L2 MTH1314 2015-2016

Correction du Devoir Maison n° 1

Solution de l'exercice 1

Vous avez été nombreux à bien écrire l'analyse-synthèse. Voici une rédaction compacte dans laquelle l'unicité est soulignée directement par l'analyse.

Analyse/Unicité. Soit $M \in \mathscr{M}_n(\mathbb{R})$ une matrice fixée. Considérons un couple $(S, A) \in \mathscr{S}_n(\mathbb{R}) \times \mathscr{A}_n(\mathbb{R})$ tel que

$$M = S + A. \tag{1}$$

Cherchons à déterminer les valeurs possibles pour S et A. En prenant la transposée de M, on note que :

$$\begin{aligned} {}^tM &= {}^tS + {}^tA \qquad \text{car la transposée est linéaire,} \\ &= S - A \qquad \text{car } S \text{ est symétrique et } A \text{ antisymétrique.} \end{aligned} \tag{2}$$

Ainsi en faisant $\frac{(1)+(2)}{2}$, respectivement $\frac{(1)-(2)}{2}$, on obtient

$$S = \frac{M + {}^tM}{2} \qquad \text{et} \qquad A = \frac{M - {}^tM}{2}.$$

On remarque donc que S et A sont entièrement déterminées par M. Donc, pour une matrice fixée M, si un couple solution existe, nécessairement il est unique et vaut $(S, A) = (\frac{M+{}^tM}{2}, \frac{M-{}^tM}{2})$.

Synthèse/Existence. Montrons que le couple précédemment déterminé est solution de notre problème. On garde $M \in \mathscr{M}_n(\mathbb{R})$ fixée et on considère le couple $(S, A) = (\frac{M+{}^tM}{2}, \frac{M-{}^tM}{2})$. Montrons que ce couple est une solution.

1. D'abord,
$$S + A = \frac{M + {}^tM}{2} + \frac{M - {}^tM}{2} = M.$$
2. De plus,
$${}^tS = \frac{{}^tM + {}^t({}^tM)}{2} = \frac{{}^tM + M}{2} = S.$$
Donc $S \in \mathscr{S}_n(\mathbb{R})$.
3. Et de même,
$${}^tA = \frac{{}^tM - {}^t({}^tM)}{2} = \frac{{}^tM - M}{2} = -A.$$
Donc $A \in \mathscr{A}_n(\mathbb{R})$.

On a donc prouvé l'existence d'un couple solution.

Conclusion. Pour toute matrice $M \in \mathscr{M}_n(\mathbb{R})$, il existe un unique couple $(S, A) \in \mathscr{S}_n(\mathbb{R}) \times \mathscr{A}_n(\mathbb{R})$ tel que $M = S + A$.

Solution de l'exercice 2

Question 1

Soit g un élément fixé de G. D'après **C1**, on sait qu'il existe $(p, q) \in \mathbb{N}^2$, $0 < p < q$ tel que $g^p = g^q$. Par **C2** et **C3** on sait que l'on peut simplifier à gauche et à droite. En raisonnant avec les mains, si on était dans un groupe, on simplifierait p fois l'expression $g^p = g^q$ et obtiendrait $g^{q-p} = e$,

l'élément neutre. On ne sait pas encore que G est un groupe mais puisque $*$ est une l.c.i., et $q-p \geqslant 1$, l'élément g^{q-p} est dans G et est un bon candidat pour e_g.
On pose $e_g = g^{q-p}$. La notation avec g en indice est pertinente puisque cet élément étant construit à l'aide de g, dépend a priori de g. Montrons que

$$e_g * g = g * e_g = g.$$

Reprenons $g^q = g^p$. Premier cas $p = 1$. Dans ce cas on a $g^q = g$ et $e_g = g^{q-1}$. Donc

$$e_g * g = g^{q-1} * g = g^q = g \qquad \text{et} \qquad g * e_g = g * g^{q-1} = g^q = g.$$

Le résultat est donc démontrer si $p = 1$. Si maintenant $p \geqslant 2$, on a toujours par **C1**,

$$g^{q-1} * g = g^{p-1} * g.$$

Donc par **C3**,

$$g^{q-1} = g^{p-1}.$$

En itérant cette manipulation $p-1$ fois, puisque $q > p-1$, on trouve que

$$g^{q-(p-1)} = g$$

Ainsi

$$g^{q-p} * g = g.$$

Puisque, $\forall n \geqslant 1$, $g^n = g * g * \cdots * g$, on voit que $\forall n, m \geqslant 1$, $g^n * g^m = g^m * g^n = g^{n+m}$ (car la loi $*$ est associative). Donc on a également

$$g * g^{q-p} = g.$$

Finalement, on a bien montré que

$$e_g * g = g * e_g = g.$$

Ceci nous dit que e_g laisse stable l'élément g. Mais UNIQUEMENT g. On n'a certainement pas montré que e_g est l'élément neutre.
Note : On pouvait aller un peu plus vite en écrivant que puisque $g^q = g^p$, on a directement pour $p \geqslant 2$,

$$g^{q-p} * g * g^{p-1} = g * g^{p-1}.$$

Et par **C3** *on conclut que $g^{q-p} * g = g$.*

Question 2

Cette question a été globalement bien traitée. Soit h un autre élément de G. Puisque $g = g * e_g$, on écrit

$$g * h = g * e_g * h.$$

Ainsi grâce à **C2**,

$$h = e_g * h.$$

De même, puisque $g = e_g * g$, on a $h * g = h * e_g * g$ et donc par **C3**, $h = e_g * g$. Finalement e_g laisse stable tous les éléments de G et est donc l'unique élément neutre de G et ne dépend finalement pas de l'élément initial g (cf le cours pour l'unicité d'un élément neutre). On le note désormais e.

Question 3

La loi $*$ est une loi de composition interne associative pour G et par la question 2, e est l'élément neutre de $(G, *)$. Il nous faut donc montrer que tous les éléments sont inversibles. Intuitivement puisque $g^{q-p} = e$, ce qui s'écrit aussi $g^{q-p-1} * g = g * g^{q-p-1} = e$, le bon candidat pour l'inverse serait g^{q-p-1}. Il est formellement interdit d'écrire g^{-1} qui n'a aucun sens, avant d'avoir prouvé que g est inversible.
Soit donc g un élément quelconque de G. Par les questions 1 et 2, on a vu qu'il existe $0 < p < q$ tel que $g^{q-p} = e$. Premier cas $q - p = 1$. Dans ce cas on a $g = e$ donc $g * g = e * e = e$ et naturellement g est son propre inverse qui existe bien. Supposons $q - p > 1$ et posons $g_1 = g^{q-p-1}$. Puisque $q - p - 1 \geqslant 1$, g_1 est bien défini et est un élément de G. Puis, comme $g^{q-p} = e$, on a

$$g_1 * g = g^{q-p-1} * g = g^{q-p} = e.$$

Et de même $g * g_1 = e$. Finalement g est bien inversible d'inverse $g_1 = g^{q-p-1}$.
Conclusion $(G, *)$ est bien un groupe.

Solution de l'exercice 3

Question 1

Beaucoup d'erreurs pour la question 1 alors que vous ne devriez pas vous faire attraper là-dessus. Puisque φ est un morphisme pour $\times$,

$$\varphi(1) = \varphi(1^2) = \varphi(1)\varphi(1) = \varphi(1)^2.$$

Donc

$$\varphi(1)\left(\varphi(1) - 1\right) = 0.$$

Ainsi $\varphi(1) = 0$ ou 1.

Question 2

(a) Par récurrence. Pour tout $n \in \mathbb{N}$, on définit P_n la proposition « $\varphi(n) = n$ ».
Initialisation. Puisque φ est un morphisme pour $+$,

$$\varphi(1) = \varphi(1 + 0) = \varphi(1) + \varphi(0).$$

Donc

$$\varphi(0) = 0,$$

et P_0 est vraie.
J'acceptais aussi le fait de dire que φ est un morphisme de groupe entre $(\mathbb{Q}, +)$ et $(\mathbb{Q}, +)$ et donc l'élément neutre 0 est envoyé sur l'élément neutre 0. Quand un morphisme va d'un groupe G dans ce même groupe G on dit que c'est un endomorphisme.
Hérédité. Soit $n \in \mathbb{N}$. Supposons P_n vraie pour cet entier n. Alors puisque φ est un morphisme pour $+$,

$$\varphi(n + 1) = \varphi(n) + \varphi(1).$$

Puisque $\varphi(1) = 1$ et que P_n est vraie,

$$\varphi(n + 1) = n + 1.$$

Donc P_{n+1} est vraie. Et on a montré que $P_n \Rightarrow P_{n+1}$.
Conclusion. On a donc montré par récurrence que P_n est vraie pour tout $n \in \mathbb{N}$.

(b) On détermine d'abord $\varphi(-1)$. Puisque φ est un morphisme pour $+$,

$$\varphi(0) = \varphi(1-1) = \varphi(1) + \varphi(-1).$$

Puisque par **(a)**, $\varphi(0) = 0$ et $\varphi(1) = 1$, on trouve donc que

$$\varphi(-1) = \varphi(0) - \varphi(1) = -1.$$

Maintenant certains ont démontré par récurrence pour tout $n \in \mathbb{N}$ la proposition Q_n : « $\varphi(-n) = -n$ », ce qui est correct. D'autres ont fait une récurrence décroissante $P_p \Rightarrow P_{p-1}$ pour tout $p \in \mathbb{Z}$. C'est juste mais moins usuel, préférez plutôt l'utilisation de Q_n. Voici enfin une démonstration plus astucieuse. Puisque φ est un morphisme pour $\times$, $\forall n \in \mathbb{N}$,

$$\varphi(-n) = \varphi(-1)\varphi(n) = (-1) \times n = -n, \qquad \text{car par } \textbf{(a)},\ \varphi(n) = n.$$

Ainsi pour tout $p \in \mathbb{Z}^-$, $\varphi(p) = p$. Et par **(a)** on conclut que pour tout $p \in \mathbb{Z}$, $\varphi(p) = p$.
J'aurais accepté également le fait que φ est un morphisme du groupe $(\mathbb{Q}, +)$ dans $(\mathbb{Q}, +)$. Et donc l'image d'un inverse est l'inverse de l'image. Puisque la loi ici est $+$: $\varphi(-n) = -\varphi(n)$ pour tout $n \in \mathbb{Q}$ et on conclut à nouveau en s'aidant de **(a)**.
(c) Commençons par montrer que $\varphi(1/q) = 1/q$ pour tout $q \in \mathbb{Z}^*$. Attention φ n'est pas forcément un morphisme du groupe $(\mathbb{Q}^*, \times)$ car rien ne nous dit que l'image d'un rationnel non nul est forcément non nul (confère question 3). On ne peut pas exploiter directement le cours pour invoquer que l'image d'un inverse est l'inverse de l'image. Mais puisque φ est un morphisme pour $\times$, pour tout $q \in \mathbb{Z}^*$,

$$\varphi(1) = \varphi\left(\frac{q}{q}\right) = \varphi(q)\varphi\left(\frac{1}{q}\right).$$

Or $\varphi(1) = 1$ et par **(b)**, $\varphi(q) = q \neq 0$. Donc,

$$\varphi\left(\frac{1}{q}\right) = \frac{1}{q}.$$

Maintenant soit $r \in \mathbb{Q}$. Il existe $(p, q) \in \mathbb{Z} \times \mathbb{Z}^*$ tel que $r = p/q$. Puisque φ est un morphisme pour $\times$,

$$\varphi(r) = \varphi\left(\frac{p}{q}\right) = \varphi(p)\varphi\left(\frac{1}{q}\right).$$

Par **(b)** et ce qui précède,

$$\varphi(r) = \frac{p}{q} = r.$$

Ce qui conclut la question 2 : $\varphi = \mathrm{Id}_{\mathbb{Q}}$.

Question 3

Si $\varphi(1) = 0$, voici une solution astucieuse qui évite de recommencer tout le travail de la question 2. Pour tout $r \in \mathbb{Q}$, puisque φ est un morphisme pour $\times$,

$$\varphi(r) = \varphi(1 \times r) = \varphi(1) \times \varphi(r) = 0 \times \varphi(r) = 0.$$

Et finalement φ est l'application nulle sur $\mathbb{Q}$.
Note : lorsque que l'on définit un morphisme d'ANNEAUX, ici pour $(\mathbb{Q}, +, \times)$, on impose que les neutres pour chacune des lois vont sur les neutres respectifs. C'est-à-dire que l'on impose $\varphi(0) = 0$ (toujours vrai) et $\varphi(1) = 1$, ce qui n'est pas le cas de cette question. L'application nulle est bien un morphisme pour les deux lois mais n'est pas à proprement parler un morphisme de d'anneaux.