# Théorème de Wedderburn

## Mon développement

On dit qu'un anneau $A$ est un corps si :
(i) $A$ est non réduit à $\{0\}$,
(ii) Tout élément non nul de $A$ est inversible,
(iii) $A$ est commutatif.

**Théorème.** Soit $A$ un anneau fini vérifiant (i) et (ii). Alors, $A$ est un corps.

Il suffit de montrer que $A$ est commutatif. On note

$$Z(A) = \{x \in A \mid \forall y \in A, xy = yx\}$$

son centre. Comme $Z(A)$ est un sous-anneau commutatif de $A$ et $A$ vérifie (i) et (ii), $Z(A)$ est muni d'une structure de corps. On peut donc voir $A$ comme un $Z(A)$-espace vectoriel. Sa dimension est finie puisque $A$ est fini, on la note $l$. En notant $q = \mathrm{Card}(Z(A))$, on a $\mathrm{Card}(A) = q^l$.
Remarquons que $A$ est non réduit à $\{0\}$ donc $Z(A)$ contient 0 et 1 et donc $q \geq 2$. Cela sera utilisé à plusieurs reprises par la suite.

Pour tout $x \in A^\times$, on note $A_x = \{y \in A \mid xy = yx\}$. Comme précédemment, on montre que $A_x$ est un sous-anneau de $A$. Comme il contient $Z(A)$, il peut être vu comme un $Z(A)$-espace vectoriel, donc il existe $d_x \in \mathbb{N}^*$ tel que $\mathrm{Card}(A_x) = q^{d_x}$.
On sait que le groupe $A^\times$ opère sur lui-même par conjugaison. Pour cette action, le stabilisateur d'un élément $x \in A^\times$ est $A_x^\times$, donc le cardinal de l'orbite $\omega(x)$ de $x$ est égal à

$$\frac{\mathrm{Card}(A^\times)}{\mathrm{Card}(A_x^\times)} = \frac{q^l - 1}{q^{d_x} - 1} \ .$$

Par le lemme situé à la fin de la démonstration, cela impose que $d_x | \, l$.
De plus, on en déduit que

$$\begin{aligned} \mathrm{Card}(\omega(x)) = 1 &\Leftrightarrow \mathrm{Card}(A^\times) = \mathrm{Card}(A_x^\times) \\ &\Leftrightarrow d_x = l \quad (\text{car } q \geq 2). \end{aligned}$$

Par ailleurs, on a

$$\begin{aligned} \mathrm{Card}(\omega(x)) = 1 &\Leftrightarrow \mathrm{Card}(A^\times) = \mathrm{Card}(A_x^\times) \\ &\Leftrightarrow A_x^\times = A^\times \quad (\text{car } A_x^\times \subset A^\times) \\ &\Leftrightarrow x \in Z(A)^\times \ . \end{aligned}$$

En notant $S$ un système de représentants de l'ensemble des orbites, d'après la formule des classes, on a donc

$$\mathrm{Card}(A^\times) = \mathrm{Card}(Z(A)^\times) + \sum_{x \in S \setminus Z(A)^\times} \mathrm{Card}(\omega(x)) \ ,$$

d'où :

$$q^l - 1 = q - 1 + \sum_{x \in S \setminus Z(A)^\times} \frac{q^l - 1}{q^{d_x} - 1} \tag{1}$$

où $\forall x \in S \setminus Z(A)^\times$, $d_x | l$ et $d_x \neq l$.

Par une propriété élémentaire des polynômes cyclotomiques, on a

$$q^l - 1 = \prod_{m|\, l} \phi_m(q) \quad \text{et} \quad \forall x \in A^\times,\ q^{d_x} - 1 = \prod_{m|\, d_x} \phi_m(q)\ .$$

Donc, pour tout $x \in S \setminus Z(A)^\times$, on a

$$\frac{q^l - 1}{q^{d_x} - 1} = \prod_{\substack{m|\, l,\\ m\nmid d_x}} \phi_m(q)\ .$$

Comme $l \neq d_x$ et $q \geq 2$, on a donc

$$\phi_l(q) \left| \frac{q^l - 1}{q^{d_x} - 1} \right.\ .$$

D'après (1), on en déduit que $\phi_l(q) | q - 1$.

Par définition des polynômes cyclotomiques, il existe $r \in \mathbb{N}^*$ et des nombres complexes $\zeta_1, \ldots, \zeta_r$ de module 1, distincts, tels que

$$\phi_l(X) = \prod_{i=1}^{r} (X - \zeta_i)\ .$$

D'après l'inégalité triangulaire appliquée aux $q - \zeta_i$, on a donc

$$|\phi_l(q)| \geq \prod_{i=1}^{r} (q-1) \geq q - 1$$

car $q - 1 \geq 1$ et $r \geq 1$. Or on a vu que $\phi_l(q) | q - 1$, on est donc dans le cas d'égalité de l'inégalité triangulaire et les $\zeta_i$ sont donc égaux à 1. Puisque ceux-ci sont distincts, on en déduit que $r = 1$, $\zeta_1 = 1$, $\phi_l = X - 1 = \phi_1$ et finalement $l = 1$.
On a donc $\mathrm{Card}(A) = q = \mathrm{Card}(Z(A))$, d'où $Z(A) = A$. $A$ est donc commutatif et c'est un corps. □

**Lemme.** Soient $q, a, b \in \mathbb{N}^*$ tels que $q \geq 2$ et $q^a - 1 | q^b - 1$. Alors $a | b$.

En effet, soit $b = ka + r$, $0 \leq r < a$ la division euclidienne de $b$ par $a$. En écrivant

$$\begin{aligned} q^b - 1 &= \sum_{i=2}^{k} (q^{ia+r} - q^{(i-1)a+r}) + q^{a+r} - 1 \\ &= \sum_{i=2}^{k} (q^a - 1) q^{(i-1)a+r} + q^r (q^a - 1) + q^r - 1\ , \end{aligned}$$

on obtient que $q^r - 1 \equiv 0[q^a - 1]$. Comme $0 \leq q^r - 1 < q^a - 1$, on a $q^r - 1 = 0$. Comme $q \geq 2$, on obtient finalement $r = 0$ et $a | b$. □

## Références

J'ai utilisé [Per96, p. 82]. On peut aussi consulter [Gou09, p. 93], [Goz09, p. 82].

## Leçons correspondantes

J'utilise ce développement pour les leçons 101, 112, 151. On peut également l'utiliser pour les leçons 113, 120.

## Remarques

- En général, on trouve l'énoncé suivant du théorème de Wedderburn : « tout corps fini non nécessairement commutatif est commutatif ».
- Ce développement est archi-classique, et donc le jury peut en avoir marre de se le voir proposer ; d'autre part, il faut en maîtriser les moindres détails.
- Après coup, ce développement ne semble pas très adapté pour les leçons 120 et 151.
- On peut détailler davantage certains points, notamment au début.
- On peut traiter le lemme avec des polynômes : $X^a - 1$ divise $X^b - 1$ si et seulement si $a \mid b$.
- Implicitement, on a utilisé le fait que les polynômes cyclotomiques sont à coefficients entiers, ou du moins que $\phi_l(q) \in \mathbb{Z}$, puisqu'on parle de divisibilité dans $\mathbb{Z}$.
- Attention, a priori, $A_x$ n'est pas commutatif, donc n'est pas un corps. On ne peut donc pas utiliser le théorème de la base télescopique pour montrer que $d_x \mid l$ puisque $A$ ne peut pas être vu comme un $A_x$-espace vectoriel.

## Questions possibles

1. Donner un exemple de corps non commutatif.
2. Définir une action de groupe, une orbite et un stabilisateur.
3. Citer des propriétés des polynômes cyclotomiques.
4. Justifier que si $\phi_l = \phi_1$, alors $l = 1$.
5. À partir d'une propriété des polynômes cyclotomiques utilisée dans ce développement, montrer que
$$n = \sum_{d \mid n} \varphi(d) \ ,$$
où $\varphi$ désigne l'indicatrice d'Euler.

# Références

[Gou09] Xavier Gourdon : *Algèbre*. Ellipses, 2009.

[Goz09] Ivan Gozard : *Théorie de Galois*. Ellipses, 2009.

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