Théorème de l'élément primitif

Mon développement

Si x est un nombre algébrique sur K, on note P_x son polynôme minimal.

Théorème. Soit K un corps fini ou de caractéristique nulle. Toute extension de K de degré fini est monogène.

Soit L une extension de K de degré fini.

Dans le cas où K est fini, L est donc un corps fini. On sait donc que $(L^*, .)$ est un groupe cyclique. Il est alors clair que pour un générateur x de ce groupe, on a $L = K[x]$.

Dans le cas où K est de caractéristique nulle (donc infini), on considère $x, y \in L$. Il existe une extension M de L telle que P_xP_y soit scindé sur M. On peut alors écrire

$$P_x = \prod_{i=1}^{p}(X - x_i) \qquad \text{et} \qquad P_y = \prod_{i=1}^{q}(X - y_i)$$

où $x_1 = x$ et $y_1 = y$.

Le polynôme P_x est irréductible sur K donc on a $\text{pgcd}(P_x, P_x') = 1$. En effet, P_x' est non nul (car K est de caractéristique nulle) et $\deg(P_x') < \deg(P_x)$.
Le pgcd étant invariant par extension de corps, les polynômes P_x et P_x' n'ont donc aucune racine commune dans M, donc les racines de P_x dans M sont simples, donc les x_i sont distincts.
Le même raisonnement montre que les y_i sont également distincts.
L'ensemble

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

est donc bien défini et c'est un sous-ensemble fini de K^*, qui est infini. Il existe donc $t \in K^*$ tel que

$$\forall 1 \leq i, i' \leq p,\ \forall 1 \leq j \neq j' \leq q,\ x_i + ty_j \neq x_{i'} + ty_{j'}\ . \tag{1}$$

On note alors $z = x + ty$. On a $\text{pgcd}(P_y, P_x(z - tX)) = X - y$.
En effet, y est une racine commune à P_y et $P_x(z - tX)$. Réciproquement, si a est une racine commune à P_y et $P_x(z - tX)$, alors il existe $j \in [\![1, q]\!]$ tel que $a = y_j$ et il existe $i \in [\![1, p]\!]$ tel que $z - ta = x_i$, donc $z = x_i + ty_j$. Puisque $z = x_1 + ty_1$, d'après (1), on a $j = 1$ donc $a = y$. Finalement, y est l'unique racine commune à P_y et $P_x(z - tX)$, qui sont deux polynômes scindés à racines simples, donc $\text{pgcd}(P_y, P_x(z - tX)) = X - y$.

On a donc d'une part $K(z) \subset K(x, y)$ puisque $z = x + ty$. D'autre part, y appartient à $K(z)$ puisque $\text{pgcd}(P_y, P_x(z - tX)) \in K(z)[X]$, donc $x = z - ty$ appartient aussi à $K(z)$, d'où $K(x, y) \subset K(z)$. Finalement, $K(z) = K(x, y)$.

Une récurrence immédiate sur n permet de montrer que pour tous $a_1, \ldots, a_n \in L$, il existe $z \in L$ tel que $K(a_1, \ldots, a_n) = K(z)$.

Soit $(a_1, \ldots, a_n)$ une base de L sur K (finie car L est de degré fini sur K). Il existe donc $z \in L$ tel que $K(z) = K(a_1, \ldots, a_n) = L$. □

Remarque. Le théorème de l'élément primitif n'est pas valable pour un corps infini de caractéristique non nulle.

Avant de donner un contre-exemple, on démontre le lemme suivant.

Lemme. Soient k un corps et $n \in \mathbb{N}^*$. On a : $[k(X) : k(X^n)] = n$.

En effet, $k(X^n)$ est bien un sous-corps de $k(X)$. De plus, l'unique application $\varphi : k[Y] \to k[X^n]$ fixant k telle que $\varphi(Y) = X^n$ est un isomorphisme. L'anneau $A = k[X^n]$ est donc factoriel et X^n est irréductible dans A. D'après le critère d'Eisenstein appliqué au polynôme $P = Y^n - X^n$ dans $A[Y]$, P est irréductible sur le corps des fractions $k(X^n)$. L'élément X de $k(X)$, qui est une racine du polynôme P de $k(X^n)[Y]$, est donc de degré n sur $k(X^n)$, d'où le résultat. □

On va maintenant pouvoir donner un contre-exemple au théorème de l'élément primitif pour un corps infini de caractéristique non nulle. On note $L = \mathbb{F}_p(X, Y)$ le corps des fractions en deux indéterminées sur $\mathbb{F}_p$ (p premier) et $K = \mathbb{F}_p(X^p, Y^p)$.

On a les extensions de corps

$$\mathbb{F}_p(X^p, Y^p) \subset \mathbb{F}_p(X^p, Y) \subset \mathbb{F}_p(X, Y) \ .$$

D'après le lemme, on a

$$[\mathbb{F}_p(X^p, Y) : \mathbb{F}_p(X^p, Y^p)] = [\mathbb{F}_p(X^p)(Y) : \mathbb{F}_p(X^p)(Y^p)] = p$$

et

$$[\mathbb{F}_p(X, Y) : \mathbb{F}_p(X^p, Y)] = [\mathbb{F}_p(Y)(X) : \mathbb{F}_p(Y)(X^p)] = p$$

donc $[\mathbb{F}_p(X, Y) : \mathbb{F}_p(X^p, Y^p)] = p^2$.

On a donc $[L : K] = p^2$. De plus, en utilisant le morphisme de Frobenius, pour tout $x \in L$, x^p appartient à K, donc $[K(x) : K] \leq p$. L ne peut donc être une extension monogène de K, bien que de degré fini. □

Références

J'ai utilisé [Gou09, p. 89], [Ort04, p. 124]. On peut aussi consulter [Per96, p. 87].

Leçons correspondantes

J'utilise ce développement pour les leçons 116, 151. On peut également l'utiliser pour la leçon 120.

Remarques

- Ce théorème serait utile en théorie de Galois. Pour des applications plus simples, on peut consulter par exemple [FG97, p. 140] ou [Ort04, p. 125].
- Ce développement semble un peu léger pour la leçon 150.

Questions possibles

1. Justifier l'unicité de $\varphi : k[Y] \to k[X^n]$ vérifiant $\varphi(x) = x$ pour tout $x \in k$ et $\varphi(Y) = X^n$, ainsi que le fait que ce soit un isomorphisme.
2. Que dire du théorème lorsque le corps est fini ?
3. Que se passe-t-il pour un corps infini de caractéristique non nulle ?
4. Quand on dispose d'une extension monogène, peut-on trouver tous les éléments primitifs ?
5. Existe-t-il des éléments $\alpha \in \mathbb{F}_{64}$ tels que $\mathbb{F}_{64} = \mathbb{F}_2(\alpha)$? Si oui, combien en existe-t-il ?
6. Montrer que le pgcd est invariant par extension de corps.
7. Énoncer le critère d'Eisenstein.

Références

[FG97] Serge Francinou et Hervé Gianella : *Exercices de mathématiques pour l'agrégation : Algèbre 1.* Masson, 1997.

[Gou09] Xavier Gourdon : *Algèbre.* Ellipses, 2009.

[Ort04] Pascal Ortiz : *Exercices d'algèbre.* Ellipses, 2004.

[Per96] Daniel Perrin : *Cours d'algèbre.* Ellipses, 1996.