Trace et tour d'extensions quadratiques

Leçons : 125, 151.

Énoncés : • Prop : → si $K\subset F\subset L$ et $\alpha\in F$: $\chi_\alpha^{L/K} = (\chi_\alpha^{F/K})^m$ avec $m=[L:F]$;

→ si $K\subset L$ et $\alpha\in L$: $\chi_\alpha^{L/K}$ est une puissance de π_α^K.

• Appli : → la famille $\{\sqrt{d}\ ;\ d\in\mathbb{N}^*$ sans facteur carré$\}$ est libre sur $\mathbb{Q}$;

→ si $p_1,\dots,p_m\in\mathbb{P}$ deux à deux distincts, $[\mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_m}):\mathbb{Q}] = 2^m$.

⊛ Prop.

• Soient $(e_1,\dots,e_m)$ une F-base de L et B une K-base de F. D'après le th de la base télescopique, $B' = (Be_1,\dots,Be_m)$ est une K-base de L. Pour $1\leq i\leq m$, Fe_i est un sous-K-ev de L de base Be_i. Vu que $\alpha\in F$, $m_\alpha^{L/K}$ stabilise F donc Fe_i. La matrice de l'endomorphisme induit est, dans la base Be_i, $M_\alpha = \mathrm{Mat}_B(m_\alpha^{F/K})$. Celle-ci ne dépend pas de i ; on a :

$$\mathrm{Mat}_{B'}(m_\alpha^{L/K}) = \begin{bmatrix} M_\alpha & & 0 \\ & \ddots & \\ 0 & & M_\alpha \end{bmatrix} \quad \text{et} \quad \chi_\alpha^{L/K} = (\chi_\alpha^{F/K})^m.$$

• On applique ce qui précède avec $F = K(\alpha)$. Montrons que $\chi_\alpha^{K(\alpha)/K} = \pi_\alpha^K$.

D'abord, en notant $m_\alpha = m_\alpha^{K(\alpha)/K}$: $\pi_\alpha^K = \pi_{m_\alpha}$. En effet si $P = \sum_{k=0}^d a_k X^k \in K[X]$:

$P(m_\alpha) = \sum_{k=0}^d a_k m_\alpha^k = \sum_{k=0}^d m_{(a_k\alpha^k)} = m_{\left(\sum_{k=0}^d a_k\alpha^k\right)} = m_{P(\alpha)}$. On a donc $P(m_\alpha)=0$ ssi $P(\alpha)=0$, d'où le résultat.

Ensuite $\deg(\chi_\alpha^{K(\alpha)/K}) = [K(\alpha):K] = \deg(\pi_\alpha^K)$. Or ces deux polynômes sont unitaires et $\pi_\alpha^K = \pi_{m_\alpha} \mid \chi_\alpha^{K(\alpha)/K}$ d'après le théorème de Cayley-Hamilton : il y a égalité.

$\chi_\alpha^{L/K}$ est bien une puissance de $\chi_\alpha^{K(\alpha)/K} = \pi_\alpha^K$. □

⊛ Appli.

• Si $K\subset L$ et $\alpha\in L$ on note $\mathrm{Tr}_{L/K}(\alpha) = \mathrm{Tr}(m_\alpha^{L/K})$: $\mathrm{Tr}_{L/K} : L\to K$ est une forme linéaire. La prop a pour corollaire que si $K\subset F\subset L$ et $\alpha\in F$, $\mathrm{Tr}_{L/K}(\alpha) = [L:F]\cdot\mathrm{Tr}_{F/K}(\alpha)$.

Soit $d\geq 2$ sans facteur carré : la matrice de $m_{a+\sqrt{d}b}^{K/\mathbb{Q}}$ dans la base $(1,\sqrt{d})$ de $K=\mathbb{Q}(\sqrt{d})$ est $\begin{bmatrix} a & db \\ b & a\end{bmatrix}$, ce dont on déduit $\mathrm{Tr}_{K/\mathbb{Q}}(a+\sqrt{d}b) = 2a$.

Maintenant on montre par récurrence sur $m\geq 1$ que toute sous-famille de cardinal m de $\{\sqrt{d}\ ;\ d\in\mathbb{N}^*$ sans facteur carré$\}$ est libre. Initialisation à $m=1$: ok car 0 n'est pas dans la famille. Hérédité : on suppose l'hypothèse pour m ; soit $\sqrt{d_1},\dots,\sqrt{d_{m+1}}$ deux à deux distincts et $\lambda_1,\dots,\lambda_{m+1}\in\mathbb{Q}$ tq $\sum_{i=1}^{m+1}\lambda_i\sqrt{d_i} = 0$.

Si l'un des d_i est 1 on peut supposer que c'est d_{m+1}. Si l'on note $L = \mathbb{Q}(\sqrt{d_1},\dots,\sqrt{d_m})$, d'après ce qui précède, pour $1\leq i\leq m$: $\mathrm{Tr}_{\mathbb{Q}(\sqrt{d_i})/\mathbb{Q}}(\sqrt{d_i}) = 0$ donc $\mathrm{Tr}_{L/\mathbb{Q}}(\sqrt{d_i}) = 0$. Appliquer $\mathrm{Tr}_{L/\mathbb{Q}}$ à l'égalité $\sum_{i=1}^{m+1}\lambda_i\sqrt{d_i} = 0$ donne donc $0 = \lambda_{m+1}\mathrm{Tr}_{L/\mathbb{Q}}(1) = [L:\mathbb{Q}]\lambda_{m+1}$. Donc $\lambda_{m+1}=0$; on conclut par HR.

Si au contraire aucun d_i n'est 1 on multiplie par $\sqrt{d_{m+1}}$ pour obtenir $\sum_{i=1}^m \lambda_i\sqrt{d_i d_{m+1}} + \lambda_{m+1}d_{m+1} = 0$.

Pour $1 \leq i \leq n$, $\sqrt{d_i d_{n+1}} = k_i \sqrt{d_i'}$ avec $k_i \in \mathbb{N}^*$ et $d_i' \geq 2$ sans facteur carré puisque $d_i \neq d_{n+1}$.

On a donc $\sum_{i=1}^{n} (\lambda_i k_i) \sqrt{d_i'} + (\lambda_{n+1} d_{n+1}) \cdot 1 = 0$: on applique le cas précédent.

- Pour finir soit $K = \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n})$ avec $p_1, \dots, p_n \in \mathcal{P}$ deux à deux $\neq$. On montre qu'une base de K sur $\mathbb{Q}$ est $\left(\sqrt{\prod_{i \in I} p_i}\right)_{I \subset [\![1;n]\!]}$ (elle est bien de cardinal $|\mathcal{P}([\![1;n]\!])| = 2^n$).

donc $[K:\mathbb{Q}] \geq 2^n$

Cette famille est une sous-famille de la précédente puisque $\prod_{i \in I} p_i$ est sans facteur carré pour $I \subset [\![1;n]\!]$.

Mais pour $0 \leq i \leq n-1$, $[\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_{i+1}}) : \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_i})] \leq 2$ puisque $X^2 - p_{i+1}$ annule $\sqrt{p_{i+1}}$. On a donc $[K : \mathbb{Q}] \leq 2^n$. Finalement $[K:\mathbb{Q}] = 2^n$, et par dimension la famille libre est une base. $\square$

<u>Ref :</u> Samuel – Théorie algébrique des nombres : p 44 (prop).

↳ Pas de ref pour l'appli. Mais pas trop difficile.

↳ 2- "appli" est une appli du 1e point de la prop seulement. Le second est là car c'est un corollaire naturel du premier, et qu'il permet de faire la bonne longueur. Cela convient bien aussi pour

↳ Définir dans le plan π_α^K, $m_\alpha^{L/K}$, $\chi_\alpha^{L/K}$; éventuellement $\mathrm{Tr}_{L/K}(\alpha)$.

↳ Autre utilisation de la prop : dans un corps de nombres K, $\alpha \in \mathcal{O}_K$ ssi $\pi_\alpha^{\mathbb{Q}} \in \mathbb{Z}[X]$ ssi $\chi_\alpha^{K/\mathbb{Q}} \in \mathbb{Z}[X]$. En particulier si $\alpha \in \mathcal{O}_K$, $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$. Cela est utile pour mq $\mathcal{O}_K$ est un groupe abélien libre de rang $[K:\mathbb{Q}]$.

↳ Aller vite sur le début, qui n'est pas difficile.