Groupes

1 Groupes

Définition 1.1

On appelle **groupe** tout ensemble G muni d'une loi interne $*$ vérifiant les conditions suivantes :

(i) $*$ est associative,

(ii) $(E, *)$ possède un élément neutre,

(iii) tout élément est inversible.

Remarque. Il peut arriver qu'on parle d'un groupe sans préciser sa loi. Le produit de deux éléments x et y de G se notera alors simplement xy. ■

Définition 1.2 Groupe commutatif

Soit $(G, *)$ un groupe. Si la loi $*$ est commutative, on dit que le groupe $(G, *)$ est **commutatif** ou **abélien**.

Exemple 1.1

- Si E est un ensemble, $(\mathfrak{S}(E), \circ)$ est un groupe non commutatif dès que $\operatorname{card} E \geq 3$.
- $(\mathbb{Z}, +)$ est un groupe commutatif.
- $(\mathbb{C}^*, \times)$ est un groupe.
- Si $\mathbb{K}$ est un corps et $n \in \mathbb{N}^*$, $(GL_n(\mathbb{K}), \times)$ est un groupe non commutatif dès que $n \geq 2$.

Théorème 1.1 Propriétés de l'inverse

Soit $(G, *)$ un groupe.

(i) Soit $x \in G$. Alors $\left(x^{-1}\right)^{-1} = x$.

(ii) Soit $(x, y) \in G^2$. Alors $(x * y)^{-1} = y^{-1} * x^{-1}$.

Notation 1.1 Puissance

Soient $(G, *)$ un groupe d'élément neutre e, $x \in G$ et $n \in \mathbb{N}^*$.

- On pose $x^n = \underbrace{x * x * \cdots * x}_{n \text{ fois}}$.
- Par convention, on pose $x^0 = e$.
- On pose $x^{-n} = (x^{-1})^n = (x^n)^{-1}$.

Remarque. Si la loi est noté additivement $+$, on parle plutôt de **multiple** que de puissance et le «multiple $k^{\text{ème}}$» de x s'écrit kx plutôt que x^k. ■

Proposition 1.1 Règles de calcul

Soient $(G, *)$ un groupe d'élément neutre e et $x \in G$. Pour tout $(n, p) \in \mathbb{Z}^2$, $x^n * x^p = x^{n+p}$.

Attention ! En général $(x * y)^n \neq x^n * y^n$, à moins d'avoir commutativité de $*$.

Proposition 1.2 Groupe produit

Soient $(G_1, *_1), \dots, (G_n, *_n)$ des groupes d'éléments neutres $e_1, \dots, e_n$. Alors on peut munir $G = \prod_{i=1}^n G_i$ d'une structure de groupe en définissant une loi $*$ sur G par

$$\forall (x, y) \in G^2,\ x * y = (x_1 *_1 y_1, \dots, x_n *_n y_n)$$

L'élément neutre de G est alors $(e_1, \dots, e_n)$ et pour tout $x \in G$, $x^{-1} = (x_1^{-1}, \dots, x_n^{-1})$.

2 Sous-groupes

Définition 2.1 Sous-groupe

Soient $(G, *)$ un groupe et H un ensemble. On dit que H est un **sous-groupe** de G si :

(i) $H \subset G$

(ii) H contient l'élément neutre,

(iii) H est stable pour la loi $*$ i.e. $\forall (h, h') \in H^2$, $h * h' \in H$,

(iv) H est stable par passage à l'inverse i.e. $\forall h \in H$, $h^{-1} \in H$.

Exemple 2.1

Soit G un groupe d'élément neutre e. Alors G et $\{e\}$ sont des sous-groupes de G.

Remarque. Si H est un sous-groupe d'un groupe $(G, *)$. Alors pour tout $(h, n) \in H \times \mathbb{Z}$, $h^n \in H$. ■

Proposition 2.1

Soient $(G, *)$ un groupe et H un sous-groupe de G. Alors $(H, *)$ est un groupe. De plus,

(i) l'élément neutre de $(H, *)$ est l'élément neutre de $(G, *)$;

(ii) si $h \in H$, l'inverse de h en tant qu'élément du groupe $(H, *)$ est égal à son inverse en tant qu'élément du groupe $(G, *)$.

Remarque. Si on voulait être rigoureux, il faudrait munir H de la restriction de $*$ à H. ■
Remarque. Si K est un sous-groupe de H qui est un sous-groupe de G, alors K est un sous-groupe de G. ■

Théorème 2.1 Caractérisation des sous-groupes

Soient $(G, *)$ un groupe d'élément neutre e et H un ensemble. Alors H est un sous-groupe **si et seulement si**

(i) $H \subset G$;

(ii) H contient l'élément neutre ;

(iii) $\forall (h, k) \in H^2, h * k^{-1} \in H$.

Méthode **Sous-groupes en pratique**

Il est souvent plus facile de montrer qu'un ensemble muni d'une loi interne est un groupe en montrant qu'il est un sous-groupe d'un groupe connu.

Exemple 2.2

- $(\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{C}, +)$.
- $(\mathbb{Q}^*, \times)$ est un sous-groupe de $(\mathbb{C}^*, \times)$.
- Soit $n \in \mathbb{N}^*$. $(\mathbb{U}_n, \times)$ est un sous-groupe de $(\mathbb{U}, \times)$ qui est un sous-groupe de $(\mathbb{C}^*, \times)$.
- Soit E un $\mathbb{K}$-espace vectoriel. $\mathrm{GL}(\mathrm{E})$ est un sous-groupe de $\mathfrak{S}(\mathrm{E})$.

Proposition 2.2 Intersection de sous-groupes

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

Définition 2.2 Sous-groupe engendré par une partie

Soient G un groupe et $\mathrm{A} \subset \mathrm{G}$. On appelle **sous-groupe engendré** par A l'intersection de tous les sous-groupes de G contenant A.

Exemple 2.3

- Le sous-groupe engendré par la partie vide est le sous-groupe trivial contenant le seul élément neutre.
- L'ensemble des transpositions de $\mathfrak{S}_n$ engendrent $\mathfrak{S}_n$.

Proposition 2.3 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. De plus, ce sous-groupe est $\{x^k, k \in \mathbb{Z}\}$.

Proposition 2.4 Sous-groupes de $(\mathbb{Z}, +)$

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

3 Morphismes de groupes

Définition 3.1 Morphisme de groupes

Soient $(\mathrm{G}, *)$ et $(\mathrm{G}', .)$ deux groupes. On appelle **morphisme (de groupes)** de G dans G′ toute application f de G dans G′ telle que :

$$\forall (x, y) \in \mathrm{G}^2, f(x * y) = f(x).f(y)$$

On appelle **endomorphisme (de groupe)** de G tout morphisme de G dans G.

Exemple 3.1

- L'exponentielle est un morphisme de $(\mathbb{R}, +)$ dans $(\mathbb{R}^*, \times)$.
- Le module est un morphisme de $(\mathbb{C}^*, \times)$ dans $(\mathbb{R}^*, \times)$.
- La signature est un morphisme de $(\mathfrak{S}_n, \circ)$ dans $(\{-1, 1\}, \times)$.
- Si $\mathbb{K}$ est un corps, le déterminant est un morphisme de $(\mathrm{GL}_n(\mathbb{K}), \times)$ dans $(\mathbb{K}^*, \times)$.
- Si E est un espace vectoriel de dimension finie, le déterminant est un morphisme de $(\mathrm{GL}(\mathrm{E}), \times)$ dans $(\mathbb{K}^*, \times)$.

Proposition 3.1 Morphisme, élément neutre et inverse

Soit f un morphisme de $(\mathrm{G}, *)$ dans $(\mathrm{G}', .)$. On note e et e' les éléments neutres respectifs de G et G'. Alors

(i) $f(e) = e'$,

(ii) $\forall x \in \mathrm{G}, f(x^{-1}) = f(x)^{-1}$.

(iii) $\forall x \in \mathrm{G}, \forall n \in \mathbb{Z}, f(x^n) = f(x)^n$.

Proposition 3.2 Morphisme et composition

Soient $f : \mathrm{G} \to \mathrm{G}'$ et $g : \mathrm{G}' \to \mathrm{G}''$ deux morphismes de groupes. Alors $g \circ f : \mathrm{G} \to \mathrm{G}''$ est un morphisme de groupes.

Proposition 3.3 Images directe et réciproque d'un sous-groupe par un morphisme de groupes

Soit $f : \mathrm{G} \to \mathrm{G}'$ un morphisme de groupes.

(i) Si H est un sous-groupe de G, alors $f(\mathrm{H})$ est un sous-groupe de G'.

(ii) Si K est un sous-groupe de G', alors $f^{-1}(\mathrm{K})$ est un sous-groupe de G.

Définition 3.2 Noyau et image d'un morphisme

Soit $f : \mathrm{G} \to \mathrm{G}'$ un morphisme de groupes. On note e' l'élément neutre de G'.

(i) On appelle **noyau** de f l'ensemble $\mathrm{Ker} f = f^{-1}(\{e'\}) = \{x \in \mathrm{G} \mid f(x) = e'\}$.

(ii) On appelle **image** de f l'ensemble $\mathrm{Im} f = f(\mathrm{G}) = \{f(x), x \in \mathrm{G}\}$.

Remarque. L'image du morphisme f n'est autre que l'image de l'application f. ■

Théorème 3.1

Soit $f : \mathrm{G} \to \mathrm{G}'$ un morphisme de groupes.

(i) $\mathrm{Ker} f$ est un sous-groupe de G.

(ii) $\mathrm{Im} f$ est un sous-groupe de G'.

Exemple 3.2

- Le module est un morphisme de $(\mathbb{C}, *)$ dans $(\mathbb{R}, *)$. Par définition, son noyau est $\mathbb{U}$ qui est donc un sous-groupe de $(\mathbb{C}, *)$.
- De même, $\{-1, 1\}$ est un sous-groupe de $(\mathbb{R}^*, \times)$ puisque c'est le noyau de l'endomorphisme «valeur absolue» de $(\mathbb{R}^*, \times)$.
- Si E est un espace euclidien, $\mathrm{SO}(\mathrm{E})$ est un sous-groupe de $(\mathrm{O}(\mathrm{E}), \circ)$ car c'est le noyau du déterminant sur $\mathrm{O}(\mathrm{E})$.

Proposition 3.4

Soit $f : \mathrm{G} \to \mathrm{G}'$ un morphisme de groupes. On note e l'élément neutre de G.

(i) f est injectif **si et seulement si** $\mathrm{Ker} f = \{e\}$.

(ii) f est surjectif **si et seulement si** $\mathrm{Im} f = \mathrm{G}'$.

Remarque. En ce qui concerne la première proposition, pour prouver l'injectivité de f, il suffit de montrer que $\mathrm{Ker} f \subset \{e\}$ puisque $\mathrm{Ker} f$, étant un sous-groupe, contient nécessairement e. ■

Méthode **Injectivité en pratique**

Pour prouver l'injectivité d'un morphisme de groupes $f : \mathrm{G} \to \mathrm{G}'$, on commence la démonstration par : «Soit $x \in \mathrm{G}$ tel que $f(x) = e'$» et on montre que $x = e$.

Définition 3.3 Isomorphisme, automorphisme

Soient G et G' deux groupes.
On appelle **isomorphisme** de G sur G' tout morphisme bijectif de G dans G'.
On appelle **automomorphisme** de G tout endomorphisme bijectif de G. On dit que G est **isomorphe** à G' s'il existe un isomorphisme de G sur G'.

Remarque. Dire que deux groupes sont isomorphes veut dire qu'ils ont la même structure. Si on connaît l'un, on connaît l'autre. Toute propriété liée à la structure de groupe qui est vraie dans un groupe est aussi vraie dans un groupe qui lui est isomorphe. ■

Exemple 3.3

- $(\mathbb{C}, +)$ et $(\mathbb{R}^2, +)$ sont isomorphes.
- Notons $\vec{\mathrm{P}}$ et $\vec{\mathrm{E}}$ le plan et l'espace vectoriel. Alors $(\vec{\mathrm{P}}, +)$ et $(\vec{\mathrm{E}}, +)$ sont respectivement isomorphes à $(\mathbb{R}^2, +)$ et $(\mathbb{R}^3, +)$.

Théorème 3.2 Réciproque d'un isomorphisme

Soit f un isomorphisme de groupes de G sur G'. Alors f^{-1} est un isomorphisme de groupes de G' sur G.

Théorème 3.3 Groupe des automorphismes

Soit G un groupe. L'ensemble des automorphismes de G, noté $\mathrm{A}ut(\mathrm{G})$, est un sous-groupe de $(\mathfrak{S}(\mathrm{G}), \circ)$.

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

Proposition 4.1

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

Définition 4.1 $\mathbb{Z}/n\mathbb{Z}$

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 4.1

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 4.1

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 4.2 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 4.2

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

Proposition 4.3 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 4.1 Générateurs de $\mathbb{Z}/n\mathbb{Z}$

Plus précisément, si $k \in \mathbb{Z}$, alors $\overline{k}$ engendre le groupe $\mathbb{Z}/n\mathbb{Z}$ **si et seulement si** $k \wedge n = 1$.

5 Groupes monogènes

Définition 5.1 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 5.1

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

Proposition 5.1

Tout groupe monogène est commutatif.

Théorème 5.1

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

Définition 5.2 Groupe cyclique

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

Exemple 5.2

- 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 5.2

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

Exemple 5.3

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

6 Ordre d'un élément d'un groupe

Définition 6.1 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 $\min\{n \in \mathbb{N}^* \mid x^n = e\}$.

Exemple 6.1

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 6.2

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 6.1

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.

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

Proposition 6.2

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

Exercice 6.1

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 $\frac{n}{n \wedge k}$.

Proposition 6.3

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

Exemple 6.3

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

Théorème 6.1 Lagrange (hors-programme)

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