Groupes

1 Compléments sur les groupes

Proposition 1.1 Intersection de sous-groupes

Soit $(H_i)_{i\in I}$ une famille de sous-groupes d'un groupe G. Alors $\bigcap_{i\in I} H_i$ est un sous-groupe de G.

Définition 1.1 Sous-groupe engendré par une partie

Soient G un groupe et $A \subset G$. On appelle **sous-groupe engendré** par A l'intersection de tous les sous-groupes de G contenant A i.e. le plus petit sous-groupe de G contenant A.

Remarque. Si le sous-groupe engendré par A est G, on dit également que A est un **partie génératrice** de A.

Exemple 1.1

- Le sous-groupe engendré par la partie vide est le sous-groupe trivial contenant le seul élément neutre.
- L'ensemble des transpositions de S_n engendrent S_n.

Exercice 1.1

Montrer que le groupe orthogonal O(E) d'un espace euclidien E est engendré par les réflexions.

Proposition 1.2 Sous-groupe engendré par un élément

Soient G un groupe et $x \in G$. Le sous-groupe engendré par $\{x\}$ est appelé plus simplement sous-groupe engendré par x. De plus, ce sous-groupe est $\{x^k, k \in \mathbb{Z}\}$.

Remarque. Si le sous-groupe engendré par x est G, on dit également que x est un **générateur** de G.

Exemple 1.2

- Les générateurs de $(\mathbb{Z}, +)$ sont ± 1.
- Les générateurs de $\mathbb{U}_n$ sont les $e^{\frac{2ik\pi}{n}}$ avec $k \wedge n = 1$.

Proposition 1.3 Sous-groupes de $(\mathbb{Z}, +)$

Les sous-groupes de $(\mathbb{Z}, +)$ sont les $a\mathbb{Z}$ avec $a \in \mathbb{Z}$.

2 Le groupe $\mathbb{Z}/n\mathbb{Z}$

Proposition 2.1

Soit $n \in \mathbb{N}^*$. La relation de congruence modulo n définit une relation d'équivalence sur $\mathbb{Z}$.

Définition 2.1 $\mathbb{Z}/n\mathbb{Z}$

Soit $n \in \mathbb{N}^*$. On appelle $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalences de la relation de congruence modulo n.

Notation 2.1

Pour $k \in \mathbb{Z}$, on notera $\overline{k}^n$ sa classe d'équivalence modulo n ou plus simplement $\overline{k}$ s'il n'y a pas d'ambiguïté sur l'entier n.

Remarque. Par conséquent, $\overline{k}^n = \{k + pn,\ p \in \mathbb{Z}\}$.

Exemple 2.1

Dans $\mathbb{Z}/5\mathbb{Z}$, $\overline{47} = \overline{2} = \overline{-8}$.

Remarque. En considérant le reste de la division euclidienne d'un entier par $n \in \mathbb{N}^*$, on montre qu'un entier est toujous congru modulo n à un entier compris entre 0 et $n-1$. Il s'ensuit que

$$\mathbb{Z}/n\mathbb{Z} = \left\{\overline{k}^n,\ k \in [\![0, n-1]\!]\right\}$$

En particulier, $\operatorname{card}(\mathbb{Z}/n\mathbb{Z}) = n$.

Proposition 2.2 Addition sur $\mathbb{Z}/n\mathbb{Z}$

Soit $n \in \mathbb{N}^*$. On définit une addition sur $\mathbb{Z}/n\mathbb{Z}$ en posant

$$\forall (k,l) \in \mathbb{Z}^2,\ \overline{k}^n + \overline{l}^n = \overline{k+l}^n$$

Remarque. Il faut vérifier que la classe de congruence de $k+l$ modulo n ne dépend que des classes de congruence de k et l modulo n.

Exemple 2.2

Dans $\mathbb{Z}/4\mathbb{Z}$, $\overline{7} + \overline{2} = \overline{9} = \overline{1}$.

Proposition 2.3 Structure de groupe de $\mathbb{Z}/n\mathbb{Z}$

Soit $n \in \mathbb{N}^*$. $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe commutatif d'élément neutre $\overline{0}$.

Théorème 2.1 Générateurs de $\mathbb{Z}/n\mathbb{Z}$

Si $k \in \mathbb{Z}$, alors $\overline{k}$ engendre le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ si et seulement si $k \wedge n = 1$.

3 Ordre d'un élément d'un groupe

Définition 3.1 Ordre d'un élément

Un élément x d'un groupe G d'élément neutre e est dit d'**ordre fini** s'il existe $n \in \mathbb{N}^*$ tel que $x^n = e$.
Dans ce cas, on appelle **ordre** de x l'entier $\min\{n \in \mathbb{N}^*,\ x^n = e\}$.

Exemple 3.1

L'élément neutre d'un groupe est le seul élément d'ordre 1.

Remarque. Le cardinal d'un groupe est aussi appelé l'ordre de ce groupe.

Exemple 3.2

Il est clair que l'ordre d'un élément est conservé par isomorphisme. On en déduit par exemple que $\mathbb{Z}/4\mathbb{Z}$ n'est pas isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$. Ces deux groupes sont commutatifs et de cardinal 4 mais le premier contient un élément d'ordre 4 tandis que le second ne possède que des éléments d'ordre 1 ou 2.

Proposition 3.1

Soit x un élément d'un groupe G. Alors x est d'ordre fini si et seulement si le sous-groupe H engendré par x est fini et, dans ce cas, l'ordre de x est égal au cardinal de H.
Plus précisément, $\mathrm{H} = \left\{x^k,\ k \in [\![0, p-1]\!]\right\}$ où p désigne l'ordre de x.

Remarque. Tout élément d'un groupe fini est donc d'ordre fini.

Proposition 3.2

Soit x un élément d'ordre p d'un groupe G d'élément neutre e. Alors pour tout $n \in \mathbb{Z}$, $x^n = e \iff p|n$.

Exercice 3.1

Soient x un élément d'un groupe G et $k \in \mathbb{Z}$. On suppose que x est d'ordre $n \in \mathbb{N}^*$. Montrer que x^k est d'ordre $\dfrac{n}{n \wedge k}$.

Proposition 3.3

Soit x un élément d'un groupe fini G. Alors x est d'ordre fini et l'ordre de x divise le cardinal de G.

Exemple 3.3

On en déduit par exemple aisément que tout groupe de cardinal premier est cyclique.

Théorème 3.1 Lagrange (hors-programme)

Soit H un sous-groupe d'un groupe fini G. Alors le cardinal de H divise le cardinal de G.

4 Groupes monogènes

Définition 4.1 Groupe monogène

On dit qu'un groupe est **monogène** s'il est engendré par un de ses éléments.

Remarque. Un groupe monogène et fini ou dénombrable.

Exemple 4.1

Le groupe $(\mathbb{Z}, +)$ est monogène puisqu'il est engendré par 1.

Proposition 4.1

Tout groupe monogène est commutatif.

Théorème 4.1

Un groupe infini est monogène si et seulement si il est isomorphe à $(\mathbb{Z}, +)$.

Définition 4.2 Groupe cyclique

On dit qu'un groupe est **cyclique** s'il est monogène et fini.

Remarque. Si G est un groupe cyclique d'ordre n, alors pour tout générateur x de G, alors $\mathrm{G} = \left\{x^k,\ k \in [\![0, p-1]\!]\right\}$.

Exemple 4.2

- Soit $n \in \mathbb{N}^*$. Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ est cyclique puisqu'il est fini et engendré par $\overline{1}$.
- Soit $n \in \mathbb{N}^*$. Le groupe $(\mathbb{U}_n, \times)$ est cyclique puisqu'il est fini et engendré par $e^{\frac{2i\pi}{n}}$.

Théorème 4.2

Un groupe de cardinal $n \in \mathbb{N}^*$ est cyclique si et seulement si il est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$.

Exemple 4.3

A nouveau, $(\mathbb{U}_n, \times)$ est cyclique puisque l'application $\left\{\begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{U}_n \\ \overline{k} & \longmapsto & e^{\frac{2ik\pi}{n}} \end{array}\right.$ est bien définie et est un isomorphisme.