
Théorème de Wedderburn

Recasage : 101 / 102 / 123

Référence : D.Perrin "Cours d'Algèbre" p.82

Théorème 1 (Wedderburn)

Tout corps fini est commutatif

Preuve.

On découpe la preuve en plusieurs petites étapes :

► Soit K un corps fini, on introduit le centre de K que l'on note Z (c'est l'ensemble des éléments de K qui commutent avec tous le monde) :

$$Z = \{x \in K \mid y \in K \quad xy = yx\}$$

Z est un sous corps de K de cardinal $q \geq 2$, comme K est un espace vectoriel sur Z on en déduit donc qu'il existe $n \in \mathbb{N}^*$ tel que $\text{Card}(K) = q^n$ avec n la dimension du Z espace vectoriel K .

► On veut montrer que K est commutatif et donc montrer que $K = Z$ ce qui revient à montrer que $n = 1$. Par l'absurde supposons que $n > 1$. Le groupe K^* agit sur lui même par conjugaison c'est à dire que l'on regarde l'application :

$$\Psi : \begin{cases} K^* \times K^* & \longrightarrow K^* \\ (x, y) & \longmapsto yxy^{-1} \end{cases}$$

Soit $x \in K$ alors $\text{Stab}(x) = \{y \in K \mid yxy^{-1} = x\} = \{y \in K \mid xy = yx\}$ (on appelle ça aussi le centralisateur). De plus c'est un Z espace vectoriel donc il existe un entier d tel que $\text{Card}(\text{Stab}(x) \cup \{0\}) = q^d$ donc $\text{Card}(\text{Stab}(x)) = q^d - 1$ et par la formule des classes il vient alors que :

$$\text{Card}(\text{Orb}(x)) = \frac{\text{Card}(K^*)}{\text{Card}(\text{Stab}(x))} = \frac{q^n - 1}{q^d - 1}$$

Et par le théorème de Lagrange on sait alors que $q^d - 1 \mid q^n - 1$ ce qui est possible si $d \mid n$ (Voir le lemme)

► On utilise l'identité sur les polynômes cyclotomiques à savoir $X^n - 1 = \prod_{d \mid n} \Phi_d(X)$ donc on obtient alors que :

$$q^n - 1 = \prod_{m \mid n} \Phi_m(q) \quad q^d - 1 = \prod_{m \mid d} \Phi_m(q) \implies \frac{q^n - 1}{q^d - 1} = \prod_{\substack{m \mid n \\ m \nmid d}} \Phi_m(q)$$

En particulier pour $d \neq n$ $\Phi_n(q)$ divise $\frac{q^n - 1}{q^d - 1}$. On veut à présent utiliser la formule des classes ainsi (en posant $x_1, \dots, x_r$ un système de représentant des orbites pour l'action) :

$$\text{Card}(K^*) = \text{Card}(Z^*) + \sum_{i=1}^r \text{Card}(\text{Orb}(x_i)) \iff q^n - 1 = q - 1 + \sum_{i=1}^r \text{Card}(\text{Orb}(x_i))$$

On déduit alors que $\Phi_n(q)$ divise $q - 1$ donc $|\Phi_n(q)| \leq q - 1$.

► On pose alors $\zeta_1, \dots, \zeta_r \in \mathbb{C}$ les racines primitives n -ième de l'unité ainsi :

$$\Phi_n(q) = \prod_{i=1}^r (q - \zeta_i)$$

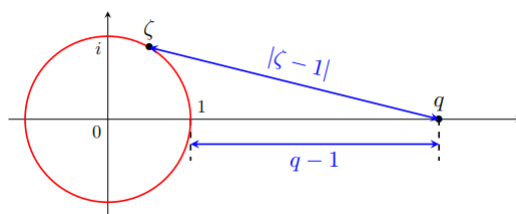
Comme $n > 1$ par hypothèse on a que $\forall i \in \llbracket 1; n \rrbracket \zeta_i \neq 1$ donc par inégalité triangulaire :

$$|\Phi_n(q)| = \left| \prod_{i=1}^r (q - \zeta_i) \right| = \prod_{i=1}^r |q - \zeta_i| > \prod_{i=1}^r (|q| - |\zeta_i|) = (q - 1)^r \geq q - 1$$

Ce qui est absurde ainsi $n = 1$ et donc $K = Z$ ce qui nous donne alors que K est commutatif

■

On peut donner une illustration graphique qui nous sert pour la dernière inégalité :



On donne ici une preuve de la formule des classes :

Lemme 1

Soit G un groupe fini et on considère une action de G sur un ensemble X fini , alors :

$$\text{Card}(G) = \text{Card}(\text{Orb}(x)) \times \text{Card}(\text{Stab}(x))$$

Preuve.

On considère l'application $\Phi : \frac{G}{\text{Stab}(x)} \longrightarrow \text{Orb}(x)$ et montrons que cette application est bijective :

► Montrons que l'application est bien définie, c'est à dire qu'elle ne dépend du choix du représentant c'est à dire que si $g_1 g_2 \in G$ tel que $\overline{g_1} = \overline{g_2}$ dans $\frac{G}{\text{Stab}(x)}$ alors il existe $h \in \text{Stab}(x)$ tel que $g_2 = g_1 h$.

$$\Phi(\overline{g_2}) = g_2 \cdot x = (g_1 h) \cdot x = g_1 \cdot (h \cdot x) = g_1 \cdot x = \Phi(\overline{g_1})$$

Donc l'application est bien définie.

► Montrons que l'application est bien injective, supposons que $\Phi(\overline{g_2}) = \Phi(\overline{g_1})$ et montrons que $\overline{g_1} = \overline{g_2}$. Comme $g_1 \cdot x = g_2 \cdot x$ donc $g_1^{-1} g_2 \in \text{Stab}(x)$ de même $g_2^{-1} g_1 \in \text{Stab}(x)$ et donc $\overline{g_1} = \overline{g_2}$.

► Montrons que l'application est bien surjective. Si $y \in \text{Orb}(x)$ alors il existe $g \in G$ tel que $y = g \cdot x$ de ce fait $y = \Phi(\overline{g})$ et donc Φ est surjective.

On a bien montré que Φ est bijective et donc $\text{Card}(G) = \text{Card}(\text{Orb}(x)) \times \text{Card}(\text{Stab}(x))$

■