Feuille d'exercices n° 2

Exercice 1

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 1

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 $\mathrm{K} \subset \mathrm{H}$ (resp. $\mathrm{H} \subset \mathrm{K}$) alors $\mathrm{H} \cup \mathrm{K} = \mathrm{H}$ (resp. $\mathrm{H} \cup \mathrm{K} = \mathrm{K}$) 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 ; alors l'un est inclus dans l'autre d'après ce qui précède et dans ce cas le plus gros est G : contradiction avec le fait que les sous-groupes soient propres.

Exercice 2

Soit G un groupe abélien fini d'ordre k. Soit n un entier premier avec k. Montrer que pour tout élément g de G il existe un élément h de G tel que $g = h^n$.

(Indication : considérer l'application $\varphi\colon \mathrm{G} \to \mathrm{G}$ définie par $\varphi(h) = h^n$ et montrer que φ est un isomorphisme de G.)

Solution 2

Soit G un groupe abélien fini d'ordre k. Soit n un entier premier avec k. Considérons l'application $\varphi\colon \mathrm{G} \to \mathrm{G}$ définie par $\varphi(g) = g^n$.

Montrons que φ est un isomorphisme.

Tout d'abord c'est un morphisme ; en effet G est abélien donc $(gh)^n = g^n h^n$, *i.e.* $\varphi(gh) = \varphi(g)\varphi(h)$.

Le noyau $\ker\varphi$ de φ est constitué des éléments g de G tels que $g^n = 1$. Donc non seulement n est premier avec k mais n est divisible par l'ordre de g qui divise k. Par suite $n = 1$ ou $g = 1$. Pour $n > 1$ nécessairement $\ker\varphi = \{1\}$. Il en résulte que φ est une injection d'un ensemble fini dans lui-même, c'est donc un morphisme bijectif de groupes et donc un isomorphisme.

Il s'en suit que φ est surjective, *i.e.* pour tout élément g de G il existe $h \in \mathrm{G}$ tel que $\varphi(h) = g$ soit tel que $h^n = g$.

Exercice 3

Montrer de la façon la plus élémentaire possible que tout groupe d'ordre 4 est abélien (Indication : utiliser le théorème de Lagrange).

Solution 3

Soit G un groupe d'ordre 4.

D'après le théorème de Lagrange tout élément non trivial de G est d'ordre 2 ou 4.

Si G admet un élément d'ordre 4, alors il est cyclique donc abélien (car isomorphe à $\mathbb{Z}/4\mathbb{Z}$).

Supposons que $\mathrm{G} \setminus \{1\}$ est constitué d'éléments d'ordre 2. Montrons que G est abélien. Soient a et b dans G.

- ◇ Si $ab = 1$, alors $a^{-1} = b$ et
  - ou bien $a = 1$ et $a^{-1} = b$ conduit à $b = 1$ auquel cas a et b commutent ;
  - ou bien $a \neq 1$, alors a est, par hypothèse, d'ordre 2 ; par suite $a = a^{-1}$ et $a^{-1} = b$ se réecrit $a = b$ auquel cas a et b commutent.
- ◇ Sinon ab est un élément de $\mathrm{G} \setminus \{1\}$ donc lui aussi d'ordre 2, *i.e.* $(ab)^2 = 1$ soit $abab = 1$ ou encore $ab = b^{-1}a^{-1}$. Mais $a = a^{-1}$ (que a soit 1 ou d'ordre 2) et $b = b^{-1}$ (que b soit 1 ou d'ordre 2 ; par conséquent $ab = b^{-1}a^{-1}$ se réécrit $ab = ba$: les éléments a et b commutent.

Exercice 4

1. Montrer qu'une matrice carrée d'ordre 2 à coefficients dans $\mathbb{Z}$ est dans $\mathrm{GL}(2, \mathbb{Z})$ si et seulement si elle a pour déterminant 1 ou -1.
2. Posons $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$. Déterminer l'ordre de A, l'ordre de B, l'ordre de AB.

Solution 4

1. Montrons qu'une matrice carrée d'ordre 2 à coefficients dans $\mathbb{Z}$ est dans $\mathrm{GL}(2, \mathbb{Z})$ si et seulement si elle a pour déterminant 1 ou -1.
   Le déterminant d'une matrice à coefficients entiers est entier. Soit A une telle matrice qu'on suppose inversible et telle que son inverse soit aussi à coefficients entiers.
   Nous avons $\det(AA^{-1}) = \det A(\det A)^{-1} = 1$. Par suite $\det A$ est inversible dans $\mathbb{Z}$ et est égal à ± 1.
   Réciproquement soit A une matrice carrée de taille $n \times n$ à coefficients dans $\mathbb{Z}$ de déterminant égal à ± 1. En tant que matrice à coefficients réels A est inversible et son inverse a pour coefficients les quotients des mineurs de taille $(n-1) \times (n-1)$ et de $\det A = \pm 1$. Ces mineurs sont des entiers, donc ces quotients sont des entiers et l'inverse de A est à coefficients dans $\mathbb{Z}$.
2. Posons $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$. L'ordre de A est 4, l'ordre de B est 3, l'ordre de $AB = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ est infini car $(AB)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$.

Exercice 5

Montrer que $\mathbb{Z} \times \mathbb{Z}$ n'est pas monogène.

Solution 5 Raisonnons par l'absurde. Supposons que $\mathbb{Z} \times \mathbb{Z}$ est monogène, *i.e.* $\mathbb{Z} \times \mathbb{Z} = \langle (x, y) \rangle$. Notons que nécessairement $xy \neq 0$. Remarquons que $\langle (x, y) \rangle = \big\{ (kx, ky) \,|\, k \in \mathbb{Z} \big\}$, en particulier $(x, 2y)$ n'appartient pas à $\langle (x, y) \rangle$ mais $(x, 2y)$ appartient à $\mathbb{Z} \times \mathbb{Z}$: contradiction.

Exercice 6

Montrer que $\mathbb{Z}$ et $\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ne sont pas isomorphes.

Solution 6

Montrer que $\mathbb{Z}$ et $\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ne sont pas isomorphes. Le groupe $\mathbb{Z}$ ne contient aucun élément d'ordre 2 alors que $(0, 1)$ est un élément d'ordre 2 de $\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Par conséquent ces deux groupes ne sont pas isomorphes.

Exercice 7

Montrer qu'un groupe est fini si et seulement si il n'a qu'un nombre fini de sous-groupes.

Solution 7

Soit G un groupe fini. L'ensemble des sous-groupes de G est un sous-ensemble de l'ensemble des parties de G qui est de cardinal fini. Ainsi G ne contient qu'un nombre fini de sous-groupes.

Réciproquement soit G un groupe ne possédant qu'un nombre fini de sous-groupes. Nous avons

$$\mathrm{G} = \bigcup_{g \in \mathrm{G}} \langle g \rangle.$$

Les sous-groupes de la forme $\langle g\rangle$, qui sont les sous-groupes monogènes, sont en nombre fini. En fixant dans chacun d'eux un générateur nous les écrivons $\langle g_1\rangle$, $\langle g_2\rangle$, …, $\langle g_k\rangle$ de sorte que

$$\mathrm{G} = \bigcup_{i=1}^{k} \langle g_i\rangle.$$

Si l'un des $\langle g_i\rangle$ est infini, il est isomorphe à $\mathbb{Z}$ et contient de ce fait une infinité de sous-groupes : contradiction avec l'hypothèse « G contient un nombre fini de sous-groupes ». Ainsi tous les sous-groupes $\langle g_i\rangle$, $i = 1, 2, \ldots, k$, sont d'ordre fini. Leur réunion est donc de cardinal fini mais cette réunion est G. Par conséquent G est un groupe fini.

Exercice 8

Donner un exemple de groupe et de sous-groupes dont la réunion n'est pas un sous-groupe.

Solution 8

Dans $\mathbb{Z}$ la réunion des sous-groupes $2\mathbb{Z}$ et $3\mathbb{Z}$ n'est pas un groupe. En effet la somme $2+3=5$ d'un élément de $2\mathbb{Z}$ et d'un élément de $3\mathbb{Z}$ n'est ni multiple de 2, ni multiple de 3.

Exercice 9

Dans les groupes suivants, donner un exemple d'élément d'ordre 4 s'il en existe, sinon donner un argument pour justifier qu'il n'y en a pas :

(a) le groupe linéaire $\mathrm{GL}(2,\mathbb{R})$;
(b) le groupe alterné $\mathcal{A}_8$;
(c) le groupe $\mathrm{Isom}^+(T) \subset \mathrm{SO}(3,\mathbb{R})$ des rotations de $\mathbb{R}^3$ préservant un tétraèdre régulier T ;
(d) un groupe d'ordre 16 quelconque (attention il s'agit de déterminer si *tout* sous-groupe d'ordre 16 admet un élément d'ordre 4).

Solution 9

(a) La rotation d'angle $\frac{\pi}{2}$ est un exemple d'élément d'ordre 4 dans $\mathrm{GL}(2,\mathbb{R})$, sa matrice est $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.
(b) $(1\,2\,3\,4)(5\,6)$ est un exemple d'élément d'ordre 4 dans $\mathcal{A}_8$.
(c) Le groupe $\mathrm{Isom}^+(T) \subset \mathrm{SO}(3,\mathbb{R})$ ne contient pas d'élément d'ordre 4. Il contient douze éléments dont huit d'ordre 3, trois d'ordre 2 et l'identité.
Autre justification possible : $\mathrm{Isom}^+(T) \subset \mathrm{SO}(3,\mathbb{R})$ est isomorphe à $\mathcal{A}_4$ et $\mathcal{A}_4$ ne contient pas d'élément d'ordre 4 (les 4-cycles ne sont pas de signature 1).
(d) Le groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ est un groupe d'ordre 16 qui contient le neutre d'ordre 1 et des éléments d'ordre 2.

Exercice 10

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 10

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 $a = 0$.

- ◇ 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 $\mathrm{G} = a\mathbb{Z}$.
- ◇ 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 $0 < x < b - a$.

- ◇ 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 $]a, b[$.
- ◇ 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 $f : x \mapsto \exp(2\mathbf{i}\pi x)$ 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 11

Montrer que si $n \geqslant 2$, le seul sous-groupe fini de $(\mathbb{C}^*, \cdot)$ de cardinal n est μ_n [1].

Solution 11

1. μ_n désigne le groupe des racines $n$ième de l'unité.

Soit G un sous-groupe fini de $(\mathbb{C}^*, \cdot)$ de cardinal n. Soit g un élément de G. L'ordre de g divise n ; en particulier $g^n = \mathrm{id}$. Il en résulte que $\mathrm{G} \subset \mu_n$.

De plus $|\mathrm{G}| = |\mu_n|$.

Il en résulte que $\mathrm{G} = \mu_n$.

Exercice 12 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 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 12

(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 [2]. 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 $xyx = y^i$ (notons que si $i = 0$, alors $xyx = y^0$ se réecrit $xyx^{-1} = \mathrm{id}$, soit $y = \mathrm{id}$: contradiction avec y d'ordre p). 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 $i^2 = 1 \bmod p$ 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 13

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 13

(1) On peut utiliser le fait que sur n'importe quel corps $\Bbbk$, toute matrice de la forme
$$N = \begin{pmatrix} 0 & a & b \\ 0 & 0 & c \\ 0 & 0 & 0 \end{pmatrix}$$

2. Le théorème de Cauchy sur les groupes finis dit que si G est un groupe fini d'ordre n alors pour tout entier p divisant n il existe un élément de G d'ordre p, autrement dit il existe un sous-groupe de G d'ordre p.

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. »