Université de Bretagne Occidentale
UFR Sciences et Techniques
L3 DE MATHEMATIQUES

GROUPES ET GEOMETRIE

Examen terminal, le 20 juin 2018, 8h30-11h30

CORRIGE et BAREME

Exercice 1. a. **(0,5 pt)** Comme $\sigma(1) = 6$, $\sigma(6) = 4$ et $\sigma(4) = 1$, le cycle $(1\,6\,4)$ est l'un des facteurs de la décomposition de σ en cycles disjoints. Comme $\sigma(2) = 3$, $\sigma(3) = 9$, $\sigma(9) = 10$ et $\sigma(10) = 2$, le cycle $(2\,3\,9\,10)$ en est un autre. Comme $\sigma(5) = 11$ et $\sigma(11) = 5$, la transposition $(5\,11)$ en est un également, tout comme la transposition $(7\,12)$. Comme $\sigma(8) = 8$, on a bien

$$\sigma = (1\,6\,4)(2\,3\,9\,10)(5\,11)(7\,12).$$

b. **(0,5 pt)** Rappelons que la signature d'un cycle de longueur ℓ est égale à $(-1)^{\ell+1}$. On a donc

$$\varepsilon(\sigma) = (-1)^4(-1)^5(-1)^3(-1)^3 = -1.$$

c. **(0,5 pt)** L'ordre de σ est le ppcm des longueurs des cycles de sa décomposition en cycles disjoints. D'où

$$\text{ordre}(\sigma) = \text{ppcm}(3, 4, 2, 2) = 12.$$

d. **(1,5 pt)** Ecrivons $\tau = (i_1\, i_2\, \dots\, i_{12})$. Comme τ est d'ordre 12, il suffit de montrer l'énoncé pour les entiers compris entre -5 et 6. Ceux qui sont premiers avec 12 sont $-5, -1, 1, 5$. Or, $\tau^1 = \tau$ est bien un cycle de longueur 12 par hypothèse. Comme

$$\tau^{-1} = (i_{12}\, i_{11}, \dots\, i_1),$$

τ^{-1} en est un également. Comme

$$\tau^5 = (i_1\, i_6\, i_{11}\, i_4\, i_9\, i_2\, i_7\, i_{12}\, i_5\, i_{10}\, i_3\, i_8),$$

τ^5 est bien un cycle de longueur 12, ainsi que

$$\tau^{-5} = (i_8\, i_3\, i_{10}\, i_5\, i_{12}\, i_7\, i_2\, i_9\, i_4\, i_{11}\, i_6\, i_1).$$

e. **(1,5 pt)** Par l'absurde, si $\sigma = \tau^n$ pour un entier n, l'ordre de σ est égal à $12/\text{pgcd}(12, n)$, d'après le cours, car τ est d'ordre 12. D'après le c, σ est d'ordre 12, donc $\text{pgcd}(12, n) = 1$. D'après le d, $\sigma = \tau^n$ est un cycle de longueur 12. Cela contredit l'unicité de la décomposition en cycles disjoints.

Exercice 2. a. **(1 pt)** Soit $\sigma \in Z(S_4)$. Montrons que $\sigma = \text{id}$. Par hypothèse, $\tau\sigma = \sigma\tau$ quel que soit $\tau \in S_4$. Cela veut dire que $\tau\sigma\tau^{-1} = \sigma$ quel que soit $\tau \in S_4$. Autrement dit, tous les conjugués (à gauche) de σ sont égaux à σ. Ou encore, σ est la seule permutation de S_4 de son type. Les types des permutations de S_4 sont

$$(4),\ (3),\ (2,2),\ (2),\ (),$$

et leur fréquence est

$$6,\ 8,\ 3,\ 6,\ 1,$$

respectivement. On voit que le seul type n'ayant qu'une permutation est le type (). Il s'ensuit que $\sigma = \text{id}$.

b. **(1 pt)** On montre les deux inclusions. Supposons que $(g,h) \in Z(G \times H)$. Montrons que $g \in Z(G)$ et que $h \in Z(H)$. Soit $k \in G$. On a $(k,e) \in G \times H$. Comme (g,h) appartient au centre de $G \times H$, on a

$$(gk,h) = (g,h)(k,e) = (k,e)(g,h) = (kg,h).$$

Il vient que $gk = kg$. D'où $g \in Z(G)$. De même $h \in Z(H)$, et donc $(g,h) \in Z(G) \times Z(H)$.

Réciproquement, supposons que $(g,h) \in Z(G) \times Z(H)$. Soit $(k,\ell) \in G \times H$. On a

$$(g,h)(k,\ell) = (gk,h\ell) = (kg,\ell h) = (k,\ell)(g,h)$$

car $g \in Z(G)$ et $h \in Z(H)$. Cela montre que $(g,h) \in Z(G \times H)$.

c. **(1 pt)** On a bien $e \in Z(D_{24})$ car le centre d'un groupe est un sous-groupe. Montrons que $r^{12} \in Z(D_{24})$. Il est clair que r^{12} commute avec r. Comme $r^{24} = e$, on a $r^{-12} = r^{12}$ et $sr^{12} = r^{-12}s = r^{12}s$, c-à-d, r^{12} commute avec s. Comme D_{24} est engendré par r et s, l'élément r^{12} commute avec tous les éléments de D_{24}, i.e., $r^{12} \in Z(D_{24})$.

Montrons que e et r^{12} sont les seuls éléments de D_{24} appartenant au centre. Supposons que r^n, où $n \in \{0,\dots,23\}$, apparient au centre. En particulier, $sr^n = r^n s$. Comme $sr^n = r^{-n}s$ dans D_{24}, on en déduit que $r^n s = r^{-n}s$, et donc que $r^n = r^{-n}$, ou encore que $r^{2n} = e$. Il s'ensuit que $24 = \text{ordre}(r) | 2n$, i.e. $n = 0$ ou $n = 12$. Cela montre que, parmi les éléments de D_{24} de la forme r^n, les seuls qui appartiennent au centre sont e et r^{12}.

Il nous reste donc à montrer que, parmi les éléments de D_{24} de la forme $r^n s$, aucun n'appartient au centre. Supposons que $r^n s$, où $n \in \{0,\dots,23\}$, appartient au centre. En particulier $r(r^n s) = (r^n s)r$. Comme $r^n sr = r^{n-1}s$, on obtient $r^{n+1}s = r^{n-1}s$, et donc $r^{n+1} = r^{n-1}$, ou encore $r^2 = e$ ce qui est absurde.

d. **(1 pt)** Prendre $H = S_4$, $G = \langle (1\,2) \rangle$ et $f\colon G \to H$ le morphisme d'inclusion. Comme G est monogène, G est commutatif. Donc $Z(G) = G \not\subseteq \{\text{id}\}$. D'après le a, $Z(H) = \{\text{id}\}$. On a donc $f(Z(G)) \not\subseteq Z(H)$.

e. **(0,5 pt)** Soit $g \in Z(G)$ et montrons que $f(g) \in Z(H)$. Soit $h \in H$. Comme f est surjectif, il existe $k \in G$ tel que $f(k) = h$. Du coup,

$$hf(g) = f(k)f(g) = f(kg) = f(gk) = f(g)f(k) = f(g)h$$

car $g \in Z(G)$. Il s'ensuit que $f(g) \in Z(H)$.

f. **(1 pt)** Soit donc

$$f\colon \mathrm{GL}_2(\mathbb{F}_3) \to \mathrm{GL}_2(\mathbb{F}_3)/\{\pm I\}$$

le morphisme quotient. Comme f est surjectif, $f(Z(\mathrm{GL}_2(\mathbb{F}_3)) \subseteq Z(\mathrm{GL}_2(\mathbb{F}_3)/\{\pm I\})$ d'après le e. Or, le groupe quotient $\mathrm{GL}_2(\mathbb{F}_3)/\{\pm I\}$ est isomorphe au groupe symétrique S_{24}, dont le centre est trivial d'après le a. Comme des groupes isomorphes ont des centres isomorphes (voir le h ci-dessous), le quotient $\mathrm{GL}_2(\mathbb{F}_3)/\{\pm I\}$ a un centre tivial. Du coup, le centre de $\mathrm{GL}_2(\mathbb{F}_3)$ est contenu dans le noyau de f, i.e., $Z(\mathrm{GL}_2(\mathbb{F}_3)) \subseteq \{\pm I\}$. Comme l'inclusion inverse est évidente, on a bien $Z(\mathrm{GL}_2(\mathbb{F}_3)) = \{\pm I\}$.

g. **(1 pt)** Comme f est surjectif, on a $f(Z(G)) \subseteq Z(H)$ d'après le e. Comme f est un isomorphisme, $f^{-1}\colon H \to G$ est également un morphisme surjectif. D'après le e, $f^{-1}(Z(H)) \subseteq Z(G)$. En appliquant f, on obtient $Z(H) \subseteq f(Z(G))$.

h. **(0,5 pt)** Comme $f(Z(G)) = Z(H)$ d'après le g, la restriction de f au sous-groupe $Z(G)$ de G est un morphisme surjectif sur $Z(H)$. Comme f est injectif, cette restriction est également injective. Cette dernière est donc un isomorphisme de $Z(G)$ sur $Z(H)$.

i. **(1 pt)** Par l'absurde. Supposons que S_4 et $Q_8 \times \mathbb{Z}/3\mathbb{Z}$ sont isomorphes. D'après le h, les centres $Z(S_4)$ et $Z(Q_8 \times \mathbb{Z}_3\mathbb{Z})$ sont isomorphes. Or, le groupe $Z(S_4)$ est trivial d'après le a, alors que

$$Z(Q_8 \times \mathbb{Z}/3\mathbb{Z}) = Z(Q_8) \times Z(\mathbb{Z}/3\mathbb{Z}) = \{\pm 1\} \times \mathbb{Z}/3\mathbb{Z}$$

ne l'est pas. Contradiction.

j. **(1 pt)** Le morphisme $\rho \circ f$ envoie le sous-groupe distingué $Z(G)$ de G sur $\{\bar{e}\}$. En effet,

$$(\rho \circ f)(Z(G)) = \rho(f(Z(G))) \subseteq \rho(Z(H)) = \{\bar{e}\}$$

d'après le e. On conclut par la propriété universelle du quotient.

k. **(1 pt)** Montrons que f est bijectif. Comme f et ρ sont surjectif, $\rho \circ f$ est surjectif. Comme $\bar{f} \circ \pi = \rho \circ f$, le composé $\bar{f} \circ \pi$ est surjectif, et donc $\bar{f}$ en particulier.

Montrons ensuite que $\bar{f}$ est injectif. Supposons que $\bar{f}(\bar{g}) = \bar{e}$. Comme $\bar{f} \circ \pi = \rho \circ f$ on a $\bar{f}(\bar{g}) = \overline{f(g)}$. D'où, $\overline{f(g)} = \bar{e}$, i.e., $f(g) \in Z(H)$. Donc $g = f^{-1}(f(g)) \in Z(G)$ d'après le e appliqué à f^{-1}. Du coup, $\bar{g} = \bar{e}$ dans $G/Z(G)$.

l. **(1 pt)** Par l'absurde. Supposons que $\mathrm{GL}_2(\mathbb{F}_3)$ et D_{24} sont isomorphes. D'après le k, les quotients $\mathrm{GL}_2(\mathbb{F}_3)/Z(\mathrm{GL}_2(\mathbb{F}_3))$ et $D_{24}/Z(D_{24})$ sont isomorphes. Or, le premier quotient est isomorph à S_4, et le deuxième à D_{12}. Comme $Z(S_4)$ est trivial et $Z(D_{12})$ ne l'est pas, il y a contradiction.

Exercice 3. a. **(0,5 pt)** L'ordre de $(\mathbb{Z}/49\mathbb{Z})^\times$ est $\varphi(49) = \varphi(7^2) = 7 \times 6 = 42$.

b. **(2 pt)** Soit $\pi\colon \mathbb{Z}/49\mathbb{Z} \to \mathbb{Z}/7\mathbb{Z}$ le morphisme d'anneaux défini par $\pi(\bar{x}) = \tilde{x}$. Il induit un morphisme de groupes multiplicatifs

$$\pi^\times\colon (\mathbb{Z}/49\mathbb{Z})^\times \to (\mathbb{Z}/7\mathbb{Z})^\times.$$

Comme $\ker(\pi) = \langle\bar{7}\rangle$, on a $\pi^{-1}(\tilde{1}) = \bar{1} + \langle\bar{7}\rangle$. Du coup,

$$\ker(\pi^\times) = (\bar{1} + \langle\bar{7}\rangle) \cap (\mathbb{Z}/49\mathbb{Z})^\times = \bar{1} + \langle\bar{7}\rangle.$$

En particulier, $|\ker(\pi^\times)| = 7$. Il s'ensuit que $\pi^\times$ est surjectif. En particulier, $\pi^\times$ envoie tout générateur sur un générateur.

c. **(0,5 pt)** Comme $(-\tilde{2})^2 = \tilde{4} \neq \tilde{1}$ et $(-\tilde{2})^3 = -\tilde{8} = -\tilde{1} \neq \tilde{1}$ dans $(\mathbb{Z}/7\mathbb{Z})^\times$, l'ordre de $-\tilde{2}$ est égal à 6 et $-\tilde{2}$ est donc un générateur de $(\mathbb{Z}/7\mathbb{Z})^\times$.

d. **(1 pt)** Compte tenu du b, il y a des chances que $-\bar{2}$ soit un générateur de $(\mathbb{Z}/49\mathbb{Z})^\times$. En effet, $(\mathbb{Z}/7\mathbb{Z})^\times$ possède $\varphi(6) = 2$ générateurs. Ces 2 générateurs possèdent 14 antécédents dans $(\mathbb{Z}/49\mathbb{Z})^\times$, dont $\varphi(42) = 12$ sont générateurs, en admettant que ce dernier groupe est effectivement cyclique !

Comme le groupe $(\mathbb{Z}/49\mathbb{Z})^\times$ est d'ordre $42 = 2 \times 3 \times 7$, il suffit de vérifier que $(-\bar{2})^6$, $(-\bar{2})^{14}$ et $(-\bar{2})^{21}$ sont différents de $\bar{1}$ dans $(\mathbb{Z}/49\mathbb{Z})^\times$. Or,

$$\begin{aligned}
(-\bar{2})^6 &= \bar{6}\bar{4} = \bar{1}\bar{5} \neq \bar{1},\\
(-\bar{2})^{14} &= \bar{2}^8 \times \bar{2}^6 = 2\bar{5}6 \times \bar{6}\bar{4} = \bar{1}\bar{1} \times \bar{1}\bar{5} = 1\bar{6}5 = \bar{1}\bar{8} \neq \bar{1}, \text{ et}\\
(-\bar{2})^{21} &= -(\bar{2}^8)^2 \times \bar{2}^5 = -1\bar{2}1 \times \bar{3}\bar{2} = 2\bar{3} \times \bar{1}\bar{7} = 3\bar{9}1 = -\bar{1} \neq \bar{1}.
\end{aligned}$$

Par conséquence, $-\bar{2}$ est bien un générateur de $(\mathbb{Z}/49\mathbb{Z})^\times$.