Théorème de Wedderburn

Réf:
- Cours d'algèbre, D. Perrin.

Leçons: 101, 123.

Théorème

Tout corps fini est commutatif.

Preuve: Soit K un corps fini.

Etape 1: un espace vectoriel sur un corps commutatif.

Notons Z l'ensemble $\{a \in K / \forall x \in K \; ax = xa\}$.

Alors Z est un sous-corps commutatif de K. Notons q son cardinal.

Comme K est un Z-ev de dimension finie (car fini), il existe $n \in \mathbb{N}^*$ tel que $\#K = q^n$.

Etape 2: Une action.

Supposons K non commutatif. Alors on a $n \geq 2$ car $K \neq Z$.

On considère l'action de $K^\times$ sur lui-même par automorphismes intérieurs.

Notons K_x l'ensemble $\{y \in K / yx = xy\}$ pour tout $x \in K^\times$.

Alors $K_x^\times$ est le stabilisateur de x, et K_x est un sous corps de K

Soit $x \in K^\times$. Comme Z est inclus dans K_x, il existe $d \in \mathbb{N}^*$ tel que $\#K_x = q^d$ et de plus on a $d \mid n$.

On obtient

$$|\mathcal{O}_x| = \frac{|K^\times|}{|K_x^\times|} = \frac{q^n - 1}{q^d - 1}$$

Etape 3 : la cyclotomie

Les polynômes cyclotomiques vérifient

$$X^n - 1 = \prod_{m|n} \Phi_m(X)$$

d'où $q^n - 1 = \prod_{m|n} \Phi_m(q)$ et $q^d - 1 = \prod_{m|d} \Phi_m(q)$.

On en déduit

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

Pour d différent de n, l'entier $\Phi_n(q)$ divise $\frac{q^n-1}{q^d-1}$.

Etape 4 :

On écrit l'équation des classes

$$|K^\times| = |Z^\times| + \sum_{x \in I} |G_x|$$

où I est un système de représentants pour les classes des orbites. On a en particulier $I \cap Z = \emptyset$.

Dans ce cas, pour tout $x \in I$ on a

$$d_x := \log_q(|K_x|) \neq n$$

En réécrivant l'équation des classes on obtient

$$q^n - 1 - \sum_{x \in I} \frac{q^n - 1}{q^{d_x} - 1} = q - 1$$

et donc $\Phi_n(q)$, qui divise les termes de gauche, divise $q-1$.

En particulier, on a $|\Phi_n(q)| \leqslant q - 1$

Etape 5 :

Notons $\zeta_1, \dots, \zeta_p$ les racines primitives n-ième de 1.

Comme $n \neq 1$, on a $\forall j \in [\![1, p]\!]$ $\zeta_j \neq 1$, et donc on a

$$\forall j \in \{1, \dots, p\} \quad |q - \zeta_j| > |q - 1|$$

De plus, comme $\Phi_n(q) = \prod_{j=1}^{p} (q - \zeta_j)$ on en déduit

$$|\Phi_n(q)| > |q-1|^p \geq |q-1|$$

Contradiction ↯ Nécessairement K est commutatif.