Sorbonne Université
Année universitaire 2025-2026, licence 3, *Algèbre* (UE 3M270).
Corrigé de l'examen partiel, le 3 novembre 2025.

Exercice 1. Question de cours. Voir la définition 2.3.1 du poly.

Exercice 2. Groupes abéliens finis.

On utlisera pour les deux questions le théorème de structure des groupes abéliens finis. Il assure que pour tout entier $n \geqslant 1$, l'ensemble des classes d'isomorphie de groupes abéliens de cardinal n est en bijection avec l'ensemble des familles finies d'entiers strictement positifs $(d_1, \dots, d_r)$ où $2 \leqslant d_1 | d_2 | \dots | d_r$ et $\prod d_i = n$ (le groupe correspondant à une telle famille est $\prod \mathbb{Z}/d_i\mathbb{Z}$).

(a) On a $42 = 2 \cdot 3 \cdot 7$. Soit $(d_1, \dots, d_r)$ une liste d'entiers comme ci-dessus avec $\prod d_i = 42$. Comme le nombre premier 2 divise $\prod d_i$ il divise l'un des d_i, donc d_r ; de même 3 et 7 divisent d_r, si bien que 42 divise d_r. On a donc nécessairement $r = 1$ et $d_1 = 42$. Le seul groupe abélien de cardinal 42 (à isomorphisme près) est donc $\mathbb{Z}/42\mathbb{Z}$.

(b) On a $60 = 2^2 \cdot 3 \cdot 5$. Soit $(d_1, \dots, d_r)$ une liste d'entiers comme ci-dessus avec $\prod d_i = 60$. Comme le nombre premier 2 divise $\prod d_i$ il divise l'un des d_i, donc d_r ; de même 3 et 5 divisent d_r, si bien que $2 \cdot 3 \cdot 5 = 30$ divise d_r. Cela laisse deux possibilités : $r = 1$ et $d_r = 60$, qui correspond au groupe $\mathbb{Z}/60\mathbb{Z}$; ou bien $r = 2, d_2 = 30$ et $d_1 = 2$ (notons que 2 divise bien 30) qui correspond au groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$. Il y a donc (à isomorphisme près) exactement deux groupes abéliens de cardinal 60, à savoir $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$ et $\mathbb{Z}/60\mathbb{Z}$.

Exercice 3.

(a) Les éléments de $\mathbb{Z}/7\mathbb{Z}^\times$ sont (en omettant d'écrire les barres) $1, -1, 2, -2, 3$ et -3. On sait que l'ordre de chacun d'eux divise 6 (qui est le cardinal de $(\mathbb{Z}/7\mathbb{Z})^\times$), donc vaut $1, 2, 3$ ou 6 ; il suffit en conséquence de calculer le carré et le cube de chacun pour conclure.

L'élément 1 est d'ordre 1 et c'est le seul (car c'est le neutre). Comme $(-1)^2 = 1$, l'élément (-1) est d'ordre 2. On a $2^2 = 4 = (-3)$ et $2^3 = 8 = 1$, donc l'élément 2 est d'ordre 3. On a $(-2)^2 = 4$ et $(-2)^3 = -2^3 = -1$, donc -2 est d'ordre 6. On a $3^2 = 9 = 2$ et $3^3 = 27 = -1$ donc 3 est d'ordre 6. On a $(-3)^2 = 3^2 = 2$ et $(-3)^3 = -3^3 = 1$, donc (-3) est d'ordre 3.

(b) Les générateurs de $(\mathbb{Z}/7\mathbb{Z})^\times$ sont ses éléments d'ordre 6. Par ce qui précède il en a deux, à savoir (-2) et 3. Un morphisme de $(\mathbb{Z}/7\mathbb{Z})^\times$ vers un groupe quelconque est déterminé par sa valeur sur n'importe quel générateur, par exemple par sa valeur en 3 ; en particulier tout automorphisme de $(\mathbb{Z}/7\mathbb{Z})^\times$ est déterminé par sa valeur en 3, qui doit être un générateur.

Soit φ un automorphisme de $(\mathbb{Z}/7\mathbb{Z})^\times$. On a donc par ce qui précède $\varphi(3) = 3$ ou $\varphi(3) = -2$. Mais si $\varphi(3)32$ alors $\varphi = \mathrm{Id}$ puisque $\mathrm{Id}(3) = 3$. Et si $\varphi(3) = -2$ alors $\varphi = (z \mapsto z^{-1})$ puisque $3 \cdot (-2) = -6 = 1$ si bien que $(-2) = 3^{-1}$.

(Remarquons que $z \mapsto z^{-1}$ est bien un automorphisme de $(\mathbb{Z}/7\mathbb{Z})^\times$ car ce dernier est abélien).

(c) D'après le cours, $\psi \mapsto \psi(1 \mod 3)$ établit un isomorphisme entre $\mathrm{Hom}(\mathbb{Z}/3\mathbb{Z}, (\mathbb{Z}/7\mathbb{Z})^\times$ et l'ensemble des éléments de 3-torsion de $(\mathbb{Z}/7\mathbb{Z})^\times$; un tel élément a de 3-torsion étant donné, le morphisme associé envoie n mod 3 sur a^n.

Les éléments de 3-torsion de $(\mathbb{Z}/7\mathbb{Z})^\times$ sont les éléments dont l'ordre divise 3, donc ceux qui sont d'ordre 1 ou 3. D'après la première question de l'exercice, les éléments en question sont $1, 2$ et (-3).

On a donc 3 morphismes de groupes de $\mathbb{Z}/3\mathbb{Z}$ vers $(\mathbb{Z}/7\mathbb{Z})^\times$, à savoir

$$\begin{cases} 0 & \mapsto & 1 \\ 1 & \mapsto & 1 \\ 2 & \mapsto & 1 \end{cases},$$

$$\begin{cases} 0 & \mapsto & 1 \\ 1 & \mapsto & 2 \\ 2 & \mapsto & 2^2 = 4 = (-3) \end{cases},$$

et

$$\begin{cases} 0 & \mapsto & 1 \\ 1 & \mapsto & (-3) \\ 2 & \mapsto & (-3)^2 = 9 = 2 \end{cases}.$$

Exercice 4. Comparaison des groupes $\mathbb{C}$ et $\mathbb{C}^\times$. Dans cet exercice $\mathbb{C}$ est vu comme groupe pour l'addition, et $\mathbb{C}^\times$ pour la multiplication.

(a) Le sous-groupe de $\mathbb{C}$ formé des éléments de n-torsion est l'ensemble des éléments z de $\mathbb{C}$ tels que $nz = 0$. Comme $n \geqslant 1$ c'est le sous-groupe trivial $\{0\}$.

Le sous-groupe de $\mathbb{C}^\times$ formé des éléments de n-torsion est l'ensemble des éléments z de $\mathbb{C}^\times$ tels que $z^n = 1$. C'est donc l'ensemble des racines n-ièmes de l'unité, c'est-à-dire $\{\exp(2ik\pi/n)\}_{0 \leqslant k \leqslant n-1}$.

(b) Par ce qui précède le sous-groupe de 2-torsion de $\mathbb{C}$ est trivial, tandis que le sous-groupe de 2-torsion de $\mathbb{C}^\times$ est $\{1, -1\}$. Ces deux groupes n'étant pas isomorphes, il n'existe pas d'isomorphisme de groupes de $\mathbb{C}$ vers $\mathbb{C}^\times$.

(c) On sait que l'application $\exp\colon \mathbb{C} \to \mathbb{C}$ est à valeurs dans $\mathbb{C}^\times$ et vérifie la formule $\exp(z + z') = \exp(z)\exp(z')$; c'est donc un morphisme de groupes de $\mathbb{C}$ vers $\mathbb{C}^\times$. Il est surjectif : si z est un élément de $\mathbb{C}^\times$ d'écriture polaire $r\exp(i\theta)$ alors $z = \exp(\log r + i\theta)$; et son noyau est $2i\pi\mathbb{Z}$.

On en déduit que $z \mapsto \exp(2i\pi z)$ est un morphisme de groupes surjectif de $\mathbb{C}$ vers $\mathbb{C}^\times$, de noyau $\mathbb{Z}$. Il induit donc par passage au quotient un isomorphisme de $\mathbb{C}/\mathbb{Z}$ avec $\mathbb{C}^\times$.

Exercice 5.

(a)(a1) Comme K est distingué le produit hkh^{-1} appartient à k, et k^{-1} appartient à K qui est un sous-groupe. Donc $hkh^{-1}k^{-1} = (hkh^{-1})k^{-1}$ appartient à K (là encore parce que K est un sous-groupe).

(a2) Comme H est un sous-groupe h^{-1} appartient à H. Comme il est distingué $kh^{-1}k^{-1}$ appartient aussi à H. Par conséquent $hkh^{-1}k^{-1} = h(kh^{-1}k^{-1})$ appartient à H, là encore parce que ce dernier est un sous-groupe.

(b) Soient $(h,k) \in H \times K$. Comme H et K sont distingués, il résulte des questions précédentes que $hkh^{-1}k^{-1}$ appartient à H et à K, donc à $H \cap K$. Or $H \cap K = \{e\}$ par hypothèse, si bien que $hkh^{-1}k^{-1} = e$, ce qui signifie précisément que $hk = kh$.

Soient (h_1,k_1) et (h_2,k_2) deux éléments de $H \times K$. Notons f l'application $(h,k) \mapsto hk$ de $H \times K$ dans G. On a alors les égalités

$$\begin{aligned} f((h_1,k_1)(h_2,k_2)) &= f(h_1h_2, k_1k_2) \\ &= h_1h_2k_1k_2 \\ &= h_1(h_2k_1)k_2 \\ &= h_1(k_1h_2)k_2 \\ &= (h_1k_1)(h_2k_2) \\ &= f(h_1,k_1)f(h_2,k_2) \end{aligned}$$

et f est donc un morphisme de groupes (la première égalité provient de la définition même de la loi de groupe produit sur $H \times K$, et la troisième du fait que tout élément de H commute à tout élément de K).

Montrons que f est injectif. Soit $(h,k) \in \ker(f)$. On a alors $hk = e$, donc $h = k^{-1}$. Or $k \in K$, et k^{-1} appartient donc aussi à K qui est un sous-groupe de G. Ainsi h appartient à la fois à H et à K, donc à $H \cap K$ qui est trivial. Ainsi $h = e$, et $k = e$ aussi puisque $hk = e$. En conséquence $\ker(f) = \{(e,e)\}$ et f est injectif.

(c) L'intersection $H \cap K$ est un sous-groupe de H et un sous-groupe de K. Son cardinal divise donc $|H|$ et $|K|$; ces deux entiers étant premiers entre eux, il vient $|H \cap K| = 1$, c'est-à-dire $H \cap K = \{e\}$. La question précédente fournit alors un morphisme de groupes injectif f de $H \times K$ vers G. Mais on a par hypothèse $|G| = |H| \cdot |K|$, et donc $|G| = |H \times K|$. Le morphisme injectif f est alors bijectif pour des raisons de cardinal ; autrement dit, f est un isomorphisme de $H \times K$ vers G.