DEVOIR n° 2

Exercice 1

1. Soit G un groupe tel que ${}^{\mathrm{G}}\!/\!_{Z(\mathrm{G})}$ est cyclique. Le groupe G est-il abélien ? Justifier.
2. Soit G un groupe tel que ${}^{\mathrm{G}}\!/\!_{Z(\mathrm{G})}$ est abélien. Le groupe G est-il abélien ? Justifier.
3. Montrer que la probabilité que deux éléments d'un groupe fini non abélien commutent est $\leqslant \frac{5}{8}$ (indication : on pourra utiliser 1.).

Solution 1

1. Soit G un groupe tel que ${}^{\mathrm{G}}\!/\!_{Z(\mathrm{G})}$ est cyclique. Le groupe G est abélien. En effet le groupe ${}^{\mathrm{G}}\!/\!_{Z(\mathrm{G})}$ étant cyclique il existe $\overline{a} \in {}^{\mathrm{G}}\!/\!_{Z(\mathrm{G})}$ tel que ${}^{\mathrm{G}}\!/\!_{Z(\mathrm{G})} = \langle \overline{a} \rangle$. Tout élément de G est alors de la forme $a^m z$ avec m dans $\mathbb{N}$ et z dans $Z(\mathrm{G})$. Soient g, h deux éléments de G ; alors g (resp. h) s'écrit $a^m z_1$ (resp. $a^p z_2$) avec m (resp. p) dans $\mathbb{N}$ et z_1 (resp. z_2) dans $Z(\mathrm{G})$. En particulier
$$\begin{array}{rcll} gh & = & (a^m z_1)(a^p z_2) & \\ & = & a^m z_1 a^p z_2 & \\ & = & a^m a^p z_1 z_2 & \text{car } z_1 \text{ appartient à } Z(\mathrm{G}) \\ & = & a^m a^p z_2 z_1 & \text{car } z_1 \text{ appartient à } Z(\mathrm{G}) \\ & = & a^{m+p} z_2 z_1 & \\ & = & a^{p+m} z_2 z_1 & \\ & = & a^p a^m z_2 z_1 & \\ & = & a^p z_2 a^m z_1 & \text{car } z_2 \text{ appartient à } Z(\mathrm{G}) \\ & = & (a^p z_2)(a^m z_1) & \\ & = & hg & \end{array}$$
2. Soit G un groupe tel que ${}^{\mathrm{G}}\!/\!_{Z(\mathrm{G})}$ est abélien. Le groupe G n'est pas nécessairement abélien, considérer par exemple $\mathrm{G} = \mathbb{H}_8$.
3. Montrer que la probabilité que deux éléments d'un groupe fini non abélien commutent est $\leqslant \frac{5}{8}$ (indication : on pourra utiliser 1.).
   Soit G un groupe fini non abélien. Désignons par n l'ordre de G et par z l'ordre de $Z(\mathrm{G})$. Puisque G n'est pas abĺien le 1. assure que ${}^{\mathrm{G}}\!/\!_{Z(\mathrm{G})}$ ne peut pas ˆetre cyclique et est donc d'ordre au moins 4. Ainsi $n \geqslant 4z$.
   Soit $x \in Z(\mathrm{G})$; par définition du centre x commute avec tout élément y de G. Soit $x \in \mathrm{G} \smallsetminus Z(\mathrm{G})$; les éléments y de G qui commutent avec x sont les éléments du centralisateur de x pour l'action par conjugaison. Nous obtenons alors un sous-groupe strict de G (car x n'est pas central) d'ordre $\leqslant \frac{n}{2}$. Nous obtenons finalement que le nombre de couples $(x, y) \in \mathrm{G} \times \mathrm{G}$ qui commutent vérifie
$$\leqslant zn + (n - z)\frac{n}{2} = \frac{zn}{2} + \frac{n^2}{2} \leqslant \frac{n^2}{8} + \frac{n^2}{2} = \frac{5}{8}n^2.$$
   Il reste à diviser par $|\mathrm{G} \times \mathrm{G}| = n^2$ pour obtenir que la probabilité est $\leqslant \frac{5}{8}$.

Exercice 2

Les groupes
$$\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/90\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z} \qquad\qquad \mathbb{Z}/100\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$$

sont-ils isomorphes ? Justifier votre réponse.

Solution 2

D'une part $12 = 2^2 \times 3$, $90 = 2 \times 3^2 \times 5$ et $25 = 5^2$ donc

$$\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/90\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z} \simeq \mathbb{Z}/\mathbb{Z} \times \mathbb{Z}/\mathbb{Z} \times \mathbb{Z}/\mathbb{Z} \times \mathbb{Z}/\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5^2\mathbb{Z};$$

d'autre part $100 = 2^2 \times 5^2$, $30 = 2 \times 3 \times 5$ et $9 = 3^2$ donc

$$\mathbb{Z}/100\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3^2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5^2\mathbb{Z}.$$

En particulier les groupes

$$\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/90\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z} \qquad\qquad \mathbb{Z}/100\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$$

sont isomorphes.

Exercice 3

Montrer qu'un p-groupe d'ordre p^n possède des sous-groupes d'ordre p^i pour tout $0 \leqslant i \leqslant n$ (indication : raisonner par récurrence).

Solution 3 Raisonnons par récurrence sur n.

- Pour $n = 0$ c'est évident.
- Supposons que tout p-groupe d'ordre p^n possède des sous-groupes d'ordre p^i pour tout $0 \leqslant i \leqslant n$. Soit G un groupe d'ordre p^{n+1} ; montrons que G possède des sous-groupes d'ordre p^i pour tout $0 \leqslant i \leqslant n+1$. Si $i = 0$, il n'y a rien à faire ; on peut donc supposer que $i \geqslant 1$. Alors $Z(\mathrm{G})$ est un sous-groupe non trivial de G ; en tant que p-groupe $Z(\mathrm{G})$ admet un élément d'ordre p et donc un sous-groupe H d'ordre p. Comme H est central, il est distingué. Notons $\pi\colon \mathrm{G} \to \mathrm{G}/\mathrm{H}$ la surjection canonique. Le groupe G/H est d'ordre p^n donc d'après l'hypothèse de récurrence possède pour tout $1 \leqslant i \leqslant n+1$ un sous-groupe K_i d'ordre p^{i-1}. Alors $\pi^{-1}(\mathrm{K}_i)$ est un sous-groupe de G d'ordre p^i pour tout $1 \leqslant i \leqslant n+1$.

Exercice 4

Montrer qu'un groupe abélien fini non cyclique possède un sous-groupe isomorphe à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ pour un certain nombre premier p.

Solution 4

Soit G un groupe abélien fini non cyclique. Le théorème de structure des groupes abéliens finis assure que

$$\mathrm{G} \simeq \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \ldots \times \mathbb{Z}/d_r\mathbb{Z}$$

pour un certain $r \in \mathbb{N}$, $d_i \geqslant 2$ pour $1 \leqslant i \leqslant r$ et $d_i \,|\, d_{i+1}$ pour $1 \leqslant i \leqslant r-1$.

Puisque G n'est pas cyclique nous avons $r \geqslant 2$ et si p est un diviseur premier de d_1, alors p est un diviseur premier de d_i pour tout $1 \leqslant i \leqslant r$. Ainsi $\mathbb{Z}/p\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}/d_i\mathbb{Z}$ pour tout $1 \leqslant i \leqslant r$. On obtient ainsi un sous-groupe de G isomorphe à $\left(\mathbb{Z}/p\mathbb{Z}\right)^r$ qui contient évidemment une copie de $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Exercice 5

Considérons le groupe $\mathrm{G} = \mathrm{GL}\left(2, \mathbb{Z}/2\mathbb{Z}\right)$ des matrices inversibles de taille 2×2 à coefficients dans $\mathbb{Z}/2\mathbb{Z}$.

1. Déterminer l'ordre de G.
2. Déterminer les classes de conjugaison de G.
3. Déterminer les centralisateurs des éléments de G (on rappelle que le centralisateur d'un élément g de G est $Z_g = \{h \in \mathrm{G} \,|\, hg = gh\}$).
4. Déterminer les sous-groupes de G.
5. Déterminer les sous-groupes de Sylow de G.
6. Déterminer les sous-groupes distingués de G.
7. Déterminer le centre de G.
8. Déterminer le groupe dérivé de G.

Solution 5 Posons $\Bbbk = \mathbb{F}_2$. Soient E le $\Bbbk$-espace vectoriel canonique $\Bbbk^2$ et $\mathcal{C} = (e_1, e_2)$ sa base canonique.

1. Le groupe G est d'ordre 6 et ses éléments sont

$$\text{id}, \quad S_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad S_2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad S_3 = {}^{\mathrm{t}}S_2, \quad R = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \quad R^2 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix},$$

2. Déterminons les classes de conjugaison de G.
   On vérifie sans difficulté que S_1, S_2, S_3 sont d'ordre 2 et R, R^{-1} sont d'ordre 3.
   Soit r l'endomorphisme canoniquement associé à R et soit $u = (1,1) \in E$. Alors $(u, r(u)) = (e_1 + e_2, e_2)$ est une base de E et la matrice de r dans cette base est $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = R^{-1}$. Ainsi R et R^{-1} sont semblables et forment une classe de conjugaison.
   La même méthode montre que S_1 et S_2 sont semblables et par suite que $\{S_1, S_2, S_3\}$ est une classe de conjugaison
   On remarque que la trace d'une matrice non scalaire caractérise sa classe de conjugaison.
3. Déterminons les centralisateurs des éléments de G.
   Le centralisateur de R ou R^{-1} est d'ordre $\frac{|\mathrm{G}|}{2} = 3$; puisqu'il contient $\langle R \rangle$ qui est d'ordre 3 il s'agit de $\langle R \rangle$.
   Le centralisateur d'un élément S de la classe de conjugaison $\{S_1, S_2, S_3\}$ est d'ordre $\frac{|\mathrm{G}|}{3} = 2$, il s'agit donc de $\langle S \rangle$.
4. Déterminons les sous-groupes de G.
   Les sous-groupes non triviaux de G sont $\langle S_1 \rangle$, $\langle S_2 \rangle$, $\langle S_3 \rangle$, et $\langle R \rangle = \langle R^{-1} \rangle$.
5. Déterminons les sous-groupes de Sylow de G.
   Notons que $|\mathrm{G}| = 2 \times 3$; par suite nous nous intéressons aux 2-Sylow et aux 3-Sylow de G.
   Les 2-Sylow de G sont $\langle S_1 \rangle$, $\langle S_2 \rangle$, $\langle S_3 \rangle$.
   Le groupe G possède un unique 3-Sylow : $\langle R \rangle = \langle R^{-1} \rangle$.
6. Déterminons les sous-groupes distingués de G.
   Puisque $\langle R \rangle$ est l'unique 3-Sylow de G, il est distingué dans G.
   Les 2-Sylow étant au nombre de 3, ils ne sont pas distingués dans G.
   Par suite G contient un unique sous-groupe distingué non trivial : $\langle R \rangle$.
7. Déterminons le centre de G.
   Le centre de G est le groupe des matrices scalaires, ici réduit à $\{\text{id}\}$.
8. Enfin $D(\mathrm{G}) = \langle R \rangle$ car ${}^{\mathrm{G}}\!/_{\langle R \rangle}$ est abélien sans que G le soit.

Remarque. Le groupe G est isomorphe à $\mathcal{S}_3$.

Exercice 6

Considérons le groupe alterné $\mathcal{A}_4$. Rappelons que $D(\mathcal{A}_4)$ désigne son groupe dérivé. Soit $\mathcal{K}$ le sous-groupe de $\mathcal{A}_4$ constitué de l'identité et des doubles transpositions.

1. Montrer que $\mathcal{K}$ est un sous-groupe distingué de $\mathcal{A}_4$.
2. Montrer que $D(\mathcal{A}_4)$ est contenu dans $\mathcal{K}$ (indication : ${}^{\mathcal{A}_4}\!/_{\mathcal{K}}$ est d'ordre 3).
3. Montrer que $D(\mathcal{A}_4)$ n'est pas trivial.
4. Montrer que $\mathcal{A}_4$ ne possède pas de sous-groupe distingué d'ordre 2.
5. En déduire que $D(\mathcal{A}_4) = \mathcal{K}$.

Solution 6

1. Montrons que $\mathcal{K} \triangleleft \mathcal{A}_4$.
   Si on conjugue la double transposition $(a\ b)(c\ d)$ par une permutation σ nous obtenons $(\sigma(a)\ \sigma(b))(\sigma(c)\ \sigma(d))$ ce qui montre que $\mathcal{K}$ est distingué dans $\mathcal{S}_4$ donc a fortiori dans $\mathcal{A}_4$.
2. Montrons que $D(\mathcal{A}_4) \subset \mathcal{K}$.
   Comme ${}^{\mathcal{A}_4}\!/_{\mathcal{K}}$ est d'ordre $\frac{12}{4} = 3$, il est cyclique d'ordre 3 (car 3 est premier) et en particulier abélien ce qui montre que $D(\mathcal{A}_4) \subset \mathcal{K}$.

3. Montrons que $D(\mathcal{A}_4) \neq \{1\}$.

   Le groupe $\mathcal{A}_4$ n'est pas abélien donc $D(\mathcal{A}_4) \neq \{1\}$.

4. Montrons que $\mathcal{A}_4$ ne possède pas de sous-groupe distingué d'ordre 2.

   Soit H un sous-groupe d'ordre 2 de $\mathcal{A}_4$. Il est composé de l'identité et d'une double transposition $\tau = (a\ b)(c\ d)$. Si on conjugue τ par $\sigma \in \mathcal{A}_4$, nous obtenons $(\sigma(a)\ \sigma(b))(\sigma(c)\ \sigma(d))$ qui n'appartient pas à H si on choisit par exemple $\sigma \in \mathcal{A}_4$ tel que $\sigma(a) = a$ et $\sigma(b) = c$ ce qui est toujours possible.

5. Montrons que $D(\mathcal{A}_4) = \mathcal{K}$.

   Nous avons vu que $D(\mathcal{A}_4) \subset \mathcal{K}$ donc l'ordre de $D(\mathcal{A}_4)$ divise 4. Mais nous avons aussi vu que $D(\mathcal{A}_4)$ n'est d'ordre ni 1, ni 2. Il en résulte que $D(\mathcal{A}_4)$ est d'ordre 4 et que $D(\mathcal{A}_4) = \mathcal{K}$.