UE2 Groupes et Géométrie — Université de Nice
2019-2020

THÉORÈME DE WEDDERBURN

Référence : Perrin, Cours d'algèbre, page 82.

Théorème 1. *Tout corps fini est commutatif.*

Soit $\mathbb{k}$ un corps et soit $n \in \mathbb{N}^*$. Supposons que n est premier à la caractéristique de $\mathbb{k}$. L'ensemble des racines n-ièmes de l'unité dans $\mathbb{k}$ est noté $\mu_n(\mathbb{k})$

$$\mu_n(\mathbb{k}) = \big\{\zeta \in \mathbb{k} \,|\, \zeta^n = 1\big\}.$$

C'est un sous-groupe de $\mathbb{k}^*$, de cardinal $\leq n$, donc cyclique.

Notons K_n le corps de décomposition de $P_n = X^n - 1$ sur $\mathbb{k}$. Alors $|\mu_n(K_n)| = n$ et $\mu_n(K_n) \simeq \mathbb{Z}/n\mathbb{Z}$. De plus comme $\mu_n(\mathbb{k})$ est inclus dans $\mu_n(K_n)$, on a $\mu_n(\mathbb{k}) \simeq \mathbb{Z}/d\mathbb{Z}$ pour un certain diviseur d de n.

Une racine n-ième primitive de 1 est un élément ζ de K_n tel que $\zeta^n = 1$ et $\zeta^d \neq 1$ pour $d < n$. Autrement dit ζ est un générateur du groupe $\mu_n(K_n)$ de sorte qu'il y a $\varphi(n)$ racines primitives de 1 (voir [Perrin, Cours d'algèbre, page 24]). Leur ensemble est noté $\mu_n^*(K_n)$.

Le n-ième polynôme cyclotomique $\phi_{n,\mathbb{k}} \in K_n[X]$ est donné par la formule

$$\phi_{n,\mathbb{k}}(X) = \prod_{\zeta \in \mu_n^*(K_n)} (X - \zeta).$$

Remarques 2.
- Si ζ est une racine n-ième primitive de l'unité, les autres sont les ζ^m avec $\mathrm{pgcd}(n, m) = 1$.
- Le polynôme $\phi_{n,\mathbb{k}}$ est unitaire, de degré $\varphi(n)$.

Proposition 3. *On a la formule*

$$X^n - 1 = \prod_{d|n} \phi_{d,\mathbb{k}}(X).$$

Démonstration. Cela résulte de l'égalité

$$X^n - 1 = \prod_{d|n} \phi_d(X)$$

(l'union est ici disjointe) qui dit que si ζ est une racine n-ième de 1, l'ordre de ζ est un diviseur de n. □

Remarque 4. En comparant les degrés des polynômes on retrouve la formule

$$n = \sum_{d|n} \varphi(d).$$

Démonstration du Théorème 1. Considérons un corps fini $\Bbbk$. On note $Z(\Bbbk)$ le centre de $\Bbbk$:

$$Z(\Bbbk) = \big\{a \in \Bbbk \,|\, \forall\, x \in \Bbbk,\, xa = ax\big\}$$

$Z(\Bbbk)$ est un sous-corps commutatif de $\Bbbk$ de cardinal $q \geq 2$. Puisque $\Bbbk$ est un $Z(\Bbbk)$-espace vectoriel on a $|\Bbbk| = q^n$.

Si $\Bbbk$ est commutatif la démonstration est terminée. Supposons donc $\Bbbk$ non commutatif. En particulier $n > 1$. Alors $\Bbbk^*$ opère sur lui-même par automorphismes intérieurs

$$\iota_g \colon \Bbbk^* \to \Bbbk^*, \qquad\qquad x \mapsto gxg^{-1}.$$

Considérons cette action. Pour $g \in \Bbbk^*$ on note $\mathcal{O}_g$ l'orbite de g. Posons

$$\Bbbk_g = \big\{x \in \Bbbk \,|\, gx = xg\big\}.$$

Notons que $\Bbbk_g$ est un sous-corps de $\Bbbk$ (pas nécessairement commutatif). Le stabilisateur de g est $\Bbbk_g^*$.

On a $|\Bbbk_g| = q^d$; de plus d divise n (en effet l'inclusion $\Bbbk_g^* \subset \Bbbk^*$ entraîne que $q^d - 1$ divise $q^n - 1$ et pour $q \in \mathbb{N}$, $q \geq 2$, ceci implique que d divise n). Le cardinal de $\mathcal{O}_g$ est

$$|\mathcal{O}_g| = \frac{|\Bbbk^*|}{|\Bbbk_g^*|} = \frac{q^n - 1}{q^d - 1}.$$

Par définition des polynômes cyclotomiques on a dans $\mathbb{Z}$

$$q^n - 1 = \prod_{m|n} \phi_m(q)$$

et

$$q^d - 1 = \prod_{m|d} \phi_m(q).$$

Il en résulte que

$$\frac{q^n - 1}{q^d - 1} = \prod_{m|n,\, m\nmid d} \phi_m(q).$$

En particulier $\phi_n(q)$ divise $\frac{q^n-1}{q^d-1}$.

D'après l'équation aux classes

$$|\Bbbk^*| = |Z(\Bbbk)^*| + \sum_{g \notin Z(\Bbbk)} |\mathcal{O}_g|.$$

Or $g \notin Z(\Bbbk)$ si et seulement si $d \neq n$ de sorte que

$$q^n - 1 = q - 1 + \sum \frac{q^n - 1}{q^d - 1}$$

la somme portant sur un certain nombre de diviseurs stricts de n. Par suite $\phi_n(q)$ divise $q - 1$. En particulier $|\phi_n(q)| \leq q - 1$.

Notons $\zeta_1, \ldots, \zeta_\ell$ les racines primitives $n$ièmes de 1 ; elles vérifient

$$\begin{cases} |\xi_i| \\ \xi_i \neq 1 \text{ (car } n \neq 1) \end{cases}$$

On a $\phi_n(q) = (q-\zeta_1)(q-\zeta_2)\ldots(q-\zeta_\ell)$. Pour tout i on a $|q-\zeta_i| > q-1$. Ainsi

$$|\phi_n(q)| > (q-1)^\ell \geq q-1$$

contradiction.

□