

Structures algébriques(partie2)

Groupe anneau corps

I) Groupes .

1) Définition : Soit G un ensemble non vide muni d'une loi de composition interne (notée *).

$(G, *)$ est un groupe si et seulement si

- 1) * est associative,
- 2) * possède un élément neutre dans G
- 3) tout élément de G possède un symétrique pour * dans G.

Si de plus, * est commutative, le groupe $(G, *)$ est dit commutatif ou abélien.

2) Exemples

1) $(\mathbb{Z}; +)$; $(\mathbb{Q}; +)$; $(\mathbb{R}; +)$; $(\mathbb{C}; +)$; $(\mathbb{Q}^*; \times)$;

$(\mathbb{R}^*; \times)$; $(\mathbb{C}^*; \times)$ sont des groupes commutatifs

• $(\mathbb{C}; \times)$ n'est pas un groupe car 0 n'a pas d'inverse dans \mathbb{C} (pour \times).

• $(\mathbb{Z}; \times)$ et $(\mathbb{N}; +)$ ne sont pas des groupes car 2 n'a pas de symétrique

• $(V_2; +)$ et $(V_3; +)$ sont deux groupes commutatifs

• $(P(E); \cap)$ n'est pas un groupe car une partie $A \neq E$ n'admet pas de symétrique

• $(P(E); \cup)$ n'est pas un groupe car une partie $A \neq \emptyset$ n'admet pas de symétrique

• $(F(\mathbb{R}; \mathbb{R}); +)$; $(\mathbb{R}_n[X]; +)$ sont des groupes commutatifs

• $(M_2(\mathbb{R}); +)$ et $(M_3(\mathbb{R}); +)$ sont des groupes non commutatifs

$$\text{Ex : } A = \begin{pmatrix} 1 & 3 \\ 2 & 0 \end{pmatrix} \text{ et } B = \begin{pmatrix} 0 & 2 \\ 3 & 1 \end{pmatrix}$$

$$A \times B = \begin{pmatrix} 1 & 3 \\ 2 & 0 \end{pmatrix} \times \begin{pmatrix} 0 & 2 \\ 3 & 1 \end{pmatrix} = \begin{pmatrix} 9 & 5 \\ 0 & 4 \end{pmatrix}$$

$$B \times A = \begin{pmatrix} 0 & 2 \\ 3 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & 3 \\ 2 & 0 \end{pmatrix} = \begin{pmatrix} 4 & 0 \\ 5 & 9 \end{pmatrix}$$

Donc on a : $A \times B \neq B \times A$

• L'ensemble des translations $(T_r; \circ)$ et l'ensemble des rotations de même centre O $(R_O; \circ)$ sont des groupes commutatifs

L'ensemble des transformations du plan : $(T; \circ)$ est un groupe

Remarque : soit : $(G; *)$ un groupe

1) on utilisant une notation additive on dit que : $(G; +)$ un groupe additif

$$a)(a+b)+c=b+(a+c)$$

b) on note 0 l'élément neutre

c) le symétrique de a appelé opposé de a on le note $-a$ dans ce cas on pose : $a+(-a)=2a$

et $\underbrace{a+a+\dots+a}_{n \text{ fois}} = na$ avec la convention :

$$\begin{cases} 0a = 0 \\ 1a = a \\ n(-a) = -na \end{cases} \quad \text{Et on vérifie alors les relations}$$

suivantes : $na + ma = (n+m)a$ et

$$n \times (ma) = (n \times m)a = nma \quad \forall (n, m) \in \mathbb{Z}^2$$

2) on utilisant une notation multiplicative on dit que : $(G; \times)$ un groupe multiplicative

a) $(a \times b) \times c = b \times (a \times c)$

b) on note 1 l'élément neutre

c) le symétrique de a on le note a^{-1} (l'inverse)

d) ce cas on pose : $a \times a = a^2$ et $\underbrace{a \times a \times \dots \times a}_{n \text{ fois}} = a^n$

avec la convention :
$$\begin{cases} a^0 = 1 \\ a^1 = a \\ a^{-n} = (a^{-1})^n \end{cases}$$
 Et on vérifie

alors les relations suivantes : $a^n \times a^m = a^{n+m}$ et

$(a^n)^m = a^{n \times m} \quad \forall (n; m) \in \mathbb{Z}^2$

$(a \times b)^n = a^n \times b^n$ si le groupe est commutatif

$(a \times b)^n \neq a^n \times b^n$ si le groupe est non commutatif

(Dans la pratique on pourra supprimer le symbole \times ou on le remplaçant par un point)

Exemple : on pose $I =]-\frac{\pi}{2}; \frac{\pi}{2}[$ et $\forall (x; y) \in I^2$

On muni I de la loi de composition définie par :

$x * y = \arctan(-1 + \tan x + \tan y)$

Montrer que $(I; *)$ est un groupe commutatif

Solution : 1) soit $(x; y) \in I^2$

$x * y = \arctan(-1 + \tan x + \tan y) = \arctan(-1 + \tan y + \tan x)$

Donc $x * y = y * x$ et par suite $*$ est commutatif

2) soit $(x; y; z) \in I^3$

$(x * y) * z = (\arctan(-1 + \tan x + \tan y)) * z$
 $= \arctan(-1 + \tan((\arctan(-1 + \tan x + \tan y)) + \tan z))$

$= \arctan(-1 + (-1 + \tan x + \tan y) + \tan z)$

$= \arctan(-2 + \tan x + \tan y + \tan z)$

Et on a :

$x * (y * z) = x * (\arctan(-1 + \tan y + \tan z))$

$= \arctan(-1 + \tan x + \tan((\arctan(-1 + \tan y + \tan z))))$

$= \arctan(-1 + \tan x + (-1 + \tan y + \tan z))$

$= \arctan(-2 + \tan x + \tan y + \tan z)$

Donc : $(x * y) * z = x * (y * z)$

par suite $*$ est associative

3) $\forall x \in I$ on a :

$x * \frac{\pi}{4} = \arctan\left(-1 + \tan x + \tan \frac{\pi}{4}\right) = \arctan(-1 + \tan x + 1)$

$x * \frac{\pi}{4} = \arctan(\tan x) = x$

Et puisque $*$ est commutatif on a aussi : $\frac{\pi}{4} * x = x$

Et puisque : $\frac{\pi}{4} \in]-\frac{\pi}{2}; \frac{\pi}{2}[$

alors : $*$ possède un élément neutre $e = \frac{\pi}{4}$

4) soit : $x \in I$ on cherche $x' \in I$ tel que :

$x * x' = \frac{\pi}{4} ?$

$x * x' = \frac{\pi}{4} \Leftrightarrow \arctan(-1 + \tan x + \tan x') = \frac{\pi}{4}$

$\Leftrightarrow -1 + \tan x + \tan x' = \tan\left(\frac{\pi}{4}\right) \Leftrightarrow \tan x + \tan x' = 2$

$\Leftrightarrow \tan x' = 2 - \tan x \Leftrightarrow x' = \arctan(2 - \tan x) \in I$

Donc : tout élément de I possède un symétrique pour $*$ dans I .

Finalement : $(I; *)$ est un groupe commutatif

Exercice 1: on muni \mathbb{R}^2 d'une loi de composition interne T définit par :

$$(x; y)T(x'; y') = (x + x'; ye^{x'} + y'e^{-x'}) ; \forall (x; y) \in \mathbb{R}^2 \text{ et } \forall (x'; y') \in \mathbb{R}^2$$

Monter que $(\mathbb{R}^2; T)$ groupe non commutative

Solution: a) soient $(x; y)$; $(x'; y')$ et $(x''; y'')$ des éléments de \mathbb{R}^2

$$\begin{aligned} ((x; y)T(x'; y'))T(x''; y'') &= (x + x'; ye^{x'} + y'e^{-x'})T(x''; y'') \\ &= (x + x' + x''; (ye^{x'} + y'e^{-x'})e^{x''} + y''e^{-(x+x')}) \\ &= (x + x' + x''; ye^{-(x'+x'')} + y'e^{-x+x''} + y''e^{-(x+x')}) \\ (x; y)T((x'; y')T(x''; y'')) &= (x; y)T(x' + x''; y'e^{x''} + y''e^{-x'}) \\ &= (x + x' + x''; (y'e^{x''} + y''e^{-x'})e^{-x} + ye^{x'+x''}) \\ &= (x + x' + x''; y'e^{(x''-x)} + y''e^{-(x+x')} + ye^{x'+x''}) \end{aligned}$$

Donc :

$$((x; y)T(x'; y'))T(x''; y'') = (x; y)T((x'; y')T(x''; y''))$$

donc : T est associative

b) l'élément neutre de T ?

$$(e_1; e_2) \text{ l'élément neutre de T ssi } \forall (x; y) \in \mathbb{R}^2$$

$$(x; y)T(e_1; e_2) = (x; y) \text{ et } (e_1; e_2)T(x; y) = (x; y)$$

$$(x; y)T(e_1; e_2) = (x; y) \Leftrightarrow (x + e_1; ye^{e_1} + e_2e^{-x}) = (x; y)$$

$$\Leftrightarrow \begin{cases} x + e_1 = x \\ ye^{e_1} + e_2e^{-x} = y \end{cases} \Leftrightarrow \begin{cases} e_1 = 0 \\ e_2e^{-x} = 0 \end{cases} \Leftrightarrow \begin{cases} e_1 = 0 \\ e_2 = 0 \end{cases}$$

$$\text{Et on a : } (0; 0)T(x; y) = (x; y)$$

Donc : $(0; 0)$ est l'élément neutre de T

c) le symétrique d'un élément dans T ?

soient $(x; y) \in \mathbb{R}^2$ montrons l'existence de

$$(x'; y') \in \mathbb{R}^2 \text{ tel que : } (x; y)T(x'; y') = (0; 0) \text{ et}$$

$$(x'; y')T(x; y) = (0; 0)$$

$$(x; y)T(x'; y') = (0; 0) \Leftrightarrow (x + x'; ye^{x'} + y'e^{-x}) = (0; 0)$$

$$\Leftrightarrow \begin{cases} x + x' = 0 \\ ye^{x'} + y'e^{-x} = 0 \end{cases} \Leftrightarrow \begin{cases} x' = -x \\ (y + y')e^{-x} = 0 \end{cases}$$

$$\Leftrightarrow \begin{cases} x' = -x \\ y + y' = 0 \end{cases} \Leftrightarrow \begin{cases} x' = -x \\ y' = -y \end{cases}$$

$$\text{On a aussi : } (-x; -y)T(x; y) = (0; 0)$$

Donc : $(-x; -y)$ est le symétrique de élément $(x; y)$ dans T

Donc : $(\mathbb{R}^2; T)$ est un groupe

$$\text{Et puisque : } (1; 1)T(1; 0) = (2; e) \text{ et } (1; 0)T(1; 1) = (2; e^{-1})$$

$$\text{Alors : } (1; 1)T(1; 0) \neq (1; 0)T(1; 1)$$

donc : T n'est pas commutative

3) propriété des groupes

Théorème : soit $(G; *)$ est un groupe

- 1) l'élément neutre dans G est unique
- 2) tout élément de G possède un symétrique unique dans G.

Si x' est le symétrique de x et y' est le symétrique de y alors le symétrique de $x * y$ est $y' * x'$:

$$\text{Cad : } (x * y)' = y' * x'$$

3) tout élément de G est régulier cad :

$$\forall a \in G \text{ et } \forall (x; y) \in G^2$$

$$a * x = a * y \Rightarrow x = y \text{ et } x * a = y * a \Rightarrow x = y$$

Preuve : 1) et 2) voir la leçon précédente

3) soient : $a \in G$ et $(x; y) \in G^2$

$$x * a = y * a \Rightarrow (x * a) * a' = (y * a) * a'$$

Avec a' est le symétrique de a

$$\Rightarrow x * (a * a') = y * (a * a') \text{ Car } * \text{ est associative}$$

$$\Rightarrow x * e = y * e \text{ Car } * \text{ possède un élément neutre } e$$

$$\Rightarrow x = y \text{ De même on montre l'autre implication}$$

Exemple1 :soit $(G; \cdot)$ un groupe noté

multiplicativement et tel que : $(a; b) \in G^2$

$(ab)^2 = a^2b^2$ Montrer que ce groupe est

commutatif

Solution :par hypothèse on a quels que soient

les éléments $(a; b) \in G^2$: $abab = aabb$

Mais dans un groupe tout élément étant régulier

on peut simplifier à gauche par a et à droite par b

Donc : $abab = aabb$

Donc $ba = ab$ et par suite ce groupe est

commutatif

Proposition :si $(G; *)$ est un groupe qui admet un

élément neutre e et $(a; b) \in G^2$ et a' est le

symétrique de a alors :les équations :

$(E_1) : a * x = b$ et $(E_2) : x * a = b$ admettent une

solution unique :

•Pour (E_1) la solution est : $x = a' * b$

•Pour (E_2) la solution est : $x = b * a'$

Exemple2:(étude d'un groupe fini)

$(\mathbb{Z}/5\mathbb{Z}; +)$ et $(\mathbb{Z}/5\mathbb{Z} - \{0\}; \times)$ sont deux groupes

commutatifs :

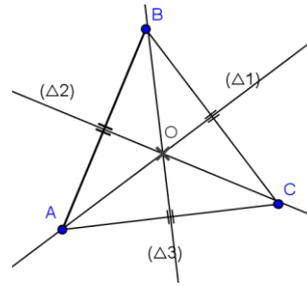
+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

Tableau de : $(\mathbb{Z}/5\mathbb{Z}; +)$ et Tableau de : $(\mathbb{Z}/5\mathbb{Z}; \times)$

×	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Exemple3 :(étude d'un groupe fini)

(ABC) un triangle équilatéral



(Δ_1) la médiatrice du segment $[BC]$

(Δ_2) la médiatrice du segment $[AB]$

(Δ_3) la médiatrice du segment $[AC]$

Soit ζ l'ensemble des transformations

suivantes : $\zeta = \{r_1; r_2; r_3; s_1; s_2; s_3\}$

r_1 la rotation de centre O et d'angle 0 : $r_1(O; 0)$

r_2 la rotation de centre O et d'angle $\frac{2\pi}{3}$: $r_2(O; \frac{2\pi}{3})$

r_3 la rotation de centre O et d'angle $\frac{4\pi}{3}$: $r_3(O; \frac{4\pi}{3})$

s_1 la symétrie axial d'axe : (Δ_1)

s_2 la symétrie axial d'axe : (Δ_2)

s_3 la symétrie axial d'axe : (Δ_3)

Donc : on utilisant la loi de composition des transformation \circ on trouve le tableau suivant :

\circ	r_1	r_2	r_3	s_1	s_2	s_3
r_1	r_1	r_2	r_3	s_1	s_2	s_3
r_2	r_2	r_3	r_1	s_3	s_1	s_2
r_3	r_3	r_1	r_2	s_2	s_3	s_1
s_1	s_1	s_2	s_3	r_1	r_2	r_3
s_2	s_2	s_3	s_1	r_3	r_1	r_2
s_3	s_3	s_1	s_2	r_2	r_3	r_1

Remarque : si $(G; *)$ est un groupe fini alors

chaque élément de G se trouve sur le tableau une fois dans chaque ligne et dans chaque colonne

Exercice 2: soit $(G; \cdot)$ un groupe noté multiplicativement et e l'élément neutre de G
 1) Montrer que si: $\forall (a; b) \in G^2 : (a \cdot b)^2 = a^2 \cdot b^2$
 alors le groupe G est commutatif

2) Montrer que si: $\forall x \in G : x^2 = e$ alors le groupe G est commutatif

Solution : 1) soit $(a; b) \in G^2$

par hypothèse on a: $(a \cdot b)^2 = a^2 \cdot b^2$

donc: $a \cdot b \cdot a \cdot b = a \cdot a \cdot b \cdot b$ puisque G un groupe tout élément de G est régulier

Donc: $b \cdot a = a \cdot b$

Par suite ce groupe est commutatif

2) soient les éléments $(x; y) \in G^2$

par hypothèse on a: $xyxy = e$

on multipliant à gauche par x et à droite par y

Donc: $xyxyxy = xey \Rightarrow x^2 yxy^2 = xey \Rightarrow eyxe = xy$

$\Rightarrow yx = xy$ Par suite ce groupe est commutatif

3) Sous-groupes

Définition : Soient $(G, *)$ un groupe et H une partie stable pour $(G, *)$

H est un sous-groupe de $(G, *)$ si et seulement si $(H, *)$ est un groupe

Remarque : si e est l'élément neutre de G $\{e\}$ et G sont des sous-groupes de $(G, *)$ appelés sous-groupes triviaux du groupe $(G, *)$. Les autres sous-groupes, s'il en existe, sont appelés sous-groupes propres de $(G, *)$.

Exemples :

• $(\mathbb{Z}; +)$; $(\mathbb{Q}; +)$; $(\mathbb{R}; +)$ sont des sous-groupes

de $(\mathbb{C}; +)$

• $(\mathbb{Q}^*; \times)$ est un sous-groupe de $(\mathbb{R}^*; \times)$

• $(\mathbb{R}_n[X]; +)$ est un sous-groupe de $(F(\mathbb{R}; \mathbb{R}); +)$

• $U = \{z \in \mathbb{C} / |z| = 1\}$

$(U; \times)$ est un sous-groupe de $(\mathbb{C}^*; \times)$

$(U; +)$ est un sous-groupe de $(\mathbb{C}; +)$

• $(\mathbb{N}; +)$ n'est pas un sous-groupe de $(\mathbb{Z}; +)$

Exemple: (on considère l'ensemble des matrices

suivante: $E = \left\{ M_a = \begin{pmatrix} 1 & a \\ 2 & 0 \end{pmatrix} / a \in \mathbb{R} \right\}$

Montrer que E n'est pas un sous-groupe de $(M_2(\mathbb{R}); +)$

Solution : soit $M_a \in E$ et $M_b \in E$

Donc: $M_a = \begin{pmatrix} 1 & a \\ 2 & 0 \end{pmatrix}$ et $M_b = \begin{pmatrix} 1 & b \\ 2 & 0 \end{pmatrix}$

$M_a \times M_b \in E?$

$M_a \times M_b = \begin{pmatrix} 1 & a \\ 2 & 0 \end{pmatrix} \times \begin{pmatrix} 1 & b \\ 2 & 0 \end{pmatrix} = \begin{pmatrix} 1+2a & b \\ 2 & 2b \end{pmatrix} \notin E$

donc: E n'est une partie stable de $(M_2(\mathbb{R}); \times)$

donc: E n'est pas un sous-groupe de $(M_2(\mathbb{R}); +)$

Théorème : (caractérisations d'un sous-groupe).

Soient $(G, *)$ un groupe et H une partie de G .

1) H est un sous-groupe de $(G, *)$

$\Leftrightarrow \begin{cases} (1) e \in H \\ (2) \forall (x, y) \in H^2; x * y \in H \\ (3) \forall x \in H; x' \in H \end{cases} \quad (I)$

2) H est un sous-groupe de $(G, *)$

$\Leftrightarrow \begin{cases} (1) H \neq \emptyset \\ (2) \forall (x, y) \in H^2; x * y' \in H \end{cases} \quad (II)$

Démonstration :

• Supposons que H soit un sous-groupe de $(G, *)$, alors la propriété (2) de (I) est vérifiée.

Notons e_H l'élément neutre de H .

On a $e_H * e = e_H$ car e est élément neutre de G et d'autre part, $e_H = e_H * e_H$ car e_H est élément neutre de H . Par suite, $e_H * e = e_H * e_H$.

Maintenant, dans le groupe $(G, *)$, tout élément

est métrisable et en particulier, tout élément est régulier. Après simplification par e_H , on obtient $e = e_H$. Ceci montre en particulier que $e \in H$.

Soit x un élément de H . Notons x'_H son symétrique pour $*$ dans H .

On a $x'_H * x * x' = e * x' = x'$ (puisque $e_H = e$) et d'autre part, $x_H * x * x' = x'_H * e = x'_H$.

Donc, le symétrique x'_H de x dans H est son symétrique x' dans G . Ceci montre en particulier que x' est dans H .

On a montré que si H est un sous-groupe de $(G, *)$ alors (I) est vérifié.

• Montrons que : (I) \Rightarrow H sous-groupe de $(G, *)$.
Supposons (I).

H est une partie non vide de G d'après (1). La restriction de $*$ à H^2 est une loi interne dans H d'après (2). $*$ est associative dans G

et donc la loi induite est associative dans H

L'élément neutre e de $(G, *)$ vérifie :

$\forall x \in H, x * e = e * x = x$ et donc e est élément neutre de H pour la loi induite.

Enfin, si x est un élément quelconque de H , le symétrique x' de x dans G est dans H et vérifie $x * x' = x' * x = e$ où e est maintenant élément neutre de H . x' est donc le symétrique de x dans H et on a montré que tout élément de H admet un symétrique dans H .

De tout ceci, on en déduit bien que H est un sous-groupe de $(G, *)$

Donc que $(H \text{ sous-groupe}) \Leftrightarrow$ (I).

• Il est clair que (I) \Rightarrow (II). Il reste à montrer que (II) \Rightarrow (I). On suppose donc que H vérifie (II).

Soit x un élément de H . Puisque e et x sont dans H alors: $H \neq \emptyset$ et $e * x' = x'$ est dans H d'après (2).

Ainsi, $\forall x \in H, x' \in H$.

Soient enfin, x et y deux éléments de H .

D'après ce qui précède, y' est encore dans H

Donc $x * (y')' = x * y$ est dans H .

On a montré que (II) \Rightarrow (I)

Finalement que (I) \Leftrightarrow (II).

Remarque : soit : $(G; *)$ un groupe

1) on utilisant une notation additive on a :

H est un sous-groupe de $(G; +)$

$$\Leftrightarrow \begin{cases} (1) H \neq \emptyset \\ (2) \forall (x, y) \in H^2; x - y \in H \end{cases}$$

2) on utilisant une notation multiplicative

on a : H est un sous-groupe de $(G; \times)$

$$\Leftrightarrow \begin{cases} (1) H \neq \emptyset \\ (2) \forall (x, y) \in H^2; xy^{-1} \in H \end{cases}$$

Exemple1 : soit I l'ensemble des nombres entiers relatifs pairs

montrer que $(I; +)$ est un sous-groupe de $(\mathbb{Z}; +)$

Solution : on a : $I \subset \mathbb{Z}$

$$(1) I \neq \emptyset \text{ car } 0 = 2 \times 0 \in I$$

$$(2) \forall (x, y) \in I^2; x - y \in I ?$$

Soient : $x \in I$ et $y \in I$ donc : $x = 2 \times p$ et $x = 2 \times q$

$$x - y = 2 \times p - 2 \times q = 2 \times (p - q) = 2 \times k \in I$$

Donc : $(I; +)$ est un sous-groupe de $(\mathbb{Z}; +)$ d'après

La propriété caractéristique d'un sous-groupe

Exemple2 : montrer que : $H = \{3^m 7^n \mid m \in \mathbb{Z}; n \in \mathbb{Z}\}$

est un sous-groupe de $(\mathbb{R}^*; \times)$

Solution : on a : $H \subset \mathbb{R}^*$ car $\forall (n, m) \in \mathbb{Z}^2; 3^m 7^n \in \mathbb{R}^*$

$$(1) H \neq \emptyset \text{ car } 3^0 7^0 = 1 \in H$$

$$(2) \forall (x, y) \in H^2; x \times y^{-1} \in H ?$$

Soient : $x \in H$ et $y \in H$ donc :

$$\exists (n, m) \in \mathbb{Z}^2; x = 3^m 7^n$$

$$\text{Et } \exists (p, q) \in \mathbb{Z}^2; y = 3^p 7^q$$

$$x \times y^{-1} = 3^m 7^n \times (3^p 7^q)^{-1} = 3^m 7^n \times 3^{-p} 7^{-q}$$

$$x \times y^{-1} = 3^m 7^n \times (3^p 7^q)^{-1} = 3^{m-p} 7^{n-q} = 3^e 7^f$$

Avec : $(e, f) \in \mathbb{Z}^2$ donc :

$$(2) \forall (x, y) \in H^2; x \times y^{-1} \in H$$

Donc : $(H; \times)$ est un sous-groupe de $(\mathbb{R}^*; \times)$

D'après la propriété caractéristique d'un sous-groupe

Exemple 3 : Si E est un ensemble, l'intersection dans P(E) est interne, commutative, associative et possède un élément neutre, à savoir E.

Soit alors F une partie stricte de E. P(F) est une partie non vide de P(E), stable pour l'intersection (l'intersection de deux parties de F reste une partie de F). L'intersection possède un élément neutre dans P(F), à savoir F. Cet élément neutre est distinct de l'élément neutre de $(P(E), \cap)$. Une conséquence est que $(P(E), \cap)$ n'est pas un groupe.

Exemple 4 : $U = \{z \in \mathbb{C} / |z| = 1\}$

Montrer que $(U; \times)$ est un sous-groupe de $(\mathbb{C}^*; \times)$

Solution :

1) Un nombre complexe de module 1 est non nul et donc $U \subset \mathbb{C}^*$

Et 1 a pour module 1 et donc $1 \in U$.

Soit alors $(z_1; z_2) \in U^2$.

$$z_1 \times z_2^{-1} \in U ???$$

$$|z_1 \times z_2^{-1}| = |z_1| \times |z_2^{-1}| = |z_1| \times |z_2|^{-1} = 1 \times 1 = 1 \times 1 \in U$$

Exercice 3: on considère l'ensemble des matrices suivante :

$$E = \left\{ M_a = \begin{pmatrix} \ln a & 0 \\ 0 & \ln a \end{pmatrix} / a \in \mathbb{R}^{++} \right\}$$

Monter que E est un sous-groupe de $(M_2(\mathbb{R}); +)$

$$\text{Solution : 1) on a } M_e = \begin{pmatrix} \ln e & 0 \\ 0 & \ln e \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$$

Donc : $I_2 \in E$ donc : $E \neq \emptyset$

2) soit $M_a \in E$ et $M_b \in E$

$M_a - M_b \in E ?$:

$$M_a - M_b = \begin{pmatrix} \ln a & 0 \\ 0 & \ln a \end{pmatrix} - \begin{pmatrix} \ln b & 0 \\ 0 & \ln b \end{pmatrix}$$

$$M_a - M_b = \begin{pmatrix} \ln a - \ln b & 0 \\ 0 & \ln a - \ln b \end{pmatrix} = \begin{pmatrix} \ln \frac{a}{b} & 0 \\ 0 & \ln \frac{a}{b} \end{pmatrix} = M_{a/b}$$

Et puisque $a \in \mathbb{R}^{++}$ et $b \in \mathbb{R}^{++}$ alors $a/b \in \mathbb{R}^{++}$

Donc : $M_a - M_b = M_{a/b} \in E$

Donc : E est un sous-groupe de $(M_2(\mathbb{R}); +)$

Exercice 4 : soit $(G; \cdot)$ un groupe noté

multiplicativement et soit $a \in G$

On pose : $C_a = \{x \in G / ax = xa\}$

(centralisateur de a)

$$\text{Et : } Z(G) = \{x \in G / \forall y \in G : xy = yx\}$$

(centre de G)

Montrer que C_a et $Z(G)$ sont des sous-groupes

de $(G; \cdot)$

Solution : 1) Montrons que C_a est un sous-

groupe de $(G; \cdot)$?

Soit e l'élément neutre du groupe $(G; \cdot)$

a) on a : $ae = ea = a$ donc $e \in C_a$ donc : $C_a \neq \emptyset$

b) soient les éléments $(x; y) \in C_a^2$

montrons que : $xy^{-1} \in C_a$ cad montrons que :

$$a(xy^{-1}) = (xy^{-1})a ??$$

On a $(x; y) \in C_a^2$ donc : $\begin{cases} ax = xa(1) \\ ay = ya(2) \end{cases}$

$$(2) \Leftrightarrow (ay)^{-1} = (ya)^{-1} \Leftrightarrow y^{-1}a^{-1} = a^{-1}y^{-1}$$

$$\Rightarrow y^{-1}a^{-1} = a^{-1}y^{-1} \text{ et } ax = xa(1)$$

$$\Rightarrow axy^{-1}a^{-1} = xaa^{-1}y^{-1} \Rightarrow axy^{-1}a^{-1} = xey^{-1}$$

$$\Rightarrow axy^{-1}a^{-1} = xy^{-1} \Rightarrow axy^{-1}a^{-1}a = xy^{-1}a$$

$$\Rightarrow axy^{-1}e = xy^{-1}a \Rightarrow axy^{-1} = xy^{-1}a \text{ donc } xy^{-1} \in C_a$$

Donc : C_a est un sous-groupe de $(G; \cdot)$

2) Montrons que $Z(G)$ est un sous-groupe de $(G; \cdot)$?

a) on a : $\forall y \in G : ey = ye$ donc $e \in Z(G)$

donc : $Z(G) \neq \emptyset$

b) soient les éléments $(a; b) \in Z(G)^2$

montrons que : $ab^{-1} \in Z(G)$ cad montrons que :

$$(ab^{-1})y = y(ab^{-1}) \quad \forall y \in G ??$$

On a $(a; b) \in Z(G)^2$ donc : $\begin{cases} ay = ya(1) \\ by = yb(2) \end{cases}$

De la même façon que précédemment on trouve

$$(ab^{-1})y = y(ab^{-1}) \quad \forall y \in G \text{ donc } ab^{-1} \in Z(G)$$

Donc : $Z(G)$ est un sous-groupe de $(G; \cdot)$

Théorème : Si H et K sont des sous-groupes de $(G, *)$, $H \cap K$ est un sous-groupe de $(G, *)$. Ainsi, une intersection de sous-groupes est un sous-groupe.

Démonstration. (On utilise la caractérisation (II) ci-dessus). Soient H et K deux sous-groupes.

D'après ce qui précède, H et K contiennent l'élément neutre e de G et donc $e \in H \cap K$.

D'autre part, bien sûr $H \cap K \subset G$.

Soient alors x et y deux éléments de $H \cap K$.

$$(x, y) \in (H \cap K)^2 \Rightarrow ((x, y) \in H^2$$

$$\text{et } (x, y) \in K^2) \Rightarrow (x * y' \in H \text{ et } x * y' \in K)$$

$$\Rightarrow x * y' \in H \cap K.$$

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

Théorème : soit f un homomorphisme du groupe $(G, *)$ Dans un groupe $(F; T)$

L'image du groupe $(G, *)$ par l'homomorphisme f C'est le groupe $(f(G); T)$

Démonstration : on a déjà montré que $f(G)$

Est une partie stable $(F; T)$ et donc :

* est associative dans : $(G, *)$ donc :

* est associative dans : $(f(G), T)$ soit e l'élément

neutre de $(G, *)$ donc : $f(e)$ est l'élément neutre

de $(f(G), T)$ et si x' est le symétrique de x dans

$(G, *)$ alors $f(x')$ est le symétrique de $f(x)$

Dans $(f(G); T)$

Donc : $(f(G); T)$ est un groupe

Remarque :

Si f un homomorphisme surjectif alors $f(G) = F$

Dans ce cas L'image du groupe $(G, *)$ par

l'homomorphisme f c'est le groupe $(F; T)$

1)Exemples :

Les applications suivantes :

$$g : (\mathbb{R}^{*+}; \times) \rightarrow (\mathbb{R}; +) \quad f : (\mathbb{Z}; +) \rightarrow (\mathbb{R}^{*+}; \times)$$

$$x \mapsto \ln x$$

$$r \mapsto 2^r$$

$$h : (\mathbb{C}; \times) \rightarrow (\mathbb{C}; \times)$$

$$l : (\mathbb{R}; +) \rightarrow (\mathbb{R}^{*+}; \times)$$

$$z \mapsto \bar{z}$$

$$x \mapsto e^x$$

Sont des homomorphismes de groupes

Exercice 5 : On munit \mathbb{R} de la loi de composition interne définie par :

$$x * y = x\sqrt{y^2 + 1} + y\sqrt{x^2 + 1}; \forall (x; y) \in \mathbb{R}^2$$

1) soit l'application :

$$f : \mathbb{R} \rightarrow \mathbb{R} \text{ définie par : } f(x) = \frac{e^x - e^{-x}}{2}$$

Montrer que f est un isomorphisme de $(\mathbb{R}; +)$

vers $(\mathbb{R}; *)$

2) En déduire la structure de $(\mathbb{R}; *)$

Solution : 1) a) f est une fonction continue et

dérivable sur \mathbb{R} et $f'(x) = \frac{e^x + e^{-x}}{2} > 0$

Donc f est strictement croissante sur \mathbb{R}

Par suite f est une fonction bijectif de \mathbb{R}

Dans $f(\mathbb{R}) = \mathbb{R}$

b) soient $x; y \in \mathbb{R}$

$$f(x+y) = \frac{e^{x+y} - e^{-(x+y)}}{2}$$

$$f(x) * f(y) = f(x) \sqrt{f(y)^2 + 1} + f(y) \sqrt{f(x)^2 + 1}$$

Et on a :

$$f(y)^2 + 1 = 1 + \left(\frac{e^y - e^{-y}}{2}\right)^2 = \frac{e^{2y} + 2 + e^{-2y}}{4} = \left(\frac{e^y + e^{-y}}{2}\right)^2$$

Donc : $\sqrt{f(y)^2 + 1} = \frac{e^y + e^{-y}}{2}$ de même on a :

$$\sqrt{f(x)^2 + 1} = \frac{e^x + e^{-x}}{2} \quad \text{Donc :}$$

$$f(x) * f(y) = \left(\frac{e^x - e^{-x}}{2}\right) \left(\frac{e^y + e^{-y}}{2}\right) + \left(\frac{e^x + e^{-x}}{2}\right) \left(\frac{e^y - e^{-y}}{2}\right)$$

$$f(x) * f(y) = \frac{e^{x+y} - e^{-(x+y)}}{2}$$

Finalement : $f(x+y) = f(x) * f(y)$

Donc : f est un homomorphisme bijectif de $(\mathbb{R}; +)$

vers $(\mathbb{R}; *)$ donc un isomorphisme

2) puisque : f est un isomorphisme de $(\mathbb{R}; +)$ vers

$(\mathbb{R}; *)$ et $(\mathbb{R}; +)$ est un groupe commutatif

Alors : $(\mathbb{R}; *)$ est un groupe commutatif

II) Anneaux

1) Distributivité d'une loi sur une autre

Définition : Soient E un ensemble non vide
 $*$ et T deux lois de composition internes sur E .
 T est distributive sur $*$ $\Leftrightarrow \forall (x, y, z) \in E^3$
 $x T (y * z) = (x T y) * (x T z)$

Et $(y * z) T x = (y T x) * (z T x)$.

Remarque : Si on sait que T est commutative,
une et une seule des deux égalités ci-dessus
suffit.

Exemples : 1) Dans \mathbb{C} , la multiplication est
distributive sur l'addition

$$\forall (x; y; z) \in \mathbb{C}^3 : x \times (y + z) = x \times y + x \times z$$

2) Dans $P(E)$, l'intersection est distributive sur la
réunion et la réunion est distributive sur

l'intersection : $\forall (A; B; C) \in P(E)^3 :$

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \quad \text{et} \quad A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

3) Dans $(F(\mathbb{R}; \mathbb{R}); \circ)$ est distributive à droite

sur $+$, mais pas à gauche $((g+h) \circ f = g \circ f + h \circ f$, mais
en général, $f \circ (g+h) \neq f \circ g + f \circ h$.

1) dans $M_2(\mathbb{R})$ et $M_3(\mathbb{R})$ la multiplication est
distributive sur l'addition mais l'addition

$$\forall (A; B; C) \in M_3(\mathbb{R})^3 :$$

$$A \times (B + C) = (A \times B) + (A \times C)$$

$$(A + B) \times C = (A \times C) + (B \times C)$$

4) dans $\mathbb{N} ; \mathbb{Z} ; \mathbb{Q} ; \mathbb{R} ; \mathbb{C}$ l'addition n'est pas
distributive sur la multiplication :

$$1 + (5 \times 3) \neq (1 + 5) \times (1 + 3)$$

5) on muni \mathbb{N} de la loi

5) on muni \mathbb{N} d'une loi de composition interne $*$

défini par : $a * b = a^b$ si $a \neq 0$ et $a \neq 0$;

Et $a * 0 = 1$

Etudions la distributivité de la loi $*$ par rapport à la
multiplication ??

$$a) a*(b \times c) = a^{bc}$$

$$(a*b) \times (a*c) = a^b \times a^c = a^{b+c}$$

$a*(b \times c) \neq (a*b) \times (a*c)$ donc la loi $*$ n'est pas distributive a gauche sur la multiplication

$$b) (b \times c)*a = (bc)^a$$

$$(b*a) \times (c*a) = b^a \times c^a = (bc)^a$$

Donc : $(b \times c)*a = (b*a) \times (c*a)$ donc la loi $*$ est distributive à droite sur la multiplication
Finalement : la loi $*$ n'est pas distributive sur la multiplication

2) Anneaux

Définition : Soit A un ensemble non vide ayant au moins deux éléments muni de deux lois de composition interne (notées $*$ et T).

$(A, *, T)$ est un anneau \Leftrightarrow

1) $(A, *)$ est un groupe commutatif

2) T est associative

3) T est distributive sur $*$

L'anneau est commutatif si et seulement si T est commutative si de plus T admet un élément neutre on dira qu'il est unitaire

Notation additif et multiplicatif :

On note en général la première loi $+$ et la deuxième loi \times

On aura alors l'anneau $(A, +, \times)$

On note 0 l'élément neutre pour la loi $+$ et on

l'appelle l'élément nul de l'anneau A

Si la loi \times admet un élément neutre on le note 1

et on l'appelle l'élément unitaire de l'anneau A

Donc **les conditions (axiomes) pour un anneau**

$(A, +, \times)$ deviennent :

$$1) \forall (x; y; z) \in A^3 : x + (y + z) = (x + y) + z$$

$$2) \forall (x; y) \in A^2 : x + y = y + x$$

$$3) \exists 0 \in A \forall x \in A : x + 0 = x$$

$$4) \forall x \in A \exists -x \in A : x + (-x) = 0$$

$$5) \forall (x; y; z) \in A^3 : x \times (y \times z) = (x \times y) \times z$$

$$6) \forall (x; y; z) \in A^3 : x \times (y + z) = x \times y + x \times z \text{ et}$$

$$(x + y) \times z = x \times z + y \times z$$

3) Exemples anneaux :

$$1) (\mathbb{Z}; +; \times) ; (\mathbb{Q}; +; \times) ; (\mathbb{R}; +; \times) ; (\mathbb{C}; +; \times)$$

Sont des anneaux commutatifs unitaires
(1 l'élément unitaire)

2) $(\mathbb{N}; +; \times)$ n'est pas un anneau (car $(\mathbb{N}, +)$ n'est pas un groupe)

3) L'anneau des polynômes de degré inférieur a n
 $(\mathbb{R}_n[X]; +; \times)$ Est un anneau commutatif unitaire

4) $(M_2(\mathbb{R}); +; \times) ; (M_3(\mathbb{R}); +; \times)$ Sont des anneaux non commutatifs mais unitaires
(ls matrice unitaires sont resp:

$$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ et } I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

5) $(F(\mathbb{R}; \mathbb{R}); +; \circ)$ n'est pas un anneau car la loi \circ n'est distributive sur l'addition

En effet : $f : x \rightarrow x$ et $g : x \rightarrow 1$ et $h : x \rightarrow \sqrt{|x|}$

On montre que :

$$[h \circ (f + g)](x) \neq (h \circ f)(x) + (h \circ g)(x)$$

6) $(F(\mathbb{R}; \mathbb{R}); +; \times)$ est un anneau commutatif unitaire
(U : $x \rightarrow 1$ l'élément unitaire)

7) $(P(E); \Delta; \cap)$ est un anneau commutatif unitaire
(E l'élément unitaire)

8) $(P(E); \Delta; \cup)$ n'est pas un anneau car la loi \cup n'est distributive sur Δ

4) Calculs dans un anneau

Théorème : Soit $(A, +, *)$ un anneau. On note 0_A l'élément neutre de A pour $+$.

$\forall x \in A, x * 0_A = 0_A * x = 0_A$ (l'élément neutre pour l'addition est toujours absorbant pour la multiplication).

Démonstration :

Soit $x \in A$. $0_A * x = (0_A + 0_A) * x = 0_A * x + 0_A * x$ car $*$ est distributive sur $+$. Maintenant, $(A, +)$ est un groupe et dans un groupe, tout élément est régulier.

Donc, $0_A * x + 0_A * x = 0_A * x = 0_A * x + 0_A$

entraîne $0_A * x = 0_A$. de même, $x * 0_A = 0_A$. \square

Théorème : Soit $(A, +, *)$ un anneau.

$\forall (a, b) \in A^2$

$(-a) * b = a * (-b) = -(a * b)$

Démonstration : Soit $(a, b) \in A^2$

$a * b + (-a) * b = (a + (-a)) * b = 0_A * b = 0_A$

et donc $(-a) * b = -a * b$.

De même, $a * b + a * (-b) = a * (b + (-b))$

$= a * 0_A = 0_A$ et donc $a * (-b) = -a * b$.

Remarques : Dans un anneau (ayant au moins deux éléments) on montre aisément

que $0_A \neq 1_A$ et que 0_A n'a pas de symétrique (pour la 2^{ième} loi). Si tous les autres éléments de A sont inversibles, on montrera que l'ensemble des éléments non nuls $A^* = A - \{0_A\}$

Forme un groupe (pour la loi 2^{ième} loi)

Théorème : Soit $(A, +, \times)$ un anneau.

On note A^* l'ensemble des éléments de A qui sont inversibles c'est-à-dire l'ensemble des éléments de A symétrisables pour \times

(A^*, \times) est un groupe.

Démonstration : 1_A est un élément de A^*

car 1_A est inversible pour \times , d'inverse lui-même.

Donc : $A^* \neq \emptyset$

• Si x et y sont deux éléments de A^* on sait que $x \times y$ est dans A^* et que : $(x \times y)^{-1} = y^{-1} \times x^{-1}$

Donc, \times induit une loi de composition interne sur A^* que l'on note encore \times .

\times est associative dans A et donc \times est associative dans A^*

$1_A \in A^*$ et pour tout x de A^* , $1_A \times x = x \times 1_A = x$.

Donc, \times possède un élément neutre 1_A dans A^*

Soit $x \in A^*$. On sait que $x^{-1} \in A^*$ et que

$(x^{-1})^{-1} = x$. Donc, tout élément de A^* admet un symétrique pour \times dans A^*

Donc : (A^*, \times) est un groupe

4) Diviseurs de zéro - Anneau intègre

4-1) Diviseurs de zéro

Exemple : Considérons les deux matrices carrées d'ordre 2 suivantes :

$$M = \begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix}, N = \begin{pmatrix} 2 & -4 \\ -1 & 2 \end{pmatrix}$$

Aucune de ces deux matrices n'est la matrice nulle, et pourtant leur produit vérifie :

$$M \times N = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

On dit que les matrices M et N sont des *diviseurs de zéro*.

Plus généralement, on a les définitions suivantes :

Définition 1: Soit $(A; *, T)$ un anneau et e

l'élément neutre pour $*$

Un élément $a \neq e$ de A est appelé un diviseur de zéro s'il existe un autre élément $b \neq e$ de A tel que $aTb = e$ et $bTa = e$

Définition 2 : l'anneau $(A; *, T)$ est dit intègre

S'il ne possède pas de diviseurs de zéros

Définition 3 : l'anneau $(A; +; \times)$ est intègre

Ssi : $a \times b = 0 \Rightarrow a = 0$ ou $b = 0$

Exemples :

- $(\mathbb{Z}; +; \times)$ est un anneau intègre : le produit de deux entiers relatifs est nul si et seulement si l'un de ces deux entiers est nul.
- L'exemple précédent montre que $(M_2(\mathbb{R}); +; \times)$ n'est pas un anneau intègre.

De même pour $(M_3(\mathbb{R}); +; \times)$

- $(F(\mathbb{R}; \mathbb{R}); +; \times)$ est un anneau commutatif unitaire

Non intègre en effet :

$$f : x \rightarrow \begin{cases} \frac{1}{x^2+1}; x \geq 0 \\ 0; x < 0 \end{cases} \text{ et } g : x \rightarrow \begin{cases} 0; x \geq 0 \\ x^5; x < 0 \end{cases}$$

On a : $f \neq \theta$ et $g \neq \theta$ avec $\theta : x \rightarrow 0$ l'élément

neutre de $(F(\mathbb{R}; \mathbb{R}); +)$

On montre que : $f \times g = \theta$

- $(\mathbb{Z}/6\mathbb{Z}; +; \times)$ n'est pas un anneau intègre.

Car : $\bar{2} \neq \bar{0}$ et $\bar{3} \neq \bar{0}$ mais $\bar{2} \times \bar{3} = \bar{6} = \bar{0}$

$\bar{3}$ est un diviseur de zéro et $\bar{2}$ aussi

- $(\mathbb{Z}/5\mathbb{Z}; +; \times)$ est un anneau intègre.

Tableau de : $(\mathbb{Z}/5\mathbb{Z}; \times)$

\times	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

proposition : soit $(A; *, T)$ un anneau unitaire

si $a \in A$ admet un symétrique pour T alors a

n'est pas un diviseur de zéro dans $(A; *, T)$

Preuve : Soit e l'élément neutre pour $*$ et Soit

f l'élément neutre pour T et a' le symétrique

De a

Supposons qu'il existe $b \in A$ tel que : $aTb = e$ et

$$bTa = e$$

$$aTb = e \Leftrightarrow a'T(aTb) = a'Te \Leftrightarrow (a'Ta)Tb = e$$

$$\Leftrightarrow fTb = e \Leftrightarrow b = e$$

Exercice 6 : on considère l'ensemble suivant :

$$E = \{a + b\sqrt{3} / (a; b) \in \mathbb{Q}^2\}$$

1) Monter que $(E; +)$ est un groupe commutatif

2) Monter que E est une partie stable de $(\mathbb{Q}; \times)$

3) Monter que $(E; +; \times)$ est un anneau commutatif unitaire

Solution : 1) Montrons que $(E; +)$ est un sous-groupe de $(\mathbb{Q}; +)$?

On a $E \subset \mathbb{Q}$ et on a $1 = 1 + 0\sqrt{3}$ donc : $1 \in E$

donc : $E \neq \emptyset$

soit $x \in E$ et $y \in E$ montrons $x - y \in E$?

$$x \in E \Leftrightarrow \exists (a; b) \in \mathbb{Q}^2 / x = a + b\sqrt{3}$$

$$y \in E \Leftrightarrow \exists (c; d) \in \mathbb{Q}^2 / y = c + d\sqrt{3}$$

$$x - y = (a + b\sqrt{3}) - (c + d\sqrt{3}) = (a - c) + (b - d)\sqrt{3}$$

On a $(a; b; c; d) \in \mathbb{Q}^4$ donc : $a - c \in \mathbb{Q}$ et $b - d \in \mathbb{Q}$

Donc : $x - y = a'' + b''\sqrt{3}$ par suite : $x - y \in E$

Donc : $(E; +)$ est un sous-groupe de $(\mathbb{Q}; +)$

donc $(E; +)$ est un groupe

2)) Montrons que E est une partie stable de $(\mathbb{Q}; \times)$?

soit $x \in E$ et $y \in E$ montrons $x \times y \in E$?

$$x \times y = (a + b\sqrt{3}) \times (c + d\sqrt{3}) = (ac + 3bd) + (ad + bc)\sqrt{3}$$

puisque $(a; b; c; d) \in \mathbb{Q}^4$ alors : $ac + 3bd \in \mathbb{Q}$ et

$ad + bc \in \mathbb{Q}$ donc : $x \times y \in E$

$$: E = \{a + b\sqrt{3} / (a; b) \in \mathbb{Q}^2\}$$

Donc : E est une partie stable de $(\mathbb{Q}; \times)$

3) on a $(\mathbb{Q}; +; \times)$ est un anneau commutatif

Donc La multiplication est commutative et distributive par rapport à l'addition dans E

Par suite $(E; +; \times)$ un anneau commutatif

Et $1 = 1 + 0\sqrt{3}$ donc : $1 \in E$ et 1 est l'élément

neutre de la multiplication dans $(\mathbb{Q}; \times)$

Donc : 1 est l'élément neutre de la multiplication dans E

Conclusion : $(E; +; \times)$ est un anneau commutatif unitaire

Exercice 7: Soit $(A; +; \times)$ un anneau.

Tel que : $x^2 = x \quad \forall x \in A$ ($(A; +; \times)$ s'appelle anneau

De Boole)

1) calculer $(x+x)^2$

2) en déduire que : $x+x=0_A$ (0_A est l'élément

neutre de $(A; +)$)

3) soient : $x \in A$ et $y \in A$

a) calculer $(x+y)^2$ en fonction de x et y

b) en déduire que $(A; +; \times)$ est commutatif

c) en déduire : $xy(x+y)$

4) on suppose que : $x \neq 0_A$ et $y \neq 0_A$ et $y \neq x$

a) montrer que : a) $x+y \neq 0_A$ b) $x+y \neq y$

5) déterminer le tableau de la somme pour les éléments : $0_A ; x ; y ; x+y$

Solution : 1) soit $x \in A$ on a :

$$(x+x)^2 = (x+x)(x+x) = xx+xx+xx+xx$$

$$(x+x)^2 = x^2+x^2+x^2+x^2 = x+x+x+x \text{ car } x^2 = x$$

$$\text{Donc : } (x+x)^2 = x+x+x+x$$

2)a) soient : $x \in A$ et $y \in A$

$$(x+y)^2 = (x+y)(x+y) = xx+xy+yx+yy$$

$$(x+y)^2 = x^2+xy+yx+y^2$$

$$(x+y)^2 = x+xy+yx+y \text{ car } x^2 = x \quad \forall x \in A$$

b) on a : $(x+y)^2 = x+xy+yx+y$ et $(x+y)^2 = x+y$

$$\text{donc : } x+xy+yx+y = x+y$$

$$\text{donc : } xy+yx = 0_A \text{ et puisque } xy+xy = 0_A$$

$$\text{Alors : } xy+yx = xy+xy \text{ donc } yx = xy$$

Donc : $(A; +; \times)$ est commutatif

c) déduction de : $xy(x+y)$

soient : $x \in A$ et $y \in A$

$$xy(x+y) = xyx+xy^2 = xxy+xy^2 = x^2y+xy^2 = xy+xy$$

$$\text{et puisque } xy+xy = 0_A \text{ alors : } xy(x+y) = 0_A$$

4) on suppose que : $x \neq 0_A$ et $y \neq 0_A$ et $y \neq x$

a) on suppose que $x+y=0_A$ et puisque $x+x=0_A$

$$\text{Alors : } x+y = x+x \text{ cad } y = x \text{ contradiction}$$

$$\text{Donc : } x+y \neq 0_A$$

b) on suppose que $x+y=y$ donc : $x=0_A$

Contradiction donc $x+y \neq y$

5) on a : $x+x=0_A$ et $x+0_A=0_A+x=x$

+	0_A	x	y	$x+y$
0_A	0_A	x	y	$x+y$
x	x	0_A	$x+y$	y
y	y	$x+y$	0_A	x
$x+y$	$x+y$	y	x	0_A

III) corps

1) Définition : Soit $(K, +, \times)$ un anneau.

$(K, +, \times)$ est un corps si et seulement si tout élément non nul de K admet un inverse (pour \times) dans K et le corps est commutatif si et seulement si $*$ est commutative.

Exemples : 1) $(\mathbb{Q}; +; \times)$; $(\mathbb{R}; +; \times)$; $(\mathbb{C}; +; \times)$ sont des corps commutatifs.

2) $(\mathbb{Z}; +; \times)$ Est un anneau commutatif qui n'est pas un corps car par exemple, le nombre 2 n'est pas inversible dans \mathbb{Z} .

3) $(M_2(\mathbb{R}); +; \times)$ n'est pas un corps car par

exemple : $A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ n'est pas inversible

4) $(\mathbb{Z}/6\mathbb{Z}; +; \times)$ n'est pas un corps car par

exemple $\bar{3}$ n'est pas inversible

2) Notation additif et multiplicatif d'un corps :

On note en général la première loi $+$ et la deuxième loi \times

On aura alors le corps $(K, +, \times)$

On note 0 l'élément neutre pour la loi $+$ et on l'appelle l'élément nul du corps K

l'élément neutre pour la loi \times on le note 1 et on l'appelle l'élément unitaire corps K

Donc les conditions (axiomes) pour un corps

$(K, +, \times)$ devient :

1) $\forall (x; y; z) \in K^3 : x + (y + z) = (x + y) + z$

2) $\forall (x; y) \in K^2 : x + y = y + x$

3) $\exists 0 \in K \quad \forall x \in K : x + 0 = x$

4) $\forall x \in K \quad \exists -x \in K : x + (-x) = 0$

5) $\forall (x; y; z) \in K^3 : x \times (y \times z) = (x \times y) \times z$

6) $\exists 1 \in K \quad \forall x \in K : x \times 1 = x \times 1 = x$

7) $\forall x \in K - \{0\} \quad \exists x^{-1} \in K - \{0\} : x \times x^{-1} = x^{-1} \times x = 1$

8) $\forall (x; y; z) \in K^3 : x \times (y + z) = x \times y + x \times z$ et

$$(x + y) \times z = x \times z + y \times z$$

Théorème : Dans un corps, un produit de facteurs est nul si et seulement si l'un de ces facteurs est nul :

$$\forall (x; y) \in K^3 : x \times y = 0 \Leftrightarrow x = 0 \text{ ou } y = 0$$

Donc un un corps ne contient pas de diviseur de zéro

Démonstration. Soit $(K, +, \times)$: on note 0 (resp. 1) l'élément neutre pour $+$ (resp. \times).

Soit $(a, b) \in K^2$ tel que : $a \times b = 0$.

Si $a \neq 0$, a admet un inverse pour \times noté a^{-1}

On peut écrire : $a \times b = 0 \Rightarrow$

$$a^{-1} \times a \times b = a^{-1} \times 0$$

$$\Rightarrow 1 \times b = 0 \Rightarrow b = 0.$$

Exercice : soit $(K, +, \times)$ un corps fini :

$$K = \{0; e; x_1; x_2; \dots; x_m\} ; m \in \mathbb{N}^*$$

Avec : 0 (resp. e) l'élément neutre pour $+$ (resp. \times).

1) montrer que : $-e$ et e sont les seuls éléments de K qui sont égaux à leurs symétriques pour la loi \times

2) montrer que le produit de tous les éléments de K est égal à $-e$

3) on considérant le corps $(\mathbb{Z}/n\mathbb{Z}; +; \times)$ avec n

premier montrer que : $\overline{(n-1)! + 1} \equiv 0 [n]$

Solution : 1)

$$\forall x \in K - \{0\} \quad x = x^{-1} \Leftrightarrow x \times x = x^{-1} \times x \Leftrightarrow x^2 = e$$

$$\Leftrightarrow x^2 - e = 0 \Leftrightarrow x^2 - e^2 = 0 \Leftrightarrow (x - e)(x + e) = 0$$

$$\Leftrightarrow x = -e \text{ ou } x = e \text{ car } (K, +, \times) \text{ un corps}$$

2) puisque : $-e$ et e sont les seuls éléments de K qui sont égaux à leurs symétriques pour la loi \times

$$\text{Alors : } K - \{0\} = \{-e; e; a_1; a_1^{-1}; a_2; a_2^{-1} \dots; a_p; a_p^{-1}\}$$

$$\text{Donc : } -e \times e \times a_1 \times a_1^{-1} \times a_2 \times a_2^{-1} \dots \times a_p \times a_p^{-1} = -e \times e \times e \times e \dots \times e = -e$$

$$3) \mathbb{Z}/n\mathbb{Z} = \{\bar{0}; \bar{1}; \bar{2}; \dots; \overline{n-1}\} \text{ (un corps)}$$

D'après les questions précédentes on a :

$\overline{1} \times \overline{2} \times \dots \times \overline{n-1} = \overline{-1}$ donc :

$$\overline{1 \times 2 \times 3 \times \dots \times (n-1)} = \overline{-1}$$

donc : $\overline{(n-1)! + 1} \equiv 0 [n]$

Théorème : Dans un corps, tout élément de

$K - \{0\}$ est régulier pour la loi \times :

$$\forall (x; y) \in K^3 \text{ et } \forall a \in K - \{0\}$$

$$ax = ay \Rightarrow x = y \text{ et } xa = ya \Rightarrow x = y$$

Exercice8: on considère l'ensemble des matrices suivante :

$$E = \left\{ M_{(a;b)} = \begin{pmatrix} a & -2b \\ b & a \end{pmatrix} / (a;b) \in \mathbb{R}^2 \right\}$$

1) Monter que $(E; +)$ est un groupe commutatif

2) Monter que E est une partie stable de

$$(M_2(\mathbb{R}); \times)$$

3) soit f l'application qui associe à chaque

matrice $M_{(a;b)}$ de $E - \{0_2\}$ le nombre complexe :

$$a + ib\sqrt{2} \text{ de } \mathbb{C}^*$$

a) Monter que f est un morphisme bijectif de

$$(E - \{0_2\}, \times) \text{ dans } (\mathbb{C}^*; \times)$$

b) en déduire la structure de $(E - \{0_2\}, \times)$

4) Monter que $(E; +; \times)$ est un corps

Solution : 1) on a : $M_{(0;0)} = 0_2 \in E$ donc : $E \neq \emptyset$

Et on a $E \subset (M_2(\mathbb{R}); \times)$

soit $M_{(a;b)} \in E$ et $M_{(c;d)} \in E$

$$\text{Donc : } M_{(a;b)} = \begin{pmatrix} a & -2b \\ b & a \end{pmatrix} \text{ et } M_{(c;d)} = \begin{pmatrix} c & -2d \\ d & c \end{pmatrix}$$

$$M_{(a;b)} - M_{(c;d)} = \begin{pmatrix} a & -2b \\ b & a \end{pmatrix} - \begin{pmatrix} c & -2d \\ d & c \end{pmatrix} = \begin{pmatrix} a-c & -2(b-d) \\ b-d & a-c \end{pmatrix}$$

Donc : $M_{(a;b)} - M_{(c;d)} = M_{(a-c; b-d)}$

Et puisque : $(a;b;c;d) \in \mathbb{R}^4$ alors : $a-c \in \mathbb{R}$ et

$$b-d \in \mathbb{R} \text{ donc : } M_{(a;b)} - M_{(c;d)} \in E$$

Donc : $(E; +)$ est un un sous-groupe de $(M_2(\mathbb{R}); +)$

donc $(E; +)$ est un groupe commutatif

$$2) M_{(a;b)} \times M_{(c;d)} = \begin{pmatrix} a & -2b \\ b & a \end{pmatrix} \times \begin{pmatrix} c & -2d \\ d & c \end{pmatrix} =$$

$$M_{(a;b)} \times M_{(c;d)} = \begin{pmatrix} ac-2bd & -2(ad+bc) \\ ad+bc & ac-2bd \end{pmatrix} = M_{(ac-2bd; ad+bc)}$$

Et puisque : $(a;b;c;d) \in \mathbb{R}^4$ alors : $ac-2bd \in \mathbb{R}$ et

$$ad+bc \in \mathbb{R} \text{ donc : } M_{(a;b)} \times M_{(c;d)} \in E$$

E est une partie stable de $(M_2(\mathbb{R}); \times)$

3) soient : $M_{(a;b)} \in E$ et $M_{(c;d)} \in E$

$$f(M_{(a;b)} \times M_{(c;d)}) = f(M_{(ac-2bd; ad+bc)})$$

$$= ac - 2bd + i(ad + bc)\sqrt{2}$$

$$f(M_{(a;b)}) \times f(M_{(c;d)}) = (a + ib\sqrt{2})(c + id\sqrt{2})$$

$$= ac - 2bd + i(ad + bc)\sqrt{2} = f(M_{(ac-2bd; ad+bc)})$$

$$= f(M_{(a;b)} \times M_{(c;d)})$$

f est un morphisme de $(E - \{0_2\}, \times)$ dans $(\mathbb{C}^*; \times)$

Soit $x + iy \in \mathbb{C}^*$ avec $(x; y) \in \mathbb{R}^2$

On cherche $M_{(a;b)} \in E$ tel que : $f(M_{(a;b)}) = x + iy$

$$f(M_{(a;b)}) = x + iy \Leftrightarrow a + ib\sqrt{2} = x + iy$$

$$\Leftrightarrow \begin{cases} a = x \\ b\sqrt{2} = y \end{cases} \Leftrightarrow \begin{cases} a = x \\ b = \frac{y}{\sqrt{2}} \end{cases} \quad (a; b) \in \mathbb{R}^2 \text{ Existe et il}$$

est unique

donc : f est un morphisme bijectif de

$(E - \{0_2\}, \times)$ dans $(\mathbb{C}^*; \times)$

b) $(E - \{0_2\}, \times)$ et $(\mathbb{C}^*; \times)$ sont isomorphes

et $(\mathbb{C}^*; \times)$ un groupe commutatif donc aussi

et on a $(E - \{0_2\}, \times)$ un groupe commutatif

4) La multiplication est distributive par rapport à l'addition dans $M_2(\mathbb{R})$ et E est une partie stable

de $(M_2(\mathbb{R}); \times)$ donc La multiplication est

distributive par rapport à l'addition dans E

Donc on a :

$(E; +)$ est un groupe commutatif et

$(E - \{0_2\}, \times)$ un groupe commutatif

La multiplication est distributive par rapport à l'addition dans E

Conclusion :

$(E; +; \times)$ est un corps

Exercice 9: Soit $(K; +; \times)$ un corps.

On note : 0_K l'élément neutre de $(K; +)$ et 1_K

l'élément neutre de $(K; \times)$ et on suppose qu'il

existe un homomorphisme f bijectif de $(K; +)$

vers $(K - \{0_K\}; \times)$

1) on suppose que $1_K + 1_K = 0_K$

montrer que : $f(K) = \{1_K\}$

2) on suppose que : $1_K + 1_K \neq 0_K$ et on pose :

$$\alpha = f^{-1}(1_K) \text{ et } \beta = f^{-1}(-1_K)$$

a) montrer que : $\alpha + \alpha = \beta + \beta$

b) en déduire que $\alpha = \beta$

3) en déduire qu'il n'existe pas

d'homomorphisme f bijectif de $(K; +)$ vers

$(K - \{0_K\}; \times)$

Solution : 1) on suppose que $1_K + 1_K = 0_K$

soit $x \in K$ on a donc : $x \times (1_K + 1_K) = x \times 0_K$

donc : $x \times 1_K + x \times 1_K = x \times 0_K$

donc : $x + x = 0_K$ donc : $f(x + x) = f(0_K)$

puisque f homomorphisme bijectif de $(K; +)$ vers

$(K - \{0_K\}; \times)$ on a donc : $f(x) \times f(x) = 1_K$

donc : $(f(x))^2 = 1_K$ donc : $(f(x) - 1_K)(f(x) + 1_K) = 0_K$

donc : $f(x) = 1_K$ ou $f(x) = -1_K = 1_K$ car

$$1_K + 1_K = 0_K$$

donc : $\forall x \in K f(x) = 1_K$ donc : $f(K) = \{1_K\}$

2) a) on a : $1_K + 1_K \neq 0_K$ et $\alpha = f^{-1}(1_K)$ et $\beta = f^{-1}(-1_K)$

$\alpha = f^{-1}(1_K) \Leftrightarrow f(\alpha) = 1_K$ et $\beta = f^{-1}(-1_K) \Leftrightarrow f(\beta) = -1_K$

donc : $f(\alpha + \alpha) = (f(\alpha))^2 = (1_K)^2 = 1_K$

et $f(\beta + \beta) = (f(\beta))^2 = (-1_K)^2 = 1_K$

donc : $f(\alpha + \alpha) = f(\beta + \beta)$

donc : $\alpha + \alpha = \beta + \beta$ car f bijectif

b) on a : $\alpha + \alpha = \beta + \beta \Leftrightarrow (\alpha - \beta) + (\alpha - \beta) = 0_K$

$\alpha + \alpha = \beta + \beta \Leftrightarrow (\alpha - \beta) \times (1_K + 1_K) = 0_K$

$\alpha + \alpha = \beta + \beta \Leftrightarrow \alpha - \beta = 0_K$ ou $1_K + 1_K = 0_K$

$$\alpha + \alpha = \beta + \beta \Leftrightarrow \alpha - \beta = 0_K \text{ car } 1_K + 1_K \neq 0_K$$

$$\alpha + \alpha = \beta + \beta \Leftrightarrow \alpha = \beta$$

3) s'il existe un homomorphisme f bijectif de

$(K; +)$ vers $(K - \{0_K\}; \times)$ on alors deux cas :

1 cas : $1_K + 1_K = 0_K$ d'après 1) on a :

$$\forall x \in K \quad f(x) = 1_K \Leftrightarrow \forall x \in K; f(x) = f(0_K)$$

Puisque f bijectif : $\forall x \in K \quad x = 0_K$

Cad $K = \{0_K\}$ et donc : $K - \{0_K\} = \emptyset$

contradiction

2 cas : $1_K + 1_K \neq 0_K$ d'après 2) et on posons :

$$\alpha = f^{-1}(1_K) \text{ et } \beta = f^{-1}(-1_K) \text{ on trouve : } \alpha = \beta$$

Cad $f^{-1}(-1_K) = f^{-1}(1_K)$ et Puisque f^{-1} bijectif

Alors : $-1_K = 1_K$ cad $1_K + 1_K = 0_K$ contradiction

Avec le fait que $1_K + 1_K \neq 0_K$

Donc : qu'il n'existe pas d'homomorphisme f

bijectif de $(K; +)$ vers $(K - \{0_K\}; \times)$

Exercice10 :

1) On munit de la loi de composition interne

définie par : $x * y = xy + (x^2 - 1)(y^2 - 1); \forall (x; y) \in \mathbb{R}^2$

Montrer que $*$ est commutative, non associative, et que 1 est élément neutre.

2) On munit \mathbb{R}^{+*} de la loi de $*$ composition interne

définie par : $x * y = \sqrt[3]{x^2 + y^2} \quad \forall (x; y) \in \mathbb{R}^2$

Montrer que $*$ est commutative, associative, et que 0 est élément neutre. Montrer que aucun élément de \mathbb{R}^{+*} n'a de symétrique pour $*$

3) On munit \mathbb{R} de la loi de composition interne $*$

définie par : $x * y = \sqrt[3]{x^3 + y^3} \quad \forall (x; y) \in \mathbb{R}^2$

Montrer que l'application : $x \rightarrow x^3$ est un

isomorphisme de $(\mathbb{R}; *)$ vers $(\mathbb{R}; +)$ En déduire que

$(\mathbb{R}; *)$ est un groupe commutatif

Solution : 1) $x * y = xy + (x^2 - 1)(y^2 - 1)$

$$= yx + (y^2 - 1)(x^2 - 1)$$

La loi est commutative

Pour montrer que la loi n'est pas associative, il

suffit de trouver $x; y; z \in \mathbb{R}$ et tels que :

$$x * (y * z) \neq (x * y) * z$$

1 sera l'élément neutre il ne faut pas prendre 1

dans $x; y; z$ et.

Prenons, par exemple : $x = 0; y = 2; z = 3$

$$x * (y * z) = 0 * (2 * 3) = 0 * (2 \times 3 + (2^2 - 1)(3^2 - 1))$$

$$= 0 * 30 = 0 \times 30 + (0^2 - 1)(30^2 - 1) = -899$$

$$(x * y) * z = (0 * 2) * 3 = 0 * 2 + (0^2 - 1)(2^2 - 1) * 3$$

$$= -3 * 3 = 0 * 2 + ((-3)^2 - 1)(3^2 - 1) = -9 + 8^2 = 55$$

La loi n'est pas associative

$$1 * x = 1x + (1^2 - 1)(x^2 - 1) = x$$

De plus, comme la loi est commutative

$$x * 1 = 1 * x$$

On a bien $x * 1 = 1 * x = x$, 1 est l'élément neutre.

$$x * y = \sqrt{x^2 + y^2} = \sqrt{y^2 + x^2} = y * x$$

La loi est commutative.

$$(x * y) * z = (\sqrt{x^2 + y^2}) * z = (\sqrt{x^2 + y^2}) * z = \sqrt{(\sqrt{x^2 + y^2})^2 + z^2}$$

$$(x * y) * z = \sqrt{x^2 + y^2 + z^2}$$

En reprenant le calcul ci-dessus en changeant

$$\text{en } (x; y; z) \text{ en } (y; z; x) \quad (y * z) * x = \sqrt{y^2 + z^2 + x^2}$$

Comme $*$ est commutative :

$(y * z) * x = x * (y * z)$ Et finalement :

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

La loi est associative.

Remarque : On aurait pu calculer directement

$$x * (y * z)$$

$$0 * x = \sqrt{0^2 + x^2} = |x| \text{ car } x \geq 0$$

Comme $*$ est commutative : $0 * x = x * 0 = x$

0 est l'élément neutre.

Supposons x qu'admette un symétrique y

$$x * y = 0 \Leftrightarrow \sqrt{x^2 + y^2} = |x| \Leftrightarrow x^2 + y^2 = 0 \Leftrightarrow x + y = 0$$

Or $x > 0$ et $y > 0$ donc : $x * y = 0$ est impossible,

pour tout $x > 0$ x n'a pas de symétrique.

3) On pose $\rho(x) = x^3$ ET $\rho'(x) > 0$ pour tout

$x \neq 0$ et est nul en 0, ρ est une fonction

strictement croissante \mathbb{R} de sur \mathbb{R} , ρ est une

bijection de \mathbb{R} sur \mathbb{R} . Il reste à montrer qu'il s'agit d'un morphisme.

$$\rho(x * y) = (x * y)^3 = \left(\sqrt[3]{x^3 + y^3}\right)^3 = x^3 + y^3 = \rho(x) + \rho(y)$$

ρ est un morphisme de $(\mathbb{R}; *)$ dans $(\mathbb{R}; +)$ et

donc un isomorphisme de $(\mathbb{R}; *)$ dans $(\mathbb{R}; +)$

(puisque ρ est bijective).

ρ^{-1} est un isomorphisme de $(\mathbb{R}; +)$ dans $(\mathbb{R}; *)$

donc un morphisme, $(\mathbb{R}; +)$ est un groupe commutatif

et l'image d'un groupe commutatif par un morphisme de groupe est un groupe.

$(\mathbb{R}; *)$ est un groupe.

Exercice 11 : on considère l'ensemble des matrices suivante :

$$G = \left\{ M_{(a;b)} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} / a^2 + b^2 = 1 \text{ et } (a;b) \in \mathbb{R}^2 \right\}$$

1) Monter que : $G \neq \emptyset$

2) Monter que : $G = \left\{ \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix} / \theta \in \mathbb{R} \right\}$

3) Monter que G est une partie stable de

$$(M_2(\mathbb{R}); \times)$$

4) est ce que G est une partie stable de

$$(M_2(\mathbb{R}); +) ?$$

5) on pose : $M(\theta) = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}$

calculer $M^n(\theta) \forall n \in \mathbb{N}^*$

$$\text{ou : } M^n(\theta) = \underbrace{M(\theta) \times M(\theta) \times \dots \times M(\theta)}_{n \text{ fois}}$$

6) soit f l'application de \mathbb{R} dans G tel que :

$$f(\theta) = M(\theta)$$

a) Monter que f est un morphisme surjectif de

$$(\mathbb{R}; +) \text{ dans } (G; \times)$$

b) en déduire la structure de $(G; \times)$

7) soit l'ensemble : $U = \{z \in \mathbb{C} / |z| = 1\}$

a) Monter que : $U = \{e^{i\theta} / \theta \in \mathbb{R}\}$

b) Monter que $(U; \times)$ est un groupe commutatif

Solution : 1) on a : $M_{(1;0)} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$ et $0^2 + 1^2 = 1$

donc : $G \neq \emptyset$

2)

$$M \in G \Leftrightarrow \exists (a;b) \in \mathbb{R}^2 / M = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \text{ et } a^2 + b^2 = 1$$

$$\exists \theta \in \mathbb{R} / a = \cos \theta \text{ et } b = \sin \theta$$

$$\text{Donc : } M \in G \Leftrightarrow \exists \theta \in \mathbb{R} / M = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}$$

$$G = \left\{ \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix} / \theta \in \mathbb{R} \right\}$$

3) soit : $M_1 = \begin{pmatrix} \cos \theta_1 & -\sin \theta_1 \\ \sin \theta_1 & \cos \theta_1 \end{pmatrix}$ et $M_2 = \begin{pmatrix} \cos \theta_2 & -\sin \theta_2 \\ \sin \theta_2 & \cos \theta_2 \end{pmatrix}$

Deux éléments de G

$$M_1 \times M_2 = \begin{pmatrix} \cos \theta_1 & -\sin \theta_1 \\ \sin \theta_1 & \cos \theta_1 \end{pmatrix} \begin{pmatrix} \cos \theta_2 & -\sin \theta_2 \\ \sin \theta_2 & \cos \theta_2 \end{pmatrix}$$

$$= \begin{pmatrix} \cos \theta_1 \cos \theta_2 - \sin \theta_1 \sin \theta_2 & -\cos \theta_1 \sin \theta_2 - \sin \theta_1 \cos \theta_2 \\ \sin \theta_1 \cos \theta_2 + \cos \theta_1 \sin \theta_2 & -\sin \theta_1 \sin \theta_2 - \cos \theta_1 \cos \theta_2 \end{pmatrix}$$

$$M_1 \times M_2 = \begin{pmatrix} \cos(\theta_1 + \theta_2) & -\sin(\theta_1 + \theta_2) \\ \sin(\theta_1 + \theta_2) & \cos(\theta_1 + \theta_2) \end{pmatrix}$$

Donc : $M_1 \times M_2 \in G$

Donc G est une partie stable de $(M_2(\mathbb{R}); \times)$

4) on a ; $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$ et $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I_2$

Deux éléments de G

Et puisque : $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \notin G$

Car $0^2 + 0^2 = 0 \neq 1$

Donc G n'est pas une partie stable de $(M_2(\mathbb{R}); +)$

5) on pose : $M(\theta) = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}$

Calculons : $M^n(\theta)$

$$M^2(\theta) = M(\theta) \times M(\theta) = \begin{pmatrix} \cos 2\theta & -\sin 2\theta \\ \sin 2\theta & \cos 2\theta \end{pmatrix}$$

Montrons que :

$$M^n(\theta) = \begin{pmatrix} \cos n\theta & -\sin n\theta \\ \sin n\theta & \cos n\theta \end{pmatrix} = M(n\theta)$$

par récurrence sur \mathbb{N}^*

a) on a : $M^1(\theta) = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix} = M(1\theta)$

la ptté est vraie pour $n=1$

b) on suppose que :

$$M^n(\theta) = \begin{pmatrix} \cos n\theta & -\sin n\theta \\ \sin n\theta & \cos n\theta \end{pmatrix} = M(n\theta)$$

c) montrons que :

$$M^{n+1}(\theta) = \begin{pmatrix} \cos(n+1)\theta & -\sin(n+1)\theta \\ \sin(n+1)\theta & \cos(n+1)\theta \end{pmatrix} = M((n+1)\theta) ?$$

$$M^{n+1}(\theta) = M(\theta) M^n(\theta) = \begin{pmatrix} \cos n\theta & -\sin n\theta \\ \sin n\theta & \cos n\theta \end{pmatrix} \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}$$

$$= \begin{pmatrix} \cos(n\theta + \theta) & -\sin(n\theta + \theta) \\ \sin(n\theta + \theta) & \cos(n\theta + \theta) \end{pmatrix} = M((n+1)\theta)$$

Donc : $\forall n \in \mathbb{N}^* \quad M^n(\theta) = M(n\theta)$

6)a) Soit $(\theta_1; \theta_2) \in \mathbb{R}^2$

On a : $f(\theta_1 + \theta_2) = M(\theta_1 + \theta_2) = M(\theta_1) \times M(\theta_2)$

donc : $f(\theta_1 + \theta_2) = f(\theta_1) \times f(\theta_2)$

donc : f est un morphisme de $(\mathbb{R}; +)$ dans $(G; \times)$

et on a : $\forall M \in G \quad \exists \theta \in \mathbb{R} / f(\theta) = M(\theta)$

donc f est un morphisme surjectif de $(\mathbb{R}; +)$ dans

$(G; \times)$

6)b) puisque f est un morphisme surjectif de

$(\mathbb{R}; +)$ dans $(G; \times)$ on a $f(G) = \mathbb{R}$ et on a aussi

$(\mathbb{R}; +)$ est un groupe commutatif alors aussi

$(G; \times)$ est un groupe commutatif

7) a) Montrons que : $U = \{e^{i\theta} / \theta \in \mathbb{R}\} ?$

Soit $z \in \mathbb{C}$ alors $z = a + ib$ avec $(a; b) \in \mathbb{R}^2$

$$z \in U \Leftrightarrow |z| = 1 \Leftrightarrow |a + ib| = 1$$

$$z \in U \Leftrightarrow a^2 + b^2 = 1$$

$$\Leftrightarrow \exists \theta \in \mathbb{R} / a = \cos \theta \text{ et } b = \sin \theta \text{ et } z = a + ib$$

$$z \in U \Leftrightarrow \exists \theta \in \mathbb{R} : z = \cos \theta + i \sin \theta = e^{i\theta}$$

$$\text{Donc : } U = \{e^{i\theta} / \theta \in \mathbb{R}\}$$

b) Montrons que $(U; \times)$ est un sous-groupe de $(\mathbb{C}^*; \times)$

on a $U \subset \mathbb{C}^*$ et $U \neq \emptyset$ car $1 \in U$

Soient $z_1 \in U$ et $z_2 \in U$ montrons que

$$z_1 \times z_2^{-1} \in U ?$$

$$z_1 \in U \Leftrightarrow \exists \theta_1 \in \mathbb{R} : z_1 = e^{i\theta_1}$$

$$z_2 \in U \Leftrightarrow \exists \theta_2 \in \mathbb{R} : z_2 = e^{i\theta_2}$$

$$\text{On a : } z_1 \times z_2^{-1} = e^{i\theta_1} \times (e^{i\theta_2})^{-1} = e^{i\theta_1} \times e^{-i\theta_2} = e^{i(\theta_1 - \theta_2)}$$

$$\text{Avec } \theta_1 - \theta_2 \in \mathbb{R} \text{ donc : } z_1 \times z_2^{-1} \in U$$

Donc : $(U; \times)$ est un un sous-groupe de $(\mathbb{C}^*; \times)$

Et puisque $(\mathbb{C}^*; \times)$ est commutatif

Alors : $(U; \times)$ est un groupe commutatif

$$2) M_{(a;b)} \times M_{(c;d)} = \begin{pmatrix} a & -2b \\ b & a \end{pmatrix} \times \begin{pmatrix} c & -2d \\ d & c \end{pmatrix} =$$

$$M_{(a;b)} \times M_{(c;d)} = \begin{pmatrix} ac - 2bd & -2(ad + bc) \\ ad + bc & ac - 2bd \end{pmatrix} = M_{(ac-2bd; ad+bc)}$$

Et puisque : $(a; b; c; d) \in \mathbb{R}^4$ alors : $ac - 2bd \in \mathbb{R}$ et

$$ad + bc \in \mathbb{R} \text{ donc : } M_{(a;b)} \times M_{(c;d)} \in E$$

E est une partie stable de $(M_2(\mathbb{R}); \times)$

3) soient : $M_{(a;b)} \in E$ et $M_{(c;d)} \in E$

$$f(M_{(a;b)} \times M_{(c;d)}) = f(M_{(ac-2bd; ad+bc)})$$

$$= ac - 2bd + i(ad + bc)\sqrt{2}$$

$$f(M_{(a;b)}) \times f(M_{(c;d)}) = (a + ib\sqrt{2})(c + id\sqrt{2})$$

$$= ac - 2bd + i(ad + bc)\sqrt{2} = f(M_{(ac-2bd; ad+bc)})$$

$$= f(M_{(a;b)} \times M_{(c;d)})$$

f est un morphisme de $(E - \{0_2\}, \times)$ dans $(\mathbb{C}^*; \times)$

Soit $x + iy \in \mathbb{C}^*$ avec $(x; y) \in \mathbb{R}^2$

On cherche $M_{(a;b)} \in E$ tel que : $f(M_{(a;b)}) = x + iy$

$$f(M_{(a;b)}) = x + iy \Leftrightarrow a + ib\sqrt{2} = x + iy$$

$$\Leftrightarrow \begin{cases} a = x \\ b\sqrt{2} = y \end{cases} \Leftrightarrow \begin{cases} a = x \\ b = \frac{y}{\sqrt{2}} \end{cases} \quad (a; b) \in \mathbb{R}^2 \text{ Existe et il}$$

est unique

donc : f est un morphisme bijectif de

$(E - \{0_2\}, \times)$ dans $(\mathbb{C}^*; \times)$

b) $(E - \{0_2\}, \times)$ et $(\mathbb{C}^*; \times)$ sont isomorphes

et $(\mathbb{C}^*; \times)$ un groupe commutatif donc aussi

et on a $(E - \{0_2\}, \times)$ un groupe commutatif

4) La multiplication est distributive par rapport à l'addition dans $M_2(\mathbb{R})$ et E est une partie stable

de $(M_2(\mathbb{R}); \times)$ donc La multiplication est

distributive par rapport à l'addition dans E

Donc on a :

$(E; +)$ est un groupe commutatif et

$(E - \{0_2\}, \times)$ un groupe commutatif

La multiplication est distributive par rapport à l'addition dans E

Conclusion : $(E; +; \times)$ est un corps

Exercice 12: Soit $(A; +; \times)$ un anneau.

Et 1_A est l'élément neutre de $(A; \times)$

soient : $a \in A$ et $b \in A$ tels que :

$$a) ab + ba = 1_A$$

$$b) a^2b + ba^2 = a$$

$$1) \text{montrer que : } a^2b = ba^2$$

$$2) \text{montrer que : } aba + aba = a$$

$$3) \text{en déduire que : } ab = ba$$

$$\text{Solution : } 1) \text{on a : } a^2b + ba^2 = a$$

$$\text{donc : } a^2b + ba^2 = a1_A$$

$$\text{donc : } a^2b + ba^2 = a(ab + ba)$$

$$\text{donc : } a^2b + ba^2 = a^2b + aba$$

$$\text{donc : } ba^2 = aba(1)$$

$$\text{et on a : } a^2b + ba^2 = a = 1_A a$$

$$\text{donc : } a^2b + ba^2 = (ab + ba)a$$

$$\text{donc : } a^2b + ba^2 = aba + ba^2$$

$$\text{donc : } a^2b = aba(2)$$

$$\text{de (1) et (2) en déduit que : } a^2b = ba^2$$

$$2) \text{d'après ce qui précède on a :}$$

$$ba^2 = aba \text{ et } a^2b = aba$$

$$\text{Donc : } aba + aba = a^2b + ba^2 \text{ et d'après b) on a}$$

$$aba + aba = a$$

$$3) \text{on a : } (ab)(ab) = abab = (aba)b = (ba^2)b$$

$$(ba)(ba) = baba = b(aba) = b(a^2b)$$

$$(\text{Car : } aba = a^2b)$$

$$\text{Et on a : } (ab)(ab) = (1_A - ba)(1_A - ba)$$

$$(ab)(ab) = 1_A - ba - ba + (ba)(ba)$$

$$\text{Donc : } ba^2b = 1_A - ba - ba + ba^2b$$

$$\text{Car : } (ab)(ab) = (ba)(ba) = ba^2b$$

$$\text{Donc : } ba + ba = 1_A \text{ et puisque : } ba + ab = 1_A$$

$$\text{Alors : } ab = ba$$

Exercice13: Soit $(K; +; \times)$ un corps.

On note : 1_K l'élément neutre de $(K; \times)$

Soient x et y deux éléments de $K - \{0_K\}$

Qui vérifient les conditions suivantes :

$$a) x + y = 1_K \quad b) x^{-1} + y^{-1} = 1_K$$

avec : x^{-1} le symétrique de x pour la loi \times

$$1) \text{montrer que : } xy = yx = -1_K$$

$$2) \text{montrer que : } x^4 + y^4 = 7 \cdot 1_K$$

$$\text{Avec : } 7 \cdot 1_K = \underbrace{1_K + 1_K + \dots + 1_K}_{7 \text{ fois}}$$

Solution : 1) Soient x et y deux éléments de

$$K - \{0_K\} \text{ on a : } xy = x(x^{-1} + y^{-1})y$$

$$xy = xx^{-1}y + xy^{-1}y = y + x = -1_K$$

$$\text{Donc : } xy = yx = -1_K$$

$$2) \text{on a : } 1_K = (x + y)^2 = x^2 + xy + yx + y^2$$

$$1_K = x^2 - 1_K - 1_K + y^2$$

$$\text{Donc : } x^2 + y^2 = 3 \cdot 1_K$$

$$\text{Donc : } 9 \cdot 1_K = (x^2 + y^2)^2$$

$$\text{Donc : } 9 \cdot 1_K = x^4 + x^2y^2 + y^2x^2 + y^4$$

$$\text{Donc : } 9 \cdot 1_K = x^4 + 1_K + 1_K + y^4$$

$$\text{Donc : } x^4 + y^4 = 7 \cdot 1_K$$

« C'est en forgeant que l'on devient forgeron »

Dit un proverbe.

C'est en s'entraînant régulièrement aux calculs et exercices Que l'on devient un mathématicien

