DEGRÉ DE $\mathbb{Q}[\{\sqrt{p_i}\}_{1\leq i\leq n}]$ SUR $\mathbb{Q}$

[Cog00, §2.1, p60–62]

ÉNONCÉ

THÉORÈME. *Pour tout entier $n \in \mathbb{N}^*$ et toute famille $(p_i)_{1\leq i\leq n}$ d'entiers supérieurs ou égaux à 2, tous sans facteur carré, et premiers deux à deux, on a :*

$$\left[\mathbb{Q}[\{\sqrt{p_i}\}_{1\leq i\leq n}] : \mathbb{Q}\right] = 2^n .$$

DÉVELOPPEMENT

Lorsque les $(p_i)_{1\leq i\leq n}$ sont fixés, on note $\mathbb{Q}_k = \mathbb{Q}\big[\{\sqrt{p_i}\}_{1\leq i\leq k}\big]$ pour $k \in [\![0,n]\!]$.

LEMME. *Soient $n \in \mathbb{N}^*$ et $(p_i)_{1\leq i\leq n}$ des entiers satisfaisants.*
Pour $J \subset [\![1,n]\!]$, on note $P_J = \prod_{j\in J}\sqrt{p_j}$, puis on pose $K_n = \big\{P_J : J \subset [\![1,n]\!]\big\}$.
Alors $\mathbb{Q}_n = \mathrm{Vect}_{\mathbb{Q}}(K_n)$.

En effet, on vérifie que si $P_J, P_{J'} \in K_n$, alors $P_J P_{J'} \in \mathrm{Vect}_{\mathbb{Q}}(K_n)$ puisque

$$P_J P_{J'} = P_{J\oplus J'} \prod_{i\in J\cap J'} p_i \,, \qquad \text{où } J \oplus J' = (J\cup J') \setminus (J\cap J') \,.$$

Ainsi $\mathrm{Vect}_{\mathbb{Q}}(K_n)$ est stable par produit, donc est une algèbre contenant $\mathbb{Q}$ et les $(\sqrt{p_i})_{1\leq i\leq n}$. C'est de plus la plus petite algèbre possédant cette propriété, donc $\mathbb{Q}_n = \mathrm{Vect}_{\mathbb{Q}}(K_n)$.

Montrons maintenant par récurrence forte sur $n \in \mathbb{N}^*$ que pour toute famille $(p_i)_{1\leq i\leq n}$ d'entiers satisfaisants, on a $[\mathbb{Q}_n : \mathbb{Q}_{n-1}] = 2$.

Le résultat attendu découlera alors du théorème de la base télescopique :

$$[\mathbb{Q}_n : \mathbb{Q}] = \prod_{k=1}^{n} [\mathbb{Q}_k : \mathbb{Q}_{k-1}] = 2^n \,.$$

Dans la suite, on notera $D_k = [\mathbb{Q}_k : \mathbb{Q}_{k-1}]$ pour $k \in [\![1,n]\!]$.

- Pour $n = 1$, soit $p_1 \geq 2$ sans facteur carré. $X^2 - p_1$ est un polynôme annulateur de $\sqrt{p_1}$.
Si $\sqrt{p_1} \notin \mathbb{Q}$, c'est en fait un polynôme irréductible sur $\mathbb{Q}$, et donc $\mathbb{Q}_1$ est le corps de rupture de ce polynôme. Ainsi $D_1 = \deg(X^2 - p_1) = 2$. Supposons que ce ne soit pas le cas, et écrivons $\sqrt{p_1} = \frac{p}{q} \in \mathbb{Q}$ avec $p \wedge q = 1$, $q \in \mathbb{N}^*$. Alors $p_1 q^2 = p^2$ et donc $p \neq 0$ et $p^2 \mid p_1$, ce qui est faux par hypothèse sur p_1. Ainsi $D_1 = 2$.
- Pour l'hérédité, fixons alors un $n \in \mathbb{N}$ tel que la propriété est vraie pour tout rang inférieur ou égal à n. Soient $p_1, \dots, p_{n+1}$ satisfaisants.
Comme précédemment, il est clair que $D_{n+1} \leq 2$ car $X^2 - p_{n+1}$ est un polynôme annulateur de $\sqrt{p_{n+1}}$ sur $\mathbb{Q}_n$. Pour que l'extension soit de degré 2, il faut et il suffit donc que $\sqrt{p_{n+1}} \notin \mathbb{Q}_n$. Supposons que ce n'est pas le cas.
Par hypothèse de récurrence, on a que $\sqrt{p_{n+1}} \in \mathbb{Q}_n = \mathbb{Q}_{n-1}[\sqrt{p_n}]$.
Or, le théorème de la base télescopique donne $[\mathbb{Q}_n : \mathbb{Q}] = 2^n$ et, en reprenant les notations du Lemme, on a que K_n est une famille de cardinal 2^n engendrant $\mathbb{Q}_n$, donc c'est en fait une $\mathbb{Q}$-base de $\mathbb{Q}_n$. En particulier, on a
$$\mathbb{Q}_n = \mathbb{Q}_{n-1} \oplus \sqrt{p_n}\,\mathbb{Q}_{n-1} \,.$$
Soient donc $a, b \in \mathbb{Q}_{n-1}$ tels que $\sqrt{p_{n+1}} = a + b\sqrt{p_n}$. On a alors :
$$p_{n+1} = \big(a^2 + b^2 p_n\big) + 2ab\sqrt{p_n} \,.$$
Par unicité de la décomposition d'un élément de $\mathbb{Q} \subset \mathbb{Q}_n$ en $\mathbb{Q}_{n-1} \oplus \sqrt{p_n}\mathbb{Q}_{n-1}$, on a donc nécessairement $2ab = 0$.
  - Si $a = 0$, alors $\sqrt{p_n p_{n+1}} = b\,p_n \in \mathbb{Q}_{n-1}$, ce qui contredit l'hypothèse de récurrence appliquée à la famille $p_1, \dots, p_{n-1}$ et $p_n p_{n+1}$ (ce dernier entier est bien sans facteur carré et premier avec les autres).
  - Sinon, $b = 0$ et alors $\sqrt{p_{n+1}} = a \in \mathbb{Q}_{n-1}$, ce qui contredit à nouveau l'hypothèse de récurrence appliquée à la famille $p_1, \dots, p_{n-1}$ et p_{n+1}.

  On a donc une contradiction. Ainsi $D_{n+1} = 2$ et on a le résultat au rang $n+1$.

On conclut par principe de récurrence.

COMMENTAIRES

A-t-on $\mathbb{Q}_n = \mathbb{Q}[\sqrt{p_1 \cdots p_n}]$?

Le lemme est là pour rallonger un peu le développement, mais à la place il est possible de montrer le théorème de la base télescopique.