Théorème de l'élément primitif

Réf:
- Extension de corps, J. Calais

Leçons: 125, 141, 151

Théorème (Elément primitif)

Soient K un corps et L une extension de degré fini de K séparable.

Alors L est une extension simple de K

Preuve: on suppose K de cardinal infini, et notons n le degré $[L:K]$ que l'on suppose strictement plus grand que 1.

Par récurrence, il suffit de montrer le résultat pour $n=2$.

Soient α, β dans L tels que $L = K(\alpha,\beta)$ (α,β base de L sur K)

Comme $\frac{L}{K}$ est une extension de degré fini, elle est algébrique.

Notons P_α et P_β les polynômes minimaux respectifs de α et β sur K.
Notons f le produit $P_\alpha P_\beta$.

Etape 1: soit M un corps de décomposition de f sur K contenant L

Notons r le degré de P_α et s celui de P_β.

Soient $\alpha_1, \alpha_2, \dots, \alpha_r, \beta_1, \dots, \beta_s$ les racines de P_α, P_β dans M avec $\alpha_1 = \alpha$ et $\beta_1 = \beta$.

Comme L est séparable sur K les éléments $\alpha_1, \dots, \alpha_r$ et $\beta_1, \dots, \beta_s$ sont respectivement deux à deux distincts dans M.

Etape 2: Montrons qu'il existe $t \in K^\times$ tel que

$$\forall (i,j) \in [\![2,r]\!] \times [\![2,s]\!] \quad \alpha_i + t\beta_j \neq \alpha + t\beta$$

L'ensemble Φ défini par

$$\Phi = \left\{ -\frac{\alpha - \alpha_i}{\beta - \beta_j} \; ; \; 2 \leq i \leq r, 2 \leq j \leq s \right\}$$

est une partie non vide fini de M^*. Comme K est infini, il existe alors $t \in K^*$ tel que $t \notin \Phi$.

Or on a

$$t \notin \Phi \Rightarrow \forall (i,j) \in [\![2,r]\!] \times [\![2,s]\!] \quad \alpha + t\beta \neq \alpha_i + t\beta_j$$

Etape 3 : on se donne $t \in K$ vérifiant $t \notin \Phi$.

Notons θ l'élément $\alpha + t\beta$. On a alors

$$\forall (i,j) \in [\![2,r]\!] \times [\![2,s]\!] \quad \theta - t\beta_j \neq \alpha_i$$

On considère le polynôme $h \in K(\theta)[X]$ défini par

$$h(X) = P_\alpha(\theta - tX)$$

On a alors

$$h(\beta) = P_\alpha(\alpha) = 0$$

et $\forall j \in [\![2,s]\!] \quad h(\beta_j) = P_\alpha(\theta - t\beta_j) \neq 0$

Alors β est algébrique sur $K(\theta)$ et est la seule racine commune aux polynômes h et P_β de $K(\theta)[X]$.

Notons μ le polynôme irréductible de β sur $K(\theta)$.

Alors on obtient que μ divise h et P_β dans $K(\theta)[X]$.

Ainsi toute racine de μ est une racine commune à P_β et h.

Etape 4 : comme L est séparable sur K, il est aussi séparable sur $K(\theta)$. Ainsi comme β est algébrique sur $K(\theta)$, μ est séparable et n'admet que des racines simples dans M

D'où $\mu(X) = X - \beta$ et ainsi $\beta \in K(\theta)$. Puis on en déduit

$$\alpha = \theta - t\beta \in K(\theta)$$

et donc $K(\alpha, \beta) \subset K(\theta)$. On en déduit $K(\alpha, \beta) = K(\theta)$.

Suite de la récurrence :

Comme $[L:K]=n$, il existe $\alpha_1, \dots, \alpha_n$ dans L tels que

$$L = K(\alpha_1, \dots, \alpha_n)$$
$$\| = K(\alpha_1, \dots, \alpha_{n-1})(\alpha_n)$$

Par hypothèse de récurrence, il existe $\alpha \in L$ tel que

$$K(\alpha) = K(\alpha_1, \dots, \alpha_{n-1})$$

On a alors

$$L = K(\alpha)(\alpha_n) = K(\alpha, \alpha_n)$$

et le cas $n=2$ permet de conclure.

Rmq : un corps de caractéristique 0 est séparable.

Soit K un corps de caractéristique 0, $P \in K[X]$ un polynôme irréductible.

Comme P est irréductible, P est non constant.

On en déduit $P' \neq 0$ car $car(K) = 0$.

Or on a alors $\deg(P') < \deg(P)$ et donc comme P est irréductible, $P \wedge P' = 1$ dans $K[X]$.

Il suffit ensuite de remarquer que le pgcd est invariant si on le considère dans $L[X]$ avec L un corps de décomposition de K. (algo Euclide, identité de Bézout)

Exemple : on a $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$

En effet, notons α la somme $\sqrt{2} + \sqrt{3}$. Il suffit de montrer que $\sqrt{2} \in \mathbb{Q}(\alpha)$ car $\alpha - \sqrt{2} = \sqrt{3}$.

On a $\alpha^2 = 5 + 2\sqrt{2}\sqrt{3}$ d'où $\sqrt{2} = \dfrac{\alpha^2 - 1}{2\alpha} \in \mathbb{Q}(\alpha)$.