

$\mathbb{Q}$ -liberté par la trace

Bouly Florent

27 mars 2019

Théorème 1 *Soient $p_1, \dots, p_n$ des nombres premiers distincts. Alors la famille $(\sqrt{p_i})_{1 \leq i \leq n}$ est $\mathbb{Q}$ -libre.*

Soit $\mathbb{K} \hookrightarrow \mathbb{L}$ une extension finie de corps ; on munit ainsi $\mathbb{L}$ d'une structure de $\mathbb{K}$ espace vectoriel. Pour tout y dans $\mathbb{L}$ on introduit $a_y \in \mathcal{L}_{\mathbb{K}}(\mathbb{L})$ par $a_y : x \mapsto yx$ ce qui nous permet de définir pour tout $y \in \mathbb{L}$, $\text{Tr}_{\mathbb{L} \setminus \mathbb{K}}(y) := \text{Tr}(a_y) \in \mathbb{K}$. Enfin, on introduit une forme bilinéaire ϕ sur $\mathbb{L}$ définie par $\phi(x, y) := \text{Tr}_{\mathbb{L} \setminus \mathbb{K}}(xy)$.

On a toute suite deux lemmes très simples :

Lemme 1 : *Soient $v_1, \dots, v_n \in \mathbb{K}^n$ et $B : \mathbb{K}^n \times \mathbb{K}^n \rightarrow \mathbb{K}$ bilinéaire. Si $\det((B(v_i, v_j))_{1 \leq i, j \leq n})$ est non nul alors la famille $(v_1, \dots, v_n)$ est $\mathbb{K}$ -libre.*

En effet, si la famille était liée, les colonnes de la matrice le seraient aussi.

Lemme 2 : *Pour tout P dans $\mathbb{K}[X]$ on a $P(a_y) = a_{P(y)}$.*

C'est une conséquence immédiate des relations $a_x + a_y = a_{x+y}$ et $a_x a_y = a_{xy}$.

Par la suite, pour un endomorphisme u , on notera π_u son polynôme minimal unitaire et χ_u son polynôme caractéristique.

Une conséquence du lemme 2 est que P est annulateur pour a_y si et seulement si $P(y) = 0$; en particulier tous les π_{a_y} sont irréductibles.

A y fixé, on peut donc utiliser la structure d'anneau factoriel de $\mathbb{K}[X]$ pour écrire $\chi_{a_y} = (\pi_{a_y})^m Q$ où Q est premier avec π_{a_y} . De plus, Q et π_{a_y} n'ont pas de racines en commun (on peut par exemple utiliser le théorème de Bezout). Si Q était non constant, χ_{a_y} aurait donc des racines distinctes de celles de π_{a_y} ce qui est absurde puisque ces deux polynômes ont exactement les valeurs propres comme racines. Ces deux derniers étant unitaires, on en déduit que χ_{a_y} est une puissance de π_{a_y} .

Plaçons nous maintenant dans le cas qui nous intéresse : $\mathbb{K} = \mathbb{Q}$ et $\mathbb{L} = \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n})$. On a :

$$\phi(\sqrt{p_i}, \sqrt{p_i}) = \text{Tr}_{\mathbb{L} \setminus \mathbb{Q}}(p_i) = p_i \text{Tr}_{\mathbb{L} \setminus \mathbb{Q}}(1) = p_i [\mathbb{L} : \mathbb{Q}].$$

$$\text{Si } i \neq j : \phi(\sqrt{p_i}, \sqrt{p_j}) = \text{Tr}_{\mathbb{L}|\mathbb{Q}}(\sqrt{p_i}\sqrt{p_j}) = \text{Tr}(a_{\sqrt{p_i p_j}}).$$

Le polynôme $X^2 - p_i p_j$ est le polynôme minimal de $\sqrt{p_i p_j}$ sur $\mathbb{Q}$ et donc :

$$\chi_{a_{\sqrt{p_i p_j}}} = (X^2 - p_i p_j)^m.$$

En particulier, le coefficient devant X^{2m-1} qui correspond à la trace est nul et donc $\text{Tr}(a_{\sqrt{p_i p_j}}) = 0$.

Le déterminant de la matrice $(\phi(\sqrt{p_i}, \sqrt{p_j}))_{1 \leq i, j \leq n}$ est donc $p_1 \dots p_n [\mathbb{L} : \mathbb{Q}]^n \neq 0$ et le lemme 1 permet de conclure.

Remarque : Chaque extension $\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_i}) \hookrightarrow \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_{i+1}})$ est de degré au plus 2 car $X^2 - p_{i+1}$ est annulateur ; on peut donc majorer $[\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n}) : \mathbb{Q}]$ par 2^n .

En fait, c'est exactement 2^n : la famille des $\sqrt{\prod_{i \in I} p_i}$ où I est un sous ensemble de $\{1, \dots, n\}$ est libre et de cardinal 2^n . On peut le montrer exactement de la même façon que précédemment.