Théorème de Wedderburn avec les polynômes cyclotomiques

Berhuy page 649

Lemme Soit $n \in \mathbb{N}^*$.
On a alors $X^n - 1 = \prod_{d|n} \Phi_d$.

Notons pour $k \in \mathbb{N}^*$, $\mathbb{U}_k'$ l'ensemble des éléments d'ordre k de $\mathbb{U}_k$.

▷ Montrons que $\mathbb{U}_n$ est l'union disjointe des $\mathbb{U}_d'$ avec $d|n$:
Comme tout élément de $\mathbb{U}_d'$ est racine n-ième de l'unité, on a : $\bigcup_{d|n} \mathbb{U}_d' \subset \mathbb{U}_n$.
Inversement, soit $\omega \in \mathbb{U}_n$ d'ordre d dans $\mathbb{C}^*$ alors $d|n$ et $\omega \in \mathbb{U}_d$. Donc $\omega \in \mathbb{U}_d'$.
On a donc :
$$\mathbb{U}_n = \bigcup_{d|n} \mathbb{U}_d'$$
De plus, les éléments de $\mathbb{U}_d'$ sont d'ordre d dans $\mathbb{C}^*$, donc les ensembles $\mathbb{U}_d'$ sont deux à deux disjoints.

▷ On a alors :
$$X^n - 1 = \prod_{\omega \in \mathbb{U}_n} (X - \omega) = \prod_{d|n} \prod_{\omega \in \mathbb{U}_d'} (X - d) = \prod_{d|n} \Phi_d$$

Lemme Soient $n, d, q \in \mathbb{N}^*$ avec $q \geq 2$.
Alors $q^d - 1 \mid q^n - 1$ si et seulement si $d|n$. Le cas échéant, on a $\Phi_n(q) \mid \frac{q^n - 1}{q^d - 1}$ pour tout d diviseur strict de n.

On écrit $n = md + r$ avec $r \in [\![0, d-1]\!]$, on remarque alors que $m \geq 0$.
On a alors :
$$q^n - 1 = q^{md} q^r - 1 = (q^d - 1 + 1)^m q^r - 1 \quad \text{d'où : } q^n - 1 \equiv q^r - 1 \ [q^d - 1]$$
car $q^d - 1$ divise $\binom{q^d-1}{k}$
Il existe alors $k \in \mathbb{Z}$ tel que :
$$q^n - 1 = k(q^d - 1) + q^r - 1 \quad \text{avec } q^d - 1 > 0 \text{ et } 0 \leq q^r - 1 < q^d - 1$$
Donc $q^r - 1$ est le reste dans la division euclidienne de $q^n - 1$ par $q^d - 1$ et $q^r - 1 = 0 \iff r = 0$.
Ainsi : $q^d - 1 \mid q^n - 1 \iff d|n$.

De plus, si $d|n$,
$$X^n - 1 = (X^d - 1) \prod_{d'|n,\, d' \nmid d} \Phi_{d'}$$
Donc, si $d \neq n$,
$$X^n - 1 = (X^d - 1) Q \Phi_n \quad \text{avec } Q \in \mathbb{Z}[X].$$
car $\Phi_d \in \mathbb{Z}[X]$
On a alors : $\Phi_n(q) \mid \frac{q^n - 1}{q^d - 1}$.

Théorème de Wedderburn
Tout corps fini est commutatif.

Soit A un corps fini, on note $Z := Z(A) = \{x \in A \mid \forall y \in A,\ xy = yx\}$.
Alors Z est un sous-corps commutatif de A, fini car A est fini de cardinal $q \geq 2$.
car c'est un corps
On a A est un Z espace vectoriel de dimension $n \geq 1$ donc $A \simeq Z^n$ et $|A| = q^n$.

commutant de Z
Faisons agir Z^* sur lui-même par conjugaison.
Pour $d \in Z^*$, $\mathrm{Stab}(d) = \{x \in Z^* \mid xdx^{-1} = d\} = \{x \in Z^* \mid xd = dx\} = C(d) \setminus \{0\}$
On $C(d)$ est un sous-anneau de A contenant Z, il existe alors $n_d \in \mathbb{N}^*$ tel que $|C(d)| = q^{n_d}$.
Donc :
$$|O_d| = \frac{|Z^*|}{|\mathrm{Stab}(d)|} = \frac{q^n - 1}{q^{n_d} - 1}, \text{ d'après le lemme } n_d | n.$$
De plus, $|O_d| = 1 \iff C(d) \setminus \{0\} = Z^* \iff d \in Z^*$.
Donc, par la formule aux classes,
$$|Z^*| = q^n - 1 = q - 1 + \sum_{d \in \mathcal{R}'} \frac{q^n - 1}{q^{n_d} - 1} \quad \text{où } n_d \text{ diviseur strict de } n$$
A^* par Z^*
$\mathcal{R}'$ classe de représentants d'orbites de cardinal > 1

D'après le lemme, $\Phi_n(q)$ divise chaque terme de la somme indexée par $\mathcal{R}'$ et si $\mathcal{R}'$ est vide la somme est nulle donc divisible par $\Phi_n(q)$.

De plus, $q^n - 1 = \prod_{d|n} \Phi_d(q)$ donc $\Phi_n(q)$ divise $q^n - 1$.

Ainsi :

$$\Phi_n(q) \mid q-1 \quad \text{d'où} \quad |\Phi_n(q)| \leqslant q-1$$

Or pour tout $\omega \in \mathbb{U}_n'$,

$$|q-\omega| \geqslant |q-|\omega|| = q-1 \geqslant 1$$

Donc :

$$q-1 \leqslant |q-\omega| \leqslant \prod_{z \in \mathbb{U}_n'} |q-z| = |\Phi_n(q)| \leqslant q-1 \quad \text{donc} \quad |q-\omega| = q-1.$$

Ce qui se réécrit : ——— en notant $\omega = e^{2i\pi/n}$

$$\left[q - \cos\left(\frac{2\pi}{n}\right)\right]^2 + \sin\left(\frac{2\pi}{n}\right)^2 = (q-1)^2 \iff 2q\cos\left(\frac{2\pi}{n}\right) = 2q \iff \cos\left(\frac{2\pi}{n}\right) = 1 \iff n = 1.$$

Autrement dit, $\dim_{\mathbb{Z}}(A) = 1$, i.e. $\mathbb{Z} = A$. Donc A est commutatif. ——— car $\mathbb{Z}$ est le centre de A