Gourdon

Théorème de Wedderburn

Thm: Tout corps fini est commutatif.

dém: On procède par récurrence sur le cardinal du corps fini.

→ Si $\mathbb{K}$ est de cardinal 2, alors $\mathbb{K}$ est commutatif.

→ Soit $\mathbb{K}$ un corps fini et on suppose que tout corps fini $\mathbb{L}$ de cardinal $|\mathbb{L}| < |\mathbb{K}|$ est commutatif. On veut montrer que $\mathbb{K}$ est commutatif.

On procède par l'absurde et on suppose que $\mathbb{K}$ n'est pas commutatif.

① Posons $Z = \{x \in \mathbb{K},\ \forall y \in \mathbb{K},\ xy = yx\}$ le centre de $\mathbb{K}$. C'est un sous-corps de $\mathbb{K}$.
Par hypothèse $Z \subsetneq \mathbb{K}$ donc Z est commutatif si bien que $|\mathbb{K}| = |Z|^d$ pour $d \geq 2$.

② Si $x \in \mathbb{K}$, on pose $\mathbb{K}_x = \{y \in \mathbb{K},\ yx = xy\}$. C'est un sous-corps de $\mathbb{K}$.
De plus, $Z \subset \mathbb{K}_x$ donc $|\mathbb{K}_x| = |Z|^\alpha$ pour $\alpha \geq 1$. Montrons que $\alpha | d$:

* Si $\mathbb{K}_x = \mathbb{K}$, on a donc $|\mathbb{K}_x| = |Z|^d$ et $\alpha = d \geq 2$.
* Si $\mathbb{K}_x \neq \mathbb{K}$, $\underbrace{\text{alors}}_{\mathbb{K}_x \text{ étant commutatif}}$ $|\mathbb{K}| = |\mathbb{K}_x|^\beta$ pour $\beta \geq 1$ d'où $|\mathbb{K}| = |Z|^{\alpha\beta} = |Z|^d$

donc $\alpha | d$.

③ On considère l'action par conjugaison
$$\begin{array}{ccc} \mathbb{K}^* \times \mathbb{K}^* & \longrightarrow & \mathbb{K}^* \\ (y, x) & \longmapsto & y.x = yxy^{-1} \end{array}$$

Si $x \in \mathbb{K}^*$, $\mathrm{Stab}(x) = \{y \in \mathbb{K}^*,\ y.x = x\} = \mathbb{K}_x^*$

L'équation aux classes donne alors

$$|\mathbb{K}^*| = \sum_{O \text{ orbite}} \frac{|\mathbb{K}^*|}{|\mathrm{Stab}(x)|_{\text{où } x \in O}} = |Z^*| + \sum_{\text{orbite}} \frac{|\mathbb{K}^*|}{|\mathbb{K}_x^*|}$$

On a $|\mathbb{K}^*| = |Z|^d - 1$ et $|\mathbb{K}_x^*| = |Z|^\alpha - 1$ avec $\alpha | d$.

En notant λ_α le nombre d'orbite distincte tel que $|\mathbb{K}_x^*| = |Z|^\alpha - 1$, on en déduit

$$|\mathbb{K}^*| = q - 1 + \sum_{\alpha | d} \lambda_\alpha \frac{q^d - 1}{q^\alpha - 1}.$$

④ On a

$$X^d - 1 = \prod_{\beta | d} \overset{\beta^{\text{ième}} \text{ polynôme cyclotomique}}{\Phi_\beta}$$

Si $\underset{\alpha \neq d}{\alpha | d}$, $X^d - 1 = \Phi_d \cdot \underbrace{\prod_{\beta | \alpha} \Phi_\alpha}_{X^\alpha - 1} \cdot \prod_{\substack{\beta \nmid \alpha \\ \beta | d}} \Phi_\beta$ donc $\Phi_d \left| \dfrac{X^d - 1}{X^\alpha - 1} \right.$ pour $\underset{\alpha \neq d}{\alpha | d}$

De plus, $\Phi_d \mid X^d - 1$ donc $\Phi_d \left| X^d - 1 - \sum_{\substack{\alpha | d \\ \alpha \neq d}} \lambda_\alpha \dfrac{X^d - 1}{X^\alpha - 1} \right.$

d'où $\Phi_d(q) \left| q^d - 1 - \sum_{\substack{\alpha | d \\ \alpha \neq d}} \lambda_\alpha \dfrac{q^d - 1}{q^\alpha - 1} \right. = q - 1$ d'après ③

donc $|\Phi_d(q)| \leq q - 1$.

Or $|\Phi_d(q)| = \left| \prod_{\xi \in U_d} (q - \xi) \right| \underset{\substack{\uparrow \\ \text{strict car} \\ d > 1}}{>} \prod_{i=1}^{\varphi(d)} |q - 1| \geq q - 1$ d'où une contradiction.

On a bien démontré par récurrence que tout corps fini est commutatif.