Perrin p 82.

Développement : Théorème de Wedderburn.

101
123
190

Tout corps finis est commutatif.

Preuve : On montre d'abord le lemme suivant :

⓪ Lemme : Soit $L_1 \subset L_2$ deux corps finis, avec L_1 commutatif. Alors il existe $k \in \mathbb{N}^*$ tel que $|L_2| = |L_1|^k$

Preuve : L_1 étant un sous corps commutatif de L_2, L_2 est un L_1 ev de dimension $\dim_{L_1} L_2 = k < +\infty$ car $\dim L_2 < +\infty$. Le corps L_2 est donc isomorphe comme L_1 ev à L_1^k et on en déduit $|L_2| = |L_1^k| = |L_1|^k$.

① Soit $\mathbb{K}$ un corps fini, on note $Z(\mathbb{K})$ le centre de $\mathbb{K}$. Alors $Z(\mathbb{K})$ est un sous corps commutatif de $\mathbb{K}$ de cardinal $q = \ell$ (0 et 1 sont dedans).
Par le lemme 0, $\exists m \in \mathbb{N}^*$, $|\mathbb{K}| = q^m$.

② On suppose $\mathbb{K}$ non commutatif, donc $m > 1$. Alors $\mathbb{K}^*$ opère sur lui même par conjugaison. Pour $x \in \mathbb{K}^*$ on note $Orb(x)$ l'orbite de x. On pose $k_x = Stab(x) \cup \{0\}$, c'est un sous corps de $\mathbb{K}$.
De même, $Z(\mathbb{K})$ est un sous corps commutatif de k_x, d'après le lemme 0 $\exists d \in \mathbb{N}^*$, $|k_x| = q^d$. ⚠ d dépend de x. (noter d_x).
$(k_x^*, \times)$ et $(\mathbb{K}^*, \times)$ sont des groupes
De plus $k_x^* \subset \mathbb{K}^*$, d'après Lagrange $|k_x^*| = q^d - 1 \mid q^m - 1 = |\mathbb{K}^*|$
donc $d \mid m$ (voir annexe).
Le cardinal de l'orbite de x est alors :

$$|Orb(x)| = \frac{|\mathbb{K}^*|}{|Stab(x)|} = \frac{q^m - 1}{q^d - 1}$$

des polynômes d'un corps

③ On a dans $\mathbb{Z}$, par définition des polynômes cyclotomiques :

$$q^m - 1 = \prod_{n \mid m} \Phi_n(q) \quad ; \quad q^d - 1 = \prod_{n \mid d} \Phi_n(q) \text{ donc } \frac{q^m - 1}{q^d - 1} = \prod_{\substack{n \mid m \\ n \nmid d}} \Phi_n(q)$$

Pour $d \neq m$, on voit que $\Phi_m(q) \mid \frac{q^m - 1}{q^d - 1}$

④ On considère $\{x_1, \dots, x_n\} \subset \mathbb{K}^*$ un système de représentant des orbites non triviales. Avec la formule des classes :

$$|\mathbb{K}^*| = |Z(\mathbb{K}^*)| + \sum_{i=1}^{n} |Orb(x_i)| \quad \text{et} \quad q^m - 1 = q - 1 + \sum_{i=1}^{n} Card(Orb(x_i))$$

Or, d'après 3, $\Phi_m(q) \mid q^m - 1$ et $\Phi_m(q) \mid |Orb(x_i)| \ \forall i \in [\![1, n]\!]$ donc $\Phi_m(q) \mid q - 1$ donc $|\Phi_m(q)| \leq q - 1$.

⑤ On a $\Phi_m(q) = (q - u_1) \dots (q - u_{\varphi(m)})$ où $(u_i) \in \mathbb{C}$ sont les racines primitives de l'unité donc $|u_i| = 1$ et $u_i \neq 1$ (par définition).

Alors $|\Phi_m(q)| = \prod_{i=1}^{\varphi(m)} |u_i - q| > \prod_{i=1}^{\varphi(m)} |1q - u_i|| = \prod_{i=1}^{\varphi(m)} q - 1 \geq q - 1$

(inégalités strictes)

ce qui fournit une contradiction avec ④. On en conclut que $\mathbb{K}$ est commutatif.

ANNEXE :

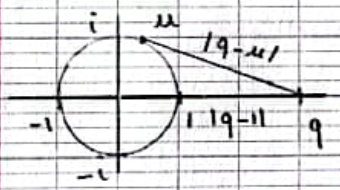

Schéma pour ⑤

Lemme : Soit $(q, n, d) \in \mathbb{N}^{*3}$ avec $q \geq 2$. On a l'équivalence

$$d \mid n \iff q^d - 1 \mid q^n - 1.$$

Preuve :

$\Rightarrow$ Si $n = dk$, $q^n - 1 = (q^d)^k - 1 = (q^d - 1) \sum_{i=0}^{k-1} q^{id}$ donc $q^d - 1 \mid q^n - 1$.

$\subset$ On utilise la division euclidienne $\exists (a, b) \in \mathbb{Z}^2$, $n = da + b$ et $0 \leq b < d$.

Alors $q^n - 1 = q^b (q^{da} - 1) + (q^b - 1)$. En utilisant $\Rightarrow$ et l'hypothèse, $q^d - 1 \mid q^b - 1$. Comme $q \geq 2$, ce n'est possible que si $b = 0$ i.e. $d \mid n$.

Exemple d'un corps infini non commutatif : le corps des quaternions.