1.5 Théorème de Wedderburn

Recasage : 101, 103, 123.
Références : Cours d'algèbre, Perrin.

Théorème 1.3 (Wedderburn)**.** *Tout corps fini est commutatif.*

Démonstration. On va procéder en plusieurs étapes :

Étape 1 : Soit k un corps fini (pas nécessairement commutatif), on définit le centre de k par $Z := \{a \in k \ ; \ \forall x \in k, ax = xa\}$. Alors Z est un sous-corps commutatif de k, de cardinal $q \geq 2$. On peut donc voir k comme un Z-espace vectoriel, et $|k| = |q|^n$, $n \in \mathbb{N}^*$. En effet, cela vient du lemme suivant :

Lemme 1.4. *Soient $\mathbb{K}$, $\mathbb{L}$ deux corps finis tels que $\mathbb{K}$ est commutatif, et $\mathbb{K} \subseteq \mathbb{L}$. Alors, il existe $d \in \mathbb{N}^*$ tel que $|\mathbb{L}| = |\mathbb{K}|^d$.*

Démonstration. Comme $\mathbb{L}$ est un $\mathbb{K}$-espace vectoriel de dimension finie d (car $\mathbb{L}$ est fini), $\mathbb{L}$ est donc isomorphe à $\mathbb{K}^d$ en tant que $\mathbb{K}$-espace vectoriel. En particulier, $|\mathbb{L}| = |\mathbb{K}|^d$. □

Étape 2 : Supposons dans la suite que k n'est pas commutatif, alors $n > 1$ (sinon, $|k| = q$, donc $k = Z$, mais k est supposé non-commutatif). Alors, k^* opère sur lui-même par automorphismes intérieurs :

$$\begin{array}{ccc} k^* \times k^* & \to & k^* \\ (a, x) & \mapsto & axa^{-1} \end{array}.$$

Pour $x \in k^*$, on note $\omega(x)$ l'orbite de x. On pose également $k_x := \{y \in k \ ; \ yx = xy\}$. Alors, k_x est un sous-corps de k (pas nécessairement commutatif), et le stabilisateur de x dans l'action est k_x^*. Comme précédemment, on peut voir k_x comme un Z-espace vectoriel, et écrire $|k_x| = q^d$. Montrons que d divise n :
Par le théorème de Lagrange, comme k_x^* est un sous-groupe de k^*, alors $q^d - 1$ divise $q^n - 1$. Posons alors $n = dl + r$, on a :

$$q^n - 1 = q^{dl+r} - 1 = (q^d - 1)(q^{n-d} + q^{n-2d} + \cdots + q^{n-dl}) + q^r - 1.$$

Comme $q^d - 1$ divise $q^n - 1$, alors $q^r - 1 = 0 \Leftrightarrow r = 0$, et donc $n = dl$, i.e. d divise n. Alors, le cardinal de $\omega(x)$ est :

$$|\omega(x)| = \frac{|k^*|}{|k_x^*|} = \frac{q^n - 1}{q^d - 1}.$$

Étape 3 : Par définition des polynômes cyclotomiques, on a :

$$q^n - 1 = \prod_{m|n} \Phi_m(q) \ , \ q^d - 1 = \prod_{m|d} \Phi_m(q),$$

donc :

$$\frac{q^n - 1}{q^d - 1} = \prod_{m|n, m\nmid d} \Phi_m(q).$$

En particulier, pour $d \neq n$, $\phi_n(q)$ divise $\frac{q^n-1}{q^d-1}$.

Étape 4 : Remarquons que :

$$k_x^* = k^* \Leftrightarrow \forall y \in k^*, xy = yx \Leftrightarrow x \in Z^*.$$

En se donnant $\mathcal{R}$ un système de représentants, l'équation aux classes donne donc :

$$|k^*| = |Z^*| + \sum_{x \in \mathcal{R},\ x \notin Z} |\omega(x)|,$$

mais $x \notin Z \Leftrightarrow d \neq n$, d'où :

$$q^n - 1 = q - 1 + \sum_{d|n, d \neq n} m(d) \frac{q^n - 1}{q^d - 1},$$

où $m(d)$ désigne la multiplicité de d. Aussi, $\Phi_n(q) \mid q^n - 1$, $\Phi_n(q) \mid \frac{q^n-1}{q^d-1}$, pour tout $d \mid n$, $d \neq n$. On a donc que $\Phi_n(q)$ divise $q - 1$, et par suite, $|\Phi_n(q)| \leq q - 1$.

Étape 5 : On a :

$$\Phi_n(q) = (q - \zeta_1) \dots (q - \zeta_i),$$

où $\zeta_1, \dots, \zeta_i \in \mathbb{C}$ sont les racines primitives n-ièmes de l'unité, donc $|\zeta_j| = 1$, et $\zeta_j \neq 1$ (puisque $n \neq 1$), $\forall 1 \leq j \leq i$. Or, $\forall j \in \{1, \dots, i\}$, $|q - \zeta_j| > q - 1$ (se voit facilement sur un dessin), donc $|\Phi_n(q)| > (q-1)^i \geq q - 1$, ce qui nous fournit une contradiction.

On en conclut que k est forcément un corps commutatif. □

Commentaires : Le lemme que l'on utilise est également valable sans l'hypothèse de commutativité. La théorie des espaces vectoriels à gauche et à droite, sans commutativité, existebien, et admet une théorie de la dimension et du rang. Cependant, la théorie du déterminant n'est plus valable dans ce cadre.