Dans tout ce chapitre, E est un ensemble.

Définition

*On appelle **loi de composition interne sur E (lci)** toute application de $E \times E$ dans E.*

Exemple

$$p : \begin{cases} \mathbb{R}^2 & \to & \mathbb{R} \\ (x,y) & \mapsto & x+y \end{cases}$$

Définition

*On appelle **magma** tout couple constitué d'un ensemble et d'une lci.*

Example

- $(\mathbb{R}, +)$ est un magma.
- $(\mathbb{Z}, -)$ est un magma.
- $(\mathbb{N}, -)$ n'est pas un magma : en effet $3 - 4 \notin \mathbb{N}$

Dans toute la suite, $\star$ est une lci sur E.

Définition

Soit $(E, \star)$ un magma.

- *On dit que E est **associatif** si pour tout $x, y, z \in E$, on a :*

$$x \star (y \star z) = (x \star y) \star z$$

L'élément $x \star (y \star z) = (x \star y) \star z$ est alors noté $x \star y \star z$.

- *On dit que E est **commutatif** si pour tout $x, y \in E$, on a :*

$$x \star y = y \star x$$

- *Soit $*$ une seconde lci sur E.*
  *On dit que dans E $\star$ est **distributive** par rapport à $*$ si pour tout $x, y, z \in E$, on a :*
  - $x \star (y * z) = (x \star y) * (x \star z)$
  - $(y * z) \star x = (y \star x) * (z \star x)$.

Remarque

On dit que dans $(E, \star)$ est distributive à gauche par rapport à $*$ si pour tout $x, y, z \in E$, on a :

$$x \star (y * z) = (x \star y) * (x \star z)$$

De même, on a la notion de distributivité à droite.

Example

1. $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$, $\mathbb{N}$ avec $+$ ou $\times$ sont associatifs, mais pas $(\mathbb{Z}, -)$ car $1-(2-3) \neq (1-2)-3$.
2. $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$, $\mathbb{N}$ avec $+$ ou $\times$ sont commutatifs, mais pas $(\mathbb{Z}, -)$, ni $(\mathscr{F}(\mathbb{R}, \mathbb{R}), \circ)$.
3. Sur $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}, \mathbb{N}$ la loi de composition interne $\times$ est distributive par rapport à $+$.
4. $\mathscr{P}(E)$, $\cap$ et $\cup$ sont distributives l'une par rapport à l'autre.

Définition (Elément neutre)

Soit $e \in E$.
On dit que e est un ***élément neutre à gauche*** *(resp. à droite) pour $\star$ si pour tout $x \in E$ on a*

$$e \star x = x$$

On dit que e est un ***élément neutre à droite*** *(resp. à droite) pour $\star$ si pour tout $x \in E$ on a*

$$x \star e = x$$

On dit que e est un ***élément neutre*** *pour $\star$ si c'est un élément neutre à gauche et à droite, i.e.*

$$\forall x \in E, e \star x = x \star e = x$$

Définition (Elément inversible)

Soit e un neutre pour $\star$ et soit $x \in E$.

- *On dit que x est **inversible à gauche** s'il existe un élément $y \in E$ tel que*

$$y \star x = e$$

Un tel élément y s'appelle UN inverse à gauche x.

- *On dit que x est **inversible à droite** s'il existe un élément $y \in E$ tel que*

$$x \star y = e$$

Un tel élément y s'appelle UN inverse à droite x.

- *On dit que x est **inversible** s'il est inversible à gauche et à droite, i.e. il existe $y \in E$ tel que*

$$y \star x = x \star y = e$$

Dans ce cas y est UN inverse de x.

Example

- 0 est un élément neutre pour $+$ dans $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$, $\mathbb{Z}$, $\mathbb{N}$.
- 1 est un élément neutre pour $\times$ dans $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$.
- Id_E est un élément neutre pour $\circ$ (composition) dans $\mathscr{F}(E,E)$ et les bijections sont tous les éléments inversibles de cet ensemble.

Remarque

1. Être inversible seulement à gauche ou à droite ne suffit pas pour être inversible tout court.

   Soit $f : \begin{cases} \mathbb{N} & \to & \mathbb{N} \\ n & \mapsto & 2n \end{cases}$ et $g : \begin{cases} \mathbb{N} & \to & \mathbb{N} \\ n & \mapsto & \begin{cases} \frac{n}{2} & \text{Si } n \text{ pair} \\ 0 & \text{Si } n \text{ impair} \end{cases} \end{cases}$

   On a $g \circ f = Id$ pour tout $h \in \mathscr{F}(\mathbb{N},\mathbb{N})$, $f \circ h \neq Id$ car 3 par exemple n'a pas d'antécédent par $f \circ h$ donc $f \circ h$ n'est pas l'identité.
2. Un neutre est toujours inversible et est son propre inverse.
   En effet, par définition du neutre, $e \star e = e \star e = e$

Proposition

Si $\star$ admet un neutre, alors ce neutre est unique.

Démonstration.

Soient e et e' deux neutres.
Alors $e \star e' = e$ car e' est une neutre
et $e \star e' = e'$ car e est un neutre.
donc $e = e'$. □

Proposition

On suppose la loi $\star$ associative, et admettant un neutre e.
*Si un élément est **inversible**, alors il a un **seul** inverse.*

Démonstration.

Soient y et y' deux inverses de $x \in E$.
Alors $y \star x = e$ et $x \star y' = e$.
Donc $y \star (x \star y') = y \star e = y$ et $(y \star x) \star y' = e \star y' = y'$, d'où $y = y'$. □

Remarque

On utilise souvent les notations **additives** et **multiplicatives**.

1. En notation **additive**, $\star$ est notée $+$
   - $x + x + \cdots + x$ ($n-$fois) se note nx.
   - Si x est inversible, son inverse se note $-x$. On l'appelle alors l'**opposé** de x.
   - On notera le neutre d'une telle structure 0 ou 0_E.
2. En notation **multiplicative**, $\star$ est en général notée par $\times$ (et ce symbole est même souvent omis)
   - $x \times x \times \cdots \times x$ ($n-$fois) se note x^n
   - Si x est inversible, son inverse se note x^{-1}. On l'appelle alors l'inverse de x.
   - On notera le neutre d'une telle structure 1 ou 1_E.

Pour éviter toute erreur, on essaiera au maximum de n'utiliser la notation additive que pour des lois qui ont les mêmes propriétés que la loi $+$ sur $\mathbb{R}$.

La notation $+$ est en général réservée à des lci commutatives et pour lesquelles les éléments sont tous inversibles.

Par exemple, noter $+$ une lci non commutative peut-être déroutant, ainsi que pour une lci pour laquelle tous les éléments ne sont pas inversibles.

La notation multiplicative est la plus couramment utilisée pour des lois associatives

Par exemple il est fréquent d'utiliser $\times$ même pour une lci non commutative et pour laquelle les éléments ne sont pas tous inversibles.

Attention

En général on aura $xy \neq yx$, et x^{-1} n'existera pas forcément !

Dans toute la suite, on adoptera la notation multiplicative, et on suppose que E a un neutre noté 1.

Proposition

On suppose la loi $\star$ associative. Soient $x, y, z \in E$.

1. *Simplification par un inversible : si x est inversible, alors*
$$x \star y = x \star z \Leftrightarrow y = z$$
2. *Inverse d'un produit : si x et y sont inversibles alors $x \star y$ l'est aussi et*
$$(x \star y)^{-1} = y^{-1} \star x^{-1}$$
3. *Puissances négatives : si x est inversible, on pose pour $n \in \mathbb{N}^*$, $x^{-n} = \left(x^{-1}\right)^n$. Alors $x^{-n} = (x^n)^{-1}$.*
4. *Inverse d'un inverse : si x est inversible, x^{-1} l'est aussi et $\left(x^{-1}\right)^{-1} = x$.*

Attention : l'inverse de $x \star y$ n'a aucune raison d'être $x^{-1} \star y^{-1}$.

Démonstration.

- On a $xy = xz \Leftrightarrow x^{-1}xy = x^{-1}xz \Leftrightarrow ey = ez \Leftrightarrow y = z$
- $(xy)(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = xex^{-1} = xx^{-1} = e$ et de même $(y^{-1}x^{-1})(xy) = y^{-1}(x^{-1}x)y = y^{-1}ey = y^{-1}xx^{-1} = e$ Donc $y^{-1}x^{-1}$ est bien l'inverse à gauche et à droite de xy..
- Par récurrence.
  Initialisation : Vrai si $n = 0$.
  Hérédité : Soit $n \in \mathbb{N}$, si on suppose vraie pour vrai pour n, alors $x^{n+1} \star x^{-n-1} = x^n \star x \star x^{-1} \star x^{-n} = x^n \star e \star x^{-n} = x^n \star x^{-n} = e$.
- Vrai par unicité de l'inverse.

□

Définition

Soit $(E, \star)$ un magma et F une partie de E.
On dit que F est une partie stable (de E par $\star$) si pour tous $x, y \in F, x \star y \in F$.

Example

$\{-1, 1\}$ est une partie stable de $(\mathbb{R}, \times)$, mais pas $\{-2, 2\}$.

Définition

*On appelle **groupe** tout magma associatif, ayant un neutre, et dont tout élément est inversible.*

*Si un groupe est **commutatif** (ce qui signifie en fait que sa loi est commutative), il est dit **abélien**.*

Par défaut on utilise la notation multiplicative pour un groupe, sauf pour les groupes abéliens pour lesquels on utilise la notation additive.

Example

1. $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}$ sont des groupes avec la loi $+$, mais pas avec la loi $\times$.
2. Pour $n \in \mathbb{N}^*$, pour $E = \mathbb{C}^n$, $E = \mathbb{R}^n$, $E = \mathbb{Q}^n$ ou $E = \mathbb{Z}^n$.
   On définit l'addition $+$ par

   $$(x_1, x_2, \ldots, x_n) + (y_1, y_2, \ldots, y_n) = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n)$$

   alors $(E, +)$ sont des groupes avec la loi $+$.
3. $\mathbb{C}^*, \mathbb{R}^*, \mathbb{Q}^*$, sont des groupes avec la loi $\times$.
4. $(\mathbb{N}, +)$ n'est pas un groupe..
   En effet 3 n'admet pas d'opposé dans $\mathbb{N}$
5. $(\mathbb{N}, \times)$ n'est pas un groupe.
   En effet 3 n'admet pas d'inverse dans $\mathbb{N}$

Définition

Soit X un ensemble non vide.

*On appelle **groupe des permutations de** X l'ensemble des bijections de X dans X muni de la loi de composition $\circ$.*

On le note $\mathscr{S}_X$.

Dans toute la suite, $(G, \star)$ est un groupe de neutre e. On adopte la notation multiplicative.

Définition

On appelle ***sous-groupe de*** $(G, \star)$ *tout ensemble* H *vérifiant les propriétés suivantes :*

1. $H \subset G$;
2. $e \in H$;
3. *Stabilité par produit :* $\forall x, y \in H, x \star y \in H$;
4. *Stabilité par passage à l'inverse :* $\forall x \in H$, *on a* $x^{-1} \in H$.

Example

Sont des sous-groupes :

1. $\{e\}$ et G dans $(G, \star)$.
2. $\mathbb{U}$ (ensemble des complexes de module 1) dans $(\mathbb{C}^*, \times)$.
3. $n\mathbb{Z}$ dans $(\mathbb{Z}, +)$.
4. $H = \{f \in \mathscr{S}_{\mathbb{R}} \mid f(0) = 0\}$ dans $(\mathscr{S}_{\mathbb{R}}, \circ)$.

Proposition

Un ensemble H est un ***sous groupe*** *de $(G, \star)$ si et seulement si H est un* ***sous-ensemble non vide de*** *G et pour tout $(x, y) \in H^2$, on a*

$$x^{-1} \star y \in H$$

Démonstration.

Montrons l'implication et sa réciproque :

1. "$\Rightarrow$" Supposons que H est un sous-groupe de G.Alors H contient e et n'est donc pas vide.
   De plus, soit $(x, y) \in H$.
   H étant stable par passage à l'inverse,
   on a alors $x^{-1} \in H$ et par stabilité par produit, on a donc $x^{-1} \star y \in H$.

Démonstration.

2. "$\Leftarrow$" Réciproquement, supposons que H est non vide et que pour tout $(x, y) \in H^2$, on a $x^{-1} \star y \in H$.
   Montrons que H possède les trois propriétés énumérées dans sa définition :
   1. H étant non vide, il possède au moins un élément x_0. On a alors $e = x_0^{-1} \star x_0 \in H$.
   2. Soit $x \in H$. On a alors $(x, e) \in H^2$, donc $x^{-1} \star e = x^{-1} \in H$.
   3. Soit $(x, y) \in H$. D'après ce qui précède, on a alors $x^{-1} \in H$, donc $(x^{-1}, y) \in H^2$, donc $x \star y = \left(x^{-1}\right)^{-1} \star y \in H$.

□

Remarque

On a aussi la propriété équivalente en remplaçant ci-dessus la condition $x^{-1} \star y \in H$ par $x \star y^{-1} \in H$.

Définition

Soit $(G, \star)$ un groupe et H, un sous-groupe de $(G, \star)$.
On peut définir sur H une loi appellée ***loi induite*** $\triangle$ *telle que*

$$\forall (x, y) \in H, x \triangle y = x \star y$$

Remarque

Par la suite, par soucis de simplification on notera la loi sur H : $\triangle$ avec le même symbole que la lci sur G : $\star$

Theorem

Un ***sous-groupe*** *muni de la loi induite du groupe est lui-même un* ***groupe***.

Démonstration.

Soit $(G, \star)$ un groupe de neutre e et H un sous-groupe de G.

1. Montrons qu'on peut restreindre $\star : G \times G \to G$ au départ à $H \times H$ et à l'arrivée à H.
   On a $H \times H \subset G \times G$, donc la restriction au départ est légitime, pour effectuer la restriction à l'arrivée, il suffit de montrer que pour tout $(x, y) \in H^2$, on a $x \star y \in H$, c'est-à-dire que H est stable par $\star$.
   Or H est un sous-groupe de G : la définition d'un sous-groupe assure cette stabilité.

Démonstration.

2. H muni de la loi induite par $\star$ est un magma associatif.
En effet $(G, \star)$ est un magma associatif, on a donc

$$\forall (x, y, z) \in G^3 \qquad (x \star y) \star z = x \star (y \star z)$$

Or $H \subset G$ donc

$$\forall (x, y, z) \in H^3 \qquad (x \star y) \star z = x \star (y \star z)$$

Donc la restriction de $\star$ à H est associative, d'où le résultat.

3. e est neutre pour la loi induite par $\star$ sur H. En effet, e est le neutre de $\star$, donc

$$\forall x \in G \qquad e \star x = x \star e = x$$

D'où le résultat.

Démonstration.

4. Tout élément de H admet un inverse pour la loi induite par $\star$.
   En effet tout élément x de H admet un inverse x^{-1} dans G pour la loi $\star$ et par stabilité de l'inverse sur le sous-groupe H, on a $x^{-1} \in H$.
   Donc tout élément de H admet un inverse dans H pour la loi induite par $\star$.
5. On déduit des points précédents que H muni de la loi induite par $\star$ est un groupe.

□

Remarque

La réciproque de ce théorème est également vraie (bien que moins utilisée) : si H est un sous-ensemble de G tel que, muni de la loi induite par celle de G, H soit un groupe, alors H est un sous-groupe de G.

Example

Si $n \in \mathbb{N}^*$, $\mathbb{U}_n$ est un sous-groupe de $(\mathbb{U}, \times)$, donc $(\mathbb{U}_n, \times)$ est un groupe.

Remarque

Il est plus facile de montrer qu'un ensemble est un sous-groupe que de montrer que c'est un groupe (pas besoin de redémontrer l'associativité, etc.).

Par exemple $(\mathbb{U}, \times)$ est un groupe, vu comme sous-groupe de $(\mathbb{C}^*, \times)$.

À chaque fois que l'on essaiera de montrer qu'un ensemble est muni d'une structure de groupe, on tentera de le voir comme un sous-groupe d'un groupe bien connu.

Morphismes de groupes

Définition

Soient $(G, \star)$ et $(G', *)$ deux groupes et $\varphi : G \to G'$.

1. *On dit que φ est un* ***morphisme*** *du groupe $(G, \star)$ dans le groupe $(G', *)$, si*

$$\forall x, y \in G, \qquad \varphi(x \star y) = \varphi(x) * \varphi(y).$$

2. *Tout morphisme d'un groupe dans lui-même est appelé* ***endomorphisme***.
3. *Tout morphisme de G dans G' qui est une bijection est appelé* ***isomorphisme*** *de G sur G'.*
   Dans ce cas on dit que G et G' sont ***isomorphes***.
   Un morphisme qui est à la fois un isomorphisme et un endomorphisme est appelé ***automorphisme***.

Example

1. $\begin{cases} (\mathbb{Z},+) & \to & (\mathbb{Z},+) \\ x & \mapsto & 2x \end{cases}$
est un morphisme, mais pas un isomorphisme.
2. $\begin{cases} (\mathbb{C}^*,\times) & \to & (\mathbb{R}^*,\times) \\ z & \mapsto & |z| \end{cases}$ est un morphisme, mais pas un isomorphisme.
3. $\begin{cases} (\mathbb{R},+) & \to & (\mathbb{C}^*,\times) \\ x & \mapsto & e^{ix} \end{cases}$
est un morphisme, mais pas un isomorphisme.
4. $\begin{cases} (\mathbb{R},+) & \to & (\mathbb{R}^{*+},\times) \\ x & \mapsto & e^{x} \end{cases}$ est un isomorphisme de réciproque ln, qui est aussi un isomorphisme.

Example

Etudions les applications suivantes

1. Si $n \in \mathbb{N}^*$,
$$\begin{array}{rccc} \varphi_n & : & (\mathbb{C}^*, \times) & \to & (\mathbb{C}^*, \times) \\ & & z & \mapsto & z^n \end{array}$$
2. Si $n \in \mathbb{N}^*$ et $a_1, \ldots, a_n \in \mathbb{K}^n$, l'application
$$\begin{array}{rccc} \varphi_n & : & (\mathbb{K}^n, +) & \to & (\mathbb{K}, +) \\ & & (x_1, \ldots, x_n) & \mapsto & a_1 x_1 + \cdots + a_n x_n \end{array}$$

Dans toute la suite, $(G, \star)$ et $(G', *)$ sont deux groupes de neutres e et e', on adopte une notation multiplicative, et $\varphi : G \to G'$ est un morphisme.

Theorem

Soit φ un morphisme de G sur G', on a, e et e' désignant les neutres de G et G' :

1. $\varphi(e) = e'$
2. $\forall x \in G,\ \varphi(x^{-1}) = (\varphi(x))^{-1}$.

Démonstration.

1. On a $\varphi(e) * \varphi(e) = \varphi(e \star e) = \varphi(e) = \varphi(e) * e'$, donc en simplifiant par $\varphi(e)$, on en déduit $\varphi(e) = e'$.
2. Soit $x \in G$. Alors $\varphi(x^{-1}) * \varphi(x) = \varphi(x^{-1} \star x) = \varphi(e) = e$.

□

Corollary

Sous les mêmes hypothèses, on a

$$\forall x \in G \qquad \forall k \in \mathbb{Z} \qquad \varphi(x^k) = \varphi(x)^k.$$

Démonstration.

- On démontre par récurrence :
  Soit $x \in G$.
  Initialisation : D'après le théorème précédent, on a

  $$\varphi(x^0) = \varphi(e) = e' = \varphi(x)^0.$$

  Hérédité : Soit $n \in \mathbb{N}$, on suppose $\varphi(x^n) = \varphi(x)^n$.
  On a alors $\varphi(x^{n+1}) = \varphi(x^n x) = \varphi(x^n)\varphi(x) = \varphi(x)^n\varphi(x) = \varphi(x)^{n+1}$
- D'après le théorème précédent, pour tout $n \in \mathbb{N}$,

  $$\varphi(x^{-n}) = \varphi(x^n)^{-1}$$

  d'où $\varphi(x^{-n}) = \varphi(x)^{-n}$. On en déduit le résultat.

Example

1. $\mathbb{C}^* \to \mathbb{R}^*, z \mapsto |z|$ est un morphisme de $(\mathbb{C}^*, \times)$ dans $(\mathbb{R}^*, \times)$, donc pour tout $z \in \mathbb{C}^*$, on a
$$\left|\frac{1}{z}\right| = \frac{1}{|z|}$$
2. exp est un morphisme de $(\mathbb{C}, +)$ dans $(\mathbb{C}^*, \times)$, donc pour tout $z \in \mathbb{C}$, $e^{-z} = \frac{1}{e^z}$.
3. ln est un morphisme de $(\mathbb{R}_+^*, \times)$ dans $(\mathbb{R}, +)$, donc pour tout $x \in \mathbb{R}_+^*$, on a $\ln\left(\frac{1}{x}\right) = -\ln(x)$.

Theorem

1. *La **composée** de deux morphismes de groupes est un morphisme de groupe.*
   Plus précisément, soit $(G_1, \star_1)$, $(G_2, \star_2)$ et $(G_3, \star_3)$ trois groupes, φ un morphisme de G_1 dans G_2 et φ un morphisme de G_2 dans G_3. Alors $\psi \circ \varphi$ est un morphisme de G_1 dans G_3.
2. *La fonction **réciproque** d'un isomorphisme (en tant qu'application bijective) est un isomorphisme.*
   Plus précisément, soit $(G_1, \star_1)$ et $(G_2, \star_2)$ deux groupes et φ un isomorphisme de G_1 sur G_2. Alors φ^{-1} est un isomorphisme de G_2 sur G_1.

Démonstration.

- Pour tout $(x, y) \in G_1^2$, $(\psi \circ \varphi)(xy) = \psi(\varphi(xy)) = \psi(\varphi(x)\varphi(y)) = \psi(\varphi(x))\psi(\varphi(y)) = (\psi \circ \varphi)(x)(\psi \circ \varphi)(y)$
- Pour tout $(x, y) \in G_2^2$,
  $\varphi(\varphi^{-1}(x)\varphi^{-1}(y)) = \varphi(\varphi^{-1}(x))\varphi(\varphi^{-1}(y)) = xy = \varphi(\varphi^{-1}(xy))$.
  On a donc en appliquant φ^{-1}, $\varphi^{-1}(x)\varphi^{-1}(y) = \varphi^{-1}(xy)$

Theorem

*L'**image** d'un sous-groupe par un morphisme de groupes est un sous-groupe.*

Démonstration.

Soient $(G, \star)$ et $(G', *)$ deux groupes de neutres respectifs e et e', et $\varphi : G \to G'$ un morphisme de groupes. Soit H un sous-groupe de G. Montrons que $\varphi(H)$ est un sous-groupe de G'.

1. On a évidemment $\varphi(H) \in G'$ et de plus $e \in H$ et $e' = \varphi(e) \in \varphi(H)$.
2. Soit $x', y' \in \varphi(H)$. Alors x' possède un antécédent $x \in H$ et y' un antécédent $y \in H$ par φ. On a alors successivement

$$\begin{aligned} x' * y'^{-1} &= \varphi(x) * \varphi(y)^{-1} && \text{par définition de} x \text{ et } y \\ &= \varphi(x) * \varphi(y^{-1}) && \text{car } \varphi \text{ est un morphisme} \\ &= \varphi(x \star y^{-1}) && \text{car } \varphi \text{ est un morphisme} \end{aligned}$$

Donc $x' * y'^{-1} \in \varphi(H)$ et finalement $\varphi(H)$ est donc un sous-groupe de G'.

Theorem

*L'**image réciproque** d'un sous-groupe par un morphisme est un sous-groupe.*

Démonstration.

Gardons les même notations que dans le premier point, et notons H' un sous-groupe de G'.

1. On a évidemment $\varphi^{-1}(H') \subset G$ et de plus $e' \in H'$ et $e' = \varphi(e) \in H'$ donc $e \in \varphi^{-1}(H')$.
2. Soit $x, y \in \varphi^{-1}(H')$.
   Alors $\varphi(x), \varphi(y) \in H'$
   donc $\varphi(x \star y^{-1}) = \varphi(x) * (\varphi(y))^{-1} \in H'$
   donc $x \star y^{-1} \in \varphi^{-1}(H')$.
   $\varphi^{-1}(H)$ est donc un sous-groupe de G.

□

Remarque

Lorsque l'on veut montrer qu'un ensemble est muni d'une structure de groupe, on commence toujours par essayer de l'identifier comme image réciproque (ou directe) d'un sous-groupe d'un groupe bien connu par un morphisme.

Définition

Soit $\varphi : G \to G'$ un morphisme de groupe.

1. *On appelle **noyau** de φ, noté $\mathrm{Ker}\,\varphi$, l'image réciproque de $\{e'\}$ par φ, autrement dit l'ensemble des antécédents de e' par φ*

$$\mathrm{Ker}\,\varphi = \{x \in G \mid \varphi(x) = e'\}.$$

2. *On appelle **image** de φ notée $\mathrm{Im}\varphi$, l'image directe de G par φ. Autrement dit*

$$\mathrm{Im}\varphi = \{\varphi(x) \mid x \in G\}.$$

Theorem

Les noyaux et les images sont des sous-groupes respectivement de G et G'.

Démonstration.

- $\{e'\}$ est un sous-groupe de G' et $\operatorname{Ker}\varphi$ est donc l'image réciproque d'un sous-groupe donc un sous-groupe.
- G est un sous-groupe de G donc son image par le morphisme φ est un sous-groupe de G'.

□

Démonstration directe.

Montrons que $\mathrm{Ker}\,\varphi$ est un sous-groupe de G :

1. On a $\mathrm{Ker}\,\varphi \subset G$ et de plus $\varphi(e) = e'$ donc $\mathrm{Ker}\,\varphi$ est un sous-ensemble non vide de G.
2. Soit $x, y \in \mathrm{Ker}\,\varphi$. Alors on a successivement

$$\begin{aligned} \varphi(x \star y^{-1}) &= \varphi(x) * \varphi(y)^{-1} \\ &= e' * e'^{-1} \\ &= e' \end{aligned}$$

Donc $x \star y^{-1} \in Ker\varphi$.Donc $\mathrm{Ker}\,\varphi$ est un sous-groupe de G.

□

Remarque

Lorsque l'on veut montrer qu'un ensemble est muni d'une structure de groupe, on commence toujours par essayer de l'identifier comme noyau ou image d'un morphisme.

Example

$\mathbb{U}$ est le noyau du morphisme « module », de $(\mathbb{C}^*, \times)$ dans $(\mathbb{R}^*, \times)$.

Theorem

φ surjectif si et seulement si $\mathrm{Im}\varphi = G'$.

Démonstration.

Définition ! □

Theorem

φ injectif si et seulement si $\operatorname{Ker}\varphi = \{e\}$.

Démonstration.

On montre l'implication et sa réciproque :
"$\Rightarrow$" Supposons φ injectif. On sait que $\varphi(e) = e'$. Donc e est un antécédent de e' et comme φ est injective, c'est le seul. Donc $\operatorname{Ker}\varphi = \{e\}$.
"$\Leftarrow$" Réciproquement, supposons $\operatorname{Ker}\varphi = \{e\}$ et montrons que φ est injectif.
Soit $(x, y) \in G^2$ vérifiant $\varphi(x) = \varphi(y)$. Alors on a successivement

$$\begin{aligned} \varphi(x \star y^{-1}) &= \varphi(x) * \varphi(y)^{-1} \text{ car } \varphi \text{ est un morphisme} \\ &= \varphi(x) * \varphi(x)^{-1} \\ &= e' \end{aligned}$$

Donc $x \star y^{-1} \in Ker\varphi$, donc $x \star y^{-1} = e$, donc $x = y$.

□

Remarque

Pour montrer qu'un morphisme est injectif, on utilisera TOUJOURS le noyau et JAMAIS (ou presque) la méthode classique pour des fonctions quelconques : c'est beaucoup plus rapide !