Théorème de Wedderburn

Notions utilisées : action de conjuguaison, cyclotomie, théorie des corps finis.

Théorème 1. *Tout corps gauche fini est commutatif.*

Preuve. Soit k un corps fini.

Etape 1 (facultative) : montrer que le cardinal de k est de la forme q^n. Pour cela, on remarque que le centre de k

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

est un sous-corps commutatif de k de cardinal $q \geq 2$ fini. En particulier, k est un Z-espace vectoriel (à gauche) et donc $\exists n \in \mathbb{N}, |k| = q^n$, en prenant une Z-base par exemple.

Etape 2 : Supposons par l'absurde que k est non commutatif. On considère **l'action du groupe $k^\times$ sur lui-même par conjugaison**, et on s'intéresse aux **orbites**.

Soit $x \in k^\times$ et $k_x := \{a \in k, ax = xa\}$. D'une part, c'est un sous-corps de k donc on peut noter q^d son cardinal, et on a $d|n$. En effet, on a $k_x^\times \subset k^\times$ en tant que sous-groupe, d'où $q^d - 1 | q^n - 1$. On a notamment $q^n - 1 \equiv 0[q^d - 1]$ et donc l'ordre de q dans $\Big(\mathbb{Z}/(q^d-1)\mathbb{Z}\Big)^\times$ divise n. Or cet ordre est d car $q^d \equiv 1[q^d - 1]$ et pour $m < d$ on a $0 < q^m < q^d - 1$ dans $\mathbb{Z}$ car $(q \geq 2)$ et donc $q^m \not\equiv 1[q^d - 1]$. On a ainsi bien montré que $d|n$.

D'autre part, $k_x^\times$ est le stabilisateur de x sous l'action de conjuguaison considérée. On en déduit

$$|Orb(x)| = \frac{|k^\times|}{k_x^\times} = \frac{q^n - 1}{q^d - 1}$$

Etape 3 : On traduit l'égalité précédente en terme de **polynômes cyclotomiques évalués en q** :

$$q^n - 1 = \prod_{m|n} \Phi_m(q) \text{ et donc } \frac{q^n - 1}{q^d - 1} = \frac{\prod_{m|n} \Phi_m(q)}{\prod_{m|d} \Phi_m(q)} = \prod_{m|n, m\not|d} \Phi_m(q).$$

En particulier si $d \neq n$ on constate que $\Phi_n(q) \,\Big|\, \dfrac{q^n - 1}{q^d - 1}$.

Etape 4 : D'après l'**équation aux classes** on a

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

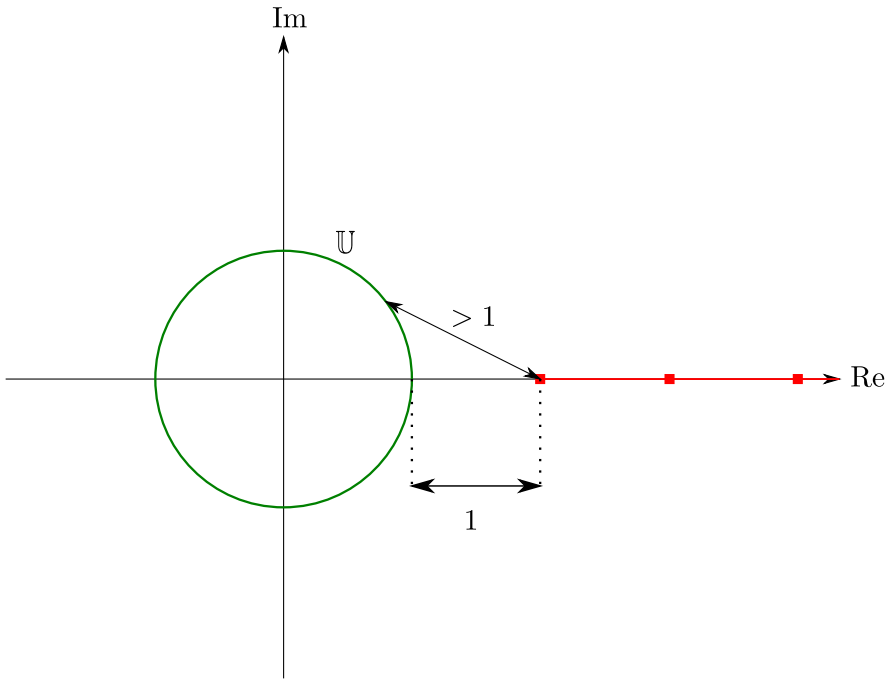
et en remarquant que $x \notin Z \Rightarrow d \neq n$, on obtient

$$q^n - 1 = q - 1 + \sum_{\mathcal{A}} \frac{q^n - 1}{q^d - 1}$$

où $\mathcal{A} \subset \{d \in \mathbb{N}, d|n, d \neq n\}$ est un certain ensemble de diviseurs propres de n. On obtient en particulier $\Phi_n(q)|q-1$ donc

$$|\Phi_n(q)| \leq q - 1.$$

Etape 5 : On va mettre en évidence une **contradiction** dans la dernière affirmation.
On écrit, par définition, $\Phi_n(X) = \prod_i X - \zeta_i$ avec $\zeta_i \neq 1$ les racines primitives n-ièmes de l'unité. En dessinant dans $\mathbb{C}$ la demi-droite horizontale des entiers $n \geq 2$ et le cercle unité, on voit que $\forall i, |q - \zeta_i| > |q-1| = q-1$ car $\zeta_i \in \mathbb{U} \setminus \{1\}$. On en déduit par produit que $|\Phi_n(q)| > q-1$, ce qui contredit l'affirmation $|\Phi_n(q)| \leq q - 1$ obtenue précédemment.



□