# Groupes

# Examen final + corrigé

Durée: 2 heures

*Documents, calculatrice ou téléphone interdits. Le barème est sur 20 + 2 points bonus (partie III).*

## I - Exemples (5 points)

Justifier chacun des exemples en une ou deux phrases.

1. Donner un exemple d'élément d'ordre 15 dans le groupe symétrique $S_8$.

   Solution. (**1 point**)
   $\sigma = (1\,2\,3\,4\,5)(6\,7\,8)$ *convient, car l'ordre d'une permutation est le PPCM des ordres des cycles de sa décomposition canonique.*

2. Donner un exemple de deux éléments d'ordre 3 non conjugués dans le groupe symétrique $S_6$.

   Solution. (**1 point**)
   $(1\,2\,3)$ *et* $(1\,2\,3)(4\,5\,6)$ *sont deux éléments d'ordre 3 dans* $S_6$*, qui sont non conjugués car de types différents.*

3. Donner un exemple de groupe $G$ et de deux éléments $a, b \in G$ d'ordre 2 tel que $ab$ soit d'ordre 3.

   Solution. (**1 point**)
   *On peut prendre* $G = S_3$, $a = (1\,2)$ *et* $b = (2\,3)$, *on a bien* $ab = (1\,2\,3)$ *d'ordre 3.*

4. Donner un exemple d'élément d'ordre 4 dans le groupe $\mathrm{GL}_2(\mathbb{R})$ des matrices $2 \times 2$ inversibles à coefficients réels.

   Solution. (**1 point**)
   *La matrice* $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ *convient, elle correspond à la rotation d'angle* $\pi/2$ *dans le plan* $\mathbb{R}^2$.

5. Donner un exemple d'élément d'ordre infini dans le groupe $\mathrm{SO}_2(\mathbb{R})$ des rotations du plan.

   Solution. (**1 point**)
   *Toute matrice de la forme* $\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ *avec* $\theta = 2\pi\alpha$ *et* $\alpha \notin \mathbb{Q}$ *convient, en effet les rotations d'ordre fini du plan sont exactement les rotations d'angle un multiple rationnel de* $2\pi$.

   *NB: c'est bien* $\alpha$ *qui doit être irrationnel, et pas* $\theta$ *lui-même. Par exemple* $\theta = \pi$ *est irrationnel mais correspond à une rotation d'ordre 2...*

## II - Groupes abéliens (6 points)

Les questions de cet exercice sont indépendantes. On attend une rédaction concise et précise.

1. Soit $G$ un groupe abélien, $a \in G$ d'ordre $m$, et $b \in G$ d'ordre $n$, avec $m$ et $n$ premiers entre eux. Montrer que $ab$ est d'ordre $mn$.

   SOLUTION. (**2 points**)
   *Notons $d$ l'ordre de $ab$ : par définition, $d$ est le plus petit entier $\geq 1$ tel que $(ab)^d = 1$.*

   *D'une part, comme $ab = ba$, on a*

   $$(ab)^{mn} = a^{mn}b^{mn} = (a^m)^n(b^n)^m = 1^n 1^m = 1.$$

   *On en déduit que $d \leq mn$.*

   *D'autre part (très peu ont su faire cette deuxième partie de l'argument...)*

   $$1 = (ab)^d = a^d b^d$$

   *implique $a^d = b^{-d}$ appartient à $\langle a \rangle \cap \langle b \rangle$. Comme $\langle a \rangle$ est d'ordre $m$, et $\langle b \rangle$ est d'ordre $n$, avec $m, n$ premiers entre eux, on en déduit par le théorème de Lagrange que $\langle a \rangle \cap \langle b \rangle = \{1\}$, donc $a^d = b^d = 1$, et finalement $d$ est un multiple commun de $m$ et $n$, en particulier $d \geq mn$.*

   *Conclusion : $d = mn$.*

2. Soit $G$ un groupe dont tous les éléments (à part le neutre) sont d'ordre 2. Montrer que $G$ est abélien.

   SOLUTION. (**2 points**)
   *Soit $a, b \in G$. Par hypothèse l'élément $ab$ est d'ordre 2 (ou 1), on a donc*

   $$1 = (ab)^2 = abab,$$

   *et donc $ab = b^{-1}a^{-1}$. De plus $a^{-1} = a$ et $b^{-1} = b$ (à nouveau car $a^2 = b^2 = 1$) donc*

   $$ab = b^{-1}a^{-1} = ba,$$

   *autrement dit $a$ et $b$ commutent.*

3. Soit $\mathbb{R}$ le groupe additif des nombres réels, et $U \subset \mathbb{C}^*$ le sous-groupe multiplicatif des complexes de module 1. Expliciter un morphisme surjectif de $\mathbb{R}$ vers $U$, et en déduire que $U$ est isomorphe à un quotient de $\mathbb{R}$ que l'on précisera.

   SOLUTION. (**2 points**)
   *On considère l'application suivante*

   $$\begin{aligned} \varphi \colon \mathbb{R} &\to U \\ x &\mapsto e^{ix} \end{aligned}$$

   *D'une part $\varphi$ est un morphisme car $\varphi(x+y) = e^{i(x+y)} = e^{ix}e^{iy} = \varphi(x)\varphi(y)$, et $\varphi$ est surjectif car tout complexe de module 1 s'écrit sous la forme $e^{ix}$. Le noyau de $\varphi$ est égal à*

   $$\ker \varphi = \{x \in \mathbb{R}; e^{ix} = 1\} = 2\pi\mathbb{Z}$$

   *où $2\pi\mathbb{Z}$ désigne le sous-groupe des multiples entiers de $2\pi$. Par le théorème d'isomorphisme, on en déduit que $U \simeq \mathbb{R}/2\pi\mathbb{Z}$.*

## III - Centre d'un $p$-groupe (3 points)

Il y avait une erreur d'énoncé dans les deux dernières questions de cette partie (errare humanum est...). Ci-dessous pour info les énoncés corrects, et concernant le barême j'ai neutralisé ces deux questions (avec 0.5 ou 1 point bonus pour ceux qui m'ont dit des choses correctes en dépit de l'énoncé incorrect, et 2 points bonus pour l'unique personne qui a repéré qu'il y avait un problème avec l'énoncé...)

1. Rappeler la définition générale du centre $\mathcal{Z}(G)$ d'un groupe $G$.

   Solution. (**1 point**)

$$\begin{aligned}\mathcal{Z}(G) &= \{x \in G; gx = xg \textit{ pour tout } g \in G\} \\ &= \{x \in G; gxg^{-1} = x \textit{ pour tout } g \in G\}.\end{aligned}$$

Soit $p$ un nombre premier, et $G$ un $p$-groupe non trivial, c'est-à-dire un groupe d'ordre $|G| = p^a$ avec $a \geq 1$.

2. Écrire une action de $G$ sur lui-même de façon à ce que les orbites singleton soit précisément les éléments du centre $\mathcal{Z}(G)$.

   Solution. (**1 point**)
   *On considère l'action*

$$\begin{aligned}G \times G &\to G \\ (g, x) &\mapsto gxg^{-1}\end{aligned}$$

   *On voit que* $\mathrm{Orb}(x) = \{x\}$ *équivaut à* $gxg^{-1} = x$ *pour tout* $g \in G$, *autrement dit équivaut à* $x \in \mathcal{Z}(G)$.

3. Montrer que $|\mathcal{Z}(G)|$ est congru à 0 modulo $p$. Que cela implique-t-il sur $\mathcal{Z}(G)$ ?

   Solution. (**1 point**)
   *Par la formule* $|G| = |\mathrm{Stab}(x)| \cdot |\mathrm{Orb}(x)|$, *les orbites de l'action sont de cardinal ou bien 1 ou bien* $p^a$ *avec* $a \geq 1$. *En écrivant* $G$ *somme une union d'orbites, on écrit* $|G|$ *comme la somme des cardinaux des orbites. En considérant cette égalité modulo* $p$, *on obtient*

$$|G| \equiv |\mathcal{Z}(G)| \mod p$$

   *Comme* $G$ *est un* $p$*-groupe non trivial,* $|G| \equiv 0 \mod p$, *on obtient donc* $|\mathcal{Z}(G)| \equiv 0 \mod p$, *ce qui implique que* $\mathcal{Z}(G) \neq \{1\}$.

Dans les deux dernières questions on suppose que $G$ est un groupe d'ordre $p^2$ non cyclique.

4. Montrer que $\mathcal{Z}(G)$ contient un sous-groupe $K$ isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

   Solution. (**0 point**)
   *Soit* $g \in \mathcal{Z}(G) \setminus \{1\}$, *un tel* $g$ *existe par la question précédente. Posons* $K = \langle g \rangle$. *Par le théorème de Lagrange,* $g$ *est d'ordre* $p$ *ou* $p^2$. *Mais ordre*$(g) = p^2$ *impliquerait que* $G = K$ *est cyclique de générateur* $g$, *contrairement à l'hypothèse. Donc* $g$ *est d'ordre* $p$, *et* $K \simeq \mathbb{Z}/p\mathbb{Z}$.

5. Soit $h \in G$ un élément non contenu dans $K$. Donner l'ordre de $h$, et montrer qu'on a une structure de produit direct $G = K \times \langle h \rangle$.

   Solution. (**0 point**)
   *$h$ est d'ordre $p$ : $h \neq 1$ car sinon on aurait $h \in K$, et $h$ n'est pas d'ordre $p^2$ sinon $G$ serait cylique engendré par $h$. $K \cap \langle h \rangle$ étant un sous-groupe strict de $\langle h \rangle$, par Lagrange il est trivial. De plus le groupe engendré par $K$ et $h$ contient strictement $K$, par Lagrange à nouveau il est égal à $G$. Enfin $g\langle h \rangle g^{-1} = \langle h \rangle$ pour tout élément de $\langle h \rangle$, pour tout élément de $K \subset \mathcal{Z}(G)$, et donc finalement pour tout élément de $G$ : ainsi $\langle h \rangle$ est distingué dans $G$, et on conclut que $G = K \times \langle h \rangle$.*

## IV - Le groupe du tétraèdre (6 points)

Soit $T$ un tétraèdre régulier de $\mathbb{R}^3$, on notera $A_1, A_2, A_3, A_4$ ses sommets. On rappelle que la notation $\mathrm{Isom}(T)$ désigne le groupe des isométries de $\mathbb{R}^3$ préservant $T$.

1. Expliciter de façon synthétique (sans faire de listes !) un morphisme injectif $\varphi$ de $\mathrm{Isom}(T)$ vers le groupe symétrique $S_4$ (et justifier l'injectivité).

   Solution. (**2 points**)
   *Un morphisme de $\mathrm{Isom}(T)$ vers $S_4$ est donné par*

$$\begin{aligned} \varphi \colon \mathrm{Isom}(T) &\to S_4 \\ f &\mapsto \sigma \end{aligned}$$

   *où $f(A_i) = A_{\sigma(i)}$. Ce morphisme est injectif car tout $f \in \mathrm{Isom}(T)$ peut être vu comme un élément de $\mathrm{GL}_3(\mathbb{R})$ en prenant le centre du tétraèdre comme origine, et si $f(A_i) = A_i$ pour $i = 1, 2, 3$, ces trois points formant une base de $\mathbb{R}^3$, on en déduit que $f = id$.*

2. Quelle est la préimage de la transposition $(12)$ par le morphisme $\varphi$ ? Et celle de la permutation $(12)(34)$ ?

   Solution. (**1 point**)
   *Soit $P$ le plan passant par $A_3, A_4$ et le milieu du segment $[A_1, A_2]$. Alors la symétrie orthogonale $S_P$ de plan $P$ fixe $A_3, A_4$ et échange $A_1$ et $A_2$, autrement dit $\varphi(S_P) = (12)$ .*

   *Par ailleurs soit $D$ la droite passant par les milieux des segments $[A_1, A_2]$ et $[A_3, A_4]$, alors la rotation $R_{D,\pi}$ d'axe $D$ et d'angle $\pi$ échange $A_1$ et $A_2$ d'une part, $A_3$ et $A_4$ d'autre part, donc $\varphi(R_{D,\pi}) = (12)(34)$.*

3. Montrer que $\varphi$ est un isomorphisme entre $\mathrm{Isom}(T)$ et $S_4$.

   Solution. (**1 point**)
   *On a vu à la question précédente que $(12)$ est dans l'image de $\varphi$, on montre de même que toute transposition $(i, j)$ est dans l'image de $\varphi$. Comme les transpositions engendrent $S_4$, on en déduit que l'image de $\varphi$ est $S_4$. Ainsi $\varphi$ est injective et surjective, c'est un isomorphisme.*

4. En utilisant l'action de $\mathrm{Isom}(T)$ sur les paires d'arêtes opposées de $T$, montrer qu'il existe un morphisme surjectif de $\mathrm{Isom}(T)$ vers $S_3$.

   Solution. (**1 point**)
   *Notons $P_1$, $P_2$, $P_3$ les 3 paires d'arêtes opposées. On définit un morphisme de $\mathrm{Isom}(T)$*

*vers $S_3$ en posant*

$$\begin{aligned}\psi\colon \operatorname{Isom}(T) &\to S_3\\ f &\mapsto \sigma\end{aligned}$$

*où $f(P_i) = P_{\sigma(i)}$. Une rotation $R$ d'angle $2\pi/3$ et d'axe passant par un sommet et le milieu de la face opposée est envoyé par $\psi$ sur un 3-cycle. D'autre part la symétrie orthogonale $S_P$ où $P$ est le plan passant par $A_3, A_4$ et le milieu du segment $[A_1, A_2]$ est envoyé sur une transposition. Comme $S_3$ est engendré par tout choix d'une transposition et d'un 3-cycle, on en déduit que $\psi$ est surjectif.*

5. En déduire que $S_3$ est isomorphe à un quotient de $S_4$, en précisant le sous-groupe distingué mis en jeu dans ce quotient.

Solution. (**1 point**)
*On applique le théorème d'isomorphisme au morphisme surjectif $\psi\circ\varphi$ obtenu en composant les morphismes des questions précédentes. On obtient*

$$S_4/\ker(\psi\circ\varphi) \simeq S_3$$

*Donc $\ker(\psi\circ\varphi)$ est un sous-groupe distingué de $S_4$ d'ordre $24/6 = 4$, c'est donc le sous-groupe $\{id, (12)(34), (13)(24), (14)(23)\}$.*