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

Soit A une partie d'un groupe 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. On note ce sous-groupe $\langle A\rangle$.

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

Proposition 1.2

Soit A une partie d'un groupe G. Alors

$$\begin{aligned}\langle A\rangle &= \left\{a_1^{\varepsilon_1}a_2^{\varepsilon_2}\dots a_p^{\varepsilon_p},\ p\in\mathbb{N},\ (a_1,\dots,a_p)\in A^p,\ (\varepsilon_1,\dots,\varepsilon_p)\in\{-1,1\}^p\right\}\\ &= \left\{a_1^{n_1}a_2^{n_2}\dots a_p^{n_p},\ p\in\mathbb{N},\ (a_1,\dots,a_p)\in A^p,\ (n_1,\dots,n_p)\in\mathbb{Z}^p\right\}\end{aligned}$$

Remarque. Dans le cas où $p=0$, on retrouve l'élément neutre.

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.

Exercice 1.2

On note A_n l'ensemble des permutations de S_n de signature 1. Montrer que A_n est un sous-groupe de S_n engendré par les 3-cycles.

Proposition 1.3 Sous-groupe engendré par un élément

Soient G un groupe et $x \in \mathrm{G}$. Le sous-groupe engendré par $\{x\}$ est appelé plus simplement sous-groupe engendré par x. On le note $\langle x \rangle$.

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

Proposition 1.4

Soient G un groupe et $x \in \mathrm{G}$. Alors $\langle x \rangle = \left\{x^k,\ k \in \mathbb{Z}\right\}$.

Exemple 1.2

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

Exercice 1.3 Partie génératrice et morphisme

Soient f un morhisme d'un groupe G dans un groupe H et A une partie de G. Montrer que $\langle f(\mathrm{A}) \rangle = f(\langle \mathrm{A} \rangle)$.

Proposition 1.5 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

On notera $\overline{k}$ la classe de congruence de k modulo n.

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

Exemple 2.1

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

Remarque. De manière générale, $\overline{k} = \overline{m}$ dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $k \equiv m[n]$.

Exercice 2.1

Montrer que l'application $\left\{\begin{array}{rcl} [\![0, n-1]\!] & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ k & \longmapsto & \overline{k} \end{array}\right.$ est bijective.

Proposition 2.2

Soit $n \in \mathbb{N}^*$. Alors $\mathbb{Z}/n\mathbb{Z} = \left\{\overline{k},\ k \in [\![0, n-1]\!]\right\}$. De plus, $\operatorname{card}(\mathbb{Z}/n\mathbb{Z}) = n$.

Proposition 2.3 Addition sur $\mathbb{Z}/n\mathbb{Z}$

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

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

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, et non des entiers k et l choisis.

Exemple 2.2

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

Proposition 2.4 Structure de groupe de $\mathbb{Z}/n\mathbb{Z}$

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

Remarque. L'application $k \in \mathbb{Z} \mapsto \overline{k}$ est un morphisme de groupes de $(\mathbb{Z}, +)$ dans $(\mathbb{Z}/n\mathbb{Z}, +)$.

Proposition 2.5

Soit $(m, k, n) \in \mathbb{Z}^2 \times \mathbb{N}^*$. Alors $m\overline{k} = \overline{mk}$ dans $\mathbb{Z}/n\mathbb{Z}$.

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

Soit $(k, n) \in \mathbb{Z} \times \mathbb{N}^*$. 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.

Exemple 3.2

L'ordre d'un cycle de longueur p est p.

Exercice 3.1

Déterminer l'ordre de la permutation $\sigma \in S_7$ telle que

$$\sigma(1) = 3 \qquad \sigma(2) = 6 \qquad \sigma(3) = 5 \qquad \sigma(4) = 7 \qquad \sigma(5) = 1 \qquad \sigma(6) = 2 \qquad \sigma(7) = 4$$

Exemple 3.3

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.

Définition 3.2 Ordre d'un groupe

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

Exemple 3.4

$(S_n, \circ)$ est un groupe d'ordre $n!$.

Exercice 3.2

Soit x un élément d'ordre d d'un groupe G. Montrer que l'application $\left\{\begin{array}{rcl} [\![0, d-1]\!] & \longrightarrow & \langle x \rangle \\ k & \longmapsto & x^k \end{array}\right.$ est bijective.

Proposition 3.1 Ordre et sous-groupe engendré par un élément

Soit x un élément d'un groupe G. Alors x est d'ordre fini si et seulement si $\langle x \rangle$ est d'ordre fini.
Dans ce cas, les ordres de x et $\langle x \rangle$ sont égaux et $\langle x \rangle = \left\{x^k, \ k \in [\![0, d-1]\!]\right\}$, où d 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 d d'un groupe G d'élément neutre e. Alors pour tout $n \in \mathbb{Z}$, $x^n = e \iff d \mid n$.

Exercice 3.3

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

1. Montrer que n divise kd.
2. Montrer que d divise $\frac{n}{n \wedge k}$.
3. En déduire que $d = \frac{n}{n \wedge k}$.

Exercice 3.4

Soit $(k, n) \in \mathbb{Z} \times \mathbb{N}^*$. On note d l'ordre de $\overline{k}$ dans $\mathbb{Z}/n\mathbb{Z}$.

1. Montrer que n divise kd.
2. Montrer que d divise $\frac{n}{n \wedge k}$.
3. En déduire que $d = \frac{n}{n \wedge k}$.

Proposition 3.3

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

Remarque. Notamment, si x est un élément d'un groupe d'ordre n et d'élément neutre e, alors $x^n = e$.

Théorème 3.1 Lagrange (hors-programme)

Soit H un sous-groupe d'un groupe fini G. Alors l'ordre de H divise l'ordre 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 est 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 est infini 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, $\mathrm{G} = \left\{x^k,\ k \in [\![0, p-1]\!]\right\}$.

Remarque. Un groupe d'ordre n est cyclique si et seulement si il possède un élément d'ordre n.

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 $e^{\frac{2i\pi}{n}}$.
- Pour tout entier $n \geq 3$, S_n n'est pas cyclique puisqu'il n'est même pas commutatif.
- Pour tout entier $n \geq 2$, $(\mathbb{Z}/n\mathbb{Z})^2$ n'est pas cyclique : il est d'ordre n^2 mais les ordres de ses éléments sont des diviseurs de n.

Exercice 4.1

Montrer que tout groupe d'ordre premier est cyclique.

Théorème 4.2

Soit $n \in \mathbb{N}^*$. Un groupe est cyclique d'ordre n 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.

Sous-groupes de $\mathbb{Z}/n\mathbb{Z}$

On peut prouver que les sous-groupes de $(\mathbb{Z}/n\mathbb{Z}, +)$ sont cycliques. En effet, si H est un sous-goupe non nul de $\mathbb{Z}/n\mathbb{Z}$, on peut montrer que $\mathrm{H} = \langle \overline{m} \rangle$ où $m = \min\{k \in [\![1, n-1]\!], \ \overline{k} \in \mathrm{H}\}$.
Comme tout groupe cyclique d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$, on en déduit que les sous-groupes d'un groupe cyclique sont cycliques.

Exercice 4.2

Montrer que si G est un groupe cyclique d'ordre n, alors pour tout diviseur d de n, il existe un unique sous-groupe de G d'ordre d.