Théorème d'Artin et application

Antoine Dequay

21 septembre 2022

Notes

— Prof : .

— Leçons : 141, 162.

— Références :

  — Le Barbenchon.

Notation Dans toute la suite, E et F désigneront des corps et G un sous-groupe fini de $\mathrm{Aut}(E)$.

On notera le corps fixe de G dans E (l'ensemble des points de E fixés par G) :

$$E^G = \{\alpha \in E, \forall \sigma \in G, \sigma(\alpha) = \alpha\}$$

Dans la suite, E/F désigne une extension de corps et $\mathrm{Aut}(E/F)$ le groupe des F-automorphismes de E, i.e. le groupe des automorphismes de E qui fixent F.

Proposition 1 Soit E une extension finie de F et L une extension de F. Il existe au plus $[E : F]$ différents F-morphismes de E dans L.

Preuve. **Lemme 2** Soit α un nombre algébrique sur F, de polynôme minimal P et K une extension de F. Soit $\phi_0 : F \to K$ un morphisme de corps. Alors il existe une correspondance bijective ψ :

$$\psi : \left(\begin{array}{ccc} \left\{ \begin{array}{c} \text{Prolongements de } \phi_0 \\ \phi : F[\alpha] \to K \end{array} \right\} & \xrightarrow{\sim} & \left\{ \begin{array}{c} \text{Racines de } \phi_0(P) \\ \text{dans } K \end{array} \right\} \\ \phi & \longmapsto & \phi(\alpha) \end{array} \right)$$

Preuve. Soit $\phi : F[\alpha] \to K$ un morphisme de corps qui prolonge ϕ_0. Montrons que $\phi(\alpha)$ est une racine de $\phi_0(P)$. Avec $P = \sum_{i=0}^{n} a_i X^i$, $(a_i)_{i \in [\![1,n]\!]} \in F^n$ et $n = deg(P) \in \mathbb{N}$, on a :

$$\phi(P) = \phi\left(\sum_{i=0}^{n} a_i X^i\right) = \sum_{i=0}^{n} \phi(a_i) X^i = \sum_{i=0}^{n} \phi_0(a_i) X^i = \phi_0\left(\sum_{i=0}^{n} a_i X^i\right) = \phi_0(P)$$

On a donc, par propriété des morphismes de corps :

$$\phi_0(P)(\alpha) = \phi(P)(\alpha) = \phi(P(\alpha)) = 0$$

donc $\phi(\alpha)$ est bien une racine de $\phi(P) = \phi_0(P)$. L'application ψ est donc bien définie.

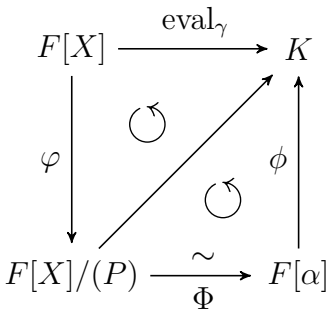
Montrons que ψ est surjective. Soit $\gamma \in K$ une racine de $\phi_0(P)$. L'application

$$\mathrm{eval}_\gamma : \left(\begin{array}{ccc} F[X] & \longrightarrow & K[\gamma] \\ Q(X) & \longmapsto & \phi_0(Q)(\gamma) \end{array} \right)$$

contient l'idéal (P) dans son noyau, et se factorise donc par le quotient $F[X]/(P)$. En considérant

$$\Phi : \left(\begin{array}{ccc} F[X]/(P) & \xrightarrow{\sim} & F[\alpha] \\ X + (P) & \longmapsto & \alpha \end{array} \right)$$

on obtient $\phi : F[\alpha] \to K$:



L'application ϕ ainsi définie est bien un morphisme prolongeant ϕ_0 et tel que $\phi(\alpha) = \gamma$.

Montrons enfin que ψ est injective. Soient ϕ, ϕ' deux morphismes qui étendent ϕ_0 et qui ont la même valeur en α. Il sont alors nécessairement égaux sur $F[\alpha]$ et donc égaux en tant que morphismes, ce qui termine la preuve de la bijectivité.

□

Lemme 3 Soit E une extension finie de F engendrée par les racines d'un polynôme $P \in F[X]$ et soit K une extension de F. Le nombre de F-morphismes $\phi : E \to K$ est inférieur à $[E : F]$.

Preuve. On raisonne par récurrence sur le nombre $n \in \mathbb{N}^*$ de racines de P.

— Initialisation : Pour $n = 1$, on a $E = F[\alpha_1]$. Soit $P_1 \in F[X]$ le polynôme minimal de α_1. Par le lemme 2, il y a au plus $deg(P_1) = [F[\alpha_1] : F] = [E : F]$ tels prolongements.

— On suppose l'hypothèse de récurrence prouvée pour un certain $n \in \mathbb{N}^*$. Montrons la au rang $n+1$: On note $E = F[\alpha_1, \ldots, \alpha_{n+1}]$. Un morphisme $E \to K$ est en particulier un morphisme qui étend le morphisme $F[\alpha_1, \ldots, \alpha_n]$ sous-jacent. Soit $P \in F[\alpha_1, \ldots, \alpha_n][X]$ le polynôme minimal de α_{n+1}. Par le lemme 2, il y a au plus
deg(P) $= [F[\alpha_1, \ldots, \alpha_{n+1}] : F[\alpha_1, \ldots, \alpha_n]]$ tels prolongements. Par hypothèse de récurrence, il y a au plus $[F[\alpha_1, \ldots, \alpha_n] : F]$ morphismes à prolonger. Par multiplicativité de l'indice, il y a donc bien au plus $[F[\alpha_1, \ldots, \alpha_{n+1}] : F]$ F-morphismes $E \to K$, ce qui permet de conclure.

□

On note $E = F[\alpha_1, \ldots, \alpha_n]$ et P le produit des polynômes minimaux des α_i. On note K le corps de décomposition de P considéré dans $L[X]$. comme K contient L, un F morphisme $E \to K$ est en particulier un F-morphisme $E \to L$.

Par le lemme 3, il existe au plus $[E : F]$ F-morphismes $E \to K$, donc au plus $[E : F]$ F-morphismes $E \to L$.

□

Théorème 4 (Théorème d'Artin)

$$\left[E : E^G\right] \leq |G|$$

Preuve. On note $G = \{\sigma_i\}_{i\in[\![1,m]\!]}$ avec $\sigma_1 = Id_E$, $m \in \mathbb{N}^*$. On suppose par l'absurde que $n = \left[E : E^G\right] > |G|$. Soit donc $\alpha_1, \dots, \alpha_n$ une base de E sur E^G, avec $n > m$. Montrons que les α_i sont linéairement indépendants sur E^G. On considère :

$$\left\{\sum_{i=1}^{n} \sigma_j(\alpha_i)X_i = 0\right._{\left.j\in[\![1,m]\!]\right.} \tag{1}$$

Ce système étant sous-déterminé, il admet des solutions non-triviales sur E. Soit $(c_i)_{i\in[\![1,n]\!]}$ une telle solutions, telle que $\#\{c_i \neq 0, i \in [\![1,n]\!]\}$ soit minimal. Qui à renuméroter, on peut supposer $c_1 \neq 0$. Quitte à multiplier par une constante, on peut supposer $c_1 \in E^G$. Montrons qu'il est est de même pour tous les c_i.

Pour $k \in [\![1,m]\!]$, en appliquant σ_k au système, puisque σ_k permute les éléments de G (ici permute les lignes...), on a :

$$\left\{\sigma_j(\alpha_1)c_1 + \sum_{i=2}^{n} \sigma_j(\alpha_i)\sigma_k(c_i) = 0\right._{\left.j\in[\![1,m]\!]\right.} \tag{2}$$

En soustrayant (2) à (1) appliquée à $(c_i)_{i\in[\![1,n]\!]}$, on trouve que $(0, \sigma_k(c_i) - c_i)_{i\in[\![2,n]\!]}$ est solution (1). Par minimalité de $\#\{c_i \neq 0, i \in [\![1,n]\!]\}$, on en déduit que $\forall i \in [\![2,n]\!]$, $\sigma_k(c_i) = c_i$. Ceci étant vrai pour tout $k \in [\![1,m]\!]$, on en déduit que les c_i sont dans E^G. L'équation de (1) associée à $j = 1$ s'écrit

$$\sum_{i=1}^{n} \alpha_i c_i$$

et est donc une relation de dépendance linéaire entre les α_i dans E^G. Cela contredit la définition des α_i comme base de E dans E^G, d'où $n \leq m$, et donc $\left[E : E^G\right] \leq |G|$.

□

Théorème 5 Pour tout groupe fini $G \subset \mathrm{Aut}(E)$, $G = \mathrm{Aut}\left(E/E^G\right)$.

Preuve. Par définition de E^G, on a $G \subseteq \mathrm{Aut}\left(E/E^G\right)$. Il reste à prouver l'égalité des cardinaux.

Par le lemme 2, la propriété et le théorème d'Artin, on a :

$$\left[E : E^G\right] \leq |G| \leq \left|\mathrm{Aut}\left(E/E^G\right)\right| \leq \left[E : E^G\right]$$

Ainsi, toutes les inégalités sont des égalités, ce qui permet de conclure.

□