Théorème de l'élément primitif

Ce développement est issu de Francinou et Gianella, *Exercices de mathématiques pour l'agrégation.* On admet ici que le groupe multiplicatif d'un corps fini est cyclique.

Théorème. *Soit L/K une extension finie de caractéristique nulle (ou une extension finie d'un corps fini). Alors, il existe $\alpha \in L$ tel que $L = K(\alpha)$.*

Démonstration. Si L est finie, Le groupe multiplicatif de L est alors cyclique. Soit α un de ses générateurs. Il est alors clair que $K(\alpha) = L$.
Si maintenant L est de caractéristique nulle, on commence par supposer que $L = K[x, y]$. On note π_x et π_y les polynômes minimaux de x et y. Soit enfin M un corps de décomposition de $\pi_x\pi_y$. Dans M, on peut écrire

$$\pi_x = (X - x)\prod_{i=2}^{m}(X - x_i) \quad \text{et} \quad \pi_y = (X - y)\prod_{j=2}^{n}(X - x_j).$$

Puisque π_x et π_y sont irréductibles dans L de caractéristique nulle, leurs racines dans M sont simples donc les x_i et les y_j sont deux à deux distincts (et respectivement distincts de x et de y). On considère alors l'ensemble (bien défini)

$$\mathcal{E} = \left\{ \frac{x - x_i}{y - y_j} \right\}.$$

$\mathcal{E}$ a au plus $(m-1)(n-1)$ éléments. Comme K est infini, il existe $t \in K \setminus \{0\}$ tel que $t \notin \mathcal{E}$, c'est-à-dire tel que $\forall i, j\ z = x + ty \neq x_i + ty_j$.

On considère alors $K' = K[z]$ et on note $F(X) = \pi_x(z - tX)$. Ainsi, $K \subset K' \subset L$. $\pi_x \in K'[X]$ et $z - tX \in K'[X]$, donc $F \in K'[X]$ par composition. Dans M, F est scindé (car π_x l'est) donc on peut écrire

$$F(X) = (z - tX - x)\prod_{i=2}^{m}(z - tX - x_i) = t(y - X)\prod_{i=1}^{m}(x - x_i + t(y - X)).$$

De par la définition de t, pour tout $j \geqslant 2$, $F(y_j) \neq 0$ donc $F \wedge \pi_y = (X - y)$ (dans M, donc dans L). En particulier, $X - y \in K'[X]$ donc $y \in K'$.
En reproduisant exactement le même raisonnement, on montre que $x \in K'$ donc $L = K'$ est monogène.

On va maintenant montrer le cas général par récurrence. On a vu le cas $n = 2$. On suppose le résultat vrai pour une extension de degré $n - 1$. Soit L/K une extension finie de degré n : $L = K(x_1, \cdots, x_n)$. On écrit alors $L = K(x_1, \cdots, x_{n-1})(x_n)$. Par hypothèse de récurrence, il existe $\alpha \in L$ tel que $K(x_1, \cdots, x_{n-1}) = K(\alpha)$. Le cas $n = 2$ permet alors de conclure. □

Remarque : si $K = \mathbb{F}_p(X, Y)$ et $K_0 = \mathbb{F}_p(X^p, Y^p)$, K/K_0 n'est pas monogène. Pour le montrer, on commence par remarquer que $(X^iY^j)_{0 \leqslant i,j<p}$ est une base de K/K_0. On a aussi (Frobenius), pour tout $F \in \mathbb{F}_p[X, y]$, $F(X, Y)^p = F(X^p, Y^p)$. Si K est monogène ($= K_0(\alpha)$), puisque $\alpha^p \in K_0$, $[K : K_0] \leqslant p$, contradiction (la base contient p^2 éléments).

Corollaire. *Soit L/K une extension finie (de caractéristique quelconque). Alors L/K admet un nombre fini d'extensions intermédiaires si et seulement si L/K est monogène.*

Démonstration. ($\Rightarrow$) Si K est fini, L est fini donc est une extension monogène. On supposera donc K infini. Soient alors a, b deux éléments quelconques de L. On va montrer que $K(a,b)/K$ est monogène. Pour tout $c \in K$, les extensions $K(a+cb)$ forment des extensions intermédiaires entre K et $K(a,b)$. Puisqu'il n'y en a qu'un nombre fini et que K est infini, il existe donc $c \neq c'$ tels que $K(a+cb) = K(a+c'b)$, c'est-à-dire en particulier que $a + c'b \in K(a+cb)$, donc que $a + c'b - (a+cb) = b(c'-c) \in K(a+cb)$, donc que $b \in K(a+cb)$. Alors, $a = a+cb-cb \in K(a+cb)$, ce qui montre que $K(a+cb) = K(a,b)$. La même récurrence que plus haut permet d'affirmer que L est monogène.

($\Leftarrow$) Soit M un corps intermédiaire de $L = K(\alpha)$ et soit P, Q les polynômes minimaux de α respectivement sur K et M. Alors $Q \mid P$. Soit M' le sous-corps de K engendré par les coefficients de Q. Évidemment, $M' \subset M$. Le polynôme minimal de α sur M' est encore Q, donc $[L : M] = [L : M'] = \deg(Q)$. Ainsi, $M = M'$.

Les corps intermédiaires sont donc engendrés par les différents facteurs (unitaires) de P dans $L[X]$. Ceux-ci sont en nombre fini, ce qui conclut la démonstration.

□