PRÉPARATION À L'AGRÉGATION EXTERNE : THÉORÈME DE WEDDERBURN

TONY LIMAGNE

Résumé. A priori, il n'existe aucun lien apparent entre le nombre d'éléments d'un système algébrique et la loi de multiplication de ce système. Pourtant c'est ce qu'illustre une preuve du théorème de Wedderburn dûe à Ernst Witt. L'idée fondamentale est de voir un anneau intègre fini comme un espace vectoriel sur son centre (donc comme un système algébrique) puis d'étudier le comportement de cette structure par rapport à l'action par conjuguaison (donc de faire jouer la loi de multiplication). D'ailleurs l'étude de cette action fait naturellement intervenir les polynômes cyclotomiques dont on connait les propriétés arithmétiques, ce qui est intéressant puisqu'on réduit alors le problème à des considérations purement arithmétiques. Le tout permet de démontrer par l'absurde l'un des résultat fondateur de la théorie des groupes finis : le théorème de Wedderburn.

Le développement ci-dessous est adapté pour les leçons 101, 102, 103, 104, 123 et 125.

1. Préliminaires autour des polynômes cyclotomiques

La preuve du théorème de Wedderburn repose sur la théorie des groupes. Le premier résultat remarquable de la théorie est le lemme 1 qui servira pour prouver la proposition 2.

Lemme 1. Soit G un groupe cyclique d'ordre n.

(1) Tout sous-groupe de G est cyclique.

(2) Pour tout diviseur $d > 0$ de n il existe un unique sous-groupe (cyclique) H_d d'ordre d.

En particulier, on en déduit la formule

$$n = \sum_{d|n} \phi(d). \tag{E}$$

où ϕ désigne l'indicatrice d'Euler.

Démonstration. Sans perte de généralité on suppose $G = \mathbb{Z}/n\mathbb{Z}$.
(1) On note $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ la surjection canonique, et on fixe H un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$. Comme $\pi^{-1}(H)$ est un sous-groupe de $\mathbb{Z}$ il existe $a \in \mathbb{N}$ tel que

$$\pi^{-1}(H) = a\mathbb{Z}.$$

Et puisque π est surjective on a $H = \pi(\pi^{-1}(H)) \subseteq \langle \pi(a) \rangle$ et donc $H = \langle \pi(a) \rangle$.
(2) Fixons d un diviseur (positif) de n. On pose $a = \frac{n}{d}$. Pour tout $m \in \mathbb{Z}$ on a

$$\pi(a)m = 0 \quad \Leftrightarrow \quad \pi(am) = 0 \quad \Leftrightarrow \quad n|am.$$

L'entier minimal qui vérifie cette propriété est bien sûr $m = d$. Ainsi $H = \langle \pi(a) \rangle$ est un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ d'ordre d.

Date: Année 2024.

Soient H et H' deux sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ d'ordre d. On sait d'après le point (1) qu'il existe $a, a' \in \mathbb{N}$ tel que $H = \langle \pi(a) \rangle$ et $H' = \langle \pi(a') \rangle$. Comme H et H' sont deux sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ alors $\pi^{-1}(\{0\}) = n\mathbb{Z}$ est à la fois inclus dans $\pi^{-1}(H) = a\mathbb{Z}$ et dans $\pi^{-1}(H') = a'\mathbb{Z}$, et donc n divise à la fois a et a'. Posons $b = n/a$ et $b' = n/a'$. On sait que par ce qui précède que H est d'ordre n/b et H' est d'ordre n/b' si bien que

$$d = \frac{n}{b} = \frac{n}{b'},$$

ce qui implique $a = a'$ et donc $H = H'$.

Notons $N(d)$ le nombre déléments de $\mathbb{Z}/n\mathbb{Z}$ d'ordre d. Si x est un élément de G d'ordre d alors $\langle x \rangle$ est un groupe d'ordre d de $\mathbb{Z}/n\mathbb{Z}$ si bien que $H_d = \langle x \rangle$. Ainsi on a $N(d) \leqslant \phi(d)$ et donc $N(d) = \phi(d)$. On conclut par le théorème de Lagrange $n = \sum_{d|n} N(d) = \sum_{d|n} \phi(d)$. □

Référence : [C, Chap. III, §B, Théorème 3.10 et Théorème 3.14].

Pour $n \in \mathbb{N}^*$ on appelle *racine n^e primitive de l'unité* tout générateur du groupe des racines n^e de l'unité (dans $\mathbb{C}$). Le n^e *polynôme cyclotomique* est défini par

$$\Phi_n(X) = \prod_{\zeta \in \mu_n^*} (X - \zeta),$$

où μ_n^* est l'ensemble des racines primitives n^e de l'unité.

Proposition 2. Soit $n \geqslant 1$ un entier.

(1) On a $X^n - 1 = \prod_{d|n} \Phi_d$.

(2) Le polynôme Φ_n est à coefficients entiers.

Démonstration. (1) Comparons ces deux polynômes. On vérifie facilement que

$$\bigcup_{d|n} \{\text{racines de } \Phi_d\} = \{\text{racines de } X^n - 1\}.$$

On sait que les racines de $X^n - 1$ sont bien simples. Les racines de $\prod_{d|n} \phi_d$ sont aussi simples. En effet, si α est une racine commune à Φ_d et $\Phi_{d'}$ pour d, d' deux diviseurs de n alors α est à la fois un générateur de $\mathbb{U}_d$ et un générateur de $\mathbb{U}_{d'}$. Or $\mathbb{U}_d$ et $\mathbb{U}_{d'}$ sont des sous-groupes de $\mathbb{U}_n$ (car d et d' divisent n). Par unicité de l'ordre de α dans $\mathbb{U}_n$, on a $o(\alpha) = d = d'$. Enfin les polynômes $X^n - 1$ et $\prod_{d|n} \phi_d$ sont tous deux unitaires et de même degré par la formule (E).

(2) On raisonne par récurrence forte sur n. On a $\Phi_1(X) = X - 1$, $\Phi_2(X) = X + 1$, $\Phi_3(X) = X^2 + X + 1$. Fixons $n \in \mathbb{N}^*$. On suppose que les polynômes $\Phi_1, \ldots, \Phi_{n-1}$ sont à coefficients entiers. On a la factorisation

$$X^n - 1 = \Phi_n \prod_{d|n, d \neq n} \Phi_d.$$

En notant $F(X) = \prod_{d|n, d\neq n} \Phi_d$ on a $F(X) \in \mathbb{Z}[X]$ par hypothèse de récurrence. Et puisque $F(X)$ est unitaire on peut effectuer la division euclidienne de $X^n - 1$ par $F(X)$ dans $\mathbb{Z}[X]$: $X^n - 1 = Q(X)F(X) + R(X)$ avec $\deg(R(X)) < \deg(F(X))$. On a alors

$$(\Phi_n(X) - Q(X))F(X) = R(X),$$

ce qui donne au niveau des degrés

$$\deg(\Phi_n(X) - Q(X)) + \deg(F(X)) = \deg(R(X)) < \deg(F(X)),$$

et donc $\deg(\Phi_n(X) - Q(X)) = -\infty$ c'est-à-dire $\Phi_n(X) = Q(X) \in \mathbb{Z}[X]$. □

Référence : [P, Chap. III, §4, Proposition 4.5 et Proposition 4.8].

2. Anneau vu comme espace vectoriel sur son centre

En ce qui nous concerne, on appellera *corps* tout anneau **commutatif** unitaire dont tous les éléments non nuls sont inversibles.

2.1. Une "formule des degrés".

Lorsque A est un anneau unitaire on sait que le centre Z de A est un corps. La multiplication interne de A permet de munir A d'une structure d'espace vectoriel sur Z.

Lemme 3 ("Formule des degrés")**.** Soit A un anneau unitaire dont on note Z le centre. Soit B un sous-corps de A qui contient Z. L'anneau A est un B-espace vectoriel et on a

$$\dim_Z(A) = \dim_B(A) \cdot \dim_Z(B).$$

Démonstration. Le corps B est une extension du corps Z (pour l'inclusion naturelle). Fixons $(a_i)_{i\in I}$ une base de A sur B et $(b_j)_{j\in J}$ une base de B sur Z. La famille $(b_j a_i)$ est libre. En effet, si

$$\sum_{i,j} \lambda_{ij} b_j a_i = 0,$$

avec $(\lambda_{ij}) \in Z^{(I\times J)}$ alors $\sum_i \left(\sum_j \lambda_{ij} b_j\right) a_i = 0$. On note $\mu_i = \sum_j \lambda_{ij} b_j$. Puisque (a_i) est une base de A sur B et que les μ_i sont dans B on a $\mu_i = 0$ pour tout i. Enfin, puisque (b_j) est une base de B sur Z on a $\mu_{ij} = 0$ pour tout i, j. La famille $(b_j a_i)$ est également génératrice. En effet, si $x \in A$ on l'écrit $x = \sum_i \mu_i a_i$, pour $(\mu_i) \in B^{(I)}$ puis on décompose $\mu_i = \sum_j \lambda_{ij} b_j$ avec $\lambda_{ij} \in Z^{(J)}$ d'où finalement $x = \sum_{ij} \lambda_{ij} b_j a_i$. □

Par analogie avec les extensions de corps, on note $\dim_Z(A) = [A : Z]$ et $\dim_B(A) = [A : B]$ en gardant à l'esprit que A n'est pas nécessairement un corps.

2.2. Développement.

Théorème 4 (Wedderburn)**.** Tout anneau unitaire intègre fini est un corps.

Démonstration. Soit A un anneau unitaire intègre fini. Pour $a \in A\backslash\{0\}$ l'application

$$A \setminus \{0\} \to A \setminus \{0\}, b \mapsto ab,$$

est injective (par intégrité de A) et donc bijective (par finitude de A). Il existe donc $b \neq 0$ tel que $ab = 1$. Toujours par intégrité de A on a aussi $ba = 1$ car

$$ab = 1 \quad \Rightarrow \quad bab = b \quad \Leftrightarrow \quad (ba - 1)b = 0 \quad \Leftrightarrow \quad ba = 1.$$

Ainsi a est inversible et donc $A^\times = A \setminus \{0\}$. On opère $A^\times$ sur A par conjugaison. Le stabilisateur d'un point $x \in A$ est $C_x^* = \{\sigma \in A^\times : \sigma x = x\sigma\}$. L'ensemble $C_x = C_x^* \cup \{0\}$ est un sous-corps de A, de même que l'ensemble

$$Z = \bigcap_{x\in A} C_x.$$

Comme A est fini on a une tour d'espaces vectoriels de dimensions finies

$$Z \subseteq C_x \subseteq A,$$

et par la "formule des degrés" : $[A : Z] = [A : C_x][C_x : Z]$. On note $n_x = [C_x : Z]$ et $n = [A : Z]$. Par l'absurde, supposons A non commutatif c'est-à-dire

$$\Lambda = \{x \in A : C_x \neq A\} = \{x \in A : n_x < n\} \neq \emptyset.$$

Fixons $\{x_1, \dots, x_t\}$ un système de représentants des orbites non singletons. Par l'équation aux classes on a

$$|A| = |Z| + \sum_{i=1}^{t} \frac{|A^\times|}{|C^*_{x_i}|}.$$

En notant $q = |Z|$ et $n_{x_i} = n_i$ cette formule devient, après compensation par -1,

$$q^n - 1 = q - 1 + \sum_{i=1}^{t} \frac{q^n - 1}{q^{n_i} - 1}. \tag{1}$$

Fisons $i \in [\![1, t]\!]$. La proposition 2 donne

$$q^n - 1 = \prod_{d|n} \Phi_d(q) = \Phi_n(q) \prod_{d|n_i} \Phi_d(q) \prod_{d|n, d\neq n, d\nmid n_i} \Phi_d(q) = \Phi_n(q)(q^{n_i} - 1)P_i(q),$$

avec $P_i(q) \in \mathbb{Z}$. Ainsi $\Phi_n(q)$ divise à la fois $q^n - 1$ et $\frac{q^n-1}{q^{n_i}-1}$ et donc $\Phi_n(q)$ divise $q - 1$. Or une racine λ de Φ_n vérifie $|\lambda| = 1$ et $|\Re(\lambda)| < 1$ (faire un dessin) et donc $\Phi_n(q)^2 = \prod_\lambda |q - \lambda|^2 > \prod_\lambda (q - 1)^2 \geqslant (q - 1)^2$. Absurde. [1] □

Référence : [P, Chap. III, §4, Théorème 4.9].

3. Quelques questions bêtes auxquelles il faut absolument savoir répondre rapidement

(1) À quels endroits de la preuve a-t-on utilisé l'hypothèse $\Lambda \neq \emptyset$?

(2) Montrer qu'une algèbre de dimension finie sur un corps est un corps.

Références

[P] D. Perrin, *Cours d'algèbre*, Ellipses, 1996.

[C] J. Calais, *Éléments de théorie des groupes*, Puf, 2016.

1. Pour $n = 2$ la dernière phrase du raisonnement est faux (car $\lambda = -1$). Pour ce cas particulier il faut remarquer que $\Phi_2(q) = q + 1 > q - 1$.