

Théorème de Wedderburn

Arnaud GIRAND

5 juillet 2012

Référence :

– [Per96], p. 82

Proposition 1 (Wedderburn)

Tout anneau à division fini est un corps.

DÉMONSTRATION : Soit \mathbb{K} un anneau à division fini. Considérons son centre $Z := \{a \in \mathbb{K} \mid \forall x \in \mathbb{K}, ax = xa\}$. Alors Z est un corps contenu dans \mathbb{K} , de cardinal $q \geq 2$ (car $0, 1 \in Z$). De fait, on peut munir \mathbb{K} d'une structure de Z -espace vectoriel de dimension finie $n \geq 1$, qui nous donne l'égalité $|\mathbb{K}| = q^n$.

Supposons à présent \mathbb{K} non commutatif, i.e $n > 1$. Remarquons que le groupe \mathbb{K}^* agit sur lui-même par conjugaison. Si $x \in \mathbb{K}^*$, on note $\omega(x)$ son orbite sous cette action, $\mathbb{K}_x := \{y \in \mathbb{K} \mid yx = xy\}$ et $\mathbb{K}_x^* := \{y \in \mathbb{K}^* \mid yx = xy\}$ son stabilisateur. \mathbb{K}_x est un sous-anneau de \mathbb{K} contenant Z et peut donc être vu comme un Z -espace vectoriel de dimension finie $d \geq 1$ avec de facto l'égalité $|\mathbb{K}_x| = q^d$.

Comme \mathbb{K}_x^* est un sous-groupe de \mathbb{K}^* , alors par théorème de Lagrange $q^d - 1 \mid q^n - 1$ et donc comme $q \geq 2$, $d \mid n$. Ainsi, pour $x \in \mathbb{K}^*x$, on a :

$$|\omega(x)| = \frac{|\mathbb{K}^*|}{|\mathbb{K}_x^*|} = \frac{q^n - 1}{q^d - 1} = \frac{\prod_{m \mid n} \phi_m(q)}{\prod_{m \mid d} \phi_m(q)} = \prod_{m \mid n, m \nmid d} \phi_m(q)$$

Où ϕ_m dénote le m -ième polynôme cyclotomique sur \mathbb{C} . Alors, dans le cas où $d \neq n$ (possible car $n > 1$), on a :

$$\phi_n(q) \mid \frac{q^n - 1}{q^d - 1} \tag{1}$$

La formule des classes s'écrit alors :

$$|\mathbb{K}^*| = |Z^*| + \sum |\omega(x)| \tag{2}$$

Où la somme compte chaque orbite une fois. On a donc :

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

Où la somme décrit un sous ensemble des diviseurs stricts de n associé aux orbites par le procédé précédent. Comme $\phi_n(q)$ divise $q^n - 1$ et par la relation (1), on a :

$$\phi_n(q) \mid q - 1$$

De fait, $|\phi_n(q)| \leq q - 1$. Mais si on note ξ_1, \dots, ξ_ℓ les racines primitives n -ièmes de l'unité sur \mathbb{C} (les $\xi_i \neq 1$ car $n \neq 1$) alors :

$$\phi_n(q) = \prod_{i=1}^{\ell} (q - \xi_i)$$

De plus $\forall i \in [\ell]$, $|q - \xi_i| > 1$ (car les ξ_i sont sur le cercle unité et différentes de 1 : faire un dessin), d'où :

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

Ce qui apporte la contradiction désirée.

Détails supplémentaires :

- Il est bon de savoir démontrer le lemme suivant :

Lemme 1

Soit $q \in \mathbb{N}$, $q \geq 2$.

Soient $n, d \in \mathbb{N}$ tels que $q^d - 1 \mid q^n - 1$.

Alors $d \mid n$.

DÉMONSTRATION : Par division euclidienne, il existe un unique couple (a, b) d'entiers naturels tels que $n = ad + b$ et $0 \leq b < d$. En remarquant que $q^d \equiv 1[q^d - 1]$, on a :

$$q^n \equiv (q^d)^a q^b \equiv q^b [q^d - 1]$$

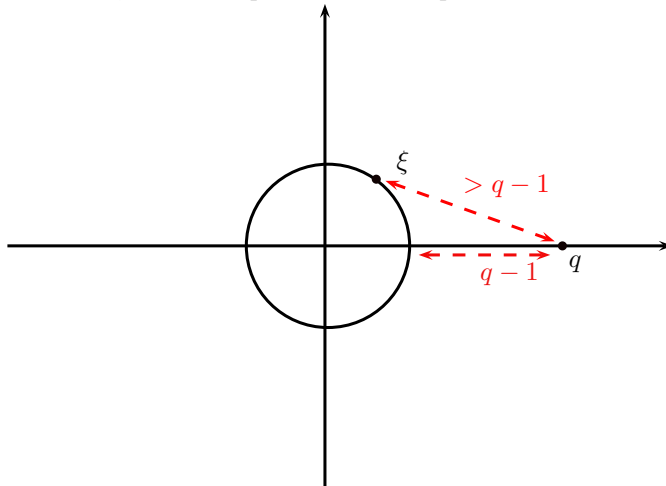
Or $q^n \equiv 1[q^d - 1]$ par hypothèse d'où $q^d - 1 \mid q^b - 1$. Cependant, $b < d$ et $q \geq 2$ donc $q^b - 1 < q^d - 1$ donc nécessairement $b = 0$.

- On trouve l'écriture suivante de la formule (2) dans [Per96] :

$$|\mathbb{K}^*| = |Z^*| + \sum_{x \notin Z} |\omega(x)|$$

Cependant on "compte" alors chaque orbite plusieurs fois, d'où la nécessité de restreindre la somme à un représentant par orbite (on peut aussi sommer sur l'espace quotient \mathbb{K}^*/\sim , où $x \sim y \Leftrightarrow \exists g \in \mathbb{K}^*, gxg^{-1} = y$). On pourra se référer à [Art91], p. 198.

- Si ξ est une racine primitive n -ième de l'unité alors les autres sont les ξ^m , avec $m \wedge n = 1$. Ainsi dans la démonstration, $\ell = \varphi(n)$ (cf. [Per96], p.80).
- En bonus, un dessin pour mieux comprendre la fin de la démonstration :



Références

[Art91] Michael Artin. *Algebra*. Prentice-Hall, 1991.

[Per96] Daniel Perrin. *Cours d'algèbre*. Ellipses, 1996.