

thm: Soit k un corps et G un gpe de cardinal n formé d'automorphismes de k . On pose $k^G = \{x \in k / \forall \sigma \in G, \sigma(x) = x\}$.
Alors $[k : k^G] = n$ et $\text{Aut}_{k^G} k = G$

1) lemme: Soit k un corps et G un gpe et $\chi_1, \dots, \chi_m : G \rightarrow k^*$ des mph 2 à 2 distincts. Alors χ_1, \dots, χ_m sont k -linéairement indépendants.

• Par récurrence sur m . le cas $m=1$ est clair.

• On suppose le résultat pour $m-1$ et soient $a_1, \dots, a_m \in k$ tq

$$\sum_{i=1}^m a_i \chi_i = 0 \quad \forall x, y \in G, \quad \sum_{i=1}^{m-1} a_i \chi_i(x) \chi_i(y) = 0$$
 et

$$\sum_{i=1}^{m-1} a_i \chi_i(x) \chi_m(y) = 0$$
 par différence:
$$\sum_{i=1}^{m-1} a_i (\chi_i(y) - \chi_m(y)) \chi_i(x) = 0$$

et donc $\forall y \in G, \sum_{i=1}^{m-1} a_i (\chi_i(y) - \chi_m(y)) \chi_i = 0$

par hypothèse de récurrence: $\forall y \in G, \forall i=1 \dots m-1,$

les $(\chi_i)_i$ étant 2 à 2 distincts,

$$a_i (\chi_i(y) - \chi_m(y)) = 0$$

$\forall i=1 \dots m-1, \exists y \in G, \chi_i(y) \neq \chi_m(y)$ et alors $a_i = 0$.

On en déduit $a_1, \dots, a_{m-1} = 0$ puis $a_m \chi_m = 0$ puis $a_m = 0$

et le résultat.

2) lemme: Soit $k \subset L$ une extension de corps. si L a au moins n automph k -linéaires, alors $[L : k] \geq n$.

• Par l'absurde $n := [L : k] < n$. Soient $\sigma_1, \dots, \sigma_n$ des automph k -linéaires de L , 2 à 2 distincts. et soit $(e_1, \dots, e_n) = \beta$ une k -base de L .

Considérons le système linéaire homogène

$$\begin{cases} x_1 \sigma_1(e_1) + \dots + x_n \sigma_n(e_1) = 0 \\ x_1 \sigma_1(e_2) + \dots + x_n \sigma_n(e_2) = 0 \\ \vdots \\ x_1 \sigma_1(e_n) + \dots + x_n \sigma_n(e_n) = 0 \end{cases}$$
 d'inconnue $x = (x_1, \dots, x_n) \in \mathbb{Z}^n$

il y a m inconnues pour $n < m$ équations et il existe donc une solution (x_1, \dots, x_n) non triviale ainsi $\sum_{i=1}^n x_i v_i$ s'annule sur la base $\beta = (e_1, \dots, e_n)$ et

il est donc nul. Contradiction avec le lemme 1)

3) Montrons $[k: k^G] = m$: On a déjà $[k: k^G] \geq m$ via lemme 2)

• Montrons que toute famille $(k_1, \dots, k_{n+1}) \in k^{n+1}$ est k^G -liée.

Soit $T_n: x \in k \mapsto \sum_{v \in G} v(x) \in k^G$

par le lemme 1), $T_n \neq 0$. De plus T_n est k^G -linéaire.

• Considérons le système linéaire homogène:

$$\forall g \in G, \sum_{i=1}^{n+1} g(x_i) k_i = 0 \Leftrightarrow \begin{cases} \sum_{i=1}^{n+1} x_i g^{-1}(k_i) = 0 \\ \forall g \in G \end{cases}$$

d'inconnue $x = (x_1, \dots, x_{n+1}) \in k^{n+1}$

Ce système a $|G| = m$ équations pour $n+1$ inconnues et il a donc une solution non triviale (x_1, \dots, x_{n+1}) .

Un des $(x_i)_{i=1}^{n+1}$, disons x_j est non nul.

$(y \in k \mapsto x_j y \in k)$ est bijective donc $y \in k \mapsto T_n(x_j y) \in k^G$ est non nulle: $\exists y \in k, T_n(x_j y) \neq 0$ ($y \neq 0$)

• On a: $\forall g \in G, \sum_{i=1}^{n+1} g(x_i y) k_i = \sum_{i=1}^{n+1} g(x_i) k_i g(y) = 0$ et en sommant:

$$\sum_{i=1}^{n+1} T_n(x_i y) k_i = 0, \text{ et comme}$$

$T_n(x_j y) \neq 0$, c'est une relation de liaison non triviale

4) $\text{Aut}_{k^G}(k) = G$: $[k: k^G] = m \xrightarrow{\text{lemme 2)}} \Rightarrow |\text{Aut}_{k^G}(k)| \leq m$

mais $G \subset \text{Aut}_{k^G}(k)$ et $|G| = m$ donc $G = \text{Aut}_{k^G}(k)$.