Avignon Université - UFR STS | Année 2021/2022
**L3 S5 mathématiques** | Algèbre générale 1

# Corrigé du CC1

**Exercice 1.** On définit une loi de composition interne $\otimes$ sur $\mathbb{R}^* \times \mathbb{R}$ en posant

$$(a,b) \otimes (a',b') = (aa', ab' + b)$$

Montrer que $(\mathbb{R}^* \times \mathbb{R}, \otimes)$ est un groupe. Ce groupe est-il commutatif?

i) Montrons que $\otimes$ est associative. Soit $x = (a,b)$, $x' = (a',b')$, $x'' = (a'',b'')$ des éléments de $\mathbb{R}^* \times \mathbb{R}$. On a

$$\begin{aligned} ((a,b) \otimes (a',b')) \otimes (a'',b'') &= (aa', ab'+b) \otimes (a'',b'') \\ &= ((aa')a'', (aa')b'' + (ab'+b)) \\ &= (aa'a'', aa'b'' + ab' + b) \end{aligned}$$

et

$$\begin{aligned} (a,b) \otimes ((a',b') \otimes (a'',b'')) &= (a,b) \otimes (a'a'', a'b'' + b') \\ &= (a(a'a''), a(a'b''+b') + b) \\ &= (aa'a'', aa'b'' + ab' + b) \end{aligned}$$

D'où

$$\forall (x,x',x'') \in (\mathbb{R}^* \times \mathbb{R})^3\,,\ (x \otimes x') \otimes x'' = x \otimes (x' \otimes x'')\,.$$

La loi $\otimes$ est associative.

ii) Pour tout $x = (a,b) \in \mathbb{R}^* \times \mathbb{R}$,

$$(a,b) \otimes (1,0) = (a, 0+b) = (a,b) \qquad \text{et} \qquad (1,0) \otimes (a,b) = (a, b+0) = (a,b)\,,$$

donc la loi $\otimes$ admet $(1,0)$ comme élément neutre.

iii) Soit $(a,b), (a',b') \in \mathbb{R}^* \times \mathbb{R}$. On a

$$(a,b) \otimes (a',b') = (1,0) \iff \begin{cases} aa' = 1 \\ ab' + b = 0 \end{cases} \iff \begin{cases} a' = 1/a \\ b' = -b/a \end{cases}$$

On a donc, pour $x = (a,b) \in \mathbb{R}^* \times \mathbb{R}$, $x \otimes (1/a, -b/a) = (1,0)$. De plus $(1/a, -b/a) \otimes x = (1, b/a - b/a) = (1,0)$. Donc tout $x \in \mathbb{R}^* \times \mathbb{R}$ admet un inverse pour la loi $\otimes$.

iv) Conclusion : $(\mathbb{R}^* \times \mathbb{R}, \otimes)$ est un groupe. Ce groupe n'est pas commutatif, car $(2,1) \otimes (1,1) = (2,3)$ alors que $(1,1) \otimes (2,1) = (2,2)$.

**Exercice 2.** Soit $(G,*)$ un groupe. Pour $g \in G$, on pose

$$Z_g = \{x \in G \,|\, g * x = x * g\}$$

1. Montrer que $Z_g$ est un sous-groupe de $(G,*)$ contenant $g$.

i) $g$ commutant avec lui-même, $g \in Z_g$. En particulier $Z_g \neq \emptyset$.
ii) Soit $x, y$ in $Z_g$. On a

$$g * (x * y) = (g * x) * y = (x * g) * y = x * (g * y) = x * (y * g) = (x * y) * g\,.$$

Dans la suite d'égalités ci-dessus, on a utilisé l'associativité de la loi $*$, en plus de l'appartenance de $x$ et $y$ à $G$. D'où $x * y \in Z_g$. $Z_g$ est stable pour la loi $*$.
iii) Soit $x \in Z_g$. On a $g * x = x * g$ donc

$$x^{-1} * (g * x) * x^{-1} = x^{-1} * (x * g) * x^{-1} ,$$

ce qui donne (en utilisant l'associativité de $*$) $x^{-1} * g = g * x^{-1}$, et donc $x^{-1} \in Z_g$. Ainsi $Z_g$ est stable par passage à l'inverse.
Conclusion : $Z_g$ est un sous-groupe de $(G, *)$.

2. On suppose dans cette question que $(G, *) = (GL(2, \mathbb{R}), \times)$. Déterminer $Z_g$ dans les cas suivants.

$$i)\ g = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad ii)\ g = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

i) On suppose $g = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Pour $x = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$,

$$\begin{aligned} gx = xg \quad &\Longleftrightarrow \quad \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \Longleftrightarrow \begin{pmatrix} a & b \\ -c & -d \end{pmatrix} = \begin{pmatrix} a & -b \\ c & -d \end{pmatrix} \\ &\Longleftrightarrow \quad b = 0 \text{ et } c = 0 . \end{aligned}$$

Donc

$$Z_g = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \ ; \ a, d \in \mathbb{R}^* \right\} ,$$

c'est-à-dire : $Z_g$ est l'ensemble des matrices de $M_2(\mathbb{R})$ qui sont diagonales et inversibles.

ii) On suppose $g = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Pour $x = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$,

$$\begin{aligned} gx = xg \quad &\Longleftrightarrow \quad \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \Longleftrightarrow \begin{pmatrix} c & d \\ -a & -b \end{pmatrix} = \begin{pmatrix} -b & a \\ -d & c \end{pmatrix} \\ &\Longleftrightarrow \quad d = a \text{ et } b = -c . \end{aligned}$$

Donc

$$Z_g = \left\{ \begin{pmatrix} a & -c \\ c & a \end{pmatrix} \ ; \ a, c \in \mathbb{R} ,\ (a, c) \neq (0, 0) \right\} ,$$

la condition $(a, c) \neq (0, 0)$ étant là pour que le déterminant $a^2 + c^2$ de la matrice soit non nul.

**Exercice 3.** Soit $(G, *)$ un groupe. Un élément $a$ de $G$ est appelé carré s'il existe $x \in G$ tel que $a = x^2 = x * x$. On note $K$ l'ensemble des carrés de $G$ :

$$K = \{x * x \,;\ x \in G\} , \qquad K \subset G .$$

1. Déterminer $K$ dans chacun des cas suivants.

*i)* $(G, *) = (\mathbb{R}^*, \times)$ *ii)* $(G, *) = (\mathbb{C}^*, \times)$ *iii)* $(G, *) = (\mathbb{Z}/3\mathbb{Z}, +)$ *iv)* $(G, *) = (\mathbb{Z}/6\mathbb{Z}, +)$

i) Dans $(\mathbb{R}^*, \times)$, l'ensemble $K$ des carrés est $\mathbb{R}_+^*$.
ii) Pour tout $a \in \mathbb{C}^*$, l'équation $z^2 = a$ a deux solutions (opposées) dans $\mathbb{C}^*$, donc si $(G, *) = (\mathbb{C}^*, \times)$, $K = \mathbb{C}^*$.

iii) Dans $(\mathbb{Z}/3\mathbb{Z}, +)$ , on a le tableau suivant :

| | | | |
|---|---|---|---|
| $x$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |
| $x + x$ | $\bar{0}$ | $\bar{2}$ | $\bar{1}$ |

. Donc $K = \mathbb{Z}/3\mathbb{Z}$.

iv) Dans $(\mathbb{Z}/6\mathbb{Z},+)$ , on a le tableau suivant :

| $x$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ | $\overline{4}$ | $\overline{5}$ |
|---|---|---|---|---|---|---|
| $x+x$ | $\overline{0}$ | $\overline{2}$ | $\overline{4}$ | $\overline{0}$ | $\overline{2}$ | $\overline{4}$ |

. Donc $K = \{\overline{0}, \overline{2}, \overline{4}\}$.

2. On suppose dans cette question que $(G, *)$ est un groupe d'ordre fini *impair.* Montrer que $K = G$. *Indication : pour $a \in G$, chercher une solution de l'équation $x^2 = a$ sous la forme d'une puissance de $a$.*

Soit $a \in G$. D'après un corollaire du théorème de Lagrange, on a $a^n = e$, où $n$ est l'ordre de $G$ et $e$ l'élément neutre. On a supposé $n$ impair, $n = 2p+1$, avec $p \in \mathbb{N}$. On a

$$(a^{p+1})^2 = a^{2p+2} = a^{2p+1} * a = e * a = a\,.$$

Donc l'équation (dans $G$) $x^2 = a$ a une solution $x = a^{p+1}$. On a montré que tout élément $a$ de $G$ est un carré. D'où $K = G$.

**Exercice 4.**

1. Quel peut être l'ordre d'un sous-groupe de $(\mathbb{Z}/15\mathbb{Z},+)$?

L'ordre d'un sous-groupe de $(\mathbb{Z}/15\mathbb{Z},+)$ peut être 1, 3, 5 ou 15 car d'après le théorème de Lagrange, c'est un diviseur de 15, l'ordre de $(\mathbb{Z}/15\mathbb{Z},+)$.

2. Déterminer tous les sous-groupes de $(\mathbb{Z}/15\mathbb{Z},+)$.

- $(\mathbb{Z}/15\mathbb{Z},+)$ a un unique sous-groupe d'ordre 1, $H_1 = \{\overline{0}\}$ et un unique sous-groupe d'ordre 15, $H_2 = \mathbb{Z}/15\mathbb{Z}$.
- si $H$ est un sous-groupe d'ordre 3 de $(\mathbb{Z}/15\mathbb{Z},+)$, alors pour tout $x = \overline{n} \in H$, $x+x+x = \overline{3n} = \overline{0}$ (conséquence du théorème de Lagrange déjà utilisée dans l'exercice précédent), donc 15 divise $3n$, donc 5 divise $n$. Ceci montre que le seul sous-groupe de $(\mathbb{Z}/15\mathbb{Z},+)$ d'ordre 3 est
$$H_3 = \langle \overline{5} \rangle = \{\overline{0}, \overline{5}, \overline{10}\}\,.$$
- De même, si $H$ est un sous-groupe d'ordre 5 de $(\mathbb{Z}/15\mathbb{Z},+)$, alors pour tout $\overline{n} \in H$, $\overline{5n} = \overline{0}$, donc 15 divise $5n$, donc 3 divise $n$. Le seul sous-groupe de $(\mathbb{Z}/15\mathbb{Z},+)$ d'ordre 5 est donc
$$H_4 = \langle \overline{3} \rangle = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}, \overline{12}\}\,.$$