L2 MTH1314 2016-2017

Correction du devoir maison n ° 2

Solution de l'exercice 1

Question 1.

1. On sait, cela fait partie des exemples classiques, que $(\mathbb{R}^2, +)$ est un groupe commutatif (en tant que groupe produit du groupe commutatif $(\mathbb{R}, +)$) où l'élément neutre $\tilde{0}$ est donné par $\tilde{0} = (0, 0)$ et l'inverse de chaque élément $(x, y) \in \mathbb{R}^2$ est bien sûr $(-x, -y) \in \mathbb{R}^2$.

2. La loi $*$ est plus exotique. Vérifions que $*$ est une loi de composition interne. Soient (x, y) et (a, b) deux éléments de $\mathbb{R}^2$. Alors

$$(x, y) * (a, b) = (\underbrace{xa}_{\in\mathbb{R}}, \underbrace{xb + ya}_{\in\mathbb{R}}).$$

   Donc $(x, y) * (a, b) \in \mathbb{R}^2$ pour tout $(x, y, a, b) \in \mathbb{R}^4$ et donc $*$ est une loi de composition interne.

3. La loi $*$ est associative. En effet pour tout (x, y), (a, b) et (u, v) dans $\mathbb{R}^2$, on a

$$(x, y) * [(a, b) * (u, v)] = (x, y) * (au, av + bu) = (xau, xav + xbu + yau).$$

   D'autre part,

$$[(x, y) * (a, b)] * (u, v) = (xa, xb + ya) * (u, v) = (xau, xav + xbu + yau).$$

   Donc pour tout $(x, y, a, b, u, v) \in \mathbb{R}^6$, $(x, y) * [(a, b) * (u, v)] = [(x, y) * (a, b)] * (u, v)$ et donc la loi $*$ est associative.

4. Considérons $(1, 0)$ qui est naturellement un élément de $\mathbb{R}^2$. Pour tout $(x, y) \in \mathbb{R}^2$, on a $(x, y) * (1, 0) = (1, 0) * (x, y) = (x, y)$. Donc $(1, 0)$ est l'élément neutre pour la loi $*$.

5. Montrons que $*$ est commutative. Soit $((x, y), (a, b)) \in (\mathbb{R}^2)^2$, on a $(x, y) * (a, b) = (xa, xb + ya) = (ax, ay + bx) = (a, b) * (x, y)$. Donc $*$ est bien commutative.

6. Montrons que $*$ est distributive sur $+$. Soient (x, y), (a, b) et (u, v) trois éléments de $\mathbb{R}^2$. On a

$$(x, y) * [(a, b) + (u, v)] = (x, y) * (a + u, b + v) = (xa + xu, xb + xv + ya + yu).$$

   D'autre part,

$$[(x, y) * (a, b)] + [(x, y) * (u, v)] = (xa, xb + ya) + (xu, xv + yu) = (xa + xu, xb + ya + xv + yu).$$

   Donc pour tout (x, y), (a, b) et (u, v) dans $\mathbb{R}^2$, $(x, y) * [(a, b) + (u, v)] = [(x, y) * (a, b)] + [(x, y) * (u, v)]$ et la loi $*$ est distributive à gauche. Maintenant puisque la loi $*$ est commutative, on va montrer qu'elle est aussi distributive à droite. Pour tout $(x, y, a, b, u, v) \in \mathbb{R}^6$,

$$\begin{aligned}
[(a, b) + (u, v)] * (x, y) &= (x, y) * [(a, b) + (u, v)] && \text{car } * \text{ est commutative,} \\
&= [(x, y) * (a, b)] + [(x, y) * (u, v)] && \text{car } * \text{ est distributive à gauche,} \\
&= [(a, b) * (x, y)] + [(u, v) * (x, y)] && \text{car } * \text{ est commutative.}
\end{aligned}$$

   Ce qui montre bien que $*$ est distributive à droite également.

Tous ces résultats nous assurent que $(\mathbb{R}^2, +, *)$ est un anneau commutatif.

Question 2. On considère $X \in \mathbb{R}^2$ et on pose pour cette question $X = (x, y)$.

(a)

$$\begin{aligned} X^2 = X \Leftrightarrow (x,y) * (x,y) = (x,y) &\Leftrightarrow (x^2, 2xy) = (x,y) \\ &\Leftrightarrow \begin{cases} x^2 = x \\ 2xy = y \end{cases} \\ &\Leftrightarrow \begin{cases} x = 0 \\ y = 0 \end{cases} \text{ ou } \begin{cases} x = 1 \\ y = 0 \end{cases} \\ &\Leftrightarrow X = (0,0) \text{ ou } X = (1,0). \end{aligned}$$

L'ensemble des solutions de l'équation $X^2 = X$ est donc $\{(0,0),\ (1,0)\}$.

(b)

$$\begin{aligned} X^2 = \tilde{0} \Leftrightarrow (x,y) * (x,y) = (0,0) &\Leftrightarrow (x^2, 2xy) = (0,0) \\ &\Leftrightarrow \begin{cases} x^2 = 0 \\ 2xy = 0 \end{cases} \\ &\Leftrightarrow \begin{cases} x = 0 \\ y \text{ est quelconque.} \end{cases} \end{aligned}$$

L'ensemble des solutions de l'équation $X^2 = \tilde{0}$ est donc $\{(0, y),\ \text{avec } y \in \mathbb{R}\}$.

(c)

$$\begin{aligned} X^2 = \tilde{1} \Leftrightarrow (x,y) * (x,y) = (1,0) &\Leftrightarrow (x^2, 2xy) = (1,0) \\ &\Leftrightarrow \begin{cases} x^2 = 1 \\ 2xy = 0 \end{cases} \\ &\Leftrightarrow \begin{cases} x = 1 \\ y = 0 \end{cases} \text{ ou } \begin{cases} x = -1 \\ y = 0 \end{cases} \\ &\Leftrightarrow X = (1,0) \text{ ou } X = (-1,0). \end{aligned}$$

L'ensemble des solutions de l'équation $X^2 = \tilde{0}$ est donc $\{(1,0),\ (-1,0)\}$.

Question 3. Soit $(x, y) \in \mathbb{R}^2$. On suppose (x, y) inversible (pour $*$ naturellement puisque pour $+$ tous les éléments sont toujours tous inversibles dans un anneau). Alors il existe $(a, b) \in \mathbb{R}^2$ tel que $(x, y) * (a, b) = \tilde{1} = (1, 0)$. Donc $(xa, xb + ya) = (1, 0)$ et donc

$$\begin{cases} xa = 1 \\ xb + ya = 0. \end{cases}$$

On note que puisque $xa = 1$, nécessairement $x \neq 0$, ce qui restreint la quantité d'inversibles. On sait déjà que tous les $(0, y)$ ne peuvent pas être inversibles. Continuons notre analyse avec $(x, y) \in \mathbb{R}^* \times \mathbb{R}$. Puisque $x \neq 0$, on a

$$\begin{cases} a = \dfrac{1}{x} \\ xb + \dfrac{y}{x} = 0 \end{cases} \Rightarrow \begin{cases} a = \dfrac{1}{x} \\ b = -\dfrac{y}{x^2}. \end{cases}$$

On détermine donc de façon unique un inverse pour $(x,y) \in \mathbb{R}^* \times \mathbb{R}$. On a déjà vu que les inversibles sont inclus dans l'ensemble $\mathbb{R}^* \times \mathbb{R}$. Démontrons maintenant la réciproque. Synthèse : soit $(x,y) \in \mathbb{R}^* \times \mathbb{R}$ alors l'élément $(a,b) = \left(\frac{1}{x}, \frac{-y}{x^2}\right)$ existe bien dans $\mathbb{R}^2$. De plus,

$$(x,y) * (a,b) = (x,y) * \left(\frac{1}{x}, \frac{-y}{x^2}\right) = \left(1, \frac{-y}{x} + \frac{-y}{x}\right) = \tilde{1}.$$

Et de même $(a,b) * (x,y) = \tilde{1}$ puisque la loi $*$ est commutative. Donc (x,y) est inversible (et d'inverse $\left(\frac{1}{x}, \frac{-y}{x^2}\right)$). D'où le fait que l'ensemble des inversible de $(\mathbb{R}^2, +, *)$ est exactement $\mathbb{R}^* \times \mathbb{R}$.

Question 4(a). Pour tout $n \geqslant 0$ on note P_n la proposition « $X^n = (x^n, 0)$ ». Démontrons par récurrence que pour tout $n \geqslant 0$, P_n est vraie.
Initialisation : par définition $X^0 = \tilde{1} = (1,0) = (x^0, 0)$. Donc P_0 est vraie.
Hérédité : supposons qu'il existe un entier $n \in \mathbb{N}$ tel que P_n soit vraie. Alors $X^n = (x^n, 0)$. Donc

$$X^{n+1} = X^n * X = (x^n, 0) * (x, 0) = (x^{n+1}, 0).$$

Donc P_{n+1} est vraie. Ainsi on a montré que la propriété est héréditaire : $P_n \Rightarrow P_{n+1}$.
Par ce qui précède, P_n est vraie pour tout $n \geqslant 0$. Donc pour tout $n \geqslant 0$, $X^n = (x^n, 0)$.

Question 4(b). On calcul d'abord $X^2 = (0,y) * (0,y) = (0,0)$. Donc pour tout $n \geqslant 2$, on a

$$X^n = X^{n-2} * X^2 = X^{n-2} * (0,0) = (0,0) \qquad \text{(l'élément } (0,0) \text{ est dit absorbant).}$$

Donc pour tout $n \geqslant 2$, $X^n = \tilde{0}$ et reprécisons que $X^1 = X = (0,y)$ et $X^0 = \tilde{1}$.

Question 4(c). Soit $X = (x,y) \in \mathbb{R}^2$. On note que $X = (x,0) + (0,y)$ et que $(x,0)$ et $(0,y)$ commutent (puisque $*$ est commutative). Donc par la formule de binôme de Newton, on a

$$X^n = [(x,0) + (0,y)]^n = \sum_{k=0}^{n} \binom{n}{k} (x,0)^{n-k} * (0,y)^k.$$

Or d'après la question 4(b), on sait que $(0,y)^k = \tilde{0}$ pour tout $k \geqslant 2$. Donc, pour $n \geqslant 1$ (mieux vaut traiter le cas $n = 0$ à part)

$$X^n = (x,0)^n * \tilde{1} + n(x,0)^{n-1} * (0,y) = (x^n, 0) + (0, nx^{n-1}y) \qquad \text{en utilisant la question 4(a).}$$

Et finalement pour tout $n \geqslant 1$, $X^n = (x^n, nx^{n-1}y)$, formule qui reste éventuellement encore valide pour $n = 0$ avec la convention $nx^{n-1}y = 0$ pour $n = 0$.

Question 4(d). Redémontrons cette formule directement par récurrence. On fixe $(x,y) \in \mathbb{R}^2$. Considérons pour tout $n \geqslant 1$ la proposition Q_n : « $X^n = (x^n, nx^{n-1}y)$ ».
Initialisation : pour $n = 1$, on voit que $X^1 = (x,y) = (x^1, 1 \times x^0 y)$. Donc Q_1 est vraie.
Hérédité : supposons qu'il existe un entier $n \geqslant 1$ telle que la proposition Q_n soit vraie. Alors $X^n = (x^n, nx^{n-1}y)$. Donc

$$X^{n+1} = X^n * X = (x^n, nx^{n-1}y) * (x,y) = (x^{n+1}, x^n y + nx^n y) = (x^{n+1}, (n+1)x^n y).$$

Ainsi Q_{n+1} est vraie et on a montré que $Q_n \Rightarrow Q_{n+1}$.
Bilan, pour tout $n \geqslant 1$, Q_n est vraie et donc $X^n = (x^n, nx^{n-1}y)$.

Solution de l'exercice 2

Question 1. De façon très concise, on peut se reporter au cours pour dire que puisque $\left((\mathbb{Z}/13\mathbb{Z})^\times, \times\right)$ est un groupe, il est stable sous l'action de $\times$. Donc si $x \in (\mathbb{Z}/13\mathbb{Z})^\times$ alors $x^2 = x \times x \in (\mathbb{Z}/13\mathbb{Z})^\times$ et donc $x^3 = x^2 \times x \in (\mathbb{Z}/13\mathbb{Z})^\times$. Et donc φ est bien définie.

Question 2. Soient x et y deux éléments de $(\mathbb{Z}/13\mathbb{Z})^\times$. On a $\varphi(xy) = (xy)^3 = x^3y^3$ car $\times$ est commutative dans $(\mathbb{Z}/13\mathbb{Z})^\times$. Donc $\varphi(xy) = \varphi(x)\varphi(y)$ et φ est un bien un endomorphisme de $(\mathbb{Z}/13\mathbb{Z})^\times$.

Question 3(a). Soit $x \in \ker(\varphi)$. Par définition, $\varphi(x) = x^3 = 1$. Donc

$$x^3 - 1 = 0.$$

En développant l'expression $(x-1)(x^2+x+1)$ par les règles de calculs valides pour $+$ et $\times$ dans l'anneau $\mathbb{Z}/13\mathbb{Z}$, on a $(x-1)(x^2+x+1) = x^3+x^2+x-x^2-x-1 = x^3-1$. Puisque $x^3-1=0$, on en déduit que

$$(x-1)(x^2+x+1) = 0.$$

Maintenant vous êtes très nombreux à être tombés dans le piège présent dans cette question. « Un produit de facteurs est nul si et seulement si un des facteurs au moins est nul ». Cette affirmation bien connue dans $\mathbb{R}$ tombe en défaut en général dans $\mathbb{Z}/n\mathbb{Z}$. Pour exemple considérez $\mathbb{Z}/4\mathbb{Z}$ dans lequel $x^2 = 0$ n'implique pas $x = 0$. En effet $x = 2 \neq 0$ et pourtant $x^2 = 4 = 0$. En fait si la phrase précédente entre guillemets est vraie on dit l'anneau *intègre*. C'est le cas notamment de tous les corps (comme $\mathbb{Z}/13\mathbb{Z}$) car on peut, si l'on est non nul, toujours composer par l'inverse et simplifier. Concrètement dans $\mathbb{Z}/13\mathbb{Z}$, voici comment il fallait rédiger.
Premier cas $x = 1$ alors $x - 1 = 0$ et il n'y a rien de plus à démontrer.
Second cas $x \neq 1$ id est $x - 1 \neq 0$. Or puisque 13 est premier, tous les éléments non nuls sont inversibles ($\mathbb{Z}/13\mathbb{Z}$ est un corps ou encore $(\mathbb{Z}/13\mathbb{Z})^* = (\mathbb{Z}/13\mathbb{Z})^\times$). Ainsi on sait que $x-1$ est inversible. En composant par son inverse :

$$(x-1)^{-1}(x-1)(x^2+x+1) = (x-1)^{-1} \times 0$$

et donc $x^2+x+1 = 0$.
Ainsi dans tous les cas, $x = 1$ ou $x^2+x+1 = 0$.

Question 3(b). A nouveau plutôt que d'utiliser le discriminant qui fait ensuite appel à la racine carrée qui n'est pas appropriée dans $\mathbb{Z}/13\mathbb{Z}$, il faut remonter à son origine, la factorisation. Puisque $1 = -12$, on a

$$\begin{aligned} x^2+x+1 = x^2-12x+1 = (x-6)^2-36+1 = (x-6)^2-35 = (x-6)^2-9 = (x-6)^2-3^2 \\ = (x-9)(x-3). \end{aligned}$$

Question 3(c). D'après la question 3(a), si $x \in \ker(\varphi)$ alors $x = 1$ ou $x^2+x+1 = 0$. Puis par la question 3(b), si $x^2+x+1 = 0$ alors $(x-9)(x-3) = 0$. Donc, comme dans la question 3(a), deux cas se présentent : $x = 3$ ou $x \neq 3$. Si $x \neq 3$ alors $x-3$ est inversible. Donc $(x-9)(x-3) = 0$ implique $(x-9)(x-3)(x-3)^{-1} = (x-9) = 0 \times (x-3)^{-1} = 0$ et donc $x = 9$. De tous ces cas on en déduit que si $x \in \ker(\varphi)$ alors $x = 1$ ou $x = 3$ ou $x = 9$. Réciproquement si $x \in \{1,3,9\}$, puisque $\varphi(1) = 1$, $\varphi(3) = 27 = 13 \times 2 + 1 = 1$ et $\varphi(9) = 9^3 = (-4)^3 = 16 \times (-4) = 3 \times (-4) = -12 = 1$, on en déduit que $x \in \ker(\varphi)$. Conclusion : $\ker(\varphi) = \{1,3,9\}$.

Question 4. Montrons que la relation $\sim$ définie par $a \sim b \Leftrightarrow \varphi(a) = \varphi(b)$ est une relation d'équivalence.
Puisque $\varphi(a) = \varphi(a)$ on en déduit que $a \sim a$ et donc la relation est réflexive..
De plus si $a \sim b$ alors $\varphi(a) = \varphi(b)$. Donc $\varphi(b) = \varphi(a)$ et donc $b \sim a$. Le relation est symétrique.
Enfin si $a \sim b$ et $b \sim c$ alors $\varphi(a) = \varphi(b)$ et $\varphi(b) = \varphi(c)$ et donc $\varphi(a) = \varphi(c)$ c'est-à-dire $a \sim c$. La relation est donc transitive.
Tous ces points montrent que la relation $\sim$ est une relation d'équivalence.

Question 5. Procédons par double inclusion. Supposons que a et b fassent partie de la même classe d'équivalence, $a \sim b$. Alors $\varphi(a) = \varphi(b)$. Or $\varphi(a)$ est inversible et même puisque φ est un morphisme, on sait que $\varphi(a)^{-1} = \varphi(a^{-1})$. Donc

$$1 = \varphi(b)\varphi(a^{-1}).$$

En utilisant à nouveau le fait que φ est un morphisme, on obtient

$$\varphi(ba^{-1}) = 1$$

et donc par définition $ba^{-1} \in \ker(\varphi)$. Par la question 3 on en déduit que $ba^{-1} \in \{1, 3, 9\}$ et finalement en remultipliant par a : $b \in \{a, 3a, 9a\}$. Réciproquement, si $b \in \{a, 3a, 9a\}$, alors $\varphi(b) \in \{\varphi(a), \varphi(3a), \varphi(9a)\}$. Or φ est un morphisme. Donc $\varphi(b) \in \{\varphi(a), \varphi(3)\varphi(a), \varphi(9)\varphi(a)\}$. On a déjà vu que $\varphi(3) = \varphi(9) = 1$ (éléments du noyau). Donc $\varphi(b) = \varphi(a)$ et $b \sim a$. Ceci conclut la réciproque et donc $a \sim b$ si et seulement si $b \in \{a, 3a, 9a\}$.
Si $a = 1$ on obtient la première classe d'équivalence $\{1, 3, 9\}$ (le noyau). Si $a = 2$ on obtient $\{2, 6, 5\}$. Si $a = -1 = 12$, on obtient $\{-1, -3, -9\} = \{12, 10, 4\}$. Et si $a = -2 = 11$ on obtient $\{-2, -6, -5\} = \{11, 7, 8\}$. Chaque élément a été listé une fois (et une seule fois les classes d'équivalence partitionnent l'ensemble) et on a les quatre classes d'équivalence $\{1, 3, 9\}$, $\{2, 6, 5\}$, $\{12, 10, 4\}$ et $\{11, 7, 8\}$.

Question 6. Par définition de la relation d'équivalence, tous les éléments d'une même classe d'équivalence on la même image et de plus si deux éléments font partie de classes distinctes alors leurs images sont différentes. On en déduit que φ a exactement 4 images que l'on détermine en calculant l'image d'un représentant de chaque classe :

$$\mathrm{Im}\,(\varphi) = \{\varphi(1), \varphi(2), \varphi(-1), \varphi(-2)\} = \{1, 8, -1, -8\} = \{1, 8, 12, 5\}.$$

Question 7(a). Soient x, y, z entiers tels que $5x^3 + 11y^3 + 13z^3 = 0$. Supposons $y \neq 0$ [13], alors $5x^3 + 11y^3 = 0$ [13] et donc $5x^3 = -11y^3 = 2y^3$ [13]. On commence par noter que $x^3 = 5^{-1} \times 2y^3$ [13] et puisque $y \neq 0$ [13], on sait que $y \in (\mathbb{Z}/13\mathbb{Z})^\times$ et on a donc également $x^3 \in (\mathbb{Z}/13\mathbb{Z})^\times$ et donc

$$x^3 = \varphi(x)\ [13].$$

Maintenant, puisque $y \in (\mathbb{Z}/13\mathbb{Z})^\times$ on a

$$2 = 5x^3y^{-3}\ [13].$$

Or on a vu que $5 = \varphi(-2)$ et que $x^3 = \varphi(x)$ [13]. Donc $2 = \varphi(-2)\varphi(x)\varphi(y^{-1})$. Comme φ est un morphisme, on en déduit que $2 = \varphi(-2xy^{-1}) \in \mathrm{Im}\,(\varphi)$. Ce qui est contradictoire avec la question 6. Donc on en déduit que $y = 0$ [13]. L'équation initiale devient donc dans $\mathbb{Z}/13\mathbb{Z}$,

$$5x^3 = 0\ [13]$$

Puisque 5 est inversible, en composant par 5^{-1} on en déduit que $x^3 = 0$ [13] et donc $x = 0$ [13] (c'est la contraposée de $x \neq 0 \Rightarrow x^3 \neq 0$ vu à la question 1). Donc 13 divise x.

Question 7(b). Puisque x et y sont divisibles par 13, il existe x_1 et $x_2 \in \mathbb{Z}$ tels que $x = 13x_1$ et $y = 13y_1$. Donc l'équation initiale devient

$$5x^3 + 11y^3 + 13z^3 = 13\left(5 \times 13^2x_1^3 + 11 \times 13^2y_1^3 + z^3\right) = 0.$$

Donc $5 \times 13^2x_1^3 + 11 \times 13^2y_1^3 + z^3 = 0$. On en déduit que $z^3 = 0$ [13] et donc (comme précédemment, $\mathbb{Z}/13\mathbb{Z}$ est un corps) $z = 0$ [13] et donc 13 divise z.

Question 7(c). Raisonnons par l'absurde. Soit $(x, y, z) \in \mathbb{Z} \setminus \{(0, 0, 0)\}$ tel que $5x^3 + 11y^3 + 13z^3 = 0$. Par les questions 7(a) et 7(b), on sait que 13 divise x, y et z. Puisque $(x, y, z) \neq (0, 0, 0)$, il existe $k \geqslant 1$ et $(x_1, y_1, z_1) \neq (0, 0, 0)$ tel que $(x, y, z) = (13^kx_1, 13^ky_1, 13^kz_1)$ et k est choisi pour faire en sorte que x_1 ou y_1 ou z_1 ne soit pas divisible par 13 (le $pgcd(x_1, y_1, z_1)$ n'est pas divisible par 13). Or puisque $5x^3 + 11y^3 + 13z^3 = 0$ on voit que $13^{3k}\left(5x_1^3 + 11y_1^3 + 13z_1^3\right) = 0$ et donc (on travaille dans $\mathbb{Z}$) que $5x_1^3 + 11y_1^3 + 13z_1^3 = 0$. De cette façon (x_1, y_1, z_1) est une solution de la même équation. Et donc par les questions 7(a) et 7(b), on en déduit que 13 divise x_1, y_1 et z_1 ce qui est contradictoire avec leur construction. Donc la seule solution entière de $5x_1^3 + 11y_1^3 + 13z_1^3 = 0$ est le triplet $(0, 0, 0)$.