Développement: Théorème de Wedderburn

Adrien Fontaine

6 septembre 2013

Référence : Daniel Perrin, Cours d'algèbre, p82

Théorème 1

Tout corps fini est commutatif.

Démonstration : 1. Soit k un corps fini, a priori non nécéssairement commutatif, et Z le centre de k, *i.e*

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

Z est un sous-corps de k, commutatif, de cardinal $q \geq 2$ (il contient au moins 0 et 1). De plus, k est un Z-espace vectoriel, donc $|k| = q^n$.

2. On suppose par l'absurde que k est non commutatif, *i.e* $n \geq 2$. Alors, $k^\times$ opère de façon non triviale sur lui même par automorphisme intérieur. Pour $x \in k^\times$, on note $\omega(x)$ son orbite, *i.e*

$$\omega(x) = \{axa^{-1}, a \in k\}$$

On pose $k_x = \{y \in k, yx = xy\}$, l'ensemble des éléments qui commutent avec x. Alors, k_x est un sous-corps de k, et le stabilisateur de x sous l'action de $k^\times$ sur $k^\times$ est $k_x^\times$.
De plus, k_x est un Z-espace vectoriel, donc $|k_x| = q^d$. Et $k_x^\times$ est un sous-groupe de $k^\times$, donc $q^d - 1 \mid q^n - 1$. Écrivons la division euclidienne de n par d. Il existe $(q, r) \in \mathbb{N}^* \times \mathbb{N}$ tel que

$$n = dq + r \text{ et } r < d \text{ ou } r = 0$$

Alors,

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

Comme $n - qd = r < d$, cela constitue la division euclidienne de $q^n - 1$ par $q^d - 1$. Comme $q^d - 1 \mid q^n - 1$, on en déduit $q^r - 1 = 0$. D'où $r = 0$ et $d \mid n$.
On a alors

$$|\omega(x) = \frac{|k^\times|}{|k_x^\times|} = \frac{q^n - 1}{q^d - 1} \text{ avec } d \mid n$$

3. On a, dans $\mathbb{Z}$, par une propriété classique des polynômes cyclotomiques :

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

Et de même,

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

Donc,

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

Pour $d \neq n$, on voit donc en particulier que $\Phi_n(q) \mid \frac{q^n-1}{q^d-1}$.

4. Écrivons désormais l'équation aux classes :

$$|k^\times| = |Z^\times| + \sum_{x \notin Z} |\omega(x)|$$

De plus, dire que $x \notin Z$ signifie que l'on a $d \neq n$, de sorte que

$$q^n - 1 = q - 1 + \sum \frac{q^n - 1}{q^d - 1}$$

la somme portant sur un certain nombre de diviseurs stricts de n. Comme $\Phi_n(q) \mid q^n - 1$ et $\Phi_n(q) \mid \frac{q^n-1}{q^d-1}$ pour un diviseur strict d de n, on en déduit que $\Phi_n(q) \mid q - 1$. En particulier, $|\Phi_n(q)| \leq q - 1$.

5. On a $\Phi_n(q) = (q - \xi_1)...(q - \xi_l)$, où $\xi_1, ..., \xi_l$ sont les racines primitives n-ièmes de l'unité. En particulier, $|\xi_i| = 1$ et $\xi_i \neq 1$ car $n \neq 1$. Mais alors, on a, pour tout i, $|q - \xi_i| > q - 1$ (faire un dessin). Donc, $|\Phi_n(q) > (q - 1)^l \geq q - 1$. Contradiction. ■