

Groupe multiplicatif d'un corps fini

Salim Rostam

Soit p un nombre premier. On veut montrer que $(\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}$. Plus généralement, on va montrer le résultat suivant.

Théorème 1. *Soit k un corps (commutatif). Tout sous-groupe fini de k^\times est cyclique.*

Le théorème nous permettra bien de conclure puisque $\mathbb{Z}/p\mathbb{Z}$ est un corps. On va donner deux démonstrations : la deuxième sera plus longue mais sera l'occasion de montrer quelques résultats sur $\mathbb{Z}/n\mathbb{Z}$.

Soit k un corps (commutatif). On rappelle le résultat suivant, qui nous servira pour les deux démonstrations.

Proposition 2. *Un polynôme de degré n sur k possède au plus n racines.*

Démonstration. Si $a \in k$ est une racine de $P \in k[X]$ alors par division euclidienne on peut écrire $P = (X - a)Q$ avec $\deg Q = \deg P - 1$. On recommence, et on s'arrête au plus tard quand le degré du quotient devient nul. \square

Remarque 3. Cette proposition n'est plus valable si k n'est pas commutatif ! Par exemple, le polynôme $X^2 + 1$ possède une infinité de racines dans le corps (non commutatif, donc) des quaternions.

1 Première preuve

On rappelle tout d'abord les résultats suivants.

Lemme 4. *Soit G un groupe et soit $g \in G$ un élément d'ordre fini n . Alors pour tout $a \in \mathbb{N}^*$, l'élément g^a est d'ordre $\frac{n}{\text{pgcd}(n,a)}$. En particulier, si n et a sont premiers entre eux alors g^a est d'ordre n .*

Démonstration. Tout d'abord, remarquons que l'ordre de g^a divise n puisque $(g^a)^n = g^{an} = (g^n)^a = 1^a = 1$. L'ordre de g^a est donné par le plus petit $\omega \in \{1, \dots, n\}$ tel que $(g^a)^\omega = 1$. On a $g^{a\omega} = 1$ donc $n \mid a\omega$, donc il existe $k \in \mathbb{N}^*$ tel que $a\omega = kn$. Écrivons $n = \text{pgcd}(n,a)n'$ et $a = \text{pgcd}(n,a)a'$, avec donc n' et a' premiers entre eux. On obtient $a'\omega = kn'$, donc n' divise ω . Le plus petit ω possible est donc $n' = \frac{n}{\text{pgcd}(n,a)}$. \square

Lemme 5. *Soit G un groupe et soit g (resp. h) un élément d'ordre fini a (resp. b) de G . Si g et h commutent et si a et b sont premiers entre eux, alors gh est d'ordre ab .*

Démonstration. Puisque g et h commutent on a $(gh)^{ab} = (g^a)^b(h^b)^a = 1$ donc l'ordre de gh divise ab . Mais si $(gh)^k = 1$ alors $g^k = h^{-k}$ est un élément dont l'ordre divise a et b donc divise $\text{pgcd}(a,b) = 1$, donc $g^k = h^{-k} = 1$ donc a et b divisent k donc ab divise k (puisque a et b sont premiers entre eux). \square

Remarque 6. Les deux hypothèses sont essentielles !

- Si les éléments ne commutent pas c'est la catastrophe car gh peut devenir d'ordre infini. Par exemple, on peut considérer le groupe $\langle a, b : a^2 = b^2 = 1 \rangle$, ou bien, pour ceux qui n'aiment pas les groupes définis par générateurs et relations, on peut considérer le sous-groupe des isométries de \mathbb{R}^2 engendré par les symétries orthogonales d'axe $x = 0$ et $x = 1$. Si on veut rester dans un groupe fini, on peut par exemple considérer les deux matrices $g := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $h := \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ d'ordre 2 de $\text{GL}_2(\mathbb{Z}/2\mathbb{Z})$, dont le produit $gh = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ est d'ordre 3.
- Si les éléments commutent mais que les ordres ne sont pas premiers entre eux, on peut par exemple prendre $h := g^k$. Par le Lemme 4, l'élément h est d'ordre $\frac{a}{\text{pgcd}(a,k)}$ et $gh = g^{k+1}$ est d'ordre $\frac{a}{\text{pgcd}(a,k+1)}$, qui n'a aucune raison d'être égal à $a \frac{a}{\text{pgcd}(a,k)}$ (si vous n'êtes pas convaincus, prenez $h = g^{-1}$!).

(Je ne trouve plus la référence bibliographique pour la suite de la preuve, si vous en avez une n'hésitez pas à me l'indiquer.) Soit H un sous-groupe fini non trivial de k^\times . Notons $n := |H|$ et écrivons $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ la décomposition de n en produit de facteurs premiers. Par le Lemme 5, il suffit de montrer que H possède un élément d'ordre $p_i^{\alpha_i}$ pour chaque i .

S'il existe $x \in H$ d'ordre $p_i^{\alpha_i} q$ avec $q := \prod_{j \neq i} p_j^{\beta_j}$ et $0 \leq \beta_j \leq \alpha_j$, alors par le Lemme 4 l'élément x^q est d'ordre $p_i^{\alpha_i}$ et c'est gagné. On va montrer que l'on est nécessairement dans ce cas. Si chaque $x \in H$ est d'ordre $p_i^{\beta_i} q$ où $q := \prod_{j \neq i} p_j^{\beta_j}$ avec $\beta_i < \alpha_i$ et $0 \leq \beta_j \leq \alpha_j$ si $j \neq i$, alors x est d'ordre divisant $p_i^{\alpha_i - 1} q = \frac{n}{p_i}$. Ainsi, les éléments de H sont des racines de $X^{\frac{n}{p_i}} - 1$, mais alors par la Proposition 2 on aurait $|H| \leq \frac{n}{p_i}$ ce qui est absurde.

2 Deuxième preuve

Cette preuve est plus longue mais sera l'occasion d'énoncer quelques résultats complémentaires.

2.1 Indicatrice d'Euler

Définition 7. Si $n \in \mathbb{N}^*$, on note $\varphi(n)$ le nombre d'éléments de $\{1, \dots, n\}$ premiers avec n . La fonction $\varphi : \mathbb{N}^* \rightarrow \mathbb{N}^*$ est appelée *indicatrice d'Euler*.

Énonçons quelques propriétés élémentaires de la fonction φ .

Propriété 8. Si p est premier alors $\varphi(p) = p - 1$.

Démonstration. En effet, chaque élément de $\{1, \dots, p - 1\}$ est premier à p . □

Propriété 9. Si $n \in \mathbb{N}^*$ on a $|(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n)$.

Démonstration. Vient du fait que $k \in \{1, \dots, n\}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si k est premier à n . □

Proposition 10. Soit $n \in \mathbb{N}^*$. On a $n = \sum_{d|n} \varphi(d)$.

Démonstration. (Voir [Gou, Proposition 6 page 32].) On écrit les fractions $\frac{1}{n}, \frac{2}{n}, \dots, \frac{n}{n}$ sous forme irréductible. On obtient chaque $\frac{k}{d}$, où $d | n$ et $k \in \{1, \dots, d\}$ est premier à d . Ainsi, pour chaque $d | n$ il y a exactement $\varphi(d)$ fractions avec d au dénominateur. Au départ on avait n fractions, on conclut donc que $n = \sum_{d|n} \varphi(d)$. □

On peut également déduire cette proposition du lemme suivant.

Lemme 11. Soit $n \in \mathbb{N}^*$ et soit $d \mid n$. Le nombre d'éléments d'ordre d dans $\mathbb{Z}/n\mathbb{Z}$ est $\varphi(d)$.

Démonstration. Soit $a \in \{1, \dots, n\}$ d'ordre divisant d dans $\mathbb{Z}/n\mathbb{Z}$. On a $n \mid da$, autrement dit, il existe $k \in \mathbb{N}$ tel que $da = kn$ et donc $a = k\frac{n}{d}$ (on a bien $\frac{n}{d} \in \mathbb{N}^*$). Puisque $a \in \{1, \dots, n\}$, l'entier k est dans $\{1, \dots, d\}$. Cela montre qu'il y a exactement d éléments d'ordre divisant d dans $\mathbb{Z}/n\mathbb{Z}$, ces éléments étant $\frac{n}{d}, 2\frac{n}{d}, \dots, d\frac{n}{d}$. Mais $\frac{n}{d}$ est d'ordre d dans $\mathbb{Z}/n\mathbb{Z}$, donc par le Lemme 4 (pris en notation additive) les seuls éléments d'ordre d sont ceux de la forme $k\frac{n}{d}$ avec $k \in \{1, \dots, n\}$ premier à d . Par définition de φ , il y en a exactement $\varphi(d)$. \square

On retrouve bien la proposition précédente en écrivant $\mathbb{Z}/n\mathbb{Z} = \sqcup_{d \mid n} \{\text{éléments d'ordre } d\}$ et en passant au cardinaux.

2.2 Sous-groupe fini du groupe multiplicatif d'un corps

(Cf. [Per, Théorème 2.7 page 74].) Soit H un sous-groupe fini de k^\times . On note n l'ordre de H . Soit $x \in H$ et notons $d \mid n$ son ordre. Remarquons que $\langle x \rangle \simeq \mathbb{Z}/d\mathbb{Z}$ et que chaque élément de $\langle x \rangle$ est d'ordre divisant d , donc $y^d = 1$ pour tout $y \in \langle x \rangle$. Ainsi, $\langle x \rangle$ est inclus dans l'ensemble des racines de $X^d - 1 \in k[X]$, et on a en fait égalité par la Proposition 2. De plus, puisque chaque élément $z \in H$ d'ordre divisant d est racine de $X^d - 1$, on en déduit que tous les éléments de H d'ordre divisant d sont dans $\langle x \rangle$.

On a donc montré que $\langle x \rangle$ est exactement l'ensemble des éléments d'ordre divisant d de H . Les éléments d'ordre exactement d de H sont donc les éléments exactement d'ordre d de $\langle x \rangle \simeq \mathbb{Z}/d\mathbb{Z}$, qui sont au nombre de $\varphi(d)$ par le Lemme 11.

Finalement, si N_d désigne le nombre d'éléments d'ordre d dans H , on a soit $N_d = 0$ (s'il n'y a pas d'élément d'ordre d dans H) soit $N_d = \varphi(d)$. Puisque $\sum_{d \mid n} N_d = |H| = n$, par la Proposition 10 on en déduit que $N_d = \varphi(d)$ pour tout $d \mid n$. En particulier, il y a $\varphi(n) \geq 1$ éléments d'ordre n dans H donc H est cyclique.

Références

- [Per] D. PERRIN, *Cours d'algèbre*. CAPES / Agrégation, Ellipses.
- [Gou] X. GOURDON, *Algèbre* (2^e édition). Les maths en tête, Ellipses.