Planche TD 2

Exo 1, Exo 3 faits

Exo 2. La table de la multiplication sur $\mathbb{Z}_{30}^{\times}$

Rappel Soit $k \in \mathbb{Z}$, $n \in \mathbb{N}^*$

$$[k]_n \in \mathbb{Z}_n^{\times} \iff pgcd(k,n) = 1$$

$$\mathbb{Z}_{30}^{\times} = \{[1], [7], [11], [13], [17], [19], [23], [29]\}$$

nous avons écrit $[k]$ au lieu de $[k]_{30}$

Pour faire la table de la multiplication :

$$[k][l] = [kl]$$

$$[23] = [-7], \quad [29] = [-1]$$

$\cdot$	$[1]$	$[7]$	$[11]$	$[13]$	$[17]$	$[19]$	$[23]$	$[29]$
$[1]$	$[1]$	$[7]$	$[11]$	$[13]$	$[17]$	$[19]$	$[23]$	$[29]$
$[7]$	$[7]$	$[19]$	$[17]$	$[1]$	$[29]$	$[13]$	$[11]$	$[23]$
$[11]$	$[11]$	$[17]$	$[1]$	$[23]$	$[7]$	$[29]$	$[13]$	$[19]$
$[13]$	$[13]$	$[1]$	$[23]$	$[19]$	$[11]$	$[7]$	$[29]$	$[17]$
$[17]$	$[17]$	$[29]$	$[7]$	$[11]$	$[19]$	$[23]$	$[1]$	$[13]$
$[19]$	$[19]$	$[13]$	$[29]$	$[7]$	$[23]$	$[1]$	$[17]$	$[11]$
$[23]$	$[23]$	$[11]$	$[13]$	$[29]$	$[1]$	$[17]$	$[19]$	$[7]$
$[29]$	$[29]$	$[23]$	$[19]$	$[17]$	$[13]$	$[11]$	$[7]$	$[1]$

$$\begin{array}{r} 13 \\ \times\ 13 \\ \hline 143 \end{array} \qquad 143 = 4 \cdot 30 + 23$$

$$13 \cdot 13 = 169 = 5 \cdot 30 + 19$$

Rappel
$(\mathbb{Z}_n^\times, \cdot)$ est un groupe abélien

$30 = 5 \cdot 6$ et $pgcd(5,6) = 1$

$n_1 = 5,\ n_2 = 6,\ n = 30$

D'après la version multiplicative du théorème chinois, on obtient un isomorphisme $\mathbb{Z}_{30}^\times \xrightarrow{h} \mathbb{Z}_5^\times \times \mathbb{Z}_6^\times$

$h([k]_{30}) = ([k]_5, [k]_6)$

Exo 4.

1 $(2\mathbb{Z}, +)$. D'après le cours

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

donc, muni de la lci induite

(c'est à dire de l'addition), est un groupe

2. $(2\mathbb{Z}+1, \cdot)$

Remarque $\cdot$ est bien une lci sur $2\mathbb{Z}+1$:

$$(2k+1)(2\ell+1) = \underbrace{4k\ell + 2k + 2\ell}_{2(k\ell+k+\ell)} + 1$$

Argument plus rapide :

$$[1]_2 \cdot [1]_2 = [1]_2$$

associativité : oui

élément neutre : $1 \in 2\mathbb{Z}+1$ oui

3 n'admet pas de symétrique, donc le

3me axiome dans la définition d'un groupe n'est pas satisfait

la réponse est : NON

3. $(\mathbb{C}, -)$ - est bien une lci sur $\mathbb{C}$

Est-ce que $-$ est associative (sur $\mathbb{C}$) ?

Soient $z_1, z_2, z_3 \in \mathbb{C}$. À comparer

$(z_1 - z_2) - z_3$ avec $z_1 - (z_2 - z_3) = z_1 - z_2 + z_3$

$\| $

$z_1 - z_2 - z_3$

on n'a pas égalité si $z_3 \neq 0$

- n'est pas associative

$(\mathbb{C}, -)$ n'est pas un groupe

4. $(\mathcal{F}(\mathbb{R},\mathbb{R}),+)$ est bien un groupe.

Plus généralement, soient X un ensemble, $(G,*)$ un groupe, $\mathcal{F}(X,G) := \{f : X \to G \mid f \text{ application}\}$

Sur $\mathcal{F}(X,G)$ soit $*$ la loi définie

$$(f*g)(x) := f(x) * g(x)$$

Alors $(\mathcal{F}(X,G),*)$ est un groupe :

(a) $*$ associative : Soient $f,g,h \in \mathcal{F}(X,G)$.

À démontrer : $(f*g)*h = f*(g*h)$

Il s'agit d'applications définies sur X à valeurs dans G. Soit $x \in X$

$$((f*g)*h)(x) = (f*g)(x)*h(x) = (f(x)*g(x))*h(x)$$

De la même manière

$$(f*(g*h))(x) = f(x)*(g(x)*h(x))$$

Puisque $(G,*)$ est un groupe, on a égalité pour tout $x \in X$

(ii) Soit e l'élément neutre de $(G,*)$
d'application constante $\tilde{e} : X \longrightarrow G$ donnée par: $\forall x \in X,\ \tilde{e}(x) = e$ est élément neutre pour $*$ sur $\mathcal{F}(X,G)$. En effet:
$\forall x \in X,\ (\tilde{e}*f)(x) = \tilde{e}(x)*f(x) = e*f(x) = f(x)$. Donc $\tilde{e}*f = f$
Pareil : $f*\tilde{e} = f$

(iii) Soit $f \in \mathcal{F}(X,G)$.
Définissons $f' \in \mathcal{F}(X,G)$ par $f'(x) := f(x)'$
(le symétrique de $f(x)$ dans $(G,*)$).

$$\forall x \in X,\ (f * f')(x) = f(x) * f'(x) = f(x) * (f(x))' = e = \tilde{e}(x)$$

$$\Downarrow$$

$$f * f' = \tilde{e}$$

Pareil : $f' * f = \tilde{e}$, donc f' est bien le symétrique de f par rapport à $*$

Attention ! f' désigne le symétrique de f par rapport à la lci $*$ sur $\mathcal{F}(X, G)$, n'a rien à voir avec la dérivée

Par exemple, si $(G, *) = (\mathbb{R}, +)$, on va noter $-f$ au lieu de f'.

5. $(\mathcal{F}(\mathbb{R},\mathbb{R}), \cdot)$. Pour $f, g \in \mathcal{F}(\mathbb{R},\mathbb{R})$, $f \cdot g$ est définie par $(f \cdot g)(x) := f(x)\, g(x)$

(0) $\cdot$ est bien une lci sur $\mathcal{F}(\mathbb{R},\mathbb{R})$

(1) $\cdot$ est associative sur $\mathcal{F}(\mathbb{R},\mathbb{R})$ parce que la multiplication est associative sur $\mathbb{R}$ (voir Q4)

(2) L'application constante $\tilde{1} \in \mathcal{F}(\mathbb{R},\mathbb{R})$, $\tilde{1}(x) = 1$ $\forall x \in \mathbb{R}$ est élément neutre pour $\cdot$ (voir Q4)

(3): Toute application qui a un point d'annulation n'admet pas de symétrique par rapport à $\cdot$.

Réponse : NON.

6. $(\mathcal{F}(\mathbb{R},\mathbb{R}), \circ)$

(0). $\circ$ est bien une lci sur $\mathcal{F}(\mathbb{R},\mathbb{R})$

Rappel  $g\circ f : A \to C$

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

la composition définit une lci sur $\mathcal{F}(A,A)$

(1) $\circ$ est associative (voir L 1)

(2) $id_{\mathbb{R}}$ est élément neutre pour $\circ$ (voir L 1)

(3) Une application $f : \mathbb{R} \to \mathbb{R}$ admet un symétrique par rapport à $\circ$ ssi f est bijective et, si c'est le cas, alors son symétrique sera f^{-1} (voir L 1). Soit $f : \mathbb{R} \to \mathbb{R}$

non-bijective (par exemple une application constante)
Alors f n'admet pas de symétrique par rapport à $\circ$. Réponse : NON

Exo 5 M.q. les couples suivants sont des groupes :

1 $(\{\pm 1\}, \cdot)$, $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$

D'après le cours $(\mathbb{C}^*, \cdot)$ est un groupe et $\{\pm 1\} \subset \mathbb{Q}^* \subset \mathbb{R}^* \subset \mathbb{C}^*$ sont des inclusions de sous-groupe.

2. $(\mathbb{R}_n[X], +)$, $(\mathbb{R}[X], +)$, $(\mathbb{R}^n, +)$

$\mathbb{R}[X]$ est l'ensemble des polynômes à coefficients réels

$\mathbb{R}_n[X]$ " " " " " de degré $\leq n$

$(\mathbb{R}^n, +)$ groupe abélien (voir le cours)

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} := \begin{pmatrix} x_1+y_1 \\ \vdots \\ x_n+y_n \end{pmatrix}$$

$$\mathbb{R}[X] = \left\{ \sum_{i=0}^{n} a_i X^i \;\middle|\; n \in \mathbb{N},\ a_i \in \mathbb{R} \text{ pour } 0 \leq i \leq n \right\}$$

$$P = \sum_{i=1}^{n} a_i X^i \quad , \quad Q = \sum_{i=1}^{m} b_i X^i$$

$$P+Q = \sum_{i=1}^{N} (a_i + b_i) X^i \quad \text{où } N := \max(m,n)$$

En utilisant les propriétés de + sur $\mathbb{R}$ on obtient $(\mathbb{R}[X], +)$ est un groupe dont l'élément neutre est le polynôme nul. Si $f = \sum_{i=0}^{n} a_i X^i$, son symétrique est $\sum_{i=0}^{n} (-a_i) X^i$.

$\mathbb{R}_n[X]$ est un sous-groupe de $(\mathbb{R}[X], +)$ donc devient groupe si muni de la lci induite (i.e de l'addition des polynômes)