Théorème de Wedderburn

Théorème 1 (Wedderburn)**.** *Tout corps fini est commutatif.*

Démonstration.

Soit $\mathbb{K}$ un corps fini. Notons $Z = \{a \in \mathbb{K} \mid \forall\, x \in \mathbb{K}, ax = xa\}$ le centre de $\mathbb{K}$. C'est un sous-corps commutatif de $\mathbb{K}$ de cardinal $q \geqslant 2$, et comme $\mathbb{K}$ est un Z-espace vectoriel, on a $|\mathbb{K}| = q^n$ avec $n \in \mathbb{N}^\star$.

Supposons par l'absurde que $\mathbb{K}$ n'est pas commutatif, donc que $n > 1$. Alors $\mathbb{K}^\times$ agit sur lui-même par conjugaison. Pour tout $x \in \mathbb{K}^\times$, on note $\omega(x)$ l'orbite de x. On pose par ailleurs $\mathbb{K}_x = \{y \in \mathbb{K} \mid yx = xy\}$, sous-corps de Z et de $\mathbb{K}$, qui est alors de cardinal q^{d_x} avec $d_x \mid n$.

Le stabilisateur de $x \in \mathbb{K}^\times$ est $\{y \in \mathbb{K}^\times \mid yx = xy\} = \mathbb{K}_x^\times$. Le cardinal de son orbite $\omega(x)$ est alors :

$$|\omega(x)| = \frac{|\mathbb{K}^\times|}{|\mathbb{K}_x^\times|} = \frac{q^n - 1}{q^{d_x} - 1}$$

En notant θ un système de représentants des orbites, l'équation aux classes donne alors :

$$q^n - 1 = |\mathbb{K}^\times| = |Z^\times| + \sum_{x \in \theta \setminus Z^\times} |\omega(x)| = |Z^\times| + \sum_{x \in \theta \setminus Z^\times} \frac{|\mathbb{K}^\times|}{|\mathbb{K}_x^\times|} = q - 1 + \sum_{x \in \theta \setminus Z^\times} \frac{q^n - 1}{q^{d_x} - 1}$$

Or, pour $x \in \theta \setminus Z^\times$, on a $d_x \neq n$, car sinon on a $x \in Z^\times$. On peut donc écrire :

$$q^n - 1 = q - 1 + \sum_{\substack{d \mid n \\ d \neq n}} \lambda_d \frac{q^n - 1}{q^d - 1}$$

où λ_d désigne le nombre de $x \in \theta \setminus Z^\times$ tels que $|\omega(x)| = q^d - 1$.

Si $d \mid n$ et $d \neq n$, on a :

$$X^n - 1 = \Phi_n \prod_{\substack{e \mid n \\ e \neq n}} \Phi_e = \Phi_n \left(\prod_{e \mid d} \Phi_e \right) \left(\prod_{\substack{e \mid n \\ e \neq n, e \nmid d}} \Phi_e \right) = \Phi_n (X^d - 1) \left(\prod_{\substack{e \mid n \\ e \neq n, e \nmid d}} \Phi_e \right)$$

Ainsi, Φ_n divise $\frac{X^n - 1}{X^d - 1}$ dans $\mathbb{Z}[X]$, puis $\Phi_n(q)$ divise $q - 1$. En particulier, $|\Phi_n(q)| \leqslant q - 1$. Or $n \neq 1$, donc :

$$|\Phi_n(q)| = \prod_{\xi \in \mu_n(\mathbb{C})} |q - \xi| > \prod_{i=1}^{\varphi(n)} |q - 1| \geqslant |q - 1|$$

Cela est absurde. Le corps fini $\mathbb{K}$ est donc commutatif.

□

Références

[Per] Daniel Perrin. *Cours d'Algèbre.* Ellipses
[Gou] Xavier Gourdon. *Les Maths en Tête : Algèbre.* Ellipses, 2e edition