Théorie des groupes

Table des matières

1. Introduction.

1.1. Groupes.

Définition 1.1 (Groupe)**.** Un *groupe* est un couple constitué d'un ensemble non vide G et d'une opération $* : GxG \to G$ qui vérifie les propriétés :
(1) d'associativité : $\forall a, b, c \in G, (a * b) * c = a * (b * c)$.
(2) d'existence d'un élément neutre: $\exists e \in G, \forall x \in G, x * e = e * x = x$.
(3) d'existence d'un inverse : $\forall x \in G, \exists y \in G, x * y = y * x = e$. On note y=x^(-1)

Exemple 1.2.
1. $(\mathbb{Z}, +)$ est un groupe. $+ : \mathbb{Z}^2 \to \mathbb{Z}$; $(a, b) \mapsto a + b$ est associatif, l'élément neutre est 0, l'inverse d'un $n \in \mathbb{Z}$, est $n^{-1} \coloneqq -n$.
2. $(\mathbb{R}, +), (\mathbb{Q}, +), (\mathbb{C}, +)$...
3. $(\mathbb{R}, \cdot)$ n'est pas un groupe car 0 n'admet pas d'inverse.
4. $(\mathbb{N}, +)$ n'est pas un groupe car il n'y a pas d'inverse.
5. $(\mathrm{GL}_n, \cdot), \mathrm{GL}_n(\mathbb{R}) = \{A \in M_{nxn}(\mathbb{R}) \mid \det A \neq 0\}$ est un groupe : le + est associatif (exo), l'élément neutre est la matrice identité de taille n, et l'inverse de A est A^{-1} et on a bien $AA^{-1} = A^{-1}A$

Définition 1.3 (Commuter)**.** Soit $(G, *)$ un groupe, $a, b \in G$,. On dit que a et b *commutent* si $a * b = b * a$,

Définition 1.4 (Abélien)**.** Soit $(G, *)$ un groupe. On dit que $(G, *)$ est *abélien* ou *commutatif* si tout élément de $(G, *)$ commute.

Définition 1.5 (Monoïde)**.** On appelle *monoïde* un ensemble non vide G avec une opération $* : GxG \to G$ qui satisfait seulement l'associativité et l'existence d'un élément neutre. (sans inverse).

Remarque 1.6. $\{\text{monoÏdes}\} \subset \{\text{groupes}\} \subset \{\text{groupes abéliens}\}$

Notation 1.7.
(1) On utilise $*$ ou $\cdot$ pour l'opération d'un groupe et $+$ pour un groupe abélien.
(2) On utilise $e, e_G, 1, 1_G$ pour l'élément neutre d'un groupe, et 0 lorsqu'il est abélien.
(3) $x^{-1} \coloneqq -x$ dans un groupe abélien.
(4) $a * b * c = (a * b * c) = a * (b * c) = abc$
(5) On définit la puissance d'un groupe $(G, *)$ par, $\forall x \in G, n \in \mathbb{Z}, x^n = \begin{cases} e \text{ si } n=0 \\ x*\ldots*x \text{ si n>0} \\ x^{-1}*\ldots*x^{-1} \text{ si } n<0 \end{cases}$.

Exemples 1.8. Soit X un ensemble non-vide,
1. $(S_X = \{f : X \to X \mid f \text{ bijective}\}, \circ)$ forme un groupe non abélien de symétrie X.
2. $Y \subset X$ $(S_Y \coloneqq \{f : X \to X \text{ bijective} \mid f(y) = y\}, \circ)$ forme un groupe.

Exemple 1.9. Pour $X = \{1, \ldots, n\}_{n \in \mathbb{N} \setminus \{0\}}$. On note $S_X = S_n \coloneqq \{f : X \to X \text{ bijectives}\}$ le groupe de permutations de n éléments $e = \mathrm{id}_f$, f^{-1} = la réciproque de f. On note $\sigma \coloneqq \begin{pmatrix} 1 & \ldots & n \\ \sigma(1) & \ldots & \sigma(n) \end{pmatrix}$ Quelques exemples on a $S_2 \coloneqq \left\{\mathrm{id}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}\right\}, S_3 \coloneqq \left\{\mathrm{id}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}\right\}$. S_2 est abélien tandis que S_3 ne l'est pas car : $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$.

Remarque 1.10. On montrera que $(G, *)$ tel que Card $G \leq 5$ est abélien.

Exemple 1.11. $(\mathbb{Z}/_{n\mathbb{Z}}) \coloneqq \left\{(\overline{x} = \overline{y}) \coloneqq n \mid (x - y)\right\} = \left\{\overline{0}, \ldots, \overline{n-1}\right\}$ est un groupe abélien fini à n éléments. On a $\overline{a} + \overline{b} = \overline{a + b}$. Le + est associatif dans $\mathbb{Z}/_{n\mathbb{Z}}$ car il l'est dans $\mathbb{Z}$. L'élement neutre est le $\overline{0}$. l'inverse de $\overline{x}$ est $\overline{x}^{-1} \coloneqq \overline{n - x} = \overline{-x}$.

Définition 1.12 (Ordre)**.** Soit $(G, *)$ un groupe. On appelle *ordre* de G son cardinal et on peut écrire sa table de multiplication pour $*$. $G = \{e, g_1, \ldots, g_n\}$.

$*$	e	g_1	$\ldots$	g_n
e	$e * e$	$e * g_1$	$\ldots$	$e * g_n$
g_1	$g_1 * e$	$g_1 * g_1$	$\ldots$	$g_1 * g_n$
g_i		$g_i * g_j$		

Proposition 1.13. Soit $(G, *)$ un groupe. Alors
(1) L'élément neutre est unique.
(2) Pour tout $x \in G$, l'inverse de x est unique.
(3) En particulier, $\left(x^{-1}\right)^{-1} = x$.

Démonstration.
(1) Supposons que $e, e' \in G$ sont des éléments neutres de G alors $\forall x \in G, e * x = x * e = x = e' * x = x * e'$. On prend $x = e'$. On a $e' = e * e' = e$ car e et e' sont éléments neutre donc $e' = e$.
(2) Soit $x \in G$, $y, y' \in G$ deux inverses de x dans G.

$$(1) \coloneqq x * y = y * x = e, (2) \coloneqq x * y' = y' * x = e$$

. On a $y' = y' * e = y' * (x * y) \underset{\text{assoc}}{=} (y' * x) * y = e * y = y$.
(3) Comme x^{-1} est l'inverse de x, $x^{-1} * x = x * x^{-1} = e$ donc x est l'inverse de x^-1 par (2).

□

Définition 1.14 (Groupe produit)**.** Soit $(G, *)$, $(H, \cdot)$ deux groupes. Le *groupe produit* $(GxH, \star)$ est définit par: $\star : (GxH)x(GxH) \to (GxH)\,;\ (g_1{,}h_1{,}g_2{,}h_2) \mapsto (g_1{,}h_1) \star (g_2{,}h_2) \coloneqq (g_1 * g_2{,}h_1 \cdot h_2)$.

Proposition 1.15. Soit $(G, *)$, $(H, \cdot)$ deux groupes. Le *groupe produit* $(GxH, \star)$ est un groupe.

Démonstration.
(1) L'associativité s'ensuit de l'associativité de $*$ et $\cdot$.
(2) L'élement neutre est (e_G, e_H): $(g, h) \star (e_G, e_H) = (g * e_G, h \cdot e_H) = (g, h) = (e_G, e_H) \star (g, h)$.
(3) L'inverse de $(g, h) \in GxH$ est $\left(g^{-1}, h^{-1}\right)$.

□

1.2. Sous-groupes.

Définition 1.16 (Sous-groupe)**.** Soit $(G, *)$ un groupe. On appelle *sous-groupe* de $(G, *)$, un sous-ensemble non vide $H \subseteq G$ tel que :
(1) $e_G \in H$,
(2) $\forall x, y \in H, xy \in H$,
(3) $\forall x \in H, x^{-1} \in H$.

Notation 1.17. On pourra noter pour un sous-groupe de G, $H < G$

Exemple 1.18.
1. $\mathbb{Z} < (\mathbb{R}, +)$, $\mathbb{Q} < (\mathbb{R}, +)$, $(\mathbb{R}, +) < (\mathbb{C}, +)$.
2. $\mathbb{N} \nless (\mathbb{Z}, +)$ car $-1 \notin \mathbb{N}$.
3. Soit $H = 2\mathbb{Z} = \{2n \mid n \in \mathbb{Z}\} < \mathbb{Z}$:
   a. $0 \in 2\mathbb{Z}$.
   b. $a = 2m, b = 2n \in H \Rightarrow a + b = 2(n + m) \in H$

c. $a = 2m \in H \Rightarrow -a = 2(-m) \in H$.

Proposition 1.19. Soit $(G, *)$ un groupe et $H \subseteq G$. Alors H est un sous-groupe de G si et seulement si $e \in H$, et $\forall x, y \in H, x * y^{-1} \in H$.

Démonstration.
$\Rightarrow$ Supposons que H soit un sous groupe. Alors il verifie $e \in H$. Montrons que $x * y^{-1} \in H$ est satisfait.
Soit $(x, y) \in H$, alors $y^{-1} \in H \Rightarrow x * y^{-1} \in H$.
$\Leftarrow$ Montrons que $(H, *)$ est un sous-groupe. On a $e \in H$ Soit $x \in H, a = e, b = x$. Alors

$$a * b^{-1} = e * x^{-1} = x^{-1} \in H$$

Soit $x, y \in H, a = x, b = y^{-1}$ $a * b^{-1} = x * \left(y^{-1}\right)^{-1} = x * y \in H$. $\square$

Proposition 1.20. Soit $(G, *)$ un groupe, $H \subseteq G$. Alors $H < G$ si et seulement si $(B) := \forall x, y \in H, x * y \in H$ et $(E) := (H, *)$ forme un groupe.

Démonstration.
$\Rightarrow$ Supposons $H < G$, alors (B). Montrons que $(H, *)$ forme un groupe.
(1) $*$ est associatif.
(2) $H < G \Rightarrow e \in H$ et $\forall x \in H, x * e = e * x = x$.
(3) Soit $x \in H, H < G$ alors $x^{-1} \in H$ et $x * x^{-1} = e$.

$\Leftarrow$ On suppose (B) et (E). Montrons que $H < G$ donc (A) et (C).
A MONTRER (A) $(H, *)$ est un groupe, notons e_H son élément neutre, $(G, *)$ est un groupe, notons e_G son élément neutre.
$\forall x \in H \subseteq G$, e_G élément neutre de G donc $x * e_G = e_G * x = x$

Preuve de (c) Soit $x \in H$, soit g l'inverse de x dans G , y' l'inverse de x dans H alors $x * y' = y' * x = e$ or l'inverse est unique donc $y = y' \in H$. $\square$

Proposition 1.21. Soit $(G, *)$ un groupe et $H_1, H_2 \subseteq G$. On a $H_1 \cap H_2 < G$.
Plus généralement, si $(G_i)_{i \in I}$est une famille de sous-groupes de G, alors $\bigcap_{i \in I} H_i < G$.

Démonstration. $\forall i \in I, e \in G_i$, $e \in \bigcap H_i$ donc on a (A). De plus, $\forall x, y \in \bigcap_{i \in I}$, $x, y \in H_i \Rightarrow xy^{-1} \in H_i \forall i \in I \Rightarrow xy^{-1} \in \bigcap_{i \in I} H_i$. $\square$

Définition 1.22. Soit $(G, *)$ un groupe, $S \subset G$. On appelle sous-groupe engendré par S, noté $\langle S \rangle$ le plus petit sous-groupe de G contenant S.

Remarque 1.23. equivalent a si $H < G$ et $S \subset H$ alors $\langle S \rangle \subseteq H$

Proposition 1.24. $\langle S \rangle$ est bien définit et on a :

$$\langle S \rangle := \bigcap_{(H<G), S \subset H} H = \{g_1, \ldots, g_n \mid g_i \in S \text{ ou } S^{-1} \in S\}$$

Démonstration.
(1) bien définit : Soit $I = \{H < G \mid S \subset H\} \neq \{\}$ car $G \in I$ Soit $H_I = \cap_{H \in I} H < G$ par la prop précédente. Montrons que H_I est le plus petit ssgpe contenant
   (a) $S \subset H, \forall H \in I, S \subset H_I$

(b) Soit $H < G$ tel que $S \subset H \overset{?}{\Rightarrow} H_I < H$ Or $H \in I$ donc $I_I = H \bigcap \left(\bigcap_{H \in I} H'\right) \subset H$ donc $< S >= H_I$.

(2) Montrons que $\langle S \rangle = H_S$ par double inclusion.

(a) $H_S \subset < S >$

$H_S < G$ car $e = gg^{-1} \in H_S$ pour un $g \in S$ Si $x = (g_1)$ A FAIRE

□

Définition 1.25 (Engendré)**.** Soit $(G, *)$ un groupe. Si $G = \langle S \rangle$, on dit que G est engendré par S ou que S est un système de générateurs pour G.

Notation 1.26. Si $S = \{g_1, ..., g_n\}$, on note $\langle g_1, ..., g_n \rangle := \langle S \rangle$.

Définition 1.27 (Monogène)**.** Soit $(G, *)$ un groupe. Si il existe $x \in G$ tel que $G = \langle x \rangle$, on dit que G est *monogène*, si de plus G est fini, on dit qu'il est cyclique.

Définition 1.28 (Finiment engendré)**.** On dit que G est finiment engendré si $\exists S \subset G$ fini tel que $G = \langle S \rangle$.

Exemple 1.29.
1. $G = \langle G \rangle$
2. $(\mathbb{Z}, +) = \langle 1 \rangle = \langle 2, 3 \rangle$ est monogène
3. $\left(\mathbb{Z}^2, +\right) = <(1{,}0), (0{,}1)>: 1 = 3 - 2 \in \langle 2, 3 \rangle \Rightarrow \langle 1 \rangle \subseteq \langle 2, 3 \rangle$
4. $(\mathbb{Z}/_{3\mathbb{Z}} x \mathbb{Z}/_{5\mathbb{Z}}, +) = \left\langle \left(\overline{1}, \overline{1}\right) \right\rangle$. (exo)
5. $(\mathbb{Z}/_n\mathbb{Z}, +) = \left\langle \overline{1} \right\rangle$ est cyclique.
6. $(S_n, \circ)$ n'est pas cyclique pour n>2

Lemme 1.30. Tout groupe monogène est abélien.

Démonstration. G monogène $\Rightarrow \exists x \in G = \langle x \rangle = \{g_1, ..., g_n\}$ □

1.3. Les sous-groupes de $(\mathbb{Z}, +)$.

Remarque 1.31 (★)**.** Soit $n \in \mathbb{Z}$, $\langle n \rangle = \{an + b(-n) \,|a, b \in \mathbb{N}\} < (\mathbb{Z}, +)$

Proposition 1.32.
(1) $< n >= n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\} \forall n \in \mathbb{Z}$.
(2) Tout sous-groupe de $\mathbb{Z}$ est de la forme $\langle n \rangle$ pour un certain $n \in \mathbb{Z}$.
(3) Si $a \neq 0, b \neq 0, a, b \in \mathbb{Z}$. On a $a \,|b$ si et seulement si $b\mathbb{Z} \subset a\mathbb{Z}$.
(4) Soit $a, b \in \mathbb{Z} \setminus \{0\}$, $\langle a, b \rangle = d\mathbb{Z}, d =$ pgcd de a et de b. et $\langle a \rangle \cap \langle b \rangle = m\mathbb{Z}$, $m =$ le ppcm de a et de b.

Démonstration.
(1) $< n \geq n\mathbb{Z}$ provient de (★) car $\{a - b \mid a, b \in \mathbb{N}\} = \mathbb{Z}$
(2) Soit $H < \mathbb{Z}$ Si $H = \{0\}, H = \langle 0 \rangle$. Sinon $\exists d \in H, d \neq 0$. Comme H est sous-groupe, $-d \in H$ donc H contient un nombre positif (d ou $-d$). Soit $n \in H$, le nombre positif minimal $n > 0$. On veut montrer $H = \langle n \rangle$.
Soit $x \in H$. La division euclidienne donne $x = an + r$, $a \in \mathbb{Z}, r \in \mathbb{N}, 0 \leq r < n$. On a $r = x - an \in H$. Comme $0 \leq r < n$ et n minimal dans H, $r = 0$ donc $x = an \in \langle n \rangle$ donc $H \subseteq \langle n \rangle$ D'où $H = \langle n \rangle$
(3) Soit $a, b \in \mathbb{Z} \setminus \{0\}$ Supposons $a \mid b \Rightarrow \exists m \in \mathbb{Z}$ tel que $b = ma \in \langle a \rangle \Rightarrow \langle b \rangle = b\mathbb{Z} = b\mathbb{Z} \subseteq \langle a \rangle = a\mathbb{Z}$. Réciproquement, si $b \in b\mathbb{Z} \subseteq a\mathbb{Z}$ alors $b \in a\mathbb{Z} \Rightarrow \exists m \in \mathbb{Z}$ tel qeu $b = ma \Leftrightarrow a \,|b$.
(4) Soit $d = \text{PGCD}(a, b) \in \mathbb{N} \Leftrightarrow \begin{cases} d \,|a, d|\, b \\ d'|a \text{ et } d'|b \Rightarrow d'|d \end{cases}$, $m = \text{PPCM}(a, b) \in \mathbb{N} \Leftrightarrow \begin{cases} a|m, b|\, m \\ a|m' \text{ et } b|m' \Rightarrow m|m' \end{cases}$.
Par le (2), on sait qu'il existe $d', m' \in \mathbb{N}$ tel que $\langle a, b \rangle = c\mathbb{Z}$

On montre que c est un PGCD de a et de b. $c \in c\mathbb{Z} = \langle a, b\rangle$. $a \in < a, b \geq c\mathbb{Z} \Rightarrow a\mathbb{Z} \subset c\mathbb{Z} \Rightarrow c|a$. De même avec b, on obtient $c\,|b$ Si $d'|a$ et $d'|b$ alors $a\mathbb{Z} \subset d'\mathbb{Z}$ et $b\mathbb{Z} \subset d'\mathbb{Z} \Rightarrow a, b \in d'\mathbb{Z} \Rightarrow\Rightarrow \langle a, b\rangle \subseteq d'\mathbb{Z}$.
On montre que $l = \langle a\rangle \cap \langle b\rangle$ est un PPCM de a et de b. On a $l \in l\mathbb{Z} \subset \langle a\rangle = a\mathbb{Z} \Rightarrow a|l$. et $l \in l\mathbb{Z} \subset \langle b\rangle = b\mathbb{Z} \Rightarrow b|l$ Si $m' \in \mathbb{Z}$ verfiei $a\,|m'$ et $b|m'$ alors $m'\mathbb{Z} \subset a\mathbb{Z}$ et $m'\mathbb{Z} \subset b\mathbb{Z} \Rightarrow m'\mathbb{Z} \subset a\mathbb{Z} \cap b\mathbb{Z} = l\mathbb{Z} = \langle a, b\rangle\mathbb{Z} \Rightarrow l\,|m'$ Donc l est le ppcm de a et de b et donc $l = m$. □

Théorème 1.33 (Théorème de Bézout)**.** Soit $a, b \in \mathbb{Z} \setminus \{0\}$, $d =$pgcd(a, b). Il existe $u, v \in \mathbb{Z}$ tel que $d = ua + bv$.

Démonstration. $d\mathbb{Z} = \langle a, b\rangle \Rightarrow d \in \langle a, b\rangle = \{ua + vb\,|u, v \in \mathbb{Z}\}$. □

2. Ordre d'un élément.

Remarque 2.1 (Rappel)**.** L'ordre d'un groupe G est son cardinal.

Définition 2.2. Soit $(G, \cdot)$ un groupe, $x \in G$. L'ordre de X est ord $x = \mathrm{Card}(\langle x\rangle)$.

Remarques 2.3.
(1) Si G est fini alors tout élementde G est d'ordre fini.
(2) ord e =1.

Proposition 2.4. Soit $(G, \cdot)$ un groupe, $x \in G$. On a
$$\mathrm{ord}\, x = \inf\{d \in \mathbb{N} \setminus \{0\} \mid x^d = e\}.$$

Proposition 2.5. Soit $(G, \cdot)$ un groupe, $x \in G$, $m \in \mathbb{Z}$ tel que $x^m = e$ alors ord $x\,|m$

Remarque 2.6. Par convention, $\inf \varnothing = +\infty$.

Exemple 2.7.
1. ord $x = 1 \Leftrightarrow x = e$,
2. Dans $\left(\mathbb{Z}_{/4\mathbb{Z}}, +\right)$, ord `overline` $(2) = 2$,
3. Dans $(\mathbb{Z}, +)$, ord $2 = \inf$

Remarque 2.8. Dans un groupe abélien, ord $x = \inf\{k \in \mathbb{N} \setminus \{0\} \mid kx = e\}$

3. Morphismes de groupes.

Définition 3.1. Soit $(G, \cdot)$, $(H, \star)$ deux groupes, $\varphi : G \to H$. On dit que φ est un *morphisme de groupes* si pour tout $a, b \in G$, on a $\varphi(a \cdot b) = \varphi(a) \star \varphi(b)$

Lemme 3.2. Si $\varphi : G \to H$ est un morphisme alors $\begin{cases}\varphi(e_G)=e_H \\ \varphi(x^{-1})=\varphi(x)^{-1}\end{cases} \forall x \in G$