

Sixième fascicule : 24/03/2008

4 Corps de Nombres

4.1 Norme, trace, discriminant

Rappelons que tous les anneaux considérés sont commutatifs et unitaires. Les éléments inversibles (on dit encore *les unités*) d'un anneau A forment un groupe multiplicatif noté A^\times .

Soient A un anneau, M un A -module libre de type fini et u un endomorphisme de M . On note $\text{Tr}(u)$, $N(u)$ et $P_u(X)$ la trace, la norme et le polynôme caractéristique de u respectivement. Dans une base (e_1, \dots, e_n) de M sur A , si $A = (a_{ij})_{1 \leq i, j \leq n}$ désigne la matrice attachée à u , on a

$$\text{Tr}(u) = \sum_{i=1}^n a_{ii} \quad \text{et} \quad N(u) = \det(A).$$

D'autre part en désignant par I l'endomorphisme identité de M on a

$$P_u(X) = \det(XI - u) = X^n - \text{Tr}(u)X^{n-1} + \dots + (-1)^n N(u).$$

Quand u_1 et u_2 sont des endomorphismes de M on a

$$\text{Tr}(u_1 + u_2) = \text{Tr}(u_1) + \text{Tr}(u_2) \quad \text{et} \quad N(u_1 \circ u_2) = N(u_1)N(u_2).$$

Supposons de plus que M est un anneau - on le notera B . Soit donc B un anneau contenant A qui est un A -module libre de rang fini. Pour $x \in B$ l'application

$$[x] : \begin{array}{ccc} B & \longrightarrow & B \\ y & \longmapsto & xy \end{array}$$

est un endomorphisme du A -module B et l'application $x \mapsto [x]$ est un homomorphisme d'anneaux de B dans l'anneau des endomorphismes de B .

La norme, la trace et le polynôme caractéristique de $[x]$ sont appelés *norme*, *trace* et *polynôme caractéristique* de x de B sur A et notés respectivement

$$N_{B/A}(x), \quad \text{Tr}_{B/A}(x) \quad \text{et} \quad P_{B/A}(x; X).$$

On a donc, pour x et y dans B ,

$$N_{B/A}(xy) = N_{B/A}(x)N_{B/A}(y) \tag{4.1}$$

et

$$\mathrm{Tr}_{B/A}(x + y) = \mathrm{Tr}_{B/A}(x) + \mathrm{Tr}_{B/A}(y).$$

Soit L/K une extension finie de corps et soit $m = [L : K]$ son degré. La norme de L sur K définit un homomorphisme du groupe multiplicatif L^\times de L dans le groupe multiplicatif K^\times de K et la trace un homomorphisme du groupe additif L dans le groupe additif K .

Lemme 4.2. *Soit L/K une extension séparable de degré n . Soit N une extension finie de L , normale sur K et soient $\sigma_1, \dots, \sigma_n$ les différents K -isomorphismes de L dans N . Alors pour $\alpha \in L$ on a*

$$\mathrm{Tr}_{L/K}(\alpha) = \sum_{i=1}^n \sigma_i(\alpha), \quad \mathrm{N}_{L/K}(\alpha) = \prod_{i=1}^n \sigma_i(\alpha)$$

et

$$P_{L/K}(\alpha; X) = \prod_{i=1}^n (X - \sigma_i(\alpha)).$$

Démonstration. Soit d le degré de α sur K et

$$P(X) = X^d + a_1 X^{d-1} + \dots + a_d \in K[X]$$

son polynôme irréductible sur K . Supposons dans un premier temps que α est un élément primitif de l'extension L/K , c'est-à-dire que $L = K(\alpha)$ ou encore que $d = n$. Quand on prend $\{1, \alpha, \dots, \alpha^{d-1}\}$ comme base de L sur K , la matrice associée à l'endomorphisme $[\alpha]$ est

$$M_\alpha = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_d \\ 1 & 0 & \cdots & 0 & -a_{d-1} \\ 0 & 1 & \cdots & 0 & -a_{d-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_1 \end{pmatrix}.$$

Par conséquent le polynôme caractéristique de $[\alpha]$ est le polynôme irréductible de α sur K . Le fait qu'il s'écrive

$$\prod_{i=1}^d (X - \sigma_i(\alpha))$$

provient du Théorème 2.19.

Dans le cas général on note $d = [K(\alpha) : K]$ et $m = [L : K(\alpha)]$, de sorte que $n = md$ et on prend une base (e_1, \dots, e_m) de L sur $K(\alpha)$. Dans la base $\{e_i \alpha^j ; 1 \leq i \leq m, 0 \leq j < d\}$ de L sur K la matrice de $[\alpha]$ s'écrit comme un bloc diagonal $\mathrm{diag}(M_\alpha, \dots, M_\alpha)$. Donc

$$P_{L/K}(\alpha; X) = P(X)^m,$$

$$\mathrm{Tr}_{L/K}(\alpha) = m \mathrm{Tr}_{K(\alpha)/K}(\alpha), \quad \mathrm{N}_{L/K}(\alpha) = (\mathrm{N}_{K(\alpha)/K}(\alpha))^m.$$

Enfin la suite $(\sigma_1(\alpha), \dots, \sigma_n(\alpha))$ est formée des d conjugués de α sur K , chacun étant répété m fois. \square

Lemme 4.3. Soit L/K une extension finie séparable. L'application

$$\begin{aligned} L \times L &\rightarrow K \\ (x, y) &\mapsto \text{Tr}_{L/K}(xy) \end{aligned}$$

est une forme bilinéaire symétrique non dégénérée sur L .

Il en résulte que l'application qui à $x \in L$ associe $y \mapsto \text{Tr}_{L/K}(xy)$ est un isomorphisme du K -espace vectoriel L sur son dual $\text{Hom}_K(L, K)$.

Démonstration du lemme 4.3. Que ce soit une forme bilinéaire symétrique est clair. Dire qu'elle est non dégénérée signifie que si $x \in L$ est tel que $\text{Tr}_{L/K}(xy) = 0$ pour tout $y \in L$, alors $x = 0$. Cela résulte du lemme 4.4 suivant. \square

Lemme 4.4 (Lemme de Dedekind sur l'indépendance linéaire des caractères). Soient G un groupe, k un corps, $\sigma_1, \dots, \sigma_n$ des homomorphismes deux-à-deux distincts de G dans le groupe multiplicatif k^\times . Alors $\sigma_1, \dots, \sigma_n$ sont linéairement indépendants sur k dans l'espace vectoriel k^G .

Démonstration. On démontre le résultat par récurrence sur n . Pour $n = 1$ il est trivial. Supposons $n \geq 2$. Soient a_1, \dots, a_n des éléments de k tels que

$$\sum_{i=1}^n a_i \sigma_i(x) = 0 \quad \text{pour tout } x \in G.$$

Alors pour tout $x \in G$ et tout $y \in G$ on a

$$\sum_{i=1}^n a_i \sigma_i(x) \sigma_i(y) = 0.$$

Comme $\sigma_n \neq \sigma_1$ il existe $y \in G$ tel que $\sigma_n(y) \neq \sigma_1(y)$. En utilisant la relation

$$\sum_{i=2}^n a_i (\sigma_i(y) - \sigma_1(y)) \sigma_i(x) = 0$$

avec l'hypothèse de récurrence, on en déduit $a_n = 0$, puis $a_1 = \dots = a_n = 0$. \square

Remarque. Sous l'hypothèse supplémentaire que la caractéristique de K est soit nulle, soit première avec $[L : K]$, le fait que la forme bilinéaire $(x, y) \mapsto \text{Tr}_{L/K}(xy)$ soit non dégénérée se déduit aussi de la relation

$$\text{Tr}_{L/K}(\alpha^n) + a_1 \text{Tr}_{L/K}(\alpha^{n-1}) + \dots + a_{n-1} \text{Tr}_{L/K}(\alpha) + a_n [L : K] = 0$$

quand le polynôme irréductible de α sur K est $X^n + a_1 X^{n-1} + \dots + a_{n-1} X + a_n \in K[X]$: comme $a_n \neq 0$, l'un des nombres $\text{Tr}_{L/K}(\alpha^i)$, ($1 \leq i \leq n$) n'est pas nul.

Définition. Soient $A \subset B$ deux anneaux. On suppose que B est un A -module libre de rang n . On définit une application $D_{B/A} : B^n \rightarrow A$ appelée *discriminant de B sur A* par

$$D_{B/A}(x_1, \dots, x_n) = \det(\text{Tr}_{B/A}(x_i x_j))_{1 \leq i, j \leq n}.$$

Lemme 4.5. Soient $A = (a_{ij})_{1 \leq i, j \leq n}$ une matrice $n \times n$ à coefficients dans A . On pose

$$y_j = \sum_{i=1}^n a_{ij} x_i, \quad (1 \leq j \leq n).$$

Alors

$$D_{B/A}(y_1, \dots, y_n) = (\det A)^2 D_{B/A}(x_1, \dots, x_n)$$

Démonstration. Cela résulte du fait que l'application $(x, y) \mapsto \text{Tr}_{B/A}(xy)$ est bilinéaire. \square

Donc si x_1, \dots, x_n sont linéairement dépendants sur A , alors $D_{B/A}(x_1, \dots, x_n) = 0$ (on a supposé A intègre).

Si $\{x_1, \dots, x_n\}$ et $\{y_1, \dots, y_n\}$ sont deux bases de B comme A -module, alors la matrice de passage A est inversible, donc $\det A$ est une unité de A . En particulier l'idéal principal de A engendré par le discriminant $D_{B/A}(x_1, \dots, x_n)$ d'une base ne dépend pas de la base $\{x_1, \dots, x_n\}$: on le note $\mathcal{D}_{B/A}$ et on l'appelle *idéal discriminant de B sur A* .

Si $A = \mathbf{Z}$ le déterminant $\det A$ d'une matrice de passage entre deux bases de B sur \mathbf{Z} est ± 1 , donc son carré est $+1$ et le discriminant $D_{B/\mathbf{Z}}(x_1, \dots, x_n)$ d'une base de B sur \mathbf{Z} ne dépend pas de la base $\{x_1, \dots, x_n\}$. C'est le *discriminant absolu* de B , que l'on note \mathcal{D}_B .

Lemme 4.6. Soient $A \subset B$ deux anneaux; on suppose que B est un A -module libre de rang n et que l'idéal $\mathcal{D}_{B/A}$ n'est pas l'idéal $\{0\}$. Soit $(x_1, \dots, x_n) \in B^n$. Alors $D_{B/A}(x_1, \dots, x_n)$ engendre l'idéal $\mathcal{D}_{B/A}$ si et seulement si $\{x_1, \dots, x_n\}$ est une base de B comme A -module.

Démonstration. Par définition de l'idéal discriminant $\mathcal{D}_{B/A}$, si $\{x_1, \dots, x_n\}$ est une base de B comme A -module, alors $D_{B/A}(x_1, \dots, x_n)$ est un générateur de l'idéal $\mathcal{D}_{B/A}$.

Inversement supposons que $D_{B/A}(x_1, \dots, x_n)$ engendre l'idéal $\mathcal{D}_{B/A}$. Soit $\{e_1, \dots, e_n\}$ une base de B sur A . On écrit $x_i = \sum_{j=1}^n a_{ij} e_j$ ($1 \leq i \leq n$) et on note $d_x = D_{B/A}(x_1, \dots, x_n)$, $d_e = D_{B/A}(e_1, \dots, e_n)$ et $a = \det(a_{ij})$. D'après le lemme 4.5 on a $d_x = a^2 d_e$. Par hypothèse d_x et d_e engendrent le même idéal $\mathcal{D}_{B/A}$. Donc $d_x = u d_e$ avec $u \in A^\times$. Alors $(a^2 - u) d_e = 0$. Comme l'idéal principal $\mathcal{D}_{B/A}$ contient un élément non nul et que A est intègre, il en résulte que a^2 est inversible, donc que a est aussi une unité de A , donc la matrice (a_{ij}) est inversible, son inverse étant une matrice à coefficients dans A et par conséquent $\{x_1, \dots, x_n\}$ est une base de B sur A . \square

Proposition 4.7. Soit L/K une extension séparable de degré n , soit N une extension finie de L , normale sur K , x_1, \dots, x_n des éléments de L et soient $\sigma_1, \dots, \sigma_n$ les différents K -isomorphismes de L dans N . Alors

$$D_{L/K}(x_1, \dots, x_n) = \left(\det(\sigma_h(x_j))_{1 \leq h, j \leq n} \right)^2.$$

De plus (x_1, \dots, x_n) est une base de L sur K si et seulement si

$$D_{L/K}(x_1, \dots, x_n) \neq 0.$$

Démonstration. On utilise le lemme 4.2 :

$$\text{Tr}_{L/K}(x_i x_j) = \sum_{h=1}^n \sigma_h(x_i) \sigma_h(x_j).$$

Donc

$$D_{L/K}(x_1, \dots, x_n) = \det(\text{Tr}_{L/K}(x_i x_j)) = \det(\sigma_h(x_i)) \det(\sigma_h(x_j)) = (\det(\sigma_h(x_j)))^2.$$

Pour compléter la démonstration il reste à voir que la matrice $(\sigma_h(x_j))$ est régulière. Si b_1, \dots, b_n sont des éléments de N tels que $b_1 \sigma_1(x_j) + \dots + b_n \sigma_n(x_j) = 0$ pour $1 \leq j \leq n$, alors $b_1 \sigma_1(x) + \dots + b_n \sigma_n(x) = 0$ pour tout $x \in B$ et d'après le lemme 4.4 il en résulte $b_1 = \dots = b_n = 0$. \square

Soit P un polynôme non nul à coefficients dans un corps K et soit E une extension de K dans laquelle P est complètement décomposé :

$$P(X) = a_0 \prod_{i=1}^n (X - x_i),$$

où n est le degré de P , a_0 son coefficient directeur et $x_i \in E$. Nous avons déjà défini le *discriminant* de P par

$$D(P) = a_0^{n(n-1)} \prod_{1 \leq i < j \leq n} (x_i - x_j)^2 = (-1)^{n(n-1)/2} a_0^{n(n-1)} \prod_{\substack{1 \leq i, j \leq n, \\ i \neq j}} (x_i - x_j).$$

De la définition on déduit $D(P) = 0$ si et seulement si P a au moins une racine multiple. La théorie de Galois §2.8 montre que $D(P)$ est un élément de K . De la proposition 4.7, on déduit que si $P \in K[X]$ est un polynôme unitaire irréductible de degré n et si $L = K(\alpha)$ est un corps de rupture de P sur K , avec $P(\alpha) = 0$, alors

$$D(P) = D_{L/K}(1, \alpha, \dots, \alpha^{n-1}).$$

Exercice. Vérifier que le discriminant du polynôme $aX^2 + bX + c$ est $b^2 - 4ac$ et que celui de $X^3 + pX + q$ est $-4p^3 - 27q^2$.

4.2 Entiers algébriques

Proposition 4.8. Soient A un anneau intègre, K un corps contenant A et $\alpha \in K$. Les propriétés suivantes sont équivalentes :

- (i) α est racine d'un polynôme unitaire à coefficients dans A .
- (ii) Le sous-anneau $A[\alpha]$ de K engendré par α sur A est un A -module de type fini.
- (iii) $A[\alpha]$ est contenu dans un sous-anneau de K qui est de type fini comme A -module.

Exemple : Le sous-anneau de \mathbf{C} engendré par $1/2$:

$$\mathbf{Z}[1/2] = \{a/2^n ; a \in \mathbf{Z}, n \in \mathbf{Z}_{\geq 0}\}$$

n'est pas un \mathbf{Z} -module de type fini, alors que $\mathbf{Z}[i] = \mathbf{Z} + \mathbf{Z}i$ et $\mathbf{Z}[\sqrt{2}] = \mathbf{Z} + \mathbf{Z}\sqrt{2}$ sont des \mathbf{Z} -modules de type fini.

Démonstration. Supposons la propriété (i) vérifiée ; soit

$$X^n + a_1 X^{n-1} + \dots + a_{n-1} X + a_n \in A[X]$$

un polynôme unitaire à coefficients dans A ayant α comme racine. De la relation

$$\alpha^n = -a_1\alpha^{n-1} - \dots - a_{n-1}\alpha - a_n$$

on déduit par récurrence sur m

$$\alpha^m \in A + A\alpha + \dots + A\alpha^{n-1} \quad \text{pour tout } m \geq 1,$$

donc $A[\alpha] = A + A\alpha + \dots + A\alpha^{n-1}$ et par conséquent l'anneau $A[\alpha]$ est un A -module de type fini.

L'implication (ii) \Rightarrow (iii) est triviale.

Supposons la propriété (iii) vérifiée. Soit B un sous-anneau de K contenant $A[\alpha]$. On suppose que B est un A -module de type fini et on écrit $B = Ax_1 + \dots + Ax_m$. Pour $1 \leq i \leq m$ le fait que αx_i appartienne à B entraîne qu'il existe des éléments a_{ij} de A ($1 \leq j \leq m$) tels que

$$\alpha x_i = \sum_{j=1}^m a_{ij} x_j.$$

Posons $M = (a_{ij})_{1 \leq i, j \leq m}$ et soit I la matrice identité $m \times m$. La matrice $\alpha I - M$ est associée à un endomorphisme de \overline{K}^m dont le noyau contient (x_1, \dots, x_m) . Soit $P \in A[X]$ le déterminant de la matrice $XI - M$. Alors P est un polynôme unitaire qui admet α comme racine. D'où (i). \square

Définition. On dit que $\alpha \in K$ est *entier sur A* s'il vérifie les propriétés équivalentes de la proposition 4.8.

Par exemple si A est un corps, un élément de K est entier sur A si et seulement s'il est algébrique sur A .

Corollaire 4.9. *L'ensemble des éléments de K entiers sur A est un sous-anneau de K .*

Démonstration. Si α et β sont des éléments de K entiers sur A , alors l'anneau $A[\alpha, \beta]$ est un sous- A -module de type fini de K (un système générateur fini est formé d'éléments $\alpha^i \beta^j$), donc tous ses éléments sont entiers sur A . \square

Définition. L'ensemble des éléments de K qui sont entiers sur A est appelé la *fermeture intégrale de A dans K* .

De la proposition 4.8 on déduit que la relation d'intégralité est transitive :

Corollaire 4.10. *Soient K un corps, A un sous-anneau de K , A_0 la fermeture intégrale de A dans K et B un sous-anneau de A_0 contenant A . Alors la fermeture intégrale de B dans K est A_0 .*

Démonstration. Soit B_0 la fermeture intégrale de B dans K . Un élément de A_0 est entier sur A , donc sur B , et par conséquent appartient à B_0 . Pour voir l'inclusion dans l'autre sens, on considère un élément x de B_0 , il est entier sur B , donc racine d'un polynôme unitaire à coefficients dans B . Soient b_1, \dots, b_m les coefficients de ce polynôme; le sous-anneau $A[b_1, \dots, b_m]$ de B est un A -module de type fini, il en est de même de $A[b_1, \dots, b_m, x]$, donc par la proposition 4.8 on en déduit que x est entier sur A , ce qui montre $B_0 \subset A_0$. \square

Définition. La *clôture intégrale* d'un anneau est la fermeture intégrale de cet anneau dans son corps des fractions.

La clôture intégrale de A est un anneau qui contient A et qui est contenu dans la fermeture intégrale de A dans K , pour tout corps K contenant A .

Définition. Un anneau est dit *intégralement clos* s'il est égal à sa clôture intégrale.

Un anneau factoriel est intégralement clos : en effet, si A est un anneau factoriel de corps des fractions K et si $\alpha \in K$ est racine d'un polynôme unitaire à coefficients dans A :

$$\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0,$$

on écrit $\alpha = p/q$ avec p et q dans A sans facteurs irréductibles communs et de la relation

$$p^n + a_1p^{n-1}q + \cdots + a_nq^n = 0$$

on déduit que q divise p , donc que q est inversible et $\alpha \in A$.

En particulier un anneau principal est intégralement clos. On en déduit par exemple qu'un nombre rationnel qui est entier sur \mathbf{Z} est dans \mathbf{Z} .

L'anneau $\mathbf{Z}[2i] = \mathbf{Z} + 2i\mathbf{Z}$ n'est pas intégralement clos, puisque son corps des fractions $\mathbf{Q}(i)$ contient i , qui est racine du polynôme $X^2 + 1$, donc est entier sur $\mathbf{Z}[2i]$, mais n'appartient pas à $\mathbf{Z}[2i]$.

Définition. On appelle *nombre algébrique* tout nombre complexe qui est algébrique sur \mathbf{Q} et *entier algébrique* tout nombre complexe qui est entier sur \mathbf{Z} .

Si α est un nombre algébrique, dont le polynôme irréductible sur \mathbf{Q} est

$$X^n + a_1X^{n-1} + \cdots + a_n \in \mathbf{Q}[X],$$

l'unique polynôme irréductible de $\mathbf{Z}[X]$ qui s'annule au point α et dont le coefficient directeur soit positif est

$$dX^n + da_1X^{n-1} + \cdots + da_n \in \mathbf{Z}[X], \quad (4.11)$$

où d est le plus petit commun multiple des dénominateurs des nombres a_1, \dots, a_n . Nous appellerons ce polynôme (4.11) le *polynôme minimal de α sur \mathbf{Z}* .

Si α est un entier algébrique, alors les valeurs propres de $[\alpha]$ sont des entiers algébriques, donc le polynôme caractéristique de α sur \mathbf{Z} est à coefficients dans \mathbf{Z} ; en particulier $N_{K/\mathbf{Q}}(\alpha)$ et $\text{Tr}_{K/\mathbf{Q}}(\alpha)$ sont dans \mathbf{Z} .

Le lemme de Gauss 2.24 montre que pour un nombre algébrique α les conditions suivantes sont équivalentes :

- (i) α est entier (sur \mathbf{Z})
- (ii) Le polynôme minimal de α sur \mathbf{Z} est unitaire.
- (iii) Le polynôme irréductible de α sur \mathbf{Q} a ses coefficients dans \mathbf{Z} .
- (iv) Le polynôme minimal de α sur \mathbf{Z} coïncide avec son polynôme irréductible sur \mathbf{Q} .

Quand on parle du polynôme irréductible ou du polynôme minimal d'un nombre algébrique, on omet souvent de préciser "sur \mathbf{Q} " et "sur \mathbf{Z} " respectivement.

Le corollaire 4.9 montre que les entiers algébriques forment un sous-anneau de \mathbf{C} , dont le corps des fractions est le corps $\overline{\mathbf{Q}}$ des nombres algébriques. Si α est un nombre algébrique, l'ensemble des

entiers $d \in \mathbf{Z}$ tels que $d\alpha$ soit entier algébrique est un idéal non nul de \mathbf{Z} : il contient le coefficient directeur du polynôme minimal de α sur \mathbf{Z} .

On appelle *corps de nombres* une extension finie de \mathbf{Q} . D'après le théorème de l'élément primitif 2.21, un corps de nombres est un sous-corps de \mathbf{C} de la forme $\mathbf{Q}(\alpha)$ avec α nombre algébrique. Le degré d'un corps de nombres est son degré sur \mathbf{Q} . Un *corps quadratique* est une extension de \mathbf{Q} de degré 2, un *corps cubique* une extension de \mathbf{Q} de degré 3, un corps *biquadratique* une extension de degré 4. . .

L'*anneau des entiers* d'un corps de nombres K est l'intersection de K avec l'anneau des entiers algébriques. On le notera \mathbf{Z}_K . Le corps des fractions de \mathbf{Z}_K est K et \mathbf{Z}_K est un anneau intégralement clos (cf. Corollaire 4.10).

Les éléments inversibles (*unités*) de l'anneau \mathbf{Z}_K forment un groupe multiplicatif \mathbf{Z}_K^\times ; ce sont les éléments de \mathbf{Z}_K de norme ± 1 .

Quand K est un corps de nombres, on utilise des expressions comme "unités de K ", "idéaux de K ", "discriminant de K " pour parler des unités, des idéaux ou du discriminant de l'anneau des entiers de K .

Définition. Soit α un nombre algébrique. On appelle *norme absolue* de α (resp. *trace absolue* de α) la norme (resp. la trace) $N_{\mathbf{Q}(\alpha)/\mathbf{Q}}(\alpha)$ (resp. $\text{Tr}_{\mathbf{Q}(\alpha)/\mathbf{Q}}(\alpha)$). On les note respectivement $N(\alpha)$ et $\text{Tr}(\alpha)$.

Du lemme 4.2 on déduit que si α est un nombre algébrique dont le polynôme irréductible sur \mathbf{Q} est

$$P(X) = X^d + a_1X^{d-1} + \dots + a_d \in \mathbf{Q}[X],$$

alors

$$N(\alpha) = (-1)^d a_d \quad \text{et} \quad \text{Tr}(\alpha) = -a_1.$$

Plus généralement, si K est un corps de nombres de degré n sur \mathbf{Q} , α un élément de K , d le degré de α sur \mathbf{Q} et $\alpha_1, \dots, \alpha_d$ les conjugués de α dans \mathbf{C} , alors

$$N_{K/\mathbf{Q}}(\alpha) = (\alpha_1 \cdots \alpha_d)^{n/d} \quad \text{et} \quad \text{Tr}_{K/\mathbf{Q}}(\alpha) = \frac{n}{d}(\alpha_1 + \cdots + \alpha_d).$$

Soit k un corps quadratique. Il existe un entier $d \in \mathbf{Z}$ sans facteur carré tel que $k = \mathbf{Q}(\sqrt{d})$. Soit α un élément de k , alors α est racine du polynôme $X^2 - X\text{Tr}_{k/\mathbf{Q}}(\alpha) + N_{k/\mathbf{Q}}(\alpha)$, donc α est entier si et seulement si $\text{Tr}_{k/\mathbf{Q}}(\alpha)$ et $N_{k/\mathbf{Q}}(\alpha)$ sont dans \mathbf{Z} .

Soit $\alpha = x + y\sqrt{d} \in k$, avec x et y dans \mathbf{Q} . On a $\text{Tr}_{k/\mathbf{Q}}(\alpha) = 2x$ et $N_{k/\mathbf{Q}}(\alpha) = x^2 - dy^2$. Si α est entier, alors les nombres $a = 2x$ et $b = x^2 - dy^2$ sont dans \mathbf{Z} . Comme d n'est pas divisible par 4, le nombre $c = 2y$ est aussi dans \mathbf{Z} . Alors de la relation $a^2 - dc^2 = 4b$ on déduit que soit a et c sont pairs, soit a et c sont impairs et dans ce dernier cas $d \equiv 1 \pmod{4}$. Par conséquent l'anneau \mathbf{Z}_k des entiers de k est

$$\mathbf{Z}_k = \begin{cases} \mathbf{Z} + \mathbf{Z}\sqrt{d} & \text{si } d \equiv 2 \text{ ou } 3 \pmod{4} \\ \mathbf{Z} + \mathbf{Z}\frac{1+\sqrt{d}}{2} & \text{si } d \equiv 1 \pmod{4}. \end{cases}$$

Ainsi $\mathbf{Z}_k = \mathbf{Z} + \mathbf{Z}\alpha$ où α est une des deux racines du polynôme $X^2 - d$ si $d \equiv 2$ ou $3 \pmod{4}$, et l'une des deux racines du polynôme $X^2 - X - (d-1)/2$ si $d \equiv 1 \pmod{4}$.

Le discriminant D_k de k est le discriminant $D_{\mathbf{Z}_k}$ de l'anneau des entiers de k :

$$D_k = \begin{cases} \det \begin{vmatrix} 2 & 0 \\ 0 & 2d \end{vmatrix} = 4d & \text{si } d \equiv 2 \text{ ou } 3 \pmod{4} \\ \det \begin{vmatrix} 2 & 1 \\ 1 & (1+d)/2 \end{vmatrix} = d & \text{si } d \equiv 1 \pmod{4}. \end{cases}$$

Ainsi le discriminant est toujours congru à 0 ou 1 modulo 4 et le corps quadratique s'écrit aussi $k = \mathbf{Q}(\sqrt{D_k})$.

Le groupe des racines de l'unités d'un corps de nombres quadratique k est $\{1, i, -1, -i\}$ si k a pour discriminant -4 — c'est-à-dire $k = \mathbf{Q}(i)$ —, c'est $\{1, \varrho, \varrho^2, -1, -\varrho, -\varrho^2\}$ si k a pour discriminant -3 , où ϱ est une racine primitive cubique de l'unité (c'est-à-dire pour $k = \mathbf{Q}(\sqrt{-3})$) enfin les seules racines de l'unité dans \mathbf{Z}_k sont $\{\pm 1\}$ sinon.

Quand d est négatif, il est facile de vérifier que le groupe des unités du corps $k = \mathbf{Q}(\sqrt{d})$ est fini : il est composé des racines de l'unité. Nous verrons au § 4.4 que pour $d > 0$ le groupe \mathbf{Z}_k^\times des unités de \mathbf{Z}_k est un \mathbf{Z} -module de rang 1.

Proposition 4.12. *Soit K un corps de nombres de degré n . Alors l'anneau des entiers \mathbf{Z}_K de K est un \mathbf{Z} -module libre de rang n .*

Démonstration. La conclusion signifie qu'il existe n éléments e_1, \dots, e_n de \mathbf{Z}_K , linéairement indépendants sur \mathbf{Q} , tels que

$$\mathbf{Z}_K = \mathbf{Z}e_1 + \dots + \mathbf{Z}e_n.$$

Soit f_1, \dots, f_n une base de K sur \mathbf{Q} formée d'éléments de \mathbf{Z}_K (partant d'une base quelconque il suffit de multiplier par un dénominateur pour obtenir une telle base).

La forme bilinéaire $(x, y) \mapsto \text{Tr}_{K/\mathbf{Q}}(xy)$ étant non dégénérée (lemme 4.2), il existe une base f_1^*, \dots, f_n^* de K sur \mathbf{Q} telle que $\text{Tr}_{K/\mathbf{Q}}(f_i f_j^*) = \delta_{ij}$ (symbole de Kronecker). Soit $a \in \mathbf{Z}$, $a > 0$ tel que $a f_j^*$ soit entier algébrique pour $1 \leq j \leq n$.

Pour $x \in K$ on écrit

$$x = x_1 f_1 + \dots + x_n f_n$$

avec x_1, \dots, x_n dans \mathbf{Q} et on a $\text{Tr}_{K/\mathbf{Q}}(x f_j^*) = x_j$. Maintenant si $x \in \mathbf{Z}_K$ on a $a x f_j^* \in \mathbf{Z}_K$, donc $\text{Tr}_{K/\mathbf{Q}}(a x f_j^*) = a x_j \in \mathbf{Z}$. On en déduit

$$\mathbf{Z}f_1 + \dots + \mathbf{Z}f_n \subset \mathbf{Z}_K \subset \frac{1}{a}(\mathbf{Z}f_1 + \dots + \mathbf{Z}f_n).$$

Pour conclure on utilise alors les résultats du § 4.3 suivant sur la structure des modules sur un anneau principal (proposition 4.15). □

Il résulte de la Proposition 4.12 que tout idéal de \mathbf{Z}_K est un \mathbf{Z} -module libre de rang n . Une base de \mathbf{Z}_K comme \mathbf{Z} -module est une base d'entiers de K , son discriminant ne dépend pas de la base, c'est le *discriminant du corps de nombres K* .

Soient k un corps de nombres et n son degré. D'après le théorème de l'élément primitif 2.21, il existe $\alpha \in k$ tel que $k = \mathbf{Q}(\alpha)$. On décompose le polynôme irréductible $P \in \mathbf{Q}[X]$ de α dans $\mathbf{R}[X]$:

soient r_1 le nombre de facteurs irréductibles de degré 1 et r_2 le nombre de facteurs irréductibles de degré 2. Ainsi $r_1 + 2r_2 = n$. Notons $\alpha_1, \dots, \alpha_{r_1}$ les racines réelles de P :

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

Pour $r_1 + 1 \leq j \leq r_1 + r_2$ le polynôme $X^2 + b_j X + c_j$ a deux racines complexes conjuguées, que l'on note α_j et $\alpha_{r_2+j} = \bar{\alpha}_j$. Ainsi la décomposition de P en facteurs irréductibles dans \mathbf{C} est

$$P(X) = \prod_{i=1}^n (X - \alpha_i).$$

Il y a n \mathbf{Q} -isomorphismes $\sigma_1, \dots, \sigma_n$ de k dans \mathbf{C} , qui sont déterminés respectivement par

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

Pour $1 \leq j \leq r_1$ l'image $\sigma_j(k)$ de k par σ_j est dans \mathbf{R} , tandis que σ_{r_1+j} et $\sigma_{r_1+r_2+j}$ sont complexes conjugués pour $1 \leq j \leq r_2$. L'ensemble $\{\sigma_1, \dots, \sigma_{r_1}\}$ des plongements réels et celui $\{\sigma_{r_1+1}, \dots, \sigma_{r_1+2r_2}\}$ des plongements non réels ne dépendent pas du choix de l'élément primitif α . Le *plongement canonique* de k est l'application \mathbf{Q} -linéaire injective $\underline{\sigma} : k \rightarrow \mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$ définie par

$$\underline{\sigma}(x) = (\sigma_1(x), \dots, \sigma_{r_1+r_2}(x)).$$

Le seul choix qui ne soit pas intrinsèque est celui entre un plongement non réel et son conjugué. On identifie \mathbf{C} à \mathbf{R}^2 par $z = \Re(z) + i\Im(z)$ et on note encore $\underline{\sigma}$ l'application \mathbf{Q} -linéaire de k dans \mathbf{R}^n qui envoie $x \in k$ sur

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

Le couple (r_1, r_2) est la *signature* du corps de nombres k . Le degré de k est alors $r_1 + 2r_2$.

Lemme 4.13. *Le signe du discriminant absolu d'un corps de nombres k de signature (r_1, r_2) est $(-1)^{r_2}$.*

Démonstration. Dans le développement du déterminant de la matrice des $\sigma_i(\alpha_j)$ (cf. proposition 4.7), les nombres réels ont des carrés positifs, les nombres imaginaires purs ont des carrés négatifs et il y en a r_2 . Voir [C], Prop. 4.8.11. \square

Exercice. Soit T un polynôme unitaire irréductible de degré n de $\mathbf{Z}[X]$ et $K = \mathbf{Q}(\theta)$. On désigne par $D(T)$ le discriminant de T et par D_K celui du corps de nombres K .

- Montrer que le discriminant de $1, \theta, \dots, \theta^{n-1}$ est $D(T)$.
- Soit f l'indice de $\mathbf{Z}[\theta]$ dans \mathbf{Z}_K . Vérifier $D(T) = D_K f^2$.

Référence : [C], § 4.4.

Une famille $(\alpha_1, \dots, \alpha_n)$ de n éléments dans un corps de nombres de degré n est une base d'entiers de K si et seulement si les deux conditions suivantes sont satisfaites :

- Les α_i sont entiers
- Le discriminant $D(\alpha_1, \dots, \alpha_n)$ est égal au discriminant de K .

Exercice. Montrer que le discriminant d'un corps de nombres est congru à 0 ou 1 modulo 4
Indication : en utilisant la proposition 4.7 développer le déterminant de la matrice des $\sigma_i(\alpha_j)$ et regrouper les termes de signature paire et ceux de signature impaire pour écrire le discriminant sous la forme $(P - N)^2 = (P + N)^2 - 4PN$ et vérifier que $P + N$ et PN sont des entiers.
 En déduire que si T est un polynôme unitaire irréductible dans $\mathbf{Z}[X]$ de discriminant D qui est soit sans facteur carré et congru à 1 modulo 4, soit de la forme $4d$ avec d sans facteur carré et congru à 1 modulo 4, si θ est une racine de T dans une extension de \mathbf{Q} , alors $(1, \theta, \dots, \theta^{n-1})$ est une base d'entiers de $\mathbf{Q}(\theta)$.

4.3 Structure des modules sur les anneaux principaux

Dans la démonstration de la Proposition 4.12, nous avons utilisé un théorème sur la structure des sous-modules d'un module libre de type fini sur un anneau principal. En voici l'énoncé.

Quand A est un anneau (intègre, rappelons-le) et M un A -module, on définit le *rang de M* comme le nombre maximal ($\leq \infty$) d'éléments de M linéairement indépendants sur A . Si K est le corps des fractions de A , et si M est un A -module libre, il possède une base, et on peut plonger M dans un K -espace vectoriel V . Le rang de M est donc le nombre d'éléments d'une base de M comme A -module, et plus généralement le rang d'un sous-module N de M est la dimension du K -espace vectoriel engendré par N dans V .

Proposition 4.14. (Modules sur les anneaux principaux.) *Soit A un anneau principal, soit M un A -module libre de rang m et soit N un sous- A -module de M . Alors N est libre de rang $n \leq m$. De plus il existe une base $\{e_1, \dots, e_m\}$ de M comme A -module et des éléments a_1, \dots, a_n de A tels que $\{a_1 e_1, \dots, a_n e_n\}$ soit une base de N sur A et que a_i divise a_{i+1} dans A pour $1 \leq i < n$.*

Les idéaux $a_1 A \supset a_2 A \supset \dots \supset a_n A$ de A sont appelés *facteurs invariants* du sous- A -module N de M : ils ne dépendent pas de la base (a_1, \dots, e_n) de M vérifiant les conditions de la proposition 4.15.

Démonstration. Voir [S] § 1.5. □

Références :

[C] H. Cohen. *A course in computational algebraic number theory*, Graduate texts in Math. **138**, Springer Verlag (1993),

[S] P. Samuel, *Théorie algébrique des nombres*, Hermann, Collection Méthodes, 1967.