Université de Bordeaux

Licence 3 - année 2022-2023
Structures algébriques 2 - 4TMFF502U

Corrigé du devoir maison n°1

Exercice

Soit p un nombre premier. Le but de cet exercice est de redémontrer que tout groupe fini possède un p-Sylow. On n'utilisera donc pas ce résultat.

Soit G un groupe fini d'ordre $n = p^a m$ avec $a \in \mathbf{N}_{>0}$ et $\mathsf{pgcd}(m, p) = 1$.

(1) Montrer que pour tout $i \in \{0, \dots, p^a - 1\}$, on a $v_p\big(\frac{p^a m - i}{p^a - i}\big) = 0$ (où $v_p(x)$ désigne la valuation p-adique de $x \in \mathbf{Q}^\times$). En déduire que l'entier $\binom{p^a m}{p^a}$ est premier avec p.

(2) Montrer que l'action de G sur lui-même par translation à gauche induit une action de G sur l'ensemble X des parties de cardinal p^a de G.

(3) Montrer qu'il existe $P \in X$ telle que $\#\,\mathsf{stab}_G(P)$ soit divisible par p^a.

(4) Soit $x \in P$. Montrer que $\{gx\}_{g \in \mathsf{stab}_G(P)} \subset P$. En déduire que $\mathsf{stab}_G(P)$ est un p-Sylow de G.

Solution : (1) C'est trivial si $i = 0$: supposons $1 \leq i < p^a$. Écrivons $i = p^b m'$ avec $p \nmid m'$: on a $0 \leq b < a$ car $0 < i < p^a$. Comme $a - b > 0$ et $p \nmid m'$, on a $p \nmid p^{a-b} m - m'$ et $p \nmid p^{a-b} - m'$, *i.e.* $v_p(p^{a-b} m - m') = v_p(p^{a-b} - m') = 0$, de sorte que $v_p\big(\frac{p^a m - i}{p^a - i}\big) = v_p\big(\frac{p^{a-b} m - m'}{p^{a-b} - m'}\big) = 0$.

On a $\binom{p^a m}{p^a} = \prod_{i=0}^{p^a - 1} \frac{p^a m - i}{p^a - i}$: ce qui précède montre donc que $v_p\big(\binom{p^a m}{p^a}\big) = 0$, *i.e.* que $\binom{p^a m}{p^a}$ est premier avec p.

(2) Si $g \in G$, l'application $x \mapsto gx$ est une bijection de G dans lui-même (attention, *ce n'est pas* un automorphisme lorque $g \neq e$...) : si $A \in X$, on a $\#gA = \#A$, où $gA = \{ga\}_{a \in A}$. L'application $G \times X \to X$ qui envoie (g, A) sur gA est donc bien définie. On a bien sûr $eA = A$ et $g(hA) = ghA = (gh)A$ pour sous $g, h \in G$ et $A \in X$. Cela montre que l'application définie ci-dessus (induite par l'action de G sur lui-même par translation à gauche) est une action du groupe G sur X.

(3) Soit $\{A_1, \dots, A_r\}$ un système complet de représentants des orbites de X pour l'action qui précède : l'équation aux classes s'écrit $\#X = \sum_{k=1}^{r} \#\,\mathsf{orb}(A_k)$. Comme p ne divise pas $\#X = \binom{p^a m}{p^a}$ en vertu de la question (1), il existe $k \in \{1, \dots, r\}$ tel que $p \nmid \#\,\mathsf{orb}(A_k)$. Posons $P = A_k$: on a $p^a m = \#G = \#\,\mathsf{orb}(P) \#\,\mathsf{stab}(P)$, comme $\mathsf{pgcd}(p, \#\,\mathsf{orb}(P)) = 1$, le lemme de Gauss implique que $p^a \mid \#\,\mathsf{stab}(P)$.

(4) Si $g \in \mathsf{stab}(P)$, on a $gx \in gP = P$, donc $\{gx\}_{g \in \mathsf{stab}(P)} \subset P$. Avec $x = e$, cela montre que $\mathsf{stab}(P) \subset P$, et donc $\#\,\mathsf{stab}(P) \leq \#P = p^a$. Comme $p^a \mid \#\,\mathsf{stab}(P)$ d'après la question précédente, on a nécessairement $\#\,\mathsf{stab}(P) = p^a$ *i.e.* $\mathsf{stab}(P)$ est un p-Sylow de G.

Remarque. Cela montre en fait que l'inclusion $\mathsf{stab}(P) \subset P$ est une égalité, et donc que le P trouvé dans la question (3) est un p-Sylow de G.

Problème

Dans tout ce qui suit, G désigne un groupe fini et Z son centre.
(1) Montrer que le groupe G/Z ne peut pas être cyclique d'ordre > 1.
(2) Soient p un nombre premier et G un p-groupe d'ordre > 1. Montrer que Z n'est pas réduit à l'élément neutre.
(3) En déduire qu'à isomorphisme près, les seuls groupes d'ordre p^2 sont $\mathbf{Z}/p^2\,\mathbf{Z}$ et $(\mathbf{Z}/p\,\mathbf{Z})^2$.

Le but du reste de l'exercice est de classifier les groupes d'ordre 8 à isomorphisme près. On suppose donc désormais que G est d'ordre 8.

(4) Dans cette question, on suppose G abélien.
(a) On suppose que G n'est pas cyclique, mais qu'il contient un élément g_0 d'ordre 4 : on pose $H = \langle g_0 \rangle$. Notons $f\colon G \to G$ l'application définie par $f(g) = g^2$ et posons $C = \mathsf{Ker}(f)$. Montrer que $f(G) \subset C$, en déduire que $\#C > 2$, puis que C n'est pas inclus dans H.
(b) Sous les hypothèses du (a), on choisit $g \in C \setminus H$: montrer qu'alors $H \times \langle g \rangle \xrightarrow{\sim} G$.
(c) En déduire qu'en général (*i.e.* en supposant G seulement abélien), G est isomorphe à $\mathbf{Z}/8\,\mathbf{Z}$, $(\mathbf{Z}/4\,\mathbf{Z}) \times (\mathbf{Z}/2\,\mathbf{Z})$ ou $(\mathbf{Z}/2\,\mathbf{Z})^3$.

On suppose désormais que G n'est *pas* abélien.

(5) Expliquer pourquoi G ne contient pas d'élément d'ordre 8, mais au moins un élément d'ordre 4.

On dispose donc d'un sous-groupe $C \leq G$ cyclique d'ordre 4.

(6) Dans cette question on suppose que $G \setminus C$ contient un élément s d'ordre 2. Expliquer pourquoi G est le produit semi-direct de C et $\langle s \rangle$. En déduire que G est isomorphe au groupe diédral D_8.

On suppose désormais que les éléments de $G \setminus C$ sont tous d'ordre 4.

(7) Montrer que $\#Z = 2$, puis que $G/Z \simeq (\mathbf{Z}/2\,\mathbf{Z})^2$.

Écrivons $Z = \{\pm 1\}$ et choisissons $i, j \in G$ dont les images dans G/Z forment une base de G/Z sur $\mathbf{Z}/2\,\mathbf{Z}$. On pose $k = ij$.

(8) Expliquer pourquoi i, j et k sont d'ordre 4. En déduire que $i^2 = j^2 = k^2 = -1$, puis que $ji = -ij$.

Ce qui précède montre que G est isomorphe au groupe quaternionique Q_8 : le sous-groupe de $\mathsf{SL}_2(\mathbf{C})$ engendré par $\left(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right)$ et $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. Finalement, on a montré qu'à isomorphisme près, il y a cinq groupes d'ordre 8.

(9) Auquel de ces cinq groupes le sous-groupe $T \leq \mathsf{GL}_3(\mathbf{Z}/2\,\mathbf{Z})$ constitué des matrices triangulaires supérieures est-il isomorphe ?
(10) Le groupe quaternionique Q_8 peut-il s'écrire de façon non triviale comme un produit semi-direct ?

Solution : Dans tout ce qui suit, on note e l'élément neutre de G.

(1) Supposons G/Z cyclique : il existe $g \in G$ tel que $G/Z = \langle \overline{g} \rangle$, *i.e.* tout élément de G peut s'écrire $g^r z$ avec $r \in \mathbf{Z}$ et $z \in Z$. Si $x = g^r z$ et $y = g^s z'$ sont des élément de G, on a $xy = g^r z g^s z' = g^{r+s} z z'$ car $z \in Z$ et $yx = g^s z' g^r z = g^{s+r} z' z$ car $z' \in Z$. On a donc $xy = yx$ et G est commutatif, *i.e.* $Z = G$. Cela contredit l'hypothèse $(G : Z) > 1$.

(2) L'équation aux classes pour l'action de G sur lui-même par conjugaison donne $\#G \equiv \#Z \mod p\,\mathbf{Z}$ (car G est un p-groupe), et donc $p \mid \#Z$. Comme $e \in Z$, on a $\#Z \geq p$ et Z n'est pas réduit à l'élément neutre.

(3) D'après la question (2), on $\#Z \in \{p, p^2\}$. Si on avait $(G : Z) = p$, alors G/Z serait cyclique (tout groupe d'ordre premier est cyclique), contredisant la question (1) : cela montre que $\#Z = p^2$, *i.e.* $Z = G$. Le groupe G est donc abélien. Si G contient un élément d'ordre p^2, alors $G \simeq \mathbf{Z}/p^2\mathbf{Z}$. Sinon, les éléments sont tous d'ordre divisant p. Le groupe G est donc en fait un $\mathbf{Z}/p\mathbf{Z}$-espace vectoriel, nécessairement de dimension 2 *i.e.* $G \simeq (\mathbf{Z}/p\mathbf{Z})^2$. À isomorphisme près, il n'y a donc que deux groupes d'ordre p^2, ce sont $\mathbf{Z}/p^2\mathbf{Z}$ et $(\mathbf{Z}/p\mathbf{Z})^2$.

(4) (a) Par hypothèse, G ne contient pas d'élément d'ordre 8 : on a $f^2(g) = g^4 = e$ pour tout $g \in G$. En particulier, on a $\mathsf{Im}(f) \subset \mathsf{Ker}(f) = C$. Comme f induit un isomorphisme $G/C \xrightarrow{\sim} \mathsf{Im}(f)$, on a $8 = \#G = \#C\#\,\mathsf{Im}(f) \leq \#C^2$, et donc $2 < \#C$. Comme H est cyclique d'ordre 4, il contient un unique élément d'ordre 2 (c'est g_0^2), donc $\#(C \cap H) = 2$, d'où $C \not\subset H$.
(b) Comme G est abélien, l'application

$$\begin{aligned} \varphi\colon H \times \langle g\rangle &\to G \\ (u, v) &\mapsto uv \end{aligned}$$

est un morphisme de groupes. Si $(u, v) \in \mathsf{Ker}(\varphi)$, alors $u = v^{-1} \in H \cap \langle g\rangle = \{e\}$, donc $(u, v) = (e, e)$, ce qui montre que φ est un injectif : par cardinalité, c'est un isomorphisme. En particulier, on a $G \simeq (\mathbf{Z}/4\mathbf{Z}) \times (\mathbf{Z}/2\mathbf{Z})$ vu que $H \simeq \mathbf{Z}/4\mathbf{Z}$ et $\langle g\rangle \simeq \mathbf{Z}/2\mathbf{Z}$.
(c) Si G contient un élément d'ordre 8, alors G est cyclique, et $G \simeq \mathbf{Z}/8\mathbf{Z}$. Si G n'est pas cyclique mais contient un élément d'ordre 4, on vient de voir que $G \simeq (\mathbf{Z}/4\mathbf{Z}) \times (\mathbf{Z}/2\mathbf{Z})$. Le dernier cas à considérer est celui où G ne contient aucun élément d'ordre 4 : tous ses éléments sont d'ordre divisant 2. Cela implique que G est naturellement muni d'une structure de $\mathbf{Z}/2\mathbf{Z}$-espace vectoriel, nécessairement de dimension 3, et $G \simeq (\mathbf{Z}/2\mathbf{Z})^3$.

(5) Si G contenait un élément d'ordre 8, il serait cyclique donc abélien ce qui n'est pas. De même, s'il ne contenait pas d'élément d'ordre 4, ses élément auraient tous un ordre divisant 2 : il serait isomorphe à $(\mathbf{Z}/2\mathbf{Z})^3$, contredisant là encore la non commutativité de G.

(6) Comme $(G : C) = 2$, le sous-groupe C est distingué dans G. Par ailleurs, on a $s \notin C$, donc $C \cap \langle s\rangle = \{e\}$ (parce que $\langle s\rangle = \{e, s\}$ vu que s est d'ordre 2). Comme $\#C\#\langle s\rangle = 8 = \#G$, cela implique que $G = C \rtimes \langle s\rangle$. Soit r un générateur de C : c'est un élément d'ordre 4. Il en est de même de son conjugué $srs \in C$: on a $srs \in \{r, r^3\}$. Si on avait $srs = r$, on aurait $sr = rs$ et s commuterait aux éléments de C : le produit serait direct et G serait commutatif, contrairement à l'hypothèse. Cela montre que $srs = r^3$, ce qui implique que G est isomorphe au groupe diédral d'ordre 8.

(7) D'après la question (2), on sait que $\#Z \neq 1$ et $\#Z \neq 8$ par hypothèse : on a $\#Z \in \{2, 4\}$. Si on avait $\#Z = 4$, on aurait $(G : Z) = 2$ et le quotient G/Z serait cyclique d'ordre 2, contredisant la question (1). On a donc nécessairement $\#Z = 2$. Le groupe G/Z est donc d'ordre 4. D'après la question (3), il est isomorphe à $(\mathbf{Z}/2\mathbf{Z})^2$ ou à $\mathbf{Z}/4\mathbf{Z}$. Cette dernière possibilité est exclue en vertu de la question (1).

(8) Le groupe C contient 2 éléments d'ordre 4 et $G \setminus C$ fournit 4 éléments d'ordre 4 : cela montre que G contient 6 éléments d'ordre 4. Il en résulte qu'il y a un seul élément d'ordre 2, c'est $-1 \in Z$. Comme $i \notin Z$, cela implique que i est d'ordre 4, et i^2 d'ordre 2, et donc $i^2 = -1$. De même, j et k sont d'ordre 4, et $j^2 = k^2 = -1$. Comme $k^2 = -1$, on a $ijij = -1 = j^2$, donc $iji = j$ et $ji = -ij$ en multipliant par $-i$ à gauche.

Remarque. Si p est un nombre premier quelconque, on a une classification analogue des groupes d'ordre p^3.

(9) Le groupe T n'est pas abélien. En outre, les matrices $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ sont d'ordre 2 : comme le groupe quaternionique n'a qu'un sul élément d'ordre 2, on a nécessairement $T \simeq D_8$.

Remarque. Autre approche (ne faisant pas appel ła classification qu'on a obtenue) : soit $\rho\colon \mathfrak{S}_4 \to \mathsf{GL}_4(\mathbf{Z}/2\,\mathbf{Z})$ le morphisme qui envoie une permutation sur la matrice de permutation associée (cela revient à faire agir $\mathfrak{S}_4$ linéairement sur $(\mathbf{Z}/2\,\mathbf{Z})^4$ par permutation des vecteurs de base). Notons $H \subset (\mathbf{Z}/2\,\mathbf{Z})^4$ l'hyperplan d'équation $x_1 + x_2 + x_3 + x_4 = 0$. Il est stable par les éléments de $\mathsf{Im}(\rho)$: en considérant la restriction à H, on en déduit un morphisme de groupes $\widetilde{\rho}\colon \mathfrak{S}_4 \to \mathsf{GL}(H) \simeq \mathsf{GL}_3(\mathbf{Z}/2\,\mathbf{Z})$. Si $\sigma \in \mathsf{Ker}(\widetilde{\rho})$, alors σ fixe tous les vecteurs somme de deux vecteurs de la base canonique, donc toutes les parties à deux éléments de $\{1,2,3,4\}$: on a $\sigma = \mathsf{Id}$, ce qui prouve que $\widetilde{\rho}$ est injective. Soit $S = \langle (1,2,3,4), (1,2)(3,4) \rangle \subset \mathfrak{S}_4$: on a $S \simeq D_8$. Alors $\widetilde{\rho}(S)$ est un sous-groupe d'ordre 8, donc un 2-Sylow de $\mathsf{GL}_3(\mathbf{Z}/2\,\mathbf{Z})$, tout comme T. Comme les 2-Sylow de $\mathsf{GL}_3(\mathbf{Z}/2\,\mathbf{Z})$ sont conjugués, cela implique que T est lui aussi isomorphe à D_8.

(10) Supposons que le groupe quaternionique s'écrit de façon non triviale comme un produit semi-direct : c'est nécessairement d'un sous-groupe d'ordre 4 (donc abélien) et d'un sous-groupe d'ordre 2. Comme -1 est l'unique élément d'ordre 2, l'un des deux sous-groupes est Z. Mézalor le produit est direct, impliquant que Q_8 est abélien, ce qui n'est pas. Finalement, Q_9 ne peut pas s'écrire de façon non triviale comme un produit semi-direct.