CALCUL DU DEGRE D'UNE EXTENSION DE CORPS

Leçons 125

Référence Cognet, Algèbre linéaire, p60-62

Soit $n \in \mathbb{N}^*$. Soient $p_1, \dots, p_n \in \mathbb{N}^*_{\geq 2}$ premiers entre eux deux à deux, sans facteurs carrés.

On note $\mathbb{Q}_0 = \mathbb{Q}$, et pour tout $n \in \mathbb{N}$, $\mathbb{Q}_n = \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n})$.

Alors : 1) $[\mathbb{Q}_n : \mathbb{Q}] = 2^n$

2) $(1, \sqrt{p_n})$ est une $\mathbb{Q}_{n-1}$ base de $\mathbb{Q}_n$

3) $\prod_{I \subset [\![1,n]\!]} \sqrt{p_i}$ est une $\mathbb{Q}$ base de $\mathbb{Q}_n$

Preuve On procède par récurrence sur $n \in \mathbb{N}^*$. (1)+2))

Soit $n=1$ On montre que $(1, \sqrt{p_1})$ est libre sur $\mathbb{Q}$.

Soient $a, b \in \mathbb{Q}$ tels que $a + b\sqrt{p_1} = 0$.

Si $b \neq 0$ alors $\sqrt{p_1} = \frac{-a}{b} \in \mathbb{Q}$.

Donc il existe $(c,d) \in \mathbb{N} \times \mathbb{N}^*$, $c \wedge d = 1$ tels que $\sqrt{p_1} = \frac{c}{d}$. donc $d^2 \wedge c^2 = 1$

Ainsi $d^2 p_1 = c^2$ donc $c^2 | d^2 p_1$ or $d \wedge c = 1$, par le lemme de Gauss $c^2 | p_1$ ce qui est absurde car p_1 est sans facteurs carrés.

Donc $b = 0$, d'où $a = 0$.

Ainsi $(1, \sqrt{p_1})$ est libre sur $\mathbb{Q}$.

Donc $[\mathbb{Q}_1, \mathbb{Q}] \geq 2$.

De plus, $X^2 - p_1 \in \mathbb{Q}[X]$ est annulateur de $\sqrt{p_1}$, donc $[\mathbb{Q}_1 : \mathbb{Q}] \leq 2$

D'où $[\mathbb{Q}_1 : \mathbb{Q}] = 2$.

En particulier, $(1, \sqrt{p_1})$ est une $\mathbb{Q}_0$ base de $\mathbb{Q}_1$.

Hérédité Soit $n \in \mathbb{N}^*$. Supposons la propriété vraie aux rangs $k \in [\![1, n]\!]$.

Soient $p_1, \dots, p_{n+1} \in \mathbb{N}_{\geq 2}$ premiers entre eux, sans facteurs carrés.

On montre que $(1, \sqrt{p_{n+1}})$ est une famille $\mathbb{Q}_{n+1}$ libre sur $\mathbb{Q}_n$.

Soient $a, b \in \mathbb{Q}_n$ tels que $a + \sqrt{p_{n+1}}\, b = 0$.

Si $b \neq 0$, alors $\sqrt{p_{n+1}} = \frac{-a}{b} \in \mathbb{Q}_n$

Or $(1, \sqrt{p_n})$ est une $\mathbb{Q}_{n-1}$ base de $\mathbb{Q}_n$ par hypothèse de récurrence, ainsi il existe $(c,d) \in \mathbb{Q}_{n-1}^2$ tels que $\sqrt{p_{n+1}} = c + d\sqrt{p_n}$.

Ainsi $\underbrace{p_{n+1}}_{\in \mathbb{Q}_{n-1}} = \underbrace{c^2 + d^2 p_n}_{\in \mathbb{Q}_{n-1}} + 2cd\sqrt{p_n}$, donc $2cd\sqrt{p_n} \in \mathbb{Q}_{n-1}$.

Si $cd \neq 0$ alors $\sqrt{p_n} \in \mathbb{Q}_{n-1}$ donc $\mathbb{Q}_{n-1} = \mathbb{Q}_{n-1}(\sqrt{p_n}) \overset{\text{déf}}{=} \mathbb{Q}_n$.
Or par hypothèse de récurrence $[\mathbb{Q}_n : \mathbb{Q}_{n-1}] = 2$, absurde ($\sqrt{p_n} \in \mathbb{Q}_{n-1}$). Donc $cd = 0$.
Par intégrité de $\mathbb{Q}_{n-1}$ (corps), on a deux cas :

- $\underline{c = 0}$: $\sqrt{p_{n+1}} = d\sqrt{p_n}$ donc $\sqrt{p_{n+1}p_n} = dp_n \in \mathbb{Q}_{n-1}$.

Donc $\mathbb{Q}_{n-1} = \mathbb{Q}_{n-1}(\sqrt{p_{n+1}p_n}) = \underbrace{\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_{n-1}}, \sqrt{p_{n+1}p_n})}_{\mathbb{Q}_n}$
Par hypothèse de récurrence, $[\mathbb{Q}_n : \mathbb{Q}] = 2^n$.
$[\mathbb{Q}_{n-1} : \mathbb{Q}] = 2^{n-1}$.

Ce qui est absurde, donc $c \neq 0$.

- $\underline{d = 0}$: $\sqrt{p_{n+1}} = c \in \mathbb{Q}_{n-1}$.

Donc $\mathbb{Q}_{n-1} = \mathbb{Q}_{n-1}(\sqrt{p_{n+1}}) = \underbrace{\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_{n-1}}, \sqrt{p_{n+1}})}_{\mathbb{Q}_n}$
Par hypothèse de récurrence : $[\mathbb{Q}_n : \mathbb{Q}] = 2^n$
$[\mathbb{Q}_{n-1} : \mathbb{Q}] = 2^{n-1}$.

Ce qui est absurde, donc $d \neq 0$.

Finalement, $b = 0$ et donc $a = 0$.
Donc $\underline{(1, \sqrt{p_{n+1}}) \text{ est une famille } \mathbb{Q}_{n+1} \text{ libre sur } \mathbb{Q}_n}$.
D'où $[\mathbb{Q}_{n+1} : \mathbb{Q}_n] \geq 2$.
De plus, $X^2 - p_{n+1} \in \mathbb{Q}_n[X]$ annule $\sqrt{p_{n+1}}$, donc $[\mathbb{Q}_{n+1} : \mathbb{Q}] \leq 2$.
D'où $[\mathbb{Q}_{n+1} : \mathbb{Q}_n] = 2$. $\underline{(1, \sqrt{p_{n+1}}) \text{ est donc une } \mathbb{Q}_n \text{ base de } \mathbb{Q}_{n+1}.}$

Par la récurrence forte et le théorème de la base télescopique, on a :

$$\underline{[\mathbb{Q}_{n+1} : \mathbb{Q}] = 2^{n+1}.}$$

D'où l'hérédité. ▨

3) On a une tour d'extension $\mathbb{Q}_n \to \mathbb{Q}_{n-1} \to \dots \to \mathbb{Q}$.
Les bases intermédiaires sont : $(1, \sqrt{p_1}), \dots, (1, \sqrt{p_n})$ par 2).
Ainsi par théorème de la base télescopique, une base de $\mathbb{Q}_n$ sur $\mathbb{Q}$ est

$$\underline{\left(\prod_{i \in I} \sqrt{p_i}\right)_{I \subset [\![1, n]\!]}}$$

▨

CALCUL DU DEGRÉ D'UNE EXTENSION DE CORPS : Questions

- Pourquoi $(\sqrt{p_1}, \sqrt{p_2}, \dots, \sqrt{p_{n-1}}, \sqrt{p_n p_{n+1}})$ sont premiers entre eux ?

Par hypothèse $\sqrt{p_1}, \dots, \sqrt{p_{n+1}}$ sont pee

Soit $p \in \mathbb{P}$ tel que $p \mid \sqrt{p_n p_{n+1}}$ et $p \mid \sqrt{p_i}$ $i \in [\![1, n-1]\!]$

Par Euclide comme $p \in \mathbb{P}$, $p \mid \sqrt{p_n}$ ou $\sqrt{p_{n+1}}$.

Or on a supposé les $\sqrt{p_j}$ $j \in [\![1, n+1]\!]$ pee, donc $p = 1$.

- Pourquoi $\sqrt{p_n p_{n+1}}$ est sans facteur carré ?

(on prend un diviseur premier car $\mathbb{Z}$ anneau factoriel)

Soit $p \in \mathbb{P}$ tq $p^2 \mid \sqrt{p_n p_{n+1}}$.

Or $\sqrt{p_n} \wedge \sqrt{p_{n+1}} = 1$ donc $p^2 \mid \sqrt{p_n}$ ou $p^2 \mid \sqrt{p_{n+1}}$.

Or $\sqrt{p_n}, \sqrt{p_{n+1}}$ sont sans facteurs carrés, absurde.

- On remplace les racines carrés par des cubiques, ça change quoi ?

On peut prendre $\mathbb{Q}[j]$.

On aura alors $[\mathbb{Q}_n : \mathbb{Q}[j]] = 3$?

La base télescopique sera le produit des bases intermédiaires $(1, \sqrt[3]{p_i}, \sqrt[3]{p_i}^2)$

(On ne met pas j car on est déjà sur $\mathbb{Q}[j]$) car $X^3 - p_i \in \mathbb{Z}[X]$

irréductible donc corps de rupture $\mathbb{Q}[X]/(X^3 - p_i)$ est une base naturelle

(Eisenstein)

est $(1, \bar{X}, \bar{X}^2)$

- Est ce qu'on peut voir $\mathbb{Q}_n$ comme le corps de décomposition d'un polynôme ?

$$P_i = \mu_{\mathbb{Q}, \sqrt{p_i}} = X^2 - p_i$$

$$P = \prod_{i=1}^{n} (X^2 - p_i)$$

$\mathbb{Q}_n$ est une extension normale (L/K, $P \in \mathrm{Irred}(K[X])$ a rac $L \Rightarrow P$ scindé sur L)

séparable car $\mathbb{Q}$ parfait (toutes les extensions sont séparables)

(tout elt $a \in L$ séparable ie $\mu_{a,K} \wedge \mu'_{aK} = 1$)

Donc $\mathbb{Q}_n/\mathbb{Q}$ est galoisienne.

$\mathrm{Gal}(L/K)$ = l'automorphisme de L laissant invariant K

extension gal si $|\mathrm{Gal}(L/K)| K < +\infty$

On a $[\mathbb{Q}_n : \mathbb{Q}] = \#\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) = 2^n$.

Soit $\sigma \in \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$, $\sigma(\sqrt{p_i})^2 = \sigma(p_i)$

$= p_i$ car $p_i \in \mathbb{Q}$.

Donc $\sigma(\sqrt{p_i}) = \pm\sqrt{p_i}$.

σ est d'ordre 2.

Groupe dont élts sont ordre 2.

Donc $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^n$.