Théorème de Wedderburn

En utilisant les polynômes cyclotomiques, nous montrons que tout corps fini est commutatif.

Lemme 1. Soient $\mathbb{K}$ et $\mathbb{L}$ deux corps finis tels que $\mathbb{K}$ est commutatif et $\mathbb{K} \subseteq \mathbb{L}$. Alors $\exists d \in \mathbb{N}^*$ tel que $|\mathbb{L}| = |\mathbb{K}|^d$.

[GOU21] p. 100

Démonstration. $\mathbb{L}$ est un espace vectoriel sur $\mathbb{K}$ de dimension finie d (car $\mathbb{L}$ est fini). Donc $\mathbb{L}$ est isomorphe en tant que $\mathbb{K}$-espace vectoriel à $\mathbb{K}^d$. En particulier, $|\mathbb{L}| = |\mathbb{K}|^d$. □

Théorème 2 (Wedderburn)**.** Tout corps fini est commutatif.

Démonstration. Soit $\mathbb{K}$ un corps. L'idée va être de procéder par récurrence sur le cardinal du corps.

— Si $|\mathbb{K}| = 2$: alors $\mathbb{K} = \{0, 1\}$ est commutatif.

— On suppose le résultat vrai pour tout corps fini de cardinal strictement inférieur à $\mathbb{K}$. On veut montrer que $\mathbb{K}$ est commutatif. Supposons par l'absurde que $\mathbb{K}$ ne l'est pas. On pose

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

le centre de $\mathbb{K}$ dont on note q le cardinal. C'est un sous-corps de $\mathbb{K}$ qui est (par hypothèse) inclus strictement dans $\mathbb{K}$. Donc Z est commutatif, et par le Lemme 1, on peut écrire $|\mathbb{K}| = q^n$ où $n \in \mathbb{N}^*$. Si $x \in \mathbb{K}$, on pose

$$\mathbb{K}_x = Z_{\mathbb{K}}(\{x\}) = \{y \in \mathbb{K} \mid xy = yx\}$$

Montrons que

$$\exists d \mid n \text{ tel que } |\mathbb{K}_x| = q^d \qquad (*)$$

Notons déjà encore une fois que $\mathbb{K}_x$ est un sous-corps de $\mathbb{K}$.

— Si $\mathbb{K}_x = \mathbb{K}$, on a $|\mathbb{K}_x| = |\mathbb{K}| = q^n$. Il suffit donc de prendre $d = n$.

— Sinon, $\mathbb{K}_x \subsetneq \mathbb{K}$, donc $\mathbb{K}_x$ est commutatif par hypothèse. Par le Lemme 1, il existe $k \in \mathbb{N}^*$ tel que $|\mathbb{K}| = |\mathbb{K}_x|^k$.

Mais, Z est un sous-corps (commutatif) de $\mathbb{K}_x$, donc d'après le Lemme 1, il existe $d \in \mathbb{N}^*$ tel que $|\mathbb{K}_x| = |Z|^d$. Donc on a

$$q^n = |\mathbb{K}| = |\mathbb{K}_x|^k = (q^d)^k = q^{dk}$$

d'où $d \mid n$.

On considère l'action par conjugaison de $\mathbb{K}^*$ sur lui-même $(x, y) \mapsto xyx^{-1}$. Si $y \in \mathbb{K}^*$, alors

$$\mathrm{Stab}_{\mathbb{K}^*}(y) = \{x \in \mathbb{K}^* \mid x.y = y\} = \mathbb{K}_y^*$$

Soit Ω un système de représentants associé à la relation d'équivalence "être dans la même orbite". L'équation aux classes donne alors

$$|\mathbb{K}^*| = \sum_{\omega\in\Omega} \frac{|\mathbb{K}^*|}{|\operatorname{Stab}_{\mathbb{K}^*}(\omega)|}$$

Or,

$$\operatorname{Stab}_{\mathbb{K}^*}(\omega) = \mathbb{K}^* \iff \forall x \in \mathbb{K}^*, \omega x = x\omega \iff \omega \in Z^*$$

donc en notant $\Omega' = \Omega \setminus Z^*$, on a :

$$|\mathbb{K}^*| = \sum_{\omega\in Z^*} \frac{|\mathbb{K}^*|}{|\operatorname{Stab}_{\mathbb{K}^*}(\omega)|} + \sum_{\omega\in\Omega'} \frac{|\mathbb{K}^*|}{|\operatorname{Stab}_{\mathbb{K}^*}(\omega)|} = |Z^*| + \sum_{\omega\in\Omega} \frac{|\mathbb{K}^*|}{|\mathbb{K}^*_\omega|} \qquad (**)$$

Soit $\omega \in \Omega'$. Par $(*)$,

$$\exists d \mid n \text{ tel que } |\operatorname{Stab}_{\mathbb{K}^*}(\omega)| = |\mathbb{K}^*_\omega| = q^d - 1$$

De plus, $d \neq n$ (car $\omega \notin Z^*$). Si maintenant on pose

$$\forall d \mid n,\ \lambda_d = |\{\omega \in \Omega' \mid |\operatorname{Stab}_{\mathbb{K}^*}(\omega)| = q^d - 1\}|$$

on peut alors écrire en remplaçant dans $(**)$:

$$q^n - 1 = |K^*| = (q-1) + \sum_{d||n} \lambda_d \left(\frac{q^n-1}{q^d-1}\right) \qquad (***)$$

Si $d \,||\, n$, on a

$$X^n - 1 = \prod_{k|n} \Phi_k = \Phi_n \left(\prod_{k|d} \Phi_k\right) \left(\prod_{\substack{k||n\\ k\nmid d}} \Phi_k\right) = \Phi_n (X^d - 1) \left(\prod_{\substack{k||n\\ k\nmid d}} \Phi_k\right)$$

Donc, $\Phi_n \mid \frac{X^n-1}{X^d-1}$ dans $\mathbb{Z}[X]$. Ceci étant vrai quelque soit d divisant strictement n, on en déduit

$$\Phi_n \mid \sum_{d||n} \lambda_d \frac{X^n-1}{X^d-1} \text{ dans } \mathbb{Z}[X]$$

Comme de plus, $\Phi_n \mid X^n - 1$ dans $\mathbb{Z}[X]$, on conclut que

$$\Phi_n \mid X^n - 1 - \sum_{d||n} \lambda_d \frac{X^n-1}{X^d-1} \text{ dans } \mathbb{Z}[X]$$

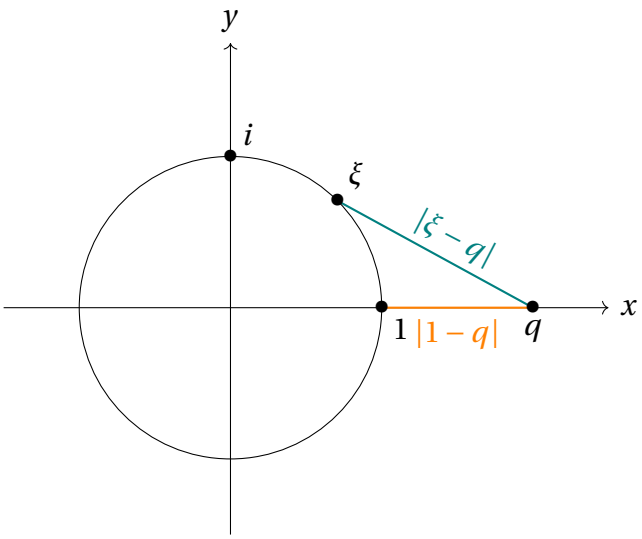
ce qui donne, une fois évalué en q :

$$\Phi_n(q) \mid q^n - 1 - \sum_{d||n} \lambda_d \frac{q^n-1}{q^d-1} \overset{(***)}{=} q - 1 \implies |\Phi_n(q)| \leq q - 1$$

Mais $n \geq 2$, donc

$$\begin{aligned} |\Phi_n(q)| &= \prod_{\xi \in \mu_n^*} |q - \xi| \\ &> \prod_{i=1}^{\varphi(n)} |q - 1| \\ &\geq |q - 1| \end{aligned}$$

On peut en effet interpréter $|q - \xi|$ comme la distance du complexe q au complexe ξ ; le premier est sur l'axe réel et est supérieur ou égal à 2, le second est sur le cercle unité mais n'est pas sur l'axe réel :



cela nous permet de justifier l'inégalité stricte. On a donc une contradiction.

□

Bibliographie

Les maths en tête **[GOU21]**

Xavier GOURDON. *Les maths en tête. Algèbre et probabilités*. 3e éd. Ellipses, 13 juill. 2021. https://www.editions-ellipses.fr/accueil/13722-25266-les-maths-en-tete-algebre-et-probabilites-3e-edition-9782340056763.html.