Théorème de l'élement primitif

Théorème 1. *Toute extension séparable de type finie est monogène. En d'autres termes si L/K est une extension telle que $L = K(a_1, \dots, a_n)$ avec les a_i séparables sur K (c'est-à-dire dont le polynôme minimal sur K est scindé à racines simples dans son corps de décomposition), alors il existe $a \in L$ telle que $L = K(a)$.*

On ne fait la preuve que dans le cas d'un corps infini. Dans le cas de la caractéristique p, on peut prendre pour élement primitif un générateur de F_q^*.

Démonstration. Soit K un corps infini. Raisonnons par récurrence sur le nombre de générateurs. On note pour $n \in \mathbb{N}^* : S(n)$ l'assertion "Si $L = K(a_1, \dots, a_n)$ est une extension algébrique de K avec au moins $(n-1)$ des a_i qui sont séparables, alors L/K est monogène."

• $S(1)$ est vraie. Démontrons $S(2)$. Soit $L = K(a, b)$ algébrique avec b séparable. On pose P le polynôme minimal de a sur K et Q le polynôme minimal de b sur K. Soit $n = deg(P)$ et $m = deg(Q)$. On note M le corps de décomposition de PQ. On note $a_1 = a, \dots, a_n$ les racines de P dans M. On note $b_1 = b, \dots, b_m$ les racines de Q dans M. Comme b est séparable alors les b_i sont distincts deux à deux.

L'idée principale est de chercher un élement primitif γ sous la forme $a + cb$ pour un bon choix de $c \in K$. Or il existe $c \in K$ tel que $a + cb \neq a_i + cb_j$ pour tout $i \in [1, n]$ et $j \in [2, m]$. En effet les élements c de K ne convenant pas sont de la forme $c = \frac{a-a_i}{b_j-b}$ qui sont donc en nombre fini. Or K est infini donc un tel c existe.

Soit $\gamma = a + cb$. Montrons que γ est un élement primitif de L. $K(\gamma) = K(a, b)$? On a déjà $K(\gamma) \subset K(a, b)$ car $\gamma = a + cb$. Montrons maintenant que $b \in K(\gamma)$. b est racine de $Q \in K(\gamma)[X]$ mais aussi de $R(X) = P(\gamma - cX) \in K(\gamma)[X]$. On note S le pgcd de Q et R sur $K(\gamma)[X]$. Alors si S est de degré 1, $b \in K(\gamma)$. Sinon S est de degré > 1. Or S divise $Q(X) = \prod_{j=1}^{m}(X - b_j)$, donc il existe b_j racine de S avec $j > 2$. b_j est alors aussi racine de R. Donc il existe $i \in [1, n]$ tel que $\gamma - cb_j = a_i$. C'est exclu par hypothèse sur c. Donc $b \in K(\gamma)$.

Or $a = \gamma - cb \in K(\gamma)$. Donc $\boxed{K(\gamma) = K(a, b)}$. On a démontré $S(2)$.

• Supposons que $S(n)$ soit vraie pour un $n \geq 2$. Démontrons $S(n+1)$. Soit $L = K(a_1, \dots, a_n, a_{n+1})$ algébrique sur K. Quitte à permuter supposons que $a_2, \dots, a_{n+1}$ soient séparables. Alors $L_1 = K(a_1, \dots, a_n)$ est monogène par $S(n)$. Il existe $a \in L$ tel que $L_1 = K(a)$. Donc $L = L_1(a_{n+1}) = K(a, a_{n+1})$. Or a_{n+1} est séparable donc d'après $S(2)$, il existe $\gamma \in L$ telle que $\boxed{L = K(\gamma)}$.

□

[Le développement étant légèrement court, on propose un calcul explicite d'un élement primitif]

Exemple : Soient p et q deux nombres premiers. $\mathbb{Q}(\sqrt{p}, \sqrt{q}) = \mathbb{Q}(\sqrt{p} + \sqrt{q})$.

Démonstration. On pose $a = \sqrt{p} + \sqrt{q}$. On a $\mathbb{Q}(a) \subset \mathbb{Q}(\sqrt{p}, \sqrt{q})$. Or $(a - \sqrt{p})^2 = q = a^2 - 2a\sqrt{p} + p^2$, donc $\sqrt{p} \in \mathbb{Q}(a)$. De même $\sqrt{q} \in \mathbb{Q}(a)$. Donc $\boxed{\mathbb{Q}(a) = \mathbb{Q}(\sqrt{p}, \sqrt{q})}$.

□

Références :

— Gozard - Théorie de Galois

Remarques : Le théorème précédent n'est pas "effectif" au sens où il faut connaître le corps de décomposition des polynômes P et Q.

Il existe une autre démonstration basée sur la théorie de Galois (utilisant $Gal(L/K)$). Voir ?

Exercice : Montrer que $\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n}) = \mathbb{Q}(\sqrt{p_1} + \cdots + \sqrt{p_n})$ pour des nombres premiers p_i distincts deux à deux.

Exercice : Donner un exemple d'extension algébrique et non-monogène.