Le lemme d'Artin.

Lemme (Dedekind)**.** *Soient $n \geq 1$ et $\varphi_1, \dots \varphi_n : \mathbf{L} \to \mathbf{K}$ des homorphismes de corps distincts entre les corps $\mathbf{K}$ et $\mathbf{L}$. Alors le système engendré par les $\varphi_1, \dots, \varphi_n$ est libre :*

$$\left[\forall x \in \mathbf{K},\ \sum_{i=1}^{n} \alpha_i \varphi_i(x) = 0\ \right] \implies \alpha_1 = \ldots = \alpha_n = 0.$$

Preuve. Raisonnons par l'absurde. Comme un homomorphisme de corps n'est jamais nul, on considère $r \geq 2$ le nombre minimal tel que, quitte à re-numéroter les φ_i, il existe une relation de dépendance linéaire :

$$\forall x \in \mathbf{K},\ \sum_{i=1}^{r} \alpha_i \varphi_i(x) = 0. \tag{1}$$

Puisque $\varphi_1 \neq \varphi_r$, il existe $y \in \mathbf{K}$ tel que $\varphi_1(y) \neq \varphi_r(y)$. On a :

$$\forall x \in \mathbf{K},\ \sum_{i=1}^{r} \alpha_i \varphi_i(yx) = \sum_{i=1}^{r} \alpha_i \varphi_i(y)\varphi_i(x) = 0. \tag{2}$$

Il suffit d'opérer : (2)$\leftarrow$(2)$-\varphi_1(y)\times$(1) et on conclut :

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

ce qui contredit la minimalité de r. □

Lemme (Artin)**.** *Soient $\mathbf{L}$ est un corps et H un sous-groupe fini de* $\mathrm{Aut}(L)$*. Alors l'extension $\mathbf{L}/\mathbf{L}^H$ est un extension finie de degré $[\mathbf{L} : \mathbf{L}^H] = |H|$.*

Preuve. On note une bonne fois pour toutes :

$$m = [\mathbf{L} : \mathbf{L}^H] \in \mathbf{N} \cup \{\infty\}, \quad n = |H| < \infty \quad \text{et} \quad H = \{\sigma_1, \dots, \sigma_n\}.$$

Étape 1. On montre que $n \leq m$.

Par l'absurde, on suppose que $m < n < \infty$ et on considère $x_1, \dots, x_m$ une $\mathbf{L}^H$-base de $\mathbf{L}$. La matrice des $(\sigma_j(x_i))_{i,j}$ est de taille $m \times n$ avec $m < n$ donc il existe une solution $(y_1, \dots, y_n)$ non nulle au système :

$$\forall i \in \{1, \dots, m\},\ \sum_{j=1}^{n} \sigma_j(x_i) y_j = 0.$$

Comme les $x_1, \ldots, x_m$ forment une $\mathbf{L}^H$-base de $\mathbf{L}$ on a obtenu une relation de dépendance linéaire entre les σ_j car si $x = \sum_{i=1}^{m} \alpha_i x_i \in \mathbf{L}$ avec $\alpha_i \in \mathbf{L}^H$, on a :

$$\sum_{j=1}^{n} y_j \sigma_j(x) = \sum_{j=1}^{n} \sum_{i=1}^{m} y_j \alpha_i \sigma_j(x_i) = \sum_{i=1}^{m} \alpha_i \sum_{j=1}^{m} \sigma_j(x_i) y_j = 0.$$

Ce qui contredit le lemme de Dedekind. Donc $n \leq m$.

Étape 2. On montre que $m \leq n$.

Toujours par l'absurde, on suppose que $n < m \in \mathbf{N} \cup \{\infty\}$. C'est dire qu'il existe $n+1$ éléments $x_1, \ldots, x_{n+1} \in \mathbf{L}$ linéairement indépendants sur $\mathbf{L}^H$. Comme tout à l'heure, il existe une solution $(y_1, \ldots, y_{n+1})$ non nulle au système :

$$\forall i \in \{1, \ldots, n\}, \ \sum_{j=1}^{n+1} \sigma_i(x_j) y_j = 0.$$

Quitte à re-numéroter les y_j, on peut supposer que le système est de rang r et se ré-écrit :

$$\forall i \in \{1, \ldots, n\}, \ \sum_{j=1}^{r} \sigma_i(x_j) y_j = 0. \tag{3}$$

En faisant opérer $\sigma \in H$ sur ce système, ce système est équivalent à :

$$\forall i \in \{1, \ldots, n\}, \ \sum_{j=1}^{r} \sigma_i(x_j) \sigma(y_j) = 0. \tag{4}$$

Maintenant on écrit $\sigma(y_1) \times (3) - y_1 \times (4)$ et on obtient :

$$\forall i \in \{1, \ldots, r\}, \ \sum_{j=2}^{r} \sigma_i(x_j)(y_j \sigma(y_1) - \sigma(y_j) y_1) = 0.$$

Par minimalité de r, on en déduit :

$$\forall j \in \{2, \ldots, r\}, \ y_j \sigma(y_1) - \sigma(y_j) y_1 = 0 \quad \textit{i.e.} \ \ y_j y_1^{-1} \in \mathbf{L}^H.$$

On peut conclure : en notant $y_j = y_1 z_j$ avec $z_j \in \mathbf{L}^H$, le système (3) donne pour l'indice i tel que $\sigma_i = id_{\mathbf{L}}$:

$$\sum_{j=1}^{r} x_j y_1 z_j = 0 \ \text{ donc } \ \sum_{j=1}^{r} x_j z_j = 0$$

car $y_1 \neq 0$. Mais c'est impossible car les x_j sont linéairement indépendants. □

Corollaire. *Soient* $\mathbf{L}$ *un corps et* H *un sous-groupe fini de* $\mathrm{Aut}(\mathbf{L})$*. Alors* $\mathbf{L}/\mathbf{L}^H$ *est finie et*

$$H = \mathrm{Aut}(\mathbf{L}/\mathbf{L}^H).$$

PREUVE. On note $G = \mathrm{Aut}(\mathbf{L}/\mathbf{L}^H)$. On a déjà $H \subset G$.

(1) Comme $\mathbf{L}/\mathbf{L}^H$ est une extension finie, G est un groupe fini. En effet, si $a_1, \ldots, a_n$ est une $\mathbf{L}^H$-base de $\mathbf{L}$, on peut considérer

$$P = P_1 \ldots P_r$$

où les P_i sont les polynômes minimaux des a_i sur $\mathbf{L}^H$. On appelle R l'ensemble des racines de P contenue dans $\mathbf{L}$. Alors l'application :

$$\Psi : G \longrightarrow \mathrm{Bij}(R), \;\; \sigma \longmapsto \sigma|_R$$

est un homomorphisme injectif et comme R est fini, il en est de même pour $\mathrm{Bij}(R)$ et pour G.

(2) Regardons les inclusions :

$$\mathbf{L}^G \subset \mathbf{L}^H \subset \mathbf{L} \;\text{ et }\; \mathbf{L}^H \subset \mathbf{L}^G \subset \mathbf{L}$$

où le deuxième triptyque d'inclusions provient du fait que $\mathbf{L}^{\mathrm{Aut}(\mathbf{L}/\mathbf{L}^H)}$ est un corps intermédiaire (c'est presque la définition).

(3) Finalement, $\mathbf{L}^G = \mathbf{L}^H$ et par le théorème précédent :

$$|G| = [\mathbf{L} : \mathbf{L}^G] = [\mathbf{L} : \mathbf{L}^H] = |H|$$

et comme $H \subset G$, on conclut $G = H$.

□

Sur la théorie de Galois.

Le lemme d'Artin est une étape cruciale du théorème de correspondance de Galois :

Théorème (Galois)**.** *Soit* $\mathbf{L}/\mathbf{K}$ *une extension finie galoisienne*[1]*. Alors, entre autres choses, il y a une bijection*

$$\{\textit{corps intermédiaire de } \mathbf{L}/\mathbf{K}\} \longrightarrow \{\textit{sous-groupe de } \mathrm{Gal}(\mathbf{L}/\mathbf{K})\}$$

donnée par :

$$\mathit{Gal} : \mathbf{M} \mapsto \mathrm{Gal}(\mathbf{L}/\mathbf{M}) \;\; \textit{et} \;\; \mathit{Fix} : H \mapsto \mathbf{L}^H.$$

1. C'est à dire une extension normale (tout polynôme irréductible dans $\mathbf{K}[X]$ qui a une racine dans $\mathbf{L}$ a toutes ses racines dans $\mathbf{L}$) et séparable (tout polynôme irréductible dans $\mathbf{K}$ ou dans $\mathbf{L}$ n'a que des racines simples dans son corps des racines). C'est équivalent à dire que $\mathbf{L}/\mathbf{K}$ est algébrique et

$$\mathbf{L}^{\mathrm{Gal}(\mathbf{L}/\mathbf{K})} = \mathbf{K}$$

où on note plus volontier $\mathrm{Aut}(\mathbf{L}/\mathbf{K}) \equiv \mathrm{Gal}(\mathbf{L}/\mathbf{K})$. C'est aussi équivalent à dire que $\mathbf{L}$ est le corps des racines d'un polynôme de $\mathbf{K}[X]$ ou encore que $|\,\mathrm{Gal}(\mathbf{L}/\mathbf{K})| = [\mathbf{L} : \mathbf{K}]$.

Le corollaire du lemme d'Artin dit que $Gal \circ Fix(H) = H$. Dans l'autre sens c'est plus un peu plus conceptuel mais c'est aussi plus simple : il suffit de voir que si $\mathbf{K} \subset \mathbf{M} \subset \mathbf{L}$ alors $\mathbf{L}/\mathbf{M}$ est une extension galoisienne [2] donc $\mathbf{L}^{\mathrm{Gal}(\mathbf{L}/\mathbf{M})} = \mathbf{M}$, *i.e.* $Fix \circ Gal(\mathbf{M}) = \mathbf{M}$.

Après, il s'agit aussi de montrer le lien entre les sous-groupes normaux de $\mathrm{Gal}(\mathbf{L}/\mathbf{K})$ et les corps intermédiaires $\mathbf{M}$ tels que $\mathbf{M}/\mathbf{K}$ est galoisienne.

Référence. A. Jeanneret, D. Lines, *Invitation à l'Algèbre*

125 Extensions de corps. Exemples et applications.
151 Dimension d'un espace vectoriel (on se limitera au cas de la dimension finie). Rang. Exemples et applications.
162 Systèmes d'équations linéaires ; opérations élémentaires, aspects algorithmiques et conséquences théoriques.

2. Si $\mathbf{M}$ est un corps intermédiaire de $\mathbf{L}/\mathbf{K}$, alors, puisque $\mathbf{L}/\mathbf{K}$ est galoisienne, $\mathbf{L}$ est le corps des racines d'un certain $P \in \mathbf{K}[X]$. C'est aussi le corps des racines de ce même polynôme vu dans $\mathbf{M}[X]$ donc $\mathbf{L}/\mathbf{M}$ est galoisienne.