P. Maurer

ENS Rennes

Recasages : 101, 102.

Référence : Perrin, Cours d'algèbre

Théorème de Wedderburn

Théorème 1. ***(Wedderburn)***

Tout corps fini est commutatif.

Démonstration.

Soit K un corps fini (non nécessairement commutatif, de fait). On note Z son centre :

$$Z = \{x \in K \,:\, \forall a \in K \; ax = xa\}$$

Alors K est un Z-espace vectoriel de dimension finie, donc isomorphe à Z^n pour un certain entier $n \in \mathbb{N}$, d'où $|K| = q^n$ avec $q = |Z| \geq 2$. Supposons par l'absurde que $n > 1$.

Le groupe $K^\times$ agit sur lui-même par conjugaison. Pour $x \in K$, l'ensemble $\mathrm{Stab}(x) \cup \{0\}$ est un sur-corps de Z, donc on en déduit comme précédemment qu'il existe $d \in \mathbb{N}^*$ tel que $|\mathrm{Stab}(x)| = q^d - 1$.

Comme $\mathrm{Stab}(x) \subset K^\times$, le théorème de Lagrange donne $q^d - 1 | q^n - 1$, ce qui n'est possible que si d divise n. En écrivant l'équation aux classes, il vient alors :

$$|K^\times| = |Z^\times| + \sum_{x \notin Z} \frac{|K^\times|}{|\mathrm{Stab}(x)|} \iff q^n - 1 = q - 1 + \sum \frac{q^n - 1}{q^d - 1}$$

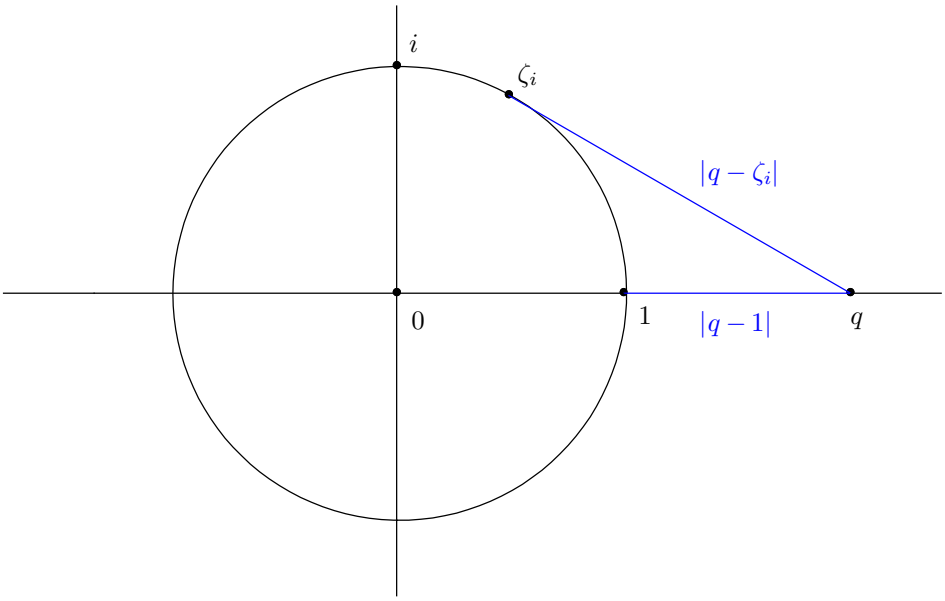
Où la somme de droite porte sur un certain nombre de diviseurs d stricts de n (car $|\mathrm{Stab}(x)| \neq |K^\times|$ pour $x \notin Z$), notons $d \in \mathfrak{D}$ avec $\mathfrak{D} \subset \{k | n,\ k < n\}$.

On a les égalités $q^n - 1 = \prod_{m|n} \Phi_m(q)$ et $q^d - 1 = \prod_{m|d} \Phi_m(q)$, où $\Phi_m(q)$ désigne le $m^{\text{ème}}$ polynôme cyclotomique. Il vient alors $\dfrac{q^n - 1}{q^d - 1} = \displaystyle\prod_{\substack{m|n \\ m \nmid d}} \Phi_m(q)$.

On a donc :

$$q - 1 = \prod_{m|n} \Phi_m(q) - \sum_{d \in \mathfrak{D}} \prod_{\substack{m|n \\ m \nmid d}} \Phi_m(q)$$

D'où $\Phi_n(q) | q - 1$, et en particulier, $|\Phi_n(q)| \leq q - 1$. Or par définition, $\Phi_n(q) = (q - \zeta_1) \cdots (q - \zeta_s)$ où $\zeta_1, \ldots, \zeta_s$ sont des racines primitives $n^{\text{èmes}}$ de l'unité, donc comme $n > 1$, $|\zeta_i| = 1$ et $\zeta_i \neq 1$ pour tout i. En particulier, on a $|q - \zeta_i| > |q - 1|$:



On en déduit que $|\Phi_n(q)| > |q-1|^\ell \geq |q-1|$, ce qui constitue une contradiction. □