

* Théorème d'Artin: d'après 1.68, 1.25, 1.62 (1.41, 1.44) [exercice - d'Artin] 21

1) Si L/K est une extensⁿ finie et M/K une extension quelconque, alors:

$$|\text{Hom}_{M/K}(L \rightarrow M)| \leq [L:K].$$

2) (Théorème d'Artin): Si G est un sous-groupe fini de $\text{Aut}(K)$, alors:

$$[K:K^G] \leq |G|$$

En particulier:

$G = \text{Aut}_{K^G}(K)$ et l'inégalité précédente est une égalité.

preuve:

1) Soit $[L:K]$ une extensⁿ finie. On peut écrire $L = K(\alpha_1, \dots, \alpha_n)$ avec $\alpha_1, \dots, \alpha_n$ algébriques sur K .

On cherche donc à montrer par récurrence, pour $n \in \mathbb{N}$:

$H_n: \forall M, \forall L = K(x_1, \dots, x_n)$ avec $x_1, \dots, x_n$ algébriques sur K , $\forall \phi_0: K \rightarrow M$, $\exists$ au plus $[L:K]$ morphismes

$\phi: L \rightarrow M$ prolongeant ϕ_0 .

$n=0$: ok.

$n=1$: $L = K(x)$, notons $P = \mu_{x,K}$.

Soit $\phi: L \rightarrow M$ prolongeant ϕ_0 . On a $0 = \phi(P(x)) = \phi_0(P)(\phi(x))$.

Donc: $\phi(x) \in Z_M(\phi_0(P))$

Par ailleurs, $L = K(x)$ donc ϕ est entièrement déterminé par l'image de x .

Ainsi: $\{\text{prolongements de } \phi_0\} \rightarrow Z_M(\phi_0(P))$ est bien déf. et injective.

$$\phi \mapsto \phi(x)$$

Or, $|Z_M(\phi_0(P))| \leq \deg(\phi_0(P)) = \deg(P) = [L:K]$, ce qui donne le résultat.

Supposons le résultat acquis pour un certain $n \geq 1$.

Soit L/K une extens: avec $L = K(x_1, \dots, x_n)$ où les x_i sont algébriques sur K .

Soit $\phi_0: K \rightarrow M$ un morphisme.

Par H_n , $\mathcal{E} := \{\psi: K(x_1, \dots, x_n) \rightarrow M, \text{ morphisme prolongeant } \phi_0\}$ est de cardinal $e \leq [K(x_1, \dots, x_n):K]$.

Soit $\psi \in \mathcal{E}$. $L = K(x_1, \dots, x_n) = K(x_1, \dots, x_{n-1})(x_n)$ et x_n est algébrique sur K donc sur $K(x_1, \dots, x_{n-1})$.

Ainsi, par H_1 : $\mathcal{E}_\psi := \{\phi: L \rightarrow M \text{ prolongeant } \psi\}$ est de cardinal $f_\psi \leq [L:K(x_1, \dots, x_{n-1})]$.

Soit $\phi: L \rightarrow M$ prolongeant ϕ_0 . On a $\phi|_{K(x_1, \dots, x_{n-1})} \in \mathcal{E}$ et donc $\phi \in \mathcal{E}_\psi|_{K(x_1, \dots, x_{n-1})}$.

Ainsi: $\{\phi: L \rightarrow M, \phi|_K = \phi_0\} \subseteq \bigcup_{\psi \in \mathcal{E}} \mathcal{E}_\psi$ et donc $|\mathcal{E}| \leq \sum_{\psi \in \mathcal{E}} f_\psi \leq [L:K(x_1, \dots, x_{n-1})][K(x_1, \dots, x_{n-1}):K] = [L:K]$.

de principe de récurrence permet de conclure.

2) Notons $G = \{g_1, \dots, g_n\}$ avec $g_i = \text{id}_K$.

Soit $(e_1, \dots, e_m)$ une K^G -base de K , et supposons par l'absurde $m > n$.

Soit (E) le système linéaire suivant:

$$(E) \begin{cases} g_1(e_1)x_1 + \dots + g_n(e_m)x_m = 0 \\ \vdots \\ g_n(e_1)x_1 + \dots + g_n(e_m)x_m = 0 \end{cases}$$

(E) a n équations pour m inconnues et donc, comme $m > n$: $\exists (x_1, \dots, x_m) \in K^m \setminus \{0\}$ une solution non triviale de (E).

Choisissons une telle solution avec un nombre minimal de x_i non nuls et supposons $x_1 \neq 0$ quitte

à permuer les c_i .

En divisant alors (E) par λ_i , on trouve $(c_1, \dots, c_m) \in \mathbb{K}^m$ une solution non triviale avec un nombre minimal de c_i non nuls et telle que $c_1 = 1 \in \mathbb{K}^G$.

Ainsi :

$$\begin{cases} a_1 g_1(c_1) + \dots + a_m g_1(c_m) = 0 \\ \vdots \\ a_1 g_n(c_1) + \dots + a_m g_n(c_m) = 0 \end{cases} \quad (1)$$

Montrons maintenant que tous les c_i sont dans $\mathbb{K}^G$, ce qui constituera une absurdité car la première ligne entrera en contradiction avec la $\mathbb{K}^G$ -liberté de $(g_1(c_1), \dots, g_1(c_m)) = (c_1, \dots, c_m)$.

Soit $i \in \{1, \dots, n\}$. On multiplie (1) par g_i , multiplie à gauche les éléments de G par g_i revient à les permuer, et donc, en appliquant la permutation inverse aux lignes du système,

on trouve :

$$\begin{cases} g_i(c_1) g_1(c_1) + \dots + g_i(c_m) g_1(c_m) = 0 \\ \vdots \\ g_i(c_1) g_n(c_1) + \dots + g_i(c_m) g_n(c_m) = 0 \end{cases} \quad (i)$$

(i)-(1) donne alors :

$$\begin{cases} \lambda_1 g_1(c_1) + \dots + \lambda_m g_1(c_m) = 0 \\ \vdots \\ \lambda_1 g_n(c_1) + \dots + \lambda_m g_n(c_m) = 0 \end{cases} \quad \text{avec } \lambda_j = g_i(g_j) - c_j.$$

Un g_j nul donne un λ_j nul et $\lambda_i = g_i(c_i) - c_i = 0$ car $c_i \in \mathbb{K}^G$ donc, par minimalité de $(c_1, \dots, c_m)$: $(\lambda_1, \dots, \lambda_m) = 0$.

i.e. : $\forall j : g_i(g_j) = c_j$.

Ceci vaut pour $i \in \{1, \dots, n\}$ quelconque donc : $\forall j : c_j \in \mathbb{K}^G$.

On a donc bien montré :

$$[\mathbb{K} : \mathbb{K}^G] \leq |G|$$

Or, on a clairement $G \subseteq \text{Aut}_{\mathbb{K}^G}(\mathbb{K})$ donc : $|G| \leq |\text{Aut}_{\mathbb{K}^G}(\mathbb{K})| \leq [\mathbb{K} : \mathbb{K}^G]$ par 1).

Donc :

$$|G| = [\mathbb{K} : \mathbb{K}^G] \text{ et } G = \text{Aut}_{\mathbb{K}^G}(\mathbb{K}).$$