Université Claude Bernard - Lyon 1 Semestre d'automne 2024-2025

L3 Math. Gén. : Groupes 13 novembre 2024

Examen partiel : correction et barème

Une attention particulière sera apportée à la rédaction. Les téléphones, calculatrices et documents de cours sont interdits. Le barème est donné à titre indicatif.

Exercice 1 (6 points)**.** Dire si les assertions suivantes sont vraies ou fausses. Pour chaque assertion **justifier** en citant un résultat du cours (ou du TD), ou en donnant un exemple/contre-exemple, selon ce qui convient. Une réponse vrai/faux correcte mais sans justification ne donne aucun point.

1. (1 point) Soit $H := \left\{ \begin{pmatrix} 0 & a \\ b & 0 \end{pmatrix} \ : \ a, b \in \mathbb{R}, \ ab \neq 0 \right\} \subseteq M_2(\mathbb{R})$.
   L'ensemble H est un sous-groupe de $GL_2(\mathbb{R})$.
2. (1 point) Le groupe diédral D_8 possède un sous-groupe d'ordre 3.
3. (1 point) Le groupe alterné $\mathfrak{A}_4$ est simple.
4. (1 point) Soit G un groupe et soit
   $D(G) := \langle [g, h] \ : \ g, h \in G \rangle$. Le groupe $G/D(G)$ est abélien.
   (On rappelle que si $g, h \in G$ alors $[g, h] = ghg^{-1}h^{-1}$.)
5. (2 points) Tous les groupes d'ordre $n \leq 5$ sont abéliens.

Correction 1.

1. **Faux** Soit $M := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Alors $M \in H$, mais $M^2 = \mathbb{I}_2 \notin H$.
   Donc H n'est pas stable par multiplication.
   D'où le fait que $\boxed{H \text{ n'est pas un sous-groupe de } M_2(\mathbb{R}).}$
2. **Faux** Soit $H \leq D_8$. Comme $|D_8| = 8$, par Lagrange $|H|$ divise 8. Or 3 ne divise pas 8. Donc $\boxed{D_8 \text{ n'admet aucun sous-groupe d'ordre 3.}}$
3. **Faux** Le groupe $\mathfrak{A}_4$ contient le sous-groupe

   $$V_4 = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}.$$

   Montrons que ce sous-groupe est distingué dans $\mathfrak{A}_4$.
   On sait que dans $\mathfrak{S}_n$ les conjugués d'une permutation sont les permutations dont la décomposition en produit de cycles à supports disjoint ont le même nombre de cycle de chaque longueur. En particulier, donc le conjugué par un élément de $\mathfrak{S}_n$ d'une double transposition est une double transposition. Et donc, en particulier le conjugué par un élément de $\mathfrak{A}_n$ d'une double transposition est une double transposition. Ainsi V_4 est distingué dans $\mathfrak{A}_4$ et donc $\boxed{\mathfrak{A}_4 \text{ n'est pas simple.}}$

4. **Vrai** Soient $xD(G)$ et $yD(G)$ deux éléments de $G/D(G)$. Pour montrer que $G/D(G)$ est abélien, il nous faut montrer (par définition d'un groupe abélien) que $\big(xD(G)\big)\big(yD(G)\big) = \big(yD(G)\big)\big(xD(G)\big)$.
   Tout d'abord, notons que $\big(xD(G)\big)\big(yD(G)\big) = xyD(G)$, de même $\big(yD(G)\big)\big(xD(G)\big) = yxD(G)$. Donc, montrer que $G/D(G)$ est abélien revient à montrer que $xyD(G) = yxD(G)$.
   Mais $xyD(G) = yxD(G)$ si et seulement si il existe $g \in D(G)$ tel que $xy = yxg$. Or
   $$xy = \left(yx(yx)^{-1}\right) xy = \left(yxx^{-1}y^{-1}\right) xy = yx \left(x^{-1}y^{-1}xy\right) = yx \left[x^{-1}, y^{-1}\right].$$
   Mais $\left[x^{-1}, y^{-1}\right] \in D(G)$. Donc, par ce qui précède, $xyD(G) = yxD(G)$ et ainsi, $\boxed{G/D(G) \text{ est abélien.}}$
5. **Vrai** Soit G un groupe fini.
   — Si $|G| = 1$ alors $G = \{e\}$ est le groupe trivial (donc en particulier abélien).
   — Si $|G| \in \{1, 3, 5\}$, alors comme $|G|$ est premier on a $G \sim \mathbb{Z}/|G|\mathbb{Z}$. Donc en particulier, G est abélien.
   — Supposons $|G| = 4$. Soit $x \in G\backslash\{e\}$, alors (par Lagrange) $\mathrm{ord}(x)$ divise 4. Ainsi $\mathrm{ord}(x) \in \{2, 4\}$. On peut alors distinguer deux cas : ou bien G admet un élément d'ordre 4, ou bien tous les éléments non-triviaux de G sont d'ordre 2.
   Si G admet un élément d'ordre 4, alors G est cyclique et donc $G \sim \mathbb{Z}/4\mathbb{Z}$ et G est abélien.
   Sinon, tous les éléments de G sont d'ordre 2. Montrons qu'un tel groupe G est abélien : soient $x, y \in G$. Comme x $= 2 = \mathrm{ord}(y)$ ces éléments vérifient $x^{-1} = x$ et $y^{-1} = y$. Alors
   $$xyx^{-1}y^{-1} = xyxy = (xy)^2 = e,$$
   Où la dernière égalité découle du fait que $xy \in G$ est d'ordre 2. Ainsi $xy = yx$ et donc G est abélien.
   Conclusion $\boxed{\text{Tout groupe d'ordre inférieur ou égal à 5 est abélien.}}$

Exercice 2 (2 points)**.**
Montrer qu'il existe un isomorphisme de groupes entre $(\mathbb{C}/\mathbb{R}, +)$ et $(\mathbb{R}, +)$.

Correction 2. Considérons l'application $\varphi : \mathbb{C} \to \mathbb{R}$ donnée par $\varphi(a + ib) = b$ où $a, b \in \mathbb{R}$.
Cette application est un morphisme de groupes. En effet pour $z = a + ib$ et $z' = a' + ib'$, $\varphi(z + z') = b + b' = \varphi(z) + \varphi(z')$. Ce morphisme est clairement surjectif. De plus son noyau est $\{a + ib \in \mathbb{C} \mid a, b \in \mathbb{R},\ b = 0\} = \mathbb{R}$. Par les théorèmes d'isomorphisme, on obtient un isomorphisme entre $\mathbb{C}/\ker(\varphi)$ et $\mathrm{Im}(\varphi)$ donc entre $\mathbb{C}/\mathbb{R}$ et $\mathbb{R}$.

Exercice 3 (2,5 points)**.** Soit σ l'élément de $\mathfrak{S}_7$ défini par
$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 7 & 2 & 4 & 5 & 1 & 3 \end{pmatrix}$$

1. (0,5 point) Donner la décomposition de σ en produit de cycles à supports disjoints.
2. (0,5 point) Calculer la signature de σ.
3. (1,5 points) Calculer σ^{2024}.

Correction 3. 1. $\boxed{\sigma = (16)(273).}$

2. $\varepsilon(\sigma) = \varepsilon(12)\varepsilon(273) = (-1)\cdot 1 = (-1)$. Donc $\boxed{\sigma \text{ est de signature } -1.}$
3. La décomposition de σ en produit de cycles à supports disjoints est composée d'une transposition (donc d'ordre 2) et d'un 3-cycle (qui est donc d'ordre 3). Ainsi

$$\mathrm{ord}(\sigma) = \mathrm{ppcm}\left\{\mathrm{ord}(12), \mathrm{ord}(273)\right\} = \mathrm{ppcm}\{2,3\} = 6$$

Déterminons la valeur de 2024 modulo 6. On a $2024 = 6 * 337 + 2$. Donc, en utilisant de plus que σ est d'ordre 6 on obtient,

$$\sigma^{2024} = \sigma^{6*337+2} = \left(\sigma^6\right)^{337}\sigma^2 = \sigma^2$$

Calculons σ^2 (on utilise ici que (16) et (273) sont à supports disjoints, donc commutent) :

$$\sigma^2 = (16)(273)(16)(273) = \big((16)\big)^2\big((273)\big)^2 = \big((273)\big)^2 = (237).$$

D'où $\boxed{\sigma^{2024} = (237)}$

Exercice 4 (3,5 points)**.**

1. (2,5 points) Soit $f : (\mathbb{Z}^3, +) \to (\mathbb{Q}_{>0}, \times)$ définie par $f(a,b,c) = 2^a 3^b 6^c$.
   (a) Montrer que f est un morphisme de groupes et déterminer son noyau.
   (b) Le morphisme f est-il surjectif ?
2. (1 point) Existe-t-il un morphisme de groupes surjectif de $\mathbb{Z}/8\mathbb{Z}$ vers $\mathbb{Z}/6\mathbb{Z}$?

Correction 4. 1. Soit $f : (a,b,c) \in \mathbb{Z}^3 \mapsto 2^a 3^b 6^c$.

(a) Pour tout $(a,b,c), (x,y,z) \in \mathbb{Z}^3$ on a

$$\begin{aligned} f\big((a,b,c)+(x,y,z)\big) = f\big((a+x, b+y, c+z)\big) &= 2^{a+x}3^{b+y}6^{c+z} \\ &= 2^a 2^x 3^b 3^y 6^c 6^z \\ &= \left(2^a 3^b 6^c\right)\left(2^x 3^y 6^z\right) \\ &= f(a,b,c) \times f(x,y,z). \end{aligned}$$

Donc $\boxed{f \text{ est bien un morphisme de groupes.}}$ Déterminons son noyau.

$$\begin{aligned} (a,b,c) \in \ker(f) &\Leftrightarrow 2^a 3^b 6^c = 1, \\ &\Longleftrightarrow 2^{a+c}3^{b+c} = 1, \\ &\Longleftrightarrow a+c = 0 \text{ et } b+c = 0 \end{aligned}$$

$$\iff a = -c = b.$$

Donc $\boxed{\ker(f) := \{(-c,-c,c)\ : c \in \mathbb{Z}\}.}$

(b) Montrons que $5 \notin \mathrm{im}(f)$.

Pour tout $(a,b,c) \in \mathbb{Z}^3$ on a $f(a,b,c) = 2^{a+c}3^{b+c}$. En particulier, si $f(a,b,c) \in \mathbb{Z}^*$ ceci est la décomposition en produit de facteurs premiers de $f(a,b,c)$. Or des facteurs premiers de cette décomposition n'est égal à 5. Ainsi $5 \notin \mathrm{im}(f)$ et donc $\boxed{f \text{ n'est pas surjectif.}}$

2. Soit $f : \mathbb{Z}/8\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$ un morphisme. Nous allons montrer que $\bar{1} \notin \mathrm{im}(f)$.

Soit $x \in \mathbb{Z}/8\mathbb{Z}$, on note n son ordre.

— Montrons d'abord que l'ordre de $f(x)$ est un diviseur commun à 8 et à 6.
Comme f est un morphisme, $x^n = e$ implique $f(x)^n = e$. Ainsi $\mathrm{ord}(f(x))$ divise n. Comme de plus $f(x) \in \mathbb{Z}/6\mathbb{Z}$, l'ordre de $f(x)$ divise aussi $|\mathbb{Z}/6\mathbb{Z}| = 6$.

— Comme $8 = 2^3$ et $6 = 2 \cdot 3$, on a $\mathrm{pgcd}(6,8) = 2$. Ainsi, par le point précédent $\mathrm{ord}\,(f(x)) \in \{1,2\}$. En particulier $f(x)$ ne peut-être égal à $\bar{1}$ qui est d'ordre 6.

Ce qui précède étant vérifié par tout $x \in \mathbb{Z}/8\mathbb{Z}$, on a donc $\bar{1} \notin f(\mathbb{Z}/9\mathbb{Z})$. Et donc, le morphisme $\boxed{f \text{ n'est pas surjectif.}}$

Exercice 5 (6 points)**.** Soit $G = \{z \in \mathbb{C} \mid \exists n \in \mathbb{N}^*,\ z^n = 1\}$.

1. (1 point) Montrer que $(G, \times)$ est un sous-groupe de $(\mathbb{U}, \times)$ où $\mathbb{U} = \{z \in \mathbb{C} \mid |z| = 1\}$.
2. (1,5 point) Soit p un entier positif non nul. Soit $\varphi : G \to G, z \mapsto z^p$. Montrer que φ est un morphisme de groupes et déterminer son image.
3. (0,5 point) Justifier que $\ker(\varphi)$ est distingué dans G.
4. (2 points) Montrer qu'il existe un sous-groupe non-trivial et distingué H de G tel que le groupe quotient G/H soit isomorphe à G
5. (1 point) Une telle situation (celle de la question 4) serait-elle possible si G était fini ?

Correction 5.

1. Notons que G est non-vide car $1^1 = 1$ ce qui fait que $1 \in G$.
Soient $z_1, z_2 \in G$. Il existe $n_1, n_2 \in \mathbb{N}^*$ tels que $z_1^{n_1} = z_2^{n_2} = 1$. Cela implique immédiatement que $(z_1z_2)^{n_1+n_2} = 1$ et que $(1/z_1)^{n_1} = 1$ donc z_1z_2 et $1/z_1$ appartiennent à G.
2. Remarquons d'abord que φ est bien à valeurs dans G car pour $z \in \mathbb{C}$, si $z^n = 1$ pour un certain entier $n > 0$ alors $(z^p)^n = 1$.
Soient $z_1, z_2 \in G$. On a alors $\varphi(z_1z_2) = (z_1z_2)^p = z_1^pz_2^p = \varphi(z_1)\varphi(z_2)$ par commutativité de la multiplication dans $\mathbb{C}$. Montrons que φ est surjective. Soit $z \in G$. Soit alors $s \in \mathbb{C}$ une solution de l'équation polynomiale $X^p - z = 0$; on sait que tout polynôme non-constant de $\mathbb{C}[X]$ admet une racine. Puisque $z \in G$, il existe un entier $n \geq 1$ tel que $z^n = 1$. Par conséquent, $s^{np} = 1$ donc s appartient bien à G et on a $\varphi(s) = s^p = z$. Ainsi, φ est bien surjective ce qui donne $\mathrm{Im}(\varphi) = G$.

3. G étant commutatif, tout sous-groupe de G est distingué dans G.
4. Considérons le morphisme φ de la question 2 avec l'entier $p = 2$. Notons H son noyau. Le groupe H est distingué dans G par la question 3. De plus, H n'est pas trivial car il contient -1. Par les théorèmes d'isomorphisme, on a G/H isomorphe à $\mathrm{Im}(\varphi) = G$.
5. Non car si G était fini, on aurait $|G/H| = |G|$ i.e. $|G|/|H| = |G|$ donc $|H| = 1$ et H serait le sous-groupe trivial $\{1\}$.