

Chapitre 9 : « Les groupes »

M. Calciano

I. Structure de groupe

1) Définition : loi de composition interne

On appelle **loi de composition interne** d'un ensemble E toute application $*$:

$$E \times E \rightarrow E, \quad (x, y) \mapsto *(x, y).$$

On privilégie la notation : $x * y$.

Une loi de composition interne $*$ de $E \times E \rightarrow E$ est dite :

- **associative** : $\forall (a, b, c) \in E^3, a * (b * c) = (a * b) * c$.
- **commutative** : $\forall (a, b) \in E^2, a * b = b * a$.

Remarque : le couple $(E, *)$ avec $*$ loi de composition interne s'appelle **un magma**.

2) Éléments remarquables

Un élément e de $(E, *)$ est dit **neutre** si

$$\forall a \in E, a * e = e * a = a.$$

Si $(E, *)$ possède un élément neutre et si $*$ est associative, on appelle **symétrique** d'un élément x de E pour $*$, l'élément x' de E tel que

$$x * x' = x' * x = e.$$

Remarques :

- Si e est élément neutre de $(E, *)$ alors il est unique.
- S'il existe, le symétrique d'un élément de $(E, *)$ est unique aussi.

Itération : Pour $(E, *)$ avec $*$ loi de composition interne associative, alors on peut définir $x_1 * x_2 * \dots * x_n$ sans parenthèses, et en particulier $x^{*n} = x * x * \dots * x$ (n fois).

3) Quelques notations

- Pour une loi « quelconque », on privilégie $a * b$, le neutre : e , le symétrique de x est x' ,
 $x * x * \dots * x = x^{*n}$.
- Pour une loi notée « + » (souvent pour des lois commutatives), on note $a + b$, le neutre :
 0 , le symétrique de x est $-x$, et $x + x + \dots + x = nx$.
- Pour une loi notée « \times », on note $a \times b$, le neutre 1 , le symétrique de x est x^{-1} .

4) Groupe

Définition : Soit G un ensemble muni d'une loi de composition interne $*$. On dit que $(G, *)$ est **un groupe** si :

- la loi $*$ est associative,
- la loi $*$ possède un élément neutre (on dit que $*$ est unifère),
- tout élément de G possède un symétrique pour $*$.

Exemples : $(\mathbb{Z}, +)$ est un groupe, (\mathbb{R}^*, \times) est un groupe.

5) Groupe abélien

Si de plus, la loi $*$ est commutative, c'est-à-dire $\forall(a, b) \in G^2, a * b = b * a$, alors G est **dit commutatif ou abélien**.

Remarque : Une loi peut être commutative sans être associative. Par exemple, pour $(a, b) \in \mathbb{R}^2$, si on définit $a * b$ par $a * b = \frac{a + b}{2}$. Alors $(0 * 4) * 8 = 2 * 8 = 5$ et $0 * (4 * 8) = 0 * 6 = 3$ et pourtant $a * b = b * a$!

6) Étude de deux exemples

- Démontrer que $(\mathbb{C}, +)$ est un groupe abélien.
- Est-ce que $(\mathbb{N}, +)$ est un groupe?

La loi $+$ sur \mathbb{C} est clairement une loi associative, avec un élément neutre : 0. Pour tout z de \mathbb{C} , $-z$ est dans \mathbb{C} et $z + (-z) = 0$.

2 est un entier naturel dont le symétrique -2 n'est pas un entier naturel!

II. Sous-groupe

1) Définition

Une partie H d'un groupe $(G, *)$ est un **sous-groupe** de G lorsqu'elle vérifie les propriétés suivantes :

- H n'est pas vide,
- H est stable par $*$, c'est-à-dire : $\forall(x, y) \in H^2, x * y \in H$,
- le symétrique de tout élément de H est un élément de H .

2) Proposition

H est un sous-groupe de $(G, *)$ si et seulement si H contient l'élément neutre e ET $\forall(x, y) \in H^2, x * y^{-1} \in H$.

Remarque : On se contente de fusionner les deux derniers points de l'axiomatique...

3) Proposition

Toute intersection de sous-groupes de $(G, *)$ est un sous-groupe.

Démonstration : Soit H et K deux sous-groupes de $(G, *)$.

D'abord, $e_G \in H \cap K$ donc $H \cap K \neq \emptyset$.

Soit $(h, k) \in (H \cap K)^2$. $h * k \in H$ car H sous-groupe, et $h * k \in K$ car K sous-groupe, donc $h * k \in H \cap K$.

Soit $h \in H \cap K$. Comme $h \in H, h^{-1} \in H$. De même $h^{-1} \in K$, donc $h^{-1} \in H \cap K$.

Finalement $(H \cap K, *)$ est un sous-groupe de $(G, *)$.

4) Étude d'un exemple

Soit $G = \mathbb{R}^* \times \mathbb{R}$, et $*$ la loi de G définie par :

$$(x, y) * (x', y') = (xx', xy' + y).$$

Montrer que $(G, *)$ est un groupe.

En évaluant $(2, 1) * (1, 3)$ et $(1, 3) * (2, 1)$, que peut-on conclure?

On montre que $*$ est une loi, unifiée (de neutre $(1, 0)$), symétrisable, associative.
 $(2, 1) * (1, 3) = (2, 7)$ et $(1, 3) * (2, 1) = (2, 4)$ donc non commutatif.

III. Morphismes de groupe : noyaux, images

1) Définition

Soient $(G, *)$ et (G', Δ) deux groupes. On appelle morphisme de groupes de $(G, *)$ dans (G', Δ) une application f de G dans G' vérifiant :

$$\forall (a, b) \in G^2, f(a * b) = f(a) \Delta f(b).$$

Exemple : Soit $(G, *)$ un groupe et $a \in G$. Soit $\varphi : \mathbb{Z} \rightarrow G, k \mapsto a^k$ est un morphisme du groupe $(\mathbb{Z}, +)$ dans $(G, *)$.

Un **endomorphisme** est un morphisme de $(G, *)$ dans lui-même.

Un **isomorphisme** est un morphisme bijectif.

Un **automorphisme** est un endomorphisme bijectif.

Exemple : La fonction logarithme népérien est un isomorphisme de $(\mathbb{R}^{+*}, \times)$ dans $(\mathbb{R}, +)$.

2) Exercice permettant d'obtenir une propriété importante

<https://youtu.be/02EUi8eE0js>

Soit f un morphisme de $(G, *)$ dans (G', Δ) ,

Montrer que $f(e) = e'$ (e est l'élément neutre de G et e' celui de G').

Montrer que pour tout x de G : $f(x^{-1}) = f(x)^{-1}$.

Démonstration : On a $f(e * e) = f(e)$. De plus $f(e * e) = f(e) \Delta f(e)$, soit $f(e) = f(e) \Delta f(e)$. Or $f(e) \in G'$, donc est symétrisable pour la loi Δ . On compose alors par $f(e)^{-1}$ de chaque côté, et on obtient :

$$f(e)^{-1} \Delta f(e) = f(e)^{-1} \Delta f(e) \Delta f(e),$$

et $e' = f(e)$.

De plus, $\forall x \in G, f(x * x^{-1}) = f(e) = e'$ et $f(x * x^{-1}) = f(x) \Delta f(x^{-1})$ donc $f(x) \Delta f(x^{-1}) = e'$.

Soit : $f(x^{-1}) = f(x)^{-1}$.

3) Proposition

Soit f un morphisme de $(G, *)$ dans (G', Δ) .

a) Si H est un sous-groupe de G alors $f(H)$ est un sous-groupe de G' .

b) Si H' est un sous-groupe de G' , alors $f^{-1}(H') = \{x \in G \mid f(x) \in H'\}$ est un sous-groupe de G .

Démonstration : On a vu que $f(e) \in H$.

Soit $h \in H, f(h) \in f(H)$, et $f(h)^{-1} = f(h^{-1}) \in f(H)$ car $h^{-1} \in H$ (car H est un sous-groupe de G).

Soit $(h, k) \in H^2$. Est-ce que $f(h)f(k) \in f(H)$? $f(h)f(k) = f(h * k) \in f(H)$.

$f^{-1}(H') = \{x \in G \mid f(x) \in H'\}$, donc $e \in f^{-1}(H')$, car $f(e) = e'$.

Soit $h \in f^{-1}(H')$. Est-ce que $h^{-1} \in f^{-1}(H')$? On a $f(h) \in H'$ donc $f(h)^{-1} \in H', f(h^{-1}) \in H'$.

Soit $(h, k) \in (f^{-1}(H'))^2$. Est-ce que $h * k \in f^{-1}(H')$? On a $f(h) \in H'$ et $f(k) \in H'$, donc $f(h) \Delta f(k) \in H', f(h * k) \in H'$.

4) Définitions

Soit f un morphisme de $(G, *)$ dans (G', Δ) . On appelle :

- **noyau de f** , et on note $\ker(f) = \{x \in G \mid f(x) = e'\} = f^{-1}(\{e'\})$,
- **image de f** , et on note $\text{Im}(f) = \{y \in G' \mid \exists x \in G, y = f(x)\} = f(G)$.

Exemple : Justifier que $\exp : \mathbb{C} \rightarrow \mathbb{C}^*$ est un morphisme du groupe $(\mathbb{C}, +)$ vers (\mathbb{C}^*, \times) . En déterminer image et noyau.

Clairement $\exp(z + z') = \exp(z) \exp(z')$.

$\text{Ker}(f) = \{z \in \mathbb{C} \mid f(z) = 1\} = \{z \in \mathbb{C} \mid \exp(z) = 1\} = \{2ik\pi \mid k \in \mathbb{Z}\}$ et $\text{Im}(f) = \mathbb{C}^*$.

5) Propositions

Si f un morphisme de $(G, *)$ dans (G', Δ) alors $\text{Ker}(f)$ est un sous-groupe de G et $\text{Im}(f)$ est un sous-groupe de G' .

Démonstration : Montrons que $\text{Ker}(f)$ est un sous-groupe de G .

$\text{Ker}(f) = \{x \in G \mid f(x) = e_{G'}\}$.

On a : $e \in \text{Ker}(f)$ car $f(e) = e_{G'}$.

Soit $(h, k) \in (\text{Ker } f)^2$, $f(h) = e_{G'}$ et $f(k) = e_{G'}$. $f(h)\Delta f(k) = e_{G'}$ d'où $f(h * k) = e_{G'}$ et $h * k \in \text{Ker } f$.

Soit $h \in \text{Ker } f$, $f(h^{-1}) = f(h)^{-1} = e_{G'}^{-1} = e_{G'}$.

Exercice : Montrer que : $\text{Im}(f)$ est un sous-groupe de G' .

6) Propriété

On a f surjectif si et seulement si $\text{Im } f = G'$.

On a f injectif si et seulement si $\text{Ker } f = \{e\}$.

Démonstration : Montrons que f injectif si et seulement si $\text{Ker } f = \{e\}$.

Si f est injectif, si $f(x) = e_{G'}$. Comme $f(e_G) = e_{G'}$, on a $f(e_G) = f(x)$ et $x = e_G$.

Si $\text{Ker } f = \{e\}$, supposons que $f(x) = f(x')$. Alors $f(x)\Delta f(x')^{-1} = e_{G'}$, et $f(x * x'^{-1}) = e_{G'}$.

D'où $x * x'^{-1} = e_G$ et $x = x'$.

7) Définition

Deux groupes $(G, *)$ et (G', Δ) sont dits **isomorphes** s'il existe un isomorphisme de groupes de $(G, *)$ dans (G', Δ) .

8) Proposition

Si f est un isomorphisme de groupes de $(G, *)$ dans (G', Δ) , alors sa bijection réciproque f^{-1} est un isomorphisme de (G', Δ) dans $(G, *)$.

Démonstration : Clairement f^{-1} est bijective.

Est-ce que : $f^{-1}(h' \Delta k') = f^{-1}(h') * f^{-1}(k')$?

On a $f(f^{-1}(h' \Delta k')) = h' \Delta k'$ et $f(f^{-1}(h') * f^{-1}(k')) = f(f^{-1}(h')) \Delta f(f^{-1}(k')) = h' \Delta k'$.

D'où : $f^{-1}(h' \Delta k') = f^{-1}(h') * f^{-1}(k')$.

9) Exercice « classique »

Soit G un groupe noté multiplicativement. Pour $a \in G$, on note τ_a l'application de G vers G définie par $\tau_a(x) = axa^{-1}$.

- a) Montrer que τ_a est un morphisme du groupe G vers lui-même.
- b) Vérifier $\tau_a \circ \tau_b = \tau_{ab}$ pour tous a et b dans G .

c) Montrer que τ_a est bijective et exprimer son application réciproque.

Démonstration :

a) On a pour $(x, x') \in G^2$,

$$\tau_a(xx') = axx'a^{-1} = (axa^{-1})(ax'a^{-1}) \in G.$$

b) $\tau_a \circ \tau_b(x) = a(bxb^{-1})a^{-1} = abxb^{-1}a^{-1} = abx(ab)^{-1} = \tau_{ab}(x)$.

c) Soit $y \in G$. On cherche x dans G tel que $y = axa^{-1}$. D'où $a^{-1}ya = x$. τ_a est surjective.

Si $\tau_a(x) = \tau_a(x')$ alors $axa^{-1} = ax'a^{-1}$ et $x = x'$ (en composant par a^{-1} à gauche et a à droite). τ_a est injective.

Ainsi τ_a est bijective.

De $y = axa^{-1}$, on tire : $x = a^{-1}ya$, soit : $(\tau_a)^{-1} = \tau_{a^{-1}}$.

IV. Exercices

Exercice n°1

Soit $(G, *)$ un groupe tel que $\forall x \in G, x * x = e$. Montrer que G est commutatif où e désigne le neutre de G .

Exercice n°2

https://youtu.be/_w07Ho_T-XY

Soit $E = [0, 1]$. On définit une loi $*$ sur E par : $x * y = x + y - xy$.

- Montrer que $*$ est une loi de composition interne commutative et associative.
- Montrer que $*$ possède un neutre.
- Quels sont les éléments symétrisables ? (attention...les symétriques sont dans E !)

Exercice n°3

Soit ω un complexe non réel et $H = \{a + b\omega \mid (a, b) \in \mathbb{Z}^2\}$. Montrer que $(H, +)$ est un sous-groupe de $(\mathbb{C}, +)$.

Exercice n°4

Soit a un complexe non nul, et $H = \{a^n \mid n \in \mathbb{Z}\}$. Montrer que (H, \times) est un sous-groupe de (\mathbb{C}^*, \times) .

Exercice n°5

Soit $(G, *)$ un groupe. On appelle centre de G ,

$$C = \{x \in G \mid \forall y \in G, x * y = y * x\}.$$

Montrer que $(C, *)$ est un sous-groupe de $(G, *)$.

Exercice n°6

- Démontrer que $\exp : (\mathbb{C}, +) \rightarrow (\mathbb{C}^*, \times)$ est un morphisme de groupes.
- Déterminer son image et son noyau.

Exercice n°7

Soit (G, \cdot) un groupe, A et B deux sous-groupes de G .

1. Montrer que $A \cap B$ est un sous-groupe de G .
2. Montrer que $A \cup B$ est un sous-groupe de G ssi $A \subset B$ ou $B \subset A$.

Exercice n°8

On souhaite déterminer l'ensemble des morphismes de $(\mathbb{Z}, +)$ dans lui-même, et préciser lesquels sont injectifs, surjectifs.

Soit f un morphisme de $(\mathbb{Z}, +)$ dans lui-même.

- a) Montrer par récurrence que pour tout entier $n \geq 1$, on a $f(n) = nf(1)$.
- b) Montrer que le résultat persiste pour $n \in \mathbb{Z}$ et conclure sur l'ensemble des morphismes.
- c) Montrer que les seuls morphismes surjectifs correspondent à $f(1) = \pm 1$ (penser à $m = f(n)$ et $m + 1 = f(n') \dots$).
- d) Montrer que tous les morphismes sont injectifs hormis l'application nulle.

Exercice n°10**Addition des vitesses en théorie de la relativité**

Soit $c > 0$ (c correspond à la vitesse – ou célérité – de la lumière) et $I =] - c; c[$.

- (a) Montrer

$$\forall (x, y) \in I^2, \quad x * y = \frac{x + y}{1 + \frac{xy}{c^2}} \in I.$$

- (b) Montrer que la loi $*$ munit I d'une structure de groupe abélien.

Cette loi $*$ correspond à l'addition des vitesses portées par un même axe en théorie de la relativité.

Exercice n°11

1. On souhaite montrer que (\mathbb{R}^*, \times) et (\mathbb{C}^*, \times) ne sont pas isomorphes.
 - a) Soit f un isomorphisme de (\mathbb{C}^*, \times) dans (\mathbb{R}^*, \times) . Déterminer $f(1)$.
 - b) Déterminer $f(-1)$.
 - c) Conclure.
2. Soit f un morphisme des groupes $(G, *)$ dans (G', \blacksquare) . Soit H' sous-groupe de G' . Montrer que $f^{-1}(H')$ est un sous-groupe de G .

Exercice n°12

On considère sur \mathbb{R} la loi définie par $x \star y = xy + \sqrt{(1-x^2)(1-y^2)}$.

1. Cette loi est-elle commutative? Justifier.
2. Cette loi admet-elle un élément neutre? Justifier.

Exercice n°13

Soit $n \in \mathbb{N} \setminus \{0\}$. On note $U_n = \{z \in \mathbb{C} \mid z^n = 1\}$.

1. Montrer que (U_n, \times) est un groupe. (\times représente la multiplication usuelle dans \mathbb{C}).
2. On définit l'application suivante : $\varphi : \mathbb{Z} \rightarrow U_n, k \mapsto e^{\frac{2ik\pi}{n}}$. Montrer que φ est un morphisme de groupes de $(\mathbb{Z}, +)$ vers (U_n, \times) .
3. Déterminer le noyau de φ .
4. Est-ce que φ est un isomorphisme de groupes ? Justifier.

Exercice n°14 (oraux INP)

1. Soit E un ensemble. Vérifier que l'ensemble des bijections de E dans E muni de la loi de composition est un groupe (on justifiera chaque point sans le démontrer).
2. Pour tout complexe a non nul et pour tout complexe b , on considère les applications de \mathbb{C} dans \mathbb{C} :

$$f_a : z \mapsto az \quad \text{et} \quad g_b : z \mapsto z + b.$$

- a) Montrer que f_a et g_b sont des bijections.
- b) Montrer que $H = \{f_a \mid a \in \mathbb{C}^*\}$ et $H' = \{g_b \mid b \in \mathbb{C}\}$ sont des sous-groupes du groupe des bijections de \mathbb{C} dans \mathbb{C} .
- c) Déterminer les couples $(a, b) \in \mathbb{C}^* \times \mathbb{C}$ pour lesquels $f_a \circ g_b = g_b \circ f_a$.