Ordre d'un élément dans un groupe fini

1 Ordre d'un élément et exposant d'un groupe fini

Les deux résultats qui suivent ont été démontrés en TD, on les **admet**.

— Les sous-groupes de $\mathbb{Z}$ sont exactement les ensembles $n\mathbb{Z}$, n décrivant $\mathbb{N}$, et pour $n \geqslant 1$: $\quad n = \min\left(n\mathbb{Z} \cap \mathbb{N}^*\right)$.

— Le cardinal de tout sous-groupe d'un groupe fini G divise le cardinal de G (*théorème de Lagrange*).

1) Soient G un groupe fini et $x \in G$. On pose $\langle x \rangle = \left\{x^k \mid \quad k \in \mathbb{Z}\right\}$.

a) Montrer que $\langle x \rangle$ est un sous-groupe de G, appelé le *sous-groupe de G engendré par x*.

b) Montrer que $K = \left\{k \in \mathbb{Z} \mid \quad x^k = 1_G\right\}$ est un sous-groupe de $\mathbb{Z}$ non réduit à $\left\{0\right\}$.

Il existe donc un et un seul entier naturel non nul $|x|$ pour lequel $K = |x|\mathbb{Z}$. De façon équivalente, $|x|$ est le plus petit entier $k \in \mathbb{N}^*$ pour lequel $x^k = 1_G$.

c) Montrer que l'application $k \overset{\lambda}{\longmapsto} x^k$ est bijective de $[\![0, |x|-1]\!]$ sur $\langle x \rangle$ et que $x^{|G|} = 1_G$.

En particulier, $|x|$ est le cardinal du sous-groupe $\langle x \rangle$, donc divise $|G|$ d'après le théorème de Lagrange.

d) Montrer que l'application $g \overset{\varphi}{\longmapsto} e^{\frac{2i\lambda^{-1}(g)\pi}{|x|}}$ est un isomorphisme de groupes de $\langle x \rangle$ sur $\mathbb{U}_{|x|}$.

2) Déterminer l'ordre des éléments des groupes $\mathbb{U}_4$, $\mathbb{U}_6$, $\mathbb{U}_2^2$ et S_3.

3) **a)** Soit G un groupe fini de cardinal n. Montrer que si G contient un élément d'ordre n, il est isomorphe à $\mathbb{U}_n$.

b) Soit G un groupe fini de cardinal premier p. Montrer que G est isomorphe à $\mathbb{U}_p$.

4) Soient G un groupe fini et $x, y \in G$. On suppose que x et y commutent et que $|x|$ et $|y|$ sont premiers entre eux.

a) Montrer que $|x|$ divise $|y| \times |xy|$.

b) En déduire que $|xy| = |x| \times |y|$.

5) Soient G un groupe fini, $x \in G$ et d un diviseur positif de $|x|$. Montrer que $\left|x^d\right| = \dfrac{|x|}{d}$.

Pour tout groupe fini G, on appelle à présent *exposant de G* le PPCM des ordres des éléments de G.

6) Soit G un groupe fini d'exposant n. Montrer que n divise $|G|$ et que pour tout $x \in G$: $\quad x^n = 1_G$.

7) Calculer l'exposant du groupe $\mathbb{U}_n$ pour tout $n \in \mathbb{N}^*$ et celui des groupes $\mathbb{U}_2^2$ et S_3. Un groupe fini d'exposant n contient-il toujours un élément d'ordre n ?

8) Soit G un groupe commutatif fini d'exposant n.

a) Montrer que G contient un élément d'ordre divisible par $p^{v_p(n)}$ pour tout $p \in \mathbb{P}$.

b) En déduire que G contient un élément d'ordre $p^{v_p(n)}$ pour tout $p \in \mathbb{P}$.

c) En déduire que G contient un élément d'ordre n.

2 Structure des groupes commutatifs finis

Cette partie est facultative.

9) Soit G un groupe commutatif fini. On se donne un sous-groupe strict H de G, i.e. distinct de G, un élément $x \in G \setminus H$ et un morphisme de groupes de H dans $\mathbb{U}$.

a) On pose $\langle x, H\rangle = \left\{x^k h \mid \quad k \in \mathbb{Z}, \quad h \in H\right\}$. Montrer que $\langle x, H\rangle$ est un sous-groupe de G contenant x et H.

On **admet** pour gagner du temps que l'ensemble $\left\{k \in \mathbb{Z} \mid \quad x^k \in H\right\}$ est un sous-groupe de $\mathbb{Z}$. Cet ensemble est donc de la forme $d\mathbb{Z}$ pour un certain $d \in \mathbb{N}$.

b) Montrer que d divise $|x|$, puis justifier l'existence d'un élément $u \in \mathbb{U}$ pour lequel $\varphi\left(x^d\right) = u^d$.

c) Montrer que pour tous $k, k' \in \mathbb{Z}$ et $h, h' \in H$: $\quad x^k h = x^{k'} h' \quad \Longrightarrow \quad u^k \varphi(h) = u^{k'} \varphi(h')$. Expliquer pourquoi cette vérification autorise à poser pour tous $k \in \mathbb{Z}$ et $h \in H$: $\quad \widetilde{\varphi}\left(x^k h\right) = u^k \varphi(h)$.

d) Montrer que $\widetilde{\varphi}$ est un morphisme de groupes de $\langle x, H\rangle$ dans $\mathbb{U}$.

10) Soient G un groupe commutatif fini et H un sous-groupe de G. Montrer que tout morphisme de groupes de H dans $\mathbb{U}$ peut être prolongé en un morphisme de groupes de G dans $\mathbb{U}$. On pourra raisonner par récurrence sur l'entier $\left|G : H\right| = \dfrac{|G|}{|H|}$, appelé l'*indice de H dans G*.

11) Soient G un groupe commutatif et A et B deux sous-groupes de G. On suppose que $A \cap B = \left\{1_G\right\}$ et que tout élément de G est le produit d'un élément de a et d'un élément de b. Montrer que G est isomorphe à $A \times B$.

12) Soit G un groupe commutatif fini d'exposant n.

a) Exhiber un sous-groupe H de G et un morphisme de groupes χ de G dans $\mathbb{U}_n$ pour lesquels $\chi|_H$ est un isomorphisme de groupes de H sur $\mathbb{U}_n$.

b) Montrer que G est isomorphe à $H \times \operatorname{Ker} \chi$.

13) Soit G un groupe commutatif fini de cardinal supérieur ou égal à 2. Montrer l'existence d'une famille $(n_1, \ldots, n_r)$ d'entiers supérieurs ou égaux à 2 pour lesquels :

— G est isomorphe à $\mathbb{U}_{n_1} \times \ldots \times \mathbb{U}_{n_r}$,

— n_{i+1} divise n_i pour tout $i \in [\![1, r-1]\!]$.

On peut montrer que la famille $(n_1, \ldots, n_r)$ ainsi associée à G est unique. Tout groupe commutatif fini est donc isomorphe à un et un seul des groupes $\mathbb{U}_{n_1} \times \ldots \mathbb{U}_{n_r}$ avec $n_r \mid n_{r-1} \mid \ldots \mid n_1$.