Théorème d'Artin

Leçons : 125, 151, 162

Théorème 1 (*Artin*)

Si L est un corps et H est un sous-groupe fini du groupe des automorphismes de L, alors si $L^H = \{x \in L : \forall \sigma \in H, \sigma(x) = x\}$, L/L^H est une extension finie, $|H| = [L : L^H]$ et H est le groupe des L^H-automorphismes de L.

Lemme 2 (*Dedekind*)

Soient $\sigma_1, \dots, \sigma_n$ des automorphismes distincts de L, alors $(\sigma_1, \dots, \sigma_n)$ est libre sur L, c'est-à-dire que si $\forall x, \sum_{i=1}^{n} \lambda_i \sigma_i(x) = 0$, alors $\lambda_1 = \dots = \lambda_n = 0$.

Démonstration (du lemme)**.** Supposons la famille $(\sigma_1, \dots, \sigma_n)$ non libre et prenons $(\lambda_1, \dots, \lambda_n) \in L^n \setminus \{0\}$ avec un nombre minimal r de composantes non nulles tel que $\sum_{i=1}^{n} \lambda_i \sigma_i = 0$. On peut supposer sans perte de généralité que $\lambda_1, \dots, \lambda_r$ sont non nuls et $\lambda_{r+1} = \dots = \lambda_n = 0$.

Soit $y \in L$ tel que $\sigma_1(y) \neq \sigma_2(y)$. Pour tout $x \in L$, on a

$$\sum_{i=1}^{r} \lambda_i \sigma_i(x) = 0 \tag{1}$$

et par ailleurs,

$$\sum_{i=1}^{n} \lambda_i \sigma_i(xy) = \sigma_i(y) \sum_{i=1}^{r} \sigma_i(x) = 0. \tag{2}$$

Donc en effectuant (2)$-\sigma_1(y)\times$ (1), on obtient $\sum_{i=2}^{r} \lambda_i(\sigma_i(y) - \sigma_1(y))\sigma_i(x) = 0$, ce qui contredit l'hypothèse de minimalité sur r.

$\square$

Démonstration. On note $m = [L : L^H]$ (éventuellement égal à ∞) et $n = |H|$. On va vérifier dans un premier temps que $m = n$.

1 Supposons que $m < n < +\infty$. Fixons $x_1, \dots, x_m$ une base de L sur L^H et notons $H = \{\sigma_1, \dots, \sigma_n\}$. Considérons le système de m équations à n inconnues dans L, $Y_1, \dots, Y_n$ défini par

$$\forall j \in [\![1, m]\!], \sigma_1(x_j)Y_1 + \dots \sigma_n(x_j)Y_n = 0.$$

C'est un système surdéterminé donc il admet une solution non nulle $(y_1, \dots, y_n)$. Par suite, pour tout $x = \sum_{j=1}^{m} \alpha_j x_j \in L$, où $\alpha_j \in L^H$, on a

$$\sum_{i=1}^{n} \sigma_i(x) y_i = \sum_{i=1}^{n} \sum_{j=1}^{m} \alpha_j \sigma_i(x_j) y_i = \sum_{j=1}^{m} \alpha_j \left(\sum_{i=1}^{m} \sigma_i(x_j) y_i \right) = 0.$$

On a donc $\sum_{i=1}^{n} y_i \sigma_i = 0$ avec les y_i non tous nuls ce qui contredit le lemme d'indépendance de Dedekind ci-dessus. Donc $m \geqslant n$.

2 Supposons que $m > n$. Il existe donc une famille $(x_1, \ldots, x_{n+1})$ d'éléments de L libre sur L^H. Selon le même argument que pour le premier point, on peut trouver une famille non nulle $(y_1, \ldots, y_{n+1}) \in L^{n+1}$) vérifiant

$$\forall i \in [\![1, n]\!], \sigma_i(x_1)y_1 + \cdots + \sigma_i(x_{n+1})y_{n+1} = 0. \tag{3}$$

Sans perte de généralité, on peut supposer que parmi toutes les solutions non nulles, $(y_1, \ldots, y_{n+1})$ a un nombre minimal r de termes non nuls. Alors quitte à renuméroter, on peut supposer que $\forall i \leqslant r, y_i \neq 0$ et $\forall i > r, y_i = 0$. Ainsi, (2) se réécrit

$$\forall i \in [\![1, n]\!], \sigma_i(x_1)y_1 + \cdots + \sigma_i(x_r)y_r = 0.$$

Soit $\sigma \in H$, appliquons σ au système :

$$\forall i \in [\![1, n]\!], (\sigma \circ \sigma_i)(x_1)\sigma(y_1) + \cdots + (\sigma \circ \sigma_i)\sigma(y_r) = 0.$$

Comme $\tau \mapsto \sigma \circ \tau$ est une permutation de l'ensemble fini H, on a donc

$$\forall i \in [\![1, n]\!], \sigma_i(x_1)y_1 + \cdots + \sigma_i(x_r)y_r = 0. \tag{4}$$

En multipliant (2) par $\sigma(y_1)$, (4) par y_1 et en additionnant les deux systèmes, on obtient

$$\forall i \in [\![1, n]\!], \sigma_i(x_2)(\sigma(y_1)y_2 - \sigma(y_2)y_1) + \cdots + \sigma_i(x_r)(\sigma(y_1)y_r - \sigma(y_r)y_1) = 0.$$

L'entier r étant le nombre minimal de termes non nuls d'une solution non triviale de (2), on a $\forall j \in [\![2, r]\!], \sigma(y_1)y_j - y_1\sigma(y_j) = 0$, soit $\sigma(y_1 y_j^{-1}) = y_1 y_j^{-1}$ donc $\forall j \in [\![2, r]\!], y_1 y_j^{-1} \in L^H$.

Ainsi pour tout $2 \leqslant j \leqslant r$, il existe $z_j \in (L^H)^*$ tel que $y_j = z_j y_1$.

La ligne de (2) correspondant à $\sigma_i = \mathrm{id}_L$ devient alors

$$x_1 y_1 + x_2 z_2 y_1 + \cdots + x_r z_r y_1 = 0$$

donc comme $y_1 \neq 0$, on a $x_1 + x_2 z_2 + \cdots + x_r z_r = 0$, de sorte que $(x_1, \ldots, x_r)$ est une famille liée, ce qui contredit l'hypothèse initiale. Donc $m \leqslant n < +\infty$ et finalement $m = n$.

3 Notons G le groupe des L^H-automorphismes de L. Il contient H de manière évidente. Montrons que G est fini. Soit $(a_1, \ldots, a_n)$ une base de L sur L^H, $\Pi_1, \ldots, \Pi_r$ les polynômes minimaux respectifs des a_i sur L^H et $f = \Pi_1 \ldots \Pi_r \in L^H[X]$. Soit R l'ensemble (fini) des racines de f dans L. Comme $\Pi_j(a_j) = 0$ pour tout j, R contient $\{a_1, \ldots a_n\}$.

De plus, si $x = \sum_{i=1}^{n} \alpha_i a_i \in L$, où $\alpha_i \in L^H$, alors, pour tout élément σ de G, on a $\sigma(x) = \sum_{i=1}^{n} \alpha_i \sigma(a_i)$. Cela nous assure que $\psi : \begin{array}{ccc} G & \longrightarrow & \mathfrak{S}(R) \\ \sigma & \longmapsto & \sigma_{|R} \end{array}$ est injective et donc que G est fini.

On a $L^H \subset L^G \subset L$ par définition de G, et $L^G \subset L^H \subset L$ car $H \subset G$ donc $L^H = L^G$. Selon la conclusion du deuxième point, on a $|G| = [L : L^H] = [L : L^G] = |H|$ donc $G = H$.

$\square$

Quelques précisions supplémentaires : ce développement s'inscrit dans une théorie plus générale, la théorie de Galois. Étant donné une extension de corps L/K, on s'intéresse à son *groupe de Galois* $\mathrm{Gal}(L/K)$ qui est le groupe des K-automorphismes de corps de L. Le résultat majeur de cette théorie est la correspondance de Galois entre les corps intermédiaires $K \subset M \subset L$ et les sous-groupes H de $\mathrm{Gal}(L/K)$:

Théorème 3

> *Si L/K est une extension galoisienne, les applications* $\mathrm{Fix} : H \mapsto L^H$ *et* $\mathrm{Gal} : M \mapsto \mathrm{Gal}(L/M)$ *sont réciproques l'une de l'autre, où L^H, comme défini dans l'énoncé du théorème d'Artin est appelé* sous-corps fixe *de L associé à H.*

Il est remarquable qu'en vertu du théorème d'Artin, toute extension finie vérifie $\mathrm{Gal} \circ \mathrm{Fix} = \mathrm{id}$.

Définition 4

> *Soit L/K une extension algébrique. On dit que c'est une extension* galoisienne *si $L^{\mathrm{Gal}(L/K)} = K$.*

On suppose à présent que K est un corps parfait, c'est-à-dire que si L/K est une extension algébrique, alors tout polynôme de $L[X]$ n'admet que des racines simples dans son corps de décomposition – L est dit *séparable*. La plupart des corps usuels sont parfaits : $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, les corps finis. En revanche pour p premier, $\mathbb{F}_p(T)$ n'est pas parfait.

Définition 5

> *L'extension algébrique L/K est dite* normale *si tout polynôme* ***irréductible*** *$f \in K[X]$ admettant une racine dans L se décompose en produit de facteurs de degré 1 dans L.*

Par exemple $\mathbb{C}/\mathbb{R}$ est une extension normale.

Proposition 6

> *Soit L/K une extension finie, alors on a l'équivalence entre :*
>
> ***1*** *L/K est galoisienne ;*
>
> ***2*** *L/K est normale ;*
>
> ***3*** *L est le corps de décomposition d'un polynôme $f \in K[X]$;*
>
> ***4*** $\mathrm{Gal}(L/K)$ *est d'ordre* $[L : K]$.

En particulier si L/K est galoisienne finie et $K \subset M \subset L$ est un corps intermédiaire, alors L/M est galoisienne puisque L est le corps de décomposition de $f \in K[X] \subset M[X]$, ce qui prouve la correspondance de Galois.

Remarque.
- C'est un peu long pour 15 minutes, il vaut mieux démontrer le lemme de Dedekind que le dernier point de la démonstration du théorème.
- Pour bien se souvenir du système à poser à chaque étape, retenir qu'un système surdéterminé, c'est **plus d'inconnues que d'équations**.

Références :

- Alain JEANNERET et Daniel LINES (2008). *Invitation à l'algèbre*. Editions Cépaduès, p. 297.
- Voir également Pierre SAMUEL (1967). *Théorie algébrique des nombres*. Hermann pour la théorie de Galois.