I. L.c.i / groupes

Ex. 4 On étudie $a * b = \sup(a, b)$ sur $\mathbb{R}$.

→ <u>associative</u> Soient $a, b, c \in \mathbb{R}$.

Il est évident que $\sup(a, \sup(b, c)) = \sup(\sup(a, b), c)$

→ <u>commutative</u> La commutativité est évidente.

→ <u>neutre</u>

<u>BROUILLON</u> Si e neutre :

$\forall a : \ \sup(a, e) = a$

↳ donc $e \leqslant a \quad \forall a \in \mathbb{R}$

ce qui n'est pas possible

<u>REDACTION</u>

Il n'existe pas de neutre car si e l'était, on aurait :

$\forall a \in \mathbb{R} \quad \sup(a, e) = a$

$\Longrightarrow e \leqslant a$

→ impossible

Si on se place sur $\mathbb{R}^+$, $e = 0$ est neutre, car

$\forall a \geqslant 0 \quad \sup(a, e) = a$.

→ on peut dans ce cas poser la question du symétrique :

Si a admet un symétrique :

$\uparrow$
$\mathbb{R}^+$

$\sup(a, \tilde{a}) = 0 \ \ldots \Longrightarrow a = 0$

Ex. 5 sur

On étudie :

$(x, y) * (x', y') = (xx', xy' + y)$ sur $\mathbb{R}^{+*} \times \mathbb{R}$

⇝ <u>associativité</u>

Soient $(x, y), (x', y'), (x'', y'') \in \mathbb{R}^{+*} \times \mathbb{R}$

$(x, y) * ((x', y') * (x'', y'')) = (x, y) * (x'x'', x'y'' + y')$

$= (xx'x'', x(x'y'' + y') + y)$

$((x, y) * (x', y')) * (x'', y'') = (xx', xy' + y) * (x'', y'')$

$= (xx'x'', xx'y'' + xy' + y)$

=

Donc $*$ est associative

→ commutativité : On voit clairement que l'opération n'est pas commutative.

→ élément neutre

BROUILLON on cherche $e = (e_1, e_2)$ un neutre.
On doit avoir $\forall (x,y)$

$$\underbrace{(x,y) * (e_1, e_2)}_{(xe_1,\, xe_2 + y)} = (x, y) \iff \begin{cases} x e_1 = x & \leadsto e_1 = 1 \\ x e_2 + y = y & \leadsto e_2 = 0 \end{cases}$$

Donc le neutre semble être $e = (1, 0)$.

REDACTION

Soit $e = (1,0)$, montrons que c'est un élément neutre :
soit $(x,y) \in \mathbb{R}_+^* \times \mathbb{R}$

$(x,y) * (1,0) = (x.1, x.0 + y) = (x,y)$ ✓

$(1,0) * (x,y) = (1.x, 1.y + 0) = (x,y)$ ✓

Donc e est bien le neutre pour $*$.

⚠ comme $*$ n'est pas commutative, il faut vérifier les deux sens !

⇝ éléments symétrisables

BROUILLON Soit $(x,y) \in \mathbb{R}_+^* \times \mathbb{R}$. Si (x,y) est symétrisable, $\exists (\tilde{x}, \tilde{y})$ tq

$$\underbrace{(x,y) * (\tilde{x}, \tilde{y})}_{(x\tilde{x},\, x\tilde{y} + y)} = (1,0) \quad \big(= (\tilde{x}, \tilde{y}) * (x,y) \ldots \big)$$

On doit donc avoir

$$\begin{cases} x\tilde{x} = 1 & \leadsto \tilde{x} = \frac{1}{x} \quad (x \neq 0) \\ x\tilde{y} + y = 0 & \leadsto \tilde{y} = -\frac{y}{x} \quad (\underbrace{x \neq 0}_{\text{ok}}) \end{cases}$$

REDACTION montrons que tout élément de $\mathbb{R}_+^* \times \mathbb{R}$ est symétrisable.

Soit $(x,y) \in \mathbb{R}_+^* \times \mathbb{R}$, on pose $(\widetilde{x,y}) = \left(\frac{1}{x}, -\frac{y}{x}\right)$

$$(x,y) * (\widetilde{x,y}) = (x,y) * \left(\frac{1}{x}, -\frac{y}{x}\right) = \left(x.\frac{1}{x}, x\left(-\frac{y}{x}\right) + y\right) = (1,0) \checkmark$$

$$(\tilde{x},y) * (x,y) = \left(\frac{1}{x}, -\frac{y}{x}\right) * (x,y) = \left(\frac{1}{x}\cdot x, \frac{1}{x}\cdot y - \frac{y}{x}\right)$$
$$= (1,0) \quad \checkmark$$

idem, bien vérifier les 2 sens !

Donc $(\mathbb{R}_+^* \times \mathbb{R}, *)$ est un groupe non commutatif.

Ex. 6

On considère $x * y = xy + (x^2-1)(y^2-1)$

⇝ On voit clairement que l'opération est commutative.

⇝ Associativité

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

$$(x*y)*z = \left(xy + (x^2-1)(y^2-1)\right) * z$$
$$= \left(xy + (x^2-1)(y^2-1)\right) z + \left(\left(xy + (x^2-1)(y^2-1)\right)^2 - 1\right) \times (z^2-1)$$

terme du plus haut degré : $x^4y^4z^2$

$$x*(y*z) = x(y*z) + (x^2-1)\left((y*z)^2 - 1\right)$$
$$= x\left(yz + (y^2-1)(z^2-1)\right) + (x^2-1)\left(\left(yz + (y^2-1)(z^2-1)\right)^2 - 1\right)$$

terme du plus haut degré $x^2y^4z^4$

Donc ces deux termes ne peuvent être égaux ...

⇝ Neutre

BROUILLON on cherche un neutre : e tq

$x*e = x$, i.e : $\quad x.e + (x^2-1)(e^2-1) = x$

$$\iff x(e-1) + (x^2-1)(e^2-1) = 0 \qquad (e^2-1) = (e-1)(e+1)$$

$$\iff (e-1)\left(x + (x^2-1)(e+1)\right) = 0$$

On voit que $e = 1$ est toujours solution

Vérifions que $e=1$ est neutre, comme $*$ commutative, il suffit de vérifier que $x * 1 = x$

$$\underset{\shortparallel}{x*1} = x$$

$$x.1 + (x^2-1)(1-1) = x \quad ✓$$

Que $*$ soit assoc. ou non, le neutre est toujours unique ...

⇝ Symétriques

Soit $x \in \mathbb{R}$, si x est symétrisable, $\exists\, \tilde{x}$ tq

$$x * \tilde{x} = 1$$

$$\iff x\tilde{x} + (x^2-1)(\tilde{x}^2-1) = 1$$

$$\iff \tilde{x}^2(x^2-1) + \tilde{x}.x - \cancel{1} - (x^2-\cancel{1}) = 0$$

$$\iff \tilde{x}^2 \underbrace{(x^2-1)}_{a} + \tilde{x}.\underbrace{x}_{b} \underbrace{-x^2}_{c} = 0$$

Polynôme de degré 2 en $\tilde{x}$

$$⇝ \Delta = b^2 - 4ac = x^2 + 4.(x^2-1)(x^2)$$

$$= x^2 \underbrace{(1+4(x^2-1))}_{\text{signe ?}}$$

On pose

$$P(x) = 1+4(x^2-1)$$

$$P(x) = 0 \iff 1+4x^2-4 = 0$$

$$\iff x = \pm\sqrt{\frac{3}{4}} = \pm\frac{\sqrt{3}}{2}$$

x		$-\frac{\sqrt{3}}{2}$		$\frac{\sqrt{3}}{2}$	
$P(x)$	+	0	−	0	+

- Donc $x = \pm\frac{\sqrt{3}}{2}$ a un unique symétrique car $\Delta = 0$

$$\implies \tilde{x} = \frac{-b}{2a} = -\frac{x}{2(x^2-1)}$$

- Tous les $x \in \left]-\infty, -\frac{\sqrt{3}}{2}\right[\cup \left]\frac{\sqrt{3}}{2}, +\infty\right[$ admettent 2 symétriques ($*$ pas associative ...)

$$\hookrightarrow \frac{-b \pm\sqrt{\Delta}}{2a}$$

- Tous les $x \in \left]-\frac{\sqrt{3}}{2}, \frac{\sqrt{3}}{2}\right[$ ne sont pas symétrisables

Ex. 7 Sur $\mathbb{R}^+$, on considère $x * y = \sqrt{x^2+y^2}$

⇝ On voit bien que $*$ est commutative.

⇝ associativité Soient $x, y, z \in \mathbb{R}^+$:

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

$$\| $$

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

⇝ neutre

On recherche e tq $\sqrt{x^2+e^2} = x \overset{\wedge 2}{\iff} \cancel{x^2} + e^2 = \cancel{x^2}$

⇝ $e = 0$

Soit $e = 0$, on vérifie aisement que e est neutre.

⇝ symétriques

Soit $x \in \mathbb{R}_+$, x admet un symétrique $\tilde{x}$ ssi

$x * \tilde{x} = 0$

$$\sqrt{x^2+\tilde{x}^2} = 0 \iff x^2+\tilde{x}^2 = 0 \quad \text{possible ssi } x = 0 = \tilde{x}.$$

Donc seul 0 est symétrisable.

Ex. 8 On considère sur $\mathbb{R}^2$:

$$(x,y)*(x',y') = (xy, xy'+yx')$$

⇝ commutativité Il est clair que $*$ est commutative

⇝ associativité Soient $(x,y), (x',y'), (x'',y'') \in \mathbb{R}^2$

$$(x,y)*((x',y')*(x'',y'')) = (x,y)*(x'x'', x'y''+x''y')$$

$$= (xx'x'', x(x'y''+x''y') + yx'x'')$$

$$= (xx'x'', \underbrace{xx'.y''+x''(xy'+yx')})$$

$$(xx', xy'+yx')*(x'',y'')$$

$$= (xx', xy'+yx')*(x'',y'') = ((x,y)*(x',y'))*(x'',y'') \quad \checkmark$$

⇝ <u>neutre</u>

On cherche $e=(e_1,e_2)$ tq $(x,y)*(e_1,e_2) = (x,y)$ pour $(x,y)\in\mathbb{R}^2$ quelconque

$$\underset{\displaystyle (xe_1, xe_2+ye_1)}{(x,y)*(e_1,e_2)} \iff \begin{cases} xe_1 = x & \rightsquigarrow \quad e_1 = 1 \text{ convient} \\ xe_2+ye_1 = y \end{cases}$$

$$\Downarrow$$

$$x.e_2 + \cancel{y} = \cancel{y} \quad \rightsquigarrow e_2 = 0.$$

Posons $e = (1,0)$

On a bien, pour $(x,y)\in\mathbb{R}^2$:

$$(x,y)*(1,0) = (x.1 \ , x.0+y.1) = (x,y)$$

Comme $*$ associative, on en déduit que e est bien le neutre.

⇝ <u>symétriques</u>

Soit $(x,y)\in\mathbb{R}^2$, si $(\tilde{x},\tilde{y})$ est son symétrique :

$$(x,y)*(\tilde{x},\tilde{y}) = (x\tilde{x}, x\tilde{y}+y\tilde{x}) = (1,0)$$

$$\iff \begin{cases} x\tilde{x} = 1 & \longrightarrow \text{ si } x\neq 0 : \tilde{x} = \dfrac{1}{x} \\ x\tilde{y}+y\tilde{x} = 0 \end{cases}$$

$$\Longrightarrow x\tilde{y} + \frac{y}{x} = 0 \implies \tilde{y} = -\frac{y}{x^2}$$

- Soit $(x,y)\in\mathbb{R}^2$ tq $x\neq 0$.

  On pose $(\tilde{x},\tilde{y}) = \left(\dfrac{1}{x}, -\dfrac{y}{x^2}\right)$

On a bien :

$$(x,y)*\left(\frac{1}{x}, -\frac{y}{x^2}\right) = \left(1, -\cancel{x}\frac{y}{x^{\cancel{2}}} + \cancel{y\frac{1}{x}}\right) = (1,0)$$

Comme $*$ commutative, on en déduit que $(\tilde{x},\tilde{y})$ est bien le symétrique de (x,y).

- Pour tout $(0,y)$ avec $y\in\mathbb{R}$:

$$(0,y)*(a,b) = (0.a \ , 0.b+y.a) = (0, y.a) \neq (1,0) \quad \forall (a,b)$$

Donc les $(0,y)$ ne sont pas symétrisables.

Ex. 9 On suppose que $*$ vérifie qu'il existe e tq

$\forall x \quad e * x = x \quad (1)$ (e est neutre seulement "à gauche")

$\forall x\ \exists x'$ tq $\quad x x' = e \quad (2)$

et $\forall x,y,z \quad (xy)z = (yz)x \quad (3)$

donc seulement des relations partielles ...

par commodité, on note xy pour $x * y$ ...

i) On veut montrer que $x'x = e$

On commence par calculer

$$\underbrace{(xx')}_{\overset{(2)}{=} e} x \underset{(3)}{=} (x'x)x$$

$$e x \underset{(1)}{=} x$$

donc $\boxed{(x'x)x = x}$

vu ce qu'on veut montrer il faut encore bricoler

on mult. par x' à droite

$$\underbrace{((x'x)x)x'}_{} = xx' = e$$

$$((x'x)x)x' = \underbrace{(xx')}_{e}(x'x) = x'x$$

On obtient bien $\underline{x'x = e}$ (4)

ii) Soient $x, y \in \mathbb{R}$, on veut prouver qu'étant donné x' défini à partir de x précédemment, on a :

$$(x'x)y = y \quad (5) \qquad \text{et} \qquad (yx')x = y \quad (6)$$

Comme on a montré $x'x = e$

$(x'x)y = ey \underset{(1)}{=} y$ ✓

$(yx')x \underset{(3)}{=} (x'x)y = y$ ✓

iii) Comment en déduire que $*$ est commutative ?

$$x y \underset{(6)}{=} x((yx')x) \overset{(3)}{=} ((yx')x)x \overset{(3)}{=} (\underbrace{(x'x)y}_{\overset{(5)}{=} y})x = yx$$

Donc $*$ est bien commutative

iv) Passons à l'associativité

Soient $x, y, z \in \mathbb{R}$ $\quad x(yz) \overset{?}{=} (xy)z$?

On a prouvé que $*$ est commutative, donc

$$x(yz) = (yz)x \underset{(3)}{=} (zx)y \underset{(3)}{=} (xy)z$$

Donc $*$ est bien associative

v) Pour montrer que e est neutre, il faut prouver que $\forall x \quad xe = x$

Or comme on a montré que $*$ commutative :

$$xe = ex = x \quad \checkmark$$

vi) On en déduit finalement que $(E, *)$ est un groupe commutatif.

II. Sous-groupes, sous-groupes engendrés, groupes quotients.

<u>Ex. 17</u> On veut montrer que l'union ne cohabite pas du tout avec les sous-groupes (alors que $\cap$ si ...)

i.e. Soient H, K des sous-groupes de G. Montrons que :

$H \cup K$ sous-groupe ssi $H \subseteq K$ ou $K \subseteq H$

- $H \subseteq K$ ou $K \subseteq H \implies H \cup K$ sous-groupe est évident car $\searrow \implies H \cup K = H$ ou K ...

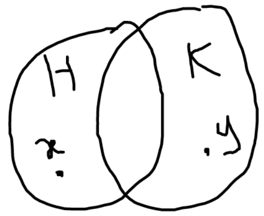
- $H \cup K$ sous-groupe $\implies H \subseteq K$ ou $K \subseteq H$?

On suppose que $H \cup K$ est un sous-groupe

Il est plus simple de raisonner par l'absurde que de prouver directement $H \subseteq K$ ou $K \subseteq H$ ...

Donc on suppose par l'absurde que $H \not\subseteq K$ et $K \not\subseteq H$

$\exists x \in H$ tq $x \notin K$ et $y \in K$ tq $y \notin H$



On ne peut pas faire grand chose d'autre que considérer xy ... et utiliser l'hypothèse ($H \cup K$ est un sous-groupe)

$$\underbrace{x \in H}_{\Downarrow \atop x \in H\cup K} \quad \underbrace{y \in K}_{\Downarrow \atop y \in H \cup K} \Longrightarrow \underbrace{xy \in H\cup K}$$

car $H\cup K$ sous groupe $\Rightarrow$ stable par $*$

donc (déf de $H \cup K$ ...)

$xy \in H$ ou $xy \in K$

mais ds ce cas :

$$\tilde{x}(xy) = (\tilde{x}x)\, y$$

$*$ associative

$\tilde{x} \in H$ car $x \in H$ et H ss-groupe, $xy \in H$

$(\tilde{x}x)\,y = ey = y$

On en déduirait que $y \in H$ ce qui est impossible.

de même en considérant $(xy)\,\tilde{y}$, on en déduirait que $x \in H$ ... impossible aussi

Donc $H\cup K$ ne peut être un sous-groupe

<u>Ex. 18</u> On considère n, m premiers entre eux et on veut montrer que

$$\mathbb{Z}/nm\mathbb{Z} \underset{\simeq}{\text{isomorphe}} \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

Donc qu'il y a un morphisme bijectif entre eux

Il est facile de trouver un morphisme

$$\mathbb{Z}/nm\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

Comme on va manipuler des classes dans des quotients différents, commençons par fixer une notation :

dans $\mathbb{Z}/nm\mathbb{Z}$: $\dot{x}$ | dans $\mathbb{Z}/n\mathbb{Z}$ $\bar{x}^n$ et $\mathbb{Z}/m\mathbb{Z}$ $\bar{x}^m$

Le morphisme le plus simple est :

$$\varphi : \mathbb{Z}/nm\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$
$$\dot{x} \longmapsto (\bar{x}^n, \bar{x}^m)$$

Prenons un exemple : $n = 3$, $m = 5$

$$\varphi : \mathbb{Z}/15\mathbb{Z} \longrightarrow \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$$
$$\dot{x} \longmapsto (\bar{x}^3, \bar{x}^5)$$

x modulo 15 $\rightsquigarrow$ $\underbrace{(x \bmod 3,\ x \bmod 5)}$

si on connait x mod 3 et 5

on peut le reconstruire mod 15 ?

Exemples de valeurs : $\dot{\varphi}(\dot{7}) = (\bar{1}^3, \bar{2}^5)$

7 mod 3   7 mod 5

φ est-elle → un morphisme de groupes ?
→ bijective ?

i) Montrons que φ est un morphisme :

Soient $\dot{x}, \dot{y} \in \mathbb{Z}/nm\mathbb{Z}$ par déf. de l'addition quotient : $\dot{x} + \dot{y} = \dot{\overline{x+y}}$

Donc $\varphi(\dot{x} + \dot{y}) = \varphi(\dot{\overline{x+y}}) = (\overline{x+y}^n, \overline{x+y}^m)$

$x+y$ modulo n

On a toujours par déf. de l'addition des $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z}$: $\overline{x+y}^n = \bar{x}^n + \bar{y}^n$

$\overline{x+y}^m = \bar{x}^m + \bar{y}^m$

Donc

$$\varphi(\dot{x} + \dot{y}) = (\bar{x}^n + \bar{y}^n, \bar{x}^m + \bar{y}^m) = (\bar{x}^n, \bar{x}^m) + (\bar{y}^n, \bar{y}^m) = \varphi(\dot{x}) + \varphi(\dot{y})$$

Donc φ est bien un morphisme de groupes.

ii) Puis, pour vérifier que φ est bijective, on va utiliser la prop. des morphismes :

φ injective ssi $\ker(\varphi) = \{\dot{0}\}$?

On conclura en disant que $\mathbb{Z}/_{nm}\mathbb{Z}$ et $\mathbb{Z}/_{n}\mathbb{Z} \times \mathbb{Z}/_{m}\mathbb{Z}$ ont le même nombre d'éléments :

$n \times m$

Et comme φ injective $\overset{+}{\Longrightarrow}$ φ surjective

Donc reste à prouver que $\ker(\varphi) = \{\dot{0}\}$!

égalité d'ensembles

$\{\dot{0}\} \subseteq \ker\varphi$?

évident car φ morphisme $\Longrightarrow$ $\varphi(\dot{0}) = (\bar{0}^n, \bar{0}^m)$

$\underline{\ker\varphi \subseteq \{\dot{0}\}}$?

$\ker\varphi = \{\dot{x} \in \mathbb{Z}/_{nm}\mathbb{Z} \;;\; \varphi(\dot{x}) = \text{neutre de } \mathbb{Z}/_{n}\mathbb{Z} \times \mathbb{Z}/_{m}\mathbb{Z}\}$

neutre de $\mathbb{Z}/_{n}\mathbb{Z} \times \mathbb{Z}/_{m}\mathbb{Z} = (\bar{0}^n, \bar{0}^m)$

Soit $\underbrace{\dot{x} \in \ker\varphi}$, montrons que $\dot{x} = \dot{0}$?

$\varphi(\dot{x}) = (\bar{0}^n, \bar{0}^m)$

Donc

$x \equiv 0\,[n]$ a.t. on $x \equiv 0\,[nm]$?

$x \equiv 0\,[m]$

Il est toujours plus simple de raisonner sur la divisibilité

$n \mid x$

$m \mid x$ a $\operatorname{pgcd}(n,m) = 1$ $\Longrightarrow$ $nm \mid x$

(th. des restes chinois)

$\Downarrow$

$x \equiv 0\,[nm]$!

ce qui conclut :

φ est bien un isomorphisme.