Théorème de WEDDERBURN

Mohamed NASSIRI

Référence :

Cours d'algèbre, Daniel Perrin - p.82

Recasage :

• • • • • 101 : Groupe opérant sur un ensemble. Exemples et applications.
• • • • • 123 : Corps finis. Applications.

Résumé :

Le théorème de WEDDERBURN est un classique de la théorie des corps finis. Avec un énoncé simple et efficace, sa démonstration comporte néanmoins plusieurs niveaux faisant appel à plusieurs domaines de l'algèbre (centre d'un groupe, actions de groupes, polynômes cyclotomiques ...).

Prérequis :

Corps finis - Actions de groupes - Polynômes cyclotomiques

Théorème de WEDDERBURN :

Tout corps fini est commutatif.

Démonstration.
Etape 1 :
Dans cette étape, on va utiliser le centre du corps k qui sera important pour la suite. En même temps, c'est le seul ensemble qui est commutatif par définition ...

Soit k un corps fini, pas nécessairement commutatif (sinon ce n'est pas du jeu ...), et Z le centre de k *i.e.*

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

Z est (assurément) un sous-corps commutatif de k de cardinal $q \geq 2$, et donc on peut voir k comme un Z-espace vectoriel. On a donc $|k| = q^n$ pour un certain $n \in \mathbb{N}^*$.

Etape 2 :
Ici, ce sont les actions de groupes et le très efficace théorème de Lagrange qui vont nous permettre de déduire des relations de divisibilité.

On suppose donc que k est non commutatif donc $n > 1$ (en effet, si $n = 1$, alors $k = Z$, et donc k est

confondu avec son centre Z et ainsi il est commutatif).
k^* opère donc sur lui-même par automorphismes intérieurs (et ceci de manière non triviale ...) :

$$\begin{aligned} k^* \times k^* &\to k^* \\ (a, x) &\mapsto axa^{-1} \end{aligned}$$

Pour $x \in k^*$, on note $\omega(x) = \{axa^{-1},\ a \in k^*\}$ l'orbite de x.
Par ailleurs, on pose $k_x = \{y \in k \mid yx = xy\}$. k_x est (assurément, et oui encore ...) un sous-corps (pas nécessairement commutatif) de k et le stabilisateur de x dans l'action est k_x^*.
Avec les même arguments que précédemment, on peut voir k_x comme un Z-espace vectoriel donc $|k_x| = q^d$.

Comme $k_x^* < k^*$, par le théorème de Lagrange, on a $q^d - 1 | q^n - 1$, et donc en écrivant $n = dq + r$ $(*)$, on a :

$$q^n - 1 = (q^d - 1)(q^{n-d} + q^{n-2d} + ... + q^{n-dq}) + q^r - 1$$

Comme $q^d - 1 | q^n - 1$, on a donc $q^r - 1 = 0 \Leftrightarrow r = 0$, et par suite par $(*)$, on en déduit que $d|n$.

En utilisant la relation entre les cardinaux de l'orbite, du stabilisateur, et du groupe, on a

$$|\omega(x)| = \frac{|k^*|}{|k_x^*|} = \frac{q^n - 1}{q^d - 1} \quad \text{avec } d|n$$

Etape 3 :
C'est dans cette étape que les polynômes cyclotomiques rentrent dans la danse ...

Par définition des polynômes cyclotomiques, on a :

$$q^n - 1 = \prod_{m|n} \Phi_m(q) \qquad \text{et} \qquad q^d - 1 = \prod_{m|d} \Phi_m(q)$$

et donc

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

Pour $d \neq n$, on voit donc que $\Phi_n(q) \mid \frac{q^n-1}{q^d-1}$.

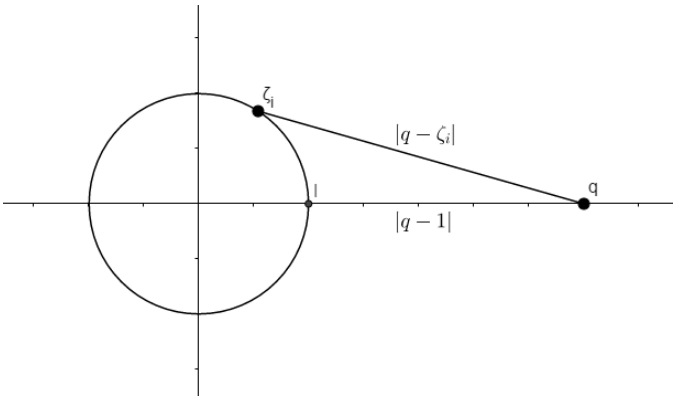
Etape 4 :
L'équation aux classes donne :

$$|k^*| = |Z^*| + \sum_{x \notin Z} |\omega(x)| \qquad \text{or } x \notin Z \Leftrightarrow d \neq n,\ \text{d'où,}$$

$$q^n - 1 = q - 1 + \sum_{\substack{d|n \\ d \neq n}} \frac{q^n - 1}{q^d - 1} \qquad \text{avec } \ \Phi_n(q) \mid q^n - 1 \text{ et } \ \Phi_n(q) \mid \frac{q^n - 1}{q^d - 1}$$

Donc $\Phi_n(q) \mid q - 1$ et par suite, $|\Phi_n(q)| \leq q - 1$

Etape 5 :
On a $\Phi_n(q) = (q - \zeta_1)...(q - \zeta_l)$ où $\zeta_1, ..., \zeta_l \in \mathbb{C}$ sont les racines primitives n-ièmes de l'unité et vérifient donc $|\zeta_i| = 1$ et $\zeta_i \neq 1$ puisque $n \neq 1$.
Mais $\forall i$, $|q - \zeta_i| > q - 1$ (pour s'en convaincre, il suffit de regarder droit dans les yeux la figure ci-dessous) et donc $|\Phi_n(q)| > (q - 1)^l \geq q - 1$. Absurde !



□

Remarques :

- Revenons un peu sur la formule :

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

Il est utile, pour se convaincre de la véracité de cette formule (et dans l'éventualité de questions tatillones d'un jury...), d'essayer pour un certain n et un certain d.
Exemple avec $n = 12$ et $d = 6$, on a :

$$q^{12}-1 = \prod_{m|12}\Phi_m(q) = \Phi_1(q)\Phi_2(q)\Phi_3(q)\Phi_4(q)\Phi_6(q)\Phi_{12}(q)$$

et

$$q^6-1 = \prod_{m|6}\Phi_m(q) = \Phi_1(q)\Phi_2(q)\Phi_3(q)\Phi_6(q)$$

et donc

$$\frac{q^{12}-1}{q^6-1} = \frac{\cancel{\Phi_1(q)}\cancel{\Phi_2(q)}\cancel{\Phi_3(q)}\Phi_4(q)\cancel{\Phi_6(q)}\Phi_{12}(q)}{\cancel{\Phi_1(q)}\cancel{\Phi_2(q)}\cancel{\Phi_3(q)}\cancel{\Phi_6(q)}} = \Phi_4(q)\Phi_{12}(q)$$

On a bien que $4|12$, $12|12$ et $4 \nmid 6$, $12 \nmid 6$.