Théorème de l'élément primitif

Dorian Cacitti-Holland

2020-2021

Références.

1. Algèbre de Xavier Gourdon

Leçons.

1. 125 Exetensions de corps, exemples et applications
2. 141 Polynômes irréductibles à une indéterminée, corps de rupture, exemples et applications
3. 144 Racines d'un polynômes, fonctions symétriques élémentaires, exemples et applications
4. 151 Dimension d'un espace vectoriel (en dimension finie), rang, exemples et applications

Lemme. Soit K un corps de caractéristique nulle, en particulier K infini, L une extension de degré fini de K et $(x, y) \in L^2$, alors il existe $z \in L$ tel que

$$K(x, y) = K(z)$$

Démonstration.
Etape 1 : Utilisation d'un corps de décomposition
Comme L est une extension de degré fini de K, L est une extension algébrique de K, donc x et y sont algébriques sur K, on peut donc considérer $\mu_x \in K[X]$ et $\mu_y \in K[X]$ leurs polynômes minimaux sur K.
Puis on considère M le corps de décomposition de $\mu_x\mu_y$, en particulier M est une extension de corps de L.
Ainsi $\mu_x\mu_y$ est scindé sur M, ie il existe $(x_1, ..., x_p, y_1, ..., y_q) \in M^{p+q}$ tel que

$$\mu_x\mu_y = \prod_{i=1}^{p}(X - x_i)\prod_{j=1}^{q}(X - y_j), \mu_x = \prod_{i=1}^{p}(X - x_i), \mu_y = \prod_{i=1}^{q}(X - y_j)$$

Et comme $\mu_x(x) = 0 = \mu_y(y)$, on peut choisir $x_1 = x, y_1 = y$.
Etpae 2 : Il existe $t \in K^*$ tel que $\forall (i, i', j, j') \in [\![1, p]\!]^2 \times [\![1, q]\!]^2, x_i + ty_j \neq x_{i'} + ty_{j'}$
Comme μ_x est le polynôme minimal de x sur K, en particulier μ_x est irréductible dans $K[X]$, donc μ_x et μ_x' sont premiers entre eux dans $K[X]$ car $deg(\mu_x') < deg(\mu_x)$ et $\mu_x' \neq 0$ (car $car(K) = 0$).
Ainsi, par théorème de Bézout sur $K[X]$, il existe $U, V \in K[X] \subset M[X]$ tel que

$$U\mu_x + V\mu_x' = 1$$

Donc, par théorème de Bézout sur $M[X]$, μ_x et μ_x' sont premiers entre eux dans $M[X]$, en particulier μ_x et μ_x' n'ont aucune racine en commun, d'où μ_x n'a que des racines simples et les x_i sont distincts.
De la même façon on en déduit que les y_j sont distincts.
On peut donc considérer

$$\Gamma = \left\{ \frac{x_i - x_{i'}}{y_j - y_{j'}}, 1 \leq i, i' \leq p, 1 \leq j, j' \leq q, j \neq j' \right\}$$

Donc Γ est fini, et comme K^* est infini, il existe

$$t \in K^*, t \notin \Gamma$$

Soit $(i, i', j, j') \in [\![1, p]\!]^2 \times [\![1, q]\!]^2$ tel que $x_i + ty_i = x_{i'} + ty_{i'}$, alors :
— Si $j \neq j'$ alors $y_j \neq y_{j'}$ et $t = \frac{x_i - x_{i'}}{y_j - y_{j'}} \in \Gamma$ ce qui n'est pas.
— Si $j = j'$ alors $y_j = y_{j'}$ donc $x_i = x_{i'}$ d'où $i = i'$
Par conséquent les $x_i + ty_j$ sont distincts entre eux.
Etape 3 : Pour $z = x + ty$, le PGCD de μ_y et $\mu_x(z - tX)$ dans $K(z)[X]$ est $X - y$
On considère $z = x + ty \in L$.
Alors

$$\mu_x(z - tX) = \prod_{i=1}^{p} (z - tX - x_i)$$

Soit $a \in M$ racine de μ_y et $\mu_x(z - tX)$, alors il existe $i \in [\![1, p]\!]$ et $j \in [\![1, q]\!]$ tels que

$$a = y_j, z - ta = x_i$$

D'où

$$z = x_i + ty_j$$

Or $z = x + ty = x_1 + ty_1$, donc, d'après la seconde étape,

$$x_i = x_1 = x, a = y_j = y_1 = y$$

D'où y est la seule racine commune à μ_y et $\mu_x(z - tX)$.
Or μ_y est scindé à racines simples, donc le PGCD de μ_y et $\mu_x(z - tX)$ dans $M[X]$ est $X - y$.
Soit D le PGCD de μ_y et $\mu_x(z - tX)$ dans $K(z)[X]$, alors il existe $(P_1, P_2) \in K(z)[X]^2$ premiers entre eux tels que

$$\mu_y = P_1 D, \mu_x(z - tX) = P_2 D$$

Donc, d'après le théorème de Bézout dans $K(z)[X]$, il existe $(U, V) \in K(z)[X]^2$ tel que

$$UP_1 + VP_2 = 1$$

D'où, d'après le théorème de Bézout dans $M[X]$, P_1 et P_2 sont premiers entre eux dans $M[X]$, d'où, comme les égalités $\mu_y = P_1 D, \mu_x(z - tX) = P_2 D$ ont également lieu dans $M[X]$,

$$X - y = D \in K(z)[X]$$

Etape 4 : $K(z) = K(x, y)$
D'après l'étape précédente

$$y \in K(z)$$

De plus, comme $t \in K$,

$$x = z - ty \in K(z)$$

D'où

$$K(x, y) \subset K(z)$$

Réciproquement, comme $z = x + ty \in K(x, y)$,

$$K(z) \subset K(x, y)$$

Par conséquent $K(x, y) = K(z)$. □

Théorème. Soit K un corps de caractéristique nulle, en particulier K infini, et L une extension de degré fini de K, alors il existe $z \in L$ tel que

$$L = K(z)$$

Démonstration.
On raisonne par récurrence sur $n = [L : K] \in \mathbb{N}^*$:

— Pour $n = 1$: $L = K$, donc, pour $x = 1$, $L = K = K(1)$.

— On suppose le résultat vrai pour les extensions de degré $n - 1$, comme L est une extension de degré fini de K de degré n, il existe $(a_1, ..., a_n) \in L^n$ tel que

$$L = K(a_1, ..., a_n)$$

Or par hypothèse de récurrence il existe $x \in L$ tel que

$$K(a_1, ..., a_{n-1}) = K(x)$$

Donc

$$L = K(a_1, ..., a_{n-1})(a_n) = K(x)(a_n) = K(x, a_n)$$

D'où, d'après le lemme précédent appliqué avec $y = a_n$, il existe $z \in L$ tel que

$$L = K(x, a_n) = K(z)$$

□

Remarque. (Pas assez de temps pour le démontrer) Si K est un corps fini et L est une extension de degré fini de K, alors il existe $z \in L$ tel que

$$L = K(z)$$

Démonstration. Comme L est un K-espace vectoriel de dimension finie et K fini, L est un corps fini, donc L^* est cyclique.
Il existe donc $z \in L^*$ engendrant L^*.
Donc pour tout $x \in L$, soit $x = 0$, soit $x \in L^*$, dans ce dernier cas il existe $k \in \mathbb{N}^*$ tel que

$$x = z^k = (X^k)(z)$$

D'où, comme L est une extension algébrique de K,

$$L \subset K[z] = K(z) \subset L$$

Par conséquent $L = K(z)$. □