Théorème de Wedderburn

Démo de Ernst Witt datant de 1931.

Recasage: 101, 123

Réf: Raisonnements divins, Aigner et Ziegler p35, Cours d'algèbre, Perrin p82

Lemme 1: $\forall n \in \mathbb{N}^*$, $X^n - 1 = \prod_{d|n} \Phi_d$. Conséquence admise : $\Phi_n \in \mathbb{Z}[X]$, $\forall n \in \mathbb{N}$.

Dém: Soit μ_d^* l'ensemble des racines primitives $d^{ème}$ de l'unité i.e les éléments de $\mathcal{U}_d$ d'ordre d. Soit $d|n$.

Il est clair que tout élément de μ_d^* est racine $n^{ème}$ de l'unité donc $\bigcup_{d|n} \mu_d^* \subset \mathcal{U}_n$

Réciproquement, si $\zeta \in \mathcal{U}_n$, ζ est d'ordre d dans $\mathbb{C}^*$ et $d|n$ donc $\zeta \in \mu_d^*$ donc $\mathcal{U}_n = \bigcup_{d|n} \mu_d^*$.

Par unicité de l'ordre dans un groupe, l'union est disjointe : $\mathcal{U}_n = \bigsqcup_{d|n} \mu_d^*$.

$$X^n - 1 = \prod_{\zeta \in \mathcal{U}_n} (X - \zeta) = \prod_{d|n} \prod_{\zeta \in \mu_d^*} (X - \zeta) = \prod_{d|n} \Phi_d(X) \text{ par déf. des } \Phi_d. \quad \square$$

Lemme 2: $\forall n, d \in \mathbb{N}^*$, $\forall q \geq 2$, $q^d - 1 \mid q^n - 1 \Rightarrow d|n$.

Pour tout d diviseur strict de n, on a $\Phi_n(q) \mid \frac{q^n - 1}{q^d - 1}$.

Dém: on écrit $n = pd + r$ avec $0 \leq r < d$ ce qui impose $p \geq 0$.

$q^d - 1$ divise $(q^{pd+r} - 1) - (q^d - 1)$

$$q^{pd+r} - q^d = q^d (q^{(p-1)d+r} - 1)$$

Donc comme $q^d \wedge q^d - 1 = 1$, par Gauss, $q^d - 1 \mid q^{(p-1)d+r} - 1$ d'où en itérant $q^d - 1 \mid q^r - 1$ ce qui n'est possible que pour $r = 0$ et donc $d|n$.

OU

On écrit $n = pd + r$ avec $p \geq 0$ et $0 \leq r < d$

On a $q^n - 1 = (q^d - 1 + 1)^p q^r - 1$ donc comme $q^d - 1 \mid \binom{q^d - 1}{k}$, il reste $q^n - 1 \equiv q^r - 1 \ [q^d - 1]$ donc $\exists k \in \mathbb{Z}$ tq $q^n - 1 = k(q^d - 1) + q^r - 1$ donc $q^r - 1$ est le reste de $q^n - 1$ mod. $q^d - 1$. Par hyp. on a donc $q^r - 1 = 0$ d'où $r = 0$ et $d|n$.

(C'est même une équivalence)

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

donc $\Phi_n(q)$ divise bien $\frac{q^n - 1}{q^d - 1}$ si $d \neq n$. $\square$

Théorème (Wedderburn) : tout corps fini K est commutatif.

Dém : Soit $Z = \{a \in K : \forall x \in K,\ ax = xa\}$ le centre de K. C'est un sous-corps commutatif de K, de cardinal $\mathrm{Card}(Z) =: q \geq 2$. On peut ainsi voir K comme un Z-espace vectoriel de dimension $n \geq 1$ de sorte que $K \simeq Z^n$ i.e $\mathrm{Card}\, K = q^n$.

car Z est commutatif.

On raisonne par l'absurde en supposant K non commutatif i.e $n > 1$. On fait agir $K^\times$ sur lui-même par conjugaison. Etant donné un $s \in K^\times$, on note $\omega(s)$ son orbite, $C_s = \{x \in K : xs = sx\}$ son centralisateur, $\mathrm{Stab}(s)$ son stabilisateur.

On a alors $\mathrm{Stab}(s) = \{x \in K^\times : xsx^{-1} = s\} = \{x \in K^\times : xs = sx\} = C_s^\times$.

Comme C_s est un sous-corps de K qui contient Z donc $\exists d_s \geq 1$ tq $\mathrm{Card}\, C_s = q^{d_s}$.

Par ailleurs $C_s^\times = \mathrm{Stab}(s) \subset K^\times$ donc le théorème de Lagrange donne $q^{d_s} - 1 \mid q^n - 1$.

D'après le lemme 2, on a $d_s \mid n$ et par conséquent, $|\omega(s)| = \dfrac{|K^\times|}{|\mathrm{Stab}(s)|} = \dfrac{q^n - 1}{q^{d_s} - 1}$.

De plus, $|\omega(s)| = 1 \iff \mathrm{Stab}(s) = C_s^\times = K^\times \iff s \in Z^\times$ donc en décomposant l'équation des classes selon le cardinal des orbites, on trouve :

la somme porte sur un système de représentants

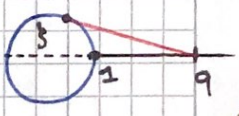
$$q^n - 1 = |K^\times| = |Z^\times| + \sum_{|\omega(s)| > 1} |\omega(s)| = q - 1 + \sum_{\substack{d_s \mid n \\ d_s \neq n}} \frac{q^n - 1}{q^{d_s} - 1}.$$

Le lemme 2 assure que $\Phi_n(q)$ divise la somme de droite et le lemme 1 montre que $q^n - 1 = \prod_{d \mid n} \Phi_d(q)$ donc $\Phi_n(q)$ divise $q^n - 1$.

Donc $\Phi_n(q)$ divise $q - 1$ et en outre $|\Phi_n(q)| \leq q - 1$.

On $\Phi_n(q) = \prod_{\zeta \in \mu_n^*} (q - \zeta)$ et si $\zeta \in \mu_n^*$ on a $|\zeta| = 1$ et $\zeta \neq 1$ car $n > 1$.

Par inégalité triangulaire, $|q - \zeta| > |q - |\zeta|| = q - 1 \geq 1$



donc $|\Phi_n(q)| = \prod_{\zeta \in \mu_n^*} |q - \zeta| > q - 1$ d'où une contradiction.

Donc $n = 1$ i.e $|K| = q$ i.e $K = Z$ i.e K est commutatif. □