Corps de nombres.

Rappel. Corps de nombres = extension finie de $\mathbb{Q}$.

$$k \; | \; \mathbb{Q} \qquad [k:\mathbb{Q}].$$

Exemples

1) $\mathbb{Q}$.

2) $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt[3]{2})$. Corps de rupture

X^2+1 $\quad X^2-2$ $\quad X^3-2$

3) Corps de décomposition

$f \in \mathbb{Q}[X]$ on décompose f dans $\mathbb{C}[X]$, $\alpha_1, -, \alpha_m$ racines

$k = \mathbb{Q}(\alpha_1, -, \alpha_m)$.

Entiers.

$$\begin{array}{ccc} \mathbb{Q} & \subset & k \\ \cup & & \cup \\ \mathbb{Z} & \subset & \mathbb{Z}_k \end{array}$$

anneau des entiers de k.

Exemples.

$k = \mathbb{Q}$ $\qquad \mathbb{Z}_{\mathbb{Q}} = \mathbb{Z}$

$k = \mathbb{Q}(i)$ $\qquad \mathbb{Z}_k = \mathbb{Z}[i]$

$k = \mathbb{Q}(\sqrt{2})$ $\qquad \mathbb{Z}_k = \mathbb{Z}[\sqrt{2}]$.

Exemple.

$\zeta = e^{2i\pi/n}$.

$k = \mathbb{Q}(\zeta)$

$\mathbb{Z}_k = \mathbb{Z}[\zeta]$.

On a aussi $\mathbb{Q}(i) = \mathbb{Q}(i/2) = \mathbb{Q}(2i)$

mais $\mathbb{Z}[2i] \subsetneq \mathbb{Z}[i] \subsetneq \mathbb{Z}[\frac{i}{2}]$

$k = \mathbb{Q}(\sqrt{5})$ $\qquad \mathbb{Z}_k = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right] = \mathbb{Z}[\phi]$

ϕ nombre d'or

$k = \mathbb{Q}(\phi)$.

Endomorphismes, norme, trace, polynôme caractéristique.

A anneau commutatif unitaire intègre

K corps des fractions.

(Exemples $A = \mathbb{Z}$ $\quad K = \mathbb{Q}$

F corps $\quad A = F[T]$ $\quad K = F(T)$)

M un A-module libre de type fini

$\exists$ base $e_1, -, e_n$. $\qquad e_j \in M$

$x \in M$ $\quad x = a_1 e_1 + - + a_n e_n$ $\quad a_j \in A$.

A-module de type fini : M

$\exists\, x_1, \ldots, x_m \in M$. engendrent M comme A-module.

tout elt de M s'écrit $a_1x_1 + \ldots + a_mx_m$, $a_i \in A$.

(pas unicité).

A-module libre : il existe $(e_i)_{i\in I}$ $e_i \in M$ tel que pour tout $x \in M$ il existe $(a_i)_{i\in I}$, $a_i \in A$, support $\{i \in I, a_i \neq 0\}$ fini, $x = \sum_{i\in I} a_i e_i$.

Libre de type fini $\quad M = A \quad$ base $\{1\}$

$A = \mathbb{Z}$

$M = \mathbb{Z}[i]$

$M = \mathbb{Z}[\sqrt{2}]$

$M = \mathbb{Z}[\phi] \qquad \phi = \frac{1+\sqrt{5}}{2}$

$M = \mathbb{Z}[\sqrt{5}]$

$M = \mathbb{Z}[\zeta] \qquad \zeta = e^{2i\pi/n}$.

De type fini pas libre.

$M = \mathbb{Z}\left[\frac{1}{2}\right] \subset \mathbb{Q}$.

$\left\{ a_0 + \frac{a_1}{2} + \ldots + \frac{a_n}{2^n},\ n \geq 1,\ a_i \in \mathbb{Z} \right\}$

Libre pas de type fini

A anneau $\qquad A^{(\mathbb{N})}$

$\mathbb{N} = \{0, 1, 2, \ldots\}$

$M = A^{(\mathbb{N})} = \left\{ (a_n)_{n\geq 0},\ a_n \in A,\ \text{support fini} \right\}$

$\mathbb{N} \longrightarrow A$
$n \longmapsto a_n$. $\quad \{n \in \mathbb{N}, a_n \neq 0\}$ fini

$m \geq 0 \quad e_m = (\delta_{nm})_{n\geq 0} \qquad \delta_{nm} = \begin{cases} 1 & n = m \\ 0 & n \neq m \end{cases}$

ni libre ni de type fini

$A = \mathbb{Z} \qquad M = \mathbb{Q}$.

A anneau

M un A-module libre de type fini

K corps des fractions $\qquad e_1, \ldots, e_n$ base de M comme A-module

$V = Ke_1 + \ldots + Ke_n \qquad K$-espace vectoriel de dimension n.

$\cup$

$M = Ae_1 + \ldots + Ae_n$

u endomorphisme du A-module M

$\longleftrightarrow$ $\mathrm{Mat}_e(u) = (a_{ij}) \in \mathrm{Mat}_{n\times n}(A)$.

u s'étend en un endomorphisme du K-e-v. V

Polynôme caractéristique.

$$\det\left(I_n X - \mathrm{Mat}_e(u)\right) \in A[X]$$

Norme polynôme unitaire de degré n.

Trace $N(u) = \det\left(\mathrm{Mat}_e u\right) = \det(a_{ij})$

$$\mathrm{Tr}(u) = -\operatorname{coeff} X^{n-1} = \sum_{i=1}^n a_{ii}$$

$$P_u(X) = X^n - \mathrm{Tr}(u) X^{n-1} + \dots + (-1)^n N(u)$$

polynôme caractéristique.

$$\mathrm{Tr}(u_1+u_2) = \mathrm{Tr}(u_1) + \mathrm{Tr}(u_2)$$

$$N(u_1 \circ u_2) = N(u_1)\, N(u_2)$$

Supposons de plus M est un anneau.

Exemples $A = \mathbb{Z}$ $M = \mathbb{Z}, \mathbb{Z}[i], \mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[\zeta], \mathbb{Z}[\phi]$

$A = F[T]$ $K = F(T)$

$M = A[\sqrt{T}]$ $V = K[\sqrt{T}]$ $e_1 = 1$, $e_2 = \sqrt{T}$.

On note $B = M$ cet anneau

$B \supset A$ A, B deux anneaux

B libre de type fini comme A-module.

$$x \in B \qquad \begin{array}{ccc} B & \xrightarrow{[x]} & B \\ \Psi & & \Psi \\ y & \longmapsto & xy \end{array}$$ endomorph. de A-modules

$N_{B/A}(x)$ norme de cet endomorphisme $\in A$

$\mathrm{Tr}_{B/A}(x)$ trace $\in A$

$P_{B/A}(x\,;X) \in A[X]$ polynôme caract. de $[x]$.

$B \ni x_1, x_2$

$$[x_1] : \begin{array}{ccc} B & \longrightarrow & B \\ \Psi & & \Psi \\ y & & x_1 y \end{array}$$

$$[x_1] + [x_2] = [x_1 + x_2]$$

$$[x_2] : \begin{array}{ccc} B & \longrightarrow & B \\ z & \longmapsto & x_2 z \end{array}$$

$$[x_1] \circ [x_2] = [x_1 x_2]$$

$$N_{B/A}(x_1)\, N_{B/A}(x_2) = N_{B/A}(x_1 x_2).$$

$$\mathrm{Tr}_{B/A}(x_1) + \mathrm{Tr}_{B/A}(x_2) = \mathrm{Tr}_{B/A}(x_1 + x_2)$$

$\mathrm{Tr}_{B/A} : B \longrightarrow A$ homomorphisme du groupe additif B dans A.

$N_{B/A}$: hom. de $B^\times$ dans $A^\times$.

$A = K$ corps.

$M = B = V = L$ extension finie de K

$N_{L|K} : L^\times \longrightarrow K^\times$ $\qquad N_{L|K}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$

$Tr_{L|K} : L \longrightarrow K.$ $\qquad Tr_{L|K}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha)$

Lemme K corps, L/K extension séparable $[L:K] = n$. N extension finie normale sur K de L

$\sigma_1, \ldots, \sigma_n$ les K-homomorphismes de L dans N; $\alpha \in L$.

$$\begin{array}{c} N \\ | \\ L \\ {\scriptstyle n}\,|\,{\scriptstyle \text{Sép}} \\ K \end{array} \quad \text{Normale}$$

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

Corollaires.

$$N_{L|K}(\alpha) = (-1)^n P_{L|K}(\alpha ; 0) = \prod_{i=1}^{n} \sigma_i(\alpha)$$

$$Tr_{L|K}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha)$$

Démonstration

1er cas Supposé $L = K(\alpha)$

Une base de L sur K est $\{1, \alpha, \ldots, \alpha^{n-1}\}$

$$[\alpha] : \begin{array}{ccc} K(\alpha) & \longrightarrow & K(\alpha) \\ \Psi & & \Psi \\ x & \longmapsto & \alpha x \end{array}$$

base : $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$

$e_1 = 1 \quad e_2 = \alpha$

$[\alpha] e_1 = \alpha$

$e_{n-1} = \alpha^{n-2}$.

$[K(\alpha) : K] = n$

$Irr_K(\alpha ; X) = X^n + a_{n-1} X^{n-1} + \ldots + a_0 \in K[X]$

$\alpha^n = - a_{n-1} \alpha^{n-1} - \ldots - a_0$.

$$\begin{array}{cccc} [\alpha]e_1 & [\alpha]e_2 & [\alpha]e_{n-1} & [\alpha]e_n \end{array}$$

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & & & -a_1 \\ 0 & 1 & & & \vdots \\ \vdots & \vdots & & 0 & \vdots \\ 0 & 0 & & 1 & -a_{n-1} \end{pmatrix}$$

$$\det \begin{pmatrix} X & 0 & 0 & & 0 & a_0 \\ -1 & X & 0 & & 0 & a_1 \\ 0 & -1 & X & & \vdots & \vdots \\ \vdots & \vdots & & & X & a_{n-2} \\ 0 & 0 & & & -1 & X + a_{n-1} \end{pmatrix}$$

$= X^n + a_{n-1} X^{n-1} + \ldots + a_0.$

$= Irr_K(\alpha ; X)$

$$\begin{array}{c} L = K(\alpha) \\ | \\ K. \end{array}$$

2e cas.

$$n \left(\begin{array}{c} L \\ | \; {\scriptstyle m} \\ K(\alpha) \\ | \; {\scriptstyle d} \\ K \end{array} \right. \qquad n = dm$$

Base de L sur K.

$1, \alpha, \dots, \alpha^{d-1}$ est une base de $K(\alpha)/K$

$e_1, \dots, e_m$ une base de L sur $K(\alpha)$

une base de L sur K est

$\{ e_i \alpha^{j-1}, \ 1 \leq i \leq m, \ 1 \leq j \leq d \}$

$\{ e_1, e_1\alpha, \dots, e_1\alpha^{d-1} ; e_2, e_2\alpha, \dots, e_2\alpha^{d-1}, \dots, e_m, e_m\alpha, \dots, e_m\alpha^{d-1} \}$

$[\alpha]$ = matrice par blocs = $\begin{pmatrix} M & 0 & \cdots & 0 \\ 0 & M & \cdots & 0 \\ \vdots & & \ddots & \\ \vdots & & & M \end{pmatrix}$

M = matrice de $[\alpha] : K(\alpha) \to K(\alpha)$

$$P_{L|K}(\alpha ; X) = \det \begin{pmatrix} I_d X - M & & 0 \\ & \ddots & \\ 0 & & I_d X - M \end{pmatrix}$$

$$= P_{K(\alpha)|K}(\alpha ; X)^m = \prod_{j=1}^{d} (X - \alpha_j)^m$$

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

L
$\big|\, m$
$K(\alpha)$
$\big|\, d$
K

$\alpha_1, \dots, \alpha_d$ conjugués de α sur K

$\sigma_1(\alpha), \dots, \sigma_n(\alpha)$ image de α dans N par les n K-isomorphismes de L dans N.

$n = md$.

$Tr_{L|K}(\alpha) = m \, Tr_{K(\alpha)|K} \, \alpha$

$N_{L|K}(\alpha) = N_{K(\alpha)|K}(\alpha)^m$

Exercice $\quad K = \mathbb{F}_2(T) \qquad \alpha = \sqrt{T} \in L$

$L = K(\sqrt{T}) \qquad [\alpha] : L \to L$

Calculer $P_{L|K}(\alpha ; X)$, $N_{L|K}(\alpha)$, $Tr_{L|K}(\alpha)$.

Lemme. Soit $L|K$ extension finie séparable. L'application

$$L \times L \longrightarrow K$$
$$(x, y) \longmapsto Tr_{L|K}(xy)$$

est une forme bilinéaire symétrique non dégénérée.

Démonstration.

$x \in L$

$y \longmapsto Tr_{L|K}(xy)$ $\qquad$ K-linéaire.

$L \longrightarrow K$ $\qquad$ · $Tr_{L|K}(x\lambda y) = \lambda Tr_{L|K}(xy)$, $\lambda \in K$.

forme linéaire. $\qquad$ · $Tr_{L|K}(x(y_1 + y_2)) = Tr_{L|K}(xy_1) + Tr_{L|K}(xy_2)$

$(x, y) \longmapsto Tr_{L|K}(xy)$

symétrique $\qquad xy = yx$.

non dégénéré $\qquad x \in L$ si $Tr_{L|K}(xy) = 0 \ \forall y \in L$. Alors $x = 0$.

$$\begin{array}{l} N \\ | \\ L \\ |\, n \\ K \end{array}$$

sép. normale.

$\sigma_1, \dots, \sigma_n : L \longrightarrow N$

$$Tr_{L|K}(xy) = \sum_{i=1}^{n} \sigma_i(xy) = \sum_{i=1}^{n} \sigma_i(x)\,\sigma_i(y).$$

$x \in L$

Supp. $\sum_{i=1}^{n} \sigma_i(x)\,\sigma_i(y) = 0 \quad \forall y \in L$.

On va montrer qu'une relation $\sum_{i=1}^{n} z_i\, \sigma_i(y) = 0 \ \forall y \in L$ avec des $z_i \in N$ implique $z_1 = \dots = z_n = 0$. Donc $x = 0$

Lemme de Dedekind – indépendance linéaire des caractères.

G groupe, k corps, $\sigma_1, \dots, \sigma_n$ homomorphismes 2 à 2 distincts de G dans $k^\times$. Alors $\sigma_1, \dots, \sigma_n$ son linéairement indépendants dans k^G

$G = L^\times$

$k = N$.

$k^G = \{ G \longrightarrow k \} \ni \sigma_1, \dots, \sigma_n$

k-e.v.

$z_1, \dots, z_n \in k$, $z_1\sigma_1 + \dots + z_n\sigma_n = 0 \Rightarrow z_1 = \dots = z_n = 0$.

Dém. par récurrence sur n.

$n = 1$ $\quad \sigma : G \longrightarrow k^\times$

$\lambda \in k$, $\lambda \neq 0$ $\quad \lambda\sigma : G \longrightarrow k$ n'est pas $x \longmapsto 0$

e = elt neutre de G $\quad \lambda\sigma(e) = \lambda$.

Supp. vrai pour $n-1$.

Soient $a_1, \dots, a_n \in k$ $\quad \sum_{i=1}^{n} a_i\sigma_i(x) = 0 \quad \forall x \in G$.

$y \in G$. $\quad \sum_{i=1}^{n} a_i\sigma_i(xy) = 0 \quad \forall x \in G$.

$\sigma_i(xy) = \sigma_i(x)\,\sigma_i(y)$.

$\sigma_n \neq \sigma_1$. Il existe $y \in G$, $\sigma_n(y) \neq \sigma_1(y)$.

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

$$\sum_{i=1}^{n} a_i\, \sigma_1(y)\, \sigma_i(x) = 0 \qquad \forall x \in G$$

$$\sum_{i=2}^{n} a_i\, \big(\sigma_i(y) - \sigma_1(y)\big)\, \sigma_i(x) = 0 \quad \forall x \in G.$$

relation de dépendance linéaire entre $\sigma_2, \dots, \sigma_n$ $\quad a_n\big(\sigma_n(y) - \sigma_1(y)\big) = 0 \Rightarrow a_n = 0$

$\sum_{i=1}^{n-1} a_i\sigma_i = 0 \Longrightarrow a_1 = \dots = a_{n-1} = 0$

Discriminant.

$$\begin{array}{c} B \\ \cup \\ A \end{array}$$ anneaux, B : A-module libre t.f. de rang n.

Discriminant de B/A :

$$D_{B/A} : \begin{array}{ccc} B^n & \longrightarrow & A \\ \cup & & \cup \\ (x_1, \dots, x_n) & \longmapsto & \det\left(\mathrm{Tr}_{B/A}\, x_i x_j\right)_{1 \leq i,j \leq n} \end{array}.$$

Proposition.

$$\begin{tikzcd} N \arrow[d, dash] \\ L \arrow[d, dash, "n"] \\ K \end{tikzcd}$$

norm ($N|K$), sep. ($L|K$)

$\sigma_1, \dots, \sigma_n : L \longrightarrow N$ K-isomorphismes

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

De plus, $x_1, \dots, x_n$ est une base de $L|K$ $\iff D_{L|K}(x_1, \dots, x_n) \neq 0$.