Corrigé TD 1

Ex 1

1. $(m,n) \longmapsto m+2n = m \circ n$

<u>Associatif</u> : NON, car sinon on aurait pour tout $m, n, l \in \mathbb{N}$

$$(m \circ n) \circ l = m \circ (n \circ l)$$

En développant on obtient

$$(m \circ n) \circ l = (m+2n) \circ l$$
$$= m + 2n + 2l$$

et $m \circ (n \circ l) = m + 2(n+2l)$
$$= m + 2n + 4l$$

$\neq$

or $m + 2n + 2l \neq m + 2n + 4l$ (p.ex. pour $m = n = 0$, $l \neq 0$)

donc $\circ$ n'est pas associatif.

<u>Commutatif</u> : NON, car sinon on aurait pour tout $m, n \in \mathbb{N}$

$$m \circ n = n \circ m$$

On calcule

$$m \circ n = m + 2n$$
$$\neq$$
$$n \circ m = n + 2m$$

(par exemple pour $m = 0$ et $n \neq 0$).

<u>Neutre</u> : NON par l'absurde, s'il existait un neutre $e \in \mathbb{N}$ il devrait satisfaire la relation $e \circ n = n$ pour tout n

$\iff$ $e + 2n = n$

$\iff$ $e = -n$ pour tout n

ce qui est impossible (e ne dépend pas de n!)

1 bis

$$\mathbb{N} \times \mathbb{N} \to \mathbb{N}$$
$$(m, n) \mapsto \min(m, n) = \text{le plus petit des deux entiers } m \text{ et } n.$$
$$\min(m,n) = m \circ n$$

<u>Associatif</u> : OUI, car on a pour tout m, n, l la relation

$$(m \circ n) \circ l = m \circ (n \circ l)$$
$$\min(\min(m,n), l) = \min(m, \min(n,l))$$

en fait ces 2 expressions sont égales à $\min(m,n,l)$ = le plus petit des trois entiers m, n et l

<u>Commutatif</u> : OUI, car la relation

$$\min(m,n) = \min(n,m) \quad \text{pour tout } m,n$$

est évidente.

<u>Neutre</u> : NON, par l'absurde s'il existait un neutre $e \in \mathbb{N}$ on devrait avoir la relation

$$\min(n,e) = n \quad \text{pour tout } n$$

donc $e \geq n$

ce qui est impossible.

<u>Remarque</u> : Si on remplace min par max la loi de composition $(m,n) \mapsto \max(m,n)$ admet un neutre, qui est égal à $0 \in \mathbb{N}$.

2. $(m,n) \longmapsto \text{pgcd}(m,n)$

= plus grand commun diviseur de m et n

p.ex. $\text{pgcd}(15,21) = 3$

En fait cette loi de composition est liée à la loi précédente $(a,b) \mapsto \min(a,b)$.

Rappel: Tout entier est produit de puissances de nombres premiers

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$$

$$\left(\text{p.ex. } 100 = 2^2 \cdot 5^2\right)$$

et si on a deux nombres n et m avec

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} \quad \text{et} \quad m = p_1^{b_1} \cdot p_2^{b_2} \cdots p_k^{b_k}$$

alors. $\text{pgcd}(n,m) = p_1^{\min(a_1,b_1)} \cdot p_2^{\min(a_2,b_2)} \cdots p_k^{\min(a_k,b_k)}$

p.ex. $100 = 2^2 \cdot 5^2$

$15 = 3 \cdot 5$

$$\text{pgcd}(15,100) = \text{pgcd}\left(2^0 \cdot 3^1 \cdot 5^1, 2^2 \cdot 3^0 \cdot 5^2\right)$$

$$= 2^{\min(0,2)} \cdot 3^{\min(1,0)} \cdot 5^{\min(1,2)}$$

$$= 2^0 \cdot 3^0 \cdot 5^1 = 5$$

Ainsi, les propriétés de la loi $\min(m,n)$ donnent via cette relation les propriétés de la loi $\text{pgcd}(m,n)$.

Donc, $(m,n) \mapsto \text{pgcd}(m,n)$ est

- <u>associative</u>, car $\min(m,n)$ associatif
- <u>commutative</u>, car $\min(m,n)$ commutatif
- n'a <u>pas</u> de neutre, car $\min(m,n)$ n'a pas de neutre

3. On remplace min par max.
On en déduit que $(m,n) \mapsto \text{ppcm}(m,n)$ est

- <u>associative</u>
- <u>commutative</u>
- <u>admet un neutre</u>, qui est égal à 1

En effet pour tout n
$\text{ppcm}(1,n) = n$

pour déterminer les éléments inversibles (6

$n \in \mathbb{N}^*$ pour la loi ppcm, on cherche les couples d'entiers $(n, m) \in \mathbb{N}^* \times \mathbb{N}^*$ qui vérifient

$$\text{ppcm}(n, m) = 1.$$

Cette relation implique immédiatement que $n = 1$ et $m = 1$.

Donc $1 \in \mathbb{N}^*$ est le seul élément inversible.

4. $(A, B) \longmapsto A \cap B$ intersection de 2 sous-ensembles de X

$\cap$ est <u>associative</u>, car $(A \cap B) \cap C = A \cap (B \cap C)$

$\cap$ est <u>commutative</u>, car $A \cap B = B \cap A$

$\cap$ admet un élément <u>neutre</u>, égal à X, car $A \cap X = A$ pour tout sous-ensemble A

Le seul élément inversible est X, car

$$X \cap X = X.$$

5. $(A,B) \longmapsto A \cup B$ réunion de 2 sous-ensembles de X

$\cup$ est <u>associative</u>, car $A \cup (B \cup C) = (A \cup B) \cup C$

$\cup$ est <u>commutative</u>, car $A \cup B = B \cup A$

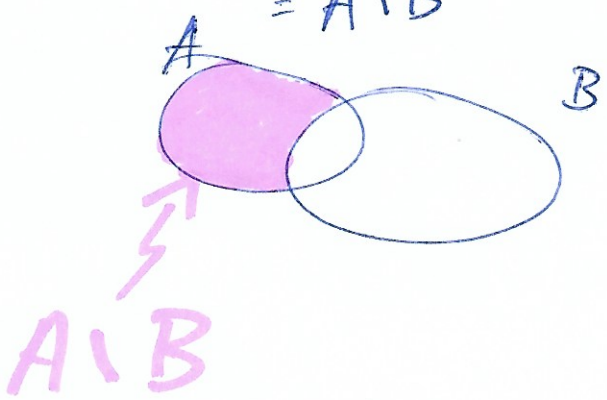
$\cup$ admet <u>un neutre</u>, égal à ϕ (= ensemble vide), car

$$A \cup \phi = A \quad \text{pour tout sous-ens. de } X$$

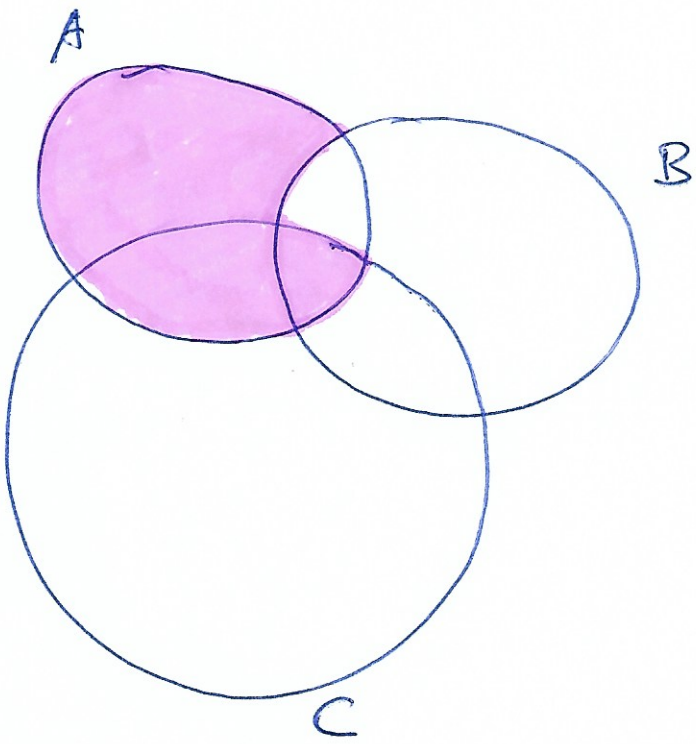
Le seul élément inversible est ϕ, car.

$$\phi \cup \phi = \phi.$$

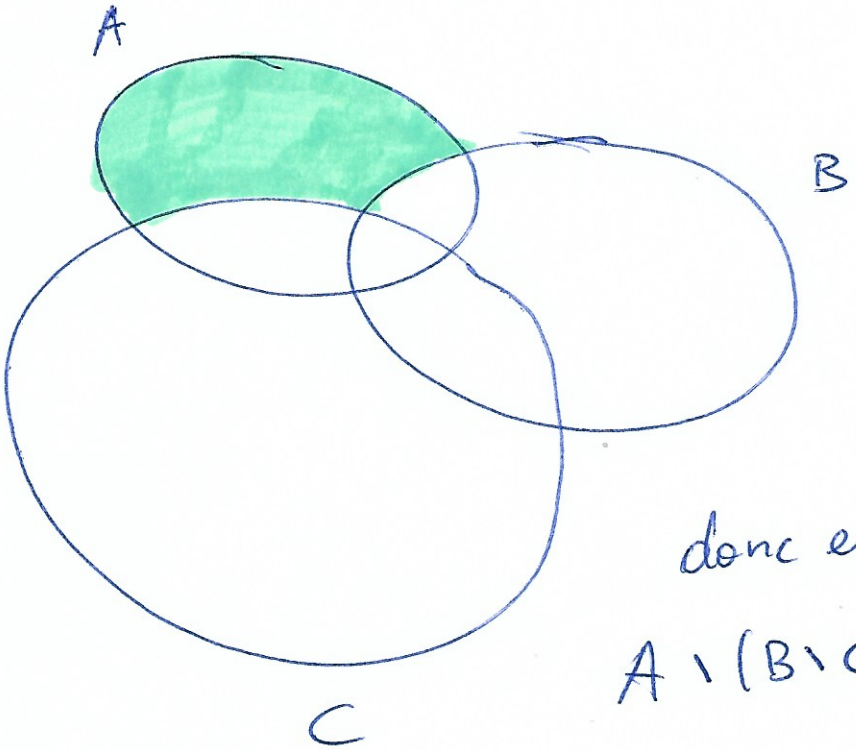
6. $(A,B) \longmapsto A \setminus (A \cap B)$ "A moins les éléments dans B".
$= A \setminus B$



$\setminus$ n'est <u>pas</u> <u>associative</u>, car sur le dessin suivant on le voit clairement !



$A \setminus (B \setminus C)$

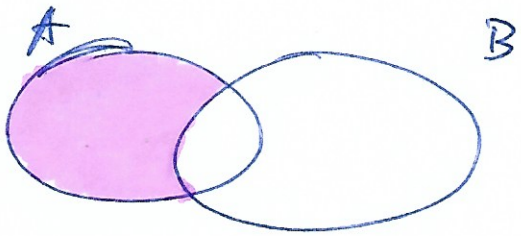


donc en général :

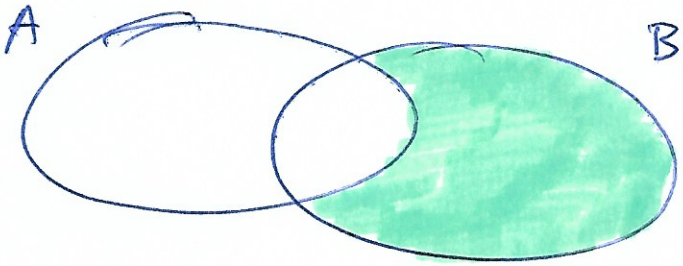
$A \setminus (B \setminus C) \neq (A \setminus B) \setminus C$

$(A \setminus B) \setminus C$

$\setminus$ n'est <u>pas</u> <u>commutative</u>, car on le voit sur le dessin



$A \setminus B$



$B \setminus A$

donc en général $A \setminus B \neq B \setminus A$.

$\setminus$ n'admet <u>pas</u> de neutre, car un élément neutre e doit satisfaire les relations suivantes pour tout $A \in \mathcal{P}(X)$

$$A \setminus e = A \quad \Rightarrow \quad e = \emptyset$$

$$e \setminus A = A \quad \Rightarrow \quad \text{contradiction}$$

(En fait le neutre existe que quand $X = \emptyset$).

7. $(f,g) \mapsto f \circ g$

$$\begin{tikzcd} X \arrow[r, "g"] \arrow[rr, bend right, "f\circ g"'] & X \arrow[r, "f"] & X \end{tikzcd}$$

$f \circ g$ = composée de 2 applications g et f, "d'abord g et ensuite f".

$\circ$ est <u>associative</u>, car pour tout $f, g, h \in \mathcal{A}(X,X)$

$$\begin{tikzcd} X \arrow[r, "h"] \arrow[rr, bend right] \arrow[rrr, bend right=60, "f\circ g\circ h"'] & X \arrow[r, "g"] \arrow[rr, bend right] & X \arrow[r, "f"] & X \end{tikzcd}$$

$$(f \circ g) \circ h = f \circ (g \circ h)$$

$\circ$ n'est <u>pas</u> <u>commutative</u> <u>en général</u>

par exemple voir (8.)

$\circ$ admet <u>un élément neutre</u>, qui est égal à l'identité de X $id_X : X \to X$
$x \mapsto x$.

en effet $id_X \circ f = f \circ id_X = f$ pour tout f

Les éléments inversibles sont les <u>bijections</u> de $X \to X$.

8. $M = M_2(\mathbb{Z})$ $\quad M \times M \to M$

$(A, B) \mapsto A \cdot B$

multiplication de deux matrices carrées à coeff dans $\mathbb{Z}$.

- est <u>associative</u>, car pour 3 matrices A, B, C

on a $(A \cdot B) \cdot C = A \cdot (B \cdot C)$

- n'est <u>pas</u> commutative. De manière générale

si $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ $\quad B = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$

alors $A \cdot B = \begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix}$

et $B \cdot A = \begin{pmatrix} ae+cf & be+fd \\ ga+hc & gb+hd \end{pmatrix}$

<u>p.ex</u> : $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ $\quad B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$

alors $AB = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ et $BA = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$

- admet un élément <u>neutre</u>, égal à la matrice identité $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

En effet $I_2 \cdot A = A \cdot I_2 = A$ pour tout $A \in M_2(\mathbb{Z})$

- les éléments <u>inversibles</u> sont les matrices $A \in M_2(\mathbb{Z})$ vérifiant $\det(A) \in \{\pm 1\}$

Corrigé TD 1

Ex3

$\underline{n=6}$. $\mathbb{Z}/6\mathbb{Z}$.

1. Tableau d'<u>addition</u> dans $\mathbb{Z}/6\mathbb{Z}$.

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$

Tableau de multiplication dans $\mathbb{Z}/6\mathbb{Z}$

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

2. élément ($\neq \bar{0}$) — inverse dans $(\mathbb{Z}/6\mathbb{Z}, +)$

élément ($\neq \bar{0}$)	inverse dans $(\mathbb{Z}/6\mathbb{Z}, +)$
$\bar{1}$	$\bar{5}$
$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{3}$
$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{1}$

3. éléments inversibles dans $(\mathbb{Z}/6\mathbb{Z}, \cdot)$ — inverse.

éléments inversibles dans $(\mathbb{Z}/6\mathbb{Z}, \cdot)$	inverse.
$\bar{1}$	$\bar{1}$
$\bar{5}$	$\bar{5}$

Corrigé TD 1

Ex 5

1. $]-1,1[$ muni de la loi $x * y = \dfrac{x+y}{1+xy}$ est-il un groupe ?

Il faut d'abord vérifier que c'est une loi de composition, c'est-à-dire que $x * y \in]-1,1[$ quand $x \in]-1,1[$ et $y \in]-1,1[$.

Il faut montrer que :

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

Multiplions ces inégalités par $1+xy$.
Comme $1+xy > 0$, cela ne changera pas le sens des inégalités.

$$-1-xy \overset{①}{<} x+y \overset{②}{<} 1+xy$$

Il faut donc vérifier l'inégalité ① et ②

① $\iff x+y+1+xy > 0$

$\iff (x+1)(y+1) > 0$.

Or ceci est vrai, car $x+1 > 0$ et $y+1 > 0$

② $\iff 1+xy-x-y > 0$

$\iff (1-x)(1-y) > 0$

Or ceci est vrai, car $1-x > 0$ et $1-y > 0$.

Vérifions l'associativité : $x, y, z \in]-1, 1[$

$$(x * y) * z = \left(\frac{x+y}{1+xy}\right) * z$$

$$= \frac{\frac{x+y}{1+xy} + z}{1 + \left(\frac{x+y}{1+xy}\right) z}$$

on multiplie numérateur et dénominateur par $1+xy$.

$$= \frac{x + y + z + xyz}{1 + xy + xz + yz}$$

$$x * (y * z) = x * \left(\frac{y+z}{1+yz}\right)$$

$$= \frac{x + \frac{y+z}{1+yz}}{1 + \left(\frac{y+z}{1+yz}\right) x}$$

on multiplie numérateur et dénominateur par $1+yz$

$$= \frac{x + xyz + y + z}{1 + yz + xy + xz}$$

On voit donc que $(x * y) * z = x * (y + z)$ $\forall x, y, z \in]-1, 1[$.

Le neutre pour $*$ est 0, car.

$$0 * x = \frac{0 + x}{1 + 0} = x$$

$$x * 0 = \frac{x + 0}{1 + 0} = x$$

d'inverse de x est $-x$, car.

$$x * -x = \frac{x-x}{1+x(-x)} = \frac{0}{1-x^2} = 0 = \text{neutre}.$$

et $-x \in]-1,1[$ si $x \in]-1,1[$.

Donc $(]-1,1[, *)$ est un <u>groupe</u>.

2. $*$ est bien une loi de composition de $\mathbb{R}$

car $x*y = x+y-xy \in \mathbb{R}$

Vérifions l'associativité

$$(x*y)*z = (x+y-xy)*z$$
$$= x+y-xy+z-(x+y-xy)z$$
$$= x+y+z-xy-xz-yz+xyz$$

$$x*(y*z) = x*(y+z-yz)$$
$$= x+y+z-yz-x(y+z-yz)$$
$$= x+y+z-yz-xy-xz+xyz$$

donc $*$ est une loi associative.

le neutre pour $*$ est 0, car.

$$x*0 = 0*x = x$$

cherchons les éléments inversibles, Si x inversible d'inverse y, alors

$$x+y-xy = 0$$

$$\Leftrightarrow \quad x = (x-1)y \quad \Leftrightarrow \quad y = \frac{x}{x-1} \quad ; x \neq 1$$

Ainsi si $x \neq 1$, x est inversible d'inverse $x^{-1} = \frac{x}{x-1}$

si $x = 1$, x n'est pas inversible car.

$$1 * y = 1 + y - y = 1 \neq 0.$$

Donc $(\mathbb{R}, *)$ n'est <u>pas</u> un groupe.

Corrigé TD 1

Ex 6

1. E = ensemble fini ou infini

$$\mathcal{B}(E) = \{ f : E \to E \quad f \text{ bijective.} \}.$$

bijective = injective et surjective

il faut vérifier que la loi de composition

$$\circ : \mathcal{B}(E) \times \mathcal{B}(E) \longrightarrow \mathcal{B}(E)$$
$$(f, g) \longmapsto f \circ g$$

(1) est associative.
(2) admet un neutre
(3) tout élément admet un inverse.

(1) $(f, g) \mapsto f \circ g$ est associative, déjà vérifié dans Ex 1 (7)

(2) l'application identité $id_E : E \to E$, $x \mapsto x$.
est le neutre car $f \circ id_E = id_E \circ f = f$

(3) Si f est bijective, on peut définir l'application inverse de la manière suivante. Soit $y \in E$, alors il existe un unique $x \in E$ tel que $f(x) = y$.
on définit $f^{-1}(y) = x$.

par construction on a alors.

$$f \circ f^{-1} = f^{-1} \circ f = id_E.$$

Donc tout $f \in \mathcal{B}(E)$ est inversible.

2. On prend $E = \{1, 2, 3, \dots, n\}$ $\quad S_n = \mathcal{B}(E)$

Alors. $|S_n| = n! = 1 \cdot 2 \cdot 3 \cdot 4 \cdots (n-1) \cdot n$

<u>Explications</u>: La donnée d'une bijection $f : E \to E$ correspond à choisir n éléments <u>distincts</u> $f(1), f(2), \dots, f(n)$ dans E.

Ainsi pour le premier éléments il y a n choix pour le 2ème élément il y a $(n-1)$ choix (il faut enlever $f(1)$ de la liste $1, 2, \dots, n$), ensuite pour le 3ème élément il y a $(n-2)$ choix (il faut enlever $f(1), f(2)$ de la liste $1, 2, \dots, n$), etc.

Donc, finalement il y a $n(n-1)(n-2) \cdots 2 \cdot 1 = n!$ choix possibles.

3. <u>Notation</u>: $(a_1\, a_2\, a_3 \cdots a_k)$ est un cycle d'ordre k où $a_1, a_2, \dots, a_k \in \{1, 2, \dots, n\}$ où les a_i sont i nombres distincts, qui correspond à la bijection

$$f(a_1) = a_2, \quad f(a_2) = a_3, \quad f(a_3) = a_4, \quad \dots, \quad f(a_k) = a_1 \quad \text{et} \quad f(x) = x$$

si $x \notin \{a_1, a_2, a_3, \dots, a_k\}$.

<u>par exemple</u>. . $(12) \in \mathcal{B}(E)$ est le 2-cycle (ou transposition définie par

$$\begin{aligned} 1 &\mapsto 2 \\ 2 &\mapsto 1 \\ 3 &\mapsto 3 \\ 4 &\mapsto 4 \\ &\vdots \\ n &\mapsto n \end{aligned}$$

. $(324) \in \mathcal{B}(E)$ est le 3-cycle défini par

$$\begin{aligned} 1 &\mapsto 1 \\ 2 &\mapsto 4 \\ 3 &\mapsto 2 \\ 4 &\mapsto 3 \\ 5 &\mapsto 5 \\ &\vdots \\ n &\mapsto n \end{aligned}$$

Ainsi avec cette notation.

. $S_2 = \{ Id_E, (12) \}$

. $S_3 = \{ Id_E, (12), (13), (32), (123), (132) \}$

. $S_4 = \{ Id_E, (12), (13), (23), (14), (24), (34),$
$(123), (132), (134), (143), (124), (142),$
$(234), (243), (12)(34), (13)(24), (14)(23),$
$(1234), (1243), (1324), (1342), (1423), (1432) \}$

Exemple : Calcul dans S_4

(a) $(132) \circ (1342)$ est la bijection qui envoie.

$1 \mapsto 3 \mapsto 2$
$2 \mapsto 1 \mapsto 3$
$3 \mapsto 4 \mapsto 4$
$4 \mapsto 2 \mapsto 1$.

Donc $(132) \circ (1342) = (1234)$

(b) $(134) \circ (24)$ est la bijection qui envoie

$1 \mapsto 1 \mapsto 3$
$2 \mapsto 4 \mapsto 1$
$3 \mapsto 3 \mapsto 4$
$4 \mapsto 2 \mapsto 2$

Donc $(134) \circ (24) = (1342)$

4. S_2 est commutatif, car $(12) \circ Id_E = Id_E \circ (12)$
$(12) \circ (12) = (12)(12)$

mais S_3 n'est pas commutatif, car par exemple. $(12) \circ (23) = (123)$
et $(23) \circ (12) = (132)$ $\neq$

donc $(12) \circ (23) \neq (23) \circ (12)$

De même comme $S_3 \subset S_n$ pour $n \geq 3$
S_n n'est pas commutatif.

Corrigé TD 1

Ex 9 bis <u>Remarque</u> : La réunion de 2 sous-groupes n'est pas nécessairement un sous-groupe

Prendre $G = \mathbb{Z}/6\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$.

voir Ex 19

prendre $H = \{\bar{0}, \bar{3}\}$ sous-groupe d'ordre 2

$K = \{\bar{0}, \bar{2}, \bar{4}\}$ sous-groupe d'ordre 3

Alors $H \cup K = \{\bar{0}, \bar{2}, \bar{3}, \bar{4}\}$. Mais ce sous-ensemble n'est pas un sous-groupes, pour plusieurs raisons.

- $|H \cup K| = 4$ et $4 \nmid 6$ (Thm de Lagrange)
- $\bar{2}, \bar{3} \in H \cup K$, mais $\bar{2} + \bar{3} = \bar{5} \notin H \cup K$.

Corrigé TD 1

Ex 9

Hypothèse : H et K sous-groupes de G

Montrer que $H \cap K$ est un sous-groupe de G.

D'après le critère du cours, il faut vérifier les trois points suivants :

(a) $e_G \in H \cap K$

neutre de G

(b) Si $x \in H \cap K$ et $y \in H \cap K$, alors

$$x \cdot y \in H \cap K$$

(c) Si $x \in H \cap K$, alors $x^{-1} \in H \cap K$.

inverse de x dans G

Vérifications :

(a) Comme H est un sous-groupe de G, on a $e_G = e_H \in H$. Comme K est un sous-groupe de G, on a $e_G = e_K \in K$. Donc

$$e_G \in H \cap K.$$

(2

(b) Comme H est un sous-groupe, $x \cdot y \in H$

Comme K est un sous-groupe, $x \cdot y \in K$

donc $x \cdot y \in H \cap K$

(c) Comme H est un sous-groupe, $x^{-1} \in H$

Comme K est un sous-groupe, $x^{-1} \in K$

donc $x^{-1} \in H \cap K$.

Corrigé TD1

Ex 13 $\langle \bar{5} \rangle = \{\bar{0}, \bar{5}, \bar{10}, \bar{15}\} \subset \mathbb{Z}/20\mathbb{Z}$

l'ordre de $\langle \bar{5} \rangle = 4$.

Ex 14 Vérifions d'abord que $SL_2(\mathbb{Z})$ est un groupe. Le produit des matrices est associatif, il reste à montrer que si $A \in SL_2(\mathbb{Z})$ alors A admet un inverse dans $SL_2(\mathbb{Z})$.

si $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, alors $A^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \in SL_2(\mathbb{Z})$

$ad - bc = 1$

car $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} ad-bc & 0 \\ 0 & ad-bc \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

On calcule

$A^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ $\quad B^2 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$ et $B^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$AB = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ $\quad (AB)^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ $\quad (AB)^3 = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}$

montrons par récurrence que $(AB)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$

$$(AB)^{n+1} = (AB)^n \cdot (AB) = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1+n \\ 0 & 1 \end{pmatrix}$$

donc $(AB)^n \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ pour tout $n \neq 0$.

$\Rightarrow (AB)$ est d'ordre infini

Corrigé TD 1

Ex 16

1. $(\mathbb{Z}/5\mathbb{Z}, +)$ est cyclique.

$\mathrm{ord}(\bar{0}) = 1$, $\mathrm{ord}(\bar{1}) = 5 = \mathrm{ord}(\bar{2}) = \mathrm{ord}(\bar{3}) = \mathrm{ord}(\bar{4})$.

Il y a donc 4 générateurs : $\bar{1}, \bar{2}, \bar{3}$ et $\bar{4}$

2. $(\mathbb{Z}/6\mathbb{Z}, +)$ est cyclique.

$\mathrm{ord}(\bar{0}) = 1$, $\mathrm{ord}(\bar{1}) = 6$, $\mathrm{ord}(\bar{2}) = 3$, $\mathrm{ord}(\bar{4}) = 3$, $\mathrm{ord}(\bar{3}) = 2$

$\mathrm{ord}(\bar{5}) = 6$

Il y a donc 2 générateurs : $\bar{1}$ et $\bar{5}$.

3. $(\mathbb{Z} \oplus \mathbb{Z}, +)$ n'est pas cyclique.

Soit $(a,b) \in \mathbb{Z} \oplus \mathbb{Z}$ un élément. Le sous-groupe $\langle (a,b) \rangle \subset \mathbb{Z} \oplus \mathbb{Z}$ est contenu dans l'ensemble $\{(x,y) \mid bx - ay = 0\} \subsetneq \mathbb{Z} \oplus \mathbb{Z}$.

donc $\langle (a,b) \rangle \neq \mathbb{Z} \oplus \mathbb{Z}$.

Sauf si $(a,b) = (0,0)$ auquel cas $\langle (0,0) \rangle = \{(0,0)\}$

4. $(\mathbb{Q}, +)$ n'est pas cyclique.

par l'absurde.

Supposons que $\langle \frac{p}{q} \rangle = \mathbb{Q}$ avec $p, q \in \mathbb{Z}$, $q \neq 0$.

Cela signifierait que tout nombre rationnel pourrait s'écrire avec un dénominateur $= q$.

Or $\frac{1}{q+1}$ ne peut pas s'écrire ainsi.

Corrigé TD 1

Ex 19

1. $\mathbb{Z}/6\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$

$\mathrm{ord}(\bar{0}) = 1$ $\quad$ $\mathrm{ord}(\bar{2}) = 3$ $\quad$ $\mathrm{ord}(\bar{4}) = 3$

$\mathrm{ord}(\bar{1}) = 6$ $\quad$ $\mathrm{ord}(\bar{3}) = 2$ $\quad$ $\mathrm{ord}(\bar{5}) = 6$

<u>Remarque</u> : Soit $H \subset \mathbb{Z}/6\mathbb{Z}$ un sous-groupe de $\mathbb{Z}/6\mathbb{Z}$, si $h \in H$, alors $\langle h \rangle \subset H$.

Regardons les sous-groupes engendrés par les éléments de $\mathbb{Z}/6\mathbb{Z}$.

$\langle \bar{0} \rangle = \{\bar{0}\}$ $\quad$ $\langle \bar{2} \rangle = \{\bar{0}, \bar{2}, \bar{4}\}$ $\quad$ $\langle \bar{4} \rangle = \{\bar{0}, \bar{2}, \bar{4}\}$

$\langle \bar{1} \rangle = \mathbb{Z}/6\mathbb{Z}$ $\quad$ $\langle \bar{3} \rangle = \{\bar{0}, \bar{3}\}$ $\quad$ $\langle \bar{5} \rangle = \mathbb{Z}/6\mathbb{Z}$.

Ainsi on obtient les sous-groupes suivants.

$\{\bar{0}\}$, $\{\bar{0}, \bar{2}, \bar{4}\}$, $\{\bar{0}, \bar{3}\}$ et $\mathbb{Z}/6\mathbb{Z}$

Inversément si on se donne un sous-groupe $H \subset \mathbb{Z}/6\mathbb{Z}$ d'ordre 2, ce sous-groupe H doit contenir un élément d'ordre 2. Or il existe un seul élément d'ordre 2 dans $\mathbb{Z}/6\mathbb{Z}$, donc $H = \langle \bar{3} \rangle$.

De même un sous-groupe $H \subset \mathbb{Z}/6\mathbb{Z}$ d'ordre 3 (2

doit contenir un élément d'ordre 3, Donc

nécessairement $H = \langle \bar{2} \rangle$ ou $H = \langle \bar{4} \rangle$.

2. $\mathbb{Z}/12\mathbb{Z}$

$ord(\bar{0}) = 1$	$ord(\bar{4}) = 3$	$ord(\bar{8}) = 3$
$ord(\bar{1}) = 12$	$ord(\bar{5}) = 12$	$ord(\bar{9}) = 4$
$ord(\bar{2}) = 6$	$ord(\bar{6}) = 2$	$ord(\overline{10}) = 6$
$ord(\bar{3}) = 4$	$ord(\bar{7}) = 12$	$ord(\overline{11}) = 12$

<u>sous-groupes de $\mathbb{Z}/12\mathbb{Z}$</u> :

$\langle \bar{0} \rangle = \{\bar{0}\}$, $\langle \bar{6} \rangle = \{\bar{0}, \bar{6}\}$, $\langle \bar{4} \rangle = \langle \bar{8} \rangle = \{\bar{0}, \bar{4}, \bar{8}\}$.

$\langle \bar{3} \rangle = \langle \bar{9} \rangle = \{\bar{0}, \bar{6}, \bar{9}, \bar{3}\}$, $\langle \bar{2} \rangle = \langle \overline{10} \rangle = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \overline{10}\}$.

et $\mathbb{Z}/12\mathbb{Z}$

3. générateurs de $\mathbb{Z}/9\mathbb{Z}$: $\bar{1}, \bar{2}, \bar{4}, \bar{5}, \bar{7}, \bar{8}$

Corrigé TD 1

Ex 20 Rappel de Ex 6

$$S_3 = \{ Id, (12), (13), (23), (123), (132) \}.$$

neutre = identité

2-cycles transposition

3-cycles

$|S_3| = 6$.

D'après le thm de Lagrange si $H \subset S_3$ sous-groupe, alors $|H|$ divise $|S_3| = 6$. Donc $|H| = 1, 2, 3$ ou 6

Si $|H| = 1$, alors $H = \{Id\}$.

. Si $|H| = 6$, alors $H = S_3$

. Si $|H| = 2$, alors $H = \{Id, x\}$ avec $x \in S_3$ un élément d'ordre 2, donc $x = (12), (13)$ ou (23)

. Si $|H| = 3$, alors $H = \{Id, x, y\}$

Si $ord(x) = 2$ et $ord(y) = 2$, alors ou bien $x = y$ et on trouve un sous-groupe d'ordre 2 ou bien $x \neq y$ et on trouve que $x \cdot y$ = 3-cycle. donc $\neq x$, et y.

p.ex. $(12) \cdot (13) = (132)$

$(12) \cdot (23) = (123)$

$(23)\ (13) = (123)$

Dans ce cas $\langle (12), (13) \rangle = S_3$

Donc le seul cas où l'on obtient un sous-groupe H d'ordre 3 est quand $\mathrm{ord}(x) = 3$ et $H = \{Id, x, x^2\} = \{Id, \underset{x}{(123)}, \underset{x^2}{(132)}\}$.

Ex 21 Un groupe d'ordre p est cyclique.

Soit $g \in G$ et $g \neq e$ (= neutre).
Considérons le sous-groupe $\langle g \rangle$ engendré par g.
C'est un sous-groupe de G d'ordre ≥ 2,

car $g \neq e$.
Par le théorème de Lagrange.

$$|\langle g \rangle| \text{ divise } p$$

Comme p est premier, on déduit que

$$|\langle g \rangle| = p, \text{ donc}$$

$$\langle g \rangle = G.$$

Donc G est cyclique.

Corrigé TD 1

Ex 23

$$\mathrm{sgn} : \mathbb{R}^* \longrightarrow \{\pm 1\}$$

$$\mathrm{sgn}(x) = \frac{|x|}{x} = \begin{cases} 1 & \text{si } x > 0 \\ -1 & \text{si } x < 0 \end{cases}$$

Il faut vérifier que $\mathrm{sgn}(xy) = \mathrm{sgn}(x) \cdot \mathrm{sgn}(y)$ pour tout $x, y \in \mathbb{R}^*$

Ceci est équivalent à la relation.

$$\frac{|xy|}{xy} = \frac{|x|}{x} \cdot \frac{|y|}{y}$$

qui est vrai puisque $|xy| = |x| \cdot |y|$.

Ex 27

Un groupe cyclique G d'ordre k est isomorphe à $(\mathbb{Z}/k\mathbb{Z}, +)$.

Comme G est cyclique d'ordre k, il existe un élément $g \in G$ d'ordre k et on peut écrire.

$$G = \{e, g, g^2, g^3, \dots, g^{k-1}\} \quad \text{avec } g^k = e.$$

Il est clair que l'application.

$$\mathbb{Z}/k\mathbb{Z} \longrightarrow G$$

$$\bar{a} \longmapsto g^a$$

est bien définie et est un homomorphisme de groupes.

- bien défini, car

si $\overline{a+nk} = \overline{a}$, alors $g^a = g^{a+nk}$.

En effet $g^{a+nk} = g^a \cdot g^{nk} = g^a \cdot (g^k)^n = g^a \cdot e^n = g$

car $g^k = e$.

- homomorphisme, car $(g^a) \cdot (g^b) = g^{a+b}$.

pour tout $a, b \in \mathbb{N}$

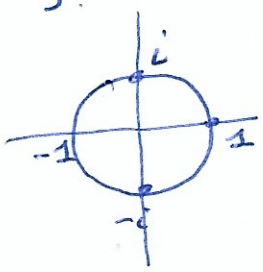
Ex 28 **1.** $(\mathbb{Z}/4\mathbb{Z}, +)$ et $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +)$

ne sont pas isomorphes, car $\mathbb{Z}/4\mathbb{Z}$ est cyclique

et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ n'est <u>pas</u> cyclique.

2. $\{1, -1, i, -i\}$ est isomorphe à $\mathbb{Z}/4\mathbb{Z}$

$$\Phi : \mathbb{Z}/4\mathbb{Z} \longrightarrow \{1, i, -1, -i\}.$$
$$\overline{k} \longmapsto i^k$$



bien défini, car $i^4 = 1$

3. $(S_3, \circ)$ et $(\mathbb{Z}/6\mathbb{Z}, +)$ ne sont pas

isomorphes, car $(S_3, \circ)$ n'est pas commutatif

et $\mathbb{Z}/6\mathbb{Z}$ est commutatif.

Autre raison :

$\mathbb{Z}/6\mathbb{Z}$ admet un élément d'ordre 6 et S_3 n'a que des éléments d'ordre 2 et 3.

Ex29

Ordre 1 : $\{e\}$

Ordre 2 : $\mathbb{Z}/2\mathbb{Z}$

Ordre 3 : $\mathbb{Z}/3\mathbb{Z}$

Ordre 5 : $\mathbb{Z}/5\mathbb{Z}$

résulte de Ex 21

<u>Ordre 4</u> : <u>1er cas</u> : G admet un élément d'ordre 4. Dans ce cas G est cyclique, donc $G = \mathbb{Z}/4\mathbb{Z}$

<u>2ème cas</u> : G n'admet pas d'élément d'ordre 4

Donc G n'admet que des éléments d'ordre 2. Donc $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

En effet soit x, y deux éléments distincts $(\neq e)$ dans G, alors $x^2 = e$, $y^2 = e$ et $x \neq y$.

Alors $xy \neq x$ (car sinon on aurait $y = e$)

$xy \neq y$

Donc $G = \{e, x, y, xy\}$.

de même $yx \neq x$ et $yx \neq y$, donc $xy = yx$

Donc G est commutatif, et on a un isomorphisme

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \longrightarrow G$$
$$(\bar{1}, \bar{0}) \longmapsto x.$$
$$(\bar{0}, \bar{1}) \longmapsto y.$$

Ex 31 Soit $f(x) = x^{-1}$

Si f homomorphisme de groupe, alors.

$$f(xy) = f(x) \cdot f(y) \quad \forall x, y \in G$$

$$(xy)^{-1} = x^{-1} \cdot y^{-1}$$

Si on multiplie cette relation avec xy :

$$e = x^{-1} y^{-1} xy$$

Si on multiplie ensuite avec yx :

$$yx = xy \iff (xy)^{-1} = x^{-1} y^{-1}$$

Cette relation est équivalent à G commutatif

Ex 32 Soit $f : \mathbb{Z} \to \mathbb{Z}$ un homomorphisme.

Alors f est entièrement déterminé par. $f(1)$

En effet, notons $a = f(1) \in \mathbb{Z}$, alors.

$$f(n) = f(\underbrace{1 + \cdots + 1}_{n \text{ fois}}) = \underbrace{f(1) + f(1) + \cdots + f(1)}_{n \text{ fois}}$$

$$= n \cdot f(1) = n \cdot a.$$

Donc les homomorphismes $f: \mathbb{Z} \to \mathbb{Z}$ sont de la forme $f(n) = n \cdot a$.

- Si $a \neq 0$, alors f est injectif
- Si $a = 1$, alors f est surjectif

Si $a \neq 1$, alors f n'est pas surjectif

Ex 34

$$\Phi : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/d\mathbb{Z}$$

$$x \bmod n \longmapsto x \bmod d$$

- bien défini, car si $x \equiv y \bmod n$, alors

$$y = x + kn$$

- et comme $n = d \cdot l$, on a

$$y = x + kdl$$

Si on réduit modulo d, on obtient

$$y \equiv x \bmod d.$$

- surjectif, car une classe $\bar{x}$ modulo d se relève en un entier x, qui modulo n donne un antécédent de $\bar{x}$.

$$\ker \Phi = \{ \bar{x} \bmod n \text{ tel que } d \mid x \}$$

$$= d\mathbb{Z}/n\mathbb{Z} \subset \mathbb{Z}/n\mathbb{Z}$$

Si on écrit $n = dl$, on a un isomorphisme.

$$\mathbb{Z}/l\mathbb{Z} \xrightarrow{\sim} d\mathbb{Z}/n\mathbb{Z}$$

$$a \longmapsto ad \bmod n$$