Théorème de l'élément primitif

Théo Jaudon

Lemme 1. *Soit K un corps, L une extension de K et $P, Q \in K[X]$. Le pgcd de P et Q dans $K[X]$ est le même que le pgcd de P et Q vus comme éléments de $L[X]$.*

Preuve. C'est l'unicité dans la division euclidienne qui assure que la division euclidienne de P par Q dans $K[X]$ est la même que la division euclidienne de P par Q vus comme éléments de $L[X]$. Le lemme en découle par l'algorithme d' Euclide.

Lemme 2. *Soit K un corps de caractéristique nulle, $P \in K[X]$ un polynôme irréductible et L une extension de K dans laquelle P est scindé. Alors toutes les racines de P dans L sont simples.*

Preuve. Supposons par l'absurde que $\alpha \in L$ est racine de P de multiplicité supérieur ou égal à 2. Alors le polynôme $X - \alpha$ divise P et P' dans $L[X]$ donc P et P' ne sont pas premiers entre eux dans $L[X]$. D'après le lemme précédent, P et P' ne sont donc pas premiers entre eux dans $K[X]$. Comme P est irréductible dans $K[X]$ cela implique que P divise P' dans $K[X]$ et donc que $P' = 0$ car $\deg(P') < \deg(P)$. Comme K est de caractéristique nulle, on en déduit que P est constant, d'où la contradiction.

Théorème 3. *Soit K un corps de caractéristique nulle et L une extension de K de degré fini. Alors il existe $\omega \in L$ tel que $L = K(\omega)$ autrement dit l'extension L/K est monogène.*

Preuve. Comme l'extension L/K est de dégré fini, il existe $x_1, \dots, x_n \in L$ tels que $L = K(x_1, \dots, x_n)$. On prouve le théorème par récurrence sur n, le cas $n = 1$ étant immédiat. En remarquant que $K(x_1, \dots, x_n) = K(x_1, \dots, x_{n-1})(x_n)$, il suffit de prouver le théorème lorsque $n = 2$.
On suppose donc que $L = K(x, y)$ et on va montrer qu'il existe $z \in L$ de la forme $x + ty$ avec $t \in K$ tel que $L = K(z)$. On note $\mu_x \in K[X]$ (resp. $\mu_y \in K[X]$) le polynôme minimal de x (resp. de y) sur K et on considère M un corps de décomposition de $\mu_x \mu_y$ sur K. Autrement dit M est une extension de K dans laquelle μ_x et μ_y sont scindés. D'après le lemme 2, les polynômes μ_x et μ_y sont scindés à racines simples dans M donc ils s'écrivent

$$\mu_x = \prod_{1 \leq i \leq n} (X - x_i) \qquad \text{et} \qquad \mu_y = \prod_{1 \leq j \leq m} (X - y_j)$$

où $x_1, \dots, x_n \in M$ (resp. $y_1, \dots, y_m \in M$) sont deux à deux distincts.
Le corps K étant de caractéristique nulle, il est en particulier infini donc il existe $t \in K$ qui ne soit pas dans l'ensemble

$$\left\{ \frac{x_i - x_{i'}}{y_j - y_{j'}} \quad | \quad 1 \leq i, i' \leq n \ , \ 1 \leq j, j' \leq m \text{ avec } j \neq j' \right\}$$

Par construction, toute égalité de la forme $x_i + ty_j = x_{i'} + ty_{j'}$ entraine $i = i'$ et $j = j'$. On pose alors $z = x + ty$ et on va montrer que $K(z) = K(x, y)$. Comme $z \in K(x, y)$ on a déja l'inclusion $K(z) \subset K(x, y)$. Pour obtenir l'inclusion réciproque il suffit de montrer que $y \in K(z)$ et alors on aura $x = z - ty \in K(z)$ d'où l'inclusion voulue.

On va calculer le pgcd des polynômes $\mu_y(X)$ et $\mu_x(z-tX)$ qui sont dans $K(z)[X] \subset M[X]$. D'après le lemme 1, ce dernier est égal au pgcd de $\mu_y(X)$ et $\mu_x(z-tX)$ vus comme éléments de $M[X]$. Comme les polynômes $\mu_y(X)$ et $\mu_x(X)$ sont scindés à racines simples dans M, il en va de même des polynômes $\mu_y(X)$ et $\mu_x(z-tX)$ et donc le pgcd de ces deux polynômes est le produit des $X-\lambda$ où λ est racine commune de $\mu_y(X)$ et $\mu_x(z-tX)$. Or λ est racine commune de ces deux polynômes si et seulement si il existe $(i,j) \in [\![1,n]\!] \times [\![1,m]\!]$ tel que $\lambda = y_j$ et $z = x_i + ty_j = x + ty$ si et seulement si $\lambda = y$ par construction de t. Finalement le pgcd de $\mu_y(X)$ et $\mu_x(z-tX)$ est le polynôme $X - y \in K(z)[X]$ et en particulier $y \in K(z)$.

Quelques remarques et compléments sur ce développement :

La preuve des deux lemmes peut se faire à l'oral selon la cadence de chacun.

Un élément ω tel que $L = K(\omega)$ est appelé un élément primitif. Plus fortement, on a montré que si $L = K(x_1, \ldots, x_n)$, alors il existe un élément primitif qui soit combinaison K-linéaire des x_i.

Ce théorème tire son importance du fait que les extensions monogènes sont les plus simples à appréhender et à manipuler grâce au théorème de structure concernant ces extensions. Par exemple le groupe de Galois d'une extension monogène est facile à décrire (cf. proposition 8) et plus généralement on peut construire la théorie de Galois en partant du théorème de l'élément primitif, mais d'autres approches sont possibles.

Exemple 4. *Montrons que* $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$.
L'inclusion $\mathbb{Q}(\sqrt{2}+\sqrt{3}) \subset \mathbb{Q}(\sqrt{2},\sqrt{3})$ *est évidente. Pour l'inclusion réciproque il suffit de montrer que* $\sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$. *Or* $(\sqrt{2}+\sqrt{3})^3 = 2\sqrt{2} + 6\sqrt{3} + 9\sqrt{2} + 3\sqrt{3} = 11\sqrt{2} + 9\sqrt{3}$ *d'où* $\sqrt{2} = \frac{1}{2}((\sqrt{2}+\sqrt{3})^3 - 9(\sqrt{2}+\sqrt{3})) \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$.

Le théorème de l'élément primitif est encore vrai lorsqu'on se place sur un corps fini.

Théorème 5. *Soit K un corps fini et L une extension de K de degré fini. Alors il existe $\omega \in L$ tel que $L = K(\omega)$.*

Preuve. Comme L est une extension de K de degré fini, L est un corps fini. On sait alors que le groupe multiplicatif L^* est cyclique et si $\omega \in L^*$ en est un générateur on a en particulier $L = K(\omega)$.

Remarque 6. *On a vu dans la preuve du théorème précédent que les générateurs de L^* sont des éléments primitifs mais la réciproque est fausse en général. Par exemple on peut construire le corps $\mathbb{F}_9$ comme $\mathbb{F}_9 = \mathbb{F}_3[X]/\langle X^2+1\rangle$ et on note $\alpha = \bar{X} \in \mathbb{F}_9$. Alors $(1,\alpha)$ est une base de $\mathbb{F}_9$ en tant que que $\mathbb{F}_3$-espace vectoriel et en particulier $\mathbb{F}_9 = \mathbb{F}_3(\alpha)$. Cependant on a $\alpha^2 = -1$ donc $\alpha^4 = 1$ et α n'est pas un générateur de $\mathbb{F}_9^*$ qui est d'ordre 8.*

Remarque 7. *Comme on l'a vu si on veut trouver un exemple d'extension de degré fini qui n'est pas monogène il faut se placer sur un corps infini de caractéristique $p > 0$. On considère le corps $L = \mathbb{F}_p(X,Y)$ et K le sous corps de L défini par $K = \mathbb{F}_p(X^p, Y^p)$. Par multiplicativité du degré il vient*

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

Maintenant $[\mathbb{F}_p(X,Y) : \mathbb{F}_p(X,Y^p)] = p$ *car* $(1, Y, \ldots, Y^{p-1})$ *est une base de* $\mathbb{F}_p(X,Y)$ *en tant qu'espace vectoriel sur* $\mathbb{F}_p(X,Y^p)$.
Pour une raison similaire on a $[\mathbb{F}_p(X,Y^p) : \mathbb{F}_p(X^p,Y^p)] = p$ *et donc* $[L : K] = p^2$. *Ainsi l'extension* L/K *est de degré fini, mais n'est pas monogène. En effet pour tout* $F \in L$ *on a* $F(X,Y)^p = F(X^p,Y^p) \in K$ *autrement dit* F *est annulé par le polynôme* $T^p - F(X^p,Y^p) \in K[T]$ *qui est de degré* p.

Proposition 8. *Soit* K *un corps de caractéristique nulle et* L *une extension de* K *de degré fini. Alors*

$$|Gal(L/K)| \leq [L : K]$$

où $Gal(L/K)$ *est le groupe des automorphismes du corps* L *qui fixe les éléments de* K.

Preuve. On note $n = [L : K]$. D'après le théorème de l'élément primitif il existe $\alpha \in L$ tel que $L = K(\alpha)$. Ainsi le polynôme $\mu_\alpha \in K[X]$ est irréductible de degré n, $(1, \ldots, \alpha^{n-1})$ est une base de L en tant que K espace vectoriel et en particulier

$$L = \{\ a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \quad | \quad (a_0, \ldots, a_{n-1}) \in K^n\ \}$$

Un élément $\sigma \in Gal(L/K)$ est alors entièrement déterminé par l'image de α et vérifie $\mu_\alpha(\sigma(\alpha)) = \sigma(\mu_\alpha(\alpha)) = 0$ donc $\sigma(\alpha)$ est racine de μ_α. Et réciproquement si $\beta \in L$ est racine de μ_α, alors il existe un unique $\sigma \in Gal(L/K)$ envoyant α sur β.
Autrement dit l'application

$$\begin{array}{ccc} Gal(L/K) & \to & \{\text{ racines de } \mu_\alpha \text{ dans } L\ \} \\ \sigma & \mapsto & \sigma(\alpha) \end{array}$$

est bijective. Comme μ_α est de degré n on a $|Gal(L/K)| \leq n$ avec égalité si et seulement si μ_α est scindé dans L (on a vu que les racines de μ_α sont toutes simples dans un corps de décomposition).

Remarque 9. *L'estimation précédente sur l'ordre du groupe de Galois est valable pour tout corps* K, *on peut le montrer en utilisant le lemme d'indépendance de Dedekind.*

Exemple 10. *On a* $Gal(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{\ Id,\ a + b\sqrt{2} \to a - b\sqrt{2}\ \} \simeq \mathbb{Z}/2\mathbb{Z}$ *mais* $Gal(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ *est réduit à l'identité.*

Recasages : 125, 141, 144, 142 etc ?c
Références : Gourdon, Algèbre.