4. Théorème de Wedderburn

Théorème

Tout corps fini est commutatif.

Attention : pour la démonstration, il faut oublier tout ce qu'on a établi sur les corps finis en supposant la commutativité ...

1. Schéma de la démonstration
2. Sous-corps des éléments qui commutent avec une partie
3. Un lemme de divisibilité
4. Polynômes cyclotomiques

1. Schéma de la démonstration

Soit $(K, +, 0, *, e)$ un corps fini.

• On considère son centre :

$$Z(K) \overset{\text{déf}}{=} \{y \in K : \quad (\forall x \in K) \quad y * x = x * y\}$$

$Z(K)$ est un sous-corps de K (exercice). $Z(K)$ est commutatif.

Objectif : Montrer que $Z(K) = K$.

• On pose $\mathrm{card}(Z(K)) = q$.

Exercice : Munir K d'une structure de $Z(K)$-espace vectoriel, et en déduire l'existence d'un $n \in \mathbb{N}$ tel que $\mathrm{card}(K) = q^n$.

Il s'agit maintenant de montrer que $n = 1$.

Schéma de la démonstration (2)

Le cœur de la démonstration : La formule des classes

pour l'action de $(K^*, *, e)$ sur lui-même par conjugaison :

$$\begin{array}{rcl} \Phi : K^* \times K^* & \longrightarrow & K^* \\ (g, x) & \longmapsto & g \cdot x = g * x * g^{-1} \end{array}$$

• Désignons par K^*/K^* l'ensemble des orbites et par $s : K^*/K^* \to K^*$ une section de la projection canonique $\pi : K^* \to K^*/K^*$. La formule des classes donne ici :

$$\boxed{q^n - 1 = \sum_{x \in s(K^*/K^*)} \frac{q^n - 1}{\mathrm{ord}(\mathrm{Stab}(x))}}$$

Rappels :

$$\mathrm{Orb}(x) \stackrel{\text{déf}}{=} \{g \cdot x = g * x * g^{-1} : \quad g \in K^*\}$$

$$\mathrm{Stab}(x) \stackrel{\text{déf}}{=} \{g \in K^* : \quad g \cdot x = x\} = \{g \in K^* : \quad g * x = x * g\}$$

Schéma de la démonstration (3)

- Calcul de $\mathrm{ord}(\mathrm{Stab}(x))$:

$$K_x \overset{\text{déf}}{=} \mathrm{Stab}(x) \cup \{0\} = \{g \in K : \quad g * x = x * g\}$$

est un sous-corps de K tel que $Z(K) \hookrightarrow K_x \hookrightarrow K$ et il existe un $r_x \in \mathbb{N}$ tel $\mathrm{card}(K_x) = q^{r_x}$, de sorte que :

$$\boxed{\mathrm{ord}(\mathrm{Stab}(x)) = q^{r_x} - 1}$$

- Avec la formule des classes, on doit avoir $q^{r_x} - 1 | q^n - 1$, ce qui équivaut à (lemme de divisibilité) :

$$\boxed{r_x \mid n}$$

Schéma de la démonstration (4)

- Distinguons les orbites à un seul élément :

$$\mathrm{card}(\mathrm{Orb}(x)) = 1 \iff \mathrm{Stab}(x) = K^* \iff x \in Z(K)^*$$

Il y a donc exactement $\mathrm{card}(Z(K)^*) = q - 1$ orbites à un seul élément, et la formule des classes se précise en :

$$\boxed{q^n - 1 \;=\; q - 1 \;+ \sum_{\substack{x \in s(K^*/K^*) \\ \mathrm{card}(\mathrm{Orb}(x)) > 1}} \frac{q^n - 1}{q^{r_x} - 1}}$$

où : $r_x | n$ et $r_x \neq n$.

Schéma de la démonstration (5)

• <u>Les polynômes cyclotomiques à la rescousse</u> :
$\Phi_n(q) | q^n - 1$ (exercice), et comme $r_x | n$ on a aussi $\Phi_n(q) | \frac{q^n - 1}{q^{r_x} - 1}$ (exercice), et donc :

$$\boxed{\Phi_n(q) | q - 1}$$

Mais par ailleurs (faire un dessin !) :

$$\Phi_n(q) = \prod_{\xi \in C_n} \underbrace{|q - \xi|}_{\geq q-1} \geq (q - 1)$$

Finalement $\Phi_n(q) = q - 1$ et $\boxed{n = 1}$.

□

2. Sous-corps des éléments qui commutent avec une partie

Soit $(K, +, 0, *, e)$ un corps.

Lemme (sous-corps des éléments qui commutent avec une partie)

Soit $A \subset K$ une partie quelconque de K. Alors l'ensemble K' des éléments de K qui commutent avec tous les éléments de A,

$$K' \stackrel{\text{déf}}{=} \{y \in K : \quad \forall x \in A, \quad y * x = x * y\}$$

est un sous-corps de K.
De plus, on peut munir K d'une structure de K'-espace vectoriel.

Démonstration : exercice.

$\square$

3. Un lemme de divisibilité

Lemme (de divisibilité)

Soient $a, b \in \mathbb{N}$*. Dans* $\mathbb{Z}[X]$*, on a :*

$$X^b - 1 | X^a - 1 \iff b | a$$

Démonstration :
Si, par division euclidienne dans $\mathbb{N}$, on a :

$$a = bq + r \qquad \text{avec } 0 \leq r < b$$

alors la division euclidienne dans $\mathbb{Z}[X]$ de $X^a - 1$ par $X^b - 1$ s'écrit

$$X^a - 1 = (X^b - 1)\left(\sum_{k=0}^{q-1} X^{bk+r}\right) + X^r - 1$$

(récurrence sur q en exercice) $\square$

4. Polynômes cyclotomiques

Soit $n \in \mathbb{N} \setminus \{0\}$.

$$C_n \overset{\text{déf}}{=} \{z \in \mathbb{C} : \quad z^n = 1\}$$

est un sous-groupe de $(\mathbb{C}^*, \cdot, 1)$, cyclique d'ordre n (engendré par $e^{i\frac{2\pi}{n}}$ par exemple). Il admet exactement $\phi(n)$ générateurs, qu'on appelle les racines primitives $n^{\text{ième}}$ de l'unité. On désigne par RP_n leur ensemble.

Définition (polynômes cyclotomiques)

$$(\forall n \in \mathbb{N} \setminus \{0\}) \qquad \Phi_n(X) \overset{\text{déf}}{=} \prod_{\xi \in RP_n} (X - \xi)$$

Polynômes cyclotomiques (2)

Lemme (factorisation de $X^n - 1$ en polynômes cyclotomiques)

$$(\forall n \in \mathbb{N} \setminus \{0\}) \qquad X^n - 1 = \prod_{d|n} \Phi_d(X)$$

Démonstration : Dans la factorisation $X^n - 1 = \prod_{\xi \in C_n}(X - \xi)$ (dans $\mathbb{C}[X]$), on regroupe les ξ selon leur ordre (qui doit diviser n). $\square$

Corollaire (les polynômes cyclotomiques sont à cœfficients entiers)

$$(\forall n \in \mathbb{N} \setminus \{0\}) \qquad \Phi_n(X) \in \mathbb{Z}[X], \ \textit{de cœf. dominant} = 1$$

Démonstration : $\Phi_1(X) = X - 1$, $\Phi_2(X) = X + 1$, puis par récurrence sur n (exercice). $\square$