Théorème de Wedderburn : Tout corps fini est commutatif.

Réf : Perrin
102
123
101

plan 1) k et son centre

2) Supposons k non commutatif, agir k^* sur lui-même pour card de $\omega(x)$.

3) $\phi_n(q) \mid \frac{q^n-1}{q^d-1}$

4) équation aux classes pour $|\phi_n(q)| \leq q-1$

5) $|\phi_n(q)| > q-1$ et ~~obtenir~~ conclure par une contradiction.

Preuve : 1) Soit k un corps fini. (a priori pas commutatif)

Z le centre de k : $Z = \{a \in k, \forall x \in k, ax = xa\}$.

Z est un sous corps commutatif de k de cardinal $q \geq 2$ $\{0,1\} \subset k$.

Comme k est un Z-espace vectoriel, on a $|k| = q^n$ pour un $n \in \mathbb{N}$.

2) Supposons k non commutatif donc $n > 1$.

On a k^* qui opère sur lui-même par automorphismes intérieurs $(g \cdot a = gag^{-1})$.

Pour $x \in k^*$ on note $\omega(x)$ l'orbite de x.

On pose par ailleurs $k_x = \{y \in k, yx = xy\} \overset{\text{si } y \in k^*}{=} \{y \in k, yxy^{-1} = x\} = k_x^*$.

k_x est un sous corps de k (a priori pas commutatif)

et le stabilisateur de x dans l'opération est k_x^*.

$Z \subset k_x$

donc Z est un sous corps de k_x.

On a $|k_x| = q^d$ pour la même raison que avant.

De plus $d \mid n$ ~~car~~ (k est k_x espace vectoriel à gauche donc $|k|$ est une puissance de $|k_x|$)

(Alternativement, $k_x^* \subset k^* \overset{\text{Lagrange}}{\Longrightarrow} q^d - 1 \mid q^n - 1 \overset{q \geq 2}{\Longrightarrow} d \mid n$.

Utile ?
Oui pour 3)

Le cardinal de l'orbite de x est alors :

$|\omega(x)| = \frac{|k^*|}{|k_x^*|} = \frac{q^n-1}{q^d-1}$. cf ... racine polynôme cyclotomique

3) On a, dans $\mathbb{Z}$, par ~~déf des~~ grâce aux polynômes cyclotomiques :

$$q^n - 1 = \prod_{m \mid n} \Phi_m(q)$$

et $$q^d - 1 = \prod_{m \mid d} \Phi_m(q)$$

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

pour $d \neq n$, on voit en particulier que $\Phi_n(q) \mid \frac{q^n - 1}{q^d - 1}$.

4) On écrit l'équation aux classes : $|G|^* = \underbrace{|Z^*|}_{\text{orbite de card} = 1} + \underbrace{\sum_{x \notin Z} |\omega(x)|}_{\text{orbite de card} \geq 2}$

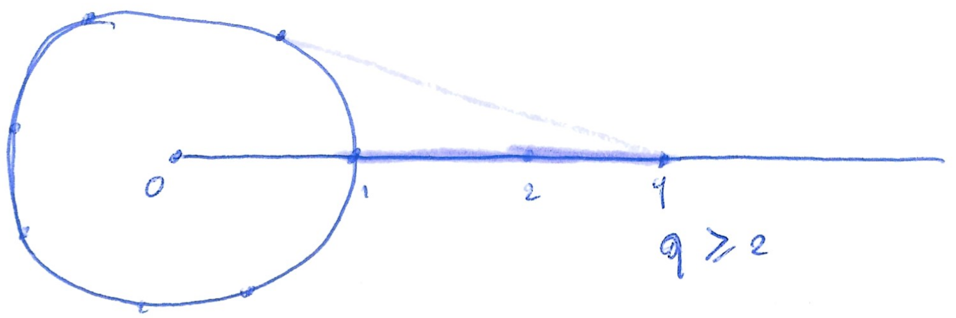
Hors que $x \notin Z$ signifie que $d \neq n$

donc $q^n - 1 = q - 1 + \sum_X \frac{q^n - 1}{q^d - 1}$ où $X \subset \{ m \in \mathbb{N}, m \mid n \} \setminus \{n\}$.

donc $\Phi_n(q) \mid q - 1$ donc $|\Phi_n(q)| \leq q - 1$.

5) $\Phi_n(q) = (q - \zeta_1) \cdots (q - \zeta_l)$ où $\zeta_1, \dots, \zeta_l \in \mathbb{C}$ sont les racines primitives ~~n~~-ième de 1 (vérifient $|\zeta_i| = 1$ et $\zeta_i \neq 1$) (car $n \neq 1$).

On a donc $\forall i$, $|q - \zeta_i| > q - 1$.



donc $|\Phi_n(q)| > (q - 1)^l \geq q - 1$. Absurde.

Donc k est commutatif.