

ALGEBRE¹

Solution succincte

Partiel du 31 mars 2005

durée : 2 heures

1 $F_\phi \neq \emptyset$ car, ϕ étant un morphisme, $\phi(e) = e$ (cours) donc $e \in F_\phi$. Montrons que si $x, y \in F_\phi$ alors $x * y^{-1} \in F_\phi$. Pour cela, il suffit de vérifier que $\phi(x * y^{-1}) = x * y^{-1}$. Or on a

$$\phi(x * y^{-1}) = \phi(x) * [\phi(y)]^{-1} = x * y^{-1},$$

la première égalité par les propriétés des morphismes, la seconde par définition de ϕ .

2

1. G_2 est non vide car $e * e = e \implies e \in G_2$. Supposons $x, y \in G_2$ et montrons $x * y^{-1} \in G_2$. On a

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

la première égalité utilise l'associativité et la commutativité, la seconde la formule sur le symétrique d'un produit, la troisième la définition de G_2 , la dernière les propriétés du neutre. On a bien montré $x * y^{-1} \in G_2$.

2. $G_2 = \{\bar{0}, \bar{2}\}$.

3. (a) $G = \{(\bar{0}, \bar{0}), (\bar{0}, \bar{1}), (\bar{1}, \bar{0}), (\bar{1}, \bar{1})\}$. La table est donnée par

\mp	$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{1})$
$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{1})$
$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{0})$
$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{1})$
$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{0})$

- (b) On voit sur la table (diagonale égale à $(\bar{0}, \bar{0})$) que tous les éléments g de G vérifient $g * g = e$ (puisque $e = (\bar{0}, \bar{0})$) donc $G_2 = G$.

4. Prendre

$$G = \underbrace{\mathbb{Z}/2\mathbb{Z} \times \cdots \times \mathbb{Z}/2\mathbb{Z}}_{n \text{ fois}}.$$

5. Si $g \in G_2$ alors g est d'ordre 1 ou bien g est d'ordre 2. Or l'ordre d'un élément divise toujours le cardinal du groupe qui est ici supposé impair. Il suit qu'il n'y a aucun élément d'ordre 2 dans G par conséquent G_2 est réduit aux éléments d'ordre 1 mais il y a un seul élément d'ordre 1 et c'est le neutre.

6. Appelons Ψ un isomorphisme de G sur G' et considérons ψ la restriction de Ψ à G_2 . Observons d'abord que $g \in G_2 \implies \psi(g) = \Psi(g)$ de sorte que $\psi(g) \circ \psi(g) = \Psi(g) \circ \Psi(g) = \Psi(g * g) = \Psi(e_G) = e_{G'}$ donc $\psi(g) \in G'_2$ de sorte que ψ est une application de G_2 dans G'_2 . Nous montrerons que cette application est un isomorphisme. C'est un morphisme injectif comme restriction à un sous-groupe d'un morphisme injectif. Montrons qu'elle est surjective. Etant donné $g' \in G'_2$ on cherche $g \in G_2$ tel que $\psi(g) = g'$ ou encore $\Psi(g) = g'$.

1. Licence de mathématiques (2-ième année), Université Paul Sabatier (Toulouse III). Année scolaire 2004-2005

On peut prendre $g = \Psi^{-1}(g')$ à condition de s'assurer que le g ainsi proposé se trouve bien dans G_2 . Mais, en utilisant que la réciproque d'un isomorphisme est encore un isomorphisme (cours), on a $\Psi^{-1}(g') * \Psi^{-1}(g') = \Psi^{-1}(g \circ g') = \Psi^{-1}(e_{G'}) = e_G$ qui prouve la propriété recherchée et achève la preuve que ψ est un isomorphisme de G_2 sur G'_2 .

7. Prenons $(G, *) = (\text{Is}(P), \circ)$. Alors G_2 contient toutes les symétries orthogonales. Si G_2 est un groupe, il contient donc le sous-groupe engendré par les symétries à savoir $\text{Is}(P)$ lui-même (cours). C'est impossible car $\text{Is}(P)$ contient des éléments qui ne sont pas d'ordre ≤ 2 par exemple n'importe quelle rotation d'angle différent de 0 et π .

3

1. $H \neq \emptyset$ car $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in H$. Prenant M et N quelconque dans H , nous montrons que $M \cdot N^{-1} \in H$ ce qui prouvera que H est un sous-groupe de $(\mathbf{GL}_2(\mathbb{R}), \cdot)$ (on a trivialement $H \subset \mathbf{GL}_2(\mathbb{R})$). Posant

$$M = \begin{pmatrix} 1 & \beta \\ 0 & \alpha \end{pmatrix} \text{ et } N = \begin{pmatrix} 1 & \beta' \\ 0 & \alpha' \end{pmatrix} \text{ avec } \alpha, \alpha' \in \mathbb{Q}^* \text{ et } \beta, \beta' \in \mathbb{Q},$$

on a

$$M \cdot N^{-1} = \begin{pmatrix} 1 & \beta \\ 0 & \alpha \end{pmatrix} \cdot \frac{1}{\alpha'} \begin{pmatrix} \alpha' & -\beta' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \beta \\ 0 & \alpha \end{pmatrix} \cdot \begin{pmatrix} 1 & \frac{-\beta'}{\alpha'} \\ 0 & \frac{1}{\alpha'} \end{pmatrix} = \begin{pmatrix} 1 & \frac{-\beta' + \beta}{\alpha'} \\ 0 & \frac{\alpha}{\alpha'} \end{pmatrix} \in H$$

car $\alpha/\alpha' \in \mathbb{Q}^*$ et $\frac{-\beta' + \beta}{\alpha'} \in \mathbb{Q}$.

2. (a) On observe d'abord que ϕ prend bien ses valeurs dans H . Ensuite, pour $q, q' \in \mathbb{Q}$ on a

$$\phi(q) \cdot \phi(q') = \begin{pmatrix} 1 & q \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & q' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & q + q' \\ 0 & 1 \end{pmatrix} = \phi(q + q')$$

et cela montre que ϕ est un morphisme. Prouvons l'injectivité.

$$q \in \ker \phi \iff \phi(q) = Id \iff \begin{pmatrix} 1 & q \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \iff q = 0$$

d'où $\ker \phi = \{0\}$ et ϕ est bien injective.

- (b) On a

$$\phi(\mathbb{Q}) = \left\{ \begin{pmatrix} 1 & q \\ 0 & 1 \end{pmatrix} \right\}.$$

Pour montrer que $\phi(\mathbb{Q})$ est un sous-groupe distingué de H , on doit vérifier que pour tout $M \in H$ et tout $\begin{pmatrix} 1 & q \\ 0 & 1 \end{pmatrix} \in \phi(\mathbb{Q})$ on a

$$M^{-1} \cdot \begin{pmatrix} 1 & q \\ 0 & 1 \end{pmatrix} \cdot M \in \phi(\mathbb{Q}).$$

Prenons un M quelconque dans H , $M = \begin{pmatrix} 1 & \beta \\ 0 & \alpha \end{pmatrix}$ et calculons l'expression ci-dessus. On a

$$\begin{pmatrix} 1 & \beta \\ 0 & \alpha \end{pmatrix}^{-1} \cdot \begin{pmatrix} 1 & q \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & \beta \\ 0 & \alpha \end{pmatrix} = \begin{pmatrix} 1 & -\beta/\alpha \\ 0 & 1/\alpha \end{pmatrix} \begin{pmatrix} 1 & \beta + q\alpha \\ 0 & \alpha \end{pmatrix} = \begin{pmatrix} 1 & q\alpha \\ 0 & 1 \end{pmatrix} \in \phi(\mathbb{Q})$$

car $q\alpha \in \mathbb{Q}$ et cela prouve que $\phi(\mathbb{Q})$ est distingué.

3. (a) Puisque ψ est un morphisme injectif, il est un isomorphisme entre \mathbb{Q} et l'ensemble image $\phi(\mathbb{Q})$. On peut donc utiliser $\phi^{-1}(u)$ tant que $u \in \phi(\mathbb{Q})$. Maintenant $\phi(\mathbb{Q})$ étant distingué (on vient de la prouver) on a $M^{-1} \cdot \phi(q) \cdot M \in \phi(\mathbb{Q})$ est l'emploi de ϕ^{-1} est donc légitime. Si $M = \begin{pmatrix} 1 & \beta \\ 0 & \alpha \end{pmatrix}$ alors, en utilisant les calculs déjà effectués, on a

$$\psi_M(q) = \phi^{-1} \left(\begin{pmatrix} 1 & q\alpha \\ 0 & 1 \end{pmatrix} \right) = q\alpha.$$

Maintenant, on vérifie immédiatement que l'application $q \rightarrow q\alpha$ est un automorphisme de $(\mathbb{Q}, +)$ (on a besoin ici de $\alpha \neq 0$).

- (b) On montre que tout automorphisme de $(\mathbb{Q}, +)$ est de la forme $q \rightarrow q\alpha$ avec $\alpha \in \mathbb{Q}^*$ donc de la forme ψ_M avec $M = \begin{pmatrix} 1 & \square \\ 0 & \alpha \end{pmatrix}$ ou \square représente n'importe quel élément de \mathbb{Q} .

Montrons l'affirmation sur les automorphismes de $(\mathbb{Q}, +)$. Nous devons prendre f un automorphisme quelconque de $(\mathbb{Q}, +)$ et montrer qu'il existe $\alpha \in \mathbb{Q}^*$ tel que $f(q) = q\alpha$ pour tout $q \in \mathbb{Q}$. Posons $\alpha = f(1)$ et montrons qu'il convient. D'abord, $\forall n \in \mathbb{N}$, on a $f(n) = f(1 + 1 + \dots + 1) = f(1) + f(1) + \dots + f(1) = nf(1)$. Puis, $0 = f(0) = f(n + (-n)) = f(n) + f(-n)$ donne $f(-n) = -f(n)$ de sorte que $f(m) = mf(1) = m\alpha$ pour tout $m \in \mathbb{Z}$. Enfin si $q = m/n$ avec $m \in \mathbb{Z}$ et $n \in \mathbb{N}$ alors $\alpha = f(1) = f(n \cdot \frac{1}{n}) = nf(1/n) \implies f(1/n) = \alpha/n \implies nf(q) = f(n \cdot q) = f(m) = m\alpha \implies f(q) = q\alpha$. On a nécessairement $\alpha \neq 0$ sans quoi f ne serait pas un automorphisme.
