

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 $v + tw$ et $v + t'w \in V_j$.

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 Normes, 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 prop $\varphi_1(w), \dots, \varphi_n(w)$.

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 prop $\varphi_1(\alpha), \dots, \varphi_n(\alpha)$.

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 une 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 de 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:

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

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

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

Proposition: Soit K un corps de nombres de deg n .

Soient $z_1, \dots, z_n \in K$ et $D = (T_{K/\mathbb{Q}}(z_i z_j))_{1 \leq i, j \leq n}$.
 Alors $\det(D) = \det(\varphi_i(z_j))^2$. En particulier,
 le discriminant d'une bse de K est non nul.

Démonstration: Soient $\varphi_1, \dots, \varphi_n$ les plongements de
 K dans $\mathbb{C}$. On a:

$$T_{K/\mathbb{Q}}(z_i z_j) = \sum_{k=1}^n \varphi_k(z_i z_j) = \sum_{k=1}^n \varphi_k(z_i) \varphi_k(z_j)$$

Si A désigne la matrice $(\varphi_i(z_j))$, on a

$$D = {}^t A \cdot A = (\varphi_j(z_i)) \cdot (\varphi_i(z_j))$$

donc $\det(D) = \det(A)^2$.

Supposons par l'absurde que $(z_1, \dots, z_n)$ est une base de K de discriminant Δ . La matrice $(\varphi_i(z_j))$ n'est pas inversible, d'où une relation $\sum_{i=1}^n c_i \varphi_i(z_j) = 0$, pour tout $1 \leq j \leq n$. L'application $\sum_{i=1}^n c_i \varphi_i : K \rightarrow \mathbb{C}$ est alors identiquement nulle, ce qui n'est pas possible car $\varphi_1, \dots, \varphi_n$ sont $\mathbb{C}$ -linéairement indépendants. (exercice). $\square$

Corollaire: Soit K un corps de nombres de degré n . Si β et β' sont des bases de K , alors

$$\text{disc}(\beta') = \det_{\beta}(\beta')^2 \text{disc}(\beta).$$

Démonstration: Prenons $\beta = (z_1, \dots, z_n)$ et $\beta' = (z'_1, \dots, z'_n)$

soit P la matrice de passage de β à β' telle que $z'_j = \sum_{k=1}^n P_{kj} z_k$ pour tout $j \in \{1, \dots, n\}$.

Soient $A = (\varphi_i(z_j))$ et $A' = (\varphi_i(z'_j))$. Alors

$$\varphi_i(z'_j) = \sum_{k=1}^n P_{kj} \varphi_i(z_k),$$

d'où $A' = PA$, donc $\text{disc}(\beta') = (\det A')^2$

$$= (\det P)^2 \det(A)^2 = \det_P (\beta^1)^2 \operatorname{disc}(\beta) \quad \square$$

En posant une base de la forme $1, \alpha, \dots, \alpha^{n-1}$
 (théorème de l'élément primitif)