Développement. Le théorème de Wedderburn

Théorème 1. Tout corps fini est commutatif.

Preuve Soit K un corps fini. Son centre
$$Z \coloneqq \{a \in K \mid \forall x \in K,\ ax = xa\}$$
est un sous-corps commutatif fini. Notons $q \geqslant 2$ son cardinal. Comme le corps K est un Z-espace vectoriel, son cardinal est de la forme $|K| = q^n$ pour un entier $n \in \mathbf{N}^*$.

Raisonnons par l'absurde et supposons que le corps K n'est pas commutatif, c'est-à-dire $n > 1$. Le groupe $K^\times$ agit sur lui-même par conjugaison. Soit $x \in K^\times$ un élément. On note son orbite
$$\mathrm{Orb}(x) \coloneqq \{yxy^{-1} \mid y \in K\} \subset K$$
et on pose l'ensemble
$$K_x \coloneqq \{y \in K \mid yx = xy\}.$$
Comme précédent, il existe un entier $d_x = d \in \mathbf{N}^*$ tel que $|K_x| = q^d$ et $d \mid n$. De plus, remarquons que l'ensemble $K_x^\times$ est le stabilisateur de l'élément x si bien que l'on peut écrire
$$|\mathrm{Orb}(x)| = \frac{|K^\times|}{|K_x^\times|} = \frac{q^n - 1}{q^d - 1}.$$
Pour $m \in \mathbf{N}^*$, on considère le m-ième polynôme cyclotomique $\Phi_m \in \mathbf{Z}[X]$. Alors les propriétés de ces derniers permettent d'écrire
$$q^n - 1 = \prod_{m \mid n} \Phi_m(q) \qquad \text{et} \qquad q^d - 1 = \prod_{m \mid d} \Phi_m(q)$$
ce qui donne
$$\frac{q^n - 1}{q^d - 1} = \prod_{\substack{m \mid n \\ m \nmid d}} \Phi_m(q).$$
Lorsque $d \neq n$, l'entier $\Phi_n(q)$ divise donc le cardinal $|\mathrm{Orb}(x)|$.

Maintenant, on écrit l'équation aux classes données par l'action par conjugaison du groupe $K^\times$ sur lui-même : on obtient
$$|K^\times| = |Z^\times| + \sum_{x \notin Z} |\mathrm{Orb}(x)|.$$
Or $x \notin Z \Leftrightarrow d_x \neq n$ pour tout élément $x \in K^\times$. La dernière relation se réécrit alors
$$q^n - 1 = q - 1 + \sum_{\substack{x \in K^\times \\ d_x \neq n}} |\mathrm{Orb}(x)|.$$
En vertu du dernier paragraphe, on obtient $\Phi_n(q) \mid q - 1$ et donc $|\Phi_n(q)| \leqslant q - 1$.

Notons $\zeta_1, \ldots, \zeta_\ell \in \mathbf{C}$ les racines n-ièmes primitives de l'unité. Comme $n > 1$, elles ne valent pas 1. Mais alors un rapide dessin permet de se convaincre de l'inégalité
$$|q - \zeta_i| > q - 1, \qquad i \in [\![1, \ell]\!].$$
Ceci permet de conclure que
$$|\Phi_n(q)| = |(q - \zeta_1) \cdots (q - \zeta_\ell)| > (q - 1)^\ell \geqslant q - 1$$
ce qui est contradictoire avec le précédent paragraphe. Finalement, le corps K est commutatif. ◁

[1] Daniel Perrin. *Cours d'algèbre*. Ellipses, 1996.