Groupes

A.Belcaid

Université Euro Méditerranéenne de Fès

December 1, 2020

Groupe

Un **groupe** $(G, *)$ est un ensemble G muni d'une **opération** $*$(dite **loi de composition**) vérifiant les propriétés suivantes:

Si on plus, l'opération $*$ vérifie:

$$\forall x, y \in G \quad x * y = y * x \tag{1}$$

On dit que le groupe G est **abélien** (**commutatif**).

Groupe

Un **groupe** $(G, *)$ est un ensemble G muni d'une **opération** $*$(dite **loi de composition**) vérifiant les propriétés suivantes:

1. **Loi Interne**: $\forall x, y \in G, \quad x * y \in G.$

Si on plus, l'opération $*$ vérifie:

$$\forall x, y \in G \quad x * y = y * x \tag{1}$$

On dit que le groupe G est **abélien** (**commutatif**).

Définition

Groupe

Un **groupe** $(G, *)$ est un ensemble G muni d'une **opération** $*$(dite **loi de composition**) vérifiant les propriétés suivantes:

1. **Loi Interne**: $\forall x, y \in G, \quad x * y \in G.$
2. **Associativité**: $\forall x, y, z \in G \quad (x * y) * z = x * (y * z).$

Si on plus, l'opération $*$ vérifie:

$$\forall x, y \in G \quad x * y = y * x \tag{1}$$

On dit que le groupe G est **abélien** (**commutatif**).

Groupe

Un **groupe** $(G, *)$ est un ensemble G muni d'une **opération** $*$(dite **loi de composition**) vérifiant les propriétés suivantes:

1. **Loi Interne**: $\forall x, y \in G, \quad x * y \in G.$
2. **Associativité**: $\forall x, y, z \in G \quad (x * y) * z = x * (y * z).$
3. **Elément neutre**: $\exists e \in G$ tel que$\forall x \in G \quad x * e = e * x = x$

Si on plus, l'opération $*$ vérifie:

$$\forall x, y \in G \quad x * y = y * x \tag{1}$$

On dit que le groupe G est **abélien** (**commutatif**).

Définition

Groupe

Un **groupe** $(G, *)$ est un ensemble G muni d'une **opération** $*$(dite loi de composition) vérifiant les propriétés suivantes:

1. **Loi Interne**: $\forall x, y \in G, \quad x * y \in G.$
2. **Associativité**: $\forall x, y, z \in G \quad (x * y) * z = x * (y * z).$
3. **Elément neutre**: $\exists e \in G$ tel que$\forall x \in G \quad x * e = e * x = x$
4. **Elément inverse**: $\forall x \in G \;\; \exists x' \in G$ tel que$x * x' = x' * x = e$

Si on plus, l'opération $*$ vérifie:

$$\forall x, y \in G \quad x * y = y * x \tag{1}$$

On dit que le groupe G est **abélien** (**commutatif**).

Unicité Elément neutre

L'élément neutre est **unique**.

Supposons qu'on possède deux éléments uniques e_1 et e_2 dans $(G, *)$.

$$\left\{ \begin{array}{ccccc} e_1 & * & e_2 & = & e_1 \\ e_1 & * & e_2 & = & e_2 \end{array} \right. \tag{2}$$

Unicité Elément neutre

L'élément neutre est **unique**.

Supposons qu'on possède deux éléments uniques e_1 et e_2 dans $(G, *)$.

$$\begin{cases} e_1 * e_2 = e_1 \\ e_1 * e_2 = e_2 \end{cases} \tag{2}$$

Unicité Inverse

De même, on prouve que l'**inverse** d'un élément x est **unique**.
Supposons que pour un $x \in G$, on possède deux inverses x_1 et x_2. alors on peut évaluer l'expression:

$$x_1 * x * x_2 = \begin{cases} (x_1 * x) * x_2 = e * x_2 = x_2 \\ x_1 * (x * x_2) = x_1 * e = x_1 \end{cases} \tag{3}$$

Mini Exercices

1. Vérifier que les ensembles muni des opérations suivantes sont des **groupes**:
   1. $(\mathbb{Q}, \times)$
   2. $(\mathbb{Z}, +)$

   Justifier pourquoi les ensembles suivants ne sont pas des groupes:
   1. $(\mathbb{Z}, \times)$
   2. $(\mathbb{N}, +)$

Puissance

Pour un groupe $(G, *)$ et un élément $x \in G$, on peut définir l'opération $x * x$ par $\mathbf{x^2}$. Plus généralement:

$$x^n = \begin{cases} e & \text{si} \quad n = 0 \\ \underbrace{x * x \ldots * x}_{n \text{ fois}} & \text{pour} \quad n > 0 \end{cases} \tag{4}$$

On possède alors les propriétés suivantes:

Puissance

Pour un groupe $(G, *)$ et un élément $x \in G$, on peut définir l'opération $x \ * \ x$ par $\mathbf{x^2}$. Plus généralement:

$$x^n = \begin{cases} e & \text{si} \quad n = 0 \\ \underbrace{x * x \ldots * x}_{n \text{ fois}} & \text{pour} \quad n > 0 \end{cases} \tag{4}$$

On possède alors les propriétés suivantes:

1. $x^m \ * \ x^n = x^{n+m}$

Puissance

Pour un groupe $(G, *)$ et un élément $x \in G$, on peut définir l'opération $x \ * \ x$ par $\mathbf{x^2}$. Plus généralement:

$$x^n = \begin{cases} e & \text{si} \quad n = 0 \\ \underbrace{x * x \ldots * x}_{n \text{ fois}} & \text{pour} \quad n > 0 \end{cases} \tag{4}$$

On possède alors les propriétés suivantes:

1. $x^m \ * \ x^n = x^{n+m}$
2. $(x^m)^n = x^{nm}$

Puissance

Pour un groupe $(G, *)$ et un élément $x \in G$, on peut définir l'opération $x * x$ par $\mathbf{x^2}$. Plus généralement:

$$x^n = \begin{cases} e & \text{si} \quad n = 0 \\ \underbrace{x * x \ldots * x}_{n \text{ fois}} & \text{pour} \quad n > 0 \end{cases} \tag{4}$$

On possède alors les propriétés suivantes:

1. $x^m * x^n = x^{n+m}$
2. $(x^m)^n = x^{nm}$
3. $(x * y)^{-1} = \mathbf{y^{-1}} * \mathbf{x^{-1}}$

Puissance

Pour un groupe $(G, *)$ et un élément $x \in G$, on peut définir l'opération $x \, * \, x$ par $\mathbf{x^2}$. Plus généralement:

$$x^n = \begin{cases} e & \text{si} \quad n = 0 \\ \underbrace{x * x \ldots * x}_{n \text{ fois}} & \text{pour} \quad n > 0 \end{cases} \tag{4}$$

On possède alors les propriétés suivantes:

1. $x^m \, * \, x^n = x^{n+m}$
2. $(x^m)^n = x^{nm}$
3. $(x \, * \, y)^{-1} = \mathbf{y^{-1} \, * \, x^{-1}}$
4. **Si G est abélien**, $(x * y)^n = x^n \, * \, y^n$

Mini Exercice

1. Soit $f_{a,b} : \mathbb{R} \to \mathbb{R}$ l'application définie par: $x \to ax + b$.
   Montrer que le groupe:

$$\left(\mathcal{F} = \{f_{a,b} \mid a \in \mathbb{R}^*, b \in \mathbb{R}\}, \circ\right) \tag{5}$$

   est un groupe non commutatif.

2. Soit $G =]-1, 1[$, Pour $x, y \in G$ on définit:

$$x * y = \frac{x + y}{1 + xy} \tag{6}$$

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

- Souvent on travaille avec des ensembles G qui sont des parties des groupes classiques comme $(\mathbb{R}, \times)$. Il existe alors une méthode **plus simple** pour démontrer que G est un groupe.

- Souvent on travaille avec des ensembles G qui sont des parties des groupes classiques comme $(\mathbb{R}, \times)$. Il existe alors une méthode **plus simple** pour démontrer que G est un groupe.

Sous groupe

Soit $(G, *)$ un groupe. Une **partie $\mathbf{H}$** $\subset G$ est un **sous groupe** de G si:

- $\mathbf{e} \in H$
- $\forall x, y \in H, \quad x * y \in H$
- $\forall x \in H, \quad x^{-1} \in H.$

- Souvent on travaille avec des ensembles G qui sont des parties des groupes classiques comme $(\mathbb{R}, \times)$. Il existe alors une méthode **plus simple** pour démontrer que G est un groupe.

Sous groupe

Soit $(G, *)$ un groupe. Une **partie $\mathbf{H}$** $\subset G$ est un **sous groupe** de G si:

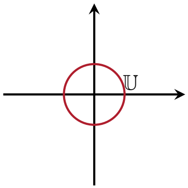
- $\mathbf{e} \in H$
- $\forall x, y \in H, \quad x * y \in H$
- $\forall x \in H, \quad x^{-1} \in H.$

Remarque

Une méthode plus simple pour prouver que H est un **sous groupe** est:

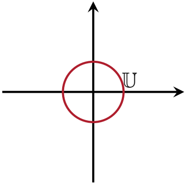
- $H \neq \emptyset$
- $\forall x, y \in H \quad x * y^{-1} \in H.$

Exemples



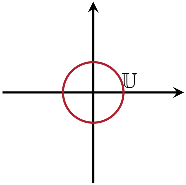
Exemples

- $\left(\mathbb{R}_+^*, \times\right)$ est un **sous groupe** de $(\mathbb{R}^*, \times)$



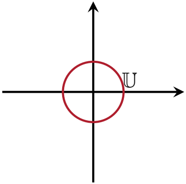
Exemples

- $\left(\mathbb{R}_+^*, \times\right)$ est un **sous groupe** de $(\mathbb{R}^*, \times)$
  - $1 \in \mathbb{R}_+^*$



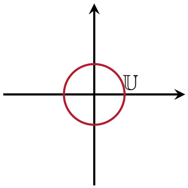
Exemples

- $\left(\mathbb{R}_+^*, \times\right)$ est un **sous groupe** de $(\mathbb{R}^*, \times)$
  - $1 \in \mathbb{R}_+^*$
  - $\forall x, y \in \mathbb{R}_+^* \quad x \times y \in \mathbb{R}_+^*.$



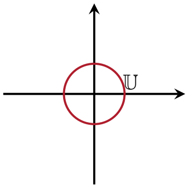
Exemples

- $\left(\mathbb{R}_+^*, \times\right)$ est un **sous groupe** de $(\mathbb{R}^*, \times)$
  - $1 \in \mathbb{R}_+^*$
  - $\forall x, y \in \mathbb{R}_+^* \quad x \times y \in \mathbb{R}_+^*.$
  - $\forall x \in \mathbb{R}_+^* \quad \dfrac{1}{x} \in \mathbb{R}_+^*$



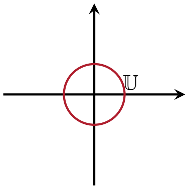
Exemples

- $(\mathbb{R}_+^*, \times)$ est un **sous groupe** de $(\mathbb{R}^*, \times)$
  - $1 \in \mathbb{R}_+^*$
  - $\forall x, y \in \mathbb{R}_+^* \quad x \times y \in \mathbb{R}_+^*$.
  - $\forall x \in \mathbb{R}_+^* \quad \dfrac{1}{x} \in \mathbb{R}_+^*$
- $(\mathbb{Z}, +)$ est un sous groupe de $(\mathbb{R}, +)$.



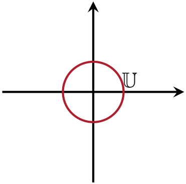
Exemples

- $(\mathbb{R}_+^*, \times)$ est un **sous groupe** de $(\mathbb{R}^*, \times)$
  - $1 \in \mathbb{R}_+^*$
  - $\forall x, y \in \mathbb{R}_+^* \quad x \times y \in \mathbb{R}_+^*.$
  - $\forall x \in \mathbb{R}_+^* \quad \dfrac{1}{x} \in \mathbb{R}_+^*$
- $(\mathbb{Z}, +)$ est un sous groupe de $(\mathbb{R}, +)$.
- Soit l'ensemble $\mathbb{U} = \{z \in \mathbb{C} \mid |z| = 1\}$



Exemples

- $(\mathbb{R}_+^*, \times)$ est un **sous groupe** de $(\mathbb{R}^*, \times)$
  - $1 \in \mathbb{R}_+^*$
  - $\forall x, y \in \mathbb{R}_+^* \quad x \times y \in \mathbb{R}_+^*$.
  - $\forall x \in \mathbb{R}_+^* \quad \dfrac{1}{x} \in \mathbb{R}_+^*$
- $(\mathbb{Z}, +)$ est un sous groupe de $(\mathbb{R}, +)$.
- Soit l'ensemble $\mathbb{U} = \{z \in \mathbb{C} \mid |z| = 1\}$
  - Sachant que $(\mathbb{C}, \times)$ est un groupe, prouvez que $\mathbb{U}$ muni de $\times$ est aussi un groupe.



Théorème

Les **seuls** sous groupes de $\mathbb{Z}$, sont les $\mathbf{n}\mathbb{Z}$ pour $n \in \mathbb{N}$.

$$n\mathbb{Z} = \{k.n \mid k \in \mathbb{Z}\} \tag{7}$$

- Lister les éléments de $3\mathbb{Z}$.
- Donner une démonstration de ce théorème.

Mini Exercices

1. Montrer que $\{2^n \mid n \in \mathbb{Z}\}$ est un sous groupe de $(\mathbb{R}^*, \times)$
2. Montrer que si H et $H^{'}$ sont deux sous groupes de $(G, *)$, alors $H \cap H^{'}$ est aussi un sous groupe.
3. Montrer que $5\mathbb{Z} \cup 8\mathbb{Z}$ n'est pas un sous groupe.

Morphisme

Soit $(G, *)$ et $(G', \diamond)$ deux **groupes**. Une application $f : G \Longrightarrow G'$ est un **morphisme de groupes** si:

$$\forall x, y \in G \quad f(x * y) = f(x) \diamond f(y) \tag{8}$$

Morphisme

Soit $(G, *)$ et $(G', \diamond)$ deux **groupes**. Une application $f : G \Longrightarrow G'$ est un **morphisme de groupes** si:

$$\forall x, y \in G \quad f(x * y) = f(x) \diamond f(y) \tag{8}$$

Les deux exemples classiques que vous connaissez sont:

- $G = (\mathbb{R}, +)$ et $G' = \left(\mathbb{R}_+^*, \times\right)$. Le morphisme classique qui transforme l'**addition** en **multiplication** est la fonction **exponentielle**

Morphisme

Soit $(G, *)$ et $(G', \diamond)$ deux **groupes**. Une application $f : G \Longrightarrow G'$ est un **morphisme de groupes** si:

$$\forall x, y \in G \quad f(x * y) = f(x) \diamond f(y) \tag{8}$$

Les deux exemples classiques que vous connaissez sont:

- $G = (\mathbb{R}, +)$ et $G' = (\mathbb{R}_+^*, \times)$. Le morphisme classique qui transforme l'**addition** en **multiplication** est la fonction **exponentielle**

$$\forall x, y \in \mathbb{R} \quad \exp(x + y) = \exp(x) \times \exp(y) \tag{9}$$

- Inversement, la fonction **logarithme** est un morphisme de groupe entre G' et G.

$$\log(x \times y) = \log(x) + \log(y) \tag{10}$$

Propriétés(1)

Proposition

Soit $f\ :\ G \Longrightarrow G^{'}$ un morphisme de groupe. On note e_G $(e_{G^{'}})$ l'élément neutre de $G(G^{'})$. Alors:

- $$f(e_G) = e_{G^{'}} \tag{11}$$
- $$\forall x \in G \quad f(x^{-1}) = (f\,(x))^{-1} \tag{12}$$

- Pour l'exemple de logarithme, on sait déjà que:

$$\log(1) = 0 \tag{13}$$

- Donner une **preuve** des deux équations.

- Soient deux morphismes $f: G \Longrightarrow G^{'}$ et $g: G^{'} \Longrightarrow G^{''}$

Composée

La composée $\mathbf{g} \circ \mathbf{f}$ est un morphisme de groupe entre G et $G^{''}$.

- Soient deux morphismes $f: G \Longrightarrow G^{'}$ et $g: G^{'} \Longrightarrow G^{''}$

Composée

La composée $g \circ f$ est un morphisme de groupe entre G et $G^{''}$.

Inverse

Si l'application est **bijective**. Alors $\mathbf{f}^{-1}$ est aussi un morphisme de groupe entre $G^{'}$ et G.

- Dans ce cas, on dit que:
  - f est un **isomorphisme**.
  - Les deux groupes G et $G^{'}$ sont **isomorphes**

- Si $f : G \longrightarrow G^{'}$ est un morphisme de groupe. Alors on identifie deux **sous groupes** importants:

Noyau

Le **noyaux** (*kernel*) de f est

$$\textbf{Kern}\ f = \{x \in G \mid f(x) = e_{G'}\} = f^{-1}\left(\{e_{G'}\}\right) \tag{14}$$

- Si $f : G \longrightarrow G^{'}$ est un morphisme de groupe. Alors on identifie deux **sous groupes** importants:

Noyau

Le **noyaux** (*kernel*) de f est

$$\textbf{Kern } f = \{x \in G \mid f(x) = e_{G^{'}}\} = f^{-1}\left(\{e_{G^{'}}\}\right) \tag{14}$$

Image

L'**image** de f est:

$$\textbf{Img } f = \{f(x) \mid x \in G\} \subset G^{'} \tag{15}$$

Voici quelque propriétés du noyau et l'image de f:.

Propriétés

1. **Kern** f est un **sous groupe** de G.
2. **Img** f est un **sous groupe** de $G^{'}$.
3. f est **injectif** si et seulement si **Kern** f $= \{e_G\}$
4. f est **surjectif** si et seulement si **Img** f $= G^{'}$

- Preuve:

Mini Exercices

1. Soit $f\ :\ (\mathbb{Z},+) \longrightarrow (\mathbb{Q}^*,\times)$ définie par $f(n) = 2^n$.
   - Montrer que f est un morphisme de groupe.
   - f est elle **injective**, **surjective**?
2. Soit $(G,*)$ un groupe et $f\ :\ G \longrightarrow G$ l'application définie par $f(x) = x^2$.
   - Montrer que si $(G,*)$ est **commutatif**, alors f est un morphisme de groupe.
   - Montrer la réciproque.
3. Montrer qu'il n'existe pas de morphisme $f : (\mathbb{Z},+) \longrightarrow (\mathbb{Z},+)$ tel que:
$$f(2) = 3$$

- Pour un $n \geqslant 1$, on rappelle que:

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{n-1}\}$$

où $\overline{p}$ désigne la classe **d'équivalence** de p modulo n.

- Sur cet ensemble, on peut définir l'opérateur d'**addition** entre les classes par:

$$\overline{p} + \overline{q} = \overline{p+q} \tag{16}$$

On prouve que:

Groupe

$(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe commutatif.

Définition

Un groupe $(G, *)$ est dit **cyclique** si

$$\exists! a \in G \quad \forall x \in G, \exists k \in \mathbb{Z} \text{ tel que } x = a^n$$

ou que le groupe G est engendré par l'élément a.

Exemple

Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe **cyclique** engendré par l'élément $a = \overline{1}$.
On peut prouver que $\forall k \in \mathbb{Z}/n\mathbb{Z}$ on a:

$$k = \underbrace{\overline{1} + \overline{1} + \ldots, \overline{1}}_{k \text{ fois}}$$

Théorème

Soit $(G, *)$ un groupe de cardinal fini n. Alors G est **isomorphe** à $\mathbb{Z}/n\mathbb{Z}$.