$$= \underbrace{\sum_{\sigma \in \mathfrak{S}_n} b_{\sigma(1),1} \cdots b_{\sigma(n),n} \operatorname{sgn}(\sigma)}_{= \det B} e_1 \wedge \cdots \wedge e_n$$

But : Calculer également les matrices des $\wedge^k(f) : \wedge^k(L) \to \wedge^k(L)$ pour $2 \leq k < n$ ($\rightsquigarrow$ autres coeff. du pol. car. de f).

Notations : Pour $k \geq 0$: $\mathcal{P}_k$ = {parties à k éléments de $\{1, \dots, n\}$}.

Pour $I \in \mathcal{P}_k$ d'éléments $i_1 < \cdots < i_k$: $e_I := e_{i_1} \wedge \cdots \wedge e_{i_k}$.

Pour $X \in M_{p \times q}(A)$ et $I \subseteq \{1, \dots, p\}$, $J \subseteq \{1, \dots, q\}$:

$X_{I,J}$:= matrice extraite $(x_{ij})_{(i,j) \in I \times J}$.

Lemme : Soient $X \in M_{n \times p}(A)$ et $x_j := \sum_{i=1}^{n} x_{ij} e_i \in L$, $1 \leq j \leq p$.

Alors $$x_1 \wedge \cdots \wedge x_p = \sum_{I \in \mathcal{P}_p} \det(X_{I, \{1, \dots, p\}})\, e_I$$

Dém. : $x_1 \wedge \cdots \wedge x_p$

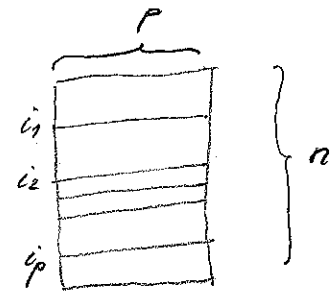
$$= \left(\sum_{i_1} x_{i_1,1} e_{i_1}\right) \wedge \cdots \wedge \left(\sum_{i_p} x_{i_p,p} e_{i_p}\right)$$

$$= \sum_{i_1, \dots, i_p} x_{i_1,1} \cdots x_{i_p,p}\, e_{i_1} \wedge \cdots \wedge e_{i_p}$$

$$= \sum_{\tau} x_{\tau(1),1} \cdots x_{\tau(p),p}\, e_{\tau(1)} \wedge \cdots \wedge e_{\tau(p)},$$

où la somme porte sur les injections $\tau : \{1, \dots, p\} \to \{1, \dots, n\}$. Or toute injection τ se factorise de façon unique en $\tau = \lambda\sigma$, où σ est une permutation de $\{1, \dots, p\}$ et λ une injection croissante.

X :



Donc :

$$x_1 \wedge \dots \wedge x_p = \sum_\lambda \sum_{\sigma \in \mathfrak{S}_p} x_{\lambda\sigma(1),1} \cdots x_{\lambda\sigma(p),p} \underbrace{e_{\lambda\sigma(1)} \wedge \dots \wedge e_{\lambda\sigma(p)}}_{= \operatorname{sgn}(\sigma)\, e_{\lambda(1)} \wedge \dots \wedge e_{\lambda(p)}}$$

$$= \sum_\lambda \det\left(X_{\{\lambda(1),\dots,\lambda(p)\},\{1,\dots,p\}} \right) \cdot e_{\lambda(1)} \wedge \dots \wedge e_{\lambda(p)} . \quad \checkmark$$

Prop. : Pour $f : L \to L$ de matrice B dans la base $e_1, \dots, e_n$, la matrice de $\wedge^k(f) : \wedge^k(L) \to \wedge^k(L)$ dans la base des e_I, $I \in \mathcal{P}_k$, est $(\det(B_{I,J}))_{I,J \in \mathcal{P}_k}$.

Dém. : $\wedge^k(f)(e_I) = f(e_{i_1}) \wedge \dots \wedge f(e_{i_k})$. $\checkmark$

Prop. : Pour $f : L \to L$ et B comme ci-dessus et $\lambda, \mu \in A$, on a

$$\det(\lambda \mathbb{1}_L + \mu f) = \sum_{k=0}^{n} \operatorname{tr}(\wedge^k(f))\, \mu^k \lambda^{n-k}$$

$$= \sum_{k=0}^{n} \Big(\sum_{I \in \mathcal{P}_k} \underbrace{\det(X_{I,I})}_{\text{mineur principal}} \Big) \mu^k \lambda^{n-k} .$$

Dém. : On a

$$\wedge^n(\lambda \mathbb{1}_L + \mu f)(e_1 \wedge \dots \wedge e_n) = (\lambda e_1 + \mu f(e_1)) \wedge \dots \wedge (\lambda e_n + \mu f(e_n))$$

$$= \sum_{k=1}^{n} \mu^k \lambda^{n-k} A_k$$

pour des $A_k \in \wedge^n(L)$ à déterminer. Pour $I \in \mathcal{P}_k$, soit $\bar{I}$ le complémentaire de I. On a

$$A_k = \sum_{I \in \mathcal{P}_k} \left(f(e_{i_1}) \wedge \dots \wedge f(e_{i_k}) \wedge e_{\bar{I}} \right) \cdot \varepsilon(I),$$

où $\varepsilon(I) \in \{1,-1\}$ est défini par

$$e_1 \wedge \dots \wedge e_n = \varepsilon(I)\, e_I \wedge e_{\bar{I}}.$$

On a

$$\sum_{I \in \mathcal{P}_k} f(e_{i_1}) \wedge \dots \wedge f(e_{i_k}) \wedge e_{\bar{I}}\, \varepsilon(I) = \sum_{I \in \mathcal{P}_k} \Lambda^k(f)(e_{i_1} \wedge \dots \wedge e_{i_k}) \wedge e_{\bar{I}} \cdot \varepsilon(I)$$

$$= \sum_{I \in \mathcal{P}_k} \left(\sum_{J \in \mathcal{P}_k} \det(B_{J,I})\, e_J \right) \wedge e_{\bar{I}} \cdot \varepsilon(I)$$

$0 \neq e_J \wedge e_{\bar{I}} \Leftrightarrow J = I$

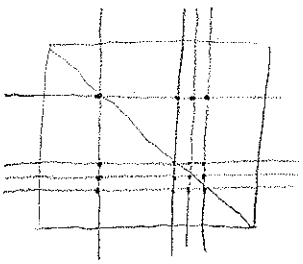
$$= \sum_{I \in \mathcal{P}_k} \det(B_{I,I})\, \underbrace{e_I \wedge e_{\bar{I}} \cdot \varepsilon(I)}_{e_1 \wedge \dots \wedge e_n}$$

$$= \operatorname{tr}(\Lambda^k(f)) \cdot e_1 \wedge \dots \wedge e_n \cdot \quad \checkmark$$

Application :

$$\chi_f(X) = \text{pol. caract. de } f = \det(X \cdot \mathbb{1} - f)$$

$$= \sum_{k=0}^{n} (-1)^k \underbrace{\operatorname{tr}(\Lambda^k(f))}_{\text{= somme des "mineurs principaux" de } B.} X^{n-k}$$



mineur principal d'ordre 4.

II. Théorie de Galois

Convention : corps = corps commutatif

1. Préliminaires

1.1 Prolongements d'isomorphismes aux corps de décomposition

Soit K un corps

Lemme 1 (rappel) : Soit $P \in K[X]$ irréductible.

a) $L = K[X]/(P)$ est un corps (le "corps de rupture" de P) et l'image x de X dans L est une racine de P.

b) Le morphisme can : $K \longrightarrow L$ est universel parmi les morphismes de K dans un corps muni d'une racine de P,

$$\begin{array}{ccc} K & \xrightarrow{\forall \varphi} & L' \ni x' \text{ racine de } P \\ {\scriptstyle can}\downarrow & \nearrow_{\exists ! \tilde{\varphi}} & \\ L \ni x & & \end{array} \quad \text{t.q. } \tilde{\varphi}(x) = x'.$$

Rque : Pour tout morph. $\varphi : K \longrightarrow L'$, on a donc une bijection

$$\{\text{prolongements } \tilde{\varphi} \text{ de } \varphi\} \xrightarrow{\sim} \{\text{racines } x' \text{ de } P \text{ dans } L'\}$$
$$\tilde{\varphi} \longmapsto \tilde{\varphi}(x)$$

Déf : Soit $P \in K[X]$. Un corps de décomposition de P est une extension $K \subset L$ telle que

a) P est scindé dans L et

b) L est engendré par les racines de P.

Rque (rappel) : Un corps de décomp. existe toujours et est unique à isomorphisme (non unique !) près.

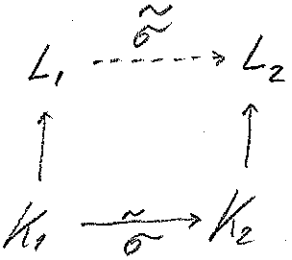
Prop. 2 : Soient $\sigma : K_1 \longrightarrow K_2$ un isom. de corps, $P_1 \in K_1[X]$, P_2 son image par σ (appliqué aux coeff. de P_1), $L_i \supset K_i$ un corps de décomposition de P_i

a) $\exists\ \tilde{\sigma} : L_1 \xrightarrow{\sim} L_2$ qui prolonge σ.

b) Soit ν le nombre de tels $\tilde{\sigma}$. Alors

$$\nu \leq [L_1 : K_1]$$

et on a l'égalité si toutes les racines de P_1 dans L_1 sont simples.



Dém. : Récurrence sur $d = [L_1 : K_1]$:

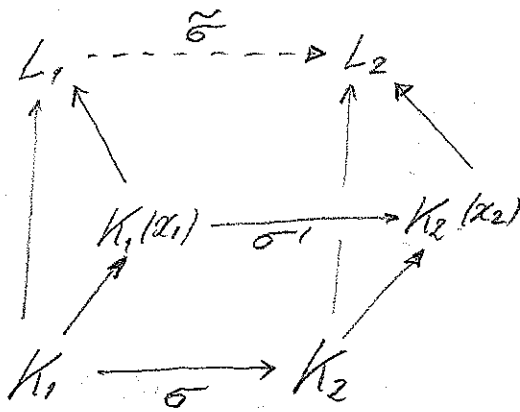
$d = 1$: $K_1 = L_1$, $K_2 = L_2$, $\nu = 1$.

$d \geq 2$: Montrons d'abord l'existence de $\tilde{\sigma}$: P_1 admet un facteur irréd. Q_1 de degré ≥ 2. Soient $x_1 \in L_1$ une racine de Q_1, $Q_2 = \sigma(Q_1)$ et x_2 une racine de Q_2 dans L_2. Par le lemme 1, σ se prolonge en un unique isom. $\sigma' : K(x_1) \longrightarrow K(x_2)$ tel que $\sigma'(x_1) = x_2$. On a $[L_1 : K(x_1)] < [L_1 : K_1]$ et L_i est un corps de décompos. de P_i sur $K(x_i)$, $i = 1, 2$. Par l'hyp. de récurrence, σ' se prolonge en $\tilde{\sigma} : L_1 \longrightarrow L_2$. OK.

Comptons maintenant les $\tilde{\sigma}$: On a

$$\#\{\text{prolongements } \sigma' : K(x_1) \to L_2\} = \#\{\text{racines de } Q_2 \text{ dans } L_2\} \leq \deg Q_2 = \deg Q_1 = [K_1(x_1) : K]$$

et on a l'égalité si les racines



de P_1 sont simples (car alors les racines de Q_1 et donc de Q_2 le sont aussi). Quand on fixe une racine x_2 et un σ' t.q. $\sigma'(x_1) = x_2$, l'hypothèse de récurrence donne

$|\{$ prolongements $\tilde{\sigma}$ de $\sigma'\}| \leq [L_1 : K_1(x_1)]$

avec égalité quand les racines de P_1 sont simples.

Donc on a

$$r \leq [K_1(x_1) : K_1] \cdot [L_1 : K_1(x_1)] = [L_1 : K_1]$$

avec égalité quand les racines de P_1 sont simples. ✓

①

Déf: Soit $K \subset L$ une extension de corps. Un K-automorphisme de L est un automorphisme $\sigma : L \xrightarrow{\sim} L$ qui fixe K :

$$\sigma(x) = x, \quad \forall x \in K.$$

Le groupe de Galois de L sur K est le groupe $Gal(L/K)$ des K-automorphismes de L.

Cor. 3 : Si $L \supset K$ est le corps de décomposition d'un polynôme P, on a $|Gal(L/K)| \leq [L : K]$.

Si les racines de P sont simples, on a l'égalité.

Exemples : 1) $Gal(\mathbb{C}/\mathbb{R}) = \{1, \sigma\}$, σ = conjugaison complexe.

2) $Gal(\mathbb{Q}(i)/\mathbb{Q}) = \{1, \sigma\}$.

3) $Gal(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (!)

① Porisme 2 : Dans la situation de la prop, soient Q_1 un facteur irréd de P_1, $Q_2 = \sigma(Q_1)$, x_i une racine de Q_i dans L_i, $i = 1, 2$. Alors il existe un prolongement $\tilde{\sigma}$ t.q. $\tilde{\sigma}(x_1) = x_2$.

(= cor. de la dém.)

1.2 Polynômes séparables

Rappel : Soient A un anneau com. et B une A-algèbre.
Une A-dérivation de B est une appl. A-linéaire

$$d : B \longrightarrow B$$

t.q. $d(b_1 b_2) = d(b_1) b_2 + b_1 d(b_2)$, $\forall b_1, b_2 \in B$.

L'algèbre $A[X]$ admet une unique A-dérivation

$\frac{d}{dX} : A[X] \longrightarrow A[X]$ t.q. $\frac{d}{dX} X = 1$.

On a $\frac{d}{dX} X^n = n X^{n-1}$, $n \geq 1$. Soit $P \in A[X]$. On pose $P' = \frac{d}{dX} P$. Pour tout $a \in A$, il existe $Q(X) \in A[X]$ t.q.

$$P(X) = P(a) + (X-a) P'(a) + (X-a)^2 \cdot Q(X). \qquad (*)$$

(division euclidienne par $(X-a)^2$ ou développement de $P(a+(X-a))$)

Soit K un corps.

Déf : $P \in K[X]$ est séparable $\Longleftrightarrow$ ses racines dans toute extension de K sont simples.

Lemme 1 : $P \in K[X]$ est séparable $\Longleftrightarrow$ $PGCD(P, P') = 1$.

Rque : Le PGCD de deux polynômes $P, Q \in K[X]$ calculé dans $K[X]$ est égal à celui calculé dans $L[X]$, $\forall L \supset K$, car l'algorithme d'Euclide n'utilise que le sous-corps engendré par les coefficients de P et Q.

Dém du lemme : "$\Longleftarrow$" P non séparable $\Longrightarrow$ P comporte un facteur $(X-x)^2$ dans une extension $L \supset K$ $\Longrightarrow$ le PGCD de P et P' est divisible par $X-x$ dans $L[X]$, donc $\neq 1$ ds $K[X]$.

"$\Longrightarrow$" Si P et P' ont un diviseur commun non constant Q, ils ont une racine commune x dans un corps de décomp. L de Q. Alors $(X-x)^2$ divise P par la "formule de Taylor" $(*)$. ✓