Développement : Théorème de l'élément primitif

Leçons : 125, 141, 144.

Théorème. *Soit K un corps de caractéristique nulle, soit L extension de K de degré fini. Alors il existe $x \in L$ tel que $L = K(x)$. De plus, le résultat reste vrai si K est un corps fini.*

Démonstration. Par récurrence sur le nombre de générateurs de l'extension. Montrons que pour tous $x, y \in L$, il existe $z \in L, K(x,y) = K(z)$.

Étape 1 : Définition du générateur.

Soit M corps de décomposition de $\pi_x \pi_y$. Ainsi, sur M, on peut écrire $\pi_x = \prod_{i=1}^{p}(X - x_i), \pi_y = \prod_{j=1}^{q}(X - y_j)$.

De plus, les (x_i) sont tous distincts : en effet, comme π_x irréductible dans $K[X]$, π_x et π_x' sont premiers entre eux dans $K[X]$. Par Bézout, il existe donc $U, V \in K[X], U\pi_x + V\pi_x' = 1$ et cette égalité vaut aussi dans $M[X]$. Cela prouve que π_x, π_x' aussi premiers entre eux dans $M[X]$, ce qui n'est pas le cas que si π_x n'a que des racines simples. Donc les x_i sont distincts, de même pour les y_j.

Soit $\Gamma = \left\{ \dfrac{x_i - x_i'}{y_j - y_j'}, i, i', j \neq j' \right\}$. Γ fini, K^* est infini, donc il existe $t \in K^* \backslash \Gamma$. Les $(x_i + t y_j)_{i,j}$ sont alors deux à deux distincts. On pose $z = x + ty$.

Étape 2 : Vérification que c'est un générateur.

Montrons que y est la seule racine commune de π_y et de $\pi_x(z - tX)$. Soit a une racine commune. Il existe i, j tels que $a = y_j = z - t x_i$, donc $x + ty = z = x_i + t y_j$, ce qui prouve $x_i = x, y_j = y = a$. Donc y est la seule racine commune, et comme ces deux polynômes sont scindés à racines simples dans $M[X]$, $(X - y)$ est leur PGCD. Comme précédemment, on montre par Bézout que si D est le PGCD de ces deux polynômes dans $K(z)[X]$, il l'est aussi dans $M[X]$, donc $X - y$ est aussi le PGCD dans $K(z)[X]$. Cela prouve que $y \in K(z)$, donc $x = z - ty \in K(z)$ et ainsi $K(x,y) \subseteq K(z)$. Et comme $z = x + ty \in K(x,y)$, on a $K(x,y) = K(z)$.

Étape 3 : Cas d'un corps fini.

Si K corps fini, alors L est aussi fini, étant un K-espace vectoriel de dimension finie. Alors L^* est cyclique, soit x générateur de L^*. On a $L = K(x)$. □

Corollaire. *Si K corps de caractéristique nulle ou corps fini, L extension de K, on a $[L : K] \leq n \Leftrightarrow \forall x \in L, [K(x) : K] \leq n$.*

Démonstration.

$\Rightarrow$: Si $[L : K] \leq n$, comme on a $[L : K] = [L : K(x)][K(x) : K]$, on a $[K(x) : K] | [L : K]$ donc $[K(x) : K] \leq n$.

$\Leftarrow$: Si $\forall x \in L, [K(x) : K] \leq n$, soit $x \in L$ tel que $[K(x) : K]$ soit maximal. Par l'absurde, si $K(x) \neq L$, soit $y \in L \backslash K(x)$. Comme x, y sont de degré fini, on a $K(x,y)$ extension finie, et par le théorème de l'élément primitif, il existe $z \in L, K(x,y) = K(z)$. Comme $y \notin K(x)$, on a $[K(x,y) : K(x)] > 1$ donc $[K(z) : K] = [K(z) : K(x)][K(x) : K] > [K(x) : K]$, ce qui contredit la maximalité. Donc $K(x) = L$ et $[L : K] \leq n$. □

Références

X. Gourdon, Les maths en tête - Algèbre, Ellipses, p. 89.
P. Ortiz, Exercices d'algèbre, Ellipses, p. 125.