CHAPITRE 5

L'anneau des entiers d'un corps de nombres

Ce chapitre a pour but d'introduire l'anneau $\mathcal{O}_K$ des entiers algébriques d'un corps de nombres K, tel qu'il a été défini en toute généralité en 1877 par Richard Dedekind, le dernier élève de Gauss, dans son livre "*Sur la théorie des nombres entiers algébriques*" (en français !). Cette définition englobe notamment les anneaux introduits par Gauss et Eisenstein dans leurs études des *lois de réciprocité supérieures*, à savoir $\mathbb{Z}[i]$ et $\mathbb{Z}[\frac{1+i\sqrt{3}}{2}]$, et plus généralement celui des entiers cyclotomiques $\mathbb{Z}[e^{\frac{2i\pi}{n}}]$, étudié en détail par Kummer dans ses travaux sur le grand théorème de Fermat. Elle contient aussi certains anneaux d'entiers quadratiques étudiés au chapitre précédent, ce qui a par exemple permis à Dedekind de découvrir un point de vue plus simple sur la loi de Gauss de composition des formes binaires, que nous exposerons par ailleurs plus tard.

Nous commençons par développer les outils fondamentaux nécessaires à l'étude des nombres algébriques, à savoir les notions de trace, norme et discriminant. Cela nous obligera à commencer par quelques rappels de théorie des extensions de corps et de leurs plongements, avec lesquels nous supposerons une certaine familiarité, bien que les démonstrations ici soient complètes. Le résultat central de ce chapitre est un théorème de structure du groupe additif de $\mathcal{O}_K$. L'étude arithmétique de ce dernier fera l'objet des chapitres suivants.

Références : Nous renvoyons par exemple au livre *Algebra* de Serge Lang pour les rudiments de théorie des corps. En ce qui concerne les entiers des corps de nombres, on pourra consulter le chapitre 12 du livre de Ireland et Rosen, le chapitre 2 du livre de Samuel, ou le livre sus-cité de Dedekind !

1. Les corps de nombres et leurs plongements

Si L est un corps et si $K \subset L$ en est un sous-corps, l'addition de L et l'application $K \times L \to L$ induite par la multiplication de L définissent une structure de K-espace vectoriel sur L. En particulier, tout sous-corps L de $\mathbb{C}$ admet ainsi une structure naturelle de $\mathbb{Q}$-espace vectoriel : $1 \in L$ par définition, et donc $\mathbb{Q} \subset L$.

Définition 5.1. *Un corps de nombres est un sous-corps de $\mathbb{C}$ qui est de dimension finie comme $\mathbb{Q}$-espace vectoriel.*

Une *extension L/K de corps de nombres* est la donnée de deux corps de nombres L et K tels que $K \subset L$. Toute famille génératrice de L comme $\mathbb{Q}$-espace vectoriel en est encore une comme K-espace vectoriel, et donc L est alors de dimension finie comme K-espace vectoriel. On note $[L : K]$ cette dimension, que l'on appelle *degré de L sur K*. Lorsque $K = \mathbb{Q}$ on parle simplement du degré $[L : \mathbb{Q}]$ du corps de nombres L. Évidemment, $[L : \mathbb{Q}] = 1$ si, et seulement si, $L = \mathbb{Q}$, qui est le plus simple des corps de nombres. De même, $[L : K] = 1$ si, et seulement si, $L = K$.

On rappelle que $x \in \mathbb{C}$ est *algébrique* s'il existe un polynôme non nul $P \in \mathbb{Q}[X]$ tel que $P(x) = 0$. On note $\overline{\mathbb{Q}} \subset \mathbb{C}$ l'ensemble des nombres algébriques. Si K est un corps de nombres de degré n, et si $x \in K$, la famille $1, x, \ldots, x^n$ a $n+1$ éléments : elle est donc $\mathbb{Q}$-liée et $x \in \overline{\mathbb{Q}}$. Autrement dit :

Proposition 5.2. *Tout corps de nombres est inclus dans $\overline{\mathbb{Q}}$.*

Si $x \in \mathbb{C}$ et si K est un sous-corps de $\mathbb{C}$, on note $K[x] = \{P(x), P \in K[X]\}$ la sous-K-algèbre de $\mathbb{C}$ engendrée par x.

Proposition-Définition 5.3. *Si K est un corps de nombres et si $x \in \overline{\mathbb{Q}}$, alors $K[x]$ est un corps de nombres, que l'on notera aussi $K(x)$.*

Une manière de voir ceci est de considérer l'ensemble $I_{x,K} = \{P \in K[X], P(x) = 0\}$ des polynômes annulateurs de x à coefficients dans K. C'est clairement un idéal de $K[X]$, donc principal, qui est non nul car $x \in \overline{\mathbb{Q}}$: il est donc engendré par un unique polynôme unitaire

$$\Pi_{x,K} \in K[X].$$

Par définition, c'est le polynôme annulateur de x unitaire, de degré minimal, à coefficients dans K, et il est appelé *polynôme minimal de x sur K*. En particulier, il est irréductible dans $K[X]$. Le morphisme surjectif d'anneaux $K[X] \to K[x]$, $P \mapsto P(x)$, a pour noyau $I_{x,K} = (\Pi_{x,K})$, et induit donc un isomorphisme d'anneaux

$$K[X]/(\Pi_{x,K}) \xrightarrow{\sim} K[x].$$

On en déduit d'une part que si $n = \deg(\Pi_{x,K})$ alors $1, x, \ldots, x^{n-1}$ est une K-base de $K[x]$ ("division euclidienne et unicité du reste dans $K[X]$"). On en déduit aussi que $K[x]$ est un corps. En effet, tout élément non nul de $K[X]/(\Pi_{x,K})$ est représenté par un polynôme $P \in K[X]$ non nul tel que $\deg(P) < n$. Comme $\Pi_{x,K}$ est irréductible, il est premier avec P, et donc il existe $U, V \in K[X]$ tels que $PU + \Pi_x V = 1$ (Bézout dans $K[X]$), et donc $PU \equiv 1 \bmod \Pi_{x,K}$: P est inversible dans $K[X]/(\Pi_{x,K})$. □

Le cas le plus important de cette définition est celui où $K = \mathbb{Q}$. Nous verrons en fait plus loin que tout corps de nombres K est de la forme $\mathbb{Q}(x)$ pour (une infinité de) $x \in K$ (théorème de l'élément primitif).

Exemple 5.4. (Corps quadratiques et cyclotomiques) Parmi les exemples historiquement importants de corps de nombres, mentionnons les *corps cyclotomiques*, qui sont les $\mathbb{Q}(\zeta)$ où ζ est une racine de l'unité, ainsi que les *corps quadratiques*, de la forme $\mathbb{Q}(\sqrt{d})$ où $d \in \mathbb{Q}$ n'est pas un carré.

Si K est un corps de nombres et si $x_1, \ldots, x_n \in \overline{\mathbb{Q}}$, on note aussi $K(x_1, \ldots, x_n)$ le corps de nombres défini récursivement comme étant $(K(x_1, \ldots, x_{n-1}))(x_n)$. C'est le plus petit corps de nombres contenant K et les x_i, il ne dépend en particulier pas de l'ordre des x_i. En particulier, si $x, y \in \overline{\mathbb{Q}}$ alors $\mathbb{Q}(x, y)$ est un corps de nombres. Comme xy et $x - y \in \mathbb{Q}(x, y)$, on en déduit le fait bien connu suivant, qui se déduirait aussi très simplement de la proposition 1.15 :

Corollaire 5.5. *$\overline{\mathbb{Q}}$ est un sous-corps de $\mathbb{C}$.*

La proposition suivante, dite "de la base télescopique", est bien connue.

Proposition 5.6. *Si $K \subset L \subset M$ sont des corps de nombres alors $[M : K] = [M : L][L : K]$.*

Démonstration — On vérifie immédiatement que si $e_1, \ldots, e_n$ est une base du L-espace vectoriel M, et si $f_1, \ldots, f_m$ est une base du K-espace vectoriel L, alors les éléments $e_i f_j$, avec $1 \leq i \leq n$ et $1 \leq j \leq m$, forment une base du K-espace vectoriel M. □

Définition 5.7. *Si K est un corps de nombres on note $\Sigma(K)$ l'ensemble des morphismes de corps $K \to \mathbb{C}$, appelés aussi plongements, ou plongements complexes, de K.*

Si L/K est une extension de corps de nombres, on note $\Sigma(L/K)$ l'ensemble des plongements K-linéaires $L \to \mathbb{C}$. Autrement dit, $\Sigma(L/K) = \{\sigma \in \Sigma(L), \sigma_{|K} = \mathrm{id}\}$. En particulier, $\Sigma(L/\mathbb{Q}) = \Sigma(L)$.

La notion de plongement est une vaste généralisation de la notion de conjugaison complexe, ingrédient crucial dans la théorie de Galois. Elle est étroitement liée à celle de conjugué d'un nombre algébrique. On rappelle que si $x \in \overline{\mathbb{Q}}$ et si K est un corps de nombres, les K-conjugués de x sont les racines dans $\mathbb{C}$ du polynôme $\Pi_{x,K}$. Le lemme suivant montre qu'il y en a exactement $\deg(\Pi_{x,K})$.

Lemme 5.8. *Si $K \subset \mathbb{C}$ est un sous-corps et si $P \in K[X]$ est irréductible (donc non constant) alors P est scindé à racines simples dans $\mathbb{C}[X]$.*

Démonstration — En effet, P est scindé car $\mathbb{C}$ est algébriquement clos. D'autre part, $P' \in K[X]$ est un polynôme non nul de degré $< \deg(P)$, et donc premier à P dans $K[X]$, de sorte que P et P' n'ont pas de racine commune dans $\mathbb{C}$ (relation de Bézout). □

Les propriétés principales des plongements se résument en la proposition qui suit.

Proposition 5.9. *(i) (Lemme de prolongement) Soient $K \subset L$ des corps de nombres. L'application de restriction $\Sigma(L) \to \Sigma(K)$, $\sigma \mapsto \sigma_{|L}$, est surjective, chaque élément de $\Sigma(K)$ ayant exactement $[L : K]$ antécédents. En particulier $|\Sigma(L/K)| = [L : K]$.*

(ii) (Conjugués et plongements) Soit $x \in \overline{\mathbb{Q}}$, l'application $\Sigma(K(x)/K) \to \mathbb{C}$, $\sigma \mapsto \sigma(x)$, induit une injection d'image l'ensemble des K-conjugués de x.

Démonstration — Vérifions d'abord le (i) quand L est de la forme $K(x)$, où $x \in \overline{\mathbb{Q}}$. Fixons $\tau \in \Sigma(K)$. L'isomorphisme d'anneaux naturel $K[X]/(\Pi_{x,K}) \xrightarrow{\sim} K(x)$ entraîne que l'application

$$T = \{\sigma \in \Sigma(K(x)), \sigma_{|K} = \tau\} \longrightarrow \mathbb{C}, \sigma \mapsto \sigma(x),$$

est une injection, d'image l'ensemble des $y \in \mathbb{C}$ tels que $\Pi_{x,K}^{\tau}(y) = 0$. Rappelons que la notation Q^{τ}, pour $Q \in K[X]$ et $\tau \in \Sigma(K)$, désigne le polynôme Q auquel on a appliqué τ à tous les coefficients, en particulier $Q^{\tau} \in \tau(K)[X]$. On vérifie immédiatement que

$$(PQ)^{\tau} = P^{\tau} Q^{\tau} \quad \text{si} \quad P, Q \in K[X].$$

En particulier, $\Pi^{\tau}_{x,K}$ est irréductible dans $\tau(K)[X]$, car $\Pi_{x,K}$ l'est dans $K[X]$. Il a donc exactement $[K(x) : K]$ racines distinctes dans $\mathbb{C}$ par le lemme 5.8, et donc $|T| = [K(x) : K]$. Notons que le (ii) en découle : c'est le cas où τ est l'identité. Pour le cas général du (i), on se ramène au cas $L = K(x)$ par induction en écrivant $L = K(x_1, \ldots, x_r)$, l'assertion sur le nombre d'antécédents résultant de la base télescopique. □

Corollaire 5.10. (Théorème de l'élément primitif) *Tout corps de nombres est de la forme $\mathbb{Q}(x)$ pour un $x \in \overline{\mathbb{Q}}$.*

Démonstration — En effet, si K est un corps de nombres et si $L \subset K$ en est un sous-corps, le plongement $\mathrm{id} \in \Sigma(L)$ se prolonge à K de $[K : L]$-manières différentes d'après le lemme 5.9 (i). Si $L \neq K$ alors $[K : L] \geq 2$, et on peut donc trouver un tel prolongement $\sigma \in \Sigma(K)\backslash\{\mathrm{id}\}$. En particulier, le sous-$\mathbb{Q}$-espace vectoriel strict $H_\sigma = \{x \in K, \sigma(x) = x\}$ contient L. Mais comme $\mathbb{Q}$ est infini, la réunion finie des H_σ avec $\sigma \in \Sigma(K)\backslash\{\mathrm{id}\}$ n'est pas K tout entier : n'importe quel élément hors de cette réunion est donc primitif. Mieux, les H_σ introduits ci-dessus sont clairement des sous-corps stricts de K, de sorte que

$$K \setminus \bigcup_{\sigma \in \Sigma(K)\backslash\{\mathrm{id}\}} H_\sigma$$

est exactement l'ensemble des éléments primitifs de K. □

2. Trace, norme et discriminant : préliminaires algébriques

Dans tout ce paragraphe, on fixe L/K une extension de corps de nombres. Le lecteur ne perdrait pas grand chose à supposer $K = \mathbb{Q}$, mais cela ne simplifierait aucun des arguments qui vont suivre.

Si $x \in L$, considérons l'application de multiplication par x :

$$m_x : L \to L, y \mapsto xy.$$

C'est une application K-linéaire, autrement dit c'est un endomorphisme du K-espace vectoriel L. On note $\chi_{x,L/K} \in K[X]$ son polynôme caractéristique, $\mathrm{Tr}_{L/K}(x)$ sa trace, et $\mathrm{N}_{L/K}(x)$ son déterminant. Notons que ces deux derniers éléments sont dans K.

Proposition-Définition 5.11. *L'application $\mathrm{Tr}_{L/K} : L \to K$ ainsi définie est K-linéaire, on l'appelle la trace de L/K. De même, l'application $\mathrm{N}_{L/K} : L \to K$ est multiplicative : $\mathrm{N}_{L/K}(xy) = \mathrm{N}_{L/K}(x)\mathrm{N}_{L/K}(y)$ pour tout $x, y \in L$, on l'appelle la norme de L/K.*

Démonstration — En effet, la première assertion découle de la linéarité de la trace et de ce que pour tout $x, y \in L$ et $\lambda \in K$, on a l'identité $m_{\lambda x+y} = \lambda m_x + m_y$ dans les endomorphismes du K-espace vectoriel L. De même, la seconde assertion découle de la multiplicativité du déterminant et de l'identité, pour tout $x, y \in L$, $m_{xy} = m_x \cdot m_y$ dans les endomorphismes du K-espace vectoriel L. □

Exemple 5.12. Considérons par exemple le cas du corps quadratique $L = \mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Q}$ non carré, et $K = \mathbb{Q}$. Alors $1, \sqrt{d}$ est une $\mathbb{Q}$-base de $\mathbb{Q}(\sqrt{d})$. La matrice de la multiplication par $x = a + b\sqrt{d}$ avec $a, b \in \mathbb{Q}$ dans cette base est visiblement

$$\begin{pmatrix} a & db \\ b & a \end{pmatrix}$$

et donc $\mathrm{Tr}_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(x) = 2a$ et $\mathrm{N}_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(x) = a^2 - db^2$. Remarquons que la multiplicativité de la norme explique notamment l'identité remarquable $(a^2 - db^2)(\alpha^2 - d\beta^2) = (a\alpha + b\beta d)^2 - d(a\beta + \alpha b)^2$ pour tout $a, b, \alpha, \beta \in \mathbb{Q}$, car $(a + b\sqrt{d})(\alpha + \beta\sqrt{d}) = (a\alpha + b\beta d) + (a\beta + b\alpha)\sqrt{d}$.

Le théorème de Cayley-Hamilton assure que $\chi_{L/K}(m_x) = 0$ dans $\mathrm{End}_K(L)$, ce qui revient en fait au même que $\chi_{x,L/K}(x) = 0$: le polynôme $\chi_{x,L/K}$ est un polynôme annulateur de x dans $K[X]$. Cela fournit notamment un algorithme simple pour trouver un polynôme annulateur d'un élément $x \in L$ si l'on connaît une K-base de L et la décomposition de x dans cette base : on calcule le polynôme caractéristique de m_x. La relation entre $\chi_{x,L/K}$ et $\Pi_{x,K}$ est donnée par la proposition suivante :

Proposition 5.13. *Si $x \in L$ alors $\chi_{x,L/K} = \Pi_{x,K}^r$ où $r = [L : K(x)]$.*

Démonstration — Soient $n = [K(x) : K]$, $r = [L : K(x)]$, et $e_1, \ldots, e_r$ une base de L comme $K(x)$-espace vectoriel. Par la base télescopique, les éléments

$$e_1, xe_1, \ldots, x^{n-1}e_1, e_2, xe_2, \ldots, x^{n-1}e_2, \ldots, e_r, xe_r, \ldots, x^{n-1}e_r$$

forment une K-base de L. Mais pour chaque $1 \leq i \leq r$, la multiplication par x préserve le sous-espace $\oplus_{k=0}^{n-1} Ke_ix^k$. Sa matrice dans la base $e_i, xe_i, \ldots, x^{n-1}e_i$ est visiblement

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \ddots & \vdots & -a_1 \\ 0 & 1 & \ddots & 0 & -a_2 \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \cdots & 0 & 1 & -a_{n-1} \end{pmatrix},$$

où $\Pi_{x,K} = X^n + \sum_{i=0}^{n-1} a_i X^i$ (c'est la matrice compagnon de $\Pi_{x,K}$). Un développement par rapport à la dernière colonne montre que le polynôme caractéristique d'une telle matrice est exactement $X^n + \sum_{i=0}^{n-1} a_i X^i$, ce qui conclut. □

Proposition 5.14. *Soient L/K une extension de corps de nombres et $x \in L$.*

(i) $\mathrm{Tr}_{L/K}(x) = \sum_{\sigma \in \Sigma(L/K)} \sigma(x)$.

(ii) $\mathrm{N}_{L/K}(x) = \prod_{\sigma \in \Sigma(L/K)} \sigma(x)$.

(iii) $\chi_{x,L/K} = \prod_{\sigma \in \Sigma(L/K)} (X - \sigma(x))$ *dans* $\mathbb{C}[X]$.

Démonstration — Les relations (i) et (ii) se déduisent de la troisième, sur laquelle nous nous concentrons donc. Partons du fait que

$$\Pi_{x,K} = \prod_{\sigma \in \Sigma(K(x)/K)} (X - \sigma(x))$$

d'après la proposition 5.9 (ii). Mais pour tout $\sigma \in \Sigma(K(x)/K)$ il existe exactement $[L : K(x)]$ éléments $\sigma' \in \Sigma(L/K)$ tels que $\sigma'(x) = \sigma(x)$, d'après la proposition 5.9 (i) et (ii). On en déduit que

$$\prod_{\sigma \in \Sigma(L/K)} (X - \sigma(x)) = \Pi_{x,K}^{[L:K(x)]} = \chi_{x,L/K},$$

la dernière égalité venant de la proposition 5.13. □

Exemple 5.15. Continuons l'exemple de $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ avec $d \in \mathbb{Q}$ non carré. On a $\Sigma(\mathbb{Q}(\sqrt{d})) = \{\mathrm{id}, a + b\sqrt{d} \mapsto a - b\sqrt{d}\}$. On retrouve bien que $\mathrm{Tr}_{K/\mathbb{Q}}(a + b\sqrt{d}) = 2a$ et $\mathrm{N}_{K/\mathbb{Q}}(a + b\sqrt{d}) = a^2 - db^2$.

La forme K-linéaire trace $\mathrm{Tr}_{L/K} : L \to K$ nous permet de considérer l'application

$$L \times L \to K, (x, y) \mapsto \mathrm{Tr}_{L/K}(xy),$$

qui est donc K-bilinéaire et symétrique. Elle est même non dégénérée : pour tout $x \in L$ non nul, il existe $y \in L$ tel que $\mathrm{Tr}_{L/K}(xy) = 1$. En effet, il suffit de considérer l'élément $y = \frac{1}{[L:K]x} \in L$.

Soit $n = [L : K]$ et soit $e_1, \ldots, e_n$ une famille d'éléments de L. Si $x_1, \ldots, x_n \in K$ on considère l'élement $x = \sum_{j=1}^n x_j e_j$. En multipliant par e_i pour tout i et en prenant la trace on obtient un système linéaire à coefficients dans K :

$$\left(\mathrm{Tr}_{L/K}(e_i e_j)\right)_{1 \le i,j \le n} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \mathrm{Tr}_{L/K}(xe_1) \\ \mathrm{Tr}_{L/K}(xe_2) \\ \vdots \\ \mathrm{Tr}_{L/K}(xe_n) \end{pmatrix}. \tag{3}$$

Cela conduit à poser la définition suivante.

Définition 5.16. *Soit L/K une extension de corps de nombres de degré n. Le discriminant relatif à K d'une famille $e_1, \ldots, e_n$ d'éléments de L est le déterminant de la matrice*

$$(\mathrm{Tr}_{L/K}(e_i e_j))_{1 \le i,j \le n} \in \mathrm{M}_n(K).$$

On le note $\mathrm{disc}_{L/K}(e_1, \ldots, e_n)$, c'est un élément de K.

On rappelle que si $P \in \mathbb{C}[X]$ est unitaire, le discriminant de P est traditionnellement le nombre complexe $\mathrm{disc}(P) = \prod_{i<j}(x_i - x_j)^2$ où $P = \prod_i (X - x_i)$.

Proposition 5.17. *Soit L/K une extension de degré n et soit $e_1, \cdots, e_n \in L$.*

(i) $\mathrm{disc}_{L/K}(e_1, \ldots, e_n) \neq 0$ *si, et seulement si, $e_1, \ldots, e_n$ est une K-base de L.*

(ii) Si $P = (p_{i,j}) \in \mathrm{M}_n(K)$, et si l'on pose $f_j = \sum_i p_{i,j} e_i$ pour $j = 1, \cdots, n$, alors

$$\mathrm{disc}_{L/K}(f_1, \ldots, f_n) = \det(P)^2 \mathrm{disc}_{L/K}(e_1, \ldots, e_n).$$

(iii) $\mathrm{disc}_{L/K}(e_1, \ldots, e_n) = \det((\sigma_i(e_j))_{1 \le i,j \le n})^2$ *où* $\Sigma(L/K) = \{\sigma_1, \ldots, \sigma_n\}$.

(iv) Si $L = K(x)$, et si $x_1, \ldots, x_n \in \mathbb{C}$ sont les K-conjugués de x, alors

$$\mathrm{disc}_{K(x)/K}(1, x, x^2, \ldots, x^{n-1}) = \prod_{i<j}(x_i - x_j)^2 = (-1)^{\frac{n(n-1)}{2}} \mathrm{N}_{K(x)/K}(\Pi'_{x,K}(x)).$$

Démonstration — Vérifions le (i). Si les e_i sont K-liés il existe des $x_i \in K$ non tous nuls tels que $\sum_i x_i e_i = 0$, la relation (3) appliquée à $x = 0$ assure donc que $\mathrm{disc}_{L/K}(e_1, \ldots, e_n) = 0$. Réciproquement, soit ${}^t(x_1, \ldots, x_n)$ dans le noyau de la matrice $(\mathrm{Tr}_{L/K}(e_i e_j))_{1 \leq i,j, \leq n}$, et soit $x = \sum_i x_i e_i$. La relation (3) assure que $\mathrm{Tr}_{L/K}(x e_i) = 0$ pour tout i, et donc $e_1, \ldots, e_n$ n'est pas K-génératrice de L par non dégénéscence de $\mathrm{Tr}_{L/K}$.

Le (ii) est une propriété générale des formes bilinéaires : pour tout $x_i, y_j \in K$ on a la relation

$$\mathrm{Tr}_{L/K}((\sum_{i=1}^{n} x_i e_i)(\sum_{j=1}^{n} y_j e_j)) = {}^t \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} (\mathrm{Tr}_{L/K}(e_i e_j))_{1 \leq i,j, \leq n} \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}.$$

Dans les notations de l'énoncé on a donc $(\mathrm{Tr}_{L/K}(f_i f_j))_{1 \leq i,j, \leq n} = {}^t P (\mathrm{Tr}_{L/K}(e_i e_j))_{1 \leq i,j, \leq n} P$, ce qui conclut en prenant le déterminant.

Pour le (iii), on rappelle que $\mathrm{Tr}_{L/K} = \sum_{k=1}^{n} \sigma_k$. On constate alors que

$$(\mathrm{Tr}(e_i e_j))_{1 \leq i,j \leq n} = {}^t(\sigma_i(e_j))(\sigma_i(e_j)),$$

ce qui implique conclut en prenant le déterminant. La première égalité du (iv) s'en déduit (déterminant de Vandermonde). La seconde découle de la proposition 5.14 (ii) appliquée à l'élément $\Pi'_{x,K}(x)$.

Observons enfin que (i) et (iv) donnent une nouvelle démonstration du lemme 5.8. □

La formule (iv) s'écrit donc encore $\mathrm{disc}_{K(x)/K}(1, x, x^2, \ldots, x^{n-1}) = \mathrm{disc}(\Pi_{x,K})$, ce qui explique un peu la terminologie employée ! On rappelle les formules classiques $\mathrm{disc}(X^2 + aX + b) = a^2 - 4b$, $\mathrm{disc}(X^3 + aX + b) = -4a^3 - 27b^2$, et plus généralement

$$\mathrm{disc}(X^n + aX + b) = (-1)^{\frac{n(n-1)}{2}} (n^n b^{n-1} + (-1)^{n-1}(n-1)^{n-1} a^n).$$

Les coefficients de $\mathrm{disc}(P)$ sont toujours des polynômes universels à coefficients entiers en les coefficients de P (pourquoi ?), cependant assez compliqués quand $\deg(P)$ grandit, par exemple :

$$\mathrm{disc}(X^3 + aX^2 + bX + c) = -4a^3 c + a^2 b^2 + 18abc - 4b^3 - 27c^2.$$

En pratique, P étant donné, on calcule son discriminant à l'aide de l'ordinateur !

3. Entiers d'un corps de nombres

Dans tout ce paragraphe K est un corps de nombres fixé.

Définition 5.18. *(Dedekind) L'anneau des entiers du corps de nombres K est l'anneau $\mathcal{O}_K = K \cap \overline{\mathbb{Z}}$.*

C'est bien un anneau, comme intersection de deux anneaux (Proposition 1.15). À bien des égards, l'anneau $\mathcal{O}_K$ est à K ce que $\mathbb{Z}$ est à $\mathbb{Q}$. Par exemple, la proposition 1.14 du chapitre 1 se traduit en

$$\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}.$$

On commence par observer que $\mathcal{O}_K$ est toujours "assez gros".

Lemme 5.19. *Pour tout $x \in K$, il existe un entier non nul $m \in \mathbb{Z}$ tel que $mx \in \mathcal{O}_K$. En particulier, $\mathcal{O}_K$ engendre K comme $\mathbb{Q}$-espace vectoriel.*

Démonstration — En effet, soient $x \in K$ et $n = [\mathbb{Q}(x) : \mathbb{Q}]$. En nettoyant les dénominateurs de l'équation algébrique $\Pi_{x,\mathbb{Q}}(x) = 0$ on constate qu'il existe des entiers $a_0, a_1, \ldots, a_n \in \mathbb{Z}$ avec $a_n \neq 0$ tels que $\sum_{i=0}^{n} a_i x^i = 0$. En multipliant cette égalité par a_n^{n-1} on en déduit que $(a_n x)^n + \sum_{i=0}^{n-1} a_i a_n^{n-i} (a_n x)^i = 0$, et donc $m = a_n$ convient. □

Par construction, l'anneau $\mathcal{O}_K$ est intégralement clos.

Proposition 5.20. *Pour tout corps de nombres K, l'anneau $\mathcal{O}_K$ est intégralement clos.*

Démonstration — C'ést une conséquence de la définition $\mathcal{O}_K = K \cap \overline{\mathbb{Z}}$ et du fait que $\overline{\mathbb{Z}}$ est intégralement clos (Théorème 4.16). □

La détermination exacte de $\mathcal{O}_K$ est un problème difficile en général que nous allons maintenant aborder. Nous aurons besoin pour cela de critères simples caractérisant les entiers algébriques.

Théorème 5.21. *(Critère d'intégralité) Soit $x \in K$, il y a équivalence entre :*

(i) $x \in \mathcal{O}_K$,

(ii) $\Pi_{x,\mathbb{Q}} \in \mathbb{Z}[X]$,

(iii) $\chi_{x,K/\mathbb{Q}} \in \mathbb{Z}[X]$.

En particulier, si $x \in \mathcal{O}_K$ alors $\mathrm{Tr}_{K/\mathbb{Q}}(x) \in \mathbb{Z}$ et $\mathrm{N}_{K/\mathbb{Q}}(x) \in \mathbb{Z}$.

Démonstration — En effet, la dernière assertion découle de (i) ⇒ (iii). De plus, la relation $\chi_{x,K/\mathbb{Q}} = \Pi_{x,K/\mathbb{Q}}^{[K:\mathbb{Q}(x)]}$ assure que (ii) ⇒ (iii) ⇒ (i). Le point crucial, à savoir (i) ⇒ (ii), découle du lemme suivant. □

Lemme 5.22. *(i) Si x est dans $\mathcal{O}_K$ et si $\sigma \in \Sigma(K)$, alors $\sigma(x) \in \overline{\mathbb{Z}}$.*

(ii) Si L/K est une extension finie de corps de nombres, et si $x \in \mathcal{O}_L$, alors $\Pi_{x,L}$ et $\chi_{L/K}$ sont dans $\mathcal{O}_L[X]$. En particulier, $\mathrm{Tr}_{L/K}(x)$ et $\mathrm{N}_{L/K}(x)$ sont dans $\mathcal{O}_L$.

Démonstration — Pour le (i), on constate que si $x \in \mathcal{O}_K$, il existe par définition $a_0, a_1, \ldots, a_{n-1} \in \mathbb{Z}$ tels que $x^n + \sum_{i=0}^{n-1} a_i x^i = 0$. En appliquant un élément $\sigma \in \Sigma(K)$, on a $\sigma(x)^n + \sum_{i=0}^{n-1} a_i \sigma(x)^i = 0$, et donc $\sigma(x) \in \overline{\mathbb{Z}}$.

Pour le (ii), on rappelle que si $x \in L$ alors $\Pi_{x,K} = \prod_{\sigma \in \Sigma(K(x)/K)} (X - \sigma(x)) \in K[X]$. Mais si $x \in \mathcal{O}_L$ alors $\Pi_{x,K} \in \overline{\mathbb{Z}}[X]$ d'après le (i), et donc $\Pi_{x,K} \in \mathcal{O}_K[X]$. On conclut car $\chi_{x,L/K} = \Pi_{x,K}^{[L:K(x)]}$. □

Utilisons ce critère pour déterminer l'anneau des entiers des corps quadratiques, cas le plus simple après $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$.

Proposition 5.23. *Soient $d \in \mathbb{Z}\backslash\{0,1\}$ sans facteur carré et $K = \mathbb{Q}(\sqrt{d})$. Alors*

$$\mathcal{O}_K = \begin{cases} \mathbb{Z} + \mathbb{Z}\sqrt{d} & \text{si } d \equiv 2, 3 \bmod 4, \\ \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{d}}{2} & \text{si } d \equiv 1 \bmod 4 \end{cases}$$

Démonstration — Il est clair que $\sqrt{d} \in \mathcal{O}_K$ et on a déjà observé que $\alpha = \frac{1+\sqrt{d}}{2} \in \mathcal{O}_K$ si $d \equiv 1 \bmod 4$, car on a la relation $\alpha^2 - \alpha + \frac{1-d}{4} = 0$. Cela démontre les inclusions $\supset$ de l'énoncé. Observons aussi que $d \not\equiv 0 \bmod 4$ car d est sans facteur carré.

Réciproquement, soit $x = a + b\sqrt{d} \in \mathcal{O}_K$ avec $a, b \in \mathbb{Q}$. On a déjà vu que $\chi_{x,K/\mathbb{Q}} = T^2 - 2aT + (a^2 - db^2)$, i.e. $\mathrm{Tr}_{K/\mathbb{Q}}(x) = 2a$ et $\mathrm{N}_{K/\mathbb{Q}}(x) = a^2 - db^2$. Le théorème 5.21 entraîne donc que $2a, a^2 - db^2 \in \mathbb{Z}$. En particulier, $(2a)^2 - d(2b)^2 \in 4\mathbb{Z}$, donc $d(2b)^2 \in \mathbb{Z}$, puis $2b \in \mathbb{Z}$ car d est sans facteur carré. De même si $a \in \mathbb{Z}$ alors $b \in \mathbb{Z}$ et on a gagné. On peut donc supposer $2a$ impair. Dans ce cas, la relation $(2a)^2 \equiv d(2b)^2 \bmod 4$ entraîne que $2b$ est impair et que $d \equiv 1 \bmod 4$. Mézalors $x - \frac{1+\sqrt{d}}{2} = a' + b'\sqrt{d} \in \mathcal{O}_K$ avec $a' \in \mathbb{Z}$, et on conclut par le cas précédent. □

En particulier, on trouve que $\mathcal{O}_{\mathbb{Q}(i)}$ est l'anneau $\mathbb{Z}[i]$ des entiers de Gauss, et $\mathcal{O}_{\mathbb{Q}(j)}$, où $j = e^{2i\pi/3} = \frac{-1+i\sqrt{3}}{2}$, est celui des entiers d'Eisenstein $\mathbb{Z}[j]$. Nous sommes maintenant en mesure de terminer la démonstration de la proposition 4.17. En effet, elle découle du calcul précédent et de la proposition 5.20.

Si $\alpha \in \mathbb{C}$, on rappelle que l'on note $\mathbb{Z}[\alpha] = \{P(\alpha), P \in \mathbb{Z}[X]\}$. C'est le plus petit sous-anneau de $\mathbb{C}$ contenant α. Un sous-anneau $A \subset \mathbb{C}$ sera dit *monogène* si $A = \mathbb{Z}[\alpha]$ pour un certain $\alpha \in \mathbb{C}$. Nous verrons beaucoup d'exemples de corps de nombres K tels que $\mathcal{O}_K$ est monogène : c'est par exemple le cas des corps quadratiques comme on vient de le voir. Il ne faut pas croire cependant que c'est un phénomène général. Par exemple, nous verrons dans l'exercice 5.9 que si $d, d' \in \mathbb{Z}\backslash\{0,1\}$ sont distincts, sans facteur carré, tous deux $\equiv 1 \bmod 8$, et si $K = \mathbb{Q}(\sqrt{d}, \sqrt{d'})$ $(= \mathbb{Q}(\sqrt{d} + \sqrt{d'}))$, alors $\mathcal{O}_K$ n'est pas monogène.

Une propriété importante des sous-anneaux monogènes de $\overline{\mathbb{Z}}$ est la suivante.

Corollaire 5.24. *Si $\alpha \in \overline{\mathbb{Z}}$ alors le morphisme d'anneaux $\mathbb{Z}[X] \to \mathbb{Z}[\alpha]$, $P \mapsto P(\alpha)$, induit un isomorphisme d'anneaux*

$$\mathbb{Z}[X]/(\Pi_{x,\mathbb{Q}}) \xrightarrow{\sim} \mathbb{Z}[\alpha].$$

En particulier, $1, x, \ldots, x^{n-1}$ est une $\mathbb{Z}$-base de $\mathbb{Z}[\alpha]$ où $n = [\mathbb{Q}(x) : \mathbb{Q}]$.

Démonstration — L'application de l'énoncé est clairement un morphisme surjectif d'anneaux, de noyau $I = \{P \in \mathbb{Z}[X], P(\alpha) = 0\}$. La proposition précédente entraîne $\Pi_{x,\mathbb{Q}} \in I$, donc $(\Pi_{x,\mathbb{Q}}) \subset I$. Réciproquement, si $P \in I$ alors $P = \Pi_{x,\mathbb{Q}} Q$ où $Q \in \mathbb{Q}[X]$ par la propriété du polynôme minimal de x. Mais la division euclidienne d'un polynôme de $\mathbb{Z}[X]$ par un polynôme *unitaire* dans $\mathbb{Z}[X]$ a toujours un reste et un quotient dans $\mathbb{Z}[X]$, et donc $Q \in \mathbb{Z}[X]$, par unicité de la division euclidienne dans $\mathbb{Q}[X]$, ce qu'il fallait démontrer. Le dernier point découle encore de l'existence et unicité du reste et du quotient de la division euclidienne d'un $P \in \mathbb{Z}[X]$ par un $Q \in \mathbb{Z}[X]$ unitaire. □

4. Structure additive de $\mathcal{O}_K$ et discriminant de K

Soit K un corps de nombres.

Théorème 5.25. *(Dedekind) Le groupe additif de $\mathcal{O}_K$ admet une $\mathbb{Z}$-base à $n = [K : \mathbb{Q}]$ éléments. En particulier, il existe $e_1, \dots, e_n \in \mathcal{O}_K$ tels que $\mathcal{O}_K = \sum_{i=1}^n \mathbb{Z}e_i$.*

Autrement dit, $\mathcal{O}_K \simeq \mathbb{Z}^n$ comme groupe abélien. Si $\mathcal{O}_K$ est monogène, cela découle du Cor. 5.24.

Démonstration — D'après le théorème de l'élément primitif, il existe $x \in K$ tel que $K = \mathbb{Q}(x)$. Quitte à multiplier x par un entier $m \in \mathbb{Z}$, on peut de plus supposer que $x \in \overline{\mathbb{Z}}$ (Lemme 5.19). En particulier, $\mathbb{Z}[x] \subset \mathcal{O}_K$. Réciproquement, soit $z \in \mathcal{O}_K$. Si $n = [\mathbb{Q}(x) : \mathbb{Q}]$ alors $z = \sum_{i=0}^{n-1} z_i x^i$ où $z_i \in \mathbb{Q}$ pour tout i. Mais $\mathrm{Tr}_{K/\mathbb{Q}}(x^j z), \mathrm{Tr}_{K/\mathbb{Q}}(x^j x^k) \in \mathbb{Z}$ pour tout $j, k \in \mathbb{N}$ car $x, z \in \mathcal{O}_K$ (Théorème 5.21). En particulier, $d = \mathrm{disc}_{K/\mathbb{Q}}(1, x, \dots, x^{n-1})$ est un entier non nul par la proposition 5.17, et l'inversion du système linéaire (3) entraîne que les z_i sont dans $\frac{1}{d}\mathbb{Z}$, i.e.

$$\mathbb{Z}[x] \subset \mathcal{O}_K \subset \frac{1}{d}\mathbb{Z}[x].$$

Mais $\frac{1}{d}\mathbb{Z}[x]$ est un groupe abélien libre de rang n d'après le lemme 5.24, dont $\mathcal{O}_K$ peut donc être vu comme sous-réseau par la propriété d'inclusion ci-dessus, il est donc également libre de rang n d'après la caractérisation algébrique des réseaux (Thm. 2.4). □

Notons que cette démonstration fournit un algorithme pour calculer $\mathcal{O}_K$ en général. En effet, on commence par choisir un $x \in \overline{\mathbb{Z}}$ tel que $K = \mathbb{Q}(x)$ (un multiple d'un élément primitif), et on calcule $d = \mathrm{disc}_{K/\mathbb{Q}}(1, x, \dots, x^{n-1})$ où $n = [\mathbb{Q}(x) : \mathbb{Q}]$. On cherche alors à determiner le groupe abélien fini

$$\mathcal{O}_K/\mathbb{Z}[x] \subset (\frac{1}{d}\mathbb{Z}[x])/\mathbb{Z}[x] \simeq (\mathbb{Z}/d\mathbb{Z})^n.$$

Pour chacun des d^n représentants z du groupe quotient $\frac{1}{d}\mathbb{Z}[x]/\mathbb{Z}[x]$ on détermine si $z \in \mathcal{O}_K$, en vérifiant que son polynôme caractéristique est dans $\mathbb{Z}[X]$. Ceci étant fait, $\mathcal{O}_K$ est le groupe abélien engendré par $\mathbb{Z}[x]$ et l'ensemble des représentants de $\frac{1}{d}\mathbb{Z}[x]/\mathbb{Z}[x]$ qui sont des éléments de $\mathcal{O}_K$.

Cet algorithme résoud en théorie le problème de déterminer $\mathcal{O}_K$, mais il est souvent inefficace en pratique à cause du trop grand nombre de vérifications à effectuer. On peut en court-circuiter certaines étapes en étudiant directement l'équation $\chi_{x,K/\mathbb{Q}} \in \mathbb{Z}[X]$, mais cela s'avère fastidieux même dans les exemples les plus simples. Nous renvoyons à l'exercice 5.7 pour l'exemple de $\mathbb{Q}(\sqrt[3]{2})$ traité par cette méthode directe.

Observons qu'une $\mathbb{Z}$-base de $\mathcal{O}_K$ est nécessairement une $\mathbb{Q}$-base de K d'après le lemme 5.19. Comme on vient de l'expliquer, K étant donné il est en général difficile d'exhiber une $\mathbb{Z}$-base de $\mathcal{O}_K$. Des considérations de discriminant peuvent être cependant très utiles pour ces questions.

Proposition 5.26. *Soit $e_1, \cdots, e_n \in \mathcal{O}_K$ une $\mathbb{Q}$-base de K alors $\mathrm{disc}_{K/\mathbb{Q}}(e_1, \cdots, e_n)$ est un entier non nul. Soit (f_i) une autre famille ayant la même propriété et soit P la matrice des f_i dans la base (e_i). On suppose $f_j \in \sum_i \mathbb{Z}e_i$ pour tout j, i.e. $P \in \mathrm{M}_n(\mathbb{Z})$. Alors*

$$\mathrm{disc}_{K/\mathbb{Q}}(f_1, \cdots, f_n) = \det(P)^2 \mathrm{disc}_{K/\mathbb{Q}}(e_1, \cdots, e_n)$$

et $\sum_i \mathbb{Z}f_i$ est d'indice fini égal à $|\det(P)|$ dans $\sum_i \mathbb{Z}e_i$.

Démonstration — En effet, si $e_1, \cdots, e_n \in \mathcal{O}_K$ alors $(\mathrm{Tr}_{L/\mathbb{Q}}(e_i e_j)_{1 \leq i,j \leq n}) \in \mathrm{M}_n(\mathbb{Z})$, d'après le théorème 5.21, et donc $\mathrm{disc}_{K/\mathbb{Q}}(e_1, \ldots, e_n) \in \mathbb{Z}$. Il est non nul si (e_i) est une $\mathbb{Q}$-base de K d'après la proposition 5.17. Le premier point du lemme se déduit alors de la proposition 5.17 (ii). Le second découle de la proposition 2.17, après avoir identifié le groupe abélien $\sum_i \mathbb{Z}e_i$ au réseau $\mathbb{Z}^n$ de $\mathbb{R}^n$ via l'application linéaire $\sum_i x_i e_i \mapsto (x_i)$. □

En appliquant ce lemme à deux $\mathbb{Z}$-bases de $\mathcal{O}_K$, de sorte que $\det(P) = \pm 1$, on donne sens à la définition suivante.

Définition 5.27. *Soit K un corps de nombres. Le discriminant relatif à $K/\mathbb{Q}$ d'une $\mathbb{Z}$-base de $\mathcal{O}_K$ est un entier non nul qui ne dépend pas du choix de la base en question. On l'appelle le discriminant de K.*

La proposition ci-dessus révèle aussi que les $\mathbb{Z}$-bases de $\mathcal{O}_K$ sont exactement les familles $e_1, \ldots, e_n \in \mathcal{O}_K$ telles que $|\mathrm{disc}_{K/\mathbb{Q}}(e_1, \ldots, e_n)|$ est non nul et minimal. Nous verrons dans les exercices comment l'utiliser pour déterminer $\mathcal{O}_K$ dans des cas particuliers.

5. Entiers des corps cyclotomiques

Nous allons conclure ce chapitre en déterminant l'anneau des entiers de certains corps cyclotomiques. Soit $n \geq 1$ un entier et soit $\zeta = e^{2i\pi/n}$. On rappelle que le n-ième polynôme cyclotomique est le polynôme

$$\Phi_n(X) = \prod_{k \in (\mathbb{Z}/n\mathbb{Z})^\times} (X - \zeta^k) \in \mathbb{C}[X].$$

Il est donc de degré $\varphi(n)$. Il est bien connu que ce polynôme est dans $\mathbb{Z}[X]$ et qu'il est irréductible dans $\mathbb{Q}[X]$ (Gauss). Autrement dit, $\Phi_n = \Pi_{\zeta,\mathbb{Q}}$. Le théorème suivant est dû à Kummer.

Théorème 5.28. *Si $K = \mathbb{Q}(\zeta)$ avec $\zeta \in \mathbb{C}$ une racine de l'unité, alors $\mathcal{O}_K = \mathbb{Z}[\zeta]$.*

Pour simplifier nous ne démontrerons ce résultat que lorsque ζ est une racine de l'unité d'ordre p^r avec p un nombre premier. Dans ce cas, $\Phi_{p^r}(X) = \frac{X^{p^r}-1}{X^{p^{r-1}}-1} = \sum_{i=0}^{p-1} X^{ip^{r-1}} \in \mathbb{Z}[X]$. De plus, l'irréductibilité de Φ_{p^r} dans $\mathbb{Q}[X]$ est une conséquence du critère d'Eisenstein, rappelons pourquoi.

On rappelle qu'un polynôme unitaire $P = X^n + \sum_{i=0}^{n-1} a_i X^i \in \mathbb{Z}[X]$ est un *polynôme d'Eisenstein en le nombre premier p* si p divise $a_0, \ldots, a_{n-1}$ mais p^2 ne divise pas a_0. Le *critère d'Eisenstein* assure alors que P est irréductible [1] dans $\mathbb{Q}[X]$.

1. Donnons-en une démonstation. D'après le lemme de Gauss, il suffit de voir qu'il est irréductible dans $\mathbb{Z}[X]$ (voir l'exercice 5.13). Soit $P = AB$ avec $A, B \in \mathbb{Z}[X]$. On peut supposer que A et

Vérifions que le polynôme $\Phi_{p^r}(X+1)$ est d'Eisenstein en p. En effet, le petit théorème de Fermat entraîne

$$\Phi_{p^r}(X+1) \equiv X^{p^r-p^{r-1}} \bmod p\mathbb{Z}[X].$$

On conclut car $\Phi_{p^r}(0) = p$ (règle de l'Hôpital !). L'irréductibilité de $\Phi_{p^r}(\mathrm{X}+1)$ dans $\mathbb{Q}[X]$ découle alors du critère d'Eisenstein, ainsi que celle de son translaté $\Phi_{p^r}(X)$.

Observons de plus que si $x = \zeta - 1$ alors (voir l'exercice 5.4)

$$\mathrm{disc}_{K/\mathbb{Q}}(1, x, \ldots, x^{\varphi(p^r)-1}) = \mathrm{disc}(\Phi_{p^r}(X+1)) = \mathrm{disc}(\Phi_{p^r}) \mid \mathrm{disc}(X^{p^r}-1) = \pm p^{rp^r}.$$

En particulier $\pm\mathrm{disc}(K)$ est une puissance de p d'après la proposition 5.26. Il suffit donc pour conclure de démontrer que $\mathbb{Z}[\zeta] = \mathbb{Z}[\zeta - 1]$ est d'indice premier à p dans $\mathcal{O}_K$. Cela découle de la proposition suivante.

Proposition 5.29. *Soit $K = \mathbb{Q}(x)$ un corps de nombres avec $x \in \overline{\mathbb{Z}}$. On suppose que $\Pi_{x,\mathbb{Q}}$ est un polynôme d'Eisenstein en le nombre premier p. Alors $\mathbb{Z}[x]$ est d'indice premier à p dans $\mathcal{O}_K$.*

Démonstration — On a déjà vu que le groupe abélien $\mathcal{O}_K/\mathbb{Z}[x]$ est fini (démonstration du théorème 5.25). Supposons que son cardinal soit multiple de p. Le lemme de Cauchy entraîne alors qu'il existe $z \in \mathcal{O}_K \backslash \mathbb{Z}[x]$ tel que $pz \in \mathbb{Z}[x]$. Ainsi, $pz = \sum_{i=0}^{n-1} b_i x^i \in p\mathcal{O}_K$ où les b_i sont $\mathbb{Z}$ et non tous dans $p\mathbb{Z}$. Nous allons contredire ceci en montrant que p divise b_i pour tout i. On part pour cela de la congruence dans $\overline{\mathbb{Z}}$

$$\sum_{i=0}^{n-1} b_i x^i \equiv 0 \bmod p. \tag{4}$$

Pour $i \geq n$, on a de plus $x^i \equiv 0 \bmod p$ par hypothèse sur $\Pi_{x,\mathbb{Q}}$. Ainsi, si l'on multiplie l'équation (4) par x^{n-1}, il ne reste que $b_0 x^{n-1} \equiv 0 \bmod p$. Autrement dit, on a $b_0 x^{n-1} = pa$ avec $a \in \mathcal{O}_K$. En prenant la norme on trouve $b_0^n \mathrm{N}_{K/\mathbb{Q}}(x)^{n-1} \equiv 0 \bmod p^n$. Mais $\mathrm{N}_{K/\mathbb{Q}}(x) = \pm a_0$ car $\chi_{x,K/\mathbb{Q}} = \Pi_{x,\mathbb{Q}}$, qui est divisible par p mais non par p^2 par hypothèse. Il vient que p divise b_0. En multipliant ensuite (4) successivement par $x^{n-2}, \ldots, x, 1$ on déduit de même successivement $b_1 \equiv \cdots \equiv b_{n-2} \equiv b_{n-1} \equiv 0 \bmod p$. □

Exemple 5.30. En guise d'exemple, vérifions que si $K = \mathbb{Q}(x)$ avec $x = \sqrt[3]{2}$, alors $\mathcal{O}_K = \mathbb{Z}[x]$. En effet, $\mathrm{disc}_{K/\mathbb{Q}}(1, x, x^2) = \mathrm{disc}(P) = -2^2 \cdot 3^3$ où $P = X^3 - 2$. En particulier, $|\mathcal{O}_K/\mathbb{Z}[x]|$ divise $2^2 \cdot 3^3$. Mais P et $P(X-1) = (X-1)^3 - 2 = X^3 - 3X^2 + 3X - 3$ sont des polynômes d'Eisenstein respectivement pour $p = 2$ et 3. Comme $\mathbb{Z}[x] = \mathbb{Z}[x-1]$, la proposition montre que $|\mathcal{O}_K/\mathbb{Z}[x]|$ est premier à 2 et à 3, c'est donc 1. On pourra comparer avec la méthode directe de l'exercice 5.7.

B sont unitaires quitte à écrire $P = (-A)(-B)$. On a $P \equiv X^n \equiv AB$ dans $(\mathbb{Z}/p\mathbb{Z})[X]$. Comme $\mathbb{Z}/p\mathbb{Z}$ est un corps, cela entraîne $A \equiv X^i$ et $B \equiv X^j$ avec $i + j = n$. Si $i, j \geq 1$, alors p divise $A(0)$ et $B(0)$, et donc p^2 divise $P(0) = A(0)B(0)$: absurde, donc $i = 1$ ou $j = 1$. Mais comme A et B sont unitaires cela entraîne $A = 1$ ou $B = 1$.

6. Exercices

Exercice 5.1. *Montrer qu'un corps de nombres de degré 2 est de la forme* $\mathbb{Q}(\sqrt{d})$ *pour un unique* $d \in \mathbb{Z}\backslash\{0,1\}$ *sans facteur carré.*

Exercice 5.2. *Montrer que tout corps quadratique est inclus dans un corps cyclotomique.*

Exercice 5.3. *Soit* $d \in \mathbb{Z}$*. Montrer que le produit de deux nombres de la forme* $a^3+db^3+d^2c^3-3abcd$*, avec* $a,b,c \in \mathbb{Z}$*, est encore de cette forme. On pourra d'abord supposer que* d *n'est pas un cube et considérer le corps de nombres* $\mathbb{Q}(\sqrt[3]{d})$*.*

Exercice 5.4. *Soient* $P, Q \in \mathbb{Z}[X]$ *des polynômes unitaires. On suppose* $\mathrm{disc}(Q) \neq 0$*. Montrer que si* P *divise* Q *dans* $\mathbb{Q}[X]$ *alors* $\mathrm{disc}(P)$ *divise* $\mathrm{disc}(Q)$ *dans* $\mathbb{Z}$*.*

Exercice 5.5. *Soit* $K = \mathbb{Q}(\sqrt{d})$ *avec* $d \in \mathbb{Z}\backslash\{0,1\}$ *sans facteur carré. Montrer que* $\mathrm{disc}(K) = d$ *ou* $4d$*, selon que* $d \equiv 1 \bmod 4$ *ou non.*

Exercice 5.6. *(i) Soient* K *un corps de nombres et* $e_1, \dots, e_n \in \mathcal{O}_K$ *tels que* $\mathrm{disc}_{K/\mathbb{Q}}(e_1, \dots, e_n)$ *est non nul et sans facteur carré. Montrer que* $e_1, \dots, e_n$ *est une* $\mathbb{Z}$*-base de* $\mathcal{O}_K$*.*

(ii) Soit $K = \mathbb{Q}(x)$ *où* $x \in \mathbb{C}$ *satisfait* $x^3 - x + 1 = 0$*. Montrer que* $[K : \mathbb{Q}] = 3$ *puis que* $\mathcal{O}_K = \mathbb{Z}[x]$*.*

Exercice 5.7. *On se propose de montrer sans utiliser la proposition 5.29 que si* $K = \mathbb{Q}(\sqrt[3]{2})$ *alors* $\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{2}]$*. On pose* $x = \sqrt[3]{2}$ *et on fixe* $z = a + bx + cx^2 \in K$ *avec* $a, b, c \in \mathbb{Q}$*.*

(i) Vérifier que $\chi_{z,K/\mathbb{Q}} = X^3 - 3aX^2 + 3(a^2 - 2bc)X - (a^3 + 2b^3 + 4c^3 - 6abc)$*.*

On suppose dorénavant $z \in \mathcal{O}_K$*.*

(ii) En considérant $\mathrm{Tr}_{K/\mathbb{Q}}(x^i z)$*, montrer que* $6b,\ 6c \in \mathbb{Z}$*.*

(iii) En déduire que $3a, 3b, 3c \in \mathbb{Z}$*. On pourra multiplier* $a^3 + 2b^3 + 4c^3 - 6abc$ *par* 2.3^3 *puis* 3^3*.*

On pose $3a = \alpha$*,* $3b = \beta$ *et* $3c = \gamma$*, de sorte que* $\alpha, \beta, \gamma \in \mathbb{Z}$*.*

(iv) Vérifier que $\alpha^2 \equiv 2\beta\gamma \bmod 3$*,* $\alpha - \beta + \gamma \equiv 0 \bmod 3$*, puis que* $\alpha \equiv \gamma \equiv -\beta \bmod 3$*.*

(v) Vérifier que $\pm\frac{1}{3}(1 - x + x^2) \notin \mathcal{O}_K$ *et conclure.*

Exercice 5.8. *Soient* $m, n \in \mathbb{Z}\backslash\{0,1\}$ *des entiers distincts, sans facteur carré, et tels que* $m \equiv n \equiv 1 \bmod 4$*. On se propose de montrer que si* $K = \mathbb{Q}(\sqrt{m}, \sqrt{n})$ *alors* $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\alpha + \mathbb{Z}\beta + \mathbb{Z}\alpha\beta$ *où* $\alpha = \frac{1+\sqrt{n}}{2}$ *et* $\beta = \frac{1+\sqrt{m}}{2}$*.*

(i) Montrer $[K : \mathbb{Q}] = 4$ *et déterminer* $\Sigma(K)$*.*

(ii) Vérifier $\mathrm{disc}_{K/\mathbb{Q}}(1,\alpha,\beta,\alpha\beta) = m^2n^2$.

(iii) Montrer $4\mathcal{O}_K \subset \mathbb{Z}+\mathbb{Z}\sqrt{n}+\mathbb{Z}\sqrt{m}+\mathbb{Z}\sqrt{mn}$ *(utiliser des traces sur* $\mathbb{Q}(\sqrt{n}), \mathbb{Q}(\sqrt{m}), \mathbb{Q}(\sqrt{mn})$*)*

(iv) Conclure.

Exercice 5.9. *(Un exemple d'anneau des entiers non monogène) On considère* $K = \mathbb{Q}(\sqrt{n},\sqrt{m})$ *avec* $m,n \in \mathbb{Z}\backslash\{0,1\}$ *sans facteur carré, distincts, et tels que* $m \equiv n \equiv 1 \bmod 8$*. On va montrer qu'il n'existe pas d'élément* $x \in \mathcal{O}_K$ *tel que* $\mathcal{O}_K = \mathbb{Z}[x]$.

(i) En utilisant le résultat de l'exercice 5.8, montrer que l'anneau $\mathcal{O}_K/2\mathcal{O}_K$ *est isomorphe à*

$$A = (\mathbb{Z}/2\mathbb{Z})[X,Y]/(X^2-X, Y^2-Y).$$

(ii) Vérifier que l'anneau A *admet exactement quatre morphismes d'anneaux distincts* $A \to \mathbb{Z}/2\mathbb{Z}$.

(iii) En déduire que l'anneau A *n'est pas isomorphe à* $(\mathbb{Z}/2\mathbb{Z})[X]/(P)$ *où* $P \in (\mathbb{Z}/2\mathbb{Z})[X]$ *est de degré* 4*. On pourra constater que les morphismes d'anneaux* $(\mathbb{Z}/2\mathbb{Z})[X]/(P) \to \mathbb{Z}/2\mathbb{Z}$ *sont en bijection avec l'ensemble des racines de* P *dans* $\mathbb{Z}/2\mathbb{Z}$.

(iv) Conclure.

Exercice 5.10. *Soit* K *un corps de nombres. Montrer que* $\mathcal{O}_K^\times = \{x \in \mathcal{O}_K, \mathrm{N}_{K/\mathbb{Q}}(x) = \pm 1\}$.

Exercice 5.11. *Soit* $K \subset \mathbb{C}$ *un corps de nombres. On note* $\mu(K) \subset \mathcal{O}_K^\times$ *l'ensemble des racines de l'unité appartenant à* K *et on pose* $U(K) = \{z \in \mathcal{O}_K, |\sigma(z)| = 1 \ \forall\ \sigma \in \Sigma(K)\}$.

(i) Montrer que $U(K)$ *est un sous-groupe de* O_K^* *contenant* $\mu(K)$.

(ii) Montrer que $\{\chi_{x,K/\mathbb{Q}}, x \in U(K)\} \subset \mathbb{Q}[X]$ *est un ensemble fini.*

(iii) En déduire que $U(K)$ *est fini, puis que* $U(K) = \mu(K) = \{\zeta \in \mathbb{C}, \zeta^n = 1\}$ *où* $n = |U(K)|$.

(iv) (suite) Montrer que $\varphi(n) \,|\, [K:\mathbb{Q}]$.

(v) (Kronecker) Montrer que si $x \in \overline{\mathbb{Z}}$ *a tous ses conjugués de module* 1 *alors* x *est une racine de l'unité.*

Exercice 5.12. *Soit* $\alpha \in \overline{\mathbb{Z}}$*. Montrer que* $\mathbb{Z}[\alpha]$ *est intégralement clos si, et seulement si,* $\mathbb{Z}[\alpha]$ *est l'anneau des entiers de* $\mathbb{Q}(\alpha)$.

L'exercice suivant donne un autre point de vue sur un théorème de Gauss (Exercice 4.12).

Exercice 5.13. (Irréductibilité dans $\mathbb{Z}[X]$ et $\mathbb{Q}[X]$)

(i) Soient $P,Q,R \in \mathbb{Q}[X]$ *des polynômes unitaires tels que* $P = QR$*. Montrer que si* $P \in \mathbb{Z}[X]$ *alors* $Q,R \in \mathbb{Z}[X]$*. On pourra observer que les racines de* P *dans* $\mathbb{C}$ *sont dans* $\overline{\mathbb{Z}}$.

(ii) En déduire que si $P \in \mathbb{Z}[X]$ est irréductible et unitaire, alors P est irréductible dans $\mathbb{Q}[X]$.

(iii) (Application) Montrer que si $P \in \mathbb{Z}[X]$ est unitaire, et s'il existe un entier $N \geq 1$ tel que $P \bmod N$ est irréductible dans $(\mathbb{Z}/N\mathbb{Z})[X]$, alors P est irréductible dans $\mathbb{Q}[X]$.

Exercice 5.14. *Soit p un nombre premier impair et $\zeta = e^{\frac{2i\pi}{p}}$. Montrer que* $\mathrm{disc}(\mathbb{Q}(\zeta)) = (-1)^{\frac{p-1}{2}} p^{p-2}$.

Exercice 5.15. (Signe du discriminant) *Soit K un corps de nombres. Montrer que le signe de* $\mathrm{disc}(K)$ *est $(-1)^s$ où $2s$ est le nombre des $\sigma \in \Sigma(K)$ tels que $\sigma(K) \not\subset \mathbb{R}$.*

Exercice 5.16. (Théorème de Stickelberger) *Soit $P \in \mathbb{Z}[X]$ un polynôme unitaire.*

(i) Si $P = \prod_{i=1}^{n}(X - x_i)$, montrer que $\prod_{1 \leq i < j \leq n}(x_i + x_j) \in \mathbb{Z}$.

(ii) En déduire que $\mathrm{disc}(P) \equiv 0, 1 \bmod 4$.

En déduire que si K est un corps de nombres alors $\mathrm{disc}(K) \equiv 0, 1 \bmod 4$.

Problème 5.1. *Soient M/L et L/K des extensions de corps de nombres. Montrer que :*

(i) $\mathrm{Tr}_{L/K} \circ \mathrm{Tr}_{M/L} = \mathrm{Tr}_{M/K}$,

(ii) $\mathrm{N}_{L/K} \circ \mathrm{N}_{M/L} = \mathrm{N}_{M/K}$.