UNIVERSITÉ DE BORDEAUX
Théorie des Groupes

Corrigé de l'examen du 15 décembre 2022

Durée 3h. Documents non autorisés

Exercice 1. Groupes d'ordre p^3q. Soient p et q deux nombres premiers distincts. Le but de cet exercice est de montrer qu'un groupe fini d'ordre p^3q n'est pas simple. Soit G un groupe d'ordre p^3q. On note n_p (respectivement n_q) le nombre de p-Sylow (respectivement q-Sylow) de G.

1) Montrer que $n_p \in \{1, q\}$ et que $n_q \in \{1, p, p^2, p^3\}$.

Solution. n_p divise $q = |G|/p^3$ et n_q divise $p^3 = |G|/q$.

2) Montrer que le cas $n_p = q$, $n_q = p$ est impossible. (Indication : utiliser le troisième théorème de Sylow).

Solution. Par le troisième théorème de Sylow $n_p \equiv 1 \pmod p$ et $n_q \equiv 1 \pmod q$. On en déduit que si $n_p = q$ et $n_q = p$, alors p divise $q-1$ et q divise $p-1$ ce qui est impossible.

3) Supposons que $n_q = p^3$. Montrer que G contient $(q-1)p^3$ éléments d'ordre q. En déduire que $n_p = 1$ et conclure.

Solution. Comme q est un nombre premier, si H_1 et H_2 sont deux sous-groupes distincts d'ordre q, alors $H_1 \cap H_2 = \{e\}$. Donc le nombre d'éléments d'ordre q est

$$(q-1) \cdot (\text{nombre de sous-groupes d'ordre } q) = (q-1)p^3.$$

Donc G possède

$$p^3q - (q-1)p^3 = p^3$$

élements d'ordre différent de q. Comme G possède au moins un p-Sylow d'ordre p^3, on en déduit que $n_p = 1$. Soit H l'unique p-Sylow de G. Alors pour tout $x \in G$ on a $x^{-1}Hx = H$, d'où on déduit que H est un sous-groupe distingué de G. Donc G n'est pas simple.

4) Supposons que $n_q = p^2$.

a) Montrer que $q \mid p-1$ ou $q \mid p+1$.

Solution. Comme $n_q \equiv 1 \pmod q$, on a $q \mid p^2 - 1 = (p-1)(p+1)$.

b) Montrer que si $q \mid p-1$, alors $n_p = 1$.

Solution. Supposons que $n_p \neq 1$. Alors $n_p = q \equiv 1 \pmod p$, d'où $p \mid q-1$. Or $q \mid p-1$, d'où $p \leqslant q-1 \leqslant p-2$. Contradiction.

c) Montrer que si $q \mid p+1$, alors $n_p = 1$ ou $p = 2$ et $q = 3$.

Solution. Si $n_p \neq 1$, alors on a $p \mid q-1$ et $q \mid p+1$. Donc $p \leqslant q-1$ et $q \leqslant p+1$. On en déduit que $p = 2$ et $q = 3$.

d) Supposons que $p = 2$, $q = 3$ et $n_q = n_3 = 2^2 = 4$. En considérant l'action de G sur l'ensemble $Syl_3(G)$ de ses 3-Sylow, prouver que G n'est pas simple.

Solution. Comme $Syl_3(G)$ est un ensemble de cardinal 4, l'action de G sur $Syl_3(G)$ induit un homomorphisme $\psi : G \to S_4$. Si ψ est injectif, alors, comme $|G| = |S_4| = 2^3 \cdot 3 = 24$, l'application ψ est un isomorphisme. Or S_4 n'est pas simple. Si ψ n'est pas injectif, alors $\ker(\psi)$ est un sous-groupe distingué non-trivial de G et G n'est pas simple.

5) Conclure.

Solution. Soit G un groupe d'ordre $p^3 q$.
a) On note que si $n_p = 1$ (respectivement $n_q = 1$), alors G possède un unique p-Sylow (respectivement q-Sylow), qui est distingué dans G. Donc dans ces cas, G n'est pas simple.
b) Si $n_q = p$, alors (cf. question 2)) $n_p = 1$.
c) Si $n_q = p^3$, alors $n_p = 1$ (cf. question 3)).
d) Si $n_q = p^2$ et $(n_p, n_q) \neq (2,3)$, alors $n_p = 1$ (cf. questions 4a-c)).
e) Si $(n_p, n_q) = (2,3)$, alors G n'est pas simple (cf. question 4d)).

Exercice 2. Soit $K = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$.

1) Prouver que K est une extension galoisienne de $\mathbf{Q}$ de degré 4. Donner une base de K sur $\mathbf{Q}$.

Solution. Soit $F = \mathbb{Q}[\sqrt{2}]$. Comme $\sqrt{2} \notin \mathbb{Q}$ et comme $\sqrt{2}$ est une racine de X^2-2, X^2-2 est le polynôme minimal de $\sqrt{2}$ sur $\mathbb{Q}$. Donc $[F:\mathbb{Q}]=2$. On montre par l'absurde que $\sqrt{3}\notin F$. Supposons que $\sqrt{3}=a+b\sqrt{2}\in L$, $a,b\in\mathbb{Q}$. Alors $3=a^2+2b^2+2ab\sqrt{2}$, d'où $\sqrt{2}\in\mathbb{Q}$. Contradiction. Donc $\sqrt{3}\notin L$ et X^2-3 est le polynôme minimal de $\sqrt{3}$ sur F. On en déduit que $[K:F]=2$. Par le théorème de la base télescopique $[K:\mathbb{Q}]=[K:F][F:\mathbb{Q}]=4$ et les éléments $1,\sqrt{2},\sqrt{3},\sqrt{6}=\sqrt{2}\cdot\sqrt{3}$ forment une base de K sur $\mathbb{Q}$.

2) Soit σ un automorphisme de $K/\mathbf{Q}$. Prouver que $\sigma(\sqrt{2})=\pm\sqrt{2}$ et $\sigma(\sqrt{3})=\pm\sqrt{3}$. Soit $\mu_2=\{-1,1\}$ le groupe multiplicatif des racines carrées de l'unité. Prouver que l'application

$$\mathrm{Gal}(K/\mathbf{Q})\to\mu_2\times\mu_2$$

qui a tout $\sigma\in\mathrm{Gal}(K/\mathbf{Q})$ associe $\left(\frac{\sigma(\sqrt{2})}{\sqrt{2}},\frac{\sigma(\sqrt{3})}{\sqrt{3}}\right)$ est un isomorphisme. Déterminer les groupes $\mathrm{Gal}(K/\mathbf{Q}[\sqrt{2}])$ et $\mathrm{Gal}(K/\mathbf{Q}[\sqrt{3}])$.

Solution. Soit σ un automorphisme de $K/\mathbb{Q}$. Alors $(\sigma(\sqrt{2}))^2=\sigma(\sqrt{2}^2)=\sigma(2)=2$, d'où $\sigma(\sqrt{2})=\pm\sqrt{2}$. De même, $\sigma(\sqrt{3})=\pm\sqrt{3}$. Soit

$$\varphi\,:\,\mathrm{Gal}(K/\mathbb{Q})\to\mu_2\times\mu_2$$

l'application qui a tout $\sigma\in\mathrm{Gal}(K/\mathbb{Q})$ associe $\left(\frac{\sigma(\sqrt{2})}{\sqrt{2}},\frac{\sigma(\sqrt{3})}{\sqrt{3}}\right)$. Om montre que φ est un homomorphisme. Soient $\sigma,\tau\in\mathrm{Gal}(K/\mathbb{Q})$. Alors

$$\frac{\sigma\tau(\sqrt{2})}{\sqrt{2}}=\frac{\sigma\tau(\sqrt{2})}{\sigma(\sqrt{2})}\cdot\frac{\sigma(\sqrt{2})}{\sqrt{2}}=\sigma\left(\frac{\tau(\sqrt{2})}{\sqrt{2}}\right)\cdot\frac{\sigma(\sqrt{2})}{\sqrt{2}}=\frac{\tau(\sqrt{2})}{\sqrt{2}}\cdot\frac{\sigma(\sqrt{2})}{\sqrt{2}}$$

et

$$\frac{\sigma\tau(\sqrt{3})}{\sqrt{3}}=\frac{\sigma(\sqrt{3})}{\sqrt{3}}\cdot\frac{\tau(\sqrt{3})}{\sqrt{3}}$$

(remarquons que $\sigma\left(\frac{\tau(\sqrt{2})}{\sqrt{2}}\right)=\frac{\tau(\sqrt{2})}{\sqrt{2}}$ puisque $\frac{\tau(\sqrt{2})}{\sqrt{2}}=\pm1\in\mathbb{Q}$). On en déduit que $\varphi(\sigma\tau)=\varphi(\sigma)\varphi(\tau)$. Donc φ est un homomorphisme. Supposons que $\sigma\in\ker(\varphi)$. Alors $\sigma(\sqrt{2})=\sqrt{2}$ et $\sigma(\sqrt{3})=\sqrt{3}$. Comme $K=\mathbb{Q}[\sqrt{2},\sqrt{3})$, on en déduit que $\sigma=\mathrm{id}_K$. Donc φ est injectif. Comme

$$|\mathrm{Gal}(K/\mathbb{Q})|=[K:\mathbb{Q}]=4=|\mu_2\times\mu_2|,$$

l'homomorphisme φ est surjectif. Donc φ est un isomorphisme.

Par la corréspondance de Galois

$$\mathrm{Gal}(K/\mathbb{Q}[\sqrt{2}])=\{e,g_1\},$$

où $g_1(\sqrt{2}) = \sqrt{2}$ et $g_1(\sqrt{3}) = -\sqrt{3}$ et

$$\mathrm{Gal}(K/\mathbb{Q}[\sqrt{3}]) = \{e, g_2\},$$

où $g_2(\sqrt{2}) = -\sqrt{2}$ et $g_2(\sqrt{3}) = \sqrt{3}$.

3) Soit $\alpha = (2+\sqrt{2})(3+\sqrt{6})$. Calculer $\sigma(\alpha)$ pour tout $\sigma \in \mathrm{Gal}(K/\mathbf{Q})$. En déduire que $K = \mathbf{Q}[\alpha]$.

Solution. On a $\mathrm{Gal}(K/\mathbb{Q}) = \{e, g_1, g_2, g_3\}$, où $g_3 = g_1 g_2$. Alors

$$\begin{aligned}
e(\alpha) &= \alpha = 6 + 3\sqrt{2} + 2\sqrt{3} + 2\sqrt{6},\\
g_1(\alpha) &= (2+\sqrt{2})(3-\sqrt{6}) = 6 + 3\sqrt{2} - 2\sqrt{3} - 2\sqrt{6},\\
g_2(\alpha) &= (2-\sqrt{2})(3-\sqrt{6}) = 6 - 3\sqrt{2} - 2\sqrt{3} - 2\sqrt{6}\\
g_3(\alpha) &= (2-\sqrt{2})(3+\sqrt{6}) = 6 - 3\sqrt{2} - 2\sqrt{3} + 2\sqrt{6}.
\end{aligned}$$

Comme $1, \sqrt{2}, \sqrt{3}, \sqrt{6} = \sqrt{2}\cdot\sqrt{3}$ forment une base de K sur $\mathbb{Q}$, on voit que $\alpha, g_1(\alpha), g_2(\alpha)$ et $g_3(\alpha)$ sont deux à deux distincts. Donc $\mathbb{Q}[\alpha] \subset K$ est une sous-extension de $K/\mathbb{Q}$ telle que $[\mathbb{Q}[\alpha] : \mathbb{Q}] \geqslant 4$. Comme $[K : \mathbb{Q}] = 4$, on en déduit que $\mathbb{Q}[\alpha] = K$.

4) Prouver que pour tout $\sigma \in \mathrm{Gal}(K/\mathbf{Q})$ l'élément $\sigma(\alpha)/\alpha$ est un carré dans K, c'est-à-dire que pour tout σ il existe $a \in K$ tel que $\sigma(\alpha)/\alpha = a^2$.

Solution. On a

$$\frac{g_1(\alpha)}{\alpha} = \frac{3-\sqrt{6}}{3+\sqrt{6}} = \frac{(3-\sqrt{6})^2}{3} = \left(\frac{3-\sqrt{6}}{\sqrt{3}}\right)^2,$$

$$\frac{g_2(\alpha)}{\alpha} = \frac{(2-\sqrt{2})(3-\sqrt{6})}{(2+\sqrt{2})(3+\sqrt{6})} = \frac{(2-\sqrt{2})^2(3-\sqrt{6})^2}{2\cdot 3} = \left(\frac{(2-\sqrt{2})\cdot(3-\sqrt{6})}{\sqrt{6}}\right)^2,$$

$$\frac{g_3(\alpha)}{\alpha} = \frac{2-\sqrt{2}}{2+\sqrt{2}} = \frac{(2-\sqrt{2})^2}{2} = \left(\frac{2-\sqrt{2}}{\sqrt{2}}\right)^2.$$

5) Soit β une racine du polynôme $X^2 - \alpha \in K[X]$. On veut prouver par l'absurde que $\beta \notin K$. Supposons que $\beta \in K$.

a) Soit $\mathrm{Gal}(K/\mathbf{Q}[\sqrt{2}]) = \{\mathrm{id}_K, \tau\}$. Prouver que $\beta\tau(\beta) \in \mathbf{Q}[\sqrt{2}]$.

Solution. On a $\tau = g_1$.

$$\tau(\beta\tau(\beta)) = \tau(\beta)\tau^2(\beta) = \tau(\beta)\beta.$$

Donc $\beta\tau(\beta) \in K^{\mathrm{Gal}(K/\mathbb{Q}[\sqrt{2}])} = \mathbb{Q}[\sqrt{2}]$.

b) Calculer $\alpha\tau(\alpha)$ et en déduire que $\beta\tau(\beta) = \pm(2+\sqrt{2})\sqrt{3}$.

Solution. On a

$$\alpha\tau(\alpha) = (2+\sqrt{2})(3+\sqrt{6})(2+\sqrt{2})(3-\sqrt{6}) = 3 \cdot (2+\sqrt{2})^2.$$

Comme $(\beta\tau(\beta))^2 = \alpha\tau(\alpha)$, on a

$$\beta\tau(\beta) = \sqrt{\alpha\tau(\alpha)} = \sqrt{3}(2+\sqrt{2}).$$

c) Trouver une contradiction et conclure.

Solution. Comme $\sqrt{3} \notin \mathbb{Q}[\sqrt{2}]$, on a

$$\beta\tau(\beta) = \sqrt{3}(2+\sqrt{2}) \notin \mathbb{Q}[\sqrt{2}].$$

Or $\beta\tau(\beta) \in \mathbb{Q}[\sqrt{2}]$ par 5a).

6) Soit $L = K[\beta]$. Prouver que $L/\mathbf{Q}$ est une extension normale de degré 8.

Solution. On a

$$[L:\mathbb{Q}] = [L:K][K:\mathbb{Q}] = 2 \cdot 4 = 8.$$

Soit $\sigma : L/\mathbb{Q} \to E/\mathbb{Q}$ un homomorphisme à valeurs dans une extension E de L. Alors $\sigma(\beta)^2 = \sigma(\alpha)$. La restriction de σ sur K coïncide avec un élément g de $\mathrm{Gal}(K/\mathbb{Q})$. Par 6), $g(\alpha) = a^2\alpha$ pour un certain $a \in K$, d'où on a

$$\sigma(\beta)^2 = \alpha a^2. \qquad (*)$$

Donc $\sigma(\alpha) = \pm\beta a \in L$ et on a prouvé que $\sigma(L) \subset L$. On en déduit que $L/\mathbb{Q}$ est normale.

7) Définir des automorphismes de $L/\mathbf{Q}$ qui prolongent les éléments de $\mathrm{Gal}(K/\mathbf{Q})$.

Solution. Comme $\beta^2 = \alpha$, on a $L = \mathbb{Q}[\beta]$. Donc tout élément $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ est complètement défini par $\sigma(\beta)$. On utilise la formule (*) pour déterminer $\sigma(\beta)$.

Les prolongements de l'automorphisme trivial $e \in \mathrm{Gal}(K/\mathbb{Q})$ vérifient $\sigma(\beta)^2 = \alpha$. On obtient, donc l'automorphisme trivial σ_{00} de $L/\mathbb{Q}$ qui vérifie $\sigma_{00}(\beta) = \beta$ et l'automorphisme σ_{01} défini par $\sigma_{01}(\beta) = -\beta$.

Les prolongements de l'automorphisme $g_1 \in \mathrm{Gal}(K/\mathbb{Q})$ vérifient $\sigma(\beta)^2 = \alpha a_1^2$, où (voir la question 6)) $a_1 = \frac{3-\sqrt{6}}{\sqrt{3}}$. On obtient donc les automorphismes σ_{10} et σ_{11} définis par

$$\sigma_{10}(\beta) = \beta\,\frac{3-\sqrt{6}}{\sqrt{3}}, \qquad \sigma_{11}(\beta) = -\beta\,\frac{3-\sqrt{6}}{\sqrt{3}}.$$

Les même raisonnement donne les prolongements de g_2 :

$$\sigma_{20}(\beta) = \beta\,\frac{(2-\sqrt{2})\cdot(3-\sqrt{6})}{\sqrt{6}}, \qquad \sigma_{21}(\beta) = -\beta\,\frac{(2-\sqrt{2})\cdot(3-\sqrt{6})}{\sqrt{6}}$$

et de g_3 :

$$\sigma_{30}(\beta) = \beta\,\frac{2-\sqrt{2}}{\sqrt{2}}, \qquad \sigma_{31}(\beta) = -\beta\,\frac{2-\sqrt{2}}{\sqrt{2}}.$$

Remarquons que $\sigma_{11} = \sigma_{10}\sigma_{01}$, $\sigma_{21} = \sigma_{20}\sigma_{01}$ et $\sigma_{31} = \sigma_{30}\sigma_{01}$.

8) Soit

$$\mathbf{H}_8 = \left\{ \pm\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, \pm\begin{pmatrix}i & 0\\ 0 & -i\end{pmatrix}, \pm\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}, \pm\begin{pmatrix}0 & i\\ i & 0\end{pmatrix} \right\},$$

où $i^2 = -1$. Vérifier que $\mathbf{H}_8$ est un groupe pour le produit matriciel. Est-il abélien?

Solution. Soient $E = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$, $I = \begin{pmatrix}i & 0\\ 0 & -i\end{pmatrix}$, $J = \begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}$, $K = \begin{pmatrix}0 & i\\ i & 0\end{pmatrix}$. Alors

$$I^2 = J^2 = K^2 = -E, \quad IJ = -JI = K, \quad JK = -KJ = I, \quad KI = -IK = J.$$

On en déduit que $\mathbf{H}_8$ est un sous-groupe non abélien de $\mathrm{GL}_2(\mathbf{C})$.

9) Prouver que $H = \left\{\pm\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\right\}$ est un sous-groupe distingué de $\mathbf{H}_8$ est que $\mathbf{H}_8/A$ est isomorphe à $\mu_2 \times \mu_2$.

Solution. Comme les matrices $\pm\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$ commutent avec toutes les matrices, A est un sous-groupe distingué de $\mathbf{H}_8$. Le quotient $\mathbb{H}_8/A$ est un groupe d'ordre $4 = 2^2$. Donc $\mathbf{H}_8/A$ est abélien. Un groupe abélien d'ordre 4 est soit cyclique, soit produit direct de deux groupes d'ordre

2. D'après les calculs précédents (cf. question 8)), on a $x^2 = e$ pour tout $x \in \mathbb{H}_8/A$. Donc $\mathbf{H}_8/A$ est isomorphe au produit direct de deux groupes d'ordre 2.

10) Prouver que $\mathrm{Gal}(L/\mathbf{Q})$ est isomorphe à $\mathbf{H}_8$.

Solution. En utilisant la question 7), il est facile de voir que $\sigma_{01}^2 = e$, $\sigma_{11}^2 = \sigma_{21}^2 = \sigma_{31}^2 = \sigma_{01}$ et $\sigma_{11}\sigma_{21} = \sigma_{31}$, $\sigma_{21}\sigma_{11} = \sigma_{01}\sigma_{31}$. On en déduit facilement que l'application $f : \mathrm{Gal}(L/\mathbb{Q}) \to \mathbb{H}_8$ définie par $f(\sigma_{01}) = -\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $f(\sigma_{11}) = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, $f(\sigma_{21}) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $f(\sigma_{31}) = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ est un isomorphisme.

FIN