2.13 Théorème d'Artin

Références : A. Jeanneret, D. Lines, *Invitation à l'algèbre*, Cépaduès, 2008, J. Calais, *Extensions de corps, théorie de Galois*, Ellipses, 2006.

Leçons concernées : 125, 151, 162.

Théorème 1 (Artin). [1] *Soit L un corps et soit H un sous-groupe fini du groupe des automorphismes de L. Alors si on note $L^H := \{x \in L \mid \sigma(x) = x,\ \forall \sigma \in H\}$, L/L^H est une extension finie de degré $[L : L^H] = |H|$.*

Lemme 2 (Dedekind). *Soit $n \geqslant 1$, K, L deux corps, et soit $\varphi_1, \dots, \varphi_n : K \to L$ n homomorphismes de corps distincts. Alors $(\varphi_1, \dots, \varphi_n)$ est libre sur L.*

Démonstration. On suppose par l'absurde que $(\varphi_1, \dots, \varphi_n)$ n'est pas libre et on se donne $(\lambda_1, \dots, \lambda_n) \in L^n \backslash \{0\}$ avec un nombre minimal r d'éléments non nuls tel que $\sum_{i=1}^n \lambda_i \varphi_i = 0$. On remarque que nécessairement $r \geqslant 2$, et quitte à renuméroter, on peut supposer que $\lambda_1, \dots, \lambda_r \neq 0$ et $\sum_{i=1}^r \lambda_i \varphi_i = 0$. Soit $y \in K$ tel que $\varphi_1(y) \neq \varphi_2(y)$. On a, pour $x \in K$,

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

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

On réalise alors $(2) - \varphi_1(y) \times (1)$ et on obtient

$$\sum_{i=2}^{r} \lambda_i \big(\varphi_1(y) - \varphi_i(y)\big)\varphi_i = 0$$

ce qui nous fournit une contradiction par minimalité puisque $\lambda_2(\varphi_1(y) - \varphi_2(y)) \neq 0$. □

Démonstration (Théorème). On pose $m = [L : L^H]$ (éventuellement infini) et $n = |H|$. On veut montrer que $m = n$.

Étape 1 : $m \geqslant n$. On suppose par l'absurde que $m < n$. On se donne $(x_1, \dots, x_m)$ une L^H-base de L et on note $\sigma_1, \dots, \sigma_n$ les éléments de H. On considère le système d'équations

$$\sigma_1(x_j)y_1 + \cdots + \sigma_n(x_j)y_n = 0, \quad j \in [|1, m|].$$

Puisque le nombre d'inconnues est strictement supérieur au nombre d'équations, il existe une solution non nulle $(y_1, \dots, y_n)$ au système. Alors, pour tout $x = \sum_{j=1}^m \lambda_j x_j \in L$ avec $\lambda_j \in L^H$,

$$\sum_{i=1}^{n} y_i \sigma_i(x) = \sum_{i=1}^{n} \sum_{j=1}^{m} y_i \sigma_i(x_j)\lambda_j = \sum_{j=1}^{m} \lambda_j \Big(\sum_{i=1}^{n} y_i \sigma_i(x_j) \Big) = 0$$

1. D'après le mathématicien autrichien Emil Artin ([artin]).

ce qui est absurde d'après le lemme précédent.

Étape 2 : $m \leqslant n$. On suppose par l'absurde que $m > n$, alors il existe une famille $(x_1, \dots, x_{n+1})$ de L libre sur L^H. Par le même raisonnement que précédemment, il existe une famille non nulle $(y_1, \dots, y_{n+1})$ de L telle que

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

On choisit $(y_1, \dots, y_{n+1})$ tel que le nombre r de ses composantes non nulles soit minimal, et quitte à renuméroter on suppose que $y_1, \dots, y_r \neq 0$ et $y_{r+1}, \dots, y_{n+1} = 0$, et on suppose que $y_1 = 1$, ce qui nous donne le système

$$\sigma_i(x_1) + \cdots + \sigma_i(x_r)y_r = 0, \quad \forall i \in [|1, n|]. \tag{3}$$

On fait alors agir $\sigma \in H$ sur le système, pour obtenir

$$\sigma(\sigma_i(x_1)) + \cdots + \sigma(\sigma_i(x_r))\sigma(y_r) = 0, \quad \forall i \in [|1, n|]$$

et puisque $\tau \mapsto \sigma \circ \tau$ réalise une permutation des éléments de H le dernier système est équivalent à

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

On réalise alors (3) − (4) ce qui nous donne

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

On a alors, par minimalité de r, $y_j - \sigma(y_j) = 0$ pour $j \in [|2, r|]$, c'est-à-dire que pour tout $j \in [|2, r|]$, $y_j \in L^H$. L'équation (3) pour $i \in [|1, n|]$ tel que $\sigma_i = \mathrm{id}_L$ devient alors

$$x_1 + x_2y_2 + \cdots + x_ry_r = 0$$

ce qui nous fournit une absurdité, par hypothèse sur $(x_1, \dots, x_{n+1})$ puisque $y_j \in L^H$. □

Corollaire 3. *Soit L un corps et soit H un sous-groupe fini du groupe des automorphismes de L. Alors H est le groupe des L^H-automorphismes de L, c'est-à-dire* $\mathrm{Gal}(L/L^H) = H$.

Démonstration. On note $G = \mathrm{Gal}(L/L^H)$. On a immédiatement $H \subset G$. Montrons que G est fini. Soient $a_1, \dots, a_n$ une L^H-base de L, m_i les polynômes minimaux sur L^H respectifs des a_i, et $f = m_1 \cdots m_n$. On note R l'ensemble des racines de f dans L. R contient évidemment $\{a_1, \dots, a_n\}$, et donc puisqu'ils constituent une L^H-base de L, $\sigma \in G$ est entièrement déterminé par ses valeurs sur R. Ainsi, l'application

$$\begin{array}{ccc} G & \to & \mathfrak{S}(R) \\ \sigma & \mapsto & \sigma_{|R} \end{array}$$

est injective, et donc puisque R étant fini, $\mathfrak{S}(R)$ est fini, G est fini.

Or on a les inclusions $L^H \subset L^G \subset L$ par définition de G, et $L^G \subset L^H \subset L$ car $H \subset G$. Ainsi $L^G = L^H$, et le théorème précédent appliqué à G et H nous donne

$$|G| = [L : L^G] = [L : L^H] = |H|$$

et donc $G = H$. □

Ce théorème s'inscrit dans la théorie de Galois, dont nous donnons quelques éléments afin de mettre en contexte le sujet.

Définition 4. On rappelle que si L/K est une extension de corps, on note $\mathrm{Gal}(L/K)$ l'ensemble des K-automorphismes de L, c'est-à-dire

$$\mathrm{Gal}(L/K) = \big\{\sigma \in \mathrm{Aut}(L) \mid \sigma_{|K} = \mathrm{id}_K \big\}.$$

Étant donné une extension L/K, on note $\mathcal{F}$ l'ensemble des corps intermédiaires de L/K et $\mathcal{H}$ l'ensemble des sous-groupes de $\mathrm{Gal}(L/K)$. Pour $H \in \mathcal{H}$, on note $\mathrm{Inv}(H)$ le sous-corps fixe de L par H l'ensemble

$$\mathrm{Inv}(H) = \big\{x \in L \mid \forall \sigma \in H, \sigma(x) = x\big\}.$$

On vérifie que $\mathrm{Inv}(H)$ est un corps intermédiaire de L/K pour tout $H \in \mathcal{H}$ et que pour tout $F \in \mathcal{F}$, $\mathrm{Gal}(L/F)$ est un sous-groupe de $\mathrm{Gal}(L/K)$. On peut donc considérer les applications

$$\mathrm{Gal} : \begin{array}{ccc} \mathcal{F} & \to & \mathcal{H} \\ F & \mapsto & \mathrm{Gal}(L/F) \end{array}, \qquad \mathrm{Inv} : \begin{array}{ccc} \mathcal{H} & \to & \mathcal{F} \\ H & \mapsto & \mathrm{Inv}(H). \end{array}$$

Définition 5. On dit qu'une extension L/K est galoisienne si elle est algébrique et que $K = \mathrm{Inv}(\mathrm{Gal}(L/K))$.

Le théorème d'Artin permet de montrer un premier théorème qui caractérise les extensions galoisiennes de degré fini.

Théorème 6. *Pour toute extension L/K, les assertions suivantes sont équivalentes*

(i) *L/K est galoisienne de degré fini*

(ii) *L/K est de degré fini, normale et séparable*

(iii) *$\mathrm{Gal}(L/K)$ est fini et $K = \mathrm{Inv}(\mathrm{Gal}(L/K))$.*

Lorsqu'une de ces conditions est vérifiée on a de plus $|\mathrm{Gal}(L/K)| = [L : K]$.

Exemple. (i) Les extension $\mathbb{C}/\mathbb{R}$ et $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ sont galoisiennes.

(ii) L'extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ n'est pas normale donc n'est pas galoisienne.

Le théorème permet également d'obtenir la proposition suivante.

Proposition 7 (correspondance de Galois)**.** *Pour toute extension L/K, les deux assertions suivantes sont équivalentes*

(i) L/K *est galoisienne de degré fini*

(ii) L/K *est de degré fini et les applications* Gal *et* Inv *sont des bijections réciproques l'une de l'autre.*

Démonstration (partielle). L'implication $(ii) \Rightarrow (i)$ est évidente. On montre que si on suppose (i), alors $\mathrm{Gal} \circ \mathrm{Inv} = \mathrm{Id}$. D'après le théorème précédent, par hypothèse, $\mathrm{Gal}(L/K)$ est fini, ainsi, tout $H \in \mathcal{H}$ est fini, et on peut donc lui appliquer le corollaire du théorème d'Artin pour obtenir $H = \mathrm{Gal}(L/\mathrm{Inv}(H)) = \mathrm{Gal} \circ \mathrm{Inv}(H)$. □

On donne enfin le théorème central de la théorie de Galois.

Théorème 8 (fondamental de la théorie de Galois)**.** *Soit L/K est extension galoisienne de degré fini. Si F est un corps intermédiaire pour cette extension, alors*

(1) L/F *est une extension galoisienne de degré fini*

(2) $[F : K] = [\mathrm{Gal}(L/K) : \mathrm{Gal}(L/F)]$

(3) les assertions suivantes sont équivalentes

(i) F/K *est normale*

(ii) $\mathrm{Gal}(L/F) \lhd \mathrm{Gal}(L/K)$

(iii) F/K *est galoisienne.*

Remarque. La théorie de Galois a de nombreuses applications, notamment dans l'étude des polygones constructibles, et la résolution des équations par radicaux.

Commentaire : voir aussi les notes de J. Le Borgne sur le sujet.