3.1 Structure de groupes

3.1.1 Définition

Soit G un ensemble muni d'une loi $\star$. $(G,\star)$ est un groupe si et seulement si :

1. **La loi $\star$ est interne, c'est à dire :**
$$(\forall x \in G)\,(\forall y \in G)\,(x \star y \in G)$$
2. **La loi $\star$ est associative, c'est à dire :**
$$(\forall x \in G)\,(\forall y \in G)\,(\forall z \in G)\,((x \star y) \star z = x \star (y \star z) = x \star y \star z)$$
3. **La loi $\star$ admet un élément neutre e, c'est à dire :**
$$(\exists e \in G)\,(\forall x \in G)\,(x \star e = e \star x = x)$$
4. **Tout élément $x \in G$, admet, pour la loi $\star$ un symétrique x', c'est à dire :**
$$(\forall x \in G)\,(\exists x' \in G)\,(x \star x' = x' \star x = e)$$

Si, de plus, la loi $\star$ est commutative, c'est à dire si :
$$(\forall x \in G)\,(\forall y \in G)\,(x \star y = y \star x)$$
Le groupe $(G,\star)$ est dit groupe commutatif ou groupe abélien

Remarque 1 :

1. Les notions de loi de composition interne, d'associativité, d'éléments neutres et de symétriques ont été rencontrées en étudiant les entiers naturels
2. Si l'ensemble G est fini et de cardinal n, on dit que n est **l'ordre** du groupe

Exemple 1 :

Exemples de groupes

1. $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$ et $(\mathbb{C},+)$ sont des groupes commutatifs pour l'addition
2. $(\mathbb{Q}^*,\times)$, $(\mathbb{R}^*,\times)$ et $(\mathbb{C}^*,\times)$ sont des groupes commutatifs pour la multiplication
3. Est ce que $\mathbb{Z}^*$ est un groupe pour la multiplication ?

Exercice 1 :

1. Montrer que $\mathcal{U} = \{z \in \mathbb{C}$ tels que $|z| = 1\}$ est un groupe pour la multiplication.
2. Soit E un ensemble et $\mathcal{B}(E)$ l'ensemble des bijections de E. Montrer que $(\mathcal{B}(E),\circ)$ est un groupe. En étudier la commutativité

3.1.2 Théorème : propriété fondamentale d'un groupe

Soit $(G,\star)$ un groupe. Alors :
Pour tout $a \in G$ les applications :

$$\left\{\begin{array}{rcl} \gamma_a : G & \longrightarrow & G \\ x : & \longmapsto & \gamma_a(x) = a \star x \end{array}\right. \quad \text{et} \quad \left\{\begin{array}{rcl} \delta_a : G & \longrightarrow & G \\ x : & \longmapsto & \delta_a(x) = x \star a \end{array}\right.$$

Sont bijectives

Démonstration

Au vu de la similarité de γ_a et δ_a, nous ne démontrons le théorème que pour une seule application δ_a, par exemple !!
Soit donc $a \in G$; nous notons e l'élément neutre de G

1. Démontrons que δ_a est injective
   Soient $x \in G$ et $y \in G$ tels que $\delta_a(x) = \delta_a(y)$; alors, $x \star a = y \star a$.
   Comme $a \in G$, a admet pour la loi $\star$ un inverse a^{-1}. Composons à droite par a^{-1}
   $$x \star a = y \star a \Longrightarrow (x \star a) \star a^{-1} = (y \star a) \star a^{-1}$$
   De l'associativité de la loi $\star$, nous avons :
   $$(x \star a) \star a^{-1} = (y \star a) \star a^{-1} \Longrightarrow x \star \left(a \star a^{-1}\right) = y \star \left(a \star a^{-1}\right) \Longrightarrow x \star e = y \star e \Longrightarrow x = y$$
   Nous avons donc l'implication $\delta_a(x) = \delta_a(y) \Longrightarrow x = y$, ce qui montre que δ_a est injective
2. Démontrons que δ_a est surjective
   Soit $y \in G$; existe-t-il $x \in G$ tel que $\delta_a(x) = y$.
   S'il existe, alors : $x \star a = y$; en composant à droite par a^{-1}, nous avons :
   $$x \star a = y \Longrightarrow (x \star a) \star a^{-1} = y \star a^{-1}$$
   De l'associativité, nous avons :
   $$(x \star a) \star a^{-1} = y \star a^{-1} \Longleftrightarrow x \star \left(a \star a^{-1}\right) = y \star a^{-1} \Longleftrightarrow x = y \star a^{-1}$$
   Ainsi, pour tout $y \in G$, il existe $x = y \star a^{-1}$ tel que $\delta_a(x) = y$
   δ_a est donc surjective

δ_a étant injective et surjective, est donc bijective

Remarque 2 :

1. Le théorème 3.1.2 peut aussi s'énoncer différemment :
   Pour tout $a \in G$ et tout $b \in G$, les équation $a \star x = b$ et $x \star a = b$ ont une unique solution
2. Le théorème 3.1.2 permet de dire que dans un groupe, tout élément est régulier , c'est à dire que :
   $$a \star b = a \star c \Longrightarrow b = c \text{ et } b \star a = c \star a \Longrightarrow b = c$$
3. Si G est un groupe fini, dans la table de multiplication du groupe, les éléments ne doivent apparaître qu'une seule fois

Exercice 2 :

Un ensemble E est muni d'une loi $\star$ interne et associative ; on suppose que, pour tout $a \in G$, γ_a et δ_a sont surjectives. Montrer que $(E, \star)$ est un groupe

3.1.3 Définition de sous-groupe

Soit $(G, \star)$ un groupe. On appelle sous-groupe, toute partie $H \subset G$ telle que :
- **H est non vide**
- **H est stable pour la loi $\star$, c'est à dire : $(\forall x \in H)(\forall y \in H)(x \star y \in H)$**
- **$(H, \star)$ est un groupe**

Remarque 3 :

1. Les sous-groupes de $(G, \star)$ ont tous le même élément neutre e
2. Les sous-groupes triviaux de $(G, \star)$ sont $(G, \star)$ lui même et $(\{e\}, \star)$

Exemple 2 :

Des exemples de sous-groupes

1. $(\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{R}, +)$
2. $(\mathbb{Q}^*, \times)$ est un sous-groupe de $(\mathbb{R}^*, \times)$
3. Pour $n \in \mathbb{N}^*$, les ensembles $n\mathbb{Z}$,des multiples entiers de n, muni de l'addition sont des sous groupes de $(\mathbb{Z}, +)$

3.1.4 Caratérisation d'un sous-groupe

Soit $(G, \star)$ un groupe. Alors $H \subset G$ est un sous-groupe de $(G, \star)$ si et seulement si :

1. **H est non vide**
2. **Pour tout $x \in H$ et tout $y \in H$, $x \star y^{-1} \in H$**

Démonstration

1. On suppose $(H, \star)$ sous-groupe de $(G, \star)$
   - ▷ Alors, comme $e \in H$, $H \neq \emptyset$
   - ▷ D'autre part, si $y \in H$, comme H est un groupe, $y^{-1} \in H$ et pour $x \in H$, comme $\star$ est une loi de composition interne, $x \star y^{-1} \in H$
2. Réciproquement, on suppose $H \neq \emptyset$ et que pour tout $x \in H$ et tout $y \in H$, $x \star y^{-1} \in H$

   Montrons que $(H, \star)$ est un groupe.
   - ▷ Tout d'abord, la loi $\star$ étant associative dans $(G, \star)$, elle l'est, aussi, à fortiori dans H
   - ▷ D'autre part, comm e$H \neq \emptyset$, il existe $x \in H$; comme $H \subset G$, $x \in G$ et x^{-1} existe, et nous avons même $x^{-1} \in G$

     De la propriété $x \star y^{-1} \in H$ vraie pour tout $x \in H$ et tout $y \in H$, en faisant $y = x$, nous avons $x \star x^{-1} \in H$, c'est à dire $e \in H$
   - ▷ Soit $y \in H$; comme $e \in H$, alors $e \star y^{-1} \in H$ i.e. $y^{-1} \in H$, c'est à dire que tout élément $y \in H$ a son inverse dans H
   - ▷ Soit $x \in H$ et $y \in H$; nous allons montrer que $x \star y \in H$ et que donc la loi $\star$ est interne dans H

     Nous venons de montrer que si $y \in H$, alors $y^{-1} \in H$ et donc, d'après la propriété de H, $x \star \left(y^{-1}\right)^{-1} \in H$. Comme $\left(y^{-1}\right)^{-1} = y$, nous avons $x \star y \in H$

   Donc, $(H, \star)$ est un groupe, et comme $H \subset G$, $(H, \star)$ est un sous-groupe de $(G, \star)$

Exemple 3 :

Montrons maintenant que pour $n \in \mathbb{N}^*$, les ensembles $n\mathbb{Z}$,des multiples entiers de n, muni de l'addition sont des sous groupes de $(\mathbb{Z}, +)$

Rappelons la définition de $n\mathbb{Z}$ pour $n \in \mathbb{N}^*$

$$n\mathbb{Z} = \{T \in \mathbb{Z} \text{ tels que il existe } u \in \mathbb{Z} \text{ tel que } T = un\}$$

Par exemple : $7\mathbb{Z} = \{T \in \mathbb{Z} \text{ tels que il existe } u \in \mathbb{Z} \text{ tel que } T = 7u\}$

$(n\mathbb{Z}, +)$ est un sous groupe de $(\mathbb{Z}, +)$

- ▷ $n\mathbb{Z} \neq \emptyset$ puisque $0 = 0 \times n \in n\mathbb{Z}$
- ▷ Soient $z_1 \in n\mathbb{Z}$ et $z_2 \in n\mathbb{Z}$; avons nous $z_1 - z_2 \in n\mathbb{Z}$

  Comme $z_1 \in n\mathbb{Z}$, alors, il existe $k_1 \in \mathbb{Z}$ tel que $z_1 = k_1 \times n$

  De même, comme $z_2 \in n\mathbb{Z}$, alors, il existe $k_2 \in \mathbb{Z}$ tel que $z_2 = k_2 \times n$

  Donc : $z_1 - z_2 = k_1 n - k_2 n = (k_1 - k_2) \times n$. Comme $k_1 - k_2 \in \mathbb{Z}$, nous avons $z_1 - z_2 \in n\mathbb{Z}$

Et donc, $n\mathbb{Z}$, muni de l'addition est un sous groupe de $(\mathbb{Z}, +)$

On peut démontrer que les seuls sous-groupes de $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$ où $n \in \mathbb{N}^*$

Exercice 3 :

Soit E un ensemble quelconque et $a \in E$ un élément de E. Nous savons que $(\mathcal{B}(E), \circ)$ est un groupe. Nous appelons $\mathcal{A}$ l'ensemble des bijections de $\mathcal{B}(E)$ laissant a fixe *(c'est à dire $f \in \mathcal{A} \Longleftrightarrow f(a) = a$)*. Démontrer que $(\mathcal{A}, \circ)$ est un sous-groupe de $(\mathcal{B}(E), \circ)$

Exercice 4 :

Soit $(G, \star)$ un groupe. On appelle centre de G l'ensemble $Z(G)$ des éléments de G qui commutent avec tous les éléments de G, c'est à dire :

$$Z(G) = \{c \in G \text{ tels que } (\forall x \in G)(x \star c = c \star x)\}$$

Démontrer que $(Z(G), \star)$ est un sous-groupe de $(G, \star)$

3.1.5 Théorème

Soit $(G, \star)$ un groupe,$(H_1, \star)$ et $(H_2, \star)$ 2 sous-groupes de$G$
Alors $H_1 \cap H_2$ est un sous-groupe de G

Démonstration

1. Premièrement, $H_1 \cap H_2 \neq \emptyset$
   En effet, $e \in H_1$ et $e \in H_2$ et donc $e \in H_1 \cap H_2$
2. Soient $x \in H_1 \cap H_2$ et $y \in H_1 \cap H_2$. Montrons que $x \star y^{-1} \in H_1 \cap H_2$
   - ▷ Comme $x \in H_1$ et $y \in H_1$, nous avons $x \star y^{-1} \in H_1$
   - ▷ Et comme $x \in H_2$ et $y \in H_2$, nous avons $x \star y^{-1} \in H_2$

   Et nous concluons donc que $x \star y^{-1} \in H_1 \cap H_2$

Donc, $H_1 \cap H_2$ est un sous-groupe de G

Remarque 4 :

Le théorème est toujours vrai pour n sous groupes $H_1, \ldots, H_n$ de G : nous avons $\bigcap\limits_{i=1}^{n} H_i$ qui est un sous-groupe de G

Exemple 4 :

Dans $(\mathbb{Z}, +)$, groupe additif, définissons $2\mathbb{Z} \cap 3\mathbb{Z}$

$2\mathbb{Z}$ et $3\mathbb{Z}$ sont des sous-groupes de $\mathbb{Z}$ et donc $2\mathbb{Z} \cap 3\mathbb{Z}$ est aussi un sous-groupe de $\mathbb{Z}$
Si $m \in 2\mathbb{Z} \cap 3\mathbb{Z}$, alors m est un multiple de 2 et de 3, donc de 6, et donc $m \in 6\mathbb{Z}$; réciproquement, il est clair que si $m \in 6\mathbb{Z}$, m est aussi un multiple de 2 et m est un multiple de 3, et donc $m \in 2\mathbb{Z} \cap 3\mathbb{Z}$; en conclusion, $6\mathbb{Z} = 2\mathbb{Z} \cap 3\mathbb{Z}$

3.1.6 Sous-groupes engendrés : définition

1. **Soit $(G, \star)$ un groupe et $A \subset G$, un sous-ensemble de G. On appelle $\Gamma(A)$ le plus petit sous-groupe de G contenant A**
   On dit que $\Gamma(A)$ est le sous-groupe de G engendré par A
2. **On appelle Groupe cyclique un groupe G engendré par un seul élément : $G = \Gamma(\{a\})$**

Remarque 5 :

1. Si A est un sous-groupe de G, alors $\Gamma(A) = A$
2. En utilisant la notation multiplicative, tout groupe cyclique est du type $G = \Gamma(\{a\}) = \{a^n \text{ où } n \in \mathbb{Z}\}$
   En reprécisant les choses :
   - $a^0 = e$ où e est le neutre de G
   - Pour $n \in \mathbb{N}^*$, $a^n = \underbrace{a \star a \star a \star \cdots \star a}_{n \text{ fois}}$
   - Toujours pour $n \in \mathbb{N}$, $a^{-n} = \underbrace{a^{-1} \star a^{-1} \star a^{-1} \star \cdots \star a^{-1}}_{n \text{ fois}}$

Exemple 5 :

<u>Exemples de groupes cycliques</u>

1. L'ensemble $\{2^n \text{ avec } n \in \mathbb{Z}\}$, muni de la multiplication est un groupe cyclique.
2. Plus généralement, pour tout $b \in \mathbb{Z}$, l'ensemble $\{b^n \text{ avec } n \in \mathbb{Z}\}$, muni de la multiplication est un groupe cyclique
3. $\mathcal{U}_n = \left\{e^{\frac{2ik\pi}{n}} \text{ avec } k \in \mathbb{Z}\right\}$, l'ensemble des racines *n-ièmes* de 1, muni de la multiplication est un groupe cyclique fini de générateur $e^{\frac{2ik\pi}{n}}$

3.1.7 Définition d'homomorphisme de groupe

Soient $(G, \star)$ et $(G_1, \top)$ 2 groupes
l'application $f : G \longrightarrow G_1$ est un <u>homomorphisme de groupe</u> si et seulement si

$$(\forall x \in G)\,(\forall y \in G)\,(f(x \star y) = f(x) \top f(y))$$

Exemple 6 :

Nous livrons, ici, les exemples les plus classiques d'homomorphismes de groupe :

1. La fonction logarithme :ln : $(\mathbb{R}^{*+}, \times) \longrightarrow (\mathbb{R}, +)$ est un premier exemple d'homomorphisme
2. La fonction exponentielle, réciproque de la fonction logarithme est aussi un homomorphisme : $\exp : (\mathbb{R}, +) \longrightarrow (\mathbb{R}^{*+}, \times)$
3. L'exponentielle complexe :
$$\left\{ \begin{array}{rcl} \varphi : (\mathbb{R}, +) & \longrightarrow & (\mathbb{C}, \times) \\ x & \longmapsto & \varphi(x) = e^{ix} \end{array} \right.$$
4. La conjugaison dans $\mathbb{C}$ est un homomorphisme de groupe additif :
$$\left\{ \begin{array}{rcl} f : (\mathbb{C}, +) & \longrightarrow & (\mathbb{C}, +) \\ z & \longmapsto & f(z) = \overline{z} \end{array} \right.$$
5. La conjugaison dans $\mathbb{C}$ est aussi un homomorphisme de groupe multiplicatif :
$$\left\{ \begin{array}{rcl} f : (\mathbb{C}, \times) & \longrightarrow & (\mathbb{C}, \times) \\ z & \longmapsto & f(z) = \overline{z} \end{array} \right.$$

3.1.8 Vocabulaire

1. **Si $f : (G, \star) \longrightarrow (G, \star)$ est un homomorphisme de groupe, on dit que f est un <u>endomorphisme</u>**
2. **Si $f : (G, \star) \longrightarrow (G_1, \top)$ est un <u>homomorphisme de groupe bijectif</u>, on dit que f est un <u>isomorphisme</u>**
3. **Si $f : (G, \star) \longrightarrow (G, \star)$ est un homomorphisme de groupe bijectif, on dit que f est un <u>automorphisme</u>**

Exemple 7 :

Les fonctions logarithme :ln : $(\mathbb{R}^{*+}, \times) \longrightarrow (\mathbb{R}, +)$ et exponentielle : exp : $(\mathbb{R}, +) \longrightarrow (\mathbb{R}^{*+}, \times)$ sont des exemples d'isomorphismes de groupe

Exercice 5 :

Soit $(G, \star)$ un groupe de neutre e et $a \in G$; on considère les applications f_a définies par :

$$\begin{cases} f_a : G & \longrightarrow & G \\ \quad\ x & \longmapsto & f_a(x) = a \star x \star a^{-1} \end{cases}$$

Montrer que f_a est un automorphisme

3.1.9 Théorème

La composée de 2 homomorphismes de groupes est un homomorphisme de groupe.
Autrement dit :
Soient $(G, \star)$, $(G_1, \top)$, $(G_2, \perp)$ 3 groupes.
Soient $f : G \longrightarrow G_1$ et $g : G_1 \longrightarrow G_2$ 2 homomorphismes de groupes, alors $g \circ f$ est aussi un homomorphisme de groupe

<u>Démonstration</u>

Soient $f : G \longrightarrow G_1$ et $g : G_1 \longrightarrow G_2$ 2 homomorphismes de groupes, $x \in G$ et $y \in G$.
Il faut donc montrer que $g \circ f(x \star y) = g \circ f(x) \perp g \circ f(y)$

$$\begin{aligned} g \circ f(x \star y) = &\ g[f(x \star y)] \\ = &\ g[f(x) \top f(y)] \text{ car } f \text{ est un homomorphisme} \\ = &\ g[f(x)] \perp g[f(y)] \text{ car } g \text{ est un homomorphisme} \\ = &\ g \circ f(x) \perp g \circ f(y) \end{aligned}$$

Ce que nous voulions, $g \circ f$ est donc un homomorphisme de groupe

3.1.10 Théorème

Soient $(G, \star)$ et $(G_1, \top)$ 2 groupes.
$f : (G, \star) \longrightarrow (G_1, \top)$ un homomorphisme de groupe.
On appelle e de neutre de G et e' celui de G_1. Alors :

1. **Nous avons $f(e) = e'$**
2. **Pour tout $x \in G$, nous avons $f(x^{-1}) = (f(x))^{-1}$**
3. **$f(G)$ est un sous-groupe de G_1 appelé <u>image de f</u> et noté $\mathrm{Im} f$**
4. **Plus généralement, si $H \subset G$ est un sous groupe de G, alors $f(H)$ est un sous-groupe de G_1**
5. **Si $X \subset G_1$ est un sous-groupe de G_1, alors $f^{-1}(X)$ est un sous-groupe de G**
6. **On note $\ker f = \{x \in G$ tel que $f(x) = e'\}$, alors $\ker f$ est un sous-groupe de G appelé <u>noyau de f</u>**

<u>Démonstration</u>

1. <u>Démontrons que $f(e) = e'$</u>
   Soit $x \in G$. Alors, $f(x) = f(x \star e) = f(x) \top f(e)$. Or, $f(x) = f(x) \top e'$ et donc $f(x) \top f(e) = f(x) \top e'$.
   Par régularité des groupes, on en déduit que $f(e) = e'$

2. <u>Démontrons que $f\left(x^{-1}\right)=\left(f\left(x\right)\right)^{-1}$</u>
   Soit $x\in G$. Alors, $f\left(e\right)=f\left(x\star x^{-1}\right)=f\left(x\right)\top f\left(x^{-1}\right)=e'$. De $f\left(x\right)\top f\left(x^{-1}\right)=e'$ on déduit que $f\left(x^{-1}\right)=\left(f\left(x\right)\right)^{-1}$
3. <u>Démontrons que $f\left(G\right)$ est un sous-groupe de G_1</u>
   - ▷ Premièrement, $f\left(G\right)\neq\emptyset$ puisque $e'=f\left(e\right)\in f\left(G\right)$
   - ▷ Soient $y_1\in f\left(G\right)$ et $y_2\in f\left(G\right)$; il faut montrer que $y_1\top\left(y_2\right)^{-1}\in f\left(G\right)$
     Il existe $x_1\in G$ tel que $f\left(x_1\right)=y_1$ et $x_2\in G$ tel que $f\left(x_2\right)=y_2$
     Donc $y_1\top\left(y_2\right)^{-1}=f\left(x_1\right)\top\left(f\left(x_2\right)\right)^{-1}=f\left(x_1\right)\top f\left(x_2^{-1}\right)=f\left(x_1\star x_2^{-1}\right)$
     Comme $x_1\in G$ et $x_2\in G$, alors $x_1\star x_2^{-1}\in G$, et de $y_1\top\left(y_2\right)^{-1}=f\left(x_1\star x_2^{-1}\right)$, nous en déduisons que $y_1\top\left(y_2\right)^{-1}\in f\left(G\right)$

   Donc, $f\left(G\right)$ est un sous-groupe de G_1
4. <u>Si $H\subset G$ est un sous groupe de G, alors $f\left(H\right)$ est un sous-groupe de G_1</u>
   La démonstration de cette affirmation est très semblable à celle qui est ci-dessus, et je la laisse faire par le lecteur en exercice
5. <u>Démontrons que si $X\subset G_1$ est un sous-groupe de G_1, alors $f^{-1}\left(X\right)$ est un sous-groupe de G</u> Qu'est ce que $f^{-1}\left(X\right)$?
   Nous avons $f^{-1}\left(X\right)=\{x\in G \text{ tels que } f\left(x\right)\in X\}$
   - ▷ Premièrement, $f^{-1}\left(X\right)\neq\emptyset$ puisque $f\left(e\right)=e'$ et $e'\in X$; donc $e\in f^{-1}\left(X\right)$
   - ▷ Soient $x_1\in f^{-1}\left(X\right)$ et $x_2\in f^{-1}\left(X\right)$; il faut montrer que $x_1\star\left(x_2\right)^{-1}\in f^{-1}\left(X\right)$
     Comme $x_1\in f^{-1}\left(X\right)$ et $x_2\in f^{-1}\left(X\right)$, alors $f\left(x_1\right)\in X$ et $f\left(x_2\right)\in X$, et X étant un sous-groupe de G_1, alors $f\left(x_1\right)\top\left(f\left(x_2\right)\right)^{-1}\in X$
     Or, $f\left(x_1\right)\top\left(f\left(x_2\right)\right)^{-1}=f\left(x_1\right)\top\left(f\left(\left(x_2\right)^{-1}\right)\right)$
     f étant un homomorphisme, nous avons $f\left(x_1\right)\top\left(f\left(\left(x_2\right)^{-1}\right)\right)=f\left(x_1\star\left(x_2\right)^{-1}\right)$ et donc $f\left(x_1\star\left(x_2\right)^{-1}\right)\in X$ et donc $x_1\star\left(x_2\right)^{-1}\in f^{-1}\left(X\right)$

   Donc, $f^{-1}\left(X\right)$ est un sous-groupe de G
6. <u>$\ker f$ est un sous-groupe de G</u>
   Il suffit de remarquer que $\ker f=f^{-1}\left(\{e'\}\right)$ et que et donc que $\ker f$ est un cas particulier du point ci-dessus

Remarque 6 :

On peut résumer l'égalité $f\left(x^{-1}\right)=\left(f\left(x\right)\right)^{-1}$ par : « *L'image de l'inverse est l'inverse de l'image* »

Exemple 8 :

1. On retrouve, à l'aide de ce théorème, les propriétés de la fonction logarithme :
   - ▷ L'image du neutre de $\left(\mathbb{R}^{*+},\times\right)$ qui est 1 est le neutre de $\left(\mathbb{R},+\right)$ qui est 0 : $\ln 1=0$
   - ▷ L'image de l'inverse est l'inverse de l'image et donc, pour tout $x>0$, nous avons $\ln\dfrac{1}{x}=-\ln x$
2. Nous retrouvons les mêmes propriétés pour la fonction exponentielle.

3.1.11 Théorème

Soient $(G,\star)$ et $(G_1,\top)$ 2 groupes e est le neutre d eG et e_1, celui de G_1 et $f:(G,\star)\longrightarrow(G_1,\top)$ un homomorphisme de groupe.Alors f est injective si et seulement si $\ker f=\{e\}$

<u>Démonstration</u>

1. <u>Supposons f injective</u>
   Et bien sûr, le seul antécédent de e_1 par f est e, et donc $\ker f=\{e\}$

2. Supposons $\ker f = \{e\}$
   Démontrons que f est injective.
   Soient $x \in G$ et $y \in G$ tels que $f(x) = f(y)$ Alors,

$$f(x) = f(y) \iff f(x) \top (f(y))^{-1} = e_1 \iff f\left(x \star y^{-1}\right) = e_1 \iff x \star y^{-1} \in \ker f$$

   Comme $\ker f = \{e\}$, $x \star y^{-1} = e$, c'est à dire $x = y$ et donc f est injective

Exemple 9 :

Soit $\varphi : \mathbb{R} \longrightarrow \mathbb{C}$, définie par :

$$\begin{cases} \varphi : (\mathbb{R}, +) & \longrightarrow & (\mathbb{C}, \times) \\ x & \longmapsto & \varphi(x) = e^{ix} \end{cases}$$

φ n'est pas injective ; en effet, $\ker \varphi = \left\{x \in \mathbb{R} \text{ tels que } e^{ix} = 1\right\} = \{2k\pi \text{ où } k \in \mathbb{Z}\}$. Le noyau de φ n'est pas réduit au seul élément neutre de $(\mathbb{R}, +)$ et n'est donc pas injective

3.1.12 Théorème

Soient $(G, \star)$ et $(G_1, \top)$ 2 groupes et $f : (G, \star) \longrightarrow (G_1, \top)$ un isomorphisme de groupe.Alors $f^{-1} : (G_1, \top) \longrightarrow (G, \star)$ est aussi un isomorphisme de groupes
On dit que les 2 groupes $(G, \star)$ et $(G_1, \top)$ sont isomorphes

Démonstration

Soient $y_1 \in G_1$ et $y_2 \in G_1$. Il faut donc montrer que $f^{-1}(y_1 \top y_2) = f^{-1}(y_1) \star f^{-1}(y_2)$
Il existe $x_1 \in G$, unique, tel que $f(x_1) = y_1 \iff x_1 = f^{-1}(y_1)$, tout comme il existe $x_2 \in G$, unique, tel que $f(x_2) = y_2 \iff x_2 = f^{-1}(y_2)$ Donc :

$$f^{-1}(y_1 \top y_2) = f^{-1}(f(x_1) \top f(x_2)) = f^{-1}(f(x_1 \star x_2)) = x_1 \star x_2 = f^{-1}(y_1) \star f^{-1}(y_2)$$

Nous venons de démontrer que $f^{-1}(y_1 \top y_2) = f^{-1}(y_1) \star f^{-1}(y_2)$
$f^{-1} : (G_1, \top) \longrightarrow (G, \star)$ est donc un homomorphisme de groupe, bijectif, et est donc un isomorphisme

Remarque 7 :

La notion d'isomorphisme est forte ; elle sous-entend que les deux groupes ont même structure, et que, quelque part, moralement, ce sont les mêmes.