

Théorème de Wedderburn (Perron) + Goursat

Recorages: 101, (102), 123, 103, 1

Théorème (Wedderburn): Tout corps fini est commutatif.

Preuve: Soit k un corps fini, pas nécessairement commutatif, Z le centre de k .

$$Z = \{a \in k \mid \forall x \in k, ax = xa\}$$

Z est un sous-corps commutatif de k de cardinal $q \geq 2$ et puisque k est un Z -espace vectoriel, $\#k = q^m$ avec $m = [k:Z]$.

2) Supposons k non commutatif donc $m > 1$. Alors k^* agit sur lui-même par conjugaison: $k^* \times k^* \rightarrow k^*$
 $(g, k) \mapsto ghg^{-1}$

Pour $x \in k^*$, on note $w(x) = \text{Orb}(x) = \{gxg^{-1} \mid g \in k^*\}$

On pose par ailleurs $k_x = \{y \in k \mid yx = xy\}$. k_x est un sous-corps de k (non nécessairement commutatif) et $\text{Stab}(x) = k_x^*$

k_x est un Z -espace vectoriel donc $\#k_x = q^d$ avec $d = [k_x:Z]$.

De plus, comme $k_x^* \subset k^*$, on a $q^d - 1 \mid q^m - 1$ (Lagrange)

et pour $q \in \mathbb{N}$, $q \geq 2$, ceci impose $d \mid m$. Alors, par la bijection entre $G/\text{Stab}(x)$ et $\text{Orb}(x)$.

$$\hookrightarrow q^m - 1 = \prod_{k \mid m} \phi_k(q) \quad q^m - 1 \mid q^d - 1$$

$$q^d - 1 = \prod_{k \mid d} \phi_k(q) \quad (=) d \mid m$$

Ces deux sont
en. donc

$$\#w(x) = \frac{\#k^*}{\#k_x^*} = \frac{q^m - 1}{q^d - 1}$$

3) Propriété des polynômes cyclotomiques

$$q^m - 1 = \prod_{m \mid n} \phi_m(q) \quad \text{et} \quad q^d - 1 = \prod_{m \mid d} \phi_m(q)$$

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

$$\Rightarrow q^m - 1 = q^{dh} - 1 = (q^d)^h - 1 = (q^d - 1) \sum_{i=0}^{h-1} q^{id}$$

$$\Rightarrow m = d \cdot h, \quad 0 \leq h \leq d$$

$$\text{donc} \quad q^m - 1 = q^{dh} - 1 = (q^d)^h - 1 = (q^d - 1) \sum_{i=0}^{h-1} q^{id}$$

Pour $d \neq m$, on voit en particulier que $\phi_m(q)$ divise $\frac{q^m - 1}{q^d - 1}$ donc $q^{dh} - 1 \mid q^d - 1$ avec $h < d$ donc $h = 0$.

4) On écrit alors l'équation aux classes

$$\#k^* = \#Z^* + \sum_{x \notin Z} \#w(x)$$

Dire que $x \notin Z$ signifie que $d \nmid n$ de sorte qu'on a

$$\#k^* = \#Z^* + \sum \frac{q^m - 1}{q^d - 1}$$

la somme portant sur un certain nombre de diviseurs stricts

Il en résulte que $\phi_n(q)$ divise $q-1$, en particulier, $|\phi_n(q)|$

$$|q - \zeta_k|$$

5) On a $\phi_n(q) = (q - \zeta_1) \dots (q - \zeta_e)$ où $\zeta_1, \dots, \zeta_e \in \mathbb{C}$ sont les e racines n -èmes de 1 donc $|\zeta_i| = 1$ et $\zeta_i \neq 1$ puisque $n \nmid 1$.
Passons alors, on a $\forall i \in \{1, \dots, e\}$, $|q - \zeta_i| \geq q - 1$ et donc $|\phi_n(q)| \geq$

$$= \sqrt{q^2 + \cos^2\left(\frac{2k\pi}{n}\right) - 2q\cos\left(\frac{2k\pi}{n}\right)}$$

$$= \sqrt{q^2 - 2q\cos\left(\frac{2k\pi}{n}\right) + 1}$$

$$> \sqrt{q^2 - 2q + 1}$$

$$= q - 1$$

d'où une contradiction.



Finalement, $n=1$ et $k \in \mathbb{Z}$ d'où k est commutatif.

Lemme: Soit $n, d \in \mathbb{N}^*$, $q \geq 2$. On pose r le reste de la division euclidienne de n par d . Alors $q^n - 1$ est le reste de la division euclidienne de $q^n - 1$ par $q^d - 1$. En particulier, $q^d - 1 \mid q^n - 1 \Leftrightarrow d \mid n$. Dans ce cas, pour tout k , $\phi_n(q) \mid \frac{q^n - 1}{q^d - 1}$.

Preuve: Soit $m \in \mathbb{Z}$, $n = dm + r$, $r \in [0, d-1]$. Comme $n, d \geq 0$, on a $r \leq n$.
Alors $q^n - 1 = (q^d)^m q^r - 1 = (q^d - 1 + 1)^m q^r - 1 = q^r - 1 + \sum_{k=1}^m \binom{m}{k} (q^d - 1)^k q^r$
Par le binôme de Newton, $q^n - 1 \equiv q^r - 1 \pmod{q^d - 1}$. Il existe donc un k tel que $q^n - 1 = k(q^d - 1) + q^r - 1$. De plus, comme $q \geq 2$, $d \geq 1$ et on a $0 \leq q^r - 1 < q^d - 1$. Donc $q^r - 1$ est le reste de la division euclidienne de $q^n - 1$ par $q^d - 1$.

De plus, comme $q \geq 2$, $q^r - 1 = 0 \Leftrightarrow r = 0 \Leftrightarrow d \mid n$.

Puis pour tout $d \mid n$, $X^n - 1 = \prod_{d \mid n} \phi_d(X) = (X^d - 1) \prod_{\substack{d' \mid n \\ d' \nmid d}} \phi_{d'}(X)$.
d $\nmid$ n, comme $n \nmid d$, on a un polynôme $Q \in \mathbb{Z}[X]$ d'où
tel que $X^n - 1 = (X^d - 1)Q(X)\phi_n(X)$. Alors, en évaluant en q , on a que $\phi_n(q) \mid \frac{q^n - 1}{q^d - 1}$.