Théorème de l'élément primitif, caractéristique 0

Florian DUSSAP

Agrégation 2018

Lemme. *Soit* $\mathbf{K}$ *un corps de caractéristique 0 et soit* $P \in \mathbf{K}[X]$ *irréductible. Si* $\mathbf{L}$ *est un corps de décomposition de* P *sur* $\mathbf{K}$*, alors* P *est à racines simples dans* $\mathbf{L}$*.*

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 $P' = 0$. Donc P est constant puisque la caractéristique de $\mathbf{K}$ est nulle, ce qui est absurde. Ainsi P et P' sont premiers entre eux dans $\mathbf{K}[X]$, donc dans $\mathbf{L}[X]$. □

Théorème. *Soit* $\mathbf{K}$ *un corps de caractéristique 0 et soit* $\mathbf{L} = \mathbf{K}(a_1, \dots, a_k)$ *une extension finie de* $\mathbf{K}$*. Alors il existe* $b \in \mathbf{L}$ *tel que* $\mathbf{L} = \mathbf{K}(b)$*.*

Démonstration. On procède par récurrence sur k.

— Si $k = 1$, il n'y a rien à montrer.

— Si $k = 2$, alors $\mathbf{L} = \mathbf{K}(x, y)$ et on veut montrer qu'il existe $z \in \mathbf{L}$ tel que $\mathbf{L} = \mathbf{K}(z)$. Considérons P_x et P_y les polynômes minimaux de x et de y sur $\mathbf{K}$ et posons $\mathbf{M}$ un corps de décomposition de $P_x P_y$ sur $\mathbf{K}$. Dans $\mathbf{M}[X]$, on écrit :

$$P_x(X) = (X - x) \prod_{i=2}^{n} (X - x_i), \qquad x_1 = x$$

$$P_y(X) = (X - y) \prod_{j=2}^{m} (X - y_j), \qquad y_1 = y$$

En vertu du lemme, les (x_i) sont tous distincts et les (y_j) sont tous distincts.
Montons qu'il existe $t \in \mathbf{K}^*$ tel que pour tous $i, j \geqslant 2$, $x + ty \neq x_i + ty_j$. En effet si $x + ty = x_i + ty_j$ alors $t = \frac{x - x_i}{y_j - y}$. Or l'ensemble $\{\frac{x - x_i}{y_j - y} : i, j \geqslant 2\}$ est fini. Comme $\mathbf{K}^*$ est infini (caractéristique 0), il existe t comme voulu.
Posons alors $z = x + ty$ et montrons que $\mathbf{K}(z) = \mathbf{K}(x, y)$. On considère pour cela le polynôme $Q(X) = P_x(z - tX) \in \mathbf{K}(z)[X]$. Calculons le PGCD de Q et de P_y dans $\mathbf{K}(z)[X]$. On le calcule d'abord dans $\mathbf{M}[X]$: soit $\alpha \in \mathbf{M}$ une racine commune de P_y et de Q. Alors il existe i, j tels que $\alpha = y_j$ et $z - t\alpha = x_i$, c'est-à-dire tels que $x + ty = x_i + ty_j$. Par choix de t, on trouve nécessairement $x = x_i$ et $y = y_j$. Ainsi $\alpha = y$. Réciproquement, y est bien une racine commune de Q et de P_y. Finalement la seule racine commune dans $\mathbf{M}$ de Q et de P_y est y. Puisque P_y est à racines simples (lemme), on en déduit que $\mathrm{PGCD}_{\mathbf{M}[X]}(Q, P_y) = X - y$. Le PGCD ne dépendant pas du corps, on obtient $\mathrm{PGCD}_{\mathbf{K}(z)[X]}(Q, P_y) = X - y$.
Par conséquent, y appartient à $\mathbf{K}(z)$ donc $x = z - ty$ aussi et on a $\mathbf{K}(x, y) \subseteq \mathbf{K}(z)$. Réciproquement, $z = x + ty$ appartient à $\mathbf{K}(x, y)$ donc $\mathbf{K}(z) \subseteq \mathbf{K}(x, y)$.

— Supposons le résultat vrai au rang $k - 1$ et montrons-le au rang k. Considérons $\mathbf{L} = \mathbf{K}(a_1, \dots, a_k)$. Par hypothèse de récurrence, il existe $b \in \mathbf{L}$ tel que $\mathbf{K}(a_1, \dots, a_{k-1}) = \mathbf{K}(b)$. Ainsi, $\mathbf{K}(a_1, \dots, a_k) = \mathbf{K}(b, a_k)$. On applique alors le cas $k = 2$: il existe $c \in \mathbf{L}$ tel que $\mathbf{K}(b, a_k) = \mathbf{K}(c)$.

□

Référence

— GOURDON, *Les maths en tête, algèbre.*