Sorbonne Université
Année universitaire 2025-2026, licence 3, *Algèbre* (UE 3M270).
Corrigé de l'examen terminal du 14 janvier 2026.

Exercice 1. Question de cours. Voir le théorème 2.11.2 du poly.

Exercice 2. Soit σ l'élément

$$(1\,6\,7\,8\,9\,2\,5\,4\,3)(3\,4\,1\,5)(1\,3\,2)$$

de S_9.

(a) On nous a donné σ sous la forme $c_1c_2c_3$ où c_1 est un 9-cycle, c_2 et 4-cycle et c_3 un 3-cycle. Il vient

$$\varepsilon(\sigma) = \varepsilon(c_1)\varepsilon(c_2)\varepsilon(c_3) = (-1)^8(-1)^3(-1)^2 = -1.$$

(b) Pour calculer l'ordre de σ, on la décompose en produit de cycles *à supports deux à deux disjoints*, à l'aide de l'algorithme vu en cours, en se rappelant que pour calculer chacune des valeurs de σ à l'aide de son écriture donnée plus haut on doit procéder ≪de droite à gauche≫. On trouve

$$\sigma = (1\,3\,5)(2\,4\,6\,7\,8\,9).$$

L'ordre de σ est alors égal au PPCM de 3 et 6, c'est-à-dire à 6.

Exercice 3.

(a) On a $84 = 7\cdot 12 = 2^2\cdot 3\cdot 7$. Si $p \notin \{2,3,7\}$ alors p ne divise pas $|G|$, si bien que G a un unique$p$-sous-groupe de Sylow (le groupe trivial) ; par conséquent,$n_p = 1$.

(b) Les théorèmes de Sylow assurent que n_2 vaut 1 modulo 2 et divise $(84/2^2) = 21$; que n_3 vaut 1 modulo 3et divise $(84/3) = 28$; et que n_7 vaut 1 modulo 7 et divise $(84/7) = 12$.

(c) L'entier n_7 vaut 1 modulo 7 et divise 12. Il est en particulier majoré par 12, si bien qu'il vaut 1 ou 8 (puisque $2\cdot 7 + 1 = 15$ est déjà trop grand) ; comme 8 ne divise pas 12 on voit que $n_7 = 1$. Ainsi G a un unique 7-sous-groupe de Sylow S. En tant qu'unique sous-groupe de G de cardinal 7 le sous-groupe S de G est distingué (et même caractéristique) ; son cardinal étant 7 il est différent de $\{e\}$ et de G.

Exercice 4. On a $260 = 26\cdot 10 = 2\cdot 13\cdot 2\cdot 5 = 2^2\cdot 5\cdot 13$. D'après le théorème de structure des groupes abéliens finis, on a une bijection entre l'ensemble des classes d'isomorphe de groupes abéliens de cardinal 260 et l'ensemble des familles finies $(d_1,\dots,d_r)$ d'entiers > 1 tels que $d_1|d_2|\dots|d_r$ et $d_1d_2\cdot d_r = 260$; à une telle famille $(d_1,\dots,d_r)$ correspond le groupe $\mathbb{Z}/d_1\mathbb{Z}\times\cdot\times\mathbb{Z}/d_r\mathbb{Z}$.

Si p est un facteur premier divisant $d_1\dots d_r = 260$ il divise l'un des d_i et donc d_r puisque d_i divise d_r. Par conséquent $2, 5$ et 13 divisent d_r, si bien que $2\cdot 5\cdot 13$ divise d_r. Il y a alors deux possibilités :

- ou bien $d_r = 2^2 \cdot 5 \cdot 13 = 260$, auquel cas $r = 1$;
- $d_r = 2 \cdot 5 \cdot 13 = 130$; dans ce cas on a nécessairement $r = 2$ et $d_1 = 2$ (notez que c'est une solution licite car $2|130$).

Il y a donc à isomorphisme près deux groupes abéliens de cardinal 260 : $\mathbb{Z}/260\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/130\mathbb{Z}$.

Exercice 5.

(a) Si $n = 0$ le seul entier m à considérer est égal à 0 aussi, et l'assertion est alors triviale (G lui-même convient).

(b) Comme $n > 0$ le groupe G est un p-groupe *non trivial*, et un théorème du cours assure alors que $\mathrm{Z}(G)$ est non trivial. Il possède donc un élément $y \neq e$. Puisque $\mathrm{Z}(G)$ est un p-groupe, y est d'ordre p^ℓ pour un certain $\ell > 0$. Mais alors $x := y^{p^{\ell-1}}$ appartient à $\mathrm{Z}(G)$ et est d'ordre p : en effet pour tout $a \in \mathbb{Z}$ on a $x^a = e$ si et seulement si $y^{p^{\ell-1}a} = e$, ce qui est le cas si et seulement si p^ℓ divise $p^{\ell-1}a$, donc si et seulement si p divise a.

(c) Soit $z \in \langle x \rangle$ et soit $g \in G$. Comme $x \in \mathrm{Z}(G)$ le groupe $\langle x \rangle$ est contenu dans $\mathrm{Z}(G)$, si bien que $gz = zg$; par conséquent gzg^{-1} est égal à z qui appartient à $\langle x \rangle$, et $\langle x \rangle$ est dès lors un sous-groupe distingué dans G.

(d) Comme x est d'ordre p le groupe $\langle x \rangle$ est de cardinal p, et $G/\langle x \rangle$ est donc de cardinal p^{n-1}. On distingue deux cas. Si $m = 0$ alors $\{e\}$ est un sous-groupe de G de cardinal p^m. Si $m > 0$ alors $m-1 \geqslant 0$, et l'hypothèse de récurrence appliquée à $G/\langle x \rangle$ assure que ce dernier possède un sous-groupe H de cardinal p^{m-1}. En tant que sous-groupe du quotient $G/\langle x \rangle$ le groupe H est de la forme $K/\langle x \rangle$ pour un unique sous-groupe K de G contenant $\langle x \rangle$. On a alors $|H| = |K|/p$, si bien que $|K| = p^m$.

Exercice 6.

(a) Supposons $G/\mathrm{Z}(G)$ cyclique. Il existe alors $g \in G$ tel que $\overline{g}$ engendre $G/\mathrm{Z}(G)$. Soient x et y deux éléments de G. Puisque $\overline{g}$ engendre $G/\mathrm{Z}(G)$ il existe deux entiers relatifs n et m tels que $\overline{x} = \overline{g}^n$ et $\overline{y} = \overline{g}^m$. Cela signifie qu'il existe h et k dans $\mathrm{Z}(G)$ tels que $x = g^n h$ et $y = g^m k$. On a alors

$$xy = g^n h g^m k = g^{n+m} hk = g^m k g^n h = yx,$$

où la deuxième et la troisième égalités proviennent du fait que h et k appartiennent à $\mathrm{Z}(G)$, donc commutent avec g et entre eux. Ainsi, G est abélien (et *a posteriori* $G/\mathrm{Z}(G)$ est le groupe trivial).

(b) Si G est abélien alors $xy = yx$ pour tout couple (x, y) d'éléments de G si bien que $p = 1$.

(c) Si n/m était inférieur ou égal à 3 le quotient $G/\mathrm{Z}(G)$ (qui est de cardinal n/m) serait de cardinal $1, 2$ ou 3, et donc serait cyclique puisque 2 et 3 sont premiers. Par la question (a) G serait alors abélien, ce qui est exclu par hypothèse. Il s'ensuit que $n/m \geqslant 4$, c'est-à-dire que $m \leqslant n/4$.

(d) On remarque que C_x est l'ensemble des éléments y de G tels que yxy^{-1} soit égal à x. C'est donc le stabilisateur de x pour l'action de G sur lui-même par conjugaison.

(e) On a

$$\begin{aligned} p &= \frac{|\{(x,y) \in G^2, xy = yx\}|}{n^2} \\ &= \frac{1}{n^2} \sum_{x \in G} |\{y \in G, xy = yx\}| \\ &= \frac{1}{n^2} \sum_{x \in G} |C_x|. \end{aligned}$$

(f) Si $x \in \mathrm{Z}(G)$ alors tout élément de G commute avec x, si bien que $C_x = G$.

(g) Soit d l'indice de C_x dans G. On a alors $|C_x| = n/d$. Si d était égal à 1 on aurait $C_x = G$, ce qui voudrait dire que tout élément de G commute avec x et donc que $x \in \mathrm{Z}(G)$, ce qui est exclu. Ainsi $d \geqslant 2$ et $|C_x| = n/d \leqslant n/2$.

(h) On a

$$\sum_{x \in G} |C_x| = \sum_{x \in \mathrm{Z}(G)} |C_x| + \sum_{x \in G \setminus \mathrm{Z}(G)} |C_x|.$$

Lorsque x appartient à $\mathrm{Z}(G)$ on a vu plus haut que $C_x = G$, ce qui entraîne que $|C_x| = n$. Comme $\mathrm{Z}(G)$ est de cardinal m, la somme $\sum_{x \in \mathrm{Z}(G)} |C_x|$ vaut nm. Par ailleurs $C_x|$ est majoré par $n/2$ lorsque x n'appartient pas à $\mathrm{Z}(G)$. La somme $\sum_{x \in G \setminus \mathrm{Z}(G)} |C_x|$ est donc majorée par $\sum_{x \in G \setminus \mathrm{Z}(G)} n/2$, qui est égal à $(n-m)(n/2)$. On a donc bien $\sum_{x \in G} |C_x| \leqslant nm + (n-m)(n/2)$.

(i) On a

$$\begin{aligned} p &= \frac{1}{n^2} \sum_{x \in G} |C_x| \\ &\leqslant \frac{nm + (n-m)(n/2)}{n^2} \\ &= \frac{(nm)/2 + n^2/2}{n^2} \\ &\leqslant \frac{n^2/8 + n^2/2}{n^2} \\ &= \frac{5n^2/8}{n^2} \\ &= \frac{5}{8}, \end{aligned}$$

où l'inégalité de la seconde ligne provient de la question précédente, et celle de la quatrième ligne de la majoration $m \leqslant n/4$ vue en (c).

(j) Supposons que $p = 5/8$. Toutes les inégalités utilisées dans les calculs de (i) sont alors des égalités. En particulier l'inégalité $(nm)/2 \leqslant n^2/8$ est une égalité

$(nm)/2 = n^2/8$ ce qui, n étant non nul (c'est le cardinal d'un groupe !) revient à dire que $m = n/4$.

Réciproquement supposons que $m = n/4$. L'inégalité $(nm)/2 \leqslant n^2/8$ est alors une égalité. Pour montrer que $p = 5/8$ il reste à s'assurer que la première inégalité du calcul de (i) est une égalité, c'est-à-dire que $\sum_{x\in G} |C_x|$ est égal à $nm + (n-m)(n/2)$. On a vu en (h) que $\sum_{x\in G} |C_x|$ est somme de $\sum_{x\in \mathrm{Z}(G)} |C_x|$, qui est égale à nm, et de $\sum_{x\in G\setminus \mathrm{Z}(G)} |C_x|$. Il suffit donc de montrer que cette dernière somme est égale à $(m-n)n/2$; comme elle comprend $(m-n)$ termes, il suffit de vérifier que $|C_x| = n/2$ pour tout $x \notin \mathrm{Z}(G)$. Fixons donc un tel x. Comme tout élément de $\mathrm{Z}(G)$ commute en particulier avec x, le centre $\mathrm{Z}(G)$ est contenu dans C_x. Il vient

$$4 = [G : \mathrm{Z}(G)] = [G : C_x][C_x : \mathrm{Z}(G)]$$

(la première égalité traduit le fait que $m = n/4$). Or puisque x n'appartient pas à $\mathrm{Z}(G)$ l'indice $[C_x : \mathrm{Z}(G)]$ est strictement supérieur à 1, et on sait que $[G : C_x]$ vaut au moins 2 puisque $|C_x| \leqslant n/2$ d'après (g). On en déduit que $[G : C_x] = [C_x : \mathrm{Z}(G)] = 2$, et partant que $|C_x| = n/2$.

Exercice 7.

(a) Soit $z \in \mathbb{C}$. Pour tout $t \in \mathbb{C}$ on a $r_u(t) = z$ si et seulement si $ut = z$, soit encore si et seulement si $t = u^{-1}z = \overline{u}z$. Et l'on a $s_u(t) = z$ si et seulement si $u\overline{t} = z$, soit encore si et seulement si $\overline{t} = u^{-1}z = \overline{u}z$, soit encore si et seulement si $t = u\overline{z}$.

Il s'ensuit que s_u est bijective de réciproque $r_{\overline{u}}$, et que s_u est bijective et est sa propre réciproque (c'est une involution).

(b) Soit $z \in \mathbb{C}$.

- ◇ On a $r_u \circ r_v(z) = u(vz) = (uv)z$; ainsi, $r_u \circ r_v = r_{uv}$.
- ◇ On a $r_u \circ s_v(z) = u(v\overline{z}) = uv\overline{z}$; ainsi, $r_u \circ s_v = s_{uv}$.
- ◇ On a $s_v \circ r_u(z) = v\overline{uz} = v\overline{u}\overline{z}$; ainsi, $s_v \circ r_u = s_{v\overline{u}}$.
- ◇ On a $s_u \circ s_v(z) = u\overline{v\overline{z}} = u\overline{v}z$; ainsi, $s_u \circ s_v = r_{u\overline{v}}$.

(c) L'ensemble G contient l'identité, qui est égale à r_1. La question (a) montre sa stabilité par inversion, et la question (b) sa stabilité par produit. C'est donc un sous-groupe de $S_{\mathbb{C}}$.

(d) Notons E l'ensemble $\{1, i, -i, -1\}$ qui peut aussi se décrire comme l'ensemble des racines quatrièmes de l'unité. Soit u un nombre complexe de module 1. Si r_u appartient à H alors $r_u(1) = u$ appartient à E. Réciproquement si u appartient à E alors pour tout $z \in E$ le nombre complexe $r_u(z) = uz$ est une racine quatrième de l'unité, et appartient donc à H. Ainsi r_u appartient à H si et seulement si u appartient à E.

Soit v un nombre complexe de module 1. Si s_v appartient à H alors $s_v(1) = v$ appartient à E. Réciproquement si v appartient à E alors pour tout $z \in E$ le nombre complexe $s_v(z) = v\overline{z}$ est une racine quatrième de l'unité, et appartient donc à H. Ainsi s_v appartient à H si et seulement si v appartient à E.

Le groupe H est donc l'ensemble $\{r_u\}_{u\in E} \cup \{s_v\}_{v\in E}$. Remarquons qu'il est de cardinal exactement 8 : en effet si $r_u = r_{u'}$ alors $u = u'$ (considérer l'image de 1), et si $s_v = s_{v'}$ alors $v = v'$ (considérer là encore l'image de 1). Et r_u ne peut jamais être égal à s_v car on aurait alors $u = v$ (considérer l'image de 1) puis $r_u(i) = ui = s_u(i) = -ui$, ce qui est absurde. Les éléments fournis par la description $\{r_u\}_{u\in E} \cup \{s_v\}_{v\in E}$ sont donc bien deux à deux distincts.

(e) Les relations vues en (b) montrent que $r_i \circ s_i = s_{-1}$ et que $s_i \circ r_i = s_1$. Comme $s_1 \neq s_{-1}$ (voir la discussion qui précède) H est non abélien.

Par ailleurs les formules de (b) montrent aussi que r_{-1} (qui est différent de $r_1 = \mathrm{Id}_{\mathbb{C}}$) commute avec tous les éléments de H. Le centre $\mathrm{Z}(H)$ est donc non trivial.

Comme H est non abélien, $\mathrm{Z}(H)$ est différent de H. La question (c) de l'exercice précédent assure alors que $|\mathrm{Z}(H)| \leqslant (8/4) = 2$. Comme $\mathrm{Z}(H)$ contient l'élément non trivial r_{-1} il est de cardinal exactement 2 et est égal à $\{\mathrm{Id}, r_{-1}\}$.

(f) Puisque $[H : \mathrm{Z}(H)]$ est exactement égal à 4, la question (j) de l'exercice précédent assure que la probabilité que deux éléments de H commutent est égale à 5/8.