Chapitre 1 : L'anneau des entiers d'un corps de nombres

① Nombres algébriques et entiers algébriques

Définition. Un nombre algébrique est un nombre complexe $z \in \mathbb{C}$ tel qu'il existe un polynôme non nul $P \in \mathbb{Q}[X]$ avec $P(z) = 0$. Un entier algébrique est un nombre complexe z tel qu'il existe un polynôme unitaire $P \in \mathbb{Z}[X]$ avec $P(z) = 0$.

On note $\overline{\mathbb{Z}} \subset \overline{\mathbb{Q}} \subset \mathbb{C}$ les ensembles des entiers algébriques et des nombres algébriques.

Exemple : Pour tout entier d, le nombre $a + b\sqrt{d}$ $(a, b \in \mathbb{Q})$ est algébrique. En effet,

$$z = a + b\sqrt{d}$$

$$z^2 = a^2 + 2ab\sqrt{d} + b^2 d$$

$$z^2 - 2az = -a^2 + b^2 d$$

$$\boxed{z^2 - 2az + a^2 - b^2 d = 0}$$

Un des premiers objectifs sera de décider quand c'est un entier algébrique. C'est par exemple le cas si $a, b \in \mathbb{Z}$, mais $\frac{1+\sqrt{3}}{2}$ l'est aussi,

racine du polynôme $X^2 - X + 1$.

Exemple : les nombres $e = \sum_{n=0}^{\infty} \frac{1}{n!}$ et $\pi = \int_{x^2+y^2 \leq 1} dx\,dy$ ne sont pas algébriques. On les appelle transcendants.

Proposition : La somme et le produit de deux nombres algébriques est algébrique. L'inverse d'un nombre algébrique est algébrique.

La somme et le produit de deux entiers algébriques sont des entiers algébriques.

$$\Rightarrow \quad \overline{\mathbb{Z}} \subset \overline{\mathbb{Q}} \subset \mathbb{C}$$

$\overline{\mathbb{Z}}$: sous-anneau de $\mathbb{C}$; $\overline{\mathbb{Q}}$: sous-corps de $\mathbb{C}$

Démonstration : * Si $\alpha \in \overline{\mathbb{Q}}^{\times}$ est annulé par un polynôme $P(X) = a_n X^n + \dots + a_0$, alors

$$0 = a_n \alpha^n + a_{n-1} \alpha^{n-1} + \dots + a_1 \alpha + a_0$$

$$0 = a_n + a_{n-1} \frac{1}{\alpha} + \dots + a_1 \frac{1}{\alpha^{n-1}} + a_0 \frac{1}{\alpha^n}$$

et donc $\frac{1}{\alpha}$ est annulé par le polynôme

$$a_n + a_{n-1} X + \dots + a_0 X^n.$$

Lemme : Soit V un espace vectoriel sur un corps K et soit $v_1, \dots, v_n$ une famille génératrice de V. Soit $f : V \to V$ un endomorphisme et soit $A = (a_{ij}) \in M_n(K)$ telle que

$$f(v_j) = \sum_{i=1}^{n} a_{ij} v_i \qquad j = 1, \dots, n$$

Si P est le polynôme caractéristique de A, on a

$$P(f) = 0.$$

Démonstration : Soit $u : K^n \to V$, $e_i \mapsto v_i$, et soit $\varphi : K^n \to K^n$ l'endomorphisme de matrice A. Alors $u \circ \varphi = f \circ u$, d'où :

$$0 = u \circ P(\varphi) = P(f) \circ u$$

$P(\varphi) = 0$ par Cayley-Hamilton

Mais comme u est surjectif, $P(f) \circ u = 0$ implique $P(f) = 0$. □

Soient x et y des nombres algébriques, annulés par des polynômes $P, Q \in \mathbb{Q}[X]$. Pour tout couple (m, n) d'entiers ≥ 0, il existe $P_{m,n} \in \mathbb{Q}[X, Y]$ de degré $\leq \deg(P) - 1$

en X et de degré $\leq \deg(Q)-1$ en Y tel que

$$X^m Y^n = P_{m,n}(X,Y)$$

(En effet, $X^m Y^n = (BP+R)(CQ+R')$ et on prend $P_{m,n}(X,Y) = R(X)R'(Y)$).

Pour $z = x+y$ ou $z = xy$, il existe donc une matrice $A = \left(a_{(i,j),(k,\ell)}\right)_{\substack{0\leq i,k<\deg P \\ 0\leq j,\ell<\deg Q}}$ avec

$$z\, x^k y^\ell = \sum_{i,j} a_{(i,j),(k,\ell)}\, x^i y^j$$

Soit Π le polynôme caractéristique de la matrice A. Appliquée à l'endomorphisme multiplication par z de l'espace vectoriel $V \subset \mathbb{Q}[X]$ engendré par $X^k Y^\ell$ ($0\leq k<\deg P$, $0\leq \ell<\deg Q$), le lemme précédent donne $\Pi(z) = 0$.

Si x et y sont des entiers algébriques, on choisit $P, Q \in \mathbb{Z}[X]$ unitaires. Alors $P_{m,n} \in \mathbb{Z}[X,Y]$ et $\Pi \in \mathbb{Z}[X]$ est unitaire. □

Exemple : Soit $z = \sqrt{2}+\sqrt{3}$. Alors :

$$(\sqrt{2}+\sqrt{3})\cdot 1 = 0 + 1\sqrt{2} + 1\cdot\sqrt{3} + 0$$

$$(\sqrt{2}+\sqrt{3})\cdot\sqrt{2} = 2 + 0\sqrt{2} + 0\sqrt{3} + \sqrt{6}$$

$$(\sqrt{2}+\sqrt{3})\cdot\sqrt{3} = 3 + 0\sqrt{2} + 0\sqrt{3} + \sqrt{6}$$

$$(\sqrt{2}+\sqrt{3})\cdot\sqrt{6} = 0 + 3\sqrt{2} + 2\sqrt{3} + 0$$

La matrice est donc $A = \begin{pmatrix} 0 & 2 & 3 & 0 \\ 1 & 0 & 0 & 3 \\ 1 & 0 & 0 & 2 \\ 0 & 1 & 1 & 0 \end{pmatrix}$, de

polynôme caractéristique

$$\det \begin{pmatrix} -X & 2 & 3 & 0 \\ 1 & -X & 0 & 3 \\ 1 & 0 & -X & 2 \\ 0 & 1 & 1 & -X \end{pmatrix} = X^4 - 10X^2 + 1$$

donc $(\sqrt{2}+\sqrt{3})^4 - 10(\sqrt{2}+\sqrt{3})^2 + 1 = 0$

Définition : le polynôme minimal d'un nombre algébrique est le polynôme unitaire de plus petit degré dans $\mathbb{Q}[X]$ qui l'annule. Son degré est appelé le degré du nombre algébrique.

(Unicité : si $P, P' \in \mathbb{Q}[X]$ unitaires de degré minimal annulent z, alors $P - P'$ annule z aussi et est de degré inférieur).

Proposition : Un nombre algébrique est un entier algébrique si et seulement si son polynôme minimal est à coefficients entiers.

Démonstration : $\Leftarrow$ évident

$\Rightarrow$ Soit z un nombre algébrique de polynôme minimal $P \in \mathbb{Q}[X]$ et soit $Q \in \mathbb{Z}[X]$ un polynôme unitaire à coefficients entiers tel que $Q(z) = 0$. Alors P divise Q et on conclut par le lemme suivant □

Lemme : Soient $A \in \mathbb{Z}[X]$ et $B \in \mathbb{Q}[X]$ des polynômes unitaires. Si B divise A, alors $B \in \mathbb{Z}[X]$.

Preuve du lemme

Elle repose sur un autre

Lemme : Soient $A, B \in \mathbb{Z}[X]$ tels que B divise A dans $\mathbb{Q}[X]$. Si B est primitif (i.e. ses coefficients sont premiers entre eux), alors B divise A dans $\mathbb{Z}[X]$.

Démonstration : Soit $R \in \mathbb{Q}[X]$ tel que $A = B \cdot R$.
Soit $a \geq 1$ le plus petit dénominateur commun des coefficients de R. On a $aA = B \underbrace{aR}_{\in \mathbb{Z}[X]}$.
Soit p un facteur premier de a. On a

$$(B \bmod p)(aR \bmod p) = 0$$

et $B \bmod p$ n'est pas nul car B est primitif.
Comme $\mathbb{Z}/p\mathbb{Z}$ est un corps, $aR \bmod p$ est nul.
Tous les coefficients de R sont donc multiples de p, c'est-à-dire $\frac{a}{p} R \in \mathbb{Z}[X]$, ce qui contredit la minimalité de a. Donc $a = 1$ et $R \in \mathbb{Z}[X]$ □

Preuve : Il reste des entiers a, b tels que $\frac{aB}{b} \in \mathbb{Z}[X]$ soit primitif. Comme B divise A, $\frac{aB}{b}$ + premiers entre eux.
$\frac{aB}{b}$ divise A dans $\mathbb{Z}[X]$ d'après le lemme.
Soit $R \in \mathbb{Z}[X]$ tel que $A = \frac{aB}{b} \cdot R$, c'est-à-dire $bA = aB \cdot R$. Comme A et B sont entiers, $b = a \cdot$ coefficient dominant de R, donc $a = 1$ car a et b sont premiers entre eux. Mais alors

$$B = b \cdot \underbrace{\frac{1}{b} B}_{\in \mathbb{Z}[X]} \in \mathbb{Z}[X]$$

□

Corollaire: Soit z un nbre algébrique de polynôme minimal $P = X^n + a_{n-1}X^{n-1} + \dots + a_0$.

(1) Soit $d \geq 1$ un entier. Pour que dz soit un entier algébrique il faut et il suffit que $d^i a_{n-i} \in \mathbb{Z}$ pour tout $i = 1, \dots, n$

(2) Si $z \neq 0$ est un entier algébrique, alors $1/z$ est un entier algébrique $\iff a_0 \in \{\pm 1\}$.

Preuve: le polynôme minimal de dz est

$$d^n P\left(\frac{X}{d}\right) = X^n + d a_{n-1} X^{n-1} + \dots$$

En effet, il est unitaire, il annule dz et c'est celui de plus petit degré car P est irréductible dans $\mathbb{Q}[X]$.

(2) Si $z \neq 0$, alors $a_0 \neq 0$. Le polynôme

$$\frac{1}{a_0} X^n \cdot P\left(\frac{1}{X}\right) = X^n + \frac{a_1}{a_0} X^{n-1} + \dots + \frac{1}{a_0}$$

est le polynôme minimal de $1/z$.

$1/z$ entier algébrique $\iff$ ce polynôme est à coefficients entiers

$\iff a_0 \in \{\pm 1\}$ □

Corollaire: $\overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$

(En effet, le polynôme minimal de $z \in \mathbb{Q}$ est $X - z$).

Lemme : le polynôme minimal d'un nombre algébrique de degré n a des racines simples dans $\mathbb{C}$.

Démonstration. Il suffit de montrer que $P \in \mathbb{Q}[X]$ unitaire irréductible de degré n n'a pas de racine multiple. Soit

$$D = pgcd(P, P') \in \mathbb{Q}[X]$$ unitaire

Comme $D \mid P$ et que P est irréductible, soit $D = P$ soit $D = 1$. Mais si $P = X^n + \dots$, alors $P' = nX^{n-1} + \dots$ est de degré $n-1$ et ne peut pas être divisible par P. Donc $D = 1$, c'est-à-dire P et P' n'ont pas de racine commune. □

Définition. Les racines du polynôme minimal sont appelées les conjugués du nombre algébrique.

Définition : Soit z un nombre algébrique de degré n. Soient $z_1, \dots, z_n$ ses conjugués. Le dénominateur de z est le plus petit entier $d \geq 1$ tel que dz soit un entier

algébrique. On le note $\deg(z)$. On appelle taille de z le nombre réel

$$t(z) = \max(\deg(z), |z_1|, \dots, |z_n|)$$

Proposition. Soit T un nombre réel. L'ensemble des nombres algébriques de degré n et taille $\leq T$ est fini.

Preuve : Soit z un nombre algébrique de degré n. Soient $d = \deg(z)$ et $z_1, \dots, z_n$ ses conjugués. Alors $|d| \leq T$, $|z_i| \leq T$ pour $i = 1, \dots, n$. Le polynôme minimal de dz est égal à

$$P(X) = \prod_{i=1}^{n} (X - dz_i) = X^n + a_1 X^{n-1} + \dots + a_n \in \mathbb{Z}[X]$$

car dz entier algébrique

Pour tout $k = 1, \dots, n$

$$(-1)^k a_k = \sum_{i_1 < \dots < i_k} dz_{i_1} \cdots dz_{i_k}$$

d'où $|a_k| \leq \sum_{i_1 < \dots < i_k} |dz_{i_1}| \cdots |dz_{i_k}| \leq \binom{n}{k} T^{2k}$,

donc les coefficients de $P \in \mathbb{Z}[X]$ sont bornés indépendamment de z. Il y a donc un nombre fini de possibilités pour P, donc pour dz, donc pour z. □

② Nombres algébriques de degré 2

Proposition : Soit z un nombre algébrique de degré 2. Il existe un unique entier sans facteur carré d et des uniques nombres rationnels $a, b \in \mathbb{Q}$ tels que

$$z = a + b\sqrt{d}$$

où $\sqrt{d}$ désigne la racine réelle positive si $d > 0$ et $i\sqrt{-d}$ si $d < 0$.

Démonstration : Le polynôme minimal de z est de la forme $X^2 + \alpha X + \beta$ avec $\alpha, \beta \in \mathbb{Q}$.

On a alors

$$\left(z + \frac{1}{2}\alpha\right)^2 = \underbrace{-\beta + \frac{\alpha^2}{4}}_{D \in \mathbb{Q} \text{ non nul car } z \notin \mathbb{Q}}$$

Écrivons $D = \pm \prod p_i^{n_i}$ et posons $d = \pm \prod p_i^{m_i}$ où $m_i = 1$ si n_i est impair et $m_i = 0$ sinon.

Alors d est sans facteur carré

$$\frac{D}{d} = \prod p_i^{\overbrace{n_i - m_i}^{\text{pair}}} \text{ est un carré}$$

On a donc $D = d r^2$ avec $r \in \mathbb{Q}$. Comme

$$\left(z + \frac{1}{2}\alpha\right)^2 = D = d r^2 = (\sqrt{d}\, r)^2$$

on trouve $z = \underbrace{-\frac{1}{2}\alpha}_{\in \mathbb{Q}} \pm \underbrace{r}_{\in \mathbb{Q}}\sqrt{d}$. Comme d est

sans facteur carré, $\sqrt{d}$ est irrationnel et les éléments $1, \sqrt{d} \in \mathbb{C}$ sont $\mathbb{Q}$-linéairement indépendants.

Démontrons l'unicité de d. Posons

$$\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$$

et supposons $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{d'})$ pour un autre entier d' sans facteur carré. Alors :

$$\sqrt{d'} = a + b\sqrt{d}$$
$$d' = a^2 + b^2 d + 2ab\sqrt{d}$$

d'où $2ab = 0$ et $d' = a^2 + b^2 d$. Mais $\sqrt{d'} \notin \mathbb{Q}$, donc $b \neq 0$. On trouve alors $a = 0$ et $d' = b^2 d$. Comme d' est sans facteur carré, $b^2 = 1$ et $d' = d$. □

Proposition : Soit d un entier non nul sans facteur carré. Un élément $z = a + b\sqrt{d}$ de $\mathbb{Q}(\sqrt{d})$ est un entier algébrique si et seulement si

* $a, b \in \mathbb{Z}$ si $d \not\equiv 1 \bmod 4$
* $2a, 2b \in \mathbb{Z}$ et $a - b \in \mathbb{Z}$ si $d \equiv 1 \bmod 4$

D'abord un petit lemme :

Lemme : Si x est un nbre rationnel tel que $dx^2 \in \mathbb{Z}$, alors x est un entier.

Preuve : Soit $n = dx^2$ et $x = \frac{p}{q}$ avec p, q premiers entre eux. Alors $p^2 d = q^2 n$, donc $q^2 \mid p^2 d$ et donc d car p, q sont premiers entre eux. Comme d est sans facteur carré, $q^2 = 1$ et $x \in \mathbb{Z}$. □

Preuve de la proposition : le polynôme minimal de $z = a + b\sqrt{d}$ est $X^2 - 2aX + a^2 - db^2$. Cet élément est un entier algébrique $\Leftrightarrow \begin{cases} 2a \in \mathbb{Z} \\ a^2 - db^2 \in \mathbb{Z} \end{cases}$.

La condition $2a \in \mathbb{Z}$ donne $a \in \mathbb{Z}$ ou $a + \frac{1}{2} \in \mathbb{Z}$.

* Si $a \in \mathbb{Z}$, alors $a^2 - db^2 \in \mathbb{Z}$ entraîne $db^2 \in \mathbb{Z}$, donc $b \in \mathbb{Z}$ d'après le lemme.
* Si $a + \frac{1}{2} \in \mathbb{Z}$, posons $n = a^2 - db^2$. Alors

$$\underbrace{4n}_{\in \mathbb{Z}} = \underbrace{(2a)^2}_{\in \mathbb{Z}} - d(2b)^2$$

montre que $d(2b)^2$ est un entier, donc $2b \in \mathbb{Z}$. Posons $A = 2a$ et $B = 2b$. Comme $a \notin \mathbb{Z}$, A est impair et $dB^2 = 4n - A^2$ est impair aussi ; donc d et B sont impairs. On trouve :

$$\frac{A-1}{2} + \frac{B-1}{2}\sqrt{d}$$

est un entier algébrique, et donc

$$z - \left(\frac{A-1}{2} + \frac{B-1}{2}\sqrt{d} \right) = \frac{1+\sqrt{d}}{2}$$

est un entier algébrique. Son polynôme minimal est

$$X^2 - X + \frac{1-d}{4}$$

d'où $d \equiv 1 \bmod 4$.

∴ Si $d \not\equiv 1 \bmod 4$, les entiers algébriques sont $a + b\sqrt{d}$ avec $a, b \in \mathbb{Z}$

Dans le cas $d \equiv 1 \bmod 4$, les entiers algébriques sont de la forme $a + b\sqrt{d}$ $a, b \in \mathbb{Z}$

$$\frac{A}{2} + \frac{B}{2}\sqrt{d} \quad A, B \in \mathbb{Z} \text{ impairs}$$

Posant $a = \frac{A}{2}$, $b = \frac{B}{2}$, on a $2a, 2b \in \mathbb{Z}$

et $a - b = \frac{A-B}{2} \in \mathbb{Z}$ □

Remarque : Soit $K = \mathbb{Q}(\sqrt{d})$ et $\mathcal{O}_K = K \cap \overline{\mathbb{Z}}$.

On peut réécrire la proposition sous la forme

$$\mathcal{O}_K = \begin{cases} \mathbb{Z} \oplus \mathbb{Z}[\sqrt{d}] & \text{si } d \not\equiv 1 \bmod 4 \\ \mathbb{Z} \oplus \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] & \text{si } d \equiv 1 \bmod 4 \end{cases}$$

(En effet, si $d \equiv 1 \bmod 4$, $\frac{1+\sqrt{d}}{2} \in \mathcal{O}_K$ et on peut écrire $z = a + b\sqrt{d} = (a-b) + 2b\,\frac{1+\sqrt{d}}{2}$, with $a-b \in \mathbb{Z}$ and $2b \in \mathbb{Z}$)

On voit en particulier que $\mathcal{O}_K$ est libre de rang 2.

↑ le groupe additif