Corrigé TD 1

Soit $E = \{1, 2, 3\}$.

Calculer $\mathcal{P}(E)$.

But : Donner tous les sous-ensembles de E

Rappel : Si E est un ensemble à n éléments alors $\mathcal{P}(E)$ possède 2^n éléments

$$\mathcal{P}(E) = \{ \emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\} \}$$

On retrouve bien que le cardinal de $\mathcal{P}(E)$ est $8 = 2^3$

(2^3 : le nombre d'éléments)

Exercice n°1

Soient E et F deux ensembles.

1) Montrer que $\underbrace{\mathcal{P}(E \cap F)}_{\text{ensemble}} = \underbrace{\mathcal{P}(E) \cap \mathcal{P}(F)}_{\text{ensemble}}$

Pour montrer une égalité entre ensemble, on montrer que TOUT éléments du premier ensemble est inclu dans et inversement :

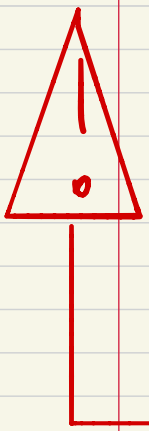
$$A = B \iff \begin{cases} \cdot\ \forall x \in A : x \in B \\ \cdot\ \forall x \in B : x \in A \end{cases}$$

- Soit $X \in \mathcal{P}(E \cap F)$ Alors $X \subset E \cap F$

donc $X \subset E$ et $X \subset F$

donc $X \in \mathcal{P}(E)$ et $X \in \mathcal{P}(F)$

donc $X \in \mathcal{P}(E) \cap \mathcal{P}(F)$. Ainsi, $\mathcal{P}(E \cap F) \subset \mathcal{P}(E) \cap \mathcal{P}(F)$



$A \in \mathcal{P}(E) \iff A$ est un sous ensemble de E

$\iff A \subset E$

- Montrons que $\mathcal{P}(E) \cap \mathcal{P}(F) \subset \mathcal{P}(E \cap F)$

Soit $X \in \mathcal{P}(E) \cap \mathcal{P}(F)$.

Alors $X \in \mathcal{P}(E)$ et $X \in \mathcal{P}(F)$

donc $X \subset E$ et $X \subset F$

donc $X \subset E \cap F$, donc $X \in \mathcal{P}(E \cap F)$

On a montré que $\boxed{\mathcal{P}(E) \cap \mathcal{P}(F) \subset \mathcal{P}(E \cap F)}$

On aurait pu raisonner par "équivalence" :

$X \in \mathcal{P}(E \cap F) \iff X \subset E \cap F$

$\iff X \subset E$ et $X \subset F$

$\iff X \in \mathcal{P}(E)$ et $X \in \mathcal{P}(F)$

$\iff X \in \mathcal{P}(E) \cap \mathcal{P}(F)$

donc $\mathcal{P}(E \cap F) = \mathcal{P}(E) \cap \mathcal{P}(F)$

2) Montrer que $\mathcal{P}(E) \cup \mathcal{P}(F) \subset \mathcal{P}(E \cup F)$

Soit $X \in \mathcal{P}(E) \cup \mathcal{P}(F)$.

Alors $X \in \mathcal{P}(E)$ ou $X \in \mathcal{P}(F)$

donc $X \subset E$ ou $X \subset F$

donc $X \subset E \cup F$ donc $X \in \mathcal{P}(E \cup F)$

Donc on a montré que :

$$\mathcal{P}(E) \cup \mathcal{P}(F) \subset \mathcal{P}(E \cup F)$$

3) Montrons que en général :

$$\mathcal{P}(E \cup F) \not\subset \mathcal{P}(E) \cup \mathcal{P}(F)$$

Posons : $\begin{cases} E = \{1\} \\ F = \{2, 3\} \end{cases}$

alors $E \cup F = \{1, 2, 3\}$

alors $\begin{cases} \mathcal{P}(E) = \{\emptyset, \{1\}\} \\ \mathcal{P}(F) = \{\emptyset, \{2\}, \{3\}, \{2, 3\}\} \\ \mathcal{P}(E \cup F) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{2, 3\}, \{1, 3\}, \{1, 2\}, \{1, 2, 3\}\} \\ \mathcal{P}(E) \cup \mathcal{P}(F) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{2, 3\}\} \end{cases}$

Mais $\{1,2\} \in \mathcal{P}(E \cup F)$ et $\{1,2\} \notin \mathcal{P}(E) \cup \mathcal{P}(F)$

ce qui veut dire que tous les éléments de $\mathcal{P}(E \cup F)$ ne sont pas inclus dans $\mathcal{P}(E) \cup \mathcal{P}(F)$:

$$\mathcal{P}(E \cup F) \not\subset \mathcal{P}(E) \cup \mathcal{P}(F)$$

Exercice n° 2

On définit sur $\mathbb{R}$ la relation :

$\forall x \in \mathbb{R}, \forall y \in \mathbb{R} : (x \mathcal{R} y) \Leftrightarrow x^3 - y^3 = x - y$

1) Montrer que $\mathcal{R}$ est une relation d'équivalence

Rappel : $\mathcal{R}$ est une relation d'équivalence sur un ensemble X si :

1) $\forall x \in X : \quad x \mathcal{R} x$ (Reflexif)
2) $\forall x, y \in X : \quad x \mathcal{R} y \Leftrightarrow y \mathcal{R} x$ (Symétrie)

3) $\forall x, y, z \in X$,

$(x R y \text{ et } y R z) \Longrightarrow (x R z)$ (Transitif)

- **Reflexivité** : Soit $x \in \mathbb{R}$.

Il faut prouver que $x R x$ c'est-à-dire que : $x^3 - x^3 = x - x$

ce qui est vrai ! $\left.\begin{array}{l} x^3 - x^3 = 0 \\ x - x = 0 \end{array}\right\}$ donc : $x^3 - x^3 = x - x$

donc $x R x$

- **Symétrie** : Soient $x, y \in \mathbb{R}$.

Il faut prouver que $x \mathcal{R} y \Leftrightarrow y \mathcal{R} x$

Par définition : $\begin{cases} x \mathcal{R} y \Leftrightarrow x^3 - y^3 = x - y \\ y \mathcal{R} x \Leftrightarrow y^3 - x^3 = y - x \end{cases}$

Or : $x^3 - y^3 = x - y \Leftrightarrow y^3 - x^3 = y - x$

donc $x \mathcal{R} y \Leftrightarrow y \mathcal{R} x$

- **Transitivité** : Soient $x, y, z \in \mathbb{R}$.

Supposons que $x \mathcal{R} y$ et $y \mathcal{R} z$

Alors $x^3 - y^3 = x - y$ et $y^3 - z^3 = y - z$

Donc, en sommant les deux égalitées :

$$x^3 - z^3 = x - z .$$

donc $x \mathcal{R} z$

2) Déterminer l'ensemble quotient :

$$\mathbb{R}/\mathcal{R}$$

Rappel : Soit X un ensemble et $\mathcal{R}$ une relation d'équivalence.

Soit $x \in X$. Alors

- $cl(x) := \{ y \in X, \ x \mathcal{R} y \}$
- $X/\mathcal{R} := \{ cl(x), \ x \in X \}$

(Par exemple, si $X = \{1, 2, 3\}$ alors

$$X/\mathcal{R} = \{ cl(1), cl(2), cl(3) \}$$
)

Pour déterminer $\mathbb{R}/_{\mathcal{R}}$, on fixe $x \in \mathbb{R}$ et on détermine $cl(x)$.

Soit $x \in \mathbb{R}$.

But : déterminer $cl(x) = \{ y \in \mathbb{R}, x \mathcal{R} y \}$

c'est-à-dire déterminer tous les $y \in \mathbb{R}$ tq : $x \mathcal{R} y$

Il faut donc résoudre l'équation d'inconnue $y \in \mathbb{R}$: $x^3 - y^3 = x - y$.

Rappel : $\forall n \in \mathbb{N}^*, \forall x, y \in \mathbb{R}$:

$$x^n - y^n = (x-y) \times \sum_{k=0}^{n-1} x^k \cdot y^{n-1-k}$$

Preuve .

- Si $x = y$: OK
- Si $x \neq y$,

$$\frac{x^n - y^n}{x - y} = \frac{y^n \left(\left(\frac{x}{y}\right)^n - 1\right)}{y\left(\frac{x}{y} - 1\right)} = \frac{y^{n-1} \cdot \left(1 - \left(\frac{x}{y}\right)^n\right)}{1 - \frac{x}{y}}$$

Rappel : $\forall n \in \mathbb{N}^*, \forall q \in \mathbb{R} \setminus \{1\}$:

$$\sum_{k=0}^{n-1} q^k = \frac{1 - q^n}{1 - q}$$

Donc : $$\frac{x^n - y^n}{x - y} = y^{n-1} \sum_{k=0}^{n-1} \left(\frac{x}{y}\right)^k$$

(Rappel avec $q = \frac{x}{y} \neq 1$ car $x \neq y$)

$$= \sum_{k=0}^{n-1} x^k \cdot y^{n-1-k}.$$

On a donc : $x^3 - y^3 = (x - y)(x^2 + xy + y^2)$

$= x - y$

Ici, $y = x$ est solution. On cherche donc les $y \in \mathbb{R}$ avec $y \neq x$ qui sont solutions.

On a : $(x - y)(x^2 + xy + y^2) = x - y$.

En divisant par $x - y$ $(x \neq y)$ on a :

$$x^2 + xy + y^2 = 1$$

$$\Leftrightarrow 1y^2 + xy + x^2 - 1 = 0$$

$$\Delta = -3x^2 + 4$$

Le signe de Δ dépend donc de x.

x	$-\infty$		$-\frac{2}{\sqrt{3}}$		$\frac{2}{\sqrt{3}}$		$+\infty$
Δ		$-$	0	$+$	0	$-$	

- 1er cas : Si $x = -\frac{2}{\sqrt{3}}$

alors $\Delta = 0$ donc une unique solution : $y_0 = -\frac{b}{2a} = -\frac{x}{2}$

donc $y_0 = \frac{-x}{2} = \frac{1}{\sqrt{3}}$

- 2ème cas : Si $x = \frac{2}{\sqrt{3}}$ alors une unique solution $y_0 = -\frac{1}{\sqrt{3}}$

- 3ème cas : Si $x \in \left]-\frac{2}{\sqrt{3}}, \frac{2}{\sqrt{3}}\right[$ alors

$\Delta > 0$ donc deux solutions :

$$\begin{cases} y_1 = \dfrac{-b - \sqrt{\Delta}}{2a} = \dfrac{-x - \sqrt{-3x^2+4}}{2} \end{cases}$$

$$\left| y_2 = \frac{-b + \sqrt{\Delta}}{2a} = \frac{-x + \sqrt{-3x^2 + 4}}{2} \right.$$

- 1ère cas : Si $x \in]-\infty, -\frac{2}{\sqrt{3}}[\cup]\frac{2}{\sqrt{3}}, +\infty[$

alors $\Delta < 0$ donc pas de solutions !

Donc : $\mathbb{R}/\mathcal{R} = \dots$

Corrigé TD 1 (suite)

Exercice n°3

Soit $n \in \mathbb{N}^*$

$$\forall x, y \in \mathbb{Z} : \quad (x R y) \iff n \text{ divise } (x - y)$$

Rappel : Soient a et $b \in \mathbb{Z}$. On dit que a divise b, notée $a \mid b$ si :

$\exists k \in \mathbb{Z}, \quad b = a \times k$

1) • Réflexivité : Soit $x \in \mathbb{Z}$. Il faut montrer que $x \mathcal{R} x$ c'est-à-dire que

$$n \mid x - x .$$

$x - x = 0 = k \times 0$ avec $k = 0 \in \mathbb{Z}$

(Donc $\exists k \in \mathbb{Z}, \quad x - x = n \times k$)

- Symétrie : Soit $x, y \in \mathbb{Z}$ tel que xRy. Montrons que yRx.

Puisque xRy alors $\exists k \in \mathbb{Z}$:

$$x - y = n \cdot k$$

Donc en posant $k' := -k \in \mathbb{Z}$

on a : $$y - x = n \cdot k'$$

Donc yRx.

• Transitivité : Soient $x, y, z \in \mathbb{Z}$

tels que $x R y$ et $y R z$. Montrons que $x R z$. Il existe $(k_1, k_2) \in \mathbb{Z}^2$ tel que :

$$\begin{cases} x - y = n k_1 \\ y - z = n k_2 \end{cases}$$

En sommant et en posant $k := \underbrace{k_1 + k_2}_{\in \mathbb{Z}}$

on obtient : $x - z = n k$

Donc $x R z$.

2)

Rappel : Soit R une relation d'équivalence sur X.

- On dit R est compatible avec la somme si

$\forall x, y, z, t \in X$:

$$\begin{cases} x R y \\ z R t \end{cases} \Rightarrow (x+z) R (y+t)$$

et compatible par produit si $\forall x, y, z, t \in X$:

$$\begin{cases} x \, R \, y \\ z \, R \, t \end{cases} \Rightarrow (x \times z) \, R \, (y \times t)$$

2) • Supposons que $n \mid x - y$ et $n \mid z - t$.

Montrons que : $n \mid (x + z) - (y + t)$.

On sait qu'il existe $(k_1, k_2) \in \mathbb{Z}^2$ tq

$$\begin{cases} x - y = n \cdot k_1 \\ z - t = n \cdot k_2 \end{cases}$$

Donc :

$$(x+z)-(y+t) = (x-y)+(z-t)$$
$$= n\cdot k_1 + n\cdot k_2$$
$$= n\,k$$

on pose $k := k_1 + k_2 \in \mathbb{Z}$

- Montrons que : $n \mid xz - yt$.

Indication : Exprimer $(x-y)(z-t)$ en fonction de $xz - yt$

Autre méthode

$$xz - yt = \dots = n\times(\underbrace{\dots}_{\in \mathbb{Z}})$$

$x = nk_1 + y$ $\quad z = nk_2 + t$

$(x-y)(z-t) = xz - xt - yz + yt$

$(x-y) = n\cdot k_1$ $\quad (z-t) = n\cdot k_2$

$= [xz - yt] + 2yt - xt - yz$

Or ,

$$2yt - xt - yz = (yt - xt) + (yt - yz)$$

$$= t(y-x) + y(t-z)$$

$$= -tnk_1 - nyk_2$$

Donc : $xz - yt = n^2 k_1 k_2 + tnk_1 + nyk_2$

$$= n\underbrace{\left(nk_1k_2 + tk_1 + yk_2\right)}_{:= k}$$

3) Déterminer l'ensemble quotient $\mathbb{Z}/R$.

Soit $x \in \mathbb{Z}$. But : déterminer $cl(x)$.

$$cl(x) := \{ y \in \mathbb{Z} , \; x R y \}$$

Soit $y \in cl(x)$. Alors $x R y$ donc

$n \mid x - y$ donc $\exists k \in \mathbb{Z} : x - y = n.k$

donc $y = x - n.k$

Ainsi :

$$cl(x) = \{ y \in \mathbb{Z} : \exists k \in \mathbb{Z} : y = nk + x \}$$

en effet :

$$\{ y \in \mathbb{Z}, \exists k \in \mathbb{Z} : y = nk + x \} = \{ y \in \mathbb{Z}, \exists k' \in \mathbb{Z}, y = -nk' + x \}$$

A

B

$cl(x)$ = L'ensemble des éléments dont le reste dans la division euclidienne par n vaut x

Rappel : La division euclidienne de a par b veut dire : $\exists (q, r) \in \mathbb{Z}^* \times \mathbb{Z}$

tq :
$$\begin{cases} a = bq + r \\ 0 \leq r < b \end{cases}$$

$$\mathbb{Z}/_{R} = \left\{ \left\{ y \in \mathbb{Z},\ \exists k \in \mathbb{Z} : y = nk + x \right\},\ x \in \mathbb{Z} \right\}$$

$$= \left\{ \left\{ nk + x,\ k \in \mathbb{Z} \right\},\ x \in \mathbb{Z} \right\}$$

Exercice n°4

1) $\forall (a,b) \in \mathbb{Z} \times \mathbb{Z}^*$, $\forall (c,d) \in \mathbb{Z} \times \mathbb{Z}^*$:

$$(a,b)\, \mathcal{R}\, (c,d) \iff ad = bc$$

- **Réflexivité** : $(a,b)\, \mathcal{R}\, (a,b)$ car $ab = ba$ (car $(\mathbb{Z}^*, \times)$ est commutatif.)

- **Symétrie** : Supposons que $(a,b)\, \mathcal{R}\, (c,d)$

alors $ad = bc$.

donc $cb = da$ donc $(c,d)\,R\,(a,b)$

- Transitivité : Supposons que :

$$\begin{cases} (a,b)\,R\,(c,d) \\ (c,d)\,R\,(e,f) \end{cases} \quad \text{càd} : \quad \begin{cases} ad = bc \\ cf = de \end{cases}$$

Montrons que : $(a,b)\,R\,(e,f)$ càd : $af = be$

$afd = bcf = bde$ donc en divisant

$ad = bc$ $\quad$ $cf = de$

par $d \neq 0$, on a : $af = be$

(On alors : $af = \frac{bcf}{d} = be$ $\quad$ $a = \frac{bc}{d}$ $\quad$ $cf = de$)

2)

$$\varphi : \quad \mathbb{Z}\times\mathbb{Z}^*/\mathcal{R} \longrightarrow \mathbb{Q}$$

$$x \longmapsto ?$$

Si $x \in \mathbb{Z}\times\mathbb{Z}^*/\mathcal{R}$ alors $\exists (a,b) \in \mathbb{Z}\times\mathbb{Z}^*$:

$$x = cl(a,b)$$

$$\left(\text{car} \quad \mathbb{Z}\times\mathbb{Z}^*/\mathcal{R} = \left\{ cl(x) \,,\, x \in \mathbb{Z}\times\mathbb{Z}^* \right\} \right)$$

$$= \{ d(a,b) \ , \ (a,b) \in \mathbb{Z} \times \mathbb{Z}^* \})$$

On pose $\varphi(x) := \frac{a}{b}$.

Rappel : Soient A et B deux ensembles et $f : A \to B$ une application. On dit que f est bien définie si :

$\forall a,b \in A$: $(a = b) \implies (f(a) = f(b))$

But : montrer que :

$$\forall\, x, y \in \mathbb{Z} \times \mathbb{Z}^* / \mathcal{R} \quad :$$

$$(x = y) \implies \varphi(x) = \varphi(y)$$

Fixons x et y dans $\mathbb{Z} \times \mathbb{Z}^* / \mathcal{R}$ tel que $x = y$. Montrons que $\varphi(x) = \varphi(y)$.

Comme $x \in \mathbb{Z} \times \mathbb{Z}^* / \mathcal{R}$ alors $\exists (a,b) \in \mathbb{Z} \times \mathbb{Z}^*$

tel que $x = cl(a,b)$

De même, $y \in \mathbb{Z} \times \mathbb{Z}^* / \mathcal{R}$ alors $\exists (c,d) \in \mathbb{Z} \times \mathbb{Z}^*$

tel que : $y = cl(c,d)$

Rappel : Soit X un ensemble et $\mathcal{R}$ une relation d'équivalence sur X. Alors, $\forall u, v \in X$:

$u \mathcal{R} v \iff cl(u) = cl(v)$

Puisque $x = y$ alors $d(a,b) = d(c,d)$

donc d'après le Rappel : $(a,b) \mathcal{R} (c,d)$

c'est-à-dire que : $ad = bc$

donc $\frac{a}{b} = \frac{c}{d}$. Ainsi

↑ car $b \neq 0$ et $d \neq 0$

$$\varphi(x) = \varphi\left(cl(a,b)\right) := \frac{a}{b} = \frac{c}{d}$$

$$= \varphi\left(cl(c,d)\right)$$

$$=: \varphi(y)$$

On a montré que $\forall x, y \in \mathbb{Z} \times \mathbb{Z}^* / \mathcal{R}$:

$$(x = y) \implies \varphi(x) = \varphi(y)$$

Rappel : Soient X, Y deux ensembles et $f : X \to Y$, on dit que :

① f est injective si : $\forall x, x' \in X$:

$$\left(f(x) = f(x') \right) \Rightarrow x = x'$$

② f surjective si : $\forall y \in Y$, $\exists x \in X$ tel que : $y = f(x)$

③ f est bijective si elle est injective ET

surjective.

- Montrons que φ est injective.

Soient $x, y \in \mathbb{Z} \times \mathbb{Z}^*/\mathcal{R}$ tels que :

$$\varphi(x) = \varphi(y).$$

Montrons que $x = y$.

Puisque $x \in \mathbb{Z} \times \mathbb{Z}^*/\mathcal{R}$ alors $F(a,b) \in \mathbb{Z} \times \mathbb{Z}^*$

tel que $x = cl(a,b)$. De même, $\exists (c,d)$ $\in \mathbb{Z} \times \mathbb{Z}^*$

tel que $y = cl(c,d)$.

On sait que $\underbrace{\varphi(x)}_{\frac{a}{b}} = \underbrace{\varphi(y)}_{\frac{c}{d}}$

Donc $a.d = b.c$ donc $(a,b) \mathcal{R} (c,d)$

donc $cl(a,b) = cl(c,d)$ donc $x = y$.

$\uparrow \Rightarrow \uparrow$ NE VEUT PAS DIRE DONC

- Soit $y \in \mathbb{Q}$. Alors $\exists (a, b) \in \mathbb{Z} \times \mathbb{Z}^*$

  tel que : $y = \frac{a}{b}$.

Rappel : $\mathbb{Q} := \left\{ \frac{a}{b}, \ a \in \mathbb{Z}, \ b \in \mathbb{Z}^* \right\}$.

But : Trouver $x \in \mathbb{Z} \times \mathbb{Z}^* / \mathcal{R}$ tel que

$$\varphi(x) = \frac{a}{b}$$

Posons $x := cl(a, b)$

Alors $\varphi(x) = \varphi(cl(a,b)) = \frac{a}{b} = y$

On a montré que :

$\forall y \in \mathbb{Q}$, $\exists x \in \mathbb{Z} \times \mathbb{Z}^* / \mathcal{R}$ tel que $y = \varphi(x)$

Ainsi : f est surjective

- f est injective et surjective donc elle est bijective !

Corrigé TD 1 (suite)

Exercice n° 5 .

1) . **Réflexivité** : Soit $(a,b) \in \mathbb{R}^2$. Montrons que $(a,b)\ \mathcal{R}\ (a,b)$

Par définition, $(a,b)\ \mathcal{R}\ (a,b)$ veut dire que :

$(a-a, b-b) \in \mathbb{Z}^2$ ce qui est vrai ! car

$a-a = 0$ et $b-b = 0$ et $0 \in \mathbb{Z}$.

$0 \in \mathbb{Z}$.

• Symétrie : Soit $(a,b) \in \mathbb{R}^2$ et $(c,d) \in \mathbb{R}^2$ telles que $(a,b)\,\mathcal{R}\,(c,d)$. Montrons que : $(c,d)\,\mathcal{R}\,(a,b)$.

Comme $(a,b)\,\mathcal{R}\,(c,d)$ alors $(a-c,\ b-d) \in \mathbb{Z}^2$

donc $\begin{cases} c-a = -\underbrace{(a-c)}_{\in \mathbb{Z}} & \in \mathbb{Z} \\ d-b = -\underbrace{(b-d)}_{\in \mathbb{Z}} & \in \mathbb{Z} \end{cases}$

$(\mathbb{Z},+)$ est un groupe !

donc $(c-a,\ d-b) \in \mathbb{Z}^2$ donc $(c,d)\,\mathcal{R}\,(a,b)$

- **Transitivité** : Soient $(a,b),(c,d),(e,f) \in \mathbb{Z}^2$

$(a,b) \mathcal{R} (c,d) \iff (a-c,\ b-d) \in \mathbb{Z}^2$

$(c,d) \mathcal{R} (e,f) \iff (c-e,\ d-f) \in \mathbb{Z}^2$

Montrons que $(a-e,\ b-f) \in \mathbb{Z}^2$

Or $(a-c),(c-e),(b-d),(d-f) \in \mathbb{Z}$

Par somme dans $\mathbb{Z}$ on a :

$$\begin{cases} a-c+c-e \in \mathbb{Z} \\ b-d+d-f \in \mathbb{Z} \end{cases} \iff \begin{cases} a-e \in \mathbb{Z} \\ b-f \in \mathbb{Z} \end{cases} \iff (a-e,\ b-f) \in \mathbb{Z}^2$$

Finalement $\mathcal{R}$ est une relat° d'équivalence.

2) Soient $(a,b), (c,d), (e,f), (g,h) \in \mathbb{R}^2$ tels que :

$$\begin{cases} (a,b)\,\mathcal{R}\,(c,d) \\ (e,f)\,\mathcal{R}\,(g,h) \end{cases}$$

Montrons que $(a+e, b+f)\,\mathcal{R}\,(c+g, d+h)$, c'est-à-dire que : $(a+e-c-g, b+f-d-h) \in \mathbb{Z}^2$

On a :

$$a+e-c-g = \underbrace{(a-c)}_{\in \mathbb{Z}} + \underbrace{(e-g)}_{\in \mathbb{Z}} \in \mathbb{Z}$$

$$b+f-d-h = \underbrace{(b-d)}_{\in \mathbb{Z}} + \underbrace{(f-h)}_{\in \mathbb{Z}} \in \mathbb{Z}$$

donc $(a+e-c-g,\ b+f-d-h) \in \mathbb{Z}^2$

donc $(a+e,\ b+f)\ \mathcal{R}\ (c+g,\ d+h)$.

donc $\mathcal{R}$ est compatible avec la somme.

3) Montrons que l'application :

$$f : \begin{array}{ccc} \mathbb{R}^2/\mathbb{Z} & \longrightarrow & \mathbb{T}^2 \\ \overline{(a,b)} & \longmapsto & \left(e^{2i\pi a}, e^{2i\pi b}\right) \end{array}$$

est bijective.

- Montrons que f est bien définie.

c'est-à-dire que si $x, y \in \mathbb{R}^2/\mathbb{Z}$ tels

que $x = y$, alors $f(x) = f(y)$.

Soient $x, y \in \mathbb{R}^2_{/\mathcal{R}}$ tq $x = y$.

Alors : $\begin{cases} \exists (a,b) \in \mathbb{R}^2 : & x = cl(a,b) \\ \exists (c,d) \in \mathbb{R}^2 : & y = cl(c,d) \end{cases}$

Rappel (Rappel) :

$u \mathcal{R} v \iff cl(u) = cl(v)$

Comme $x = y$ alors $d(a,b) = d(c,d)$

donc $(a,b) \mathcal{R} (c,d)$ c'est-à-dire que :

$(a-c, b-d) \in \mathbb{Z}^2$. Montrons que :

$$f(x) = f(y)$$

$$= \left(e^{2i\pi a}, e^{2i\pi b}\right) \qquad = \left(e^{2i\pi c}, e^{2i\pi d}\right)$$

Il suffit donc de montrer que :

$e^{2i\pi a} = e^{2i\pi c}$ et $e^{2i\pi b} = e^{2i\pi d}$

ou encore :

$$e^{2i\pi(a-c)} = 1 \quad \text{et} \quad e^{2i\pi(b-d)} = 1$$

Rappel : $\forall k \in \mathbb{Z}$: $e^{2i\pi k} = 1$.

Preuve :

Définition : Si $\theta \in \mathbb{R}$ alors :

$$e^{i\theta} := \cos(\theta) + i \sin \theta$$

Formule de Moivre : Si $\theta \in \mathbb{R}$, $k \in \mathbb{Z}$ alors :

$$e^{i\theta k} = \left(e^{i\theta}\right)^k$$

Soit $k \in \mathbb{Z}$, on a :

$$e^{2i\pi k} = \left(e^{2i\pi}\right)^k = \left(\underbrace{\cos(2\pi)}_{=1} + i\underbrace{\sin(2\pi)}_{=0}\right)^k$$

$$= 1^k = 1$$

Comme $a-c$ et $b-d$ sont des entiers

alors : $e^{2i\pi(a-c)} = 1$ et $e^{2i\pi(b-d)} = 1$

donc : $e^{2i\pi a} = e^{2i\pi c}$ et $e^{2i\pi b} = e^{2i\pi d}$

donc : $\left(e^{2i\pi a}, e^{2i\pi b}\right) = \left(e^{2i\pi c}, e^{2i\pi d}\right)$

donc $f(x) = f(y)$

- Montrons que f est injective.

Soient $x, y \in \mathbb{R}^2/_{\mathcal{R}}$ tels que $f(x) = f(y)$

Montrons que : $x = y$.

Il existe $(a,b) \in \mathbb{R}^2$ et $(c,d) \in \mathbb{R}^2$ tels que :

$$\begin{cases} x = cl(a,b) \\ y = cl(c,d) \end{cases}$$

Il suffit de montrer que : $(a,b)\,\mathcal{R}\,(c,d)$

c'est-à-dire que $a-c \in \mathbb{Z}$ et $b-d \in \mathbb{Z}$.

On sait que $f(x) = f(y)$. Donc :

$$e^{2i\pi a} = e^{2i\pi c} \quad \text{et} \quad e^{2i\pi b} = e^{2i\pi d}$$

càd : $e^{2i\pi(a-c)} = 1$ et $e^{2i\pi(b-d)} = 1$

Rappel : Soit $k \in \mathbb{R}$ tel $e^{2i\pi k} = 1$:

alors : $k \in \mathbb{Z}$.

Preuve : Soit $k \in \mathbb{R}$ tel que $e^{2i\pi k} = 1$

Alors $e^{2i\pi k} = e^{i \cdot 0}$. On sait que,

$\forall (\theta, \theta') \in \mathbb{R}^2 : \left(e^{i\theta} = e^{i\theta'}\right) \Rightarrow \theta - \theta' \in 2\pi\mathbb{Z}$

on a donc $2\pi k - 0 \in 2\pi\mathbb{Z}$

c'est-à-dire que : $k \in \mathbb{Z}$

Donc : $a - c \in \mathbb{Z}$ et $b - d \in \mathbb{Z}$.

- **Montrons que f est surjective.**

Soit $y \in T^2$. Montrons qu'il existe $x \in \mathbb{R}^2/\mathbb{R}$ tel que $y = f(x)$.

Puisque $y \in T^2$ alors $\exists (z, w) \in \mathbb{C}^2$,

$y = (z, w)$ et $|z| = |w| = 1$

Rappel : Si $z \in \mathbb{C}$ tel que $|z| = 1$

Alors $\exists \theta \in \mathbb{R}$, $z = e^{2i\pi\theta}$

D'après le rappel, il existe $a \in \mathbb{R}$ et $b \in \mathbb{R}$ telles que :

$$\begin{cases} z = e^{2i\pi a} \\ w = e^{2i\pi b} \end{cases}$$

Posons $x := d(a,b) \in \mathbb{R}^2/\mathbb{R}$

alors on a :

$$y = (z, w) = \left(e^{2i\pi a}, e^{2i\pi b}\right)$$
$$=: f\big(d(a,b)\big) = f(x)$$

Donc x est bien un antécédent de y par la fonction f.

Exercice n°6 : À faire à la maison.

Exercice n°7

1) • Reflexivité : Ok !

• Symétrie : OK !

• Transitivité : OK !

2) Soit π : $E \longrightarrow E/\mathcal{R}$

$x \longmapsto cl(x)$

Montrer qu'il existe une unique application

$$\overline{f} : E/\mathcal{R} \to F$$

tel que : $f = \overline{f} \circ \pi$.

Suite exercice n° 7.

2) Montrons qu'il existe $\bar{f} : E/R \longrightarrow F$ telle que $f = \bar{f} \circ \pi$

Posons : $\bar{f} : E/R \longrightarrow F$

$cl(x) \longmapsto f(x)$

- Montrons que $\bar{f}$ est bien définie.

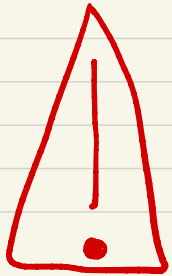
Soient $u, v \in E/\mathcal{R}$ tels que $u = v$

Montrons que $\bar{f}(u) = \bar{f}(v)$.

Il existe $x, y \in E$ tels que :

$$\begin{cases} u = cl(x) \\ v = cl(y) \end{cases}$$

RAPPEL : $x \mathcal{R} y \iff cl(x) = cl(y)$



On sait que $u = v$, donc $x \mathcal{R} y$

donc $f(x) = f(y)$ donc $\bar{f}(u) = \bar{f}(v)$

$\bar{f}(cl(x)) \quad \bar{f}(cl(y))$

$= \bar{f}(u) \quad = \bar{f}(v)$

Donc l'application $\bar{f}$ est bien définie

- Montrons que $f = \bar{f} \circ \pi$.

Rappel : Pour montrer deux fonctions sont égales, il faut montrer qu'elles sont égales en tout point :

$$f = g \iff \forall x : \quad f(x) = g(x)$$

Soit $x \in E$. Montrons que : $f(x) = \bar{f} \circ \pi(x)$.

On a :

$$\bar{f} \circ \pi(x) = \bar{f}\left(\pi(x)\right) = \bar{f}\left(cl(x)\right) = f(x)$$

- Montrons que $\bar{f}$ est l'unique application telle que : $f = \bar{f} \circ \pi$.

Pour cela, supposons qu'il existe $\bar{g} : E/\mathcal{R} \to F$ telle que $f = \bar{g} \circ \pi$

Montrons que : $\bar{f} = \bar{g}$

Soit $u \in E/\mathcal{R}$. Montrons que $\bar{f}(u) = \bar{g}(u)$.

Il existe $x \in E$ tel que $u = cl(x)$.

On a donc :

$$\bar{f}(u) = \bar{f}(cl(x)) = \bar{f}(\pi(x)) = \bar{f} \circ \pi(x)$$

$\pi(x) = cl(x)$

$$= \bar{g} \circ \pi(x) = \bar{g}(\pi(x)) = \bar{g}(cl(x)) = \bar{g}(u)$$

$\bar{f} \circ \pi = f = \bar{g} \circ \pi$

Ainsi, $\bar{f}$ est unique.

Rappel : • Soient f, g, h trois applications telles que : $g \circ f = h \circ f$

alors si f est surjective on a

$$g = h$$

• Soient f, g, h trois applications telles que : $f \circ g = f \circ h$

alors si f est injective on a

$$g = h$$

À FAIRE

- Montrons que $\bar{f}$ est injective.

Soient $u, v \in E/\mathcal{R}$ telles que $\bar{f}(u) = \bar{f}(v)$

Montrons que $u = v$.

$\exists\, x, y \in E$: $u = cl(x)$, $v = cl(y)$.

Puisque $\bar{f}(u) = \bar{f}(v)$ alors $\bar{f}(cl(x)) = \bar{f}(cl(y))$

donc $f(x) = f(y)$ donc $x \mathcal{R} y$

donc $d(x) = d(y)$ donc $u = v$.

Exercice n° 8

1) Montrer que $\mathcal{P} = \left(U_n = [n, n+2[\right)_{n \in 2\mathbb{Z}}$

est une partition de $\mathbb{R}$.

Rappel. On dit qu'une famille $(E_i)_{i \in I}$ est une partition d'un ensemble X si :

- $\forall x \in X, \ \exists i \in I : x \in E_i$
- $\forall i, j \in I$, si $i \neq j$ alors $E_i \cap E_j = \emptyset$

- Montrons que $\forall x \in \mathbb{R}$, $\exists n \in 2\mathbb{Z}$ tel que $n \leq x < n+2$

Rappel : $2\mathbb{Z} = \{2k, k \in \mathbb{Z}\}$

Cela est équivalent à montrer que :

$\forall x \in \mathbb{R}$, $\exists k \in \mathbb{Z}$ tel que : $2k \leq x < 2k+2$

Rappel : Soit $y \in \mathbb{R}$. La partie entière de y, notée $E(y)$ ou $\lfloor y \rfloor$, est l'unique entier vérifiant l'inégalité :

$$E(y) \leq y < E(y) + 1$$

Soit $x \in \mathbb{R}$. Posons $k := E\left(\frac{x}{2}\right)$.

Alors $\underbrace{E\left(\frac{x}{2}\right)}_{=k} \leq \frac{x}{2} < \underbrace{E\left(\frac{x}{2}\right)}_{=k} + 1$

c'est-à-dire :

$$k \leq \frac{x}{2} < k+1$$

Donc : $2k \leq x < 2k+2$

Ainsi, $\forall x \in \mathbb{R}$, $\exists k \in \mathbb{Z}$: $x \in [2k, 2k+2[$

donc $\forall x \in \mathbb{R}$, $\exists n \in 2\mathbb{Z}$: $x \in U_n$.

- Soit $n, m \in 2\mathbb{Z}$ tels que $n \neq m$

Montrons que $U_n \cap U_m = \emptyset$

Rappel : Pour montrer qu'un ensemble E est vide, on raisonne par l'absurde en supposant qu'il $x \in E$ et on montre que c'est impossible.

Supposons par l'absurde qu'il existe $x \in U_n \cap U_m$.

Alors $x \in U_n$ et $x \in U_m$

Donc $n \leq x < n+2$ et $m \leq x < m+2$

Puisque n et m sont dans $2\mathbb{Z}$ alors

$\exists (k, k') \in \mathbb{Z}^2$: $\begin{cases} n = 2k \\ m = 2k' \end{cases}$ et $k \neq k'$

On a donc : $\begin{cases} 2k \leq x < 2k+2 \\ 2k' \leq x < 2k'+2 \end{cases}$

c'est-à-dire que : $k \leq \frac{x}{2} < k+1$

$k' \leq \frac{x}{2} < k'+1$

Par unicité de la partie entière :

$k = E\left(\frac{x}{2}\right)$ et $k' = E\left(\frac{x}{2}\right)$

donc $k = k'$ ABSURDE !

2) Soient x et $y \in \mathbb{R}$.

$x \mathcal{R} y \iff \exists n \in 2\mathbb{Z} : \begin{matrix} x \in U_n \\ y \in U_n \end{matrix}$

3) • Montrer que : $d\left(\frac{1}{2}\right) = d\left(\frac{19}{10}\right)$

$\frac{1}{2} \mathcal{R} \frac{19}{10}$ car $\frac{1}{2}$ et $\frac{19}{10}$ sont dans U_0.

donc $d\left(\frac{1}{2}\right) = d\left(\frac{19}{10}\right)$

⚠ Remplacer $\frac{39}{10}$ par $\frac{41}{10}$ ⚠

- Montrons que $d\left(\frac{5}{2}\right) \neq d\left(\frac{41}{10}\right)$

On a $\frac{5}{2} \in U_2$ et $\frac{41}{10} \in U_4$

et $U_2 \cap U_4 = \emptyset$ donc $\frac{5}{2}$ n'est pas en relation avec $\frac{41}{10}$ donc : $d\left(\frac{5}{2}\right) \neq d\left(\frac{41}{10}\right)$

4) Il faut trouver x, y, z et $t \in \mathbb{R}$ tels que : $x \mathcal{R} y$

$z \mathcal{R} t$

mais $(x + z)$ n'est pas en relation avec $y + t$.

$\frac{1}{2} \mathcal{R} \frac{19}{10}$ et $2 \mathcal{R} \frac{22}{10}$

mais $\frac{1}{2} + 2 = \frac{5}{2}$ n'est pas

en relation avec $\frac{41}{10} = \frac{19}{10} + \frac{22}{10}$

Corrigé TD2

Exercice n° 10

Sur $\mathbb{Q}$, on définit une loi $*$:

$\forall a, b \in \mathbb{Q}$: $\quad a * b := \dfrac{a+b}{2}$

Est-elle associative ?

Rappel Soit E un ensemble et $*$ une loi de composition interne (càd $\forall a, b \in E : a * b \in E$)

On dit que $*$ est associative si $\forall a, b, c \in E$:

$$(a * b) * c = a * (b * c)$$

Soient $a, b, c \in \mathbb{Q}$,

- $(a * b) * c = \left(\frac{a+b}{2}\right) * c = \frac{\frac{a+b}{2} + c}{2}$

$$= \frac{a + b + 2c}{4}$$

- $a * (b * c) = a * \left(\frac{b+c}{2}\right) = \frac{a + \frac{b+c}{2}}{2}$

$$= \frac{2a + b + c}{4}$$

Donc si $\begin{cases} a = 1 \\ b = 0 \\ c = 0 \end{cases}$ on obtient : $(a \times b) * c = \frac{1}{4}$

$a \times (b * c) = \frac{1}{2}$

Donc l'égalité $(a \times b) * c = a * (b * c)$ est fausse en général. La loi n'est pas associative.

Exercice 11

$\forall x, y \in \mathbb{R}$:

$$x \times y = xy + (x^2 - 1)(y^2 - 1)$$

- **Commutativité.** Soient $x, y \in \mathbb{R}$.

$$\begin{aligned} x * y &= xy + (x^2-1)(y^2-1) \\ &= y \cdot x + (y^2-1)(x^2-1) \\ &= y * x \end{aligned}$$

Donc $*$ est commutative.

- **Non associativité.** But : trouver trois réels x, y, z tq : $(x * y) * z \neq x * (y * z)$.

Posons $x = -1$, $y = 0$, $z = 0$.

Alors . $(x * y) * z = 0 * z = 1$

. $x * (y * z) = -1$

Donc la loi $*$ est non associative .

. 1 est le neutre pour $*$.

Rappel : Soit E un ensemble et $*$ un loi de

composition interne. On dit que e est un élément neutre pour $*$ si :

$$\forall a \in E : \quad a * e = e * a = a$$

Soit $x \in \mathbb{R}$. Alors :

$$\begin{cases} x * 1 = x \cdot 1 + (x^2 - 1)(1^2 - 1) = x \\ 1 * x = x \end{cases}$$

Donc 1 est un élément neutre.

Exercice 12

$\forall x, y \in \mathbb{R}_+$:

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

- **Commutativité** : Soient $x, y \in \mathbb{R}_+$.

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

Donc $*$ est commutative.

- **Associativité** : Soient $x, y, z \in \mathbb{R}_+$.

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

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

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

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

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

Rappel : Soit $x \in \mathbb{R}$. Alors $\sqrt{x^2} = |x|$

- 0 est un élément neutre.

Soit $x \in \mathbb{R}_+$. Alors $x * 0 = \sqrt{x^2 + 0^2} = x$

(car $x \geqslant 0$)

et $0 * x = \sqrt{0^2 + x^2} = x$

($x \geqslant 0$)

donc 0 est un élément neutre pour $*$.

- Mq aucun élément de $]0, +\infty[$ n'a de symétrie.

Raisonnons par l'absurde. Supposons qu'il existe $x > 0$ possédant un inverse.

C'est-à-dire qu'il existe $y \in \mathbb{R}_+$ tel que

$$\begin{cases} y * x = 0 \\ x * y = 0 \end{cases}$$ (cette égalité est inutile car $x * y = y * x$)

Puisque $y * x = 0$ alors $\sqrt{y^2 + x^2} = 0$

donc $y^2 + x^2 = 0$ donc $y^2 = x^2 = 0$

En particulier, $x^2 = 0$ donc $x = 0$

ABSURDE ! (car $x > 0$)

Exercice n° 13 . $\forall a, b \in \mathbb{Q}$:

$$a \star b = a + b + a \cdot b$$

Montrer que $(\mathbb{Q} \setminus \{-1\}, \star)$ est un groupe .

Rappel On dit que $(G, *)$ est un groupe si :

① **Loi de composition interne** : $\forall a, b \in G$ alors $a * b \in G$

② **Associativité** : $\forall a, b, c \in G$:

$$(a * b) * c = a * (b * c)$$

③ **Neutre**. Il existe un élément noté e dans G vérifiant : $\forall a \in G$: $e * a = a = a * e$

④ **Symétrie**. Pour tout $a \in G$, il existe $b \in G$:

$$a * b = e = b * a$$

Si de plus, G vérifie : $\forall a, b \in G$:

$$a * b = b * a$$

Alors on dit que $(G, *)$ est un groupe commutatif

Loi de composition interne

Soient $a, b \in \mathbb{Q} \setminus \{-1\}$

alors $\exists\, x_1, x_2 \in \mathbb{Z}$, $\exists\, y_1, y_2 \in \mathbb{N}^*$:

$$\begin{cases} a = \dfrac{x_1}{y_1} \\ b = \dfrac{x_2}{y_2} \end{cases}$$

et $x_1 \neq -y_1$; $x_2 \neq -y_2$ (car $a \neq -1$, $b \neq -1$)

$$\begin{aligned} a * b &= a + b + ab \\ &= \frac{x_1}{y_1} + \frac{x_2}{y_2} + \frac{x_1 \cdot x_2}{y_1 y_2} \end{aligned}$$

$$= \frac{\boxed{x_1 \cdot y_2 + x_2 \cdot y_1 + x_1 \cdot x_2} \in \mathbb{Z}}{\boxed{y_1 \cdot y_2} \in \mathbb{N}^*}$$

$\in \mathbb{Q}$

Vérifions que $a * b \neq -1$

Résolvons par l'absurde :

Supposons que $a * b = -1$.

Donc $x_1 y_2 + x_2 y_1 + x_1 x_2 = -y_1 y_2$

Donc $x_1 y_2 + x_2 y_1 + x_1 x_2 + y_1 y_2 = 0$,

Donc $x_1 (x_2 + y_2) + y_1 (x_2 + y_2) = 0$

On a $x_2 + y_2 \neq 0$ car $x_2 \neq -y_2$.

D'où $\dfrac{x_1(x_2+y_2) + y_1(x_2+y_2)}{(x_2+y_2)} = 0$.

Ainsi $x_1 + y_1 = 0$ ABSURDE car $x_1 \neq y_1$.

Donc $a * b \neq -1$ et ainsi $a * b \in \mathbb{Q} \setminus \{-1\}$.

Donc $*$ est une loi interne.

- **Associativité.** Soient $a, b, c \in \mathbb{Q} \setminus \{-1\}$.

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

$$= a+b+a\cdot b+c+(a+b+ab)\cdot c$$

$$= a+b+a\cdot b+c+ac+bc+abc$$

$$= a+b+c+ab+bc+ac+abc$$

$$a*(b*c) = a*(b+c+b\cdot c)$$

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

$$= a+b+c+bc+ab+ac+abc$$

Donc $(a*b)*c = a*(b*c)$

• **Neutre** . Trouvons $e \in \mathbb{Q} \setminus \{-1\}$ tel que

$\forall a \in \mathbb{Q} \setminus \{-1\}$: $\quad a * e = a = e * a$

Soit $a \in \mathbb{Q} \setminus \{-1\}$ tq $\quad a * e = a$

alors $\quad a + e + e \cdot a = a$

donc $\quad e(1 + a) = 0$

donc $\quad e = 0$

car $a \neq -1$

De même, on montre que $0 * a = a$

- **Symétrie.** Soit $a \in \mathbb{Q} \setminus \{-1\}$. Trouvons $b \in \mathbb{Q} \setminus \{-1\}$ tel que : $\begin{cases} a * b = 0 \\ b * a = 0 \end{cases}$ (0 : neutre pour $*$)

Si b existe, alors :

$$a * b = 0$$

donc : $a + b + a \cdot b = 0$

donc $b + ab = -a$ donc $b(1+a) = -a$

donc $b = \dfrac{-a}{1+a}$

car $a \neq -1$

Réciproquement, $\dfrac{-a}{1+a}$ est bien un inverse de a car :

$$a * \left(\frac{-a}{1+a}\right) = \dots = 0$$

$$\left(\frac{-a}{1+a}\right) * a = \dots = 0$$

Il reste à vérifier que $\dfrac{-a}{1+a} \neq -1$

Supposons par l'absurde que : $\frac{-a}{1+a} = -1$

alors $-a = -(1+a)$ donc $0 = -1$

ABSURDE ! donc $\frac{-a}{1+a} \neq -1$

Ainsi, $\forall a \in \mathbb{Q} \setminus \{-1\}$, il existe un inverse pour a qui est $\frac{-a}{1+a} \in \mathbb{Q} \setminus \{-1\}$

Exercice n°17

- **Loi de composition interne** .

Soient $x, y \in]-1,1[$. Montrons que :

$$\frac{x+y}{1+x \cdot y} \in]-1,1[$$

- $\frac{x+y}{1+x \cdot y} < 1$

$$\frac{x+y}{1+xy} < 1 \iff x+y < 1+xy$$

car $1+xy > 0$

$$\iff x+y-1-xy < 0$$

$$\iff y(1-x) < 1-x$$

$$\iff y < 1$$

car $1-x > 0$

- De même, on montre que $\forall x,y \in]-1,1[$:

$$\frac{x+y}{1+xy} > -1 .$$

Corrigé TD2

Exercice n°18

Montrer que tout sous groupe de $(\mathbb{Z}, +)$ est de la forme $n.\mathbb{Z}$ avec $n \in \mathbb{N}$.

Il y a deux choses à montrer :

1. Si G est un sous groupe de $(\mathbb{Z}, +)$ alors il existe $n \in \mathbb{N}$ tel que $G = n.\mathbb{Z}$

(2) Si $n \in \mathbb{N}$ alors $n\mathbb{Z}$ est un sous groupe de $\mathbb{Z}$

(1) Soit G un sous-groupe de $(\mathbb{Z}, +)$.

- Si $G = \{0\}$ alors en posant $n = 0 \in \mathbb{N}$ et on a : $G = n \cdot \mathbb{Z}$
- Si $G \neq \{0\}$ alors $\exists g \in G$ ($\in \mathbb{Z}$) tel que $g \neq 0$ et son inverse $-g$ est aussi dans G.

Quitte à remplacer g par $-g$, on peut supposer que $g > 0$. Posons :

$$n := \min \{ m \in G, \ m > 0 \} \in G$$

n existe bien car l'ensemble $\{ m \in G, m > 0 \}$ est non vide (contient g) et minoré (par 0).

Rappel : • Toute partie non vide et minorée de $\mathbb{N}$ admet un plus petit élément

- Toute partie non vide et majorée de $\mathbb{N}$ admet un plus grand élément

3 Montrons que $n\mathbb{Z} \subset G$.

Soit $x \in n\mathbb{Z}$. Alors $\exists k \in \mathbb{Z} : x = n \cdot k$

Donc :

$$x = \overbrace{n}^{\in G} + \underbrace{\cdots +}_{k\text{-fois}} \overbrace{n}^{\in G} \in G$$

car G est un sous-groupe de $(\mathbb{Z}, +)$

C Montrons que $G \subset n\mathbb{Z}$

Soit $x \in G$. Montrons qu'il existe $q \in \mathbb{Z}$ tel que : $x = n \cdot q$

Effectuons la division euclidienne de x par n : $\exists (q, r) \in \mathbb{Z}^2$ tel que :

$$\begin{cases} x = n \cdot q + r \\ 0 \leq r < n \end{cases}$$

À SAVOIR

Par définition de n, le seul entier dans G

et plus petit que n est 0.

Ici :

- $r = \underbrace{x}_{\in G} - \underbrace{\underbrace{n}_{\in G}\underbrace{q}_{\in \mathbb{Z}}}_{\in G} \in G$
- $r < n$

Donc $r = 0$. Donc $x = n \cdot \underbrace{q}_{\in \mathbb{Z}}$

D'où $x \in n\mathbb{Z}$

② Soit $n \in \mathbb{N}$. Montrons que $n\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$

Exercice n° 21 .

$$A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad ; \quad B = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$$

Rappel : • Soit $n \in \mathbb{N}^*$.

$$GL(n, \mathbb{R}) = \{ M \in M_n(\mathbb{R}) \mid M \text{ inversible} \} .$$

• Soient $(G, \cdot)$ un groupe et $g \in G$.

On dit que G est d'ordre fini si il existe $n \in \mathbb{N}^*$ tel que $g^n = e$ avec e le neutre de G.

Rappel. $(GL(n, \mathbb{R}), \times)$ est un groupe

Le neutre est I_n

Pour montrer que A et B sont d'ordres finis il faut trouver $n \in \mathbb{N}^*$, $m \in \mathbb{N}^*$ tq :

$$\begin{cases} A^n = I_2 \\ B^m = I_2 \end{cases}$$

- $A^2 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$

donc $n = 2$ convient ! Donc A est d'ordre

fini.

- $B^2 = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$

donc $n = 2$ convient ! Donc B est d'ordre fini.

Pour montrer que $A \cdot B$ est d'ordre infini il faut montrer que $\forall n \in \mathbb{N}^*$:

$$(A \cdot B)^n \neq I_2 .$$

On a :

$$A \times B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

Montrons par récurrence que $\forall n \in \mathbb{N}^*$:

$$\mathcal{P}(n) : \text{"} (A \cdot B)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \text{"}$$

- <u>Initialisation</u> Pour $n = 1$ on a :

$$(AB)^1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{donc} \quad \mathcal{P}(1) \text{ vraie}$$

• Hérédité. Supposons que $\mathcal{P}(n)$ est vraie pour un certain $n \geq 2$. On a :

$$(A \cdot B)^{n+1} = (A \cdot B) \cdot (AB)^n$$

$$= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$$

$(A \cdot B)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ d'après $\mathcal{P}(n)$

$$= \begin{pmatrix} 1 & n+1 \\ 0 & 1 \end{pmatrix}$$

Donc $\mathcal{P}(n+1)$ vraie !

Ainsi :

$$\forall n \in \mathbb{N}^* : \quad (AB)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$$

donc $A \cdot B$ est d'ordre infini.

Rappel Soit $n \in \mathbb{N}^*$ et A, B deux matrices dans $\mathcal{M}_n(\mathbb{R})$ tq $A \cdot B = B \cdot A$. Alors :

$$(A+B)^n = \sum_{k=0}^{n} \binom{n}{k} A^k \cdot B^{n-k}$$

Exercice n° 22. Soit G groupe abélien et $a, b \in G$ d'ordres finis. Soit $\begin{cases} r = \text{ordre}(a) \\ s = \text{ordre}(b) \end{cases}$ avec r et s premiers entre eux.

Montrons que $\text{ordre}(a \cdot b) = r \times s$

Rappel. Soit $(G, \cdot)$ un groupe et $g \in G$.

L'ordre de g, notée $\text{ordre}(g)$, est l'entier défini par :

$$\text{ordre}(g) = \min \{ n \in \mathbb{N}^* : g^n = 1 \}$$

$g^n = g \cdot g \cdot \dots \cdot g$

où 1 désigne le neutre de G

Il faut montrer 2 choses :

1. $(a \cdot b)^{r \cdot s} = e$

2. Montrer que $r \cdot s$ est le plus petit entier tq : $(a \cdot b)^{r \cdot s} = e$

Définition. Un groupe $(G, *)$ est dit abélien ou commutatif si $\forall a, b \in G$:

$$a * b = b * a$$

En particulier : $(a * b)^n = a^n * b^n$

$$(a \cdot b)^{r \cdot s} = a^{r \cdot s} \cdot b^{r \cdot s} = \left(a^r\right)^s \cdot \left(b^s\right)^r$$

Or comme $r = \text{ordre}(a)$ alors $a^r = e$

et de même : $b^s = e$

Donc :

$$(a.b)^{r.s} = e^s \cdot e^r = e \cdot e = e$$

② Soit $k \in G$ tel que $(ab)^k \overset{(*)}{=} e$

Montrons que $rs \leq k$.

D'après $(*)$, on a : $a^k = b^{-k}$

Rappel : 1) Soit G un groupe fini d'ordre $n \in \mathbb{N}^*$. Alors $\forall g \in G$:

$$g^n = e$$

2) Soit $a \in G$, le sous groupe engendré par a, noté $\langle a \rangle$ est :

$$\langle a \rangle := \{ a^m, m \in \mathbb{Z} \}$$

et le cardinal de ce groupe est ordre(a)

b^{-k} s'écrit a^k donc $b^{-k} \in \langle a \rangle$ et donc d'après 1) $(b^{-k})^r = e$ càd : $b^{-kr} = e$ donc b^{kr}. On montre de la même manière que $a^{ks} = e$

Donc : $\begin{cases} b^{kr} = e \\ a^{ks} = e \end{cases}$

Ainsi, $\begin{cases} s := \text{ordre}(b) & \text{divise } k.r \\ r := \text{ordre}(a) & \text{divise } k.s \end{cases}$

Rappel (Lemme de Gauss)

Soient $a, b, c \in \mathbb{Z}$. Si a divise $b.c$ et a premier avec c alors a divise b

D'après le Lemme de Gauss, comme r et s sont premiers entre eux, on a :

$$\begin{cases} s \text{ divise } k \\ r \text{ divise } k \end{cases}$$

Rappel : Soient $a, b, c \in \mathbb{Z}$.

Si $\begin{cases} \cdot\ a \text{ divise } c \\ \cdot\ b \text{ divise } c \\ \cdot\ a \text{ et } b \text{ premier entre eux} \end{cases}$ Alors : $\begin{cases} a \cdot b \text{ divise} \\ c \end{cases}$

Donc $r \cdot s$ divise k

En particulier : $r \cdot s \leq k$!

Corrigé TD2

Exercice n°22 (suite)

2) Montrons que $\langle a, b \rangle = \langle a \cdot b \rangle$

Rappel : Soient A et B deux ensembles.

Si $A \subseteq B$ et $\text{Card}(A) = \text{Card}(B)$

alors $A = B$

- $\langle a, b \rangle := \left\{ a^m \cdot b^m \,,\; \begin{matrix} n \in \mathbb{Z} \\ m \in \mathbb{Z} \end{matrix} \right\}$

- $\langle a \cdot b \rangle := \left\{ (a \cdot b)^p \,,\; p \in \mathbb{Z} \right\}$

$$= \left\{ a^p \cdot b^p \,,\; p \in \mathbb{Z} \right\}$$

↑ G abélien

Donc : $\langle a \cdot b \rangle \subseteq \langle a, b \rangle$

Rappel • Soit G un groupe et $g \in G$.

Notons $\langle g \rangle$ le sous-groupe engendré par g. Alors

$$\text{Card}\left(\langle g \rangle\right) = \text{ordre}(g)$$

• L'ordre d'un groupe est son cardinal

$$\text{ordre}(G) := \text{Card}(G)$$

On sait que :

$$\mathrm{Card}\left(\langle a \cdot b \rangle\right) = r \cdot s$$

Il suffit donc de prouver que :

$$\mathrm{Card}\left(\langle a, b \rangle\right) = r \cdot s$$

On a :

$$\langle a, b \rangle = \left\{ a^n \cdot b^m \;,\; \begin{array}{l} 0 \leq n \leq r-1 \\ 0 \leq m \leq s-1 \end{array} \right\}$$

$r := \text{ordre}(a)$

$s := \text{ordre}(b)$

Soit $x \in \langle a, b \rangle$. Alors $\exists\, n, m \in \mathbb{Z}$:

$x = a^n \cdot b^m$. Montrons que : $\begin{cases} 0 \leq n \leq r-1 \\ 0 \leq m \leq s-1 \end{cases}$

La division euclidienne de n par r donne :

$$\exists q \in \mathbb{Z}, \exists R \in \mathbb{Z} \quad : \quad \begin{cases} n = r \cdot q + R \\ 0 \leq R < r \end{cases}$$

$$\Leftrightarrow \quad 0 \leq R \leq r - 1$$

Donc : $a^n = a^{r \cdot q + R} = a^{r \cdot q} \cdot a^R$

$$= \left(a^r\right)^q \cdot a^R = 1^q \cdot a^R$$

$$= a^R$$

De même, $\exists R' \in [\![0, s-1]\!]$:

$$b^m = b^{R'}$$

Donc : $x = a^R \cdot b^{R'}$ avec $0 \leq R \leq r-1$, $0 \leq R' \leq s-1$

donc $x \in \left\{ a^n \cdot b^m, \begin{array}{l} 0 \leq n \leq r-1 \\ 0 \leq m \leq s-1 \end{array} \right\}$

D'où : $\langle a, b \rangle = \left\{ a^n \cdot b^m, \begin{array}{l} 0 \leq n \leq r-1 \\ 0 \leq m \leq s-1 \end{array} \right\}$

$r \cdot s$ éléments

Finalement : $\langle a, b \rangle = \langle a \cdot b \rangle$

Exercice n° 24

$$f : (\mathbb{R}, +) \longrightarrow (E, *)$$
$$x \longmapsto \frac{e^x - e^{-x}}{e^x + e^{-x}} .$$

Mq f est un isomorphisme de groupe.

Rappel • Soient $(G_1, *)$ et (G_2, Δ) deux groupe. On dit que :

$$f : (G_1, *) \longrightarrow (G_2, \Delta)$$

est un <u>morphisme de groupe</u> si :

$$\forall x, y \in G_1 : \quad f(x * y) = f(x) \Delta f(y)$$

- On dit que $f : (G_1, *) \to (G_2, \Delta)$

est un <u>isomorphisme de groupe</u> si :

f est morphisme de groupe bijectif

- Le noyau de f, notée $\mathrm{Ker}(f)$, est le sous-groupe de G_1 :

$$\mathrm{Ker}(f) = \{ x \in G_1, \ f(x) = e_{G_2} \}$$

- Soit f un morphisme de groupe entre G_1 et G_2. Alors :

$$f \text{ injective} \iff \mathrm{Ker}(f) = \{ e_{G_1} \}$$

- Mq $\forall x, y \in \mathbb{R}$:

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

Soient $x, y \in \mathbb{R}$.

$$f(x) * f(y) = \frac{f(x) + f(y)}{1 + f(x) \cdot f(y)} = \frac{\frac{e^x - e^{-x}}{e^x + e^{-x}} + \frac{e^y - e^{-y}}{e^y + e^{-y}}}{1 + \frac{e^x - e^{-x}}{e^x + e^{-x}} \cdot \frac{e^y - e^{-y}}{e^y + e^{-y}}}$$

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

on multiplie en haut et en bas par : $(e^{x}+e^{-x})(e^{y}+e^{-y})$

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

- Mq : f est bijective

• f est injective. En effet, il faut et il suffit de montrer que $\mathrm{Ker}(f) = \{e_{\mathbb{R}}\}$

(ici, l'élément neutre de $(\mathbb{R}_+, \cdot)$ est 0 donc $e_{\mathbb{R}} = 0$). Puisque le neutre de E est 0 alors il faut montrer que :

$$f(x) = 0 \iff x = 0.$$

On a :

$$f(x) = 0 \iff \frac{e^{x} - e^{-x}}{e^{x} + e^{-x}} = 0$$

$$\iff e^{x} - e^{-x} = 0 \iff e^{x} = e^{-x}$$

$$\iff x = -x \iff 2x = 0$$

$$\iff x = 0$$

- <u>f est surjective</u>. En effet, soit

$y \in \underbrace{]-1,1[}_{\text{espace d'arrivé}}$. Le but est de montrer qu'il existe $x \in \mathbb{R}$ tel que $y = f(x)$

Raisonnons par Analyse - Synthèse.

Analyse Supposons qu'il existe $x \in \mathbb{R}$ tq $y = f(x)$. Alors

$$y = \frac{e^{x} - e^{-x}}{e^{x} + e^{-x}}, \text{ donc } y(e^{x} + e^{-x}) = e^{x} - e^{-x}$$

En multipliant par e^x, on a :

$y e^{2x} + y = e^{2x} - 1$ donc :

$e^{2x}(y-1) = -y-1$ donc : $e^{2x} = \frac{1+y}{1-y}$

d'où $x = \frac{1}{2} \ln\left(\frac{1+y}{1-y}\right)$

Synthèse Soit $y \in]-1,1[$. Posons :

$$x = \frac{1}{2} \ln\left(\frac{1+y}{1-y}\right)$$

On vérifie bien que $y = f(x)$

Finalement : f est surjective

Exercice n° 26

Soit $(A, \cdot)$ groupe abélien, $E = \{-1, 1\}$ et $G = A \times E$. $\forall a, b \in A$, $\forall x, y \in E$:

$$(a, x)(b, y) = (ab^x, xy)$$

- **Loi de composition interne** : $\forall a, b \in A$, $\forall x, y \in E$

$a \cdot b^x \in A$ car A est un groupe et

$x \cdot y = 1$ ou -1 donc $x \cdot y \in E$

donc $(a,x)\cdot(b,y) \in A \times E$

• **Neutre** : Soit $(a,x) \in G$. Trouvons $(b,y) \in G$ tel que $(a,x)\cdot(b,y) = (a,x)$. On a :

$$(a,x)(b,y) = (a,x) \iff \begin{cases} ab^x = a \\ xy = x \end{cases} \iff \begin{cases} b^x = e_A \\ y = 1 \end{cases}$$

. Si $x = 1$ alors $b^x = e_A \iff b = e_A$

. Si $x = -1$ alors $b^x = e_A \iff b^{-1} = e_A$
$\iff e_A = b$

donc dans tous les cas : $b^x = e_A \iff b = e_A$

ainsi :

$$(a,x)(b,y) = (a,x) \iff \begin{cases} b = e_A \\ y = 1 \end{cases}$$

Ainsi, G possède un élément neutre qui est $(e_A, 1)$.

- **Associativité** : Soient $(a,x), (b,y), (c,z)$ dans G. On a :

- $[(a,x)\cdot(b,y)]\cdot(c,z) = (ab^x, xy)\cdot(c,z)$

$= (ab^x c^{xy}, xyz)$

- $(a,x)\cdot[(b,y)\cdot(c,z)] = (a,x)(bc^y, yz)$

$= (a(bc^y)^x, xyz)$

$= (ab^x c^{xy}, xyz)$

Donc $[(a,x)\cdot(b,y)]\cdot(c,z) = (a,x)\cdot[(b,y)\cdot(c,z)]$

Ainsi, la loi est associative

• **Symétrie**. Soit $(a,x) \in G$. Il faut trouver $(b,y) \in G$ tel que $(a,x)\cdot(b,y) = (e_A, 1)$

On a :

$$(a,x)(b,y) = (e_A,1) \iff \begin{cases} ab^x = e_A \\ xy = 1 \end{cases}$$

• Si $x = 1$ alors : $\begin{cases} ab = e_A \\ y = 1 \end{cases}$ donc $\begin{cases} b = a^{-1} \\ y = 1 \end{cases}$

• Si $x = -1$ alors $\begin{cases} ab^{-1} = e_A \\ y = -1 \end{cases}$ donc : $\begin{cases} b = a \\ y = -1 \end{cases}$

Ainsi, l'inverse de (a, x) est

$$\begin{cases} (a^{-1}, 1) & \text{si } x = 1 \\ (a, -1) & \text{si } x = -1 \end{cases}$$

En particulier, tout élément de G possède un inverse

2) Supposons que $\text{Card}(A) = n$.

1) Mq : $\text{Card}(G) = 2 \cdot n$

Rappel. Soient E et F deux ensembles.

Notons $E \times F = \left\{ (x, y) \,,\, \begin{matrix} x \in E \\ y \in F \end{matrix} \right\}$. Alors

$$\mathrm{Card}(E \times F) = \mathrm{Card}(E) \times \mathrm{Card}(F)$$

On a :

$$\mathrm{Card}(G) = \underbrace{\mathrm{Card}(A)}_{=n} \cdot \underbrace{\mathrm{Card}(E)}_{=2} = 2n$$

2) Mq G possède au moins n éléments d'ordre 2.

On sait que le neutre de G est $(e_A, 1)$.

Un élément d'ordre 2 dans G est du type (a, x) avec $a \in A$, $x \in E$ tq

$$(a, x) \neq \underbrace{(e_A, 1)}_{\text{neutre de } G} \quad \text{et} \quad (a, x)^2 = (e_A, 1)$$

Soit $a \in A$. On a :

$$(a, -1)^2 = (a, -1) \cdot (a, -1)$$

$$(a, x) \cdot (b, y) = (a \cdot b^x, x \cdot y)$$

$$= (a a^{-1}, 1)$$

$$= (e_A, 1)$$

Les éléments de la forme $(a,-1)$ vérifie :

$$(a,-1) \neq (e_A, 1) \quad \text{et} \quad (a,-1)^2 = (e_A, 1)$$

donc ils sont d'ordres 2 et il y en a n (car il y a n valeurs possible pour a)

Ainsi, G contient au moins n éléments d'ordre 2.

On peut écrire G sous la forme :

$$G = \{(a, 1),\ a \in A\} \cup \underbrace{\{(a, -1),\ a \in A\}}_{\text{tous les éléments de cet ensemble sont d'ordre 2}}$$

Soit $a \in A$. Un élément $(a, 1)$ est d'ordre 2 ssi : $(a, 1) \neq (e_A, 1)$ et $\underbrace{(a, 1)^2}_{=(a^2, 1)} = (e_A, 1)$

ssi : $a \neq e_A$ et $a^2 = e_A$

ssi : a est un élément d'ordre 2

Il faut donc que A possède au moins un élément d'ordre 2.

Corrigé TD2

Exercice n° 27 . Soit G un groupe abélien fini et H, K ss groupes de G.

$$HK := \{ h \cdot k \ , \quad h \in H, k \in K \}$$

1) Montrer que HK est un sous-groupe de G

- $H \cdot K$ possède un élément neutre qui est $1_H \cdot 1_K$. En particulier : $H \cdot K \neq \emptyset$.

- $HK \subseteq G$ car $\forall h \in H, \forall k \in K : hk \in G$.

Rappel : Une partie H d'un groupe $(G, \cdot)$ est un sous-groupe de $(G, \cdot)$ ssi :

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

- Soient x et y deux éléments dans HK.

Montrons que $x \cdot y^{-1} \in HK$:

$$\begin{cases} \exists (h,k) \in H \times K, & x = hk \\ \exists (h',k') \in H \times K, & y = h'k' \end{cases}$$

Donc : $x \cdot y^{-1} = hk \cdot k'^{-1} h'^{-1}$

$= \underbrace{h \cdot h'^{-1}}_{\in H} \cdot \underbrace{k \cdot k'^{-1}}_{\in K}$

car G est abélien

car H sous-groupe de G

car K sous-groupe de G

$\in HK$

Ainsi, HK est un sous groupe de G

2) Soit $\varphi : \begin{array}{ccc} H \times K & \longrightarrow & HK \\ (h,k) & \longmapsto & h \cdot k \end{array}$

Montrer que φ est un morphisme de groupes.

Rappel. Soient $(G, *)$ et (H, Δ) deux groupes alors une application $f : G \to H$ est un morphisme de groupes si $\forall x, y \in G$:

$$f(x * y) = f(x) \Delta f(y)$$

- Loi sur $H \times K$: si $(h_1, k_1) \in H \times K$ et $(h_2, k_2) \in H \times K$:

$$(h_1, k_1) \odot (h_2, k_2) := (h_1 h_2, k_1 k_2)$$

Muni de cette loi, $(H \times K, \cdot)$ est un sous-groupe de G.

Soient $(h,k) \in H \times K$ et $(h',k') \in H \times K$,

$$\varphi\big((h,k)\cdot(h',k')\big) = \varphi\left(hh', kh'\right)$$

$$= h\cdot h'\cdot k\cdot k'$$

$$= \underbrace{h\cdot k}_{\varphi(h,k)} \cdot \underbrace{h'\cdot k'}_{\varphi(h',k')}$$

$$= \varphi(h,k)\cdot\varphi(h',k')$$

2) Déterminer l'image de φ.

Rappel : Soit $f : G \to H$ un morphisme de groupe.

- L'image de f est le sous-groupe de H suivant :

$$\mathrm{Im}(f) = \{ f(x),\ x \in G \}$$

- Le noyau de f est le sous-groupe de G suivant :

$$\mathrm{Ker}(f) = \{ x \in G,\ f(x) = e_H \}$$

$$\operatorname{Im}\varphi := \{ \varphi(h,k) \ , \quad (h,k) \in H \times K \}$$

$$= \{ hk \ , \quad (h,k) \in H \times K \}$$

$$= HK$$

Donc $\operatorname{Im}\varphi = HK$

- Mentions que $\operatorname{Ker}\varphi = \{ (h, h^{-1}) \ , \ h \in H \cap K \}$

$$\ker \varphi = \{ (h,k) \in H \times K \,,\ \varphi(h,k) = 1_{HK} \}$$

$1_{HK} = 1_G$

$$= \{ (h,k) \in H \times K \,,\ hk = 1_G \}$$

$$= \{ (h,k) \in H \times K \,,\ k = h^{-1} \}$$

$$\overset{(*)}{=} \{ (h, h^{-1}) \,,\ h \in H \cap K \}$$

(*) Détails ① si $(h,k) \in H \times K$ tq $k = h^{-1}$ alors $(h,k) = (h, h^{-1})$ et comme $h = k^{-1} \in K \cap H$

② Si $(a,b) \in \{(h,h^{-1}), h \in H \cap K\}$ alors :

$\exists h \in H \cap K$ tq : $\begin{cases} a = h \\ b = h^{-1} \end{cases}$

donc $(a, b) = (h, h^{-1}) \in H \times K$

$h \in H$; $h^{-1} \in K$ car $h \in H \cap K$

3) Montrer que HK est isomorphe à un quotient du groupe $H \times K$.

Rappel. Si G et H sont deux groupes, on dit qu'ils sont isomorphes s'il existe un morphisme

bijectif $f : G \to H$

Il faut trouver un sous-groupe V de $H \times K$ et un morphisme bijectif :

$$\Psi : {}^{H\times K}/_{V} \longrightarrow \underbrace{HK}_{= Im(\varphi)}$$

Rappel (Cas particulier du Théo. de Factorisation)

Soient G et H deux groupes et $\varphi : G \to H$

un morphisme de groupe. Alors il existe un morphisme bijectif entre $G/\ker f$ et $\operatorname{Im} f$ qui est :

$$\begin{aligned} \psi : G/\ker f &\to \operatorname{Im} f \\ cl(x) &\mapsto f(x) \end{aligned}$$

Posons $V := \ker \varphi$. Alors V est un sous-groupe de $H \times K$ et on a d'après le Théorème de

Factorisation : l'existence d'un morphisme bijectif : $\Psi : H \times K / V \to HK = \mathrm{Im}\,\Psi$

2.4) Montrer que $|HK| = \dfrac{|H| \cdot |K|}{|H \cap K|}$

- G est fini et HK est un sous-groupe de G donc HK est de cardinal fini.

Rappel :

- Si G groupe fini et H sous-groupe de G alors G/H est de cardinal fini égal à :

$$\frac{|G|}{|H|}$$

- Si A et B sont deux ensembles finis et $f : A \to B$ une bijection alors $|A| = |B|$

Donc :

$$|HK| = \frac{|H \times K|}{|\mathrm{Ker}\ \varphi|}$$

Montrons que $|\mathrm{Ker}\ \varphi| = |H \cap K|$. Posons :

$$g : \begin{array}{ccc} \mathrm{Ker}\ \varphi & \longrightarrow & H \cap K \\ (h, h^{-1}) & \longmapsto & h \end{array}$$

- <u>g injective</u> car si $g(h, h^{-1}) = g(h', h'^{-1})$

alors $h = h'$ donc $(h, h^{-1}) = (h', h'^{-1})$

- g surjective car si $h \in H \cap K$ alors (h, h^{-1}) est un antécédent de h par g car $g(h, h^{-1}) = h$

Ainsi,

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}$$

Exercice n° 28 et 30 : À faire à la maison

Exercice n° 29

I/ Soit $(\mathcal{C}, .)$ un groupe monogène engendré par $x \in \mathcal{C}$: $\mathcal{C} = \langle x \rangle$

Soit A sous-groupe de $\mathcal{C}$. Montrer qu'il existe $k \in \mathbb{N}$, $A = \langle x^k \rangle$

Rappel : $\langle x \rangle := \{ x^p , p \in \mathbb{Z} \}$

- Si $A = \{e\}$. Posons $k = 0$. Alors

$$\langle x^0 \rangle = \langle e \rangle = \{ e^p, p \in \mathbb{Z} \}$$
$$= \{ e, p \in \mathbb{Z} \} = \{e\} = A$$

Donc $A = \langle x^0 \rangle$

- Si $A \neq \{e\}$. Posons $X = \{ n \in \mathbb{N}^*, x^n \in A \}$

Notons $k := \min X$. Mq : $A = \langle x^k \rangle$

En particulier $k \in X$
càd : $x^k \in A$

(D) Soit $y \in \langle x^h \rangle$. Alors $\exists p \in \mathbb{Z}$,

$$y = \left(x^h\right)^p$$

donc $y = \underbrace{x^h \cdots x^h}_{p\text{-fois}} \in A$ car A est un sous-groupe de $(\mathcal{C}, \cdot)$

($x^h \in A$ et $x^h \in A$)

donc $\langle x^h \rangle \subset A$

(C) Soit $a \in A$. Alors $a \in \mathcal{C} = \langle x \rangle$

donc $\exists p \in \mathbb{Z}$: $a = x^p$

Montrons que $a \in \langle x^k \rangle$ c'est $\exists q \in \mathbb{Z}$, $a = x^{kq}$

À SAVOIR

Effectuons la division euclidienne de p par k :

$$\exists (q, r) \in \mathbb{Z}^2 : \begin{cases} p = k \cdot q + r \\ 0 \leq r < k \end{cases}$$

Si on montre que $r \in X$ alors comme k est le plus petit élément de X et que $r < k$ on a alors $r = 0$

Montrons que $r \in X$ c'est-à-dire : $x^r \in A$

Comme $p = k \cdot q + r$ alors $r = p - kq$

donc $x^r = x^{p-kq} = x^p \cdot x^{-kq}$

$= \underbrace{x^p}_{= a \in A} \cdot \underbrace{\left(x^k\right)^{-q}}_{\in A} \in A$.

Donc $r = 0$ d'où $a = x^p = x^{kq} = \left(x^k\right)^q \in \langle x^k \rangle$

Finalement, $A = \langle x^k \rangle$

I/

1) A faire à la maison.

2) Supposons que $K \neq \{e_G\}$. Soit $a \in G \setminus \{e\}$.

a) Mq : $\exists n \in \mathbb{N}$: $K = \langle a^n \rangle$

Posons $\mathcal{C} = \langle a \rangle$, c'est un sous-groupe de G et $\mathcal{C} \neq \{e\}$.

Donc $\mathcal{C} \in \mathcal{P}$

Donc $$K := \bigcap_{H \in \mathcal{P}} H$$

$$= \bigcap_{\substack{H \in \mathcal{P} \\ H \neq \mathcal{C}}} H \cap \mathcal{C}$$

$$\subseteq \mathcal{C}$$

On montre que K est un sous-groupe de $\mathcal{C}$.

D'après I/ : $\boxed{\exists n \in \mathbb{N} : K = \langle a^n \rangle}$

b) Supposons que a est d'ordre infini c'est-à-dire que :

$$\forall p \in \mathbb{N}^* : a^p \neq e_G$$

ou de manière équivalente :

$$\left(a^p = e_G\right) \Rightarrow \left(p = 0\right)$$ (utile pour (iii))

i) Posons $\forall k \in \mathbb{N}$: $H_k = \langle a^k \rangle$

$\boxed{\Rightarrow}$ Soit $m \in \mathbb{N}$: $H_k \subseteq H_m$ et

montrons que : $m \mid k$. La DE de k par m donne : $\exists (q,r) \in \mathbb{Z}^2$:

$$\begin{cases} k = mq + r \\ 0 \leq r < m \end{cases}$$

On va montrer que r est un multiple de m.

$$a^r = a^{k-mq} = a^k \cdot \left(a^m\right)^{-q}$$

$a^k \in H_k \subset H_m$; $\left(a^m\right)^{-q} \in H_m$; donc $a^r \in H_m$

Donc $a^r \in H_m = \langle a^m \rangle$

donc $\exists q \in \mathbb{Z} : \quad a^r = a^{mq}$

donc $a^{r-mq} = e$

donc comme a est d'ordre infini :

$$r - mq = 0$$

donc $r = mq$ et ainsi :

$$k = m(q+q')$$

donc : $\boxed{m \text{ divise } k}$

$\Leftarrow$ Supposons que m divise k. Alors

$\exists q \in \mathbb{Z} : \quad k = mq.$

Montrons que $H_k \subset H_m$. Soit $x \in H_k$

Alors $\exists q' \in \mathbb{Z} : \quad x = a^{kq'}$

Donc $x = a^{mqq'} = \left(a^m\right)^{qq'} \in H_m$

$k = mq$

donc : $\boxed{H_k \subset H_m}$

ii) À finir

c) Pareil

Exercice n° 28

1) • $\operatorname{Ker} f$ est un sous-groupe de $(G, .)$

• Soient $x \in G$ et $h \in \operatorname{Ker} f$. Montrons que $xhx^{-1} \in \operatorname{Ker} f$. On a :

$$f(xhx^{-1}) = f(x)\underbrace{f(h)}_{=e}f(x^{-1}) = f(x)f(x^{-1}) = f(xx^{-1})$$

(f est un morphisme de groupe)

$$= f(e) = e$$

donc $\operatorname{Ker} f$ est distingué dans G

2) • $HK \neq \emptyset$ car $1_H \cdot 1_K \in HK$

• Soient $x, y \in HK$. Alors $\exists\, (h,k) \in H \times K$

$(h',k') \in H \times K$: $\begin{cases} x = hk \\ y = h'k' \end{cases}$

donc $x \cdot y^{-1} = h \cdot k \cdot k'^{-1} \cdot h'^{-1}$

$= h \cdot \underbrace{(kk'^{-1})}_{\in G} \underbrace{h'^{-1}}_{\in H} \underbrace{(kk'^{-1})^{-1}}_{\in G} \cdot\ kk'^{-1}$

$\underbrace{\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad}_{\in H \text{ car } H \text{ est distingué dans } G}$

$\underbrace{\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad}_{\in HK}$

$\in H$ $\qquad$ $\in H$ $\qquad$ $\in K$

Donc HK est un sous-groupe de G.

Exercice n° 30

1) • Notons $n = \text{ordre}(x)$. Alors $\left(f(x)\right)^n = f(x^n) = f(e) = e$

(f morphisme)

donc $f(x)$ est d'ordre fini et d'après le Rappel :

Rappel : Si $a \in G$ tq $a^n = e$

Alors l'ordre de a divise n

On obtient que l'ordre de $f(x)$ divise l'ordre de x

2) Mq : l'ordre de x divise l'ordre de $f(x)$

Notons : $\begin{cases} n = o(x) \\ m = o(f(x)) \end{cases}$ et mq : $n \mid m$.

La DE (division euclidienne) de m par n donne :

$\exists (q, r) \in \mathbb{Z}^2$: $\begin{cases} m = nq + r \\ 0 \leq r < n \end{cases}$

Il suffit de montrer que $x^r = e$ et donc conclure par minimalité de n.

On a :

$$f(x^r) = f\left(x^{m-nq}\right) = \underbrace{f(x)^m}_{=e}\left(\underbrace{f\left(x^n\right)}_{=e}\right)^q = e$$

donc $x^r \in \operatorname{Ker} f$. Comme f est injective, alors $\operatorname{Ker} f = \{e\}$ donc $x^r = e$.

Ainsi, $r = 0$ et donc n divise m.

On a montré avant que m divise n donc finalement :

$$\boxed{n = m}$$

3) Supposons qu'il existe un isomorphisme :

$$f : (\mathbb{C}^*, \cdot) \to (\mathbb{R}, +)$$

Posons $z = i$. Alors z est d'ordre 4 car

$$\begin{cases} z^2 = -1 \neq 1 \\ z^3 = -i \neq 1 \end{cases} \quad \text{et} \quad z^4 = 1$$

Donc $0 = f(1) = f(z^4) = 4 f(z)$

↑ neutre de $(\mathbb{R}, +)$; ↑ neutre de $(\mathbb{C}^*, \cdot)$; ↑ f morphisme

donc $f(z) = 0$ ce qui veut dire que

$f(z)$ est d'ordre 1 ABSURDE (d'après la question précédente, on devrait avoir $\forall z \in \mathbb{C}^*$: z et $f(z)$ ont même ordre !)

Corrigé TD3

Exercice n° 31

Soit $(G, *)$ groupe $G \neq \{e\}$ abélien.

Deux lois sur $End(G)$: ($End(G)$ = { morphisme de groupe de G dans G })

- $(f+g)(x) := f(x) * g(x)$
- $(f \circ g)(x) := f(g(x))$

Montrer que $(End, +, \circ)$ est anneau

Rappel : Soit A un ensemble muni de deux lois de composition interne $+$ et $\times$.

On dit que $(A, +, \times)$ est un anneau si

1. $(A, +)$ groupe commutatif,
2. $\times$ est associative et possède un neutre,
3. $\times$ est distributive par rapport à $+$

c'est-à-dire : $a \times (b + c) = a \times b + a \times c$

$\forall a, b, c \in A$

Rappel (sur les groupes). Soit G un groupe muni de $*$. $H \subseteq G$

- $\forall x, y \in H,\ x * y \in H$
- $\forall x \in H,\ x^{-1} \in H$

$\Leftrightarrow$

$\forall x, y \in H :\ x * y^{-1} \in H$

$\Rightarrow$ Soit $x, y \in H$,

$x * \underbrace{y^{-1}}_{\in H} \in H$ par produit

$\Leftarrow$ • Soit $x, y \in H$

$x * y = x * (y^{-1})^{-1}$

$= x * z^{-1}$

avec $z = y^{-1}$ donc $x * y \in H$

- Si $x \in H$, $x = x * 1_G^{-1}$

$\in H$

- $(End(G), +)$ est un groupe.

- La loi $+$ est bien une l.c.i car

si $f, g \in End(G)$ alors $f + g \in End(G)$

$$(f+g)(x+y) = f(x+y) * g(x+y)$$

$$= f(x) * f(y) * g(x) * g(y)$$

$(G, *)$ est abélien $\rightarrow$

$$= [f(x) * g(x)] * [f(y) * g(y)]$$

$$= (f+g)(x) * (f+g)(y)$$

$\forall x, y \in G$.

- Associativité. Soient $f, g, h \in End(G)$

$$\forall x \in G, \quad \big((f+g)+h\big)(x) = \big(f(x) * g(x)\big) * h(x)$$

$$= f(x) * \left(g(x) * h(x)\right)$$

$*$ est associative

$$= f(x) * \left((g+h)(x)\right)$$

$$= \left(f + (g+h)\right)(x)$$

donc on a montré que $(f+g)+h = f+(g+h)$

• Neutre. Soit $f \in End(G)$. Trouvons

$g \in End(G)$ tq : $f + g = f$

càd : $\forall x \in G$: $(f+g)(x) = f(x)$

c'ad : $\forall x \in G$: $f(x) * g(x) = f(x)$ $) \in G$

$f(x) \in G$; $g(x) \in G$; $=$: égalité dans G

donc la fonction g est l'application :

$$0_{End(G)} : \begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & e \end{array}$$

c'est l'élément neutre de $End(G)$

car $\forall f \in End(G)$, $\forall x \in G$

$$\left(f + 0_{End(G)}\right)(x) = f(x) * 0_{End(G)}(x)$$

$$= f(x) * e$$

$$= f(x)$$

donc $\forall x \in G$: $\left(f + 0_{End(G)}\right)(x) = f(x)$

donc $f + 0_{End(G)} = f$

Ainsi $0_{End(G)}$ est bien l'élément neutre de $End(G)$

- Symétrie : Soit $f \in End(G)$

Trouvons $g \in End(G)$ tq $f + g = 0_{End(G)}$

c'à d : $\forall x \in G$: $(f+g)(x) = 0_{End(G),(x)}$

c'à d : $\forall x \in G$: $f(x) * g(x) = e$

donc $\forall x \in G$: $g(x) = \left(f(x)\right)^{-1}$

$f(x)$ est un élément de G. donc, $f(x)^{-1}$ = inverse de $f(x)$ dans G

Donc l'inverse de f est l'application :

$$\begin{aligned} G &\longrightarrow G \\ x &\longmapsto \left(f(x)\right)^{-1} \end{aligned}$$

- $End(G)$ est commutatif car $\forall f, g \in End(G)$

$\forall x \in G$:

$$\begin{aligned} (f+g)(x) &:= f(x) * g(x) \\ &= g(x) * f(x) \quad \text{(G abélien)} \\ &=: (g+f)(x) \end{aligned}$$

Donc $f + g = g + f$.

Ainsi, $(End(G), +)$ groupe commutatif.

- Montrons que la loi $\circ$ est associative et possède un neutre.

Soit $f, g, h \in End(G)$. Montrons que :

$$(f \circ g) \circ h = f \circ (g \circ h)$$

$\forall x \in G$:

$$\begin{aligned}
\big[(f \circ g) \circ h\big](x) &= (f \circ g)\big(h(x)\big) \\
&= f\Big(g\big(h(x)\big)\Big) \\
&= f\Big((g \circ h)(x)\Big) \\
&= \big[f \circ (g \circ h)\big](x)
\end{aligned}$$

Donc $\circ$ est bien associative !

Soit $f \in End(G)$. Trouvons $g \in End(G)$

tq : $f \circ g = f$

c'à d : $\forall x \in G$: $f(g(x)) = f(x)$

Posons : id_G : $G \longrightarrow G$, $x \longmapsto x$

Alors $id_G \in End(G)$ et :

$id_G \circ f = f \circ id_G = f$

Ainsi, id_G est l'élément neutre pour $\circ$

- **Distributivité de $\times$ par rapport à $+$**

Soit $f, g, h \in End(G)$. Montrons que

$$f \circ (g + h) = f \circ g + f \circ h$$

On a $\forall x \in G$:

$$\left[f \circ (g + h)\right](x) = f\left((g+h)(x)\right)$$

$$= f\left(g(x) * h(x)\right)$$

$$= f\left(g(x)\right) * f\left(h(x)\right)$$

f morphisme de groupe

$$= f \circ g(x) * f \circ h(x)$$

$$= \left(f \circ g \,(+)\, f \circ h\right)(x)$$

Ainsi, $f \circ (g+h) = f \circ g + f \circ h$.

Finalement : $(\mathrm{End}(G), +, \circ)$ est un anneau

Exercice n° 32 : À faire

Exercice n° 33 : Soit $d \in \mathbb{N}^*$.

Posons $A_d = \{(x,y) \in \mathbb{Z}^2, \ d \mid y-x\}$

1) Montrer que A_d est un sous-anneau de $(\mathbb{Z} \times \mathbb{Z}, +, \times)$

But : Soit A sous anneau de $(\mathbb{Z} \times \mathbb{Z}, +, \times)$

Mq : $\exists d \in \mathbb{N}$: $A = A_d$

Rappel : Soient $(A, +, \times)$ un anneau et B une partie de A ($B \neq \emptyset$). On dit que B est un sous-anneau de $(A, +, \times)$ si

1. B sous groupe de $(A, +)$
2. $\forall x, y \in B^2 : \quad x \cdot y \in B$
3. Le neutre de A appartient à B

- La loi $\vec{+}$ sur $\mathbb{Z}\times\mathbb{Z}$: Si $n, m \in \mathbb{Z}\times\mathbb{Z}$ $p, q \in \mathbb{Z}\times\mathbb{Z}$

$$(n, m) + (p, q) := (n+p, m+q)$$

- La loi $\vec{\times}$ sur $\mathbb{Z}\times\mathbb{Z}$: Si $n, m \in \mathbb{Z}\times\mathbb{Z}$ $p, q \in \mathbb{Z}\times\mathbb{Z}$

$$(n, m) \times (p, q) := (n\times p, m\times q)$$

- Montrons que A_d est un sous-groupe de $(\mathbb{Z}\times\mathbb{Z}, +)$

- $A_d \neq \emptyset$ car : $(0,0) \in A_d$ car

  d divise $0-0$ (car $0 = d \cdot \underbrace{0}_{\in \mathbb{Z}}$)

- Soient $(n, m) \in A_d$ et $(p, q) \in A_d$

  Montrer que :

$$(n-p, m-q) \in A_d$$

càd : montrer que :

$$d \mid (m-q)-(n-p)$$

càd : montrer que :

$$d \mid (m-n)-(q-p)$$

Puisque $(n, m) \in A_d$ alors d divise $m-n$

et de même, $(p, q) \in A_d$ donc d divise $q-p$

Rappel : Si n divise a et n divise b alors n divise $a-b$

(car $\exists k, k' \in \mathbb{Z}$: $a = dk$ et $b = dk'$

donc $a - b = d(\underbrace{k - k'}_{\in \mathbb{Z}})$)

Donc d divise $(m-n) - (q-p)$

Ainsi, A_d = sous-groupe de $(\mathbb{Z}\times\mathbb{Z}, +)$

- Soient $(n, m) \in A_d$ et $(p, q) \in A_d$.

  Montrons que : $(n, m) \cdot (p, q) \in A_d$.

  c'est-à-dire : d divise $mq - np$.

  On sait que : $\exists k, k' \in \mathbb{Z}$: $\begin{cases} m - n = dk \\ q - p = dk' \end{cases}$

$$mq - np = (m-n)(q-p) + mp + nq - 2np$$

$(*)$: $mp + nq - 2np = mp - np + nq - np$

$-2np = -np - np$

$= p(m-n) + n(q-p)$

Donc :

$$mq - np = \underbrace{(m-n)(q-p)}_{\text{divisible par } d} + p\underbrace{(m-n)}_{/\!/} + n\underbrace{(q-p)}_{/\!/}$$

- Le neutre de $\mathbb{Z}\times\mathbb{Z}$ pour $\times$ appartient à A_d.

Le neutre de $\mathbb{Z}\times\mathbb{Z}$ pour $\times$: $(1,1)$

et $1-1$ divisible par d donc $(1,1)\in A_d$

Finalement, A_d est un sous-anneau de $(\mathbb{Z}\times\mathbb{Z}, +, \times)$

2) Soit A un sous-anneau de $(\mathbb{Z}\times\mathbb{Z}, +, \times)$

a) • Pourquoi $(1,1) \in A$.

Le neutre de $\mathbb{Z}\times\mathbb{Z}$ pour la loi $\times$ est :

$$(1,1)$$

qui appartient à A car A sous-anneau.

• $\forall n \in \mathbb{N} : (n,n) \in A$. Soit $n \in \mathbb{N}$

$$(n,n) = \underbrace{(1,1)}_{\in A} + \underbrace{\dots}_{n\text{-fois}} + \underbrace{(1,1)}_{\in A} \in A$$

$\uparrow$ $(A,+)$ groupe

- $\forall m \in \mathbb{Z} : (m, m) \in A$

  - Si $m \geqslant 0$: OK d'après la question d'avant

  - Si $m < 0$: $(m, m) = -(\underbrace{-m}_{\in \mathbb{N}}, \underbrace{-m}_{\in \mathbb{N}})$

    $\in A$

    $\in A$ car $(A, +)$ groupe et donc l'inverse d'un élément de A est dans A.

b) En déduire que si $(x,y) \in A$ alors $(x-y, 0) \in A$

Soit $x, y \in \mathbb{R}$.

$$(x-y, 0) = \underbrace{(x,y)}_{\in A} + \underbrace{(-y, -y)}_{\in A \text{ car } -y \in \mathbb{R}}$$

$\in A$

↑ car $(A, +)$ groupe.

c) Montrer que : $H := \{ x \in \mathbb{Z},\ (x,0) \in A \}$ sous groupe de $(\mathbb{Z}, +)$

- $H \neq \emptyset$ car $0 \in H$.
- Soit $x, y \in H$. Montrons que $x - y \in H$

  On sait que : $(x,0) \in A$ et $(y,0) \in A$

  donc $(x-y, 0) = \underbrace{(x,0)}_{\in A} - \underbrace{(y,0)}_{\in A} \in A$

donc $x - y \in H$

d) Montrer que $\exists d \in \mathbb{N}^* : \quad A = A_d$

Rappel : Si H est un sous-groupe de $(\mathbb{Z}, +)$

alors $\exists n \in \mathbb{N} : \quad H = n\mathbb{Z}$

$= \{nk, k \in \mathbb{Z}\}$

Donc :

$$\exists d \in \mathbb{N}^*, \quad \{x \in \mathbb{Z}, (x,0) \in A\} = d\mathbb{Z}$$

- Montrons que $A \subseteq A_d$:

Soit $(x,y) \in A$. Alors d'après 2)b) :

$(x-y, 0) \in A$ donc $x - y \in$

Corrigé TD3

Exercice n°33 (suite)

- **Montrons que $A \subseteq A_d$:**

Soit $(x,y) \in A$. Alors d'après 2)b) :

$(x-y, 0) \in A$ donc $x - y \in H = d\mathbb{Z}$

car $H = \{p \in \mathbb{Z},\ (p,0) \in A\}$

donc $x - y \in d\mathbb{Z}$

Or $d\mathbb{Z} := \{ d \cdot k \,,\ k \in \mathbb{Z} \}$

donc $\exists\, k \in \mathbb{Z}$, $x - y = dk$.

donc $\exists\, k' \in \mathbb{Z}$, $y - x = dk'$

donc d divise $y - x$

donc $(x, y) \in A_d$. car $A_d := \{(x,y) \in \mathbb{Z}\times\mathbb{Z},$ d divise $y-x\}$

On a montré que $A \subseteq A_d$.

- **Montrons que $A_d \subseteq A$**

Soit $(x,y) \in A_d$. Alors d divise $y-x$.

donc $x-y \in d\mathbb{Z} = \{p \in \mathbb{Z} \mid (p,0) \in A\}$

donc $(x-y,0) \in A$. Or :

$$(x,y) = \underbrace{(x-y,0)}_{\in A} + \underbrace{(y,y)}_{\in A \text{ d'après 2) a)}}$$

Puisque $(A, +)$ est un groupe, alors $(x, y) \in A$. Ainsi $A_d \subseteq A$

Finalement : $\boxed{A = A_d}$

Exercice n°34

$$\mathbb{Z}[i] := \left\{ z \in \mathbb{C}, \ \exists (a,b) \in \mathbb{Z}^2 : \ z = a + ib \right\}$$

1) • $\mathbb{Z}[i] \subseteq \mathbb{C}$

- $(\mathbb{Z}[i], +)$ est un groupe abélien

  À vérifier !

- Stabilité pour la loi $\times$: Soient $z, z' \in \mathbb{Z}[i]$.

alors $\exists\, a, a', b, b' \in \mathbb{Z}$: $\begin{cases} z = a+ib \\ z' = a'+ib' \end{cases}$

Montrons que $zz' \in \mathbb{Z}[i]$

$$z \times z' = (a+ib)(a'+ib')$$

$$= \underbrace{(aa' - bb')}_{\in \mathbb{Z}} + i \underbrace{(ab' + a'b)}_{\in \mathbb{Z}}$$

$$\in \mathbb{Z}[i]$$

- Montrons que $1_{\mathbb{C}} \in \mathbb{Z}[i]$

Déjà : $1_{\mathbb{C}} = 1$

et $1 = \underbrace{1}_{\in \mathbb{Z}} + \underbrace{0}_{\in \mathbb{Z}} \cdot i \in \mathbb{Z}[i]$

2) Mq : $\forall z, z' \in \mathbb{Z}[i]$:

$$M(zz') = M(z) \times M(z')$$

où M : $\begin{cases} \mathbb{Z}[i] \longrightarrow \mathbb{N} \\ z = a+ib \longmapsto a^2 + b^2 \end{cases}$

Soient $z, z' \in \mathbb{Z}[i]$, $\exists a, a', b, b' \in \mathbb{Z}$:

$z = a+ib$, $z' = a' + ib'$. On a :

- $M(zz') = M\left([aa' - bb'] + i[ab' + a'b]\right)$
$= (aa' - bb')^2 + (ab' + a'b)^2$

$$= (aa')^2 + (bb')^2 - \cancel{2aa'bb'} + (ab')^2 + (a'b)^2$$

$$+ \cancel{2aa'bb'}$$

- $N(z) \cdot N(z') = (a^2+b^2)(a'^2 + b'^2)$

$$= (aa')^2 + (ab')^2 + (ba)^2 + (bb')^2$$

$$= N(zz')$$

3) • a) $\Rightarrow$ b) Soit z un élément inversible dans $\mathbb{Z}[i]$. Alors il existe $z' \in \mathbb{Z}[i]$: $zz' \overset{(*)}{=} 1$

Rappel : Soit $(A, +, \times)$ un anneau et $a \in A$.
On dit que a est inversible dans A si il existe $b \in A$ tel que

$$ab = ba = 1_A$$

L'ensemble des inversibles de A est noté $\mathcal{U}(A)$

Montrons que $M(3) = 1$. D'après (*)

on a $M(3 \cdot 3') = M(1) = 1$

$= M(3) \cdot M(3')$

donc : $M(3) \cdot M(3') = 1$ (**)

Rappel : $(\mathbb{Z}, +, \times)$ est un anneau.

Les éléments inversibles de $\mathbb{Z}$ sont :

$\{-1, 1\}$

D'après (**), $M(3)$ est inversible dans $\mathbb{Z}$

donc ~~$M(3) = -1$~~ ou $M(3) = 1$

car $M(3) \in \mathbb{N}$

Donc $M(3) = 1$.

- **b) ⇒ c)** Soit $z \in \mathbb{Z}[i]$ tel que $N(z) = 1$. Montrer que $z \in \{\pm 1, \pm i\}$.

z s'écrit sous la forme $z = a+ib$, $a \in \mathbb{Z}$, $b \in \mathbb{Z}$.

Alors $N(z) = 1 \iff N(a+ib) = 1$

$\iff a^2 + b^2 = 1$

$\iff (a,b) \in \{(0,1);(0,-1);(1,0);(-1,0)\}$

$\Leftrightarrow z \in \{\pm i, \pm 1\}$

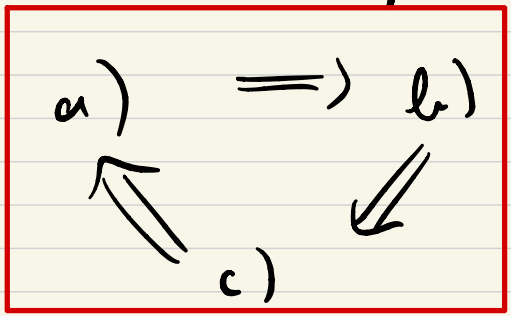
- c) $\Rightarrow$ a) Soit $z \in \{\pm i, \pm 1\}$

Montrons z est inversible dans $\mathbb{Z}[i]$.

- Si $z = i$: alors $z \in \mathcal{U}(\mathbb{Z}[i])$ d'inverse $-i$
- Si $z = -i$: // d'inverse i
- Si $z = 1$: // d'inverse 1
- Si $z = -1$: // d'inverse -1

Dans tous les cas : $z \in \mathcal{U}(\mathbb{Z}[i])$.

On a montré que :



donc a) $\Leftrightarrow$ b) $\Leftrightarrow$ c)

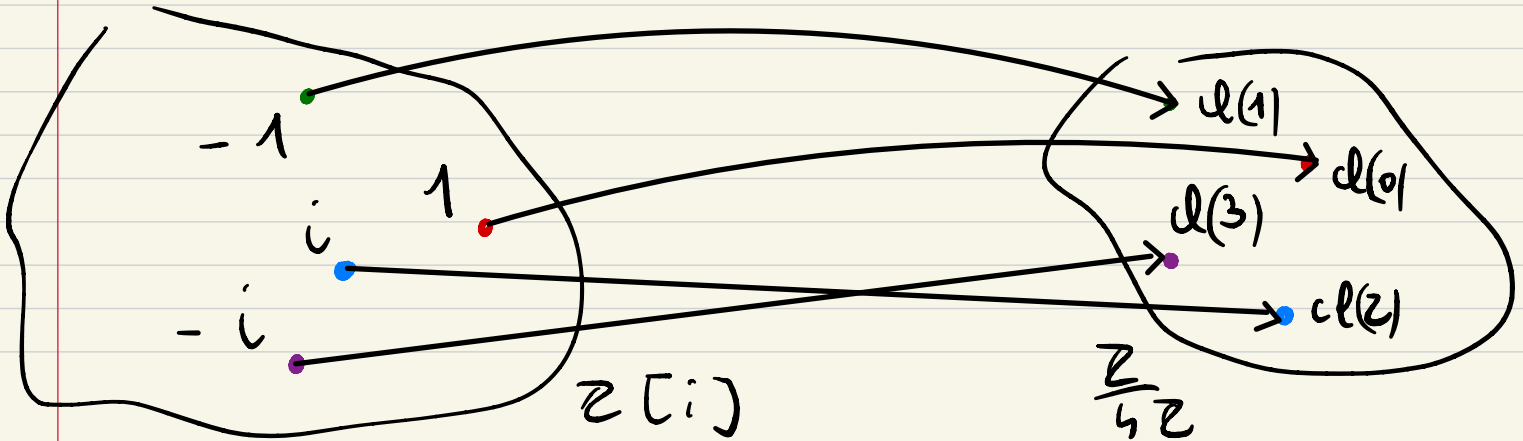
4) En déduire que $\mathcal{U}(\mathbb{Z}[i]) \underbrace{\simeq}_{\text{veut dire isomorphe.}} \frac{\mathbb{Z}}{4\mathbb{Z}}$.

On a montré que :

$$\mathcal{U}(\mathbb{Z}[i]) = \{-1, 1, -i, i\}$$

On $\dfrac{\mathbb{Z}}{4\mathbb{Z}} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$

avec $\forall m \in [\![0,3]\!]$: $\bar{m} = \{n \in \mathbb{Z},\ n - m \in 4\mathbb{Z}\}$



On définit une application

$$f : \mathcal{U}(\mathbb{Z}[i]) \longrightarrow \frac{\mathbb{Z}}{4\mathbb{Z}}$$

tq :

$$\begin{cases} \cdot\ f(-1) = \bar{0}(1) \\ \cdot\ f(1) = \bar{0}(0) \\ \cdot\ f(i) = \bar{0}(2) \\ \cdot\ f(-i) = \bar{0}(3) \end{cases}$$

le neutre de $\mathcal{U}(\mathbb{Z}[i])$ s'envoie sur le neutre de $\frac{\mathbb{Z}}{4\mathbb{Z}}$ par f

Vérifier que $\forall z z' \in \mathcal{U}(\mathbb{Z}[i])$:

$$f(z \cdot z') = f(z) + f(z')$$

loi sur le groupe $\mathcal{U}(\mathbb{Z}[i])$

loi sur le groupe $\frac{\mathbb{Z}}{4\mathbb{Z}}$

X	1	i	-1	-i
1	1	i	-1	-i
i	i	-1	-i	1
-1	-1	-i	1	i
-i	-i	1	i	-1

5) Soit $z \in \mathbb{Z}[i]$. Montrer que :

$N(z) \in \mathbb{P} \Rightarrow z$ est irréductible dans $\mathbb{Z}[i]$

$\mathbb{P}$: l'ensemble des nombre premiers

Rappel : Soit $(A, +, \times)$ un anneau commutatif intègre (c'à d $\forall a, b \in A \ (ab = 0) \Rightarrow (a = 0 \text{ ou } b = 0)$).

On dit qu'un élément $p \in A$ est irréductible

si $\begin{cases} \cdot\ p \text{ n'est pas inversible} \\ \cdot\ \text{Si } p = ab \text{ alors } a \text{ est inversible ou } b \text{ est inversible} \end{cases}$

- 3 n'est pas inversible. En effet, si 3 était inversible alors $3 \in \{-1, 1, i, -i\}$ et donc $N(3) = 1$ et par hypothèse, $\Pi(3) \in \mathbb{P}$ donc $1 \in \mathbb{P}$ ABSURDE !

- Supposons qu'il existe $z_1, z_2 \in \mathbb{Z}[i]$ tq $z = z_1 \cdot z_2$. Montrons que z_1 ou z_2 est inversible. On a :

$$\underbrace{N(z)}_{\in \mathbb{P}} = N(z_1) \cdot N(z_2)$$

donc $N(z_1) = 1$ ou $N(z_2) = 1$

d'après 3), on sait que :

$$\underbrace{(N(\omega) = 1)}_{b)} \implies \underbrace{(\omega \text{ inversible})}_{a)}$$

donc z_1 est inversible ou z_2 est inversible.

Finalement, z est irréductible dans $\mathbb{Z}[i]$.

6) Soit $f : \mathbb{Z}[i] \to \mathbb{Z}[i]$ un morphisme d'anneaux.

1) • Montrons que $\forall n \in \mathbb{N}$: $f(n) = n$

Soit $n \in \mathbb{N}$,

$$f(n) = f(\underbrace{1 + \dots + 1}_{n \text{ fois}})$$

$$= \underbrace{f(1) + \dots + f(1)}_{n \text{ fois}}$$ (f morphisme d'anneaux)

$$= \underbrace{1 + \dots + 1}_{n \text{ fois}}$$ ($f(1) = 1$)

$$= n.$$

Donc $\forall n \in \mathbb{N}$: $f(n) = n$.

- Si $n \in \mathbb{N}$,

$$f(-n) = f\Big(\underbrace{(-1)}_{\in \mathbb{Z}[i]} \times \underbrace{(n)}_{\in \mathbb{Z}[i]}\Big)$$

car $-1 = \underbrace{-1}_{\in \mathbb{Z}} + \underbrace{0}_{\in \mathbb{Z}} i$ car $n = \underbrace{n}_{\in \mathbb{Z}} + \underbrace{0}_{\in \mathbb{Z}} i$

$$= f(-1) \times f(n)$$

$$= -f(1) \times n = -n$$

Or : $f(-1) + f(1) = f(-1+1) = f(0) = 0$

donc l'inverse de $f(1)$ est égale à $f(-1)$

c'est-à-dire que : $-f(1) = f(-1)$

Donc $f(-n) = -n$, $\forall n \in \mathbb{N}$

- Montrons que $\forall n \in \mathbb{Z}$: $f(n) = n$

▸ Si $n \geq 0$: OK

▸ Si $n < 0$: $f(n) = f\left(-\underbrace{(-n)}_{\in \mathbb{N}}\right)$

$\forall n \in \mathbb{N}$, $f(-n) = -f(n)$

$= -f(-n)$

De même que précédemment, on montre que

l'inverse de $f(-m)$ est égal à $f(m)$

c'à d : $\quad -f(-m) = f(m)$

donc si $m < 0$ on a $f(m) = m$.

2) Mq : $f(i) \in \{-i, i\}$

On a :

$$1 = f(1) = f((-i)\,i)$$

$$= f(i) \times f(-i)$$

Donc $f(i)$ est inversible dans $\mathbb{Z}[i]$

Donc $f(i) = \{\pm 1, \pm i\}$.

Montrer que $f(i) \neq 1$ et $f(i) \neq -1$