Théorème de l'élément primitif en caractéristique nulle

Théorème 1. *Soit $\mathbb{K}$ un corps de caractéristique nulle, et soit $P \in \mathbb{K}[X]$ irréductible. Si $\mathbb{L}$ est un corps de décomposition de P sur $\mathbb{K}$, alors P est à racines simples dans $\mathbb{L}$.*

Démonstration.

Le polynôme P est irréductible, donc $P \wedge P'$ vaut 1 ou P. Par l'absurde, si $P \wedge P' = P$, alors P divise P'. Comme P' est de plus petit degré que P, il vient que $P' = 0$. Donc P est constant puisque la caractéristique de $\mathbb{K}$ est nulle, ce qui est absurde. Ainsi P et P' sont premiers entre eux dans $\mathbb{K}[X]$, donc dans $\mathbb{L}[X]$. □

Théorème 2 (Élément primitif en caractéristique nulle)**.** *Toute extension finie d'un corps de caractéristique nulle est monogène.*

Démonstration.

Soit $\mathbb{L}$ une extension finie d'un corps $\mathbb{K}$. Il existe alors $x_1, \dots, x_n \in \mathbb{L}$ tels que $\mathbb{L} = \mathbb{K}(x_1, \dots, x_n)$. Par une récurrence immédiate, il suffit de montrer le théorème pour $n = 2$.

Soient $x, y \in \mathbb{L}$ tels que $\mathbb{L} = \mathbb{K}(x, y)$. Soient π_x et π_y les polynômes minimaux de x et y. Soit $\mathbb{M}$ le corps de décomposition de $\pi_x \pi_y$. On pose :

$$\pi_x = \prod_{i=1}^{p}(X - x_i) \quad \text{et} \quad \pi_y = \prod_{i=1}^{q}(X - y_i) \quad \text{avec} \quad x = x_1 \quad \text{et} \quad y = y_1$$

Comme π_x et π_y sont irréductibles sur $\mathbb{K}$ qui est de caractéristique nulle, ils sont à racines simples dans $\mathbb{M}$. Ainsi, les x_i sont distincts deux à deux, tout comme les y_i. On pose alors :

$$\Gamma = \left\{ \frac{x_i - x_{i'}}{y_j - y_{j'}} \mid 1 \leqslant i, i' \leqslant p, 1 \leqslant j \neq j' \leqslant q \right\}$$

L'ensemble Γ est fini et $\mathbb{K}$ est infini, donc il existe $t \in \mathbb{K}^\star \setminus \Gamma$. Ainsi, tous les $x_i + t y_i$ sont distincts deux à deux.

On pose $z = x + ty$, et on travaille dans $\mathbb{K}(z)[X]$. Alors y est racine de $P(X) = \pi_y(X)$ et de $Q(X) = \pi_x(z - tX)$. Soit $S = \text{pgcd}(P, Q)$. Si S est de degré 1, alors $y \in \mathbb{K}(z)$. Sinon, comme S divise π_y, il existe $j > 2$ tel que y_j soit racine de S, donc racine de Q. Ainsi, il existe $i \in [\![1, p]\!]$ tel que $z - t b_j = a_i$, ce qui est exclu par hypothèse sur t. Ainsi, on a que $y \in \mathbb{K}(z)$ et $x = z - ty \in \mathbb{K}(z)$, donc $\mathbb{K}(x, y) \subseteq \mathbb{K}(z)$. Réciproquement, $\mathbb{K}(z) \subseteq \mathbb{K}(x, y)$ car $z = x + ty$. Finalement, $\mathbb{K}(x, y) = \mathbb{K}(z)$, d'où le résultat.

□

Application 3. *Soient p, q premiers. Alors $\mathbb{Q}(\sqrt{p}, \sqrt{q}) = \mathbb{Q}(\sqrt{p} + \sqrt{q})$.*

Démonstration.

Soit $a = \sqrt{p} + \sqrt{q}$. On a $\mathbb{Q}(a) \subseteq \mathbb{Q}(\sqrt{p}, \sqrt{q})$. De plus, $(a - \sqrt{p})^2 = q = a^2 - 2a\sqrt{p} + p$, donc $\sqrt{p} \in \mathbb{Q}(a)$. De même, on a $\sqrt{q} \in \mathbb{Q}(a)$. Ainsi, $\mathbb{Q}(\sqrt{p}, \sqrt{q}) \subseteq \mathbb{Q}(a)$, d'où $\mathbb{Q}(a) = \mathbb{Q}(\sqrt{p}, \sqrt{q})$. □

Références

[Gou] Xavier Gourdon. *Les Maths en Tête : Algèbre.* Ellipses, 2e edition