donne une identification de $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ à $\mathbb{R}^n$ et y fixe également la mesure de Lebesgue.

Lemme 6.13. *Soit $e_1, \dots, e_n$ une $\mathbb{Q}$-base de K. Alors $\iota(e_1), \dots, \iota(e_n)$ est une $\mathbb{R}$-base de $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ qui engendre un réseau de covolume $2^{-r_2}|\mathrm{disc}_{K/\mathbb{Q}}(e_1, \dots, e_n)|^{\frac{1}{2}}$.*

Démonstration — On considère la $\mathbb{R}$-base f de $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ constituée des $(0, \dots, 0, *, 0, \dots, 0)$ où $* = 1$ (resp. 1 ou i) s'il est à une place d'indice $\leq r_1$ (resp. sinon). Si $x \in K$, le vecteur $\iota(x)$ décomposé dans cette base est donc de la forme

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

Soit P la matrice des vecteurs $\iota(e_j)$ dans la base f. Si $r_2 = 0$, c'est-à-dire $\Sigma_1 = \Sigma(K)$, on constate que $|\det(P)| = |\det(\sigma_j(e_i))| = |\mathrm{disc}_{K/\mathbb{Q}}(e_1, \dots, e_n)|^{\frac{1}{2}} \neq 0$ (Proposition 5.17 (i) et (iii)), ce qui conclut dans ce cas. En général, on constate que si $\sigma \in \Sigma_2(K)$, on a la relation

$$\begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix} \begin{pmatrix} \mathrm{Re}\ \sigma(e_1) & \cdots & \mathrm{Re}\ \sigma(e_n) \\ \mathrm{Im}\ \sigma(e_1) & \cdots & \mathrm{Im}\ \sigma(e_n) \end{pmatrix} = \begin{pmatrix} \sigma(e_1) & \cdots & \sigma(e_n) \\ \overline{\sigma}(e_1) & \cdots & \overline{\sigma}(e_n) \end{pmatrix}.$$

La relation $|\det \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}| = 2$ montre que l'on a

$$|\det(P)| = 2^{-|\Sigma_2|}|\det(\sigma_i(e_j))| = 2^{-r_2}|\mathrm{disc}_{K/\mathbb{Q}}(e_1, \dots, e_n)|^{\frac{1}{2}}.$$

□

Démonstration — Démontrons maintenant le théorème 6.12. D'après le lemme 5.19, $\mathcal{O}_K$ contient une $\mathbb{Q}$-base de K, et l'image par ι d'une telle base est une $\mathbb{R}$-base de $V = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ d'après le lemme 6.13, donc le sous-groupe $\iota(\mathcal{O}_K)$ engendre V. Il ne reste qu'à vérifier que $\iota(\mathcal{O}_K)$ est discret.

Munissont V de sa norme sup. dans la base f de la démonstration du lemme 6.13. Soit $r > 0$ un réel. Si $x \in \mathcal{O}_K$ est tel que $|\iota(x)| < r$, alors $|\sigma(x)| < r$ pour tout $\sigma \in \Sigma_1$ et $|\mathrm{Re}\ \sigma(x)|, |\mathrm{Im}\ \sigma(x)| < r$ pour tout $\sigma \in \sigma_2$. En particulier, $|\sigma(x)| < \sqrt{2}\, r$ pour tout $\sigma \in \Sigma(K)$. Mais x est annulé par

$$\chi_{x,K/\mathbb{Q}} = \prod_{\sigma \in \Sigma(K)} (X - \sigma(x)) \in \mathbb{Z}[X].$$

La borne précédente montre que les coefficients d'un tel polynôme sont bornés par un réel ne dépendant que de r. Comme ils sont de plus entiers, il n'y a qu'un nombre fini de $\chi_{x,K/\mathbb{Q}}$ possibles pour $x \in \mathcal{O}_K$ tel que $|\iota(x)| < r$, et donc qu'un nombre fini de tels x (qui sont racines de tels polynômes) : $\iota(\mathcal{O}_K)$ est discret. □

Mentionnons qu'à ce stade, nous obtenons une autre démonstration de l'existence d'une $\mathbb{Z}$-base à n éléments du groupe additif $\mathcal{O}_K$. En effet, ι étant injective elle définit un isomorphisme (additif) de $\mathcal{O}_K$ sur $\iota(\mathcal{O}_K)$. Mais ce dernier est un réseau de l'espace vectoriel réel $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \simeq \mathbb{R}^n$, on conclut donc par le théorème 2.4 de caractérisation algébrique des réseaux. En fait, cette preuve est essentiellement la même que celle donnée au chapitre 4, même si le point de vue plus géométrique de ce chapitre l'éclaircit substantiellement.

Via l'isomorphisme additif $\iota : \mathcal{O}_K \xrightarrow{\sim} \iota(\mathcal{O}_K)$, la théorie des réseaux admet des conséquences immédiates à la structure de $\mathcal{O}_K$ et de ses ordres. On observe notamment que si $A \subset \mathcal{O}_K$ est un sous-groupe quelconque contenant une $\mathbb{Q}$-base de K (par exemple un ordre), alors $\iota(A)$ est un sous-réseau de $\iota(\mathcal{O}_K)$ d'après la proposition 5.17. En particulier, A est d'indice fini $\frac{\mathrm{covol}(\iota(A))}{\mathrm{covol}(\iota(\mathcal{O}_K))}$ dans $\mathcal{O}_K$ et admet une $\mathbb{Z}$-base à n éléments. Cela justifie le (i) de la proposition-définition suivante.

Proposition-Définition 6.14. *Soit K un corps de nombres et soit $A \subset \mathcal{O}_K$ un sous-groupe additif contenant une $\mathbb{Q}$-base de K.*

(i) A admet une $\mathbb{Z}$-base à $n := [K : \mathbb{Q}]$ éléments.

On note $\mathrm{disc}(A) \in \mathbb{Z}$ *le discriminant d'une $\mathbb{Z}$-base quelconque de A.*

(ii) On a la relation $|\mathrm{disc}(A)|^{1/2} = \mathrm{covol}(\iota(A))\ 2^{r_2(K)}$.

(iii) Si B est un sous-groupe de $\mathcal{O}_K$ contenant A alors A est d'indice fini dans B égal à $\frac{|\mathrm{disc}(A)|^{1/2}}{|\mathrm{disc}(B)|^{1/2}}$. En particulier, $\frac{|\mathrm{disc}(A)|}{|\mathrm{disc}(B)|} = |B/A|^2$ est le carré d'un entier.

Démonstration — Le fait que $\mathrm{disc}(A)$ ainsi défini est indépendant du choix de la $\mathbb{Z}$-base de A découle des propositions 2.10 (ii) et 5.17 (ii). Il est entier d'après la dernière assertion du théorème 5.21 et donné par la formule (ii) par le lemme 6.13. Le (iii) est conséquence de la proposition 2.17. □

Notons en particulier la relation $\mathrm{covol}(\iota(\mathcal{O}_K))2^{r_2(K)} = |\mathrm{disc}(\mathcal{O}_K)|^{1/2}$ conséquence du (ii). Le résultat suivant généralise la proposition 4.12.

Théorème 6.15. *Soient K un corps de nombres, A un ordre de K et $I \subset A$ un idéal non nul. Alors I est d'indice fini dans A et admet une $\mathbb{Z}$-base à $[K : \mathbb{Q}]$ éléments. En particulier, A est un anneau noethérien.*

Démonstration — En effet, il suffit de voir que I contient une $\mathbb{Q}$-base de K par la proposition qui précède. Mais comme A est un ordre de K, il contient une $\mathbb{Q}$-base de K, disons $e_1, \ldots, e_n \in A$. Soit $x \in I$ non nul, alors $xe_1, \ldots, xe_n$ est une $\mathbb{Q}$-base de K constituée d'éléments de I. □

Ce théorème justifie l'importante définition qui suit.

Définition 6.16. *Si I est un idéal non nul de l'ordre A, on définit sa* norme $\mathrm{N}(I)$ *par la formule* $\mathrm{N}(I) = |A/I|$. *C'est un entier ≥ 1.*

La terminologie norme vient du lien qu'elle partage avec la norme de $K/\mathbb{Q}$. En effet, notons aussi $\mathrm{N} = \mathrm{N}_{K/\mathbb{Q}} : K \to \mathbb{Q}$ la norme de $K/\mathbb{Q}$. On rappelle que $\mathrm{N}(zz') = \mathrm{N}(z)\mathrm{N}(z')$ et que $\mathrm{N}(\mathcal{O}_K) \subset \mathbb{Z}$. De plus, $\mathrm{N}(z) = 0$ si, et seulement si, $z = 0$ car si $z \neq 0$ alors $1 = \mathrm{N}(1) = \mathrm{N}(z)\mathrm{N}(1/z)$.

Proposition 6.17. *Pour tout idéal non nul $I \subset A$ et tout $z \in A$ non nul,* $\mathrm{N}(zI) = |\mathrm{N}(z)|\mathrm{N}(I)$. *En particulier,* $\mathrm{N}(zA) = |\mathrm{N}(z)|$.

Démonstration — (C'est une généralisation de la proposition 4.12) Soit

$$a = (a_1, \cdots, a_{r_1+r_2}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$$

avec $a_i \neq 0$ pour tout i, et soit $d_a \in \mathrm{End}_{\mathbb{R}}(\mathbb{R}^{r_1} \times \mathbb{C}^{r_2})$ la dilatation définie par $d_a((x_i)) = (a_i x_i)$. La formule du changement de variables montre que l'application d_a multiplie la mesure de Lebesgue par

$$n(a) := \prod_{i=1}^{r_1} |a_i| \prod_{i=1}^{r_2} |a_{r_1+i}|^2$$

(c'est évident !). Revenant aux notations de l'énoncé, on constate que $\iota(zI) = d_{\iota(z)}(\iota(I))$. Ainsi, $\mathrm{covol}(zI) = n(\iota(z))|\mathrm{covol}(\iota(I))$, mais $n(\iota(z))$ n'est autre que $|\mathrm{N}(z)|$. □

Nous avons tous les outils pour appliquer le lemme du corps convexe de Minkowski aux idéaux d'un ordre. Si $r \in \mathbb{R}$ et $n \geq 1$, on appelle *constante de Minkowski* la constante $C(r, n) = (\frac{4}{\pi})^r \frac{n!}{n^n}$.

Théorème 6.18. (Minkowski) *Soit A un ordre de K et soit I un idéal non nul de A. Il existe $x \in I$ non nul tel que $|\mathrm{N}(x)| \leq C(r_2, n) \cdot \mathrm{N}(I) \cdot |\mathrm{disc}(A)|^{1/2}$.*

Ce théorème entraîne la proposition 6.7 avec $C \leq C(r_2, n)|\mathrm{disc}(A)|^{1/2}$. En effet, le noyau de la projection canonique $A/xA \to A/I$ est exactement I/xA, de sorte que $|I/xA||A/I| = |A/xA|$. Mais $|A/I| = \mathrm{N}(I)$ et $|A/xA| = \mathrm{N}(xA) = |\mathrm{N}_{K/\mathbb{Q}}(x)|$ d'après la proposition 6.17, de sorte que l'énoncé ci-dessus s'écrit aussi $|I/Ax| \leq C(r_2, n)|\mathrm{disc}(A)|^{1/2}$. Le théorème entraîne donc également le corollaire :

Corollaire 6.19. (Borne de Minkowski) *Si A est un ordre d'un corps de nombres K alors*

$$C(A) \leq C(r_2, n)\, |\mathrm{disc}(A)|^{1/2}, \quad \text{où } n = [K : \mathbb{Q}] \text{ et } r_2 = r_2(K).$$

Démonstration — (du théorème) Nous allons appliquer le lemme du corps convexe de Minkowski au réseau $\iota(I)$ de $V = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. Considérons la norme $|\cdot|$ sur V définie par

$$|(x_i)| = \sum_{i=1}^{r_1} |x_i| + 2 \sum_{i=r_1+1}^{r_1+r_2} |x_i|.$$

et pour tout réel $t > 0$ considérons $C_t = \{v \in V, |v| \leq t\}$ la boule fermée associée de centre 0 et de rayon t. Le fait qu'il s'agisse d'une norme est immédiat, et il en découle que C_t est convexe, compact et symétrique. Soit μ la mesure de Lebesgue sur V identifié à $\mathbb{R}^n$ comme plus haut.

Lemme 6.20. $\mu(C_t) = 2^{r_1}(\frac{\pi}{2})^{r_2} \frac{t^n}{n!}$.

Démonstration — En effet, désignons C_t par C_{t,r_1,r_2} pour bien mentionner la dépendance en r_1 et r_2, et posons $c(r_1, r_2) = \mu(C_{1,r_1,r_2})$ et $n = r_1 + 2r_2$. Par homothétie, $\mu(C_{t,r_1,r_2}) = c_{r_1,r_2} t^n$. De plus, si $r_1 > 0$ on constate par Fubini en intégrant selon la première coordonnée $x_1 \in [-1, 1]$ que

$$c_{r_1,r_2} = 2 \int_0^1 \mu(C_{1-t,r_1-1,r_2}) = 2c_{r_1-1,r_2} \int_0^1 (1-t)^{n-1} dt = \frac{2}{n} c_{r_1-1,r_2}.$$

Enfin, si $r_2 > 0$, on trouve de manière similaire en écrivant $x_{r_1+1} \in \mathbb{C}$ sous la forme $re^{i\theta}$:

$$c_{r_1,r_2} = 2\pi \int_0^{\frac{1}{2}} \mu(C_{1-2r,r_1,r_2-1}) r dr = 2\pi c_{r_1,r_2-1} \int_0^{\frac{1}{2}} (1-2r)^{n-2} r dr = \frac{\pi}{2n(n-1)} c_{r_1,r_2-1},$$

car $\int_0^1 (1-r) r^{n-2} dr = \frac{1}{n-1} - \frac{1}{n} = \frac{1}{n(n-1)}$. □

La pertinence de notre choix de $|.|$ vient de la relation qu'elle partage avec N. En effet, la moyenne arithmético-géométrique

$$(\prod_{i=1}^{r_1} |x_i| \prod_{i=r_1+1}^{r_1+r_2} |x_i|^2)^{\frac{1}{n}} \leq \frac{1}{n} (\sum_{i=1}^{r_1} |x_i| + 2 \sum_{i=r_1+1}^{r_1+r_2} |x_i|),$$

où les x_i sont dans $\mathbb{C}$, qui découle de la convexité de l'exponentielle réelle, entraîne

$$|\mathrm{N}(x)| \leq n^{-n} |\iota(x)|^n$$

pour tout $x \in K$. Pour conclure, on choisit $t > 0$ tel que $\mu(C_t) = 2^n \mathrm{covol}(\iota(I))$. Le lemme du corps convexe de Minkovski assure l'existence d'un élément de $\iota(x) \in \iota(I)$ non nul tel que $|\iota(x)| \leq t$, et donc tel que

$$|\mathrm{N}(x)| \leq n^{-n} t^n = \frac{n!}{2^{r_1} (\frac{\pi}{2})^{r_2} n^n} 2^n \mathrm{covol}(\iota(I)) = (\frac{4}{\pi})^{r_2} \frac{n!}{n^n} \mathrm{N}(I) 2^{r_2} \mathrm{covol}(\iota(A))$$

□

Terminons par un corollaire amusant du théorème 6.18, aussi dû à Minkowski.

Corollaire 6.21. (Minkowski) *Si $K \neq \mathbb{Q}$ alors $|\mathrm{disc}(\mathcal{O}_K)| \geq \frac{\pi}{3} (\frac{3\pi}{4})^{n-1}$. En particulier, on a $\mathrm{disc}(\mathcal{O}_K) \neq \pm 1$.*

Démonstration — On applique le théorème 6.18 à $A = I = \mathcal{O}_K$ et on utilise le fait que pour tout $x \in \mathcal{O}_K$ non nul, $\mathrm{N}(x)$ est entier non nul, et donc $|\mathrm{N}(x)| \geq 1$. Cela entraîne

$$|\mathrm{disc}(\mathcal{O}_K)| \geq C(r_2, n)^{-2} \geq a_n, \quad \text{avec} \quad a_n = C(\frac{n}{2}, n)^{-2},$$

car $r_2 \leq \frac{n}{2}$ et $\pi < 4$. Mais $a_2 = \frac{\pi^2}{4}$ et $\frac{a_{n+1}}{a_n} = \frac{\pi}{4}(1 + \frac{1}{n})^{2n} \geq \frac{3\pi}{4}$ pour $n > 1$, ce qui conclut. □

5. Exercices

D	2	9	22	39	61	88	120	157	199
h	0.90	1.90	2.98	3.97	4.97	5.97	6.97	7.97	8.98

Table 1. Quelques valeurs de $h = \frac{2}{\pi}\sqrt{D}$ à 10^{-2} près

Exercice 6.1. *(i) Soit D un entier $\equiv 0, 1 \bmod 4$ vérifiant $D < 0$. Vérifier que A_D est un ordre de $\mathbb{Q}(\sqrt{D})$ et que l'on a $\mathrm{disc}\, A_D = D$.*

(i) Soient $d \in \mathbb{Z}$, supposé < 0 et sans facteur carré, et $K = \mathbb{Q}(\sqrt{d})$. On pose $D = d$ si $d \equiv 1 \bmod 4$, et $D = 4d$ sinon. Rappeler pourquoi on a $\mathcal{O}_K = A_D$ et montrer plus généralement que les ordres de K sont exactement les anneaux de la forme A_{nD} avec $n \geq 1$.

Exercice 6.2. *On considère $\alpha = \frac{1+\sqrt{-19}}{2}$ et $A = \mathbb{Z}[\alpha]$.*

(i) Montrer que tout idéal de A est équivalent à un idéal contenant 1 ou 2.

(ii) En déduire que A est principal, bien que non euclidien.

Exercice 6.3. *On considère $\alpha = \sqrt{-5}$ et $A = \mathbb{Z}[\alpha]$.*

(i) Montrer que tout idéal de A est principal ou équivalent à l'idéal $I = 2A + (\alpha - 1)A$.

(ii) Montrer que I est non principal, en déduire que $|\mathrm{Cl}(A)| = 2$.

(iii) Montrer que $I^2 = (2)$ et en déduire que $\mathrm{Cl}(A) \simeq \mathbb{Z}/2\mathbb{Z}$.

(iv) En déduire que si J est un idéal non nul de A alors on a exclusivement soit J, soit IJ principal.

Exercice 6.4. *On considère $\alpha = \sqrt{-3}$ et $A = \mathbb{Z}[\alpha]$.*

(i) Montrer que tout idéal de A est principal ou équivalent à l'idéal $I = 2A + (\alpha - 1)A$.

(ii) Montrer que I est non principal, en déduire que $|\mathrm{Cl}(A)| = 2$.

(iii) Montrer que $I^2 = 2I$.

(iv) En déduire que $\mathrm{Cl}(A)$ n'est pas un groupe et décrire sa loi de composition.

(v) En déduire que si J est un idéal non nul de A alors IJ n'est jamais principal. Comparer avec l'exercice 6.3.

Exercice 6.5. *Soit $\alpha \in \mathbb{C}$ tel que $\alpha^3 = \alpha + 1$ et soit $A = \mathbb{Z}[\alpha]$.*

(i) Montrer que $\mathrm{disc}(A) = -23$.

(ii) En déduire que A est principal.

Exercice 6.6. *Montrer que $\mathrm{Cl}(\mathbb{Z}[\frac{1+\sqrt{-23}}{2}]) \simeq \mathbb{Z}/3\mathbb{Z}$.*

Exercice 6.7. *Soit $d \in \mathbb{Z}$ qui n'est pas un cube, soient $\alpha = \sqrt[3]{d}$ et $A = \mathbb{Z}[\alpha]$.*

(i) Montrer que $\mathrm{disc}(A) = -27d^2$.

On suppose maintenant $d = 2$. On donne la valeur $\frac{16}{\pi\sqrt{3}} \simeq 2.94$ à 10^{-2} près.

(ii) Montrer que tout idéal de A est soit principal soit équivalent à $I = 2A + \alpha A$ ou $J = 2A + \alpha^2 A$.

(iii) Montrer que I et J sont principaux.

(iv) En déduire que A est principal.

(v) En déduire que A est l'anneau des entiers de $\mathbb{Q}(\sqrt[3]{2})$.

Exercice 6.8. *Montrer que $\mathbb{Z}[e^{2i\pi/5}]$ est principal.*

Exercice 6.9. *Soit A un anneau intègre. Montrer que A est isomorphe à un ordre d'un corps de nombres si, et seulement si, le groupe additif de A est finiment engendré.*

Exercice 6.10. *On se propose de montrer que $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ est principal pour $d = -43, -67$ et -163.*

(i) Soient $P \in \mathbb{Z}[X]$ unitaire et p un nombre premier. On suppose que $P \bmod p$ est irréductible dans $(\mathbb{Z}/p\mathbb{Z})[X]$. Montrer que les idéaux de $A = \mathbb{Z}[X]/(P)$ contenant p^n sont les $p^i A$ avec $0 \leq i \leq n$.

(ii) Conclure.

Exercice 6.11. *Soit $P \in \mathbb{Z}[X]$ un polynôme unitaire de degré > 1. On se propose de montrer que $\mathrm{disc}(P) \neq \pm 1$, à moins que $P = (X-n)(X-n+1)$ avec $n \in \mathbb{Z}$.*

(i) Montrer que si P est irréductible alors $\mathrm{disc}(P) \neq \pm 1$. On utilisera le Corollaire 6.21.

(ii) Conclure en utilisant l'exercice 5.4.

(iii) En déduire que $-4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2 = \pm 1$ n'a pas de solution[4] $a, b, c \in \mathbb{Z}$.

(iv) Montrer que si P n'a pas de racine dans $\mathbb{Z}$, et si $\pm\mathrm{disc}(P)$ est premier, alors P est irréductible.

Exercice 6.12. (Principe des tiroirs) *On considère l'espace vectoriel $\mathbb{R}^n$ muni de la norme $|(x_i)| = \mathrm{Sup}_i|x_i|$ et on fixe un entier $N \geq 1$. Montrer que pour tout $v \in \mathbb{R}^n$, il existe un entier $1 \leq k \leq N^n$ et un $z \in \mathbb{Z}^n$ tels que $|kv - z| < \frac{1}{N}$. On pourra considérer l'application $\psi : \mathbb{R}^n \to [0,1[^n$, $(v_i) \mapsto (v_i - [v_i])$, et appliquer le principe des tiroirs aux éléments $\psi(kv)$ pour $k = 0, \ldots, N^n$.*

Exercice 6.13. *Soit A un ordre d'un corps de nombres K. On se propose de redémontrer la finitude de $\mathrm{Cl}(A)$ en utilisant simplement le principe des tiroirs (Exercice 6.12). On fixe $e_1, \ldots, e_n \in A$ une $\mathbb{Q}$-base de K et on pose $\mathrm{N} = \mathrm{N}_{K/\mathbb{Q}}$.*

4. On pourrait vérifier qu'une telle équation a pourtant des solutions dans $\mathbb{Z}/N\mathbb{Z}$ pour tout entier N et dans $\mathbb{R}$! On pourrait également démontrer que les solutions rationnelles sont les $(a,b,c) = (3r, 3r^2 - 1, r^3 - r \pm 1/3)$ avec $r \in \mathbb{Q}$.

(i) Soit $C = \mathrm{Sup}_{i,\sigma\in\Sigma(K)}|\sigma(e_i)| \in \mathbb{R}_{>0}$. *Montrer que pour tout* $x_1, \ldots, x_n \in \mathbb{Q}$ *on a*

$$|\mathrm{N}(\sum_i x_i e_i)| \leq C \cdot (\mathrm{Sup}_i|x_i|)^n.$$

(ii) ("Division euclidienne approchée") Soit N *la partie entière supérieure de* $C^{1/n}$. *Montrer que pour tout* $z \in K$ *il existe* $u \in A$ *et* $1 \leq k \leq N^n$ *tels que* $|\mathrm{N}(kz - u)| < 1$.

(iii) En déduire que si I *est un idéal non nul de* A, *et si* $x \in I$ *est tel que* $|\mathrm{N}(x)|$ *est non nul minimal (justifier), alors* $(N^n)!I \subset xA \subset I$.

(iv) Conclure que $\mathrm{Cl}(A)$ *est fini.*

(v) On suppose par exemple $A = \mathbb{Z}[\sqrt{d}]$ *avec disons* $d < 0$. *Montrer que* $(N^2)!$ *vaut environ* $d!$ *et comparer avec la méthode du cours !*

Problème 6.1. (Lucy et Lily, d'après R. Schwartz)

Soit P *un pentagone régulier du plan (Lucy) dont on colorie les sommets de* 5 *couleurs différentes. On construit alors*[5] *une suite de polygones* $P_0, P_1, \ldots, P_n$ *telle que* $P_0 = P$ *et* P_{i+1} *est obtenu en faisant subir à* P_i *une réflexion d'axe l'un des côtés arbitraire de* P_i. *On ne note pas les étapes intermédiaires.*

Problème *: sachant que l'on connaît les coordonnées exactes du centre de* P_n, *comment faire pour le ramener à sa position initiale* P *?*

Pour formaliser le problème, on pourra supposer que $P \subset \mathbb{C}$ *a pour sommets les* ζ^k *avec* $\zeta = e^{\frac{2i\pi}{5}}$ *et* $k \in \mathbb{Z}$. *Dans ce cas, le centre de* P_n *est un élément donné de* $\mathbb{Z}[\zeta]$ *(pourquoi ?). On pourra introduire un plongement complexe* $\mathbb{Q}[\zeta] \to \mathbb{C}$ *qui n'est ni l'inclusion, ni la conjugaison complexe, ainsi que l'image de* P *par ce plongement (Lily), et utiliser que* $\iota(\mathbb{Z}[\zeta])$ *est discret !*

5. Voici une applet Java, par R. Schwartz, permettant de faire ceci : http://www.math.brown.edu/~res/Java/App12/test1.html.