Les structures Algébriques

Lois de composition internes

Introduction

L'addition de deux entiers naturels est un entier naturel, on dit que l'addition est une loi de composition interne dans N. L'addition dans N est une fonction à deux variables dans N, c'est-à-dire que l'ensemble de départ de l'additon dans N est le produit cartésien N*N, son en semble d'arrivée est N. Symboliquement $+: \mathrm{N} \times \mathrm{N} \to \mathrm{N}, (x, y) \to x + y$

La soustraction de deux entiers relatifs est un entier relatif ; on dit que la soustraction dans Z est une loi de composition interne dans Z. Symboliquement $-: Z \times Z \to Z,\ (x, y) \to x - y$

Par contre la soustraction dans N n'est pas une loi de composition interne, car $1 - 2 = -1$ et -1 n'appartient pas a N

La division dans Z n'est pas une loi de composition interne , car par exemple $2 \div 3$ n'appartient pas à Z ; elle est par contre interne dans Q.

Si on considère la loi *f* suivante $f(x, y) = 2x - y$, alors cette loi est interne dans R, Q, Z .

Mais elle n'est pas interne dans N car par exemple $f(1,3) = -1$ et -1 n'est pas dans N.

Quand on considère une loi de composition f, on écrit xfy au lieu de $f(x, y)$. Dans l'exemple précédant on a $xfy = 2x - y$

Remarquons aussi que dans les opérations élémentaires on écrit $x + y$ au lieu de $+(x, y)$, $x \times y$ au lieu de $\times\ (x, y)$ etc…

Si on considère la loi $xfy = |x - y|$, alors cette loi est interne dans N, Z, Q, et R

On peut considérer la loi de la multiplication dans l'ensemble $\{-1,1\}$, elle n'est interne dans $\{-1,1\}$, mais si on considère l'addition alors l'addition n'est pas interne dans $\{-1,1\}$, car $-1 + 1 = 0$ et 0 n'appartient pas à $\{-1,1\}$.

Généreleme nt pour avoir une loi de composition interne dans un ensemble, il faudrait que toutes les compositions possibles soit dans cet ensemble.

Définition :

Soit E un ensemble et $*$ (lire étoile) une application de $E \times E \to E$

On dit que $*$ est une loi de composition interne dans E si et seulement si on a : $\forall x, y \in E: x * y \in E$.

Et la loi ne sera pas interne si et seulement si $\exists x, y \in E: x * y \notin E$

Exemple 1

Dans Z on définit une loi par $a * b = ab + 2a + 3b$

Calculer $1 * 2,\ \ 2 * 1,\ \ 0 * (-1),\ \ -1 * 0,\ \ \ 1 * (1 * 1),\ \ \ (1 * 1) * 1,\ \ (2 * 3) * (-2),\ \ 2 * \big(3 * (-2)\big)$

On a :

$1 * 2 = 1.2 + 2.1 + 3.2 = 2 + 2 + 6 = 8 \qquad 0 * (-1) = 0.(-1) + 2.0 + 3.(-1) = -3$

$2 * 1 = 2.1 + 2.1 + 3.2 = 2 + 2 + 6 = 8 \qquad -1 * 0 = -1.0 + 2.(-1) + 3.0 = -2$

$1 * (1 * 1) = 1 * (1.1 + 2.1 + 3.1) = 1 * 6 = 1.6 + 2.1 + 3.6 = 26$

$(1 * 1) * 1 = 6 * 1 = 6.1 + 2.6 + 3.1 = 15$

$(2 * 3) * (-2) = (2.3 + 2.2 + 3.3) * (-2) = 16 * (-2) = 16.(-2) + 2.16 + 3.(-2) = -6$

$2 * \big(3 * (-2)\big) = 2 * (2.3 + 2.3 + 3.(-2) = 2 * 6 = 2.6 + 2.2 + 3.6 = 12 + 4 + 18 = 34$

Exemple 2

Dans N si on définit la loi $*$ par $a * b = a + b - 1$ alors cette loi n'est pas interne dans N car $0 * 0 = 0 + 0 - 1 = -1$ et -1 n'est pas dans N ; mais si on la définit dans Z, Q, ou R elle devient interne

Propriétés des lois de composition interne

On sait tous que $a + b = b + a$, que $a \times b = b \times a$, mais que $4 \div 2 \neq 2 \div 4$; $2 - 3 \neq 3 - 2$

On dit que l'addition et la multiplication sont commutatives, mais que la division et la soustraction ne le sont pas.

La loi définit dans l'exemple 1 dans le paragraphe définition précédent n'est pas commutative car on a vu que par exemple $-1 * 0 \neq 0 * (-1)$.

D'une façon générale :

Définition

Soit E un ensemble et $*$ une loi de composition interne dans E

On dit $*$ est commutative si et seulement si

$$\forall a, b \in E : a * b = b * a$$

Et elle ne sera pas commutative si et seulement si :

$$\exists a, b \in E : a * b \neq b * a$$

Exemple 3 :

Dans N la loi $*$ définit par $a * b = a + b + 2$ est une loi de composition interne commutative en effet : $a * b = a + b + 2 \overbrace{\underbrace{=}_{commutative}}^{+est} = b + a + 2 = b * a$

Exemple 4 :

Dans R la loi $*$ définit par $x * y = x + 2y$ n'est pas commutative, en effet :

$1 * 3 = 1 + 2 \times 3 = 7$ mais $3 * 1 = 3 + 2 \times 1 = 5$ donc $1 * 3 \neq 3 * 1$

Associativité :

Les lois associatives sont les lois qui ressemblent à l'addition et la multiplication dans leur manière de compter plusieurs nombres , pour additionner trois nombres donnés a, b, c, on addtionne deux d'entre eux , $a + b$, et on ajoute le résultat au troisième $(a + b) + c$, ou bien ajoute $'a'$ au résultat de l'addition de b à c, c'eseet à dire $a + (b + c)$. Autrement dit $(a + b) + c = a + (b + c)$

On a la même chose pour la multiplication $a \times (b \times c) = (a \times b) \times c$

D'une manière générale

Définition

Une loi de composition interne $*$ dans un ensemble E, est associative si et seulement si :

$$\forall a, b, c \in E : (a * b) * c = a * (b * c)$$

Elle ne sera pas associative si et seulement si :

$$\exists a, b, c \in E : (a * b) * c \neq a * (b * c)$$

Exemple 5:

Dans R la loi de composition interne $a * b = 2a + b$ n'est pas associative en effet :

$$1 * (1 * 3) = 1 * (2 \times 1 + 3) = 1 * 5 = 2 \times 1 + 5 = 7$$
$$(1 * 1) * 3 = (2 \times 1 + 1) * 3 = 3 * 3 = 2 \times 3 + 3 = 9$$

Ainsi $1 * (1 * 3) \neq (1 * 1) * 3$ et donc cette loi n'est pas associative.

Exemple 6 :

On définit dans Z la loi $a \circ b = a + b + ab$

Cette loi est associative en effet :

$(a \circ b) \circ c = (a + b + ab) \circ c = a + b + ab + c + (a + b + ab).c$

$$= a + b + ab + c + ac + bc + abc \overbrace{=}^{\substack{+ est \\ commut}} a + b + c + ab + ac + bc + abc$$

$a \circ (b \circ c) = a \circ (b + c + bc) = a + b + c + bc + a(b + c + bc)$

$$= a + b + c + bc + ab + ac + abc \overbrace{=}^{\substack{+ est \\ commut}} a + b + c + ab + ac + bc + abc$$

On a bien pour tous a, b, c dans R : $(a \circ b) \circ c = a \circ (b \circ c)$

Elément neutre :

On sait que 0 est l'élément neutre pour l'addition des nombres, pour tout nombre x,
$x + 0 = 0 + x = x$. On dit que 0 est élément neutre à droite et à gauche pour l'addition.
On sait aussi que 1 est l'élément neutre pour la multiplication, pour tout nombre x,
$1 \times x = x \times 1 = x$. Le nombre 1 est neutre à droite et à gauche pour la multiplication.
Si on considère la loi de composition définit dans Z par $a * b = a + b + 2$, on peut voir que -2 est l'élément neutre pour cette loi $*$, en effet
$a * (-2) = a + (-2) + 2 = a$, et $-2 * a = a * (-2) = a$ car la loi $*$ est commutative
Si on considère dans Z la loi $a \circ b = a + b + ab$, alors 0 est l'élément neutre pour cette loi, en effet :
$a \circ 0 = a + 0 + a.0 = a$ et $0 \circ a = a \circ 0 = 0$ car la loi $\circ$ est commutative.
Pour la soustraction dans R par exemple, pour tout réel a on a : $a - 0 = a$, mais $0 - 1 = -1 \neq 1$, donc 0 est élément neutre à droite mais pas à gauche pour la soustraction dans R. donc la soustration dans R n'admet pas d'élément neutre.

Définition :

Soit E un ensemble et $*$ une loi de composition interne dans E.
On dit que la loi admet un élément neutre s'il existe un élément e dans E tel que pour tout a dans E :

$$a * e = a \text{ et } e * a = a$$

Si la loi est commutative il suffit de vérifier l'une des deux inégalités.

Exemple 8

Dans R la loi $a \odot b = a + 2b$, admet 0 comme élément neutre à droite mais n'admet aucun élément neutre à gauche, en effet $a \odot 0 = a + 2.0 = a$, mais $0 \odot 1 = 0 + 2.1 = 2 \neq 1$; de plus pour tout élément e dans R autre que 0 on a : $e \odot e = e + 2.e = 3e \neq e$, donc quel que soit l'élément e non nul, e n'est pas neutre à gauche.

Exemple 9

L'addition dans N^* n'admet pas d'élément neutre, car 0 n'appartient pas à N^*.

Théorème 1

L'élément neutre quand il existe est unique

Preuve :

Supposons qu'une loi $*$ admette deux éléments neutre e et e':
puisque e est élément neutre alors $e * e' = e' * e = e'$
et puisque e' est neutre aussi alors $e * e' = e' * e = e$
Donc $e = e$'.
Ainsi une loi de composition ne peut avoir plus d'un élément neutre

Elément symétrique :

Le symétrique d'un nombre a pour l'addition est le nombre $(-a)$, on a $a + (-a) = (-a) + a = 0$, 0 étant l'élément neutre pour l'addition des nombres.
Le symétrique d'un nombre non nul a pour la multiplication est le nombre $1/a$, on a :

$a \times \frac{1}{a} = \frac{1}{a} \times a = 1$; 1 étant l'élément neutre pour la multiplication des nombres.

Dans l'exmple de la loi $a * b = a + b + 2$, définit dans Z, on a vu que (-2) est l'élément neutre et on peut voir que le nombre relatif qu'il faut composer avec a pour avoir (-2) est le nombre $-4 - a$, en effet :

$a * (-4 - a) = a + (-4 - a) + 2 = a - a - 4 + 2 = -2$ et $(-4 - a) * a = a * (-4 - a) = -2$

Donc on ava dire que $(-4 - a)$ est le symétrique de a pour la loi $*$

Définition

Soit E un ensemble et $*$ une loi de composition interne dans E, admettant un élément neutre e.

Soit a un élément de E

On dit que a admet un symétrique, que l'on note a^{-1}, si et seulement si :

$$a * a^{-1} = e \text{ et } a^{-1} * a = e$$

Si la loi est commutative, il suffit de vérifier l'une des deux égalités.

Exemple10

0 n'a pas de symétrique pour la multiplication dans R, car pour tout x dans R, on a $0 \times x = 0 \neq 1$,

Exemple 11

On considère dans Q la loi de composition interne $a * b = a + b + ab$

On a vu précédemment que 0 est l'élément neutre pour cette loi, et que cette loi est commutative.

Voyons quels sont les éléments qui admettent un symétrique dans Q :

a^{-1} est symétrique de a dans Z veut dire que $a * a^{-1} = 0$ et $a^{-1} * a = 0$, mais comme la loi est commutative, une des deux égalités suffit, on a :

$$a * a^{-1} = 0 \Leftrightarrow a + a^{-1} + aa^{-1} = 0 \Leftrightarrow a^{-1}(1 + a) = -a$$

Si $a \neq -1$ alors $a^{-1} = \frac{a}{1+a}$

Si $a = -1$, alors $a^{-1}\big(1 + (-1)\big) = 1$ ou bien $0 = -1$, ce qui est faux et que donc -1 n'a pas de symétrique.

Donc tous les éléments de Q possède un symétrique pour la loi en question sauf -1.

Exemple 12

On définit dans l'ensemble $\wp(E)$ des parties de E, la loi $A \star B = A \vartriangle B$, ou A, B sont des partie de E, et $A \vartriangle B$ est la différence symétrique de A et B.

Cette loi est interne dans $\wp(E)$ car $A \vartriangle B$ est une partie de $\wp(E)$.

Elle est commutative, car $A \star B = A \vartriangle B = (A - B) \cup (B - A) = (B - A) \cup (A - B) = B \vartriangle A$.

Elle est associative(à faire en exercice TD)

Elle possède un élément neutre, c'est $\emptyset$, en effet : $\emptyset \vartriangle A = (\emptyset - A) \cup (A - \emptyset)$

Or $A - \emptyset = \{x \in E : x \in A \; et \; x \notin \emptyset\}$ et comme $x \notin \emptyset$ est toujours vraie, alors [$x \in A \; et \; x \notin \emptyset$] équivat à $x \in A$ donc $A - \emptyset = A$, ceci d'une part ;

D'autre part $\emptyset - A = \{x \in E : x \in \emptyset \; et \; x \notin A\}$ et comme la proposition « pour tout $x \in E$ $x \in \emptyset$ » eset fausse donc $\emptyset - A = \emptyset$

Donc $\emptyset \vartriangle A = (\emptyset - A) \cup (A - \emptyset) = A$ et comme la loi est commutative on a aussi $A \vartriangle \emptyset = A$

Donc $\emptyset$ est bien un élément neutre pour la loi en question.

Voyons quels sont les éléments qui admettent un symétrique :

Pour toute partie A de E on a : $A \vartriangle A = (A - A) \cup (A - A)$, or $A - A = \emptyset$ donc $A \vartriangle A = \emptyset$, tout élément A de $\wp(E)$ est son propre symétrique.

Théorème 2

Pour une loi de composition interne $\star$, associative et possédant un élément neutre e, le symétrique d'un élément , s'il existe, est unique.

Preuve

Soit a un élément de E et e l'élément neutre. Supposons que a admette deux éléments symétriques a' et a''; on a :

$a \star a' = e \Longrightarrow a'' \star (a \star a') \overset{symtrie}{=} a'' \star e \overset{e\ est\ neutre}{=} a''$

On a aussi $a'' \star (a \star a') \overset{associativité}{=} (a'' \star a) \star a' = e \star a' = a'$

Ainsi $a' = a''$ ce qui veut dire que le symétrique s'il existe est unique.

Théorème 3

Si a et b admettent un symétrique alors $a * b$ admet un symétrique et $(a * b)^{-1} = b^{-1} * a^{-1}$

Preuve

$(a * b) * (b^{-1} * a^{-1}) \overset{associative}{=} a * (b * b^{-1}) * a^{-1} \overset{sym}{=} a * e * a^{-1} \overset{e\ neutre}{=} a * a^{-1} = e$

$(b^{-1} * a^{-1}) * (a * b) = e$ pour les mêmes raisons.

Structure de groupe

Définition :

Un groupe est un couple $(E,\star)$ composé d'un ensemble E et d'une loi de composition interne $\star$, commutative, possédant un élément neutre , et pour laquelle tout élément de l'ensemble E admet un élément symétrique dans cet ensemble.

Si de plus la loi est commutative, on dit que le groupe est commutatif, ou que le groupe est abélien.

Exemple 13

Tous les objets mathématiques suivants sont des groupes commutatifs.

$(R,+)$; $(Z,+)$; $(Q,+)$; $(C,+)$.

$(R^*,\times)$; $(Q^*,\times)$; $(Z^*,\times)$; $(C^*,\times)$

Exemple 14

On a vu que la loi $a * b = a + b + 2$ définit dans Z, est une loi de composition interne, associative, possédant -2 comme élément neutre, et que tout entier relatif a possède pour symétrique $(-4 - a)$.

Donc $(Z,*)$ est un groupe. La loi est de plus commutative, donc le groupe est commutatif aussi.

La loi $*$ définit dans Q par $a * b = a + b + ab$ est une loi associative, possédant 0 comme élément neutre, et que tout rationnel a différent de -1 possède pour symétrique $\frac{a}{1+a}$, on a vu que -1 n'admet pas de symétrique, donc $(Q,*)$ n'est pas un groupe, mais $(Q - \{-1\},*)$ est un groupe et il est de plus commutatif.

Exemple 15

Si on considère l'ensemble U des racines cubique de l'unité, c'est-à-dire les solutions dans C de l'équation $z^3 = 1$, et si on munit U de la multiplication des nombres complexes, alors $(U,\times)$ devient un groupe, en effet calculons les racines de l'équation :

Si $z = [r;\theta]$ alors $z^3 = [r^3;3\theta]$ ceci d'une part ; d'autre par $1 = [1;0]$ donc $[r^3;3\theta] = [1;0]$ d'où $r^3 = 1$ et $3\theta = 0 + 2k\pi$ d'où $r = 1$ et $\theta = \frac{2k\pi}{3}, k = 0;1;2$

Les solutions possibles sont $z_0 = [1,0] = 1$; $z_1 = \left[1;\frac{2\pi}{3}\right] = e^{\frac{2\pi}{3}i}$; $z_2 = \left[1;\frac{4\pi}{3}\right] = e^{\frac{4\pi}{3}i}$

Donc $U = \{1, e^{\frac{2\pi}{3}i}, e^{\frac{4\pi}{3}i}\}$

La multiplication est interne dans U :

$1 \times z_1 = z_1 \in U$; $1 \times z_2 = z_2 \in U$; $z_1 \times z_2 = e^{\frac{6\pi}{3}i} = e^{2i\pi} = 1 \in U$

La multiplication dans C est associative, l'élément neutre est 1 ; elle est aussi commutative.
Remarquons que $1 \times 1 = 1$ donc 1 est son propre symétrique.
Et que $z_1 \times z_2 = 1$ donc le symétrique de z_1 est z_2 est inversement.
Donc la multiplication dans U est interne dans U, elle admet pour élément neutre 1, elle est associative, tout élément de U admet un symétrique dans U,
donc $(U,\times)$ est bien un groupe et il et commutatif. Nous avons dans cet exemple un exemple de groupe fini à trois éléments
Si on considère l'ensemble des racines n^{ième} de l'unité, muni de la multiplication des nombres complexes, alors on obtient un groupe fini à n éléments.

Exemple 16

On définit dans R^2 une addition par $(x,y)+(x',y')=(x+x',y+y')$
Alors $(R^2,+)$ est un groupe commutatif, en effet $(x+x',y+y') \in R^2$ donc la l'addition est interne.
La loi est commutative : $(x,y)+(x',y')=(x+x',y+y')=(y+y',x+x')=(y,y')+(x,x')$
(0,0) est l'élément neutre : $(x,y)+(0,0)=(x+0,y+0)=(x,y)$
Le symétrique de (x,y) est $(-x,-y)$: $(x,y)+(-x,-y)=\big(x+(-x),y+(-y)\big)=(0,0)$

Théorème 4

$(R^n,+)$ est un groupe commutatif.

Preuve

C'est une répétition des arguments de l'exemple précédent.

Notions d'homomorphismes et d'isomorphismes

Soit $(G,\star)$ et $(H,\circ)$ deux groupes, et soit $f:(G,\star) \longrightarrow (H,\circ)$

Définition

On dit que f est un homomorphisme de groupe si et seulement si

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

Si de plus f est une bijection alors on dit que f est un isomorphisme de groupe

Exemple 17

$exp:(R,+) \longrightarrow (R_+^*,\times)$, $x \longmapsto e^x$
$(R,+)$ est bien un groupe, de meme pour $(R_+^*,\times)$
On a $exp(x+y)=e^{x+y}=e^x \times e^y = exp(x)\times exp(y)$
Donc la fonction exponentielle est un homomorphisme de groupe.
Remarquons que la fonction exponentielle est une bijection de R dans R_+^*, donc exp est un isomorphisme de groupe ; elle possède donc une fonction réciproque connue, c'est la fonction logarithme népérien $Ln: R_+^* \longrightarrow R$, et on peut voir que Ln est aussi un isomorphisme de groupe, en effet $Ln(ab)=Lna+Lnb$.

Théorème 5

Supposons que $f:(G,\star) \longrightarrow (H,\circ)$ soit homomorphisme , soient e_G et e_H les éléments neutres respectifs des deux groupes, on a :

1. $f(e_G)=e_H$
2. Si a^{-1} est le symétrique de a dans G, alors $f(a^{-1})$ est le symétrique de $f(a)$ dans H ; autrement dit $[f(a)]^{-1}=f(a^{-1})$

Démonstration

1. On a $e_G \star e_G = e_G$ donc $f(e_G \star e_G)=f(e_G)$ et comme f et un homomorphisme alors $f(e_G)\circ f(e_G)=f(e_G)$,
   On compose par le symétrique de $f(e_G)$ des deux cotés pour aboutir à $f(e_G)=e_H$.

2. $f(a^{-1}) \circ f(a) \underbrace{=}_{homom}^{f\ est} f(a^{-1} \star a) \overset{a'sym\ de\ a}{=} f(e_G) \overset{1.}{=} e_H$

Théorème 6

Si f: $(G,\star) \longrightarrow (H,\circ)$ est un isomorphisme alors f^{-1}: $(H,\circ) \longrightarrow (G,\star)$ est un isomorphisme aussi.

Preuve

f^{-1} étant bijectif, il reste à prouver que f^{-1} est un homomorphisme, c'est-à-dire pour tout z, t dans H on a $f^{-1}(z \circ t) = f^{-1}(z) \star f^{-1}(t)$:

Pour tous z, t dans H , il existe x, y dans G tel que $z = f(x)$ et $t = f(y)$ car f est une bijection, on a ainsi :

$f^{-1}(z \circ t) = f^{-1}[f(x) \circ f(y)] = f^{-1}[f(x \star y)] = (f^{-1} \circ f)(x \star y) = x \star y$

Mais $z = f(x)$ et $t = f(y)$ et f bijective alors $x = f^{-1}(z)$ et $y = f^{-1}(t)$

Donc $x \star y = f^{-1}(z) \star f^{-1}(t)$ et ainsi $f^{-1}(z \circ t) = f^{-1}(z) \star f^{-1}(t)$.

Sous-groupes

$(R, +)$ est un groupe, Z est inclus dans R, or $(Z, +)$ est aussi un groupe. On dit alors que $(Z, +)$ est un sous-groupe de $(R, +)$.

$(Q, +)$ est aussi un sous-groupe de $(R, +)$.

$(N, +)$ n'est pas un sous-groupe de $(Q, +)$

$(R_+^*, \times)$ est un sous-groupe de $(R^*, \times)$

Définition

Soit $(G,\star)$ un groupe et H une partie de G.

On dit que $(H,*)$ est un sous-grope de $(G,\star)$ si et seulement si $(H,*)$ est un groupe.

Exemple 18

Soit $(G,\star)$ un groupe et e son élément neutre ; $(\{e\},*)$ est le plus petit sous-groupe de G, en effet la loi reste associative dans $\{e\}$, e est dans $\{e\}$, et e est son propre symétrique. De plus tout sous-groupe contient nécessairement l'élément neutre donc il contient l'ensemble {e} ; ainsi $\{e\}$ est le plus petit sous-groupe de G.

Théorème 7

Soit $(G,\star)$ un groupe et H une partei de G

H est un sous-groupe de G si et seulement si :

1. Pour tous x, y dans H , $x * y \in H$
2. Pour tout x dans H , $x^{-1} \in H$

Preuve

La première condition signifie que la loi est interne dans H

La seconde affirme que tout élément x de$H$ admet un symétrique x^{-1} dans H, et comme la loi est interne dans H alors $x * x^{-1}$ est aussi dans H , or $x * x^{-1} = e$ donc $\underline{e \in H}$.

L'associativité est vraie dans H car elle est vraie pour n'importe quel élément de G, et H est dans G.

Théorème 8

L'intersection de deux sous-groupes d'un même groupe est aussi un sous-groupe.

Preuve

Soient H et K deux sous-groupe d'un groupe G et soient x, y deux éléments de $H \cap K$

1. $(x, y \in H \cap K) \Longrightarrow (x, y \in H$ et $x, y \in K)$ or H et K sont deux sous-groupes de G donc ils vérifient la condition 1. du théorème 7, donc $x * y \in H$ et $x * y \in K$ donc $x * y \in H \cap K$.

2. Pour tout $x \in H \cap K$, $x \in H$ et $x \in K$ or H et K sont deux sous-groupes de G, donc il vérifient la conditions 2., donc $x^{-1} \in H$ et $x^{-1} \in K$, c'est-à-dire $x^{-1} \in H \cap K$.

Ainsi $H \cap K$ vérifie les deux conditions du théorème7, donc c'est bien un sous-groupe de G.

Définition

Soit $f: (E,*) \longrightarrow (F,\circ)$ un homomorphisme de groupe. On appelle noyau de f et on le note $Kerf$ l'ensemble $Kerf = \{x \in E: f(x) = e_F\} = f^{-1}(e_F)$.

On appelle image et on le note Imf , l'ensemble $f(E) = \{y \in F, \exists x \in E: y = f(x)\}$

Remarque :

Théorème

Soit $f: (E,*) \longrightarrow (F,\circ)$ un homomorphisme de groupe. Soit e_F l'élément neutre de F. On a :

1. $f^{-1}(\{e_F\})$ est un sous-groupe de G
2. $f(E)$ est un sous-groupe de F.

Preuve

1. Soient x, y dans $f^{-1}(\{e_F\})$, alors $f(x) = f(y) = e_F$
   - $f(x * y) \overset{f\ hom}{=} f(x) \circ f(y) = e_F \circ e_F = e_F$ donc $x * y \in f^{-1}(\{e_F\}$.
   - $f(x^{-1}) \overset{thm\ 5.2}{=} [f(x)]^{-1} = e_F^{-1} = e_F$ donc $x^{-1} \in f^{-1}(\{e_F\}$

   Donc (thm7) $f^{-1}(\{e_F\})$ est un sous-groupe de E
2. Soient x, y dans $f(E)$, il existe alors a, b dans E tels que $x = f(a)$ et $y = f(b)$
   - $x * y = f(a) \circ f(b) \overset{f\ hom}{=} f(a * b)$ or $f(a * b) \in f(E)$ donc $x * y \in f(E)$.
   - $x = f(a) \overset{thm\ 5.2}{\Longrightarrow} x^{-1} = [f(a)]^{-1} = f(a^{-1}) \Longrightarrow x^{-1} \in f(E)$

   Donc (thm7) $f(E)$ est bine un sous-groupe de F.

Exemple 18

$f: (R^*,\times) \longrightarrow (R^*,\times), \qquad f(x) = |x|$

Calculons $Kerf$:

$(x \in Kerf) \Leftrightarrow [f(x) = 1] \Leftrightarrow |x| = 1 \Leftrightarrow (x = 1$ ou $x = -1)$ donc $Kerf = \{-1,1\}$

Calculons Imf

$y \in Imf \Leftrightarrow \exists x \in R^*: y = f(x)\} \Leftrightarrow (\exists x \in R^*: y = |x|)$, donc $x > 0$ donc $Imf \subset R_+^*$

Réciproquement si $x > 0$ alors $x = |x| = f(x)$ donc $x \in Imf$, c'est-à-dire $R_+^* \subset Imf$.

Ainsi $Imf = R_+^*$.

Exercice

$f: (R^2,+) \longrightarrow (R,+), f(x,y) = y - 2x$

1. Montrer que f est un homomorphisme de groupe
2. Déterminer $Kerf$ et Imf.