

③ Corps de nombres

Un sous-corps $K \subset \mathbb{C}$ contient le corps $\mathbb{Q}$ des nombres rationnels et devient ainsi un $\mathbb{Q}$ -espace vectoriel. On note $[K:\mathbb{Q}]$ sa dimension.

Définition. Un corps de nombres est un sous-corps $K \subset \mathbb{C}$ de dimension finie sur $\mathbb{Q}$. On appelle $[K:\mathbb{Q}]$ le degré de K .

Si $K \subset \mathbb{C}$ est un corps de nombres, alors K est contenu dans $\bar{\mathbb{Q}}$. En effet, soit $z \in K$.

Comme $[K:\mathbb{Q}] = d < +\infty$, les éléments

$$1, z, z^2, \dots, z^d$$

ne sont pas linéaires, donc il existe $P \in \mathbb{Q}[X]$ tel que $P(z) = 0$. De plus, tout élément de K est de degré $\leq d$.

Exemple : $\mathbb{Q}(\sqrt{d})$ pour d entier sans facteur carré. Montrons que c'est un corps:

$$\frac{1}{a+b\sqrt{d}} = \frac{a}{a^2-b^2d} - \frac{b}{a^2-b^2d} \sqrt{d} \in \mathbb{Q}(\sqrt{d})$$

et $a^2-b^2d \neq 0$ si $(a,b) \neq (0,0)$ car

$$a^2 = b^2d \Rightarrow d = \left(\frac{a}{b}\right)^2 \text{ est un carré.}$$

Plus généralement, soit $\alpha \in \overline{\mathbb{Q}}$ un nombre algébrique de degré d et polynôme minimal P .
 le sous-anneau $\mathbb{Q}[\alpha] \subset \mathbb{C}$ engendré par α ,

$$\mathbb{Q}[\alpha] = \{Q(\alpha) \mid Q \in \mathbb{Q}[X]\}$$

est un corps, le plus petit sous-corps de $\mathbb{C}$ contenant α . On le note $\mathbb{Q}(\alpha)$. En effet, soit $Z \in \mathbb{Q}[\alpha]$ un élément non nul, écrit avec $Q(\alpha)$ avec $Q \in \mathbb{Q}[X]$ un multiple de P . Comme P est irréductible et $P \nmid Q$, P et Q sont premiers entre eux, donc par l'identité de Bézout il existe $U, V \in \mathbb{Q}[X]$ tels que

$$1 = UQ + VP \Rightarrow 1 = U(\alpha)Q(\alpha)$$

et l'élément $U(\alpha) \in \mathbb{Q}[\alpha]$ est alors un inverse de $Q(\alpha)$. Par division euclidienne, on voit aussi que $\mathbb{Q}(\alpha)$ est le $\mathbb{Q}$ -espace vectoriel engendré par $1, \alpha, \alpha^2, \dots, \alpha^{d-1}$. Le morphisme injectif

$$\mathbb{Q}[X] / (P) \longrightarrow \mathbb{C}$$

$$X \longmapsto \alpha$$

a image $\mathbb{Q}(\alpha)$. La source est un corps, à nouveau par l'identité de Bézout.

Proposition: Soit K un corps de nombres de degré d . Alors $\text{Hom}(K, \mathbb{C})$ a cardinal d .

↑
l'ensemble des morphismes de corps

Plus généralement, si $L \subset K$ sont des corps de nombres et $\varphi: L \rightarrow \mathbb{C}$ un morphisme de corps, le sous-ensemble

$$\{\psi: K \rightarrow \mathbb{C} \mid \psi|_L = \varphi\} \subset \text{Hom}(K, \mathbb{C})$$

est de cardinal $[K:L]$.

Démonstration: Comme $\text{Hom}(\mathbb{Q}, \mathbb{C})$ est réduit à l'identité, la première assertion découle aussitôt de la seconde.

Par récurrence sur $[K:L] = n$.

* Évidente pour $[K:L] = 1$.

* Supposons-la connue pour les extensions de corps de degré $< n$.

Soit $\alpha \in K \setminus L$. On note

$$L \subset L(\alpha) \subset K$$

le plus petit sous-corps de K contenant L et α . Si $\psi: K \rightarrow \mathbb{C}$ satisfait à $\psi|_L = \varphi$, alors $\psi|_{L(\alpha)}: L(\alpha) \rightarrow \mathbb{C}$ aussi. On conclut par récurrence les morphismes de corps.

Soit P le polynôme minimal de α sur L , de sorte que $L(\alpha) \cong L[X]/(P)$. Une injection de corps $L(\alpha) \rightarrow \mathbb{C}$ se restreignant à L est induit par une injection

$$L[X] \longrightarrow \mathbb{C}$$

$$a_0 + a_1 X + \dots \longmapsto \varphi(a_0) + \varphi(a_1)z + \dots$$

et pour qu'il passe au quotient il faut que soit vraie de $\varphi(P) = \varphi(a_0) + \varphi(a_1)X + \dots$

P irréductible dans $L[X]$

$\Rightarrow \varphi(P)$ irréductible dans $\varphi(L)[X]$

et donc $\varphi(P)$ a exactement $\deg P$ racines dans $\mathbb{C}$.

Il s'ensuit que

$$\{ \psi' \in \text{Hom}(L(\alpha), \mathbb{C}) \mid \psi'|_{L(\alpha)} = \varphi \}$$

est de cardinal $\deg P$.

On applique alors l'hypothèse de récurrence à l'extension $L(\alpha) \subset K$ pour dire que, pour chaque $\psi' : L(\alpha) \rightarrow \mathbb{C}$, il reste $[K : L(\alpha)]$ injections, donc au total

$$[K : L(\alpha)] \cdot \deg P = [K : L]$$

$$[L(\alpha) : L]$$

□

Définition: Soit K un corps de nombres de

degré d . On appelle plongement de K dans $\mathbb{C}$ les morphismes de corps $\varphi: K \rightarrow \mathbb{C}$.

* Si $\text{Im } \varphi \subset \mathbb{R}$, plongement réel

* Si $\text{Im } \varphi \not\subset \mathbb{R}$, plongement complexe

Si $\varphi: K \rightarrow \mathbb{C}$ est un plongement complexe, alors
 $\overline{\varphi}: K \rightarrow \mathbb{C}$ est un plongement complexe distinct,
 $z \mapsto \overline{\varphi(z)}$

son conjugué complexe.

On note r_1 le nombre de plongements réels
 et $2r_2$ le nombre de plongements complexes.

On a donc:

$$d = r_1 + 2r_2$$

Exemple: Soit $K = \mathbb{Q}(\sqrt{d})$ un corps de
 nombres de degré 2 (quadratique). Les
 plongements de K dans $\mathbb{C}$ sont

$$a + b\sqrt{d} \mapsto a + b\sqrt{d}$$

$$a + b\sqrt{d} \mapsto a - b\sqrt{d}$$

Si $d > 0$, on a $r_1 = 2$ et $r_2 = 0$

(corps quadratique réel)

Si $d < 0$, on a $r_1 = 0$ et $r_2 = 1$

(corps quadratique imaginaire)

Exemple: Soit $K = \mathbb{Q}(\sqrt[3]{2})$. Le polynôme minimal de $\sqrt[3]{2}$ est $X^3 - 2$, donc les racines sont

$$\sqrt[3]{2}, \sqrt[3]{2} e^{\frac{2\pi i}{3}}, \sqrt[3]{2} e^{\frac{4\pi i}{3}}$$

le corps a une racine réelle et deux racines complexes conjuguées.

Proposition: Soit K un corps de racines de degré n , avec $\text{Hom}(K, \mathbb{C}) = \{\varphi_1, \dots, \varphi_n\}$. Soit $\alpha \in K$ de degré d et polynôme minimal $P \in \mathbb{Q}[X]$.

$$\text{Alors } P(X)^{n/d} = \prod_{i=1}^n (X - \varphi_i(\alpha)).$$

Démonstration: Dans la suite $(\varphi_i(\alpha))_{1 \leq i \leq n}$, chaque racine du polynôme P apparaît exactement n/d fois. En effet, φ a

chaque racine β de φ fournit le plongement $\mathbb{Q}(\alpha) \rightarrow \mathbb{C}$ qui se prolonge en n/d plongements

$\alpha \mapsto \beta$
de K dans $\mathbb{C}$. On a donc:

$$\prod_{i=1}^n (X - \varphi_i(\alpha)) = \prod_{j=1}^d (X - \beta_j)^{n/d} = P(X)^{n/d}$$

□

Corollaire: Si $\varphi_i(\alpha) \neq \varphi_1(\alpha)$ pour tout $i = 2, \dots, n$, alors $K = \mathbb{Q}(\alpha)$.

Démonstration. L'ensemble des $i \in \{1, \dots, n\}$ tels que $\varphi_i(\alpha) = \varphi_1(\alpha)$ est de cardinal n/d où d est le degré de α . Par hypothèse, $n/d = 1$, donc $n = d$ et $K = \mathbb{Q}(\alpha)$ $\square$

Corollaire (Théorème de l'élément primitif)

Soit K un corps de nombres. Il existe un élément $\alpha \in K$ tel que $K = \mathbb{Q}(\alpha)$.
 $\nwarrow$ élément primitif

Démonstration: Il suffit de démontrer qu'il

existe $\alpha \in K$ tel que $\varphi_i(\alpha) \neq \varphi_1(\alpha)$ pour tout $i = 2, \dots, n$. Notons

$$V_i = \{ \alpha \in K \mid \varphi_i(\alpha) = \varphi_1(\alpha) \} \subset K;$$

c'est un sous-espace vectoriel strict car $\varphi_i \neq \varphi_1$. on se doit alors vouloir à démontrer que $V_2 \cup \dots \cup V_n$ n'est pas K tout entier.

Lemme: Soit F un corps infini, soit V un F -espace vectoriel, et soit $V_1, \dots, V_n$ des sous-espaces vectoriels de V distincts de V . Alors $V_1 \cup \dots \cup V_n$ est distinct de V .

Preuve: Par récurrence sur n . le cas $n = 1$ est évident. Supposons $V_2 \cup \dots \cup V_n \neq V$.

Il existe $w \in V$ tel que $w \notin V_i$ pour $i=2, \dots, n$.
 Supposons $w \in V_1$ et soit $v \in V \setminus V_1$.

Fixons $j \in \{1, \dots, n\}$. Soient t, t' des éléments distincts de F tels que $v + tw \in V_j$
 $v + t'w \in V_j$

Alors $\underbrace{(t-t')}_{\neq 0} w \in V_j$, donc $w \in V_j \Rightarrow j=1$.

Mais alors $v = (v + tw) - tw \in V_1$, absurde.

Conclusion: il existe au plus un seul $t \in F$ tel que $v + tw \in V_j$, donc au plus n éléments $t \in F$ tels que $v + tw \in V_1 \cup \dots \cup V_n$. Comme F est infini, il existe $t \in F$ tel que $v + tw$ n'est pas dans $V_1 \cup \dots \cup V_n$. $\square$

④ Noms, traces, discriminants

Définition. Soit K un corps de nombres.
 on appelle trace et norme d'un élément w de K la trace et le déterminant de l'endomorphisme $\mathbb{Q}$ -linéaire $K \xrightarrow{\mu_w} K$. on a
 $z \mapsto wz$

on note $\text{Tr}_K(w) \in \mathbb{Q}$.
 $N_K(w)$

Comme $\mu_{w+w'} = \mu_w + \mu_{w'}$, $\mu_{ww'} = \mu_w \circ \mu_{w'}$,

$\mu_{aw} = a \mu_w$ pour $a \in \mathbb{Q}$, on a:

$$\text{Tr}_K(w + w') = \text{Tr}_K(w) + \text{Tr}_K(w')$$

$$N_K(ww') = N_K(w) N_K(w')$$

$$\text{Tr}_K(aw) = a \text{Tr}_K(w)$$

$$N_K(aw) = a^n N_K(w)$$

Proposition: Soit K un corps de nombres, avec $\text{Hom}(K, \mathbb{C}) = \{\varphi_1, \dots, \varphi_n\}$. Soit $w \in K$.
L'endomorphisme μ_w est diagonalisable de valeurs propres $\varphi_1(w), \dots, \varphi_n(w)$.

Démonstration: Soit α un élément primitif, c'est-à-dire $K = \mathbb{Q}(\alpha)$. Le polynôme minimal de l'endomorphisme μ_α est $\prod_{i=1}^n (X - \varphi_i(\alpha))$ et comme ses racines sont simples, μ_α est diagonalisable à valeurs propres $\varphi_1(\alpha), \dots, \varphi_n(\alpha)$.

Soit $w \in K$ quelconque. Alors il existe $P \in \mathbb{Q}[X]$ tel que $w = P(\alpha)$, et la matrice de μ_w dans la base fixée est $P(A)$ avec A la matrice de μ_α . Le changement de base qui diagonalise A transforme $P(A)$ en la matrice diagonale des coefficients $P(\varphi_i(\alpha)) = \varphi_i(P(\alpha)) = \varphi_i(w)$ □

Corollaire:

$$\text{Tr}_K(w) = \sum_{i=1}^n \varphi_i(w)$$

$$N_K(w) = \prod_{i=1}^n \varphi_i(w)$$

Corollaire: Si $w \in K$ est un entier algébrique, alors $\text{Tr}_K(w)$ et $N_K(w)$ sont des entiers.

Démonstration: Notons $P = X^d + a_1 X^{d-1} + \dots + a_d$ le polynôme minimal de w . Comme w est un entier algébrique, $P \in \mathbb{Z}[X]$. On a:

$$P(X)^{n/d} = \prod_{i=1}^n (X - \varphi_i(w)),$$

$$\text{d'où } \text{Tr}_K(w) = -\frac{n}{d} a_1 \in \mathbb{Z} \text{ car } d|n$$

$$N_K(w) = a_d^{n/d}$$

□

Définition. Soit K un corps de nombres de degré n . Soit $\beta = (z_1, \dots, z_n)$ une $\mathbb{Q}$ -base de K . On définit le discriminant de β comme

$$\text{disc}(\beta) = \det \left(\varphi_i(z_j) \right)_{1 \leq i, j \leq n}^2$$

(c'est indépendant de l'ordre des vecteurs $z_1, \dots, z_n$ de la base)

Exemple: Soit $\alpha \in K$ un élément primitif, et
 soit $\beta = \{1, \alpha, \dots, \alpha^{n-1}\}$. Alors:

$$\text{disc}(\beta) = \det \begin{pmatrix} \varphi_1(1) & \varphi_2(1) & \dots & \varphi_n(1) \\ \varphi_1(\alpha) & \varphi_2(\alpha) & \dots & \varphi_n(\alpha) \\ \vdots & \vdots & \ddots & \vdots \\ \varphi_1(\alpha)^{n-1} & \varphi_2(\alpha)^{n-1} & \dots & \varphi_n(\alpha)^{n-1} \end{pmatrix}^2$$

est le carré du déterminant de Vandermonde de
 $\varphi_1(\alpha), \dots, \varphi_n(\alpha)$, qui sont distincts. On a:

$$\text{disc}(\beta) = \prod_{i < j} (\varphi_j(\alpha) - \varphi_i(\alpha))^2$$

