Feuille d'exercices n° 2

Exercice 1

On dit qu'un élément g d'un groupe G est indéfiniment divisible si pour tout $n \in \mathbb{N}^*$ il existe un élément h de G tel que $h^n = g$.

1. Quels sont les éléments indéfiniment divisibles de $(\mathbb{Q}, +)$? Quels sont les éléments indéfiniment divisibles de $(\mathbb{Q}_+^*, \times)$?
2. Soit $\varphi\colon (\mathbb{Q}, +) \to (\mathbb{Q}_+^*, \times)$ un homomorphisme de groupes.
   Pour tout entier $n > 0$ calculer $\varphi(n)$, puis $\varphi(1/n)$ en fonction de $\varphi(1)$.
3. Montrer que φ est constant.
4. En déduire que $(\mathbb{Q}, +)$ et $(\mathbb{Q}_+^*, \times)$ ne sont pas isomorphes.

Remarque : par contre $(\mathbb{R}, +)$ et $(\mathbb{R}_+^*, \times)$ sont isomorphes ; la fonction $x \mapsto \exp x$ réalise un isomorphisme entre ces deux groupes.

Solution 1

1. Déterminons les éléments indéfiniment divisibles de $(\mathbb{Q}, +)$.
   Soit $x \in \mathbb{Q}$. Cet élément est indéfiniment divisible pour la loi d'addition car pour tout entier naturel n non nul nous avons $n \times \frac{x}{n} = x$. Autrement dit tous les éléments de $\mathbb{Q}$ sont indéfiniment divisibles pour l'addition.

   Déterminons les éléments indéfiniment divisibles de $(\mathbb{Q}_+^*, \times)$.
   Soit $x \in \mathbb{Q}^*$ indéfiniment divisible. Alors pour tout $n \in \mathbb{N}^*$ $x^{1/n}$ existe et appartient à $\mathbb{Q}_+^*$. Il en résulte que $x = 1$.
2. Soit $\varphi\colon (\mathbb{Q}, +) \to (\mathbb{Q}_+^*, \times)$ un homomorphisme de groupes.
   Pour tout entier $n > 0$ calculons $\varphi(n)$, puis $\varphi(1/n)$ en fonction de $\varphi(1)$. Pour tout entier $n > 0$ nous avons
   $$\varphi(n) = \varphi(1 + 1 + \ldots + 1) = \varphi(1)^n.$$
   Pour tout entier $n > 0$ nous avons
   $$\varphi(1) = \varphi\left(n \times \frac{1}{n}\right) = \varphi\left(\frac{1}{n} + \frac{1}{n} + \ldots + \frac{1}{n}\right) = \varphi\left(\frac{1}{n}\right)^n$$
   d'où $\varphi\left(\frac{1}{n}\right) = \varphi(1)^{1/n}$.
3. Montrons que φ est constant.
   Pour tout $n > 0$ il existe $h = \varphi\left(\frac{1}{n}\right)$ tel que $h^n = \varphi(1)$. Ainsi $\varphi(1)$ est indéfiniment divisible pour la multiplication. D'après ce qui précède nous avons donc $\varphi(1) = 1$.

   Ainsi pour tout n, nous avons $\varphi(n) = 1$ et $\varphi\left(\frac{1}{n}\right) = 1$. De plus pour tout rationnel $\frac{p}{q}$ nous avons $\varphi\left(\frac{p}{q}\right) = \left(\varphi\left(\frac{1}{q}\right)\right)^p = 1$. Le morphisme φ est donc constant.
4. Montrons $(\mathbb{Q}, +)$ et $(\mathbb{Q}_+^*, \times)$ ne sont pas isomorphes.
   Raisonnons par l'absurde : supposons qu'il existe un isomorphisme ψ entre $(\mathbb{Q}, +)$ et $(\mathbb{Q}_+^*, \times)$. En particulier ψ est un homomorphisme entre ces deux groupes. D'après ce qui précède ψ est donc constant ce qui n'est pas possible pour un isomorphisme.

Exercice 2

Soit G un groupe. Soient H et K deux sous-groupes de G.

Montrer que $\mathrm{H}\cup\mathrm{K}$ est un sous-groupe de G si et seulement si $\mathrm{H}\subset\mathrm{K}$ ou $\mathrm{K}\subset\mathrm{H}$.

En déduire qu'un groupe n'est jamais la réunion de deux de ses sous-groupes propres.

Solution 2

Soit G un groupe. Soient H et K deux sous-groupes de G.

Montrons que $\mathrm{H}\cup\mathrm{K}$ est un sous-groupe de G si et seulement si $\mathrm{H}\subset\mathrm{K}$ ou $\mathrm{K}\subset\mathrm{H}$.

Si $\mathrm{K}\subset\mathrm{H}$ alors $\mathrm{H}\cup\mathrm{K}=\mathrm{H}$ et $\mathrm{H}\cup\mathrm{K}$ est donc un sous-groupe de G (de même $\mathrm{H}\subset\mathrm{K}$ alors $\mathrm{H}\cup\mathrm{K}=\mathrm{K}$ et $\mathrm{H}\cup\mathrm{K}$ est donc un sous-groupe de G).

Réciproquement si $\mathrm{H}\cup\mathrm{K}$ est un sous-groupe de G et si H n'est pas inclus dans K il existe $h\in\mathrm{H}$ tel que $h\notin\mathrm{K}$, en particulier h n'est pas l'élément neutre. Alors pour tout $k\in\mathrm{K}$ nous avons $hk\in\mathrm{H}\cup\mathrm{K}$ (car $\mathrm{H}\cup\mathrm{K}$ est un sous-groupe de G) ; ainsi pour tout $k\in\mathrm{K}$ nous avons l'alternative : hk appartient à H ou hk appartient à K. Si hk appartient à K, alors puisque K est un sous-groupe de G nous avons $h=(hk)k^{-1}$ appartient à K : contradiction avec l'hypothèse. Par conséquent hk appartient à H ; comme H est un sous-groupe de G nous avons : $k=h^{-1}(hk)$ appartient à H. Il en résulte que $\mathrm{K}\subset\mathrm{H}$.

Montrons qu'un groupe n'est jamais la réunion de deux de ses sous-groupes propres.

Raisonnons par l'absurde : supposons que G soit la réunion de deux de ses sous-groupes propres H et K, *i.e.* $\mathrm{K}\cup\mathrm{H}=\mathrm{G}$; alors

- ◇ ou bien $\mathrm{H}\subset\mathrm{K}$ et $\mathrm{H}\cup\mathrm{K}=\mathrm{G}$ donc $\mathrm{H}\cup\mathrm{K}=\mathrm{G}$ équivaut à $\mathrm{K}=\mathrm{G}$: contradiction avec l'hypothèse K propre ;
- ◇ ou bien $\mathrm{K}\subset\mathrm{H}$ et $\mathrm{H}\cup\mathrm{K}=\mathrm{G}$ donc $\mathrm{H}\cup\mathrm{K}=\mathrm{G}$ équivaut à $\mathrm{H}=\mathrm{G}$: contradiction avec l'hypothèse H propre.

Exercice 3

Soit G un groupe abélien.

Montrer que les éléments d'ordre fini de G forment un sous-groupe de G.

Solution 3

Soit G un groupe abélien. Soit H l'ensemble des éléments d'ordre fini. Puisque G est abélien, si $g\in\mathrm{H}$ et $h\in\mathrm{H}$, alors gh appartient à H ; en effet $(gh)^k=g^kh^k$ et donc l'ordre de gh divise le produit des ordres de g et h.

Soit $g\in\mathrm{H}$. Notons k l'ordre de g et ℓ l'ordre de g^{-1}. D'une part $(g^{-1})^k=e$ donc ℓ divise k. D'autre part $g^\ell=e$ donc k divise ℓ. Finalement $k=\ell$.

L'élément e est d'ordre fini donc dans H.

Ainsi H est un sous-groupe de G.

Exercice 4

Soit G un groupe possédant un seul élément d'ordre 2. Notons le g.

Montrer que g est dans le centre de G.

Solution 4

Soit h un élément quelconque de G. Nous avons

$$(h^{-1}gh)(h^{-1}gh)=h^{-1}g(hh^{-1})gh=h^{-1}g^2h=h^{-1}h=e.$$

Or g est l'unique élément d'ordre 2 de G donc :

- ou bien $h^{-1}gh=e$ soit $g=e$: contradiction ;
- ou bien $h^{-1}gh=g$ soit $gh=hg$.

Il en résulte que g commute avec tous les éléments de G ; c'est-à-dire $g\in Z(\mathrm{G})$.

Exercice 5

Soit p un nombre premier. Montrer qu'à isomorphisme près il y a un seul groupe d'ordre p.

Solution 5

Soit p un nombre premier. Soit G un groupe d'ordre p. Remarquons que G n'est pas réduit à $\{e\}$ puisque $p\geqslant 2$. Soit g un élément de $\mathrm{G}\smallsetminus\{e\}$; il est nécessairement d'ordre p. Le groupe G est donc cyclique. Comme il est d'ordre p, il est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

Exercice 6

1. Déterminer l'ensemble des éléments d'ordre fini de $\mathrm{G} = \mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ (pour $n \in \mathbb{N}^*$).
2. Soit H' l'ensemble des éléments d'ordre infini de G. Considérons $\mathrm{H} = \mathrm{H}' \cup \{e\}$ où e est l'élément neutre de G.

   Montrer que, même si H n'est pas vide, H n'est pas un sous-groupe de G.

Solution 6

1. Les éléments d'ordre fini de $\mathrm{G} = \mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ (pour $n \in \mathbb{N}^*$) sont les couples $(0, x)$.
2. Soit H' l'ensemble des éléments d'ordre infini de G. Considérons $\mathrm{H} = \mathrm{H}' \cup \{(0, [0])\}$, l'élément neutre de G est $(0, [0])$.

   Montrons que, même si H n'est pas vide, H n'est pas un sous-groupe de G. Soient $(1, [0])$ et $(-1, [1])$. Ce sont des éléments de H. Leur somme $(0, [1])$ n'appartient pas à H. Il s'en suit que H n'est pas un sous-groupe de G.

Exercice 7

Soit G un groupe abélien infini. Montrer que l'ensemble T des éléments d'ordre fini de G est un sous-groupe de G.

Si $\mathrm{T} = \{e\}$, on dit que G est sans torsion.

Montrer que G/T est sans torsion.

Solution 7 Notons $o(g)$ l'ordre d'un élément g de G.

Puisque $o(e) = 1$, on a $e \in \mathrm{T}$. Soient x, $y \in \mathrm{T}$ d'ordres k, $m \in \mathbb{N}^*$. On a $(xy)^{km} = (x^k)^m (y^m)^k = e$ donc $xy \in \mathrm{T}$. Comme $o(x) = o(x^{-1})$, on a $x^{-1} \in \mathrm{T}$. Ainsi T est un sous-groupe de G.

Considérons l'application canonique $\varphi\colon \mathrm{G} \to \mathrm{G}/\mathrm{T}$. Soit $a \in \mathrm{G}/\mathrm{T}$ d'ordre fini $s \in \mathbb{N}^*$. Il existe $x \in \mathrm{G}$ tel que $a = \varphi(x)$. On a

$$\varphi(x^s) = a^s = e$$

donc $x^s \in \mathrm{T} = \ker\varphi$. Il existe donc $r \in \mathbb{N}^*$ tel que $x^{sr} = (x^s)^r = e$ ce qui prouve que $x \in \mathrm{T}$ et donc que $a = \varphi(x) = e$. Par suite G/T est sans torsion.

Exercice 8

a) Soit G un sous-groupe de $(\mathbb{R}, +)$ non réduit à $\{0\}$. Montrer que G est ou bien dense dans $\mathbb{R}$, ou bien monogène, *i.e.* de la forme $a\mathbb{Z}$ avec $a > 0$ (donc discret).

b) Soient α et β deux réels non nuls. Discuter de la nature du sous-groupe additif qu'ils engendrent.

c) Soit $\beta \notin \mathbb{Q}$. Montrer que $\mathbb{N}\beta + \mathbb{Z}$ est dense dans $\mathbb{R}$.

d) Soit $\vartheta \notin 2\pi\mathbb{Q}$. Montrer que $\{\exp(\mathbf{i}n\vartheta) \mid n \in \mathbb{N}\}$ est dense dans le cercle unité $\mathbb{S}^1$ de $\mathbb{C}$.

   En déduire

   i) qu'un sous-groupe G de $\mathbb{S}^1$ est soit fini (auquel cas égal au groupe des racines $n$ièmes de l'unité où $n = |\mathrm{G}|$), soit dense dans $\mathbb{S}^1$;

   ii) les valeurs d'adhérence de la suite $(\sin(n))_{n \geqslant 0}$.

Solution 8

a) Soit G un sous-groupe de $(\mathbb{R}, +)$ non réduit à $\{0\}$. Montrons que G est ou bien dense dans $\mathbb{R}$, ou bien monogène, *i.e.* de la forme $a\mathbb{Z}$ avec $a > 0$ (donc discret).

   Si G est monogène, *i.e.* si $\mathrm{G} = a\mathbb{Z}$, avec $a > 0$, alors a est le plus petit élément strictement positif de G. Si G est dense dans $\mathbb{R}$, alors $\mathrm{G} \cap \mathbb{R}_+^*$ n'a pas de plus petit élément mais une borne inférieure non nulle. On introduit donc

$$\mathrm{G}_+ = \mathrm{G} \cap \mathbb{R}_+^* \qquad\qquad a = \inf \mathrm{G}_+$$

   Le réel $a \geqslant 0$ est bien défini car G_+ est non vide et minorée. En effet il existe un élément g dans G non nul donc x ou $-x$ est dans G_+ qui est minoré par 0.

   On va distinguer le cas $a > 0$ du cas $a = 0$.

- $\diamond$ Supposons $a > 0$. Montrons que a appartient à G puis que $\mathrm{G} = a\mathbb{Z}$.
Raisonnons par l'absurde : supposons que a n'appartienne pas à G. Puisque $a > 0$, on a $2a > a$. Il existe g dans G_+ tel que $g < 2a$. Comme a n'appartient pas à G, on a les inégalités $a < g < 2a$. Il existe alors h dans G_+ tel que $h < g$. On a $a < h < g < 2a$ car a n'appartient pas à G. De plus comme g et h appartiennent à G, la différence $g - h$ appartient à G et on a même $g - h$ appartient à G_+. D'une part $a < h$ donc $a - h < 0$ et $2a - h < a$, d'autre part $g < 2a$ donc $g - h < 2a - h$. Par conséquent $g - h < a$: contradiction avec la définition de a. Par suite a appartient à G. Ainsi le groupe $a\mathbb{Z}$ engendré par a est inclus dans G.
Réciproquement soit g un élément de G. Posons $k = E\left(\frac{g}{a}\right) \in \mathbb{Z}$. Puisque G est un groupe le réel $g - ak$ appartient à G. Comme $k \leqslant \frac{g}{a} < k + 1$ on a $0 \leqslant g - ak < a = \min \mathrm{G}_+$. Nécessairement $g - ak = 0$ et $g = ak \in a\mathbb{Z}$. Il en résulte que $\mathrm{G} = a\mathbb{Z}$.
- $\diamond$ Supposons que $a = 0$. Montrons qu'alors G est dense dans $\mathbb{R}$, autrement dit que G rencontre tout intervalle ouvert de $\mathbb{R}$. Soit $I =]\alpha, \beta[$ un intervalle ouvert de $\mathbb{R}$. Comme $a = 0$ il existe $g \in \mathrm{G}$ tel que $0 < g < \beta - \alpha$. Le sous-groupe $g\mathbb{Z}$ engendré par g est inclus dans G et intersecte I (sinon il existerait $k \in \mathbb{Z}$ tel que $I \subset]kg, (k + 1)g[$ ce qui contredirait l'inégalité $g < \beta - \alpha$). Il s'en suit que G est dense dans $\mathbb{R}$.

b) Il s'agit d'étudier le groupe $\mathrm{G} = \alpha\mathbb{Z} + \beta\mathbb{Z} \neq \{0\}$.
Supposons qu'il existe $a > 0$ tel que $\mathrm{G} = a\mathbb{Z}$. Puisque α et β appartiennent à G, il existe k et ℓ dans $\mathbb{Z}$ tels que $\alpha = ka$ et $\beta = \ell a$. Le rapport $\frac{\alpha}{\beta}$ s'écrit aussi $\frac{k}{\ell}$ et appartient à $\mathbb{Q}$.

Réciproquement supposons que $\frac{\alpha}{\beta}$ soit rationnel. Écrivons $\frac{\alpha}{\beta}$ sous la forme $\frac{k}{\ell}$ avec k et ℓ premiers entre eux. Alors
$$\alpha\mathbb{Z} + \beta\mathbb{Z} = \beta\left(\frac{k}{\ell}\mathbb{Z} + \mathbb{Z}\right) = \frac{\beta}{\ell}(k\mathbb{Z} + \ell\mathbb{Z}) = \frac{\beta}{\ell}\mathbb{Z}$$
car k et ℓ sont premiers entre eux.
Ainsi si $\frac{\alpha}{\beta}$ appartient à $\mathbb{Q}$, alors G est monogène et sinon G est dense dans $\mathbb{R}$.

c) Soit $\beta \notin \mathbb{Q}$. Montrons que $\mathbb{N}\beta + \mathbb{Z}$ est dense dans $\mathbb{R}$.
Le sous-groupe additif $\mathrm{G} = \mathbb{Z} + \beta\mathbb{Z}$ de $\mathbb{R}$ est dense d'après b). Montrons que l'ensemble $\mathbb{N}\beta + \mathbb{Z}$ reste encore dense. Soient $a < b$ deux réels. Nous pouvons trouver un élément $x = v\beta + u \in \mathrm{G}$ tel que $0 < x < b - a$.
- $\diamond$ Supposons que v soit un entier naturel, *i.e.* que x appartienne à $\mathbb{N}\beta + \mathbb{Z}$. Choisissons un entier $n_0 < a$. Les éléments de la suite $(kx + n_0)_{k \geqslant 0}$ appartiennent à $\mathbb{N}\beta + \mathbb{Z}$ et un argument analogue à celui de a) assure que l'un d'eux au moins appartient à $]a, b[$.
- $\diamond$ Supposons que $v < 0$. Alors $-x$ appartient à $\mathbb{N}\beta + \mathbb{Z}$ et $-(b - a) < -x < 0$. Choisissons $n_0 \in \mathbb{Z}$ avec $n_0 > b$. Alors au moins un élément de la suite $(n_0 - kx)_{k \geqslant 0}$ appartient à $]a, b[$.

d) Soit $\vartheta \notin 2\pi\mathbb{Q}$. Montrons que $\{\exp(\mathbf{i}n\vartheta) \,|\, n \in \mathbb{N}\}$ est dense dans le cercle unité $\mathbb{S}^1$ de $\mathbb{C}$.
Posons $\Omega = \left\{\exp(\mathbf{i}n\vartheta) \,|\, n \in \mathbb{N}\right\}$. Il s'agit de l'image par l'application $f\colon x \mapsto \exp(2\mathbf{i}\pi x)$ de l'ensemble $\mathbb{Z} + \frac{\vartheta}{2\pi}\mathbb{N}$. Puisque f est continue et que Ω est dense dans $\mathbb{R}$ d'après c) l'image $f(\Omega)$ de Ω par f est dense dans $f(\mathbb{R}) = \mathbb{S}^1$.
   i) D'après a) un sous-groupe G de $\mathbb{S}^1$ est soit fini (auquel cas égal au groupe des racines $n$ièmes de l'unité où $n = |\mathrm{G}|$), soit dense dans $\mathbb{S}^1$.
   ii) Si $\vartheta = 1$, alors $\frac{1}{\pi}$ n'est pas rationnel et l'ensemble $\left\{\exp(\mathbf{i}n) \,|\, n \in \mathbb{N}\right\}$ est dense dans $\mathbb{S}^1$. Puisque l'application qui à un nombre complexe associe sa partie imaginaire est continue, l'ensemble $\left\{\sin(n) \,|\, n \in \mathbb{N}\right\}$ est dense dans $[-1, 1]$. Pour tout $-1 \leqslant a \leqslant 1$, pour tout $\varepsilon > 0$ et pour tout $N \in \mathbb{N}$ nous sommes alors assurés de trouver un entier $n \geqslant N$ tel que $|\sin(n) - a| \leqslant \varepsilon$. Autrement dit tout réel de $[-1, 1]$ est une valeur d'adhérence de la suite $(\sin(n))_{n \geqslant 0}$. L'autre inclusion est directe. Finalement l'ensemble des valeurs d'adhérences de la suite $(\sin(n))_{n \geqslant 0}$ est le segment $[-1, 1]$.

Exercice 9 Soit $p > 2$ un nombre premier. Soit G un groupe non abélien d'ordre $2p$.
(1) Montrer qu'il existe x, y dans G avec x d'ordre 2, y d'ordre p et $\mathrm{G} = \langle x, y\rangle$.
(2) Montrer que $xyx = y^i$ pour un certain $2 \leqslant i \leqslant p - 1$, puis montrer que $i^2 \equiv 1 \bmod p$, et en déduire que $i = p - 1$.
(3) Montrer que G est isomorphe au groupe diédral D_{2p}.

Solution 9

(1) Le fait qu'il existe $x \in \mathrm{G}$ d'ordre 2 et $y \in \mathrm{G}$ d'ordre p découle du théorème de CAUCHY. Comme $\langle x\rangle \subsetneq \langle x, y\rangle$ et $\langle y\rangle \subsetneq \langle x, y\rangle$ par LAGRANGE l'ordre du sous-groupe $\langle x, y\rangle \subset \mathrm{G}$ est un multiple strict de 2 et de p, et un diviseur de $2p$. Il s'en suit que cet ordre est égal à $2p$, et donc $\langle x, y\rangle = \mathrm{G}$.

(2) Le groupe $\langle y\rangle$ est d'indice 2 dans G, donc est distingué dans G. Par suite $xyx^{-1} = xyx \in \langle y\rangle$ ce qui revient à dire qu'il existe $1 \leqslant i \leqslant p-1$ tel que $xyx = y^i$. Enfin $i \neq 1$, car sinon x et y commutent, et comme ils engendrent G le groupe G serait abélien, en contradiction avec l'hypothèse. Puisque $x^2 = 1$, on a

$$y = x^2yx^2 = x(xyx)x = xy^ix = (xyx)^i = (y^i)^i = y^{i^2},$$

d'où $i^2 \equiv 1 \bmod p$ puisque y est d'ordre p. L'équation $x^2 = 1$ a deux solutions sur le corps ${}^{\mathbb{Z}}\!/\!_{p\mathbb{Z}}$: $x = \overline{1}$ et $x = -\overline{1}$. Mais comme on a $i \geqslant 2$, on en déduit que $\overline{i} = -\overline{1}$ et $i = p-1$.

(3) Le groupe diédral D_{2p} est engendré par une rotation r d'ordre p et une symétrie axiale s : on peut prendre r la rotation d'angle $\frac{2\pi}{p}$ et s la symétrie par rapport à l'axe des abscisses. On a alors

$$\mathrm{D}_{2p} = \{\mathrm{id},\, s,\, r,\, rs,\, r^2,\, r^2s,\, \ldots,\, r^{p-1},\, r^{p-1}s\}$$

et la loi de groupe sur D_{2p} se déduit des relations $s^2 = \mathrm{id}$, $r^p = \mathrm{id}$ et $srs = r^{-1}$. Par les questions précédentes, tout groupe G non abélien d'ordre $2p$ peut s'écrire $\mathrm{G} = \{\mathrm{id},\, x,\, y,\, yx,\, y^2,\, y^2x,\, \ldots,\, y^{p-1},\, y^{p-1}x\}$ avec $x^2 = \mathrm{id}$, $y^p = \mathrm{id}$ et $xyx = y^{-1}$. On en déduit que G est isomorphe à D_{2p} via l'isomorphisme qui envoie x sur s et y sur r.

Exercice 10

Notons $\mathrm{T} \subset \mathrm{GL}\left(3, {}^{\mathbb{Z}}\!/\!_{3\mathbb{Z}}\right)$ le sous-groupe des matrices de la forme

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$$

avec a, b et c dans ${}^{\mathbb{Z}}\!/\!_{3\mathbb{Z}}$.

(1) Montrer que tout élément non trivial de T est d'ordre 3.

(2) Le groupe T est-il isomorphe à ${}^{\mathbb{Z}}\!/\!_{3\mathbb{Z}} \times {}^{\mathbb{Z}}\!/\!_{3\mathbb{Z}} \times {}^{\mathbb{Z}}\!/\!_{3\mathbb{Z}}$?

(3) En quoi cet exemple est-il intéressant ?

Solution 10

(1) On peut utiliser le fait que sur n'importe quel corps $\Bbbk$, toute matrice de la forme

$$N = \begin{pmatrix} 0 & a & b \\ 0 & 0 & c \\ 0 & 0 & 0 \end{pmatrix}$$

est nilpotente d'indice 3, c'est-à-dire $N^3 = 0$ (plutôt que de le vérifier en faisant le produit matriciel, on peut juste constater que les vecteurs e_1, e_2 et e_3 de la base satisfont

$$N(e_1) = 0, \qquad N^2(e_2) = N(ae_1) = 0 \qquad \text{et} \qquad N^3(e_3) = N^2(be_1 + ce_2) = 0.$$

Donc une matrice de la forme $\mathrm{id} + N$ vérifie

$$(\mathrm{id} + N)^3 = \mathrm{id} + 3N + 3N^2.$$

Si maintenant le corps est de caractéristique 3 (comme ici ${}^{\mathbb{Z}}\!/\!_{3\mathbb{Z}}$), alors $(\mathrm{id}+N)^3 = \mathrm{id}$ et donc tout élément non trivial de T est d'ordre 3.

(2) Le groupe T n'est pas isomorphe à ${}^{\mathbb{Z}}\!/\!_{3\mathbb{Z}} \times {}^{\mathbb{Z}}\!/\!_{3\mathbb{Z}} \times {}^{\mathbb{Z}}\!/\!_{3\mathbb{Z}}$ car T n'est pas abélien. En effet par exemple :

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

(3) Cet exercice permet de réaliser que le raisonnement suivant n'est pas correct :
« Montrons que $\mathcal{S}_3$ et $\mathrm{Isom}(T)$, où T est un triangle, sont isomorphes. Le groupe $\mathcal{S}_3$ contient le neutre, trois éléments d'ordre 2 (les transpositions) et deux éléments d'ordre 3 (les 3-cycles). De même, $\mathrm{Isom}(T)$ contient le neutre, trois éléments d'ordre 2 (les symétries axiales) et deux rotations d'ordre 3. Comme ces groupes ont des éléments deux à deux du même ordre ils sont isomorphes. »