Théorie des Groupes et Géométrie

UNIVERSITÉ DE RENNES 1

Contrôle Continu n°1
Une heure
Correction

Il n'était pas nécessaire de faire l'intégralité du contrôle pour avoir la note maximale.
Tous les documents étaient interdits.

Questions de cours **4pts**

Soit p un nombre premier.

1. Rappeler la définition d'un p-groupe. 1pt

Un p-groupe est un groupe de cardinal p^α avec $\alpha \in \mathbb{N}^*$.

2. Rappeler la définition du centre d'un groupe. 1pt

Le centre d'un groupe G est l'ensemble des éléments qui commutent avec tous les éléments de G, c'est-à-dire $Z(G) \coloneqq \{x \in G : \forall y \in G, xy = yx\}$.

3. Montrer que le centre d'un p-groupe est non trivial. *Indication* : on pourra faire agir le groupe sur lui-même par conjugaison. 2pts

Soit G un p-groupe. On fait agit G sur lui-même par conjugaison. Pour tout $x \in G$, on remarque que l'orbite $G \cdot x = \{yxy^{-1} : y \in G\}$ de x est de taille 1 si et seulement si $x \in Z(G)$. La formule des classes donne donc

$$\#G = \#Z(G) + \sum_{\substack{x \in G\backslash G \\ \#(G\cdot x)>1}} \#(G \cdot x). \tag{1}$$

Maintenant, par la relation orbite-stabilisateur on sait que le cardinal de chaque orbite divise le cardinal du groupe, i.e. $\#(G \cdot x) \mid \#G$. Puisque $\#G = p^\alpha$ avec $\alpha \in \mathbb{N}^\times$, on en déduit que si $\#(G \cdot x) > 1$ alors $p \mid \#(G \cdot x)$. On déduit ainsi de (1) que $p \mid \#Z(G)$. On a donc $\#Z(G) \geqslant p$ (on a $\#Z(G) > 0$ car $1 \in Z(G)$) et en particulier $Z(G)$ n'est pas trivial.

Exercice 1 **7pts**

Soit G un groupe d'ordre 56. Le but de cet exercice est de montrer que G est résoluble non-simple. On commence par montrer que G n'est pas simple. Raisonnons par l'absurde et supposons que G est simple.

1. Compter le nombre d'éléments de G d'ordre 7. 2pt

On a $56 = 8 \cdot 7 = 2^3 \cdot 7$. Le nombre n_7 de 7-Sylows de G vérifie donc $n_7 \equiv 1 \pmod 7$ et $n_7 \mid 8$, d'où $n_7 \in \{1, 8\}$. Si on avait $n_7 = 1$ alors G possèderait un unique 7-Sylow, qui serait donc distingué, ce qui est impossible puisque G est simple (un 7-Sylow étant non trivial et non égal à G tout entier puisque G n'est pas un 7-groupe). On a donc $\boldsymbol{n_7 = 8}$. Finalement, si S et S' sont deux 7-Sylows, on a $\#S = 7$ (c'est bien la plus grande puissance de 7 divisant $\#G$) donc puisque $S \cap S'$ est un sous-groupe de S et que 7 est premier, *par le théorème de Lagrange on en déduit que $S \cap S' = \{1\}$ ou S. Ainsi, deux 7-Sylow distincts se rencontrent seulement en l'identité. On en conclut que chaque 7-Sylow est composé de l'identité et de 6 éléments qui ne sont dans aucun autre 7-Sylow, ces 6 éléments étant tous d'ordre 7 par le théorème de Lagrange. On en déduit que G possède exactement $6 \cdot n_7 = 6 \cdot 8 = 48$ éléments d'ordre 7 (il n'y en a pas plus car chaque élément d'ordre p est dans un p-Sylow).*

2. Toujours en comptant le nombre d'éléments, en déduire que G possède un unique 2-Sylow. 1pt

D'après la question précédente, les éléments des (ou du) 2-Sylow(s) de G sont dans un ensemble à $56 - 48 = 8$ éléments. Il y a donc la place juste pour un seul 2-Sylow (ils sont de cardinal $2^3 = 8$), donc $n_2 = 1$.

(On peut être plus précis : le nombre n_2 de 2-Sylows de G vérifie $n_2 \equiv 1 \pmod 2$ et $n_2 \mid 7$ d'où $n_2 \in \{1, 7\}$. Supposons que $n_2 = 7$ et soient S et S' deux 2-Sylows distincts. On a $\#(S \cap S') \leq 4$ donc chaque 2-Sylow possède au moins $8 - 4 = 4$ éléments qui lui sont propres (un 2-Sylow étant de cardinal $2^3 = 8$). On obtient donc $4 \cdot n_2 = 28$ éléments différents. Ces éléments n'étant dans aucun 7-Sylow, c'est absurde puisque $28 > 8$. On a donc $n_2 = 1$.)

3. Conclure à la non-simplicité de G. 2pt

Par la question précédente, le groupe G possède un unique 2-Sylow, qui est donc distingué. Ce 2-Sylow étant de cardinal $8 < 56 = \#G$, c'est un sous-groupe de G strict non trivial et distingué donc G n'est pas simple. Cela contredit l'hypothèse de symplicité de G. Ainsi, l'hypothèse est absurde et donc G n'est pas simple.

4. Montrer que tout groupe d'ordre 56 est résoluble. 2pt

Soit G un groupe d'ordre 56. Comme précédemment, par les théorèmes de Sylow on obtient $n_7 \in \{1, 8\}$ et $n_2 \in \{1, 7\}$. En comptant comme avant le nombre d'éléments[1]*, on trouve que le cas $n_7 = 8$ et $n_2 = 7$ est impossible. On est donc dans un des cas suivants (non nécessairement disjoints), où l'on rappelle la propriété suivante : un groupe H est résoluble si et seulement s'il possède un sous-groupe distingué H avec H et G/H résolubles.*

Cas 1 : $n_7 = 1$. *Le groupe G possède un unique 7-Sylow S, qui est donc distingué. De plus, le groupe quotient G/S est un 2-groupe (de cardinal 2^3). Ainsi, les groupes S et G/S sont des p-groupes, donc résolubles, donc G est résoluble.*

Cas 2 : $n_2 = 1$. *Même raisonnement où cette fois S est l'unique 2-Sylow de G et G/S est un 7-groupe.*

(On rappelle que le fait qu'un p-groupe est résoluble peut se montrer à partir de la propriété rappelée ci-avant et du fait que le centre d'un p-groupe est non trivial (cf. question 3 des Questions de cours).)

Exercice 2 **2pts**

Soit G un groupe dans lequel tout élément est d'ordre au plus 2. Montrer que G est abélien.
Pour tout $g \in G$ on a $g^2 = 1$ donc $g^{-1} = g$. Ainsi, pour tous $x, y \in G$ on a

$$\begin{aligned} xy &= x^{-1}y^{-1} \\ &= (yx)^{-1} \\ &= yx, \end{aligned}$$

finalement G est abélien.

1. Il faut faire attention ici car avant le groupe G était supposé simple.

Exercice 3 **10pts**

Le but de cet exercice est de classifier les groupes d'ordre 8.

1. Lister les groupes abéliens d'ordre 8. 2pts

Par le théorème de structure, tout groupe abélien d'ordre 8 *est isomorphe à une somme directe*

$$\bigoplus_{i=1}^{n} \mathbb{Z}/d_i\mathbb{Z},$$

où $n \in \mathbb{N}^*$ *et* $d_i \in \mathbb{N}_{\geqslant 2}$ *avec* $d_1 \mid \cdots \mid d_n$. *On a nécessairement* $8 = d_1 \cdots d_n$, *ainsi* $d_i \mid 8$ *donc* $d_i \in \{2, 4, 8\}$. *On a ainsi* $n \leq 3$ *et les différentes possibilités sont les suivantes.*

Cas 1 : $n = 3$. *L'unique possibilité est* $d_1 = d_2 = d_3 = 2$, *et on obtient* $(\mathbb{Z}/2\mathbb{Z})^3$.

Cas 2 : $n = 2$. *Puisque* 8 *n'est pas un carré le cas* $d_1 = d_2$ *est impossible, donc* $d_1 < d_2$. *On a ainsi* $d_1 = 2$ *puis* $d_2 = 4$, *et on obtient donc* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

Cas 3 : $n = 1$. *On a* $d_1 = 8$ *et on obtient* $\mathbb{Z}/8\mathbb{Z}$.

Finalement, il y a exactement trois groupes abéliens d'ordre 8 *à isomorphisme près :* $(\mathbb{Z}/2\mathbb{Z})^3, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ *et* $\mathbb{Z}/8\mathbb{Z}$.

Soit G un groupe non abélien d'ordre 8.

2. Montrer que G possède un élément r d'ordre 4 et aucun élément d'ordre 8. *Indication* : on pourra utiliser le résultat de l'Exercice 2. 2pts

Si G *possède un élément d'ordre* 8 *alors* G *est cyclique, ce qui contredit l'hypothèse sur* G. *Ainsi,* ***le groupe*** G ***ne possède aucun élément d'ordre*** 8. *Par l'Exercice 2, puisque* G *n'est pas abélien il existe un élément* $r \in G$ *qui n'est pas d'ordre* 2. *Par le théorème de Lagrange, l'ordre de* r *est donc* 4 *ou* 8, *mais ce dernier cas est exclus par ce qui précède donc* r *est d'ordre* 4.

3. Montrer que $\langle r \rangle$ est distingué dans G. 1pt

Le sous-groupe $\langle r \rangle$ *est d'indice* 2 *dans* G *donc est distingué.*

4. Soit $s \in G \setminus \langle r \rangle$.

a. Montrer que $srs^{-1} \in \{r, r^{-1}\}$. 1pt

L'élément srs^{-1} *a le même ordre que* r, *de plus il est dans* $\langle r \rangle$ *par la question précédente. On conclut car les seuls éléments d'ordre* 4 *dans* $\langle r \rangle$ *sont* r *et* r^{-1} *(l'élément* r^2 *étant d'ordre* 2*).*

b. Montrer que $srs^{-1} = r^{-1}$. 2pts

Montrons tout d'abord que $G = \langle r, s \rangle$ *(le sous-groupe engendré par* r *et* s*). Puisque* $s \notin \langle r \rangle$, *on a* $\langle r, s \rangle \supsetneq \langle r \rangle$. *Puisque* $\langle r \rangle$ *est d'indice* 2 *dans* G, *le sous-groupe* $\langle r, s \rangle$ *est nécessairement d'indice* 1 *dans* G *i.e.* $\langle r, s \rangle = G$, *comme annoncé.*

Supposons maintenant que $srs^{-1} = r$. *On a donc* $sr = rs$, *donc puisque* $G = \langle r, s \rangle$ *cela implique que* G *est commutatif, ce qui est absurde. On a donc* $srs^{-1} = r^{-1}$.

5. En déduire que si $G \setminus \langle r \rangle$ possède un élément d'ordre 2 alors G est isomorphe au groupe diédral $\mathbb{D}_4$ d'ordre 8. 1pt

Si G *possède un élément* $s \in G \setminus \langle r \rangle$ *d'ordre* 2, *par ce qui précède on a* $srs = r^{-1}$. *Ainsi, le groupe* G *est engendré par les éléments* r *et* s *avec* $r^4 = s^2 = 1$ *et* $srs = r^{-1}$, *donc* $G \simeq \mathbb{D}_4$.

6. Si $t \in G \setminus \langle r \rangle$ n'est pas d'ordre 2, montrer que $t^2 = r^2$. 2pts

Puisque $\langle r \rangle \subseteq G$ *est (distingué et) d'indice* 2, *le groupe quotient* $G/\langle r \rangle$ *est isomorphe à* $\mathbb{Z}/2\mathbb{Z}$. *Si maintenant on note* $\bar{t}$ *la classe d'un élément* $t \in G$ *modulo* $\langle r \rangle$, *l'image dans* $\mathbb{Z}/2\mathbb{Z}$ *de* $\overline{t^2} = \bar{t}^2$ *est nécessairement* 0 *(car pour tout* $x \in \mathbb{Z}/2\mathbb{Z}$ *on a* $2x = 0$*). Ainsi, on a* $t^2 \in \langle r \rangle$.

Finalement, si $t \in G \setminus \langle r \rangle$ n'est pas d'ordre 2, puisque $t^2 \in \langle r \rangle$ on a $t^2 \in \{r, r^2, r^{-1}\}$. Mais par la question 2 on sait que t n'est pas d'ordre 8 donc $t^2 \notin \{r, r^{-1}\}$, ainsi finalement $t^2 = r^2$.

Commentaire : on montre facilement que le groupe suivant, défini par générateurs et relations,

$$\mathbb{H} := \langle \mathsf{r}, \mathsf{t} : \mathsf{r}^4 = 1, \mathsf{r}^2 = \mathsf{t}^2, \mathsf{t}\mathsf{r}\mathsf{t}^{-1} = \mathsf{r}^{-1} \rangle,$$

appelé groupe des quaternions, *est d'ordre 8. On a alors montré que $G \simeq \mathbb{H}$.*

Exercice 4 — 9pts

Soit $n \geqslant 2$. Le but de cet exercice est de montrer que tout sous-groupe d'indice n de $\mathfrak{S}_n$ est isomorphe à $\mathfrak{S}_{n-1}$. Soit G un sous-groupe de $\mathfrak{S}_n$ d'indice n.

1. Traiter les cas $n \in \{2, 3\}$. 1pt

Le groupe $\mathfrak{S}_2$ est de cardinal 2 donc un sous-groupe d'indice 2 est trivial donc isomorphe à $\mathfrak{S}_1$. Le groupe $\mathfrak{S}_3$ est de cardinal 6 donc un sous-groupe d'indice 3 est de cardinal 2, nécessairement isomorphe à $\mathfrak{S}_2 \simeq \mathbb{Z}/2\mathbb{Z}$.

2. On rappelle qu'un groupe d'ordre 6 est soit cyclique soit isomorphe à $\mathfrak{S}_3$. En déduire le cas $n = 4$. 2pts

Un sous-groupe d'indice 4 de $\mathfrak{S}_4$ est de cardinal $3! = 6$, donc est isomorphe à $\mathbb{Z}/6\mathbb{Z}$ ou à $\mathfrak{S}_3$ (d'après le rappel de l'énoncé). Or, le groupe $\mathfrak{S}_4$ ne possède aucun élément d'ordre 6 (en regardant la décomposition en cycles, on voit que l'ordre d'un élément de $\mathfrak{S}_2$ est 1 (élément trivial), 2 (transpositions et doubles transpositions), 3 (3-cycles) ou 4 (4-cycles)) donc nécessairement un sous-groupe d'indice 4 de $\mathfrak{S}_4$ est isomorphe à $\mathfrak{S}_3$.

On suppose maintenant que $n \geqslant 5$. On considère l'action (à gauche) de $\mathfrak{S}_n$ sur les classes à droites $\mathfrak{S}_n/G = \{\sigma G : \sigma \in \mathfrak{S}_n\}$ et on note $\phi : \mathfrak{S}_n \to \mathfrak{S}(\mathfrak{S}_n/G)$ le morphisme associé.

3. Montrer que l'action est fidèle. (On pourra utiliser sans justification que, puisque $n \geqslant 5$, les seuls sous-groupes distingués de $\mathfrak{S}_n$ sont $\mathfrak{S}_n$, $\mathfrak{A}_n$ et $\{1\}$.) 2pts

On remarque que $\ker \phi \subseteq G$ car $\sigma G \neq G$ si $\sigma \notin G$. Ainsi, on a $\# \ker \phi \leq \#G = (n-1)!$. Puisque $\ker \phi$ est un sous-groupe distingué de $\mathfrak{S}_n$ et que $n \geqslant 5$, d'après l'indication on a $\ker \phi \in \{\mathfrak{S}_n, \mathfrak{A}_n, \{1\}\}$. Par cardinalité, on en déduit que $\ker \phi = 1$ (on a bien $(n-1)! < \frac{n!}{2}$ car $n > 2$). Ainsi ϕ est injective et l'action est donc fidèle.

4. En déduire que ϕ est un isomorphisme. 1pt

Le morphisme ϕ est une injection entre deux ensembles de même cardinal (on a bien $|\mathfrak{S}(\mathfrak{S}_n/G) = n!$ puisque $|\mathfrak{S}_n/G| = n$ car G est d'indice n dans $\mathfrak{S}_n$) donc ϕ est un surjective et donc un isomorphisme.

5. Montrer que G est le stabilisateur de la classe $G \in \mathfrak{S}_n/G$ et en déduire que G agit sur un ensemble à $n-1$ éléments. 2pts

Pour tout $\sigma \in \mathfrak{S}_n$ on a

$$\begin{aligned} \sigma \in \mathrm{Stab}_{\mathfrak{S}_n}(G) &\iff \sigma G = G \\ &\iff \sigma \in G \end{aligned}$$

donc G est bien le stabilisateur dans $\mathfrak{S}_n$ de la classe $G \in \mathfrak{S}_\mathfrak{n}/G$. Ainsi, le groupe G agit sur l'ensemble $(\mathfrak{S}_n/G) \setminus \{G\}$ (le sous-groupe $G \subseteq \mathfrak{S}_n$ agissant sur $\mathfrak{S}_n/G$ par restriction de l'action de $\mathfrak{S}_n$), qui possède bien $n-1$ éléments.

6. En déduire que $G \simeq \mathfrak{S}_{n-1}$. 1pt

Soit $\psi : G \to \mathfrak{S}(\mathfrak{S}_n/G \setminus \{G\})$ l'action précédente. Un élément $\sigma \in G$ est dans $\ker \psi$ ssi $\sigma x = x$ pour tout $x \in \mathfrak{S}_n/G \setminus \{G\}$ et donc ssi $\sigma x = x$ pour tout $x \in \mathfrak{S}_n/G$ (puisque

$\sigma \in G = \mathrm{Stab}_{\mathfrak{S}_n}(G)$). Ainsi, pour tout $\sigma \in G$ on a $\sigma \in \ker \psi \iff \sigma \in \ker \phi$ d'où $\sigma = 1$ par la question **3**. Ainsi ψ est injective et on a donc une injection $G \hookrightarrow \mathfrak{S}(\mathfrak{S}_n/G \backslash \{G\}) \simeq \mathfrak{S}_{n-1}$, qui est une bijection car $|G| = |\mathfrak{S}_{n-1}| = (n-1)!$.