

Théorème de Wedderburn

Thm: Tout corps fini est commutatif. (On toute algèbre à division finie est un corps⁹)

Preuve: Soit K un "corps fini pas forcément commutatif", i.e. une algèbre à division finie. Soit Z son centre. $Z := \{a \in K \mid \forall x \in K, ax = xa\}$.

Z est un sous-corps (commutatif) de K , de cardinal $q \geq 2$. K est alors un Z -ev, donc $|K| = q^n$.

• Supposons K non commutatif, donc $n > 1$. Alors $K^* \curvearrowright K^*$ par conjugaison.

On note $K_x = \{y \in K \mid yx = xy\}$ les éléments de K qui commutent avec x , de sorte que

$\text{Stab}_x = K_x^*$. Z est un sous-corps de K_x , donc $|K_x| = q^d$.

De plus $K_x^* < K^*$ donc (Lagrange) $q^{d-1} \mid q^n - 1$. Comme $q \geq 2$, cela implique d'abord en effet, si on écrit $n = ad + r$ avec $r \in [0, d-1]$, alors

$$q^{d-1} \mid q^n - 1 \Rightarrow q^{d-1} \mid (q^{m-1}) - (q^{d-1}) = (q^{(a-1)d+r} - 1) q^d$$

Comme $q^{d-1} \nmid q^d = 1$, donc (lemme de Gauss) $q^{d-1} \mid q^{(a-1)d+r} - 1$

En itérant, on a $q^{d-1} \mid q^r - 1$, donc $r = 0$.

On a $|\text{Orb}_x| = \frac{|K^*|}{|\text{Stab}_x|}$, i.e. $|\text{Orb}_x| = \frac{|K^*|}{|K_x^*|} = \frac{q^n - 1}{q^d - 1}$, d'où avec l'équation aux dessus:

$$|K^*| = |Z^*| + \sum_{x \notin Z} |\text{Orb}_x|, \text{ i.e. } q^n - 1 = (q - 1) + \sum_{x \notin Z} \frac{q^n - 1}{q^d - 1} \quad (*)$$

somme sur des $x \notin Z$, donc les d sont des diviseurs stricts de n .

• On utilise les polynômes cyclotomiques: $\frac{q^m - 1}{q^n - 1} = \prod_{m \mid n} \phi_m(q)$ et $\frac{q^d - 1}{q^n - 1} = \prod_{m \mid d} \phi_m(q)$.

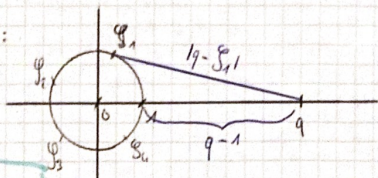
de sorte que $\frac{q^m - 1}{q^d - 1} = \prod_{\substack{m \mid n \\ m \nmid d}} \phi_m(q)$.

En particulier, pour $d < n$, $\phi_m(q) \mid \frac{q^m - 1}{q^d - 1}$

Dans $(*)$, cela implique en particulier (puisque $\phi_m(q) \mid q^m - 1$), $\phi_m(q) \mid q - 1$, et donc a fortiori $|\phi_m(q)| \leq q - 1$.

Or $\phi_n(q) = \prod_{g \in \mu_n^*} (q - g)$ or $\forall g \in \mu_n^*, |g|=1$ et $g \neq 1$ car $n \neq 1$.

Donc pour chaque g , $|q - g| > q - 1$:



Donc $|\phi_n(q)| = \prod_{g \in \mu_n^*} |q - g| > (q - 1)^{|\mu_n^*|} \geq q - 1$

Absurde! Donc k commutatif.