

Sorbonne Université

Année universitaire 2024-2025, licence 3, *Algèbre* (UE 3M270).

Correction de l'examen partiel du 21 octobre 2024.

Durée : 1h30. Les appareils électroniques et documents sont interdits.

Dans ce sujet, $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$ et $\mathbb{R}$ seront implicitement vus comme des groupes pour l'addition, $\mathbb{R}^\times$ et $\mathbb{C}^\times$ pour la multiplication, et $S_{\mathbb{R}}$ (ensemble des bijections de $\mathbb{R}$ dans lui-même) pour la composition des applications.

Exercice 1. Questions de cours. Soit G un groupe.

- (a) Voir la définition 2.2.1 du poly.
- (b) On attendait l'une des six propriétés équivalentes de l'assertion (A) du théorème 2.10.2.

Exercice 2. On sait d'après le cours (3.5.5) que $\varphi \mapsto \varphi(\bar{1})$ établit une bijection entre l'ensemble des morphismes de $\mathbb{Z}/2\mathbb{Z}$ (resp. $\mathbb{Z}/3\mathbb{Z}$) vers $\mathbb{C}^\times$ et l'ensemble $\{z \in \mathbb{C}^\times, z^2 = 1\}$ (resp. $\{z \in \mathbb{C}^\times, z^3 = 1\}$); la bijection réciproque envoie z sur $\bar{a} \mapsto z^a$.

L'ensemble $\{z \in \mathbb{C}^\times, z^2 = 1\}$ est égal à $\{1, -1\}$. On en déduit qu'il y a exactement deux morphismes φ_1 et φ_{-1} de $\mathbb{Z}/2\mathbb{Z}$ vers $\mathbb{C}^\times$, à savoir

$$\varphi_1: \begin{cases} \bar{0} \mapsto 1 \\ \bar{1} \mapsto 1 \end{cases} \quad \text{et} \quad \varphi_{-1}: \begin{cases} \bar{0} \mapsto 1 \\ \bar{1} \mapsto -1 \end{cases}$$

L'ensemble $\{z \in \mathbb{C}^\times, z^3 = 1\}$ est égal à $\{1, j, j^2\}$ (avec $j = e^{2i\pi/3}$). On en déduit qu'il y a exactement trois morphismes ψ_1, ψ_j et ψ_{j^2} de $\mathbb{Z}/3\mathbb{Z}$ vers $\mathbb{C}^\times$, à savoir

$$\psi_1: \begin{cases} \bar{0} \mapsto 1 \\ \bar{1} \mapsto 1 \\ \bar{2} \mapsto 1 \end{cases}, \quad \psi_j: \begin{cases} \bar{0} \mapsto 1 \\ \bar{1} \mapsto j \\ \bar{2} \mapsto j^2 \end{cases} \quad \text{et} \quad \psi_{j^2}: \begin{cases} \bar{0} \mapsto 1 \\ \bar{1} \mapsto j^2 \\ \bar{2} \mapsto (j^2)^2 = j^4 = j \end{cases}.$$

Les morphismes de $\mathbb{Z}/2\mathbb{Z}$ (resp. $\mathbb{Z}/3\mathbb{Z}$) vers $\mathbb{R}^\times$ sont simplement les morphismes de $\mathbb{Z}/2\mathbb{Z}$ (resp. $\mathbb{Z}/3\mathbb{Z}$) vers $\mathbb{C}^\times$ qui sont à valeurs réelles.

Or parmi $\varphi_1, \varphi_{-1}, \psi_1, \psi_j$ et ψ_{j^2} , seuls φ_1, φ_{-1} et ψ_1 sont à valeurs réelles.

Il s'ensuit qu'il y a exactement deux morphismes de $\mathbb{Z}/2\mathbb{Z}$ vers $\mathbb{R}^\times$, à savoir φ_1 et φ_{-1} (vus comme à valeurs dans $\mathbb{R}^\times$) et un morphisme de $\mathbb{Z}/3\mathbb{Z}$ vers $\mathbb{R}^\times$, à savoir ψ_1 (vu comme à valeurs dans $\mathbb{R}^\times$).

Exercice 3.

- (a) Le cardinal d'un sous-groupe de $\langle g \rangle$ divise le cardinal de $\langle g \rangle$, qui vaut p .
Un tel sous-groupe est donc de cardinal 1 ou p , ce qui veut dire qu'il est ou bien égal à $\{e\}$, ou bien à $\langle g \rangle$ tout entier. Si h est un élément de $\langle g \rangle$ autre que e , son ordre divise le cardinal p de $\langle g \rangle$ et n'est pas égal à 1 (car seul l'élément neutre est d'ordre 1 dans un groupe), c'est donc p .
- (b) L'intersection $\langle g \rangle \cap \langle h \rangle$ est à la fois un sous-groupe de $\langle g \rangle$ et un sous-groupe de $\langle h \rangle$. Si cette intersection n'est pas triviale il résulte de (a) qu'elle est égale à $\langle g \rangle$ aussi bien qu'à $\langle h \rangle$, et donc que $\langle g \rangle = \langle h \rangle$.

- (c) Soient $G_1, \dots, G_r$ les sous-groupes de G de la forme $\langle g \rangle$ avec g d'ordre p (ce sont aussi les sous-groupes de G de cardinal p , puisqu'un groupe de cardinal p est toujours cyclique). Pour tout i , posons $G'_i = G_i \setminus \{e\}$. Il résulte de la question (a) que pour tout i , tout élément de G'_i est d'ordre p . Réciproquement si g est un élément d'ordre p de G le groupe qu'il engendre est l'un des G_i , et comme $g \neq e$ (car e est d'ordre 1) l'élément g appartient à G'_i . Ainsi l'ensemble des éléments d'ordre p de G est la réunion des G'_i . Par ailleurs on déduit de (b) que $G_i \cap G_j = \{e\}$ dès que $i \neq j$, ce qui implique que $G'_i \cap G'_j = \emptyset$. Par conséquent, les G'_i sont deux à deux disjoints et l'ensemble des éléments d'ordre p de G est donc la réunion *disjointe* des G'_i . Puisque chaque G'_i est de cardinal $p - 1$, il y a $r(p - 1)$ éléments d'ordre p dans G .

Exercice 4. Soit G un groupe et soient K et H deux sous-groupes de G . On suppose que $hk = kh$ pour tout couple (h, k) appartenant à $H \times K$.

- (a) Le sous-ensemble HK de G :
- contient e puisque e est bien de la forme hk avec $h \in H$ et $k \in K$: il suffit de prendre $h = e$ et $k = e$ (comme H et K sont des sous-groupes de G ils contiennent tous les deux e) ;
 - est stable par la loi de groupe : si $(h, h', k, k') \in H^2 \times K^2$ alors $(hk)(h'k') = h(kh')k' = h(h'k)k' = (hh')(kk')$ (la seconde égalité provient de l'hypothèse de commutation entre éléments de H et de K), et $(hh')(kk')$ est bien un élément de HK car $hh' \in H$ et $kk' \in K$ puisque H et K sont des sous-groupes de G , donc sont stables par la loi interne ;
 - est stable par inversion : si $(h, k) \in H \times K$ on peut alors écrire $(hk)^{-1} = k^{-1}h^{-1} = h^{-1}k^{-1}$ (la seconde égalité provient de l'hypothèse de commutation entre éléments de H et de K), et $h^{-1}k^{-1}$ est bien un élément de HK car $h^{-1} \in H$ et $k^{-1} \in K$ puisque H et K sont des sous-groupes de G , donc sont stables par inversion.

Par conséquent, HK est un sous-groupe de G .

- (b) L'ensemble D contient $(e, e) = (e, e^{-1})$ (qui est l'élément neutre de $H \times K$) car $e \in H$ et $e \in K$. Soient g_1 et g_2 deux éléments de $H \cap K$. On a alors $(g_1, g_1^{-1})(g_2, g_2^{-1}) = (g_1g_2, g_1^{-1}g_2^{-1})$. Comme $H \cap K$ est un sous-groupe de G le produit g_1g_2 appartient à $H \cap K$, et l'on a par ailleurs $g_1^{-1}g_2^{-1} = (g_2g_1)^{-1} = (g_1g_2)^{-1}$ car $g_1g_2 = g_2g_1$ puisque g_1 appartient à H (en tant qu'élément de $K \cap H$) et que g_2 appartient à K (en tant qu'élément de $K \cap H$). Ainsi, D est stable sous la loi interne de $H \times K$. Soit enfin g un élément de $H \times K$. On a $(g, g^{-1})^{-1} = (g^{-1}, g) = (g^{-1})^{-1}$ et g^{-1} appartient à $H \cap K$ car ce dernier est un sous-groupe de G . Par conséquent $(g, g^{-1})^{-1}$ appartient à D et D est stable par inversion. Il s'ensuit que D est un sous-groupe de $H \times K$. Vérifions qu'il est distingué. Soit g un élément de $H \cap K$ et soit $(h, k) \in H \times K$. On a alors

$$\begin{aligned} (h, k)(g, g^{-1})(h, k)^{-1} &= (h, k)(g, g^{-1})(h^{-1}, k^{-1}) \\ &= (hgh^{-1}, kg^{-1}k^{-1}) = (g, g^{-1}) \in D \end{aligned}$$

où la dernière égalité provient du fait que $hg = gh$ puisque h appartient à H et g à K (en tant qu'élément de $H \cap K$) et que $g^{-1}k = kg^{-1}$ puisque

g^{-1} appartient à H (en tant qu'élément de $H \cap K$) et k à K . Le sous-groupe D de $H \times K$ est donc bien distingué.

- (c) Soit φ l'application de $H \times K$ dans HK qui envoie (h, k) sur hk . Pour tout $(h, h', k, k') \in H^2 \times K^2$ on a

$$\varphi((h, k)(h', k')) = \varphi(hh', kk') = hh'kk' = hkh'k' = \varphi(h, k)\varphi(h', k'),$$

où la troisième égalité provient du fait que $h'k = kh'$ car $h' \in H$ et $k \in K$. Par conséquent, φ est un morphisme de groupes. Il est surjectif par définition de HK . Son noyau est l'ensemble des couples $(h, k) \in H \times K$ tels que $hk = e$, c'est-à-dire tels que $h = k^{-1}$. Mais si $h = k^{-1}$ alors h appartient à K et donc à $H \cap K$, et $(h, k) = (h, h^{-1})$ appartient à D ; ainsi $\ker(\varphi) \subset D$, et l'inclusion réciproque est évidente. On a donc $\ker(\varphi) = D$. Puisque φ est surjective, il en résulte que φ induit par passage au quotient un isomorphisme de $(H \times K)/D$ sur HK .

Exercice 5. Pour tout couple $(a, b) \in \mathbb{R}^\times \times \mathbb{R}$, on note $u_{a,b}$ l'application de $\mathbb{R}$ dans $\mathbb{R}$ qui envoie x sur $ax + b$, et l'on pose $G = \{u_{a,b}\}_{a \in \mathbb{R}^\times, b \in \mathbb{R}}$.

- (a) Si $u_{a,b} = u_{a',b'}$ on a alors $u_{a,b}(0) = u_{a',b'}(0)$ et $u_{a,b}(1) = u_{a',b'}(1)$, c'est-à-dire $b = b'$ et $a + b = a' + b'$. Il en résulte aussitôt que $b = b'$ et $a = a'$; par conséquent, $(a, b) \mapsto u_{a,b}$ est injective.
- (b) Soit $(a, b) \in \mathbb{R}^\times \times \mathbb{R}$. Soit $y \in \mathbb{R}$. Pour tout $x \in \mathbb{R}$ on a alors les équivalences

$$\begin{aligned} u_{a,b}(x) = y &\iff ax + b = y \\ &\iff x = \frac{y - b}{a}, \end{aligned}$$

ce qui montre que y a un et un seul antécédent par $u_{a,b}$, à savoir $(y - b)/a$. Par conséquent $u_{a,b}$ est bijective de réciproque $y \mapsto (y - b)/a$, c'est-à-dire encore $u_{1/a, -b/a}$.

- (c) On vient de voir que G est constitué de bijections, et est stable par inversion. Par ailleurs G contient $\text{Id}_{\mathbb{R}}$ qui est égale à $u_{1,0}$. Il reste à s'assurer que G est stable par composition. Soient a et c deux réels non nuls et soient b et d deux réels. On a pour tout $x \in \mathbb{R}$ les égalités

$$\begin{aligned} u_{a,b}(u_{c,d}(x)) &= u_{a,b}(cx + d) \\ &= a(cx + d) + b \\ &= acx + ad + b \\ &= u_{ac, ad+b}(x), \end{aligned}$$

si bien que $u_{a,b}u_{c,d} = u_{ac, ad+b}$ (nous nous permettons de noter la composition par une simple juxtaposition des termes, pour éviter une profusion de symboles $\circ$; notez que $ac \neq 0$ car a et c sont non nuls, donc on a bien le droit d'écrire $u_{ac, ad+b}$). Ainsi G est stable par composition, et est donc bien un sous-groupe de $S_{\mathbb{R}}$.

- (d) On déduit de la formule donnée à la question précédente que

$$u_{1,1}u_{2,0} = u_{1 \cdot 2, 1 \cdot 0 + 1} = u_{2,1} \text{ et } u_{2,0}u_{1,1} = u_{2 \cdot 1, 2 \cdot 1 + 0} = u_{2,2}.$$

Comme $u_{2,1} \neq u_{2,2}$ par (a), on voit que G n'est pas abélien.

- (e) Soit $(a, b) \in \mathbb{R}^\times \times \mathbb{R}$. On a d'après (c) l'égalité $u_{a,b}^2 = u_{a^2, (a+1)b}$. L'élément $u_{a,b}$ de G est de 2-torsion si et seulement si $u_{a,b}^2 = \text{Id}_{\mathbb{R}}$, c'est-à-dire si et seulement si $u_{a^2, (a+1)b} = u_{1,0}$. En vertu de (a) c'est le cas si et seulement si $a^2 = 1$ et $(a+1)b = 0$, ce qui équivaut à

$$(a = 1 \text{ et } b = 0) \text{ ou } (a = -1).$$

L'ensemble des éléments de 2-torsion de G est donc

$$\{u_{1,0} = \text{Id}_{\mathbb{R}} \cup \{u_{-1,b}\}_{b \in \mathbb{R}}.$$

- (f) On a $i(b)i(b') = u_{1,b}u_{1,b'} = u_{1 \cdot 1 + 1 \cdot b' + b} = u_{1, b+b'} = i(b+b')$, ce qui montre que i est un morphisme de groupes. Un réel b appartient à $\ker(i)$ si et seulement si $u_{1,b} = \text{Id}_{\mathbb{R}} = u_{1,0}$; d'après (a), c'est le cas si et seulement si $b = 0$. Ainsi, i est injectif.
- (g) L'application φ est bien définie car en vertu de (a) l'écriture $u_{a,b}$ d'un élément de G est unique. La formule $u_{a,b}u_{c,d} = u_{ac, ad+b}$ entraîne que $\varphi(u_{a,b}u_{c,d}) = ac = \varphi(u_{a,b})\varphi(u_{c,d})$. Par conséquent φ est un morphisme de groupes.
- (h) Il résulte immédiatement des définitions que $\ker(\varphi)$ est $\{u_{1,b}\}_{b \in \mathbb{R}}$. Autrement dit $\ker(\varphi) = T$, ce qui montre que ce dernier est un sous-groupe distingué de G . Par ailleurs φ est surjective : si a est un réel non nul il est par exemple égal à $\varphi(u_{a,0})$. Il s'ensuit que φ induit un isomorphisme entre G/T et $\mathbb{R}^\times$.
- (i) Soient $(a, b, c) \in \mathbb{R}^\times \times \mathbb{R}^2$. On a alors

$$\begin{aligned} u_{a,b}u_{1,c}u_{a,b}^{-1} &= u_{a,ac+b}u_{a,b}^{-1} \\ &= u_{a,ac+b}u_{1/a, -b/a} \\ &= u_{1, -b+ac+b} \\ &= u_{1,ac}. \end{aligned}$$

(La première et la troisième égalité proviennent de la formule donnée en (c), et la seconde de la formule donnée en (b)). L'élément $u_{1,ac}$ de G appartient à T . On voit ainsi que $gtg^{-1} \in T$ pour tout $g \in G$ et tout $t \in T$. Par conséquent, T est distingué dans G .