Rappels généraux de théorie des Groupes

1 Loi de composition interne et groupe

Définition 1.1. Soit E un ensemble non-vide. On appelle *loi de composition interne* (LCI en abrégé) dans E toute application $* : E \times E \to E$. L'image par $*$ du couple (x, y) est noté $x * y$; c'est le produit de x par y pour la loi $*$.

Exemple 1.1. L'addition et la multiplication sont des LCI dans $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, etc...

Définition 1.2. Soit $*$ une LCI dans E. On dit que $*$ est

- *associative* si $x * (y * z) = (x * y) * z$ pour tous $x, y, z \in E$.
- *commutative* si $x * y = y * x$ pour tous $x, y \in E$.

Définition 1.3. Soit $*$ une LCI dans E. On dit qu'un élément $e \in E$ est un *élément neutre* pour $*$ si pour tout $x \in E$, $x * e = e * x = x$.

Définition 1.4. Soit $*$ une LCI dans E. Supposons que $*$ admet un élément neutre e. On dit qu'un élément x de E admet un *symétrique* dans E pour la loi $*$, s'il existe $x' \in G$ tel que $x * x' = x' * x = e$.

Définition 1.5. Un *groupe* $(G, *)$ est un ensemble non-vide G muni d'une loi de composition interne $*$ telles que (axiomes de la structure de groupe) :

i) la loi $*$ est associative dans G,
ii) la loi $*$ admet un élément neutre dans G,
iii) tout élément de G admet un symétrique dans G pour la loi $*$.

Définition 1.6. On appelle groupe commutatif, ou groupe abélien, tout groupe G dont la loi est commutative.

Exemples 1.1.
- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ sont des groupes *additifs*,
- $(\mathbb{Z}^*, \times)$, $(\mathbb{Q}^*, \times)$, $(\mathbb{R}^*, \times)$, $(\mathbb{C}^*, \times)$ sont des groupes *multiplicatifs*.

Exercice 1.
1. Pour chacun des groupes de l'exemple ci-dessus, donner son élément neutre et le symétrique d'un élément quelconque.

Soit $(G, *)$ un groupe.

2. Montrer l'élément neutre e est unique
3. Montrer que pour tout $g \in G$ le symétrique de g est unique.

Exercice 2. Dire parmi les ensembles munis d'une LCI suivants, lesquels sont des groupes : $(\mathbb{R}, \times)$, $(\mathbb{N}, +)$, $(\mathbb{Z}^*, \times)$, $(\mathbb{Q}, \times)$, $(\mathbb{R}_+^*, \times)$, $(\mathbb{R}_-^*, \times)$. Justifier.

Exercice 3. Montrer que pour tout entier $n \geq 1$, l'ensemble $GL_n(\mathbb{R})$ des matrices carrées d'ordre n inversibles à coefficients réels muni de la loi de multiplication des matrices $A * B = AB$ est un groupe. Déterminer son élément neutre et le symétrique d'une matrice A. Est-ce un groupe abélien ?

Exercice 4. Les ensembles suivants, pour les lois considérées, sont-ils des groupes ?

1. L'intrevalle $]-1,1[$ muni de la loi définie par $x \star y = \frac{x+y}{1+xy}$;
2. L'ensemble $\{z \in \mathbb{C} : |z| = 2\}$ pour la multiplication usuelle
3. $\{x \in \mathbb{R} \mapsto ax + b \,|\, a \in \mathbb{R} \setminus \{0\}, b \in \mathbb{R}\}$ pour la loi de composition des applications.

Exercice 5. Soit X un ensemble. On note $\mathfrak{S}(X)$ l'ensemble des bijections de X sur X. On munit $\mathfrak{S}(X)$ de la loi $\circ$, loi de decomposition des bijections.

1. Vérifier que $(\mathfrak{S}(X), \circ)$ est un groupe, déterminer son élément neutre et donner le symétrique d'un élément $f \in S(X)$.
2. Le groupe $(\mathfrak{S}(X), \circ)$ est-il un groupe abélien ?

Notations. *Soit $(G, *)$ un groupe de neutre e.*

— *Pour $g \in G$, on notera* ***souvent*** $g^n = \overbrace{g * \cdots * g}^{(n \text{ fois})}$ *avec la convention $g^0 = e$.*

— *Le symétrique d'un élément g sera* ***souvent*** *noté g^{-1}.*

Attention *toutefois, dans le cas des* groupes additifs $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, *le symétrique d'un élément est son opposé et pas son inverse et le produit de deux éléments est en fait leur* ***somme*** *(et oui !...).*

Définition 1.7. Avec les notations de l'exercice précécent, le groupe $\mathfrak{S}(\llbracket 1, \dots n \rrbracket), \circ)$, groupe des bijections de l'ensemble $\llbracket 1, \dots, n \rrbracket$ (ensemble des entiers de 1 à n) est noté $\mathfrak{S}_n$. On l'appelle *groupe symétrique d'indice n*.

Un élément de $\mathfrak{S}_n$ est appellé une *permutation*.

Rappelons que le *cardinal* d'un ensemble fini est le nombre d'éléments de cet ensemble. Si E est un ensemble fini, on note $|E|$ le cardinal de E.

Définition 1.8. Un groupe $(G, *)$ est un *groupe fini* si G est un ensemble fini. Le cardinal $|G|$ de G est alors appelé *ordre de G*.

Dans le cas d'ensembles finis, les lois de composition interne peuvent être notées sous forme de tableaux : si $E := \{a, b, c\}$ et si $*$ est une LCI sur E, l'élément $a * b$ est l'unique élément situé sur la ligne issue de a et la colonne issue de b :

$*$	a	b	c
a	a	a	a
b	a	b	b
c	a	b	c

Exercice 6. Pour chacun des LCI suivantes, dites s'il s'agit d'une loi de groupe :

$a)$

$*$	a	b	c
a	a	a	a
b	a	b	b
c	a	b	c

$b)$

$*$	a	b	c
a	b	c	a
b	c	a	b
c	a	b	c

$c)$

$*$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	d	c	b	a
d	c	d	a	b

S'il s'agit de loi de groupe, les groupes sont-ils abéliens ?

Exercice 7 (Le groupe $\mathfrak{S}_n$)**.** Il est d'usage de décrire un élément σ du group symétrique $\mathfrak{S}_n$ de la manière suivante : $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma 1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$.

1. Soient $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 4 & 6 & 5 & 8 & 1 & 7 & 3 \end{pmatrix}$ et $\sigma' = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 5 & 1 & 2 & 7 & 8 & 6 \end{pmatrix} \in S_8$. Calculer $\sigma \circ \sigma'$ et $\sigma' \circ \sigma$.
2. Écrire tous les éléments de $\mathfrak{S}_2$ et de $\mathfrak{S}_3$. Établir les tables de composition de ces deux ensembles.
3. Quel est l'ordre de $\mathfrak{S}_n$? Combien de cases contient son tableau de composition ?

Exercice 8. Montrer qu'il existe une seule table possible pour un groupe d'ordre 3. Est-ce vrai pour 4 ?

2 Sous-groupes

Définition 2.1. Soit $(G, *)$ un groupe. Un sous-ensemble non vide H de G est un *sous-groupe de G* lorsque les deux conditions suivantes sont vérifiées :

1. H est stable pour la loi : (ce qui signifie que $x.y \in H$ pour tous $x, y \in H$),
2. H est stable par passage au symétrique (ce qui signifie $x^{-1} \in H$ pour tout $x \in H$).

La définition est justifiée par l'exercice suivant.

Exercice 9. Soit $(G, *)$ un groupe et soit H une partie non vide de G. Montrer que H est un sous-groupe si et seulement si $(H, *)$ est un groupe.

Exemples 2.1.
1. $(\mathbb{Z}, +)$ et $(\mathbb{Q}, +)$ sont des sous-groupes de $(\mathbb{R}, +)$
2. $(\mathbb{R}_+^*, \times)$ et $(\mathbb{Q}^*, \times)$ sont des sous groupes de $(\mathbb{R}^*, \times)$.
3. $\mathbb{U} := \{z \in \mathbb{C} \,|\, |z| = 1\}$ est un sous-groupe de $\mathbb{C}^*$.

Exercice 10. Soit $K = \{\mathrm{Id}, \sigma_1, \sigma_2, \sigma_3\}$ où σ_1, σ_2 et σ_3 sont les permutations de $E = \{1, 2, 3, 4\}$ définies par

$$\sigma_1 = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{smallmatrix}\right), \sigma_2 = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{smallmatrix}\right), \sigma_3 = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{smallmatrix}\right).$$

Montrer que K est un sous-groupe de $\mathfrak{S}_4$.

Proposition 2.1. *Soit $(G, *)$ un groupe. L'ensemble $Z(G)$ des éléments $\gamma \in G$ tels que pour tout $g \in G$, $g * \gamma = \gamma * g$ est un sous-groupe de G. On l'appelle le* centralisateur *de G, et on le note $Z(G)$.*

Exercice 11. 1. Montrer que l'intersection de deux sous-groupes d'un groupe G est un sous-groupe de G.

2. Montrer que $3\mathbb{Z} \cup 8\mathbb{Z}$ n'est pas un sous-groupe de $\mathbb{Z}$.
3. Soit G un groupe et soient H et K deux sous-groupes de G. Montrer que $H \cup K$ est un sous-groupe de G si et seulement si $H \subset K$ ou $K \subset H$.

Exercice 12. 1. Montrer que les sous-groupes de $(\mathbb{Z}, +)$ sont les $n\mathbb{Z} = \{nz \,|\, z \in \mathbb{Z}\}$ lorsque n parcourt $\mathbb{N}$.

2. Montrer que si a et b sont deux entiers relatifs, l'ensemble $a\mathbb{Z}+b\mathbb{Z} = \{ax+by \,|\, x, y \in \mathbb{Z}\}$ est un sous-groupe de $\mathbb{Z}$.

   En déduire qu'il existe $d \in \mathbb{N}$ tel que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ et que d est le pgcd de a et de b.
3. Montrer que deux entiers relatifs a et b sont premiers entre eux si et seulement s'il existe $(u, v) \in \mathbb{Z}^2$ tel que :
$$ua + vb = 1.$$
   C'est ce qu'on appelle la *relation de Bezout*.

3 Morphisme de groupes

Définition 3.1. Soient $(G, *)$ et $(G', \star)$ deux groupes. Un morphisme (de groupes) de G dans G' est une application $f : G \to G'$ telle que pour tous x, y dans G $f(x*y) = f(x)\star f(y)$.

Proposition 3.1. *Soit $(G, *)$ et $(G', \star)$ deux groupes de neutres respectifs e et e'. Soit $f : G \to G'$ un morphisme de groupes. Alors*

1. *$f(e) = e'$.*
2. *$f(x^{-1}) = f(x)^{-1}$, pour tout $x \in G$*
3. *$f(x^n) = f(x)^n$, pour tout $x \in G$ et tout $n \in \mathbb{Z}$.*

Proposition 3.2. *Soient G et G' deux groupes et soit $f : G \to G'$ un morphisme de groupes. Alors*

1. *Pour tout sous-groupe H de G, $f(H) = \{f(x) \,|\, x \in H\}$ est un sous-groupe de G' ;*
2. *Pour tout sous-groupe H' de G', $f^{-1}(H')$ est un sous-groupe de G.*

Définition 3.2. Soit $(G, *)$ et $(G', \star)$ deux groupes de neutres respectifs e et e'. Soit $f : G \to G'$ un morphisme de groupes.

1. Le sous-groupe de G', $f(G)$ est appelé l'image de f, et est noté $\operatorname{Im} f$,
2. Le sous-groupe de G $f^{-1}(\{e'\})$ est appelé le noyau de f, et est noté $\ker f$.

Remarque 3.1. Soit $(G, *)$ et $(G', \star)$ deux groupes de neutres respectifs e et e'. Soit $f : G \to G'$ un morphisme de groupes.

1. L'application f est surjective si et seulement si $\operatorname{Im} f = G'$;
2. L'application f est injective si et seulement si $\ker f = \{e\}$.

Exercice 13. Décrire tous les homomorphismes de groupes de $\mathbb{Z}$ dans $\mathbb{Z}$. Déterminer ceux qui sont injectifs et ceux qui sont surjectifs.

Définition 3.3. oit $(G, *)$ et $(G', \star)$. On appelle *isomorphisme* (de groupes) de G sur G' tout morphisme de groupes $f : G \to G'$ qui est de plus une bijection de G sur G'.

Un isomorphisme de G dans lui-même est un *automorphisme*.

Exemples 3.1. Soit $(G, *)$ un groupe.

1. L'application $x \mapsto x^{-1}$ est un automorphisme de réciproque elle-même.
2. Pour $a \in G$, l'application $x \mapsto ax$ est un automorphisme de réciproque $x \mapsto a^{-1}x$.

Proposition 3.3. *Si f est un isomorphisme de groupes de G sur G', alors la bijection réciproque f^{-1} est un isomorphisme de groupes de G' sur G.*

Définition 3.4. Soient G et G' deux groupes. On dit que G et G' sont isomorphes lorsqu'il existe un isomorphisme de groupes de G sur G'. On note $G \simeq G'$.

Exemple 3.1. Les groupes $(\mathbb{R}, +)$ et $(\mathbb{R}_+^*, \times)$ sont isomorphes, un isomorphisme étant donné par l'application $x \to e^x$.

Exercice 14.
1. Soit $(G,*)$ un groupe d'élément neutre e. Montrer l'équivalence de :
   (i) G est abélien.
   (ii) Pour tout $a, b \in G$, on a : $(ab)^2 = a^2b^2$.
   (iii) Pour tout $a, b \in G$, on a : $(ab)^{-1} = a^{-1}b^{-1}$.
2. En déduire que si, pour tout $x \in G$, $x^2 = e$, alors G est abélien.
3. Donner un exemple de groupe G tel que pour tout $x \in G$, $x^2 = e$.

4 Ordre d'un élément, groupe monogène, groupe cyclique

Proposition 4.1. *Soit G un groupe et X un sous-ensemble non-vide de G. L'intersection de tous les sous-groupes de G contenant X est un sous-groupe de G ; c'est le plus petit sous-groupe de G qui contient X (pour la relation d'inclusion), on le note $\langle X \rangle$.*

Remarque 4.1. Tout élément de $\langle X \rangle$ est le produit d'un nombre fini d'éléments de X.

Remarque 4.2. Si $x \in G$, $\langle x \rangle := \{x^n \mid n \in \mathbb{Z}\}$.

Exercice 15. Déterminer le sous-groupe de $\mathbb{Z}$ engendré par les entiers 24, 36 et -54.

Exercice 16. Soit j le nombre complexe $e^{\frac{2i\pi}{3}}$.
1. Déterminer le sous-goupe du groupe additif $\mathbb{C}$ engendré par i et j.
2. Déterminer le sous-goupe du groupe multiplicatif $\mathbb{C}^*$ engendré par i et j.

Définition 4.1. Un groupe G est dit *monogène* lorsqu'il est engendré par un de ses éléments, c'est-à-dire s'il existe $x \in G$ tel que $G = \langle x \rangle = \{x^m, x \in \mathbb{Z}\}$.

Si de plus G est fini, on dit que G est *cyclique*.

Exemples 4.1. $\mathbb{Z}$ est monogène engendré par 1, $\mathbb{Z}/n\mathbb{Z}$ est cyclique engendré par $\bar{1}$.

Définition 4.2. Soit G un groupe et x un élément de G. On appelle *ordre de* x le cardinal de $\langle x \rangle$; on le note $o(x)$. Si $o(x)$ est infini, on dit que x est d'ordre infini.

Remarques 4.1.
1. Si G est un groupe fini et $x \in G$, alors $o(x) \leq |G|$.
2. Dans tout groupe G, l'élément neutre est le seul élément d'ordre 1.
3. Dans $(\mathbb{Z}, +)$, tous les éléments non nuls sont d'ordre infini.

Proposition 4.2. *1. Si $x \in G$ est d'ordre fini m, pour tout $n \in \mathbb{N}^*$, $x^m = e \iff m|n$.*
2. Si x est d'ordre fini n, le groupe $\langle x \rangle$ engendré par x est $\{e, x, x^2, ..., x^{n-1}\}$.

Proposition 4.3. *Soit G un groupe et x un élément d'ordre fini de G. Alors, $o(x)$ est le plus petit entier strictement positif m tel que $x^m = e$.*

Preuve. Soit $x \in G$. Soit m le plus petit entier strictement positif tel que $x^m = e$. Soit $k \in \mathbb{N}^*$, on peut écrire de façon unique $k = mq + r$ avec $q \in \mathbb{N}$ et r un entier tel que $0 \leq r < m$. Alors $x^k = x^r$, donc $\langle x \rangle = \{e, x, x^2, ..., x^{m-1}\}$ et $o(x) \leq m$.

Reste à vérifier que tous les éléments $e, x, x^2, ..., x^{m-1}$ sont distincts deux à deux. Supposons que $x^i = x^j$ pour deux entiers $1 \leq i \leq j < m$. Alors, $x^{j-i} = e$ avec $0 \leq j - i < n$, ce qui par minimalité de m implique que $i = j$. Donc, $o(x) = m$. □

Exercice 17. Pour tout $n \in \mathbb{N}^*$, notons $\mathbb{U}_n$ l'ensemble des racines n-ièmes de l'unité dans $\mathbb{C}$,

$$\mathbb{U}_n = \{z \in \mathbb{C};\ z^n = 1\} = \{e^{\frac{2ik\pi}{n}},\ 0 \leq l \leq n-1\}$$

1. Montrer que pour tout $n \in \mathbb{N}^*$, $\mathbb{U}_n$ est un sous-groupe de $(\mathbb{C}^*, \times)$.
2. Soit $n \in \mathbb{N}^*$. Montrer que $\mathbb{U}_n$ est un groupe cyclique.
3. Soient $n, d \in \mathbb{N}^*$, montrer que $\mathbb{U}_d \subset \mathbb{U}_n$ si et seulement si $d|n$.
4. Soit H un sous-groupe fini de $(\mathbb{C}^*, \times)$. Notons n son cardinal. Montrer que $H \subset \mathbb{U}_n$. En déduire que $H = \mathbb{U}_n$.
5. Soient $n, m \in \mathbb{N}^*$ et $q = ppcm(n, m)$. Montrer que $\langle e^{\frac{2ik\pi}{n}}, e^{\frac{2ik\pi}{m}} \rangle = \mathbb{U}_q$

Exercice 18. On se place dans le groupe $(\mathbb{C}^*, \times)$. Soit $z_1 = e^{\frac{2i\pi}{3}}$, $z_2 = e^{\frac{2i\pi}{5}}$, $z_3 = e^{\frac{i\pi}{15}}$.
1. Vérifier que z_1, z_2 et z_3 sont d'ordre fini et donner leurs ordres.
2. Montrer que z_1 et z_2 appartiennent au sous-groupe $\langle z_3 \rangle$.
3. Exprimer le produit $z = z_1 z_2$ comme une puissance de z_3.
4. Quel est l'ordre de z ? Le nombre z_3 appartient-il au sous-groupe engendré par z ?

Exercice 19. Soit $n \in \mathbb{N}^*$ et $G = (\mathbb{Z}/n\mathbb{Z}, +)$. Soit $k \in \mathbb{Z}$ et $d = pgcd(k, n)$. On note $\bar{k}$ (resp. $\bar{d}$) la classe de k (resp. d) modulo n.
1. Montrer que l'ordre de $\bar{k}$ dans G est égal à $\frac{n}{d}$.
2. Montrer que $\bar{k}$ et $\bar{d}$ engendrent le même sous-groupe de G.

Proposition 4.4. *Soit $n \in \mathbb{N}^*$. Les générateurs de $(\mathbb{Z}/n\mathbb{Z}, +)$ sont les classes $\bar{k}$ des entiers $k \in [\![0, n]\!]$ qui sont premiers à n.*

Proposition 4.5. *Soit $n \in \mathbb{N}^*$. Les sous-groupes de $G = (\mathbb{Z}/n\mathbb{Z}, +)$ sont les sous-groupes cycliques engendré par les classes modulo n des diviseurs de n dans $\mathbb{N}$.*

Preuve. Soit $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} : k \mapsto \bar{k}$: c'est un morphisme de groupe qui est surjectif. Soit H un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$. Alors $\pi^{-1}(H)$ est un sous-groupe de $\mathbb{Z}$, donc il existe d tel que $H = d\mathbb{Z}$. Or $n\mathbb{Z} = \ker \pi := \pi^{-1}(\bar{0}) \subset \pi^{-1}(H)$, donc d divise n.
Ainsi $H = \pi(d\mathbb{Z}) = \{\pi(dk) \,|\, k \in \mathbb{Z}\} = \langle \bar{d} \rangle$ avec d diviseur de n. □

Exercice 20. Soit le groupe $G = (\mathbb{Z}/12\mathbb{Z}, +)$.

1. Déterminer le sous-groupe H de G engendré par $\overline{6}$ et $\overline{8}$ et déterminer son ordre.
2. Déterminer les générateurs de G.
3. Quel est l'ordre de l'élément $\overline{9}$?

Exercice 21. Soit $G = \langle x \rangle$ un groupe cyclique d'ordre $n \geq 2$. Montrer que les générateurs de G sont les éléments x^k tels que les entiers k et n soient premiers entre eux.

Exercice 22. Le groupe $(\mathbb{Q}, +)$ est-il monogène ?

Proposition 4.6. *1. Tout groupe monogène infini est isomorphe au groupe $(\mathbb{Z}, +)$.*

Preuve. Comme G est monogène, il existe $x \in G$ tel que $G = \langle x \rangle$. L'application : $f : \mathbb{Z} \to G : m \mapsto x^m$ est alors un morphisme surjectif de $\mathbb{Z}$ dans G Si $m \in \ker f$, alors $x^m = e$. Or G est infini, x est d'ordre infini donc $m = 0$. Ainsi $\ker f = \{0\}$, et f est injectif : c'est un isomorphisme de groupes. □

Exercice 23. Montrer qu'il existe un unique groupe cyclique d'ordre n à isomorphisme près.

Remarque 4.3. En particulier, $(\mathbb{Z}/n\mathbb{Z}, +) \simeq (\mathbb{U}_n, .)$.