Théorème de Wedderburn

28 avril 2013

On dit qu'un anneau A est à division s'il est intègre et si pour tout $a \in A \setminus \{0\}$, il existe un unique élément noté a^{-1} tel que $aa^{-1} = a^{-1}a = 1_A$. On dit que A est fini s'il n'a qu'un combre fini d'élément. L'application $\varphi_A : \begin{array}{ccc} \mathbb{Z} & \to & A \\ k & \mapsto & k.1_A \end{array}$ est un morphisme d'anneau. $\mathrm{Ker}(\varphi_A)$ est donc un idéal de $\mathbb{Z}$ qui est principal. Il existe donc $c \in \mathbb{N}$ tel que $\mathrm{Ker}(\varphi_A) = (c) = c\mathbb{Z}$. On appelle c la caractéristique de A.

Proposition 1. *Soit K un anneau à division fini, q son cardinal et p sa caractéristique. Alors, p est un nombre premier et le sous-corps premier P de K est $\mathbb{F}_p$. Il existe $n \in \mathbb{N}$ tel que $q = p^n$.*

Démonstration. Comme K est fini $p \neq 0$. Supposons qu'il existe q et m tels que $qm = p$. Alors $q1_K \neq 0$, $m1_K \neq 0$ mais $qm1_K = 0$ ce qui est absurde car K est intègre. φ_k induit un isomorphisme d'anneau $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \simeq \mathrm{Im}\varphi_k$ qui est un sous-corps de K. Comme $P \subset \mathrm{Im}\varphi_k$ et que $\mathbb{F}_p$ est premier, on a $P \simeq \mathbb{F}_p$.

K peut être vu comme un P-espace vectoriel de dimension finie. Soit n sa dimension. K est isomorphe à P^n donc $q = p^n$. □

Proposition 2. *Equation aux classes. On note $(C_i)_{1\leq i\leq k}$ les classes de conjugaison de G. On note x_i un représentant (arbitrairement choisi) de C_i pour tout i et $\mid Z_i \mid := \mid \{g \in G \mid gx_ig^{-1} = x_i\} \mid$ l'ordre du stabilisateur de x_i sous l'action G. Dans ce cas, l'ordre de G vérifie l'équation aux classes que l'on formule ainsi :*

$$\mid G \mid = \mid Z(G) \mid + \sum_{i=1, x_i \notin Z(G)}^{k} \frac{\mid G \mid}{\mid Z_i \mid}$$

Démonstration. L'action naturelle de G est définie par $\begin{cases} G \times G & \to G \\ g, x & \mapsto gxg^{-1} \end{cases}$. D'après la relation sur les cardinaux des orbites, on a :

$$\mid G \mid = \mid Z_i \mid \cdot \mathrm{card}(C_i) \ \forall i \in \{0, \ldots, k\}$$

On sait que C_i est réduit à un élément x_i si et seulement si $x_i \in Z(G)$. Par ailleurs, comme les C_i forment une partition de G, on a

$$\begin{aligned} \mid G \mid &= \sum_{i=1}^{k} \mathrm{card}(C_i) = \sum_{i \mid x_i \in Z(G)} \mathrm{card}(C_i) + \sum_{x_i \notin Z(G)} \mathrm{card}(C_i) \\ &= \sum_{x_i \in Z(g)} 1 + \sum_{x_i \notin Z(G)} \frac{\mid G \mid}{\mid Z_i \mid} = \mid Z(G) \mid + \sum_{i=1, x_i \notin Z(G)}^{k} \frac{\mid G \mid}{\mid Z_i \mid} \end{aligned}$$

□

Proposition 3. $X^n - 1 = \prod_{d \mid n} \Phi_d(X)$ *où* $\Phi_d(X) = \prod_{\substack{1 \leq k \leq d \\ k \wedge d = 1}} (X - e^{\frac{2ik\pi}{d}})$

Démonstration. $\cup_{d \mid n} \{1 \leq k \leq d \mid k \wedge d = 1\} = \{1, \ldots, n\}$ est une union disjointe donc le résultat s'en suit. □

Théorème. *Wedderburn : Soit K un anneau à division fini. Alors, K est commutatif. En particulier, K est un corps.*

Démonstration. Soit K un anneau à division fini. On note $K^* = K \setminus \{0\}$, $p \neq 0$ la caractéristique de K et Z son centre. D'après le lemme 1, le sous-corps premier de K est $\mathbb{F}_p$. d'autre part, Z est un $\mathbb{F}_p$-espace vectoriel et K est un Z-espace vectoriel. Notons r (resp. n) la dimension du $\mathbb{F}_p$-espace vectoriel Z (resp. du Z-espace vectoriel K). Si $q = \text{card}Z$, on obtient $q = p^r$ et $\text{card}K = q^n$.

Pour $x \in K^*$, on note $C_x := \{y \in K \mid xy = yx\}$ le centralisateur de x dans K et $C_x^* = C_x \cap K^*$. C_x est un anneau à division fini et C_x^* est un groupe. Comme $Z \subset C_x$, il existe $d(x) \in \mathbb{N}^*$ tel que $\text{card}C_x = q^{d(x)}$. Comme C_x^* est un sous-groupe de K^*, $q^{d(x)} - 1$ divise $q^n - 1$.

Soit $n = s(x)d(x) + t(x)$ la division euclidienne de n par $d(x)$. On a

$$\begin{aligned} q^n - 1 &= \left(\left(q^{d(x)}\right)^{s(x)} - 1\right) q^{t(x)} + q^{t(x)} - 1 \\ &= \left(q^{d(x)} - 1\right)\left(\sum_{i=0}^{s(x)-1} q^{id(x)+t(x)}\right) + q^{t(x)} - 1 \end{aligned}$$

d'où on déduit que $q^{d(x)} - 1$ divise $q^{t(x)} - 1$. Comme $q \geq 2$ et $0 \leq t(x) < d(x)$, on déduit que $t(x) = 0$ donc $d(x)$ divise n.

Si $y \in K^*$, dire que $y \in Z$ signifie que $C_y = K$ et donc que $d(y) = n$. Supposons K non commutatif. Alors $n > 1$. On fait opérer K^* sur lui-même par conjugaison : $\begin{array}{ccc} K^* \times K^* & \to & K^* \\ x, z & \mapsto & xzx^{-1} \end{array}$. Il résulte de l'équation aux classes qu'il existe un ensemble S formé de diviseurs stricts de n tel que

$$q^n - 1 = q - 1 + \sum_{d \in S} \frac{q^n - 1}{q^d - 1} \ (*)$$

D'après la proposition 3, on

$$q^n - 1 = \prod_{m|n} \Phi_m(q),\ q^d - 1 = \prod_{m|d} \Phi_m(q)$$

On voit en particulier que si $d \mid n$ et $d < n$, $\Phi_n(q)$ divise $\frac{q^n-1}{q^d-1}$. Il resulte de $(*)$ que $\Phi_n(q)$ divise $q - 1$, donc $|\Phi_n(q)| \leq q - 1$.

Soit $\xi \in \mathbb{U}_n^*$ une racine primitive n-ième de l'unité. Comme $n \geq 2$, $\xi \neq 1$ d'où $|\xi - q| > q - 1$. En effet, si $\xi = -1$, $q + 1 > q - 1$ et si $\xi \neq -1$, $|\xi - q| > ||\xi| - |q|| = q - 1$. Alors $q - 1 \geq |\Phi_n(q)| > (q - 1)^{\varphi(n)} \geq q - 1$ ce qui est absurde. Ainsi, K est commutatif. □

Leçons concernées
101 Groupe opérant sur un ensemble. Exemples et applications.
123 Corps finis. Applications.

Références

[1] Patrice Tauvel. Corps Commuttaifs et Théorie de Galois. Calvage & Mounet.