Maths 4 : TD 4 Théorie des groupes

23.03.2021

Exercice 2

commutativité : a-t-on $a * b = b * a$ pour tout $a, b \in G$?

ici $x * y = t \neq y * x = z$ Donc la loi n'est pas commutative.

loi de groupe : vérifier que
1) associativité : $(a * b) * c = a * (b * c)$ $\forall a, b, c \in G$
2) él. neutre e : $e * a = a * e = a$ $\forall a \in G$
3) inverse : $\forall a \in G$ $\exists a' \in G$ tq $a * a' = a' * a = e$

Vérifions 2) : ici e est l'élément neutre. On le voit en examinant la table
$e * a = a = a * e$ $\forall a \in G$

Vérifions 3) : en lisant la table, on voit que $\forall a \in G$, $a * a = e$ qui est l'élément neutre.
Chaque élément est son propre inverse.

Vérifions 1) : par exemple on a $(x * y) * z = t * z = x$ et $x * (y * z) = x * t = z$
Donc la loi n'est PAS associative.

Donc $(G, *)$ n'est pas un groupe.

Exercice 3

Notons $G = \{e, x\}$

On doit avoir $\begin{cases} e * e = e \\ e * x = x \\ x * e = x \end{cases}$ pour que e soit l'élément neutre

On a ou bien $x * x = e$ ou bien $x * x = x$

Supposons que $x * x = x$
Alors on a aussi $\underbrace{(\underbrace{x^{-1} * x}_{e}) * x}_{x} \neq \underbrace{x^{-1} * x}_{e} = x^{-1} * \underbrace{(x * x)}_{x}$

contradictO car $x \neq e$

Donc c'est $x * x = e$

	e	x
e	e	x
x	x	e

On vérifie qu'on a bien les 3 axiomes :
2) OK : e est le neutre
3) OK : e inverse de e et x inverse de x
1) OK

deux façons pour vérifier :
a) faire le calcul : on vérifie tous les triplets
ou b) On constate que la table s'identifie avec la table suivante :

+	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

qui est la table de multiplication du groupe $(\mathbb{Z}/2\mathbb{Z}, +)$ qui est associative.

Donc c'est bien la table de multiplication du groupe.

Exercice 4

Soit $G = \{e, x, y\}$

On note e l'élément neutre

$*$	e	x	y
e	e	x	y
x	x		
y	y		

Examinons les possibilités pour $x * x$

- si $x * x = x$ alors $x = e$
  (voir ex précédent)

- supposons $x * x = e$. Alors $x = x^{-1}$

Mq sur chaque ligne de la table de multiplication d'un groupe, chaque élément apparait une fois et une seule.

↳ considérons la ligne associée à un élément $g \in G$
Cette ligne contient $g * h$ à la colonne associée à $h \in G$.

Or l'application $\lambda_g : G \to G$, $h \mapsto g * h$ est bijective de réciproque $G \to G$, $k \mapsto g^{-1} * k$

(on a $\lambda_g^{-1} \circ \lambda_g (h) = g^{-1} * (g * h) = (g^{-1} * g) * h = e * h = h$ de même avec $\lambda_g \circ \lambda_g^{-1}(h) = h$)

Donc si $x * x = e$, alors $x * y = y$
Mais alors $y = e$ CONTRADICTION
(multiplier à droite par y^{-1})

$*$	e	x	y
e	e	x	y
x	x	e	y
y	y		

- donc $x * x = y$

et alors $x * y = e$ car e doit apparaître sur la ligne

Dans chaque colonne aussi, chaque él doit apparaître une seule fois.

$*$	e	x	y
e	e	x	y
x	x	y	e
y	y	e	x

On a donc montré qu'un ensemble à 3 éléments admet au plus 1 structure de groupe après avoir choisi un élément neutre.

Il reste à vérifier qu'il existe au moins une structure de groupe, c'est-à-dire que cette table définit bien un groupe.
Deux possibilités :
a) vérificatO en faisant le calcul pour les $3^3 = 27$ triplets.
ou b) On observe que la table s'identifie avec celle du groupe $(\mathbb{Z}/3\mathbb{Z}, +)$

Conclusion : Pour un ensemble à 3 élément → 3 lois de groupe correspondant aux 3 choix possibles pour l'élément neutre.

Exercice 5

Abrégeons $x*y$ en xy la notation pour les produits dans G.

L'hypothèse est que $x^2 = e \ \forall x \in G$

Autrement dit $x = x^{-1} \ \forall x \in G$

Soient $x, y \in G$

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

Exercice 6

On a $yx = xy^2$ et $xy = yx^2$

Donc $yx = xyy = yx^2y = yxxy$

On multiplie à gauche par $x^{-1}y^{-1}$

$\Rightarrow \ e = xy \quad \Rightarrow \ x^{-1} = y$

Or $\underbrace{yx}_{=e} = xy^2 = \underbrace{xy}_{=e}y \quad \Rightarrow \ y = e \quad \Rightarrow \ x = y^{-1} = e$

On a bien $x = y = e = 1$.

25.03.2021

Exercice 4 (fin)

G groupe à 4 éléments, $(G, \cdot)$
$G = \{e, x, y, z\}$

$\text{ord}(x) = \min\{n \in \mathbb{N}^* \text{ tq } x^n = e\}$

Rappel: si $H \subset G$ et H et G sont finis, $|H|$ divise $|G|$ (Lagrange)

soit $H = \langle x \rangle = \{e, x, \dots, x^{n-1}\}$ où $n = \text{ord}(x)$
donc $|H| = n$

Donc $\text{ord}(x) \in \{\cancel{1}, 2, 4\}$ $\quad x \neq e$
$\text{ord}(y) \in \{\cancel{1}, 2, 4\}$ $\quad y \neq e$
$\text{ord}(z) \in \{\cancel{1}, 2, 4\}$ $\quad z \neq e$

① $\exists$ un élément d'ordre 4 dans $G = \{e, x, y, z\}$
Par symétrie, on peut supposer que c'est x.

Alors $\langle x \rangle \subset G \Rightarrow \langle x \rangle = G$ (tous les 2 d'ordre 4)

$G \cong \mathbb{Z}/4\mathbb{Z}$ $G \to (\mathbb{Z}/4\mathbb{Z}, +)$
↑ isomorphe à $x \mapsto \bar{1}$

② $\nexists$ d'él d'ordre 4

Alors $\text{ord}(x) = \text{ord}(y) = \text{ord}(z) = 2$

donc $x^2 = e$, $y^2 = e$ et $z^2 = e$

	e	x	y	z
e	e	x	y	z
x	x	e	z	y
y	y	z	e	x
z	z	y	x	e

il faut que chaque lettre apparaissent 1 fois sur la ligne et 1 fois sur la colonne

$G \cong (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +)$ ↖ groupe de Klein

$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{\underbrace{(\bar{0},\bar{0})}_{=e}, \underbrace{(\bar{0},\bar{1})}_{=x}, \underbrace{(\bar{1},\bar{0})}_{=y}, \underbrace{(\bar{1},\bar{1})}_{=z}\}$

Donc en tout y'a $\boxed{\text{2 groupes}}$.

Exercice 7

$m \in \mathbb{N}^*$

$$\mathcal{U}_m = \{z \in \mathbb{C} \text{ tq } z^m = 1\}$$
$$= \left\{\exp\left(\frac{2ik\pi}{m}\right),\ k = 0, \dots, m-1\right\}$$

1) Mq $\mathcal{U}_m$ sous-groupe de $(\mathbb{C}^*, \times)$

Vérifier: ① $1 \in \mathcal{U}_m$ donc $\mathcal{U}_m \neq \emptyset$

② $x, y \in \mathcal{U}_m$ $xy \in \mathcal{U}_m$ stabilité par le produit

③ $x \in \mathcal{U}_m$ $x^{-1} \in \mathcal{U}_m$ stabilité par l'inverse

① $1^m = 1$ donc $1 \in \mathcal{U}_m$

② $x, y \in \mathcal{U}_m$ $(xy)^m = x^m y^m = 1 \times 1 = 1$
↑ car $x, y \in \mathcal{U}_m$

donc $xy \in \mathcal{U}_m$

③ $x \in \mathcal{U}_m$ $(x^{-1})^m = (x^m)^{-1} = 1$

donc $x^{-1} \in \mathcal{U}_m$

2) Mq $\mathbb{U}_n$ cyclique d'ordre n.

$$\mathbb{U}_n = \{\exp(2i\pi k/n),\ k = 0,1,\dots,n-1\}$$
$$= \{\exp(\underbrace{2i\pi/n}_{\omega})^k,\ \dots\}$$
$$= \{1, \omega, \omega^2, \dots, \omega^{n-1}\}$$

Donc $\mathbb{U}_n = \langle \omega \rangle \subset \mathbb{C}^*$ et $\mathrm{ord}(\omega) = n$.

3) Mq $\mathbb{U}_m \subseteq \mathbb{U}_n$ ssi $m | n$

$\boxed{\Leftarrow}$ On suppose $m | n \iff \exists k$ tq $mk = n$

Soit $z \in \mathbb{U}_m$

$$z^n = z^{mk} = (z^m)^k = 1^k = 1$$

donc $z \in \mathbb{U}_n$

On a bien $\mathbb{U}_m \in \mathbb{U}_n$

$\boxed{\Rightarrow}$ On suppose $\mathbb{U}_m \subseteq \mathbb{U}_n$ donc $m \leq n$

$n = qm + r$ (div euclidienne de m par n)
$0 \leq r \leq m-1$

$z \in \mathbb{U}_m \subseteq \mathbb{U}_n$ avec $\mathrm{ord}(z) = m$ (z engendre le groupe)

donc $1 = z^n = z^{mq+r} = (z^m)^q z^r = 1^q \times z^r = z^r$

$\Rightarrow z^r = 1$

donc $\mathrm{ord}(z)$ divise r (si $r > 0$)

$r < m = \min\{k \in \mathbb{N}^* \text{ tq } z^k = 1\}$
pb $z^r = 1$

$\Rightarrow r = 0$

$\Rightarrow m | n$

Exercice 8

$(\mathbb{Z}/12\mathbb{Z}, +)$

$\mathrm{ord}(\bar{0}) = 1$ → c'est le neutre. L'ordre d'un élément ne peut pas être 0.
$\mathrm{ord}(\bar{1}) = 12$
$\mathrm{ord}(\bar{2}) = 6$ $\quad\langle \bar{2} \rangle = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \overline{10}\}$
$\mathrm{ord}(\bar{3}) = 4$
$\mathrm{ord}(\bar{4}) = 3$
$\mathrm{ord}(\bar{5}) = 12$
$\mathrm{ord}(\bar{6}) = 2$
$\mathrm{ord}(\bar{7}) = 12$
$\mathrm{ord}(\bar{8}) = 3$
$\mathrm{ord}(\bar{9}) = 4$
$\mathrm{ord}(\overline{10}) = 6$
$\mathrm{ord}(\overline{11}) = 12$

Valeurs possibles : 1 et tout ce qui divise 12
$\mathrm{ord}(\bar{k}) \in \{1, 2, 3, 4, 6, 12\}$

on cherche le 1er produit divisible par 12
$\mathrm{ord}(\bar{k}) = \min\{n \in \mathbb{N}^* \ n\bar{k} = \bar{0}\}$

Formule générale pour $\mathbb{Z}/n\mathbb{Z}$:

$$\mathrm{ord}(\bar{k}) = n / \mathrm{PGCD}(k, n)$$

$(\mathbb{Z}/12\mathbb{Z})^* = \{ \bar{k} \in \mathbb{Z}/12\mathbb{Z} \mid \exists \bar{l} \in \mathbb{Z}/12\mathbb{Z} \ \bar{k}\bar{l} = \bar{1} \}$ → les inversibles pour la multiplication.

$= \{ \bar{k} \in \mathbb{Z}/12\mathbb{Z} \text{ tq } PGCD(k, 12) = 1 \}$

$= \{ \bar{1}, \bar{5}, \bar{7}, \bar{11} \}$

↳ groupe d'ordre 4

$\text{ord}(\bar{1}) = 1$ car $1^1 \equiv 1 \mod 12$

$\text{ord}(\bar{5}) = 2$ car $5^2 = 25 \equiv 1 \mod 12$

$\text{ord}(\bar{7}) = 2$ car $7^2 = 42 \equiv 1 \mod 12$

$\text{ord}(\bar{11}) = 2$

ici $\text{ord}(\bar{k}) = \min \{ n \in \mathbb{N}^* \text{ tq } \bar{k}^n = 1 \}$

↳ pour la multiplication

$\text{ord}(\bar{k}) \in \{2, 4\}$
$\bar{k} \neq \bar{1}$

$((\mathbb{Z}/12\mathbb{Z})^*, \cdot) \simeq (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +)$

↳ pas un groupe cyclique
car pas d'él. d'ordre 4