Introduction à la théorie algébrique des nombres

Vincent Pilaud

Mars 2004

Lors de la présentation orale de cet exposé, on commencera à la partie 2, la première partie ne servant que de rappels utiles à son auteur. Les démonstrations ne seront en général que vaguement abordées. On donnera des exemples principalement sur les extensions quadratiques et cyclotomiques, puisque ce sont celles qui nous intéresseront par la suite, mais ces exemples ne sont en général pas démontrés.. Le dernier paragraphe n'est qu'une vague introduction à l'exposé suivant sur le nombre de classes.

1 Extensions de corps

Définition 1. *Soient K et L des corps tels que $K \subset L$. On dit alors que L* ***est une extension (de corps) de*** *K, et on note L/K cette extension.*

Remarque 1. *Si L est une extension de K, alors L peut être vu comme un K-espace vectoriel avec la loi externe : $\forall a \in K, \forall b \in L, a.b = ab$ (multiplication dans le corps L).*

Si L est de dimension finie sur K, on dit que l'extension L/K ***est finie*** *et la dimension de L sur K est appelée* ***degré de l'extension*** *et est notée $[L : K]$.*

Théorème 1 (de la base télescopique et de la multiplication du degré). *Soient K, L et M des corps tels que $K \subset L \subset M$. Soient $(e_i)_{i\in I}$ et $(f_j)_{j\in J}$ des bases respectives du K-espace vectoriel L et du L-espace vectoriel M.*

Alors $(e_i f_j)_{i\in I, j\in J}$ est une base du K-espace vectoriel M.

En particulier, si L/K et M/L sont finies de degrés respectifs $[L : K]$ et $[M : L]$, alors M/K est finie de degré $[M : K] = [M : L][L : K]$.

Définition 2. *Soit L/K une extension de corps et A une partie de L.*

On appelle ***extension engendrée par*** *A, et on note $K(A)$ le plus petit sous-corps de L contenant K et A. Si $A = \{a_1, \ldots, a_n\}$ est fini, on note aussi $K(A) = K(a_1, \ldots, a_n)$.*

Si $L = K(A)$, on dit que A ***engendre*** *L* ***sur*** *K. Enfin, on dit que l'extension L/K est* ***monogène*** *si il existe $a \in L$ tel que $L = K(a)$.*

Remarque 2. *Si L/K est une extension de corps et A une partie de L, on note $K[A]$ le plus petit sous-anneau de L contenant K et A. On a bien sûr $K[A] \subset K(A)$.*

Pour $a \in L$, on peut décrire $K[a]$ et $K(a)$ de la façon suivante :

- *$x \in K[a] \Leftrightarrow \exists P \in K[X], P(a) = x$*
- *$x \in K(a) \Leftrightarrow \exists P, Q \in K[X], \frac{P(a)}{Q(a)} = x$*

On peut généraliser cette description à $A = \{a_1, \ldots, a_n\}$.

Il est important de noter que $K[a]$ (resp. $K(A)$) n'est en général pas isomorphe à l'anneau des polynômes $K[X]$ (resp. au corps des fractions $K(X)$) puisqu'il peut arriver que $P(a) = 0$ avec $P \neq 0$.

Plus précisément, il y a deux situations possibles :

Définition 3. *Soit L/K une extension de corps et $a \in L$.*

Soit $\phi : K[X] \longrightarrow L$ l'homomorphisme défini par $\phi(P) = P(a)$,

1. *Si ϕ est injective, on dit que a est* ***transcendant****.*
2. *sinon, on dit que a est* ***algébrique****. Dans ce cas, l'idéal $I = Ker\phi$ est principal non nul, donc il est engendré par un unique polynôme Π unitaire, appelé* ***polynôme minimal de*** *a* ***sur*** *K.*

Proposition 1.

1. *Si a est transcendant, $K[a] \simeq K[X]$ et $K(a) \simeq K(X)$.*
2. *Si a est algébrique, $K[a] \simeq K(a) \simeq K[X]/(\Pi)$.*

Exemples 1. – $i, \sqrt[3]{2}, \ldots$ *sont algébriques sur* $\mathbb{Q}$,
– e *et* π *sont transcendants sur* $\mathbb{Q}$,
– $\sum \frac{1}{10^{n!}}$ *est transcendant.*

Preuve 1. *Soit* α *un nombre algébrique. Alors il existe* $n \in \mathbb{N}^*$ *et* $K \in \mathbb{R}^*$ *tels que* $\forall (p,q) \in \mathbb{Z} \times \mathbb{Z}^*, |\alpha - \frac{p}{q}| \geq \frac{K}{q^n}$.

En effet, soit P *tel que* $P(\alpha) = 0$. *Soient* $n = d(P)$ *et* $\frac{1}{K} = \sup_{[\alpha-1;\alpha+1]} |P'|$. *Alors* $\forall \frac{p}{q} \in [\alpha - 1; \alpha + 1], |P(\frac{p}{q})| \leq \frac{1}{K}.|\frac{p}{q} - \alpha|$. *Mais* $P(\frac{p}{q}) = \frac{N}{q^n} \geq \frac{1}{q^n}$, *et donc* $|\alpha - \frac{p}{q}| \geq \frac{K}{q^n}$.

On en déduit immédiatement que $\sum \frac{1}{10^{n!}}$ *est transcendant.*

Définition 4. *Une extension* L/K *est* ***algébrique*** *si pour tout* $a \in L$, a *est algébrique sur* K.

Remarque 3. *Une extension finie est algébrique.*

Définition 5. *Un corps* K *est dit* ***algébriquement clos*** *si il vérifie l'une des conditions équivalentes suivantes :*
– *tout polynôme* $P \in K[X]$ *de degré non nul admet une racine dans* K,
– *tout polynôme* $P \in K[X]$ *est produit de polynômes de degré* 1,
– *les éléments irréductibles de* $K[X]$ *sont les* $X - a, a \in K$,
– *si une extension* L/K *est algébrique, alors* $L = K$.

Si K *est un corps, une* ***cloture algébrique de*** K *est un corps algébriquement clos* $\tilde{K}$ *tel que* $\tilde{K}/K$ *soit algébrique.*

Théorème 2. *Soit* L/K *une extension de corps.*
Soit $E = \{x \in L | x$ *algébrique sur* $K\}$. *Alors :*

1. E *est un sous-corps de* L,
2. *tout élément de* L *algébrique sur* E *est dans* E,
3. *si* L *est alébriquement clos,* E *est algébriquement clos. C'est la cloture algébrique de* K.

2 Corps de nombres algébriques

2.1 Définition et représentation

Soit $\mathbb{K}$ un sous-corps de $\mathbb{C}$. Alors puisque $1 \in \mathbb{K}$, par addition passage à l'opposé et à l'inverse, $\mathbb{Q} \subset \mathbb{K}$.

Définition 6. *Un sous-corps de* $\mathbb{C}$, $\mathbb{K}$, *est appelé* ***corps de nombres*** *si l'extension* $\mathbb{K}/\mathbb{Q}$ *est finie. Le degré de l'extension est aussi appelé* ***degré de*** $\mathbb{K}$.

Théorème 3 (de l'élément primitif). 1. *Si* $a \in \mathbb{C}$ *est un nombre algébrique, alors* $\mathbb{Q}(a)$ *est un corps de nombre.*
2. *Réciproquement, pour tout corps de nombres* $\mathbb{K}$, *il existe* $\theta \in K$ *tel que* $\mathbb{K} = \mathbb{Q}(\theta)$. θ *est appelé* ***élément primitif*** *de* $\mathbb{K}$.

Démonstration Soit $a_1 \in \mathbb{K}^\star$. Alors $\mathbb{Q}(a_1) \subset \mathbb{K}$. Si $\mathbb{Q}(a_1) = \mathbb{K}$, alors c'est terminé. Sinon, il existe $a_2 \notin \mathbb{Q}(a_1)$. Alors $\mathbb{Q}(a_1, a_2) \subset \mathbb{K}$ et $[\mathbb{Q}(a_1, a_2) : \mathbb{Q}] > [\mathbb{Q}(a_1) : \mathbb{Q}]$.

On construit ainsi par récurrence une suite strictement croissante de sous-espaces vectoriels de $\mathbb{K}$. Puisque la dimension de $\mathbb{K}$ est finie, il existe $n \in \mathbb{N}$ tel que $\mathbb{Q}(a_1, \ldots, a_n) = \mathbb{K}$.

Il suffit donc de prouver que pour tous nombres $a, b \in \mathbb{K}$, il existe $c \in \mathbb{K}$ tel que $\mathbb{Q}(a, b) = \mathbb{Q}(c)$.

Soient donc $a, b \in \mathbb{K}$ et $P_a, P_b \in \mathbb{Q}[X]$ leurs polynômes minimaux. Soient $a_1 = a, a_2, \ldots, a_m$ et $b_1 = b, b_2, \ldots, b_n$ les racines respectives de ces polynômes. Les $(a_i)_{i=1,\ldots,m}$ et les $(b_j)_{j=1,\ldots,n}$ sont deux à deux distincts, donc pour tout $i = 1, \ldots, m$ et $j = 1, \ldots, n$, l'équation $a_i + xb_j = a_1 + xb_1$ a au plus une solution. On peut donc choisir $z \in \mathbb{Z}^*$ ne vérifiant aucune de ces équations, et soit $c = a + zb$.

Il est clair que $\mathbb{Q}(c) \subset \mathbb{Q}(a, b)$ et qu'il suffit, pour montrer l'inclusion inverse, de montrer que $b \in \mathbb{Q}(c)$. Posons $Q(X) = P_a(c - zX)$. C'est un polynôme à coefficients dans $\mathbb{Q}(c)$ et b est la seule racine commune à Q et P_b. Donc b est l'unique racine du $PGCD$ de Q et P_b qui sont tous les deux dans $\mathbb{Q}(c)$, donc $b \in \mathbb{Q}(c)$. □

Exemples 2. 1. *Soit* $d \in \mathbb{Z}$ *sans facteur carré. Alors* $\mathbb{Q}(\sqrt{d}) = \{\alpha + \beta\sqrt{d} | \alpha, \beta \in \mathbb{Z}\}$ *est un corps de nombres de degré* 2 *appelé* ***corps quadratique****.*
2. *Soit* p *un nombre premier impair et* $\omega = e^{\frac{2i\pi}{p}}$. *Alors* $\mathbb{Q}(\omega)$ *est un corps de nombres de degré* $p - 1$, *appelé* ***corps cyclotomique****.*

2.2 Conjugués, normes et traces

Définition 7. *Soit $\mathbb{K}$ un corps de nombres de degré d.*
*On appelle **morphisme de conjugaison** tout morphisme de corps σ de $\mathbb{K}$ dans $\mathbb{C}$ laissant $\mathbb{Q}$ invariant, i.e. :*

$$\begin{cases} \sigma : \mathbb{K} \longrightarrow \mathbb{C} & \\ \sigma(x+y) = \sigma(x) + \sigma(y) & \forall x, y \in \mathbb{K} \\ \sigma(xy) = \sigma(x)\sigma(y) & \forall x, y \in \mathbb{K} \\ \sigma(r) = r & \forall r \in \mathbb{Q} \end{cases}$$

En particulier, σ est une application $\mathbb{Q}$-linéaire de $\mathbb{K}$ dans $\mathbb{C}$.

Théorème 4. *Soit $\mathbb{K}$ un corps de nombres de degré d, θ un élément primitif, $\theta_1 = \theta, \theta_2, \ldots, \theta_d$ les racines (distinctes) du polynôme minimal de θ.*
Il existe exactement d morphismes de conjugaison $\sigma_1, \ldots, \sigma_d$, définis par $\forall i = 1, \ldots, d, \sigma_i(\theta) = \theta_i$.

Démonstration

1. On note $\Pi(X) = \sum_{i=0}^{d} p_i X^i$ le polynôme minimal de θ. Par définition des morphismes de conjugaison,

$$\sum_{i=0}^{d} p_i \sigma(\theta)^i = \sigma(\sum_{i=0}^{d} p_i \theta^i) = \sigma(0) = 0$$

   Donc pour tout morphisme de conjugaison σ, $\sigma(\theta)$ est une racine de Π. Comme $\sigma(\theta)$ détermine σ, il existe au plus d morphismes de conjugaison.
2. Réciproquement, on définit d morphismes de conjugaison différents en posant :

$$\sigma_i(\sum_{k=0}^{d-1} a_k \theta^k) = \sum_{k=0}^{d-1} a_k \theta_i^k$$

□

Définition 8. *Soit $\mathbb{K}$ un corps de nombres de degré d, $\sigma_1 = Id, \sigma_2, \ldots, \sigma_d$ les d morphismes de conjugaison de $\mathbb{K}$.*
*Pour $x \in \mathbb{K}$, on définit la **norme de** x, notée $N(x)$ et la **trace de** x, notée $T(x)$ par :*

$$N(x) = \sigma_1(x)\sigma_2(x)\ldots\sigma_d(x)$$

$$T(x) = \sigma_1(x) + \sigma_2(x) + \ldots + \sigma_d(x)$$

Notons que pour $x \in \mathbb{Q}, N(x) = x^d$.

Théorème 5. *Soit $\mathbb{K}$ un corps de nombres de degré d.*

$$\forall x \in \mathbb{K}, N(x) \in \mathbb{Q} \text{ et } T(x) \in \mathbb{Q}$$
$$\forall x, y \in \mathbb{K}, T(x+y) = T(x) + T(y)$$
$$\forall x, y \in \mathbb{K}, N(xy) = N(x)N(y)$$
$$\forall x \in \mathbb{K}, N(x) = 0 \Leftrightarrow x = 0$$

Démonstration

1. Un peu de théorie de Galois,
2. évident,
3. évident,
4. $N(x) = 0 \Leftrightarrow \exists i \in \{1, \ldots, d\}, \sigma_i(x) = 0$. Or si x s'écrit $x = P(\theta)$ avec $P \in \mathbb{Q}_{d-1}[X]$, $\sigma_i(x) = 0 \Leftrightarrow P(\theta_i) = 0$ et comme le polynôme minimal de θ_i est Π, qui est de degré d, $P = 0$ et donc $x = 0$.

□

Exemples 3. *1. Soit $\mathbb{Q}(\sqrt{d})$ un corps quadratique. Alors les morphismes de conjugaison sont $\sigma_1 = Id$ et $\sigma_2(\alpha + \beta\sqrt{d}) = \alpha - \beta\sqrt{d}$. Par conséquent, $N(\alpha + \beta\sqrt{d}) = \alpha^2 - d\beta^2$ et $T(\alpha + \beta\sqrt{d}) = 2\alpha$.*
2. Soit $\mathbb{Q}(\sqrt[3]{d})$ un corps cubique pur ($\theta = \sqrt[3]{(d)}$). Alors $N(\alpha+\beta\theta+\gamma\theta) = \alpha^3+d\beta^3+d^2\gamma^3-3\alpha\beta\gamma d$ et $T(\alpha+\beta\theta+\gamma\theta) = 3\alpha$.

2.3 Anneau des entiers d'un corps de nombres

Définition 9. *On dit qu'un élément $\alpha \in \mathbb{C}$ est un* ***entier algébrique*** *si il est algébrique et si son polynôme minimal est à coefficients entiers relatifs.*

Théorème 6. *Soit $\alpha \in \mathbb{C}$ un nombre algébrique sur $\mathbb{Q}$. Alors il existe $k \in \mathbb{N}$ tel que $k\alpha$ soit un entier algébrique.*

Démonstration Soit $P_\alpha(X) = \sum_{i=0}^{d} a_i X^i$ le polyôme minimal de α. Si on écrit, $\forall i \in \{0, \dots, d\}, a_i = \frac{n_i}{d_i}$, et $k = \prod_{i=0}^{d} d_i$, alors $Q_\alpha(X) = \sum_{i=0}^{d} a_i k^{d-i} X^i$ est le polynôme minimal de $k\alpha$ et est à coefficients entiers. □

Théorème 7. *Si α et β sont des entiers algébriques, alors $\alpha + \beta$ et $\alpha\beta$ sont des entiers algébriques.*

Démonstration Soient α et β deux entiers algébriques et $P_\alpha = \sum_{i=0}^{d} a_i X^i$ et P_β leurs polynômes minimaux. Soient $\beta_1 = \beta, \beta_2, \dots, \beta_p$ les racines de P_β.

Alors $Q(X) = \prod_{i=1}^{p} P_\alpha(X - \beta_i)$ est un polynôme à coefficients entiers et annule $\alpha + \beta$.

De même $R(X) = \prod_{i=1}^{p} \beta_i^d P_\alpha(\frac{X}{\beta i})$ est un polynôme à coefficients entiers et annule $\alpha\beta$. □

Définition 10. *On appelle* ***entier de*** $\mathbb{K}$ *un élément de $\mathbb{K}$ qui est un entier algébrique.*

On appelle ***anneau des entiers****, et on note $\mathcal{O}_\mathbb{K}$, l'ensemble des entiers de $\mathbb{K}$, qui est un anneau d'après le théorème précédent.*

Proposition 2. $\forall \alpha \in \mathcal{O}_\mathbb{K}, N(\alpha) \in \mathbb{Z}$ *et* $T(\alpha) \in \mathbb{Z}$

Démonstration Pour tout morphisme de conjugaison σ, $P_\alpha(\sigma(\alpha)) = P_\alpha(\alpha) = 0$, donc $\sigma(\alpha)$ est un entier de $\mathbb{K}$. Donc comme produit et somme d'entiers de $\mathbb{K}$, $N(\alpha)$ et $T(\alpha)$ sont encore des entiers de $\mathbb{K}$, qui sont entiers parce qu'ils sont dans $\mathbb{Q}$. □

Exemples 4.
1. *Soit $\mathbb{Q}(\sqrt{d})$ un corps quadratique. Alors :*
   - *(a) Si $d \equiv 2$ ou 3 [mod 4], alors $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z}[\sqrt{d}]$,*
   - *(b) Si $d \equiv 1$ [mod 4], alors $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$.*
2. *Soit $\mathbb{Q}(\omega)$ un corps cyclotomique. Alors $\mathcal{O}_{\mathbb{Q}(\omega)} = \mathbb{Z}[\omega]$.*

2.4 Unités

Définition 11. *Soit $\mathcal{O}_\mathbb{K}$ l'anneau des entiers d'un corps de nombres $\mathbb{K}$ de degré d. Soit $\mathcal{O}_\mathbb{K}^\times$ son groupe des unités.*

Théorème 8. *Alors $\forall \epsilon \in \mathcal{O}_\mathbb{K}, \epsilon \in \mathcal{O}_\mathbb{K}^\times \Leftrightarrow |N(\epsilon)| = 1$.*

Démonstration

1. $N(\epsilon) = \pm 1 = \epsilon . \prod_{i=2}^{d} \sigma_i(\epsilon)$. Or $\forall \alpha \in \mathcal{O}_\mathbb{K}, \forall i \in \{2, \dots, n\}, \sigma(\alpha) \in \mathcal{O}_\mathbb{K}$, et donc le produit $\prod_{i=2}^{d} \sigma_i(a)$ est encore dans $\mathcal{O}_\mathbb{K}$. Donc ϵ est bien inversible dans $\mathcal{O}_\mathbb{K}$.
2. Réciproquement, $\epsilon\epsilon' = 1$, *avec* $\epsilon, \epsilon' \in \mathcal{O}_\mathbb{K} \Rightarrow N(\epsilon)N(\epsilon') = 1 \Rightarrow |N(\epsilon)| = 1$ car $N(\epsilon), N(\epsilon') \in \mathbb{Z}$.

□

Théorème 9. *Soit $\mathbb{K}$ un corps de nombres. Il existe $\eta_1, \dots, \eta_k$, appelées* ***unités fondamentales****, telles que tout $\epsilon \in \mathcal{O}_\mathbb{K}^\times$ s'écrive, de manière unique, sous la forme d'un produit $\epsilon = \zeta \eta_1^{n_1} \dots \eta_k^{n_k}$, avec $n_i \in \mathbb{Z}$ et ζ est une racine de l'unité appartenant à $\mathcal{O}_\mathbb{K}^\times$.*

Exemples 5.
1. *Soit $\mathbb{Q}(i\sqrt{d})$ un corps quadratique imaginaire. Alors :*
   - *(a) Si $d = 1$, alors $\mathcal{O}_{\mathbb{Q}(i\sqrt{d})}^\times = \mathbb{U}_4$,*
   - *(b) Si $d = 3$, alors $\mathcal{O}_{\mathbb{Q}(i\sqrt{d})}^\times = \mathbb{U}_6$,*
   - *(c) Si $d \notin \{1, 3\}$, alors $\mathcal{O}_{\mathbb{Q}(i\sqrt{d})}^\times = \{\pm 1\}$.*
2. *Soit $\mathbb{Q}(\sqrt{d})$ un corps quadratique réel. Alors il existe une unité fondamentale $\lambda > 1$ telle que $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}^\times = \{\pm\lambda^n | n \in \mathbb{Z}\}$.*
3. *Soit $\mathbb{Q}(\omega)$ un corps cyclotomique. Alors les unités de $\mathbb{Q}(\omega)$ sont de la forme $\epsilon = \eta\omega^n$, où $n \in \mathbb{N}$ et η est une unité réelle.*

2.5 Discriminants et bases entières

Définition 12. *Soit $\mathbb{K} = \mathbb{Q}(\theta)$ un corps de nombres de degré d. Soit $\Lambda = (\lambda_1, \ldots, \lambda_d)$ une base de $\mathbb{K}$ en tant que $\mathbb{Q}$-espace vectoriel.*

On définit le ***discriminant*** $\Delta[\lambda_1, \ldots, \lambda_d]$ ***de cette base*** *par :*

$$\Delta[\lambda_1, \ldots, \lambda_d] = D[\lambda_1, \ldots, \lambda_d]^2 = (det \begin{bmatrix} \sigma_1(\lambda_1) & \sigma_1(\lambda_2) & \ldots & \sigma_1(\lambda_d) \\ \sigma_2(\lambda_1) & \sigma_2(\lambda_2) & \ldots & \sigma_2(\lambda_d) \\ \vdots & & \ddots & \vdots \\ \sigma_d(\lambda_1) & \sigma_d(\lambda_2) & \ldots & \sigma_d(\lambda_d) \end{bmatrix})^2$$

Proposition 3. *Soit $\mathbb{K} = \mathbb{Q}(\theta)$ un corps de nombres de degré d et Π le polynôme minimal de θ. Il est clair que $(1, \theta, \theta^2, \ldots, \theta^{d-1})$ est une base du $\mathbb{Q}$-espace vectoriel $\mathbb{K}$ et :*

$$\Delta[1, \theta, \theta^2, \ldots, \theta^{d-1}] = (-1)^{\frac{d(d-1)}{2}} N(\Pi'(\theta))$$

Démonstration On appelle $\theta_1 = \theta, \theta_2, \ldots, \theta_d$ les racines de Π. Par définition des $\sigma_i, \sigma_i(\theta^j) = \theta_i^j$, et donc :

$$\Delta[1, \theta, \theta^2, \ldots, \theta^{d-1}] = (det \begin{bmatrix} 1 & 1 & \ldots & 1 \\ \theta_1 & \theta_2 & \ldots & \theta_2 \\ \vdots & & \ddots & \vdots \\ \theta_1^{d-1} & \theta_2^{d-1} & \ldots & \theta_d^{d-1} \end{bmatrix})^2 = \prod_{1 \leq i \leq j \leq d} (\theta_i - \theta_j)^2$$

Or $\Pi(X) = \prod_{i=1}^{d}(X - \theta_i)$, et donc

$$\Pi'(X) = \sum_{j=1}^{d} \prod_{i \neq j} (X - \theta_i) \text{ et } \Pi'(\theta_j) = \prod_{i \neq j} (\theta_j - \theta_i)$$

et donc en prenant la norme,

$$N(\Pi'(\theta)) = \prod_{j=1}^{d} \prod_{i \neq j} (\theta_j - \theta_i) = (-1)^{\frac{d(d-1)}{2}} \prod_{1 \leq i \leq j \leq d} (\theta_i - \theta_j)^2 = (-1)^{\frac{d(d-1)}{2}} \Delta[1, \theta, \theta^2, \ldots, \theta^{d-1}]$$

□

Proposition 4. *Soit $\mathbb{K} = \mathbb{Q}(\theta)$ un corps de nombres de degré d. Soient $A = (\alpha_1, \ldots, \alpha_d)$ et $B = (\beta_1, \ldots, \beta_d)$ deux bases du $\mathbb{Q}$-espace vectoriel $\mathbb{K}$.*

Posons $\alpha_j = \sum_{i=1}^{d} c_{i,i}\beta_i$. Alors :

$$\Delta[\alpha_1, \ldots, \alpha_d] = (det[c_{i,j}]_{1 \leq i,j \leq d})^2 \Delta[\beta_1, \ldots, \beta_d]$$

Proposition 5. *Pour toute base $A = (\alpha_1, \ldots, \alpha_d)$ de $\mathbb{K} = \mathbb{Q}(\theta)$, $\Delta[\alpha_1, \ldots, \alpha_d] \in \mathbb{Q}^{*+}$.*

De plus, si pour tout i, $\alpha_i \in \mathcal{O}_{\mathbb{K}}$, alors $\Delta[\alpha_1, \ldots, \alpha_d] \in \mathbb{N}$.

Démonstration

$$\Delta[\alpha_1, \ldots, \alpha_d] = (det[c_{i,j}]_{1 \leq i,j \leq d})^2 \Delta[1, \theta, \theta^2, \ldots, \theta^{d-1}] = (det[c_{i,j}]_{1 \leq i,j \leq d})^2 (-1)^{\frac{d(d-1)}{2}} N(\Pi'(\theta)) \in \mathbb{Q}^{*+}$$

De plus, si tous les α_i sont des entiers algébriques, les $\sigma_j(\alpha_i)$ sont aussi des entiers algébriques, et $\Delta[\alpha_1, \ldots, \alpha_d]$, comme sommes et produits d'entiers algébriques est encore algébrique. □

Théorème 10. *Soit $\mathbb{K} = \mathbb{Q}(\theta)$ un corps de nombres de degré d et $\mathbb{I} \neq \{0\}$ un idéal de $\mathcal{O}_{\mathbb{K}}$.*

Alors il existe $\alpha_1, \alpha_2, \ldots, \alpha_d \in \mathbb{I}$, linéairement indépendants sur $\mathbb{Q}$, tels que :

$$\mathbb{I} = \{n_1\alpha_1 + \ldots + n_d\alpha_d | n_1, \ldots, n_d \in \mathbb{Z}\}$$

Autrement dit, tout idéal de $\mathcal{O}_{\mathbb{K}}$ est un $\mathbb{Z}$-module de rang d.

Remarque 4. *Si $A = (\alpha_1, \ldots, \alpha_d)$ et $B = (\beta_1, \ldots, \beta_d)$ deux bases de l'idéal $\mathbb{I}$ considéré comme $\mathbb{Z}$-module, en posant $\alpha_j = \sum_{i=1}^{d} c_{i,i}\beta_i$ et $\beta_j = \sum_{i=1}^{d} c'_{i,i}\alpha_i$, il est clair que $[c_{i,j}]_{1 \leq i,j \leq d}$ et $[c'_{i,j}]_{1 \leq i,j \leq d}$ sont inverses l'une de l'autre, et donc que $det([c_{i,j}]_{1 \leq i,j \leq d}) det([c'_{i,j}]_{1 \leq i,j \leq d}) = 1$. Ceci implique que $det([c_{i,j}]_{1 \leq i,j \leq d}) = \pm 1$ et donc*

$$\Delta[\alpha_1, \ldots, \alpha_d] = (det[c_{i,j}]_{1 \leq i,j \leq d})^2 \Delta[\beta_1, \ldots, \beta_d] = \Delta[\beta_1, \ldots, \beta_d]$$

D'où la définition :

Définition 13. *Soit $\mathbb{K} = \mathbb{Q}(\theta)$ un corps de nombres de degré d et $\mathbb{I} \neq \{0\}$ un idéal de $\mathcal{O}_\mathbb{K}$.*
*L'entier naturel $\Delta[\alpha_1, \ldots, \alpha_d]$, qui ne dépend pas de la base $(\alpha_1, \ldots, \alpha_d)$ du $\mathbb{Z}$-module $\mathbb{I}$, est appelé **discriminant de** $\mathbb{I}$ et noté $\Delta(\mathbb{I})$.*

Remarque 5. *$\mathcal{O}_\mathbb{K}$ est un idéal de $\mathcal{O}_\mathbb{K}$.*
*Son discriminant est appelé **discriminant du corps** $\mathbb{K}$, et noté $\Delta(\mathbb{K})$.*

Exemples 6. *1. Soit $\mathbb{Q}(\sqrt{d})$ un corps quadratique. Alors :*
(a) Si $d \equiv 2$ ou 3 $[mod\ 4]$, alors $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z}(\sqrt{d})$, donc $\Delta(\mathbb{Q}(\sqrt{d})) = 4d$,
(b) Si $d \equiv 1$ $[mod\ 4]$, alors $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z}(\frac{1+\sqrt{d}}{2})$, donc $\Delta(\mathbb{Q}(\sqrt{d})) = d$.
2. Soit $\mathbb{Q}(\omega)$ un corps cyclotomique. Alors $\Delta(\mathbb{Q}(\omega)) = (-1)^{\frac{p-1}{2}} p^{p-2}$

3 Idéaux

3.1 Idéaux d'un corps de nombres

Définition 14. *Soit $\mathbb{K} = \mathbb{Q}(\theta)$ un corps de nombres, $\mathcal{O}_\mathbb{K}$ l'anneau des entiers de $\mathbb{K}$ et $\alpha_1, \ldots, \alpha_n \in \mathbb{K}$.*
*On appelle **idéal fractionnaire de** $\mathbb{K}$ **engendré par** $\alpha_1, \ldots, \alpha_n$ le $\mathcal{O}_\mathbb{K}$-module engendré par $\alpha_1, \ldots, \alpha_n$.*
On note $\mathcal{I}(\mathbb{K})$ l'ensemble des idéaux fractionnaires de $\mathbb{K}$.

*Si $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_\mathbb{K}$, on dit que c'est un **idéal entier de** $\mathcal{O}_\mathbb{K}$.*

Remarque 6. *Un idéal entier de $\mathcal{O}_\mathbb{K}$ est un idéal de $\mathcal{O}_\mathbb{K}$.*

Définition 15. *Soient $A =< \alpha_1, \ldots, \alpha_n >$ et $B =< \beta_1, \ldots, \beta_m >$ deux idéaux fractionnaires de $\mathbb{K}$. On pose :*

$$A + B = \{a + b | a \in A, b \in B\}$$

$$A.B = \{\sum_{i=1}^{q} a_i b_i | q \in \mathbb{N}^*, a_i \in A, b_i \in B\}$$

Remarque 7. *Il est clair que : $A+B =< \alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m >$ et $A.B =< \alpha_1\beta_1, \ldots, \alpha_1\beta_m, \alpha_2\beta_1, \ldots, \alpha_n\beta_1, \ldots, \alpha_n\beta_m >$.*

Proposition 6. *$(\mathcal{I}(\mathbb{K})^*, .)$ est un groupe commutatif d'élément neutre $< 1 >= \mathcal{O}_\mathbb{K}$.*

Démonstration

1. La multiplication est clairement commutative et $\mathcal{O}_\mathbb{K}$ est bien neutre. Il ne reste donc qu'à montrer l'existence de l'inverse.
2. Soient $U(X) = \sum_{i=0}^{n} u_i X^i$ et $V(X) = \sum_{j=0}^{m} v_j X^j$ deux polynômes dont les coefficients sont des entiers algébriques (avec $u_n \neq 0$ et $v_m \neq 0$) et $W(X) = U(X)V(X) = \sum_{k=0}^{nm} w_k X^k$. Si il existe un entier algébrique δ tel que tous les w_k/δ soient des entiers algébriques, alors tous les $u_i v_j/\delta$ sont des entiers algébriques.
3. Soit $A =< \alpha_1, \ldots, \alpha_n >$ un idéal fractionnaire non nul (avec $\alpha_n \neq 0$). On note $\sigma_1 = Id, \sigma_2, \ldots, \sigma_d$ les morphismes de conjugaison. On pose $f(X) = \sum_{i=0}^{n} \alpha_i X^i$ et $g(X) = \prod_{j=2}^{d} (\sum_{i=0}^{n} \sigma_j(\alpha_i) X^i)$.
Alors $f(X), g(X) \in \mathcal{O}_\mathbb{K}[X]$ et $f(X)g(X) \sum_{k=0}^{(d-1)n} \gamma_k X^k \in \mathbb{Z}[X]$.
On pose $a = pgcd(\gamma_i | i \in \{0, \ldots, (d-1)n\})$. Alors $< a^{-1} > B$ est l'inverse de A.

□

Remarque 8. *La multiplication est distributive sur l'addition.*

3.2 Arithmétique des idéaux entiers

Définition 16. *Soient $A, B \in \mathcal{I}(\mathcal{O}_\mathbb{K})$ deux idéaux entiers.*
*On dit que A **divise** B, et on note $A|B$, si il existe $C \in \mathcal{I}(\mathcal{O}_\mathbb{K})$ tel que $A.C = B$.*

Théorème 11. *Soient $A, B \in \mathcal{I}(\mathcal{O}_\mathbb{K})$. Alors $A|B \Leftrightarrow B \subset A$.*

Démonstration
– $A|B \Rightarrow \exists C \in \mathcal{I}(\mathcal{O}_\mathbb{K}), B = A.C \subset A$.

– Supposons $B \subset A$. Le cas $A =< 0 >$ est trivial. Sinon, A est inversible dans $\mathcal{I}(\mathbb{K})$ et $B \subset A \Rightarrow BA^{-1} \subset< 1 >$. Donc BA^{-1} est un idéal entier C et $B = A.C$.

□

Définition 17. *On définit, de la même façon que pour les entiers, le* ***Plus Grand Diviseur Commun*** *:*

$$PGCD(A,B)|A, PGCD(A,B)|B \text{ et } D|A \text{ et } D|B \Rightarrow D|PGCD(A,B)$$

Théorème 12. *Soient $A, B \in \mathcal{I}(\mathcal{O}_\mathbb{K})$. Alors $PGCD(A,B) = A + B$.*

Démonstration

$$\left.\begin{array}{l} 0 \in A \Rightarrow A \subset (A+B) \Rightarrow (A+B)|A \\ 0 \in B \Rightarrow B \subset (A+B) \Rightarrow (A+B)|B \end{array}\right\} \Rightarrow (A+B)|PGCD(A,B)$$

$$\left.\begin{array}{l} A = PGCD(A,B)A' \\ B = PGCD(A,B)B' \end{array}\right\} \Rightarrow PGCD(A,B)|(A+B)$$

□

Définition 18. *Deux idéaux A et B sont* ***premiers entre eux*** *si $PGCD(A,B) = A + B =< 1 >$.*

Remarque 9. *On voit bien ici une généralisation de l'identité de Bezout : si $A =< a >$ et $B =< b >$ sont deux idéaux principaux, alors $A + B = \{au + bv | u, v \in \mathcal{O}_\mathbb{K}\}$.*

Théorème 13 (de Gauss). *Soient $A, B, C \in \mathcal{I}(\mathcal{O}_\mathbb{K})$.*
Si $A|BC$ et A est premier avec B, alors $A|C$.

Démonstration

$$\left.\begin{array}{l} A + B =< 1 > \\ AD = BC \end{array}\right\} \Rightarrow A(C+D) = AC + AD = AC + BC = (A+B)C = C$$

□

Définition 19. *Soit $P \in \mathcal{I}(\mathcal{O}_\mathbb{K})$ est* ***premier*** *si $P \neq< 1 >$ et si $\forall A \in \mathcal{I}(\mathcal{O}_\mathbb{K}), A|P \Rightarrow A =< 1 >$ ou $A = P$.*

Lemme 1. *Soient P et Q deux idéaux entiers tels que $B|A$.*
Alors $\Delta(A)|\Delta(B)$.
Si de plus $\Delta(A) = \Delta(B)$, alors $A = B$.

Démonstration Soient $(\alpha_1, \ldots, \alpha_d)$ et $(\beta_1, \ldots, \beta_d)$ des bases respectives de A et B.

$B|A \Rightarrow A \subset B$, donc si on écrit $\alpha_j = \sum_{i=1}^{d} c_{i,i}\beta_i$, alors les $c_{i,j}$ sont des entiers de $\mathbb{K}$, donc $det[c_{i,j}]_{1\leq i,j\leq d} \in \mathbb{Z}$ et comme $\Delta[\alpha_1, \ldots, \alpha_d] = (det[c_{i,j}]_{1\leq i,j\leq d})^2 \Delta[\beta_1, \ldots, \beta_d]$, $\Delta(A)|\Delta(B)$.

Si $\Delta(A) = \Delta(B)$, $det[c_{i,j}]_{1\leq i,j\leq d} = \pm 1$, donc $[c_{i,j}]_{1\leq i,j\leq d}$ est inversible dans $\mathcal{M}_d(\mathcal{O}_\mathbb{K})$, donc on a $\beta_j = \sum_{i=1}^{d} c'_{i,i}\alpha_i$, avec $c'_{i,j} \in \mathcal{O}_\mathbb{K}$, et donc $B \subset A$. D'où $A = B$. □

Théorème 14 (de décomposition unique en produit d'idéaux premiers). *Soit $A \in \mathcal{I}(\mathcal{O}_\mathbb{K}) \setminus \{< 0 >, < 1 >\}$.*
A s'exprime comme un produit d'idéaux premiers, unique à l'ordre des facteurs près.

Démonstration

1. existence : soit $P_1 \neq< 1 >$ un diviseur de A de discriminant minimum. D'après le lemme précédent, P est premier. De plus, si on pose $A = A_1P_1$, on a $\Delta(A) > \Delta(A_1)$. On peut donc faire une récurrence sur le discriminant de A.
2. unicité : si $A = P_1 \ldots P_n = P'_1 \ldots P'_m$, le théoreème de Gauss permet de montrer qu'il existe i tel que $P_1|P'_i$ et donc $P_1 = P'_i$. Par récurrence, on obtient $n = m$ et $\sigma \in \mathfrak{S}_n$ tel que $\forall i \in \{1, \ldots, n\}, P_i = P'_{\sigma(i)}$.

□

3.3 Norme d'un idéal

Théorème 15. *$\forall A \in \mathcal{I}(\mathcal{O}_\mathbb{K})^*, \mathcal{O}_\mathbb{K}/A$ est fini.*

Démonstration

1. construction d'une base diagonale : Soit $d = [\mathbb{K} : \mathbb{Q}]$ le degré de $\mathbb{K}$ et $\alpha_1, \ldots, \alpha_d$ une base du $\mathbb{Q}$-espace vectoriel $\mathbb{K}$. On pose $\beta_1 = c_{1,1}\alpha_1$ où $c_{1,1}$ est le plus petit entier strictement positif tel que $c_{1,1}\alpha_1 \in A$ (existe car pour $x \in \mathcal{O}_\mathbb{K}, |N(x)|\alpha_1 \in A$). On pose ensuite $\beta_2 = c_{2,1}\alpha_1 + c_{2,2}\alpha_2$ où $c_{2,2}$ est le plus petit entier strictement positif pour lequel il existe un rationel $c_{2,1}$ tel que $c_{2,1}\alpha_1 + c_{2,2}\alpha_2 \in A$ (existe car pour $x \in \mathcal{O}_\mathbb{K}, |N(x)|(\alpha_1 + \alpha_2) \in A$). On obtient ainsi par récurrence $\beta_1, \ldots, \beta_d$ de A de la forme $\beta_i = \sum_{j=1}^{i} c_{i,j}\alpha_j$, avec la propriété :

$$(x = \sum_{j=1}^{i} x_{i,j}\alpha_j \in A avec \forall i, j, x_{i,j} \in \mathbb{Z} \text{ et } x_{i,i} > 0) \Rightarrow (\forall i, x_{i,i} \geq c_{i,j} > 0)$$

   Il est clair que cette famille est libre et qu'elle est génératrice de A (par division euclidienne).

2. d'autre part, il est facile de vérifier que $E = \{\sum_{i=1}^{d} r_i\alpha_i | \forall i \in \{1, \ldots, n\}, 0 \leq r_i < c_{i,i}\}$ est un système de représentants de $\mathcal{O}_\mathbb{K}/A$. On en conclut donc que $\mathcal{O}_\mathbb{K}/A$ est fini de cardinal $card(E) = \prod_{i=1}^{d} c_{i,i}$.

□

Définition 20. *Pour tout idéal non nul A de $\mathcal{O}_\mathbb{K}$, on appelle* ***norme de*** *A l'entier : $N(A) = card(\mathcal{O}_\mathbb{K}/A)$.*

Proposition 7. *1. $\forall A \in \mathcal{I}(\mathcal{O}_\mathbb{K})^*, \Delta(A) = (N(A))^2\Delta(\mathbb{K})$,*

2. $\forall a \in \mathcal{O}_\mathbb{K}^*, N(< a >) = |N(a)|$,

3. $\forall A, B \in \mathcal{I}(\mathcal{O}_\mathbb{K})^*, N(AB) = N(A)N(B)$.

Démonstration

1. $\Delta(A) = \Delta[\beta_1, \ldots, \beta_n] = (det[c_{i,j}]_{1 \leq i,j \leq d})^2\Delta[\alpha_1, \ldots, \alpha_d] = (\prod_{i=1}^{d} c_{i,i})^2\Delta[\alpha_1, \ldots, \alpha_d] = (N(A))^2\Delta(\mathbb{K})$
2. $(a\alpha_1, \ldots, a\alpha_d)$ est une base de $< a >$, donc

$$\Delta(< a >) = (det \begin{bmatrix} \sigma_1(a\alpha_1) & \sigma_1(a\alpha_2) & \ldots & \sigma_1(a\alpha_d) \\ \sigma_2(a\alpha_1) & \sigma_2(a\alpha_2) & \ldots & \sigma_2(a\alpha_d) \\ \vdots & & \ddots & \vdots \\ \sigma_d(a\alpha_1) & \sigma_d(a\alpha_2) & \ldots & \sigma_d(a\alpha_d) \end{bmatrix})^2 = N(a)^2\Delta(\mathbb{K})$$

   Comme $\Delta(< a >) = N(< a >)^2\Delta(\mathbb{K})$, on obtient $N(a)^2 = N(< a >)^2$ d'où le résultat.

3. laissée au lecteur.

□

3.4 Nombre de classes d'idéaux

On ne donne ici que des résultats sans démonstration, les démonstrations étant présentées lors du prochain exposé.

Définition 21. *Soit $\mathbb{K}$ un corps de nombres et $\mathcal{I}(\mathbb{K})^*$ le groupe multiplicatif des idéaux non nuls de $\mathbb{K}$. Soit $\mathcal{P}(\mathbb{K})$ le sous groupe de $\mathcal{I}(\mathbb{K})^*$ formé des idéaux principaux non nuls de $\mathbb{K}$. On définit le* ***groupe des classes d'idéaux de*** *$\mathbb{K}$ par :*

$$\mathcal{C}(\mathbb{K}) = \mathcal{I}(\mathbb{K})^*/\mathcal{P}(\mathbb{K})$$

On dira que deux idéaux fractionnaires A et B sont ***équivalents*** *si ils sont égaux modulo $\mathcal{P}(\mathbb{K})$, autrement dit :*

$$\forall A, B \in \mathcal{I}(\mathbb{K})^*, A \sim B \Leftrightarrow \exists a \in \mathbb{K}, \text{ tel que } A =< a > B$$

Théorème 16. *$\mathcal{C}(\mathbb{K})$ est fini. On note $h(\mathbb{K})$ son cardinal.*

4 Références

Daniel Perrin, Cours d'algèbre, ellipses.

Daniel Duverney, Théorie des nombres, Dunod.

Kenneth Ireland & Michael Rosen, A Classical Introduction to Modern Number Theory, Graduate texts in mathematics 84.