1.5 Ordre d'un élément

Définition 1.32 (Ordre d'un élément)**.** *Soit $(G, \times)$ un groupe, de neutre e, et $x \in G$. L'ordre de x est*

- *$ord(x) = +\infty$ si pour tout $n \in \mathbb{N}^*, x^n \neq e$;*
- *$ord(x) = \min\{n \in \mathbb{N}^* | x^n = e\}$ sinon.*

On dit que x admet un ordre fini si $ord(x) \neq +\infty$.

Exemple 1.33. *1. Dans $(\mathbb{Z}, +)$, $ord(1) = +\infty$*

2. Dans $(\mathbb{Z}/n\mathbb{Z}, +)$, $ord(\overline{1}) = n$

3. Dans $(\mathbb{Z}/42\mathbb{Z}, +)$, $ord(\overline{12}) = 7$.

Proposition 1.34 (Résolution de $x^k = e$)**.** *Soit $(G, \times)$ un groupe de neutre e. Soit x un élément d'ordre fini n. Alors*

$$x^k = e \iff n \mid k.$$

Proposition 1.35 (Description de ord(x) par le groupe engendré)**.** *Soit $(G, \times)$ un groupe, et $x \in G$. Alors*

$$ord(x) = |\langle x \rangle|.$$

Éléments de preuve. Dans le cas où ord(x) est fini, égal à n, le théorème 7.1.29 donne $\langle x \rangle \simeq \mathbb{Z}/n\mathbb{Z}$. Passer au cardinal. □

Définition 1.36 (Ordre d'un groupe)**.** *L'ordre d'un groupe est son cardinal. C'est un élément de $\mathbb{N}^* \cup \{+\infty\}$.*

Corollaire 1.37. *Si G est un groupe fini, tout $x \in G$ admet un ordre fini.*

Éléments de preuve. Sinon, $\mathbb{Z} \simeq \langle x \rangle \subset G$. □

Exercise 1.38. *Soit G un groupe abélien fini et x et y deux éléments de G d'ordres respectifs a et b. On suppose que a et b sont premiers entre eux. Montrer que xy est d'ordre ab.*

Théorème 1.39 (Lagrange)**.** *Soit G un groupe fini, et $x \in G$. Alors $ord(x) \mid Card(G)$. Ainsi l'ordre d'un élément d'un groupe fini divise l'ordre de ce groupe.*

Éléments de preuve. La démonstration n'est exigible que dans le cas où G est abélien. Montrer que l'application $\varphi : g \mapsto xg$ est une bijection et en déduire que

$$\prod_{g \in G} g = \prod_{g \in G} (xg),$$

puis simplifier. □

1.6 Un deuxième théorème de Lagrange, HP

Lemme 1.40 (Partition par les classes à gauche modulo H)**.** *Soit G un groupe fini et H un sous-groupe de G. Alors $\{aH, a \in G\}$ est une partition de G.*

Éléments de preuve. C'est la partition associée à la relation d'équivalence définie sur G par

$$x \equiv y[H] \iff x^{-1}y \in H.$$

Cette relation est appelée relation de congruence à gauche modulo H. □

Remarque 1.41. *Lorsque $G = \mathbb{Z}$ et $H = n\mathbb{Z}$ (et en revenant aux notations additives), la congruence modulo H correspond à la congruence modulo n bien connue.*

Lemme 1.42 (Cardinal des classes à gauche modulo H)**.** *Pour tout $a \in G$, $|aH| = |H|$.*

Éléments de preuve. L'application $h \mapsto ah$ est une bijection de H dans aH. □

Théorème 1.43 (Lagrange pour les sous-groupes)**.** *Soit G un groupe fini et H un sous-groupe de G. Alors l'ordre de H divise l'ordre de G.*

Éléments de preuve. On a partitionné G avec des parts qui ont toutes le même cardinal que H. □

Remarque 1.44 (Groupes quotients)**.**

1. *On aurait pu faire la même chose avec les classes à droite Ha.*
2. *Quand G n'est pas abélien, la partition des classes à gauche n'est en général par la même que la partition des classes à droite.*
3. *Cela peut néanmoins arriver. Cela se produit lorsque pour tout $a \in G$, $aH = Ha$, c'est-à-dire $aHa^{-1} = H$. On dit dans ce cas que H est un sous-groupe normal de G (terminologie anglaise) ou un sous-groupe distingué de G (terminologie française).*
4. *Dans ce cas, on peut montrer que la loi de G passe sur les classes, dans le sens où la classe (à droite ou gauche) de xy ne dépend pas du choix de x et y dans leur classe respective. Cela permet de définir une loi sur l'ensemble des classes modulo H, qui en fait un groupe. C'est ce qu'on appelle le groupe quotient G/H.*
5. *Cette situation se produit systématiquement lorsque G est abélien, puisque dans ce cas, les classes à gauche et à droite sont clairement confondues. Ainsi, on peut toujours définir le groupe quotient G/H dans cette situation.*
6. *Un cas particulier est le cas du sous-groupe $n\mathbb{Z}$ de $\mathbb{Z}$: en formant le groupe quotient, on retrouve le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ déjà étudié.*

Exercise 1.45. *Soit G un groupe non réduit à son élément neutre. Montrer que G n'admet aucun sous-groupe propre (i.e. distinct de $\{e\}$ et de G) si et seulement si G est cyclique d'ordre p premier.*