UVSQ 2022/2023
Licence de sciences et technologie, santé
LSMA610 (groupes et géométrie)
23 mars 2023

Examen partiel

— durée : une heure et demie —

1 Qu'engendrent un Klein et une transposition ? [8 points]

Soit G le sous-groupe du groupe symétrique $\mathfrak{S}_4$ engendré par la transposition $t = (23)$ et par le produit $k = (12)(34)$.

1.1) Montrer que G contient le groupe de Klein, formé de l'identité et de tous les produits de transpositions à supports disjoints de $\mathfrak{S}_4$.

1.2) Trouver un 4-cycle contenu dans G et lui donner pour nom c.

1.3) Calculer le conjugué de c par t.

1.4) Montrer que tout élément de G s'écrit, de manière unique, sous la forme $t^a c^b$ où $a \in \{0, 1\}$ et $b \in \{0, 1, 2, 3\}$.

1.5) Calculer l'ordre de G.

1.6) G est-il abélien ?

1.7) G est-il distingué dans $\mathfrak{S}_4$?

2 Du côté de chez Jordan et Frobenius [12 points, ++ pour la fin]

2.1 Une inégalité de Jordan

Soient G un groupe fini et H un sous-groupe de G.

2.1) Soient $g, g' \in G$. Montrer que $gH = g'H$ si, et seulement s'il existe $h \in H$ tel que $g' = gh$.

2.2) Soient $g, g' \in G$. Montrer que si $gH = g'H$, alors $gHg^{-1} = g'Hg'^{-1}$.

2.3) On note $\mathcal{R} \subseteq G$ un système de représentants des classes à gauche modulo H. Autrement dit, pour tout $g \in G$, il existe un unique $r \in \mathcal{R}$ tel que $gH = rH$. Montrer que

$$\bigcup_{g \in G} \left(gHg^{-1} \setminus \{1\} \right) = \bigcup_{r \in \mathcal{R}} \left(rHr^{-1} \setminus \{1\} \right).$$

2.4) Déduire de ce qui précède l'*inégalité de Jordan*

$$\mathrm{Card} \left(\bigcup_{g \in G} gHg^{-1} \right) \leq |G| - [G : H] + 1 \tag{1}$$

2.5) Montrer que si $H \neq G$, alors G n'est pas la réunion des conjugués de H.

2.2 L'inégalité de Jordan est optimale

Soient $\mathbb{F}$ un corps fini de cardinal q et $\mathbb{F}^\times$ son groupe multiplicatif. Pour tous $(a, b) \in \mathbb{F}^\times \times \mathbb{F}$, on note $g_{a,b}$ l'application

$$\begin{array}{rccc} g_{a,b} : & \mathbb{F} & \longrightarrow & \mathbb{F} \\ & x & \longmapsto & ax + b. \end{array}$$

On note aussi $G = \{g_{a,b},\ a \in \mathbb{F}^\times,\ b \in \mathbb{F}\}$.

2.6) Montrer que tout élément de G est une permutation de $\mathbb{F}$.

2.7) Montrer que G est un sous-groupe du groupe symétrique $\mathfrak{S}_{\mathbb{F}}$ et calculer son ordre.

2.8) Pour tous $(a,b) \in \mathbb{F}^\times \times \mathbb{F}$, on note h_a l'*homothétie* $h_a = g_{a,0}$ et t_b la *translation* $t_b = g_{1,b}$. Montrer que les sous-ensembles

$$H = \left\{h_a,\ a \in \mathbb{F}^\times\right\} \quad \text{et} \quad T = \left\{t_b,\ b \in \mathbb{F}\right\}$$

sont des sous-groupes de G.

2.9) Les groupes H et T sont-ils distingués dans G ?

2.10) Soient $t, t' \in T$. Montrer que

$$\left(tHt^{-1}\right) \cap \left(t'Ht'^{-1}\right) \neq \{1\} \Longrightarrow t = t'.$$

2.11) En déduire que le couple (G,H) réalise l'égalité dans l'inégalité (1).

UVSQ 2022/2023
Licence de sciences et technologie, santé
LSMA610 (groupes et géométrie)
23 mars 2023

Examen partiel : un corrigé succinct

1 Qu'engendrent un Klein et une transposition ?

1.1) G contient $tkt = tkt^{-1} = (13)(24)$ et $tktk = (14)(23)$. Donc G contient K.

1.2) $c = tk = (1342)$ est un 4-cycle de G.

1.3) $tct^{-1} = (1243) = c^{-1} = c^3$.

1.4) D'abord, G est engendré par t et $k = tc$, donc par t et $c = tk$. La question précédente montre que $ct = tc^3$. Ainsi, tout produit de la forme $c^a t$, $a \in \mathbb{Z}$ s'écrit sous la forme tc^b où $b \in \mathbb{N}$ (récurrence immédiate sur $|a|$). On en déduit que tout élément de $G = \langle t, c\rangle$ s'écrit sous la forme $t^a c^b$ où $a, b \in \mathbb{Z}$. Puisque a est d'ordre 2 et c d'ordre 4, tout élément de $G = \langle t, c\rangle$ s'écrit donc sous la forme $t^a c^b$ où $a \in \{0, 1\}$ et $b \in \{0, 1, 2, 3\}$.
Il reste à montrer que cette dernière écriture est unique. Il suffit pour cela de montrer que pour tous $a \in \{0, 1\}$ et $b \in \{0, 1, 2, 3\}$, $t^a c^b = 1 \Rightarrow a = b = 0$. On suppose ainsi, sous ces hypothèses, que $t^a c^b = 1$. Alors, $t^{-a} = t^a = c^b$. Or, si $b \neq 0$, alors c^b est un 4-cycle ou un produit de transpositions disjointes. Cela oblige b à être nul, et par conséquent a aussi. On a montré l'unicité.

1.5) La question précédente montre que $|G| = \text{Card}\,\{(a, b),\ a \in \{0, 1\},\ b \in \{0, 1, 2, 3\}\} = 8$.

1.6) La réponse est non puisque t et c ne commutent pas (question **2.3)**).

1.7) La réponse est non. En effet, s'il était normal, il contiendrait tous les conjugués de t, donc toutes les transpositions de $\mathfrak{S}_4$. Comme $\mathfrak{S}_4$ est engendré par ses transpositions, on aurait $G = \mathfrak{S}_4$ ce qui n'est pas pour des raisons d'ordre.

2 Du côté de chez Jordan et Frobenius [12 points]

2.1 Une inégalité de Jordan

2.1) Si $gH = g'H$, alors $g' \in gH$ et donc il existe $h \in H$ tel que $g' = gh$. Inversement, si $g' = gh$ avec $h \in H$, alors les classes à gauche $g'H$ et gH contiennent toutes les deux g'. Or, deux classes à gauches sont égales ou disjointes, puisque ce sont des classes d'équivalence. Donc $gH = g'H$.

2.2) On suppose que $gH = g'H$. Soit ainsi $h \in H$ tel que $g' = gh$. Alors, $g'Hg'^{-1} = g(hHh^{-1})g^{-1} = gHg^{-1}$.

2.3) La question précédente montre que si $gH = rH$, alors $gHg^{-1} \setminus \{1\} = rHr^{-1} \setminus \{1\}$. L'égalité en découle immédiatement pour de simples raisons ensemblistes.

2.4) En passant aux cardinaux, l'égalité précédente s'écrit

$$\text{Card}\left(\bigcup_{g\in G} gHg^{-1} \setminus \{1\}\right) = \text{Card}\left(\bigcup_{r\in\mathcal{R}} rHr^{-1} \setminus \{1\}\right) \leq \sum_{r\in\mathcal{R}} \text{Card}\left(rHr^{-1} \setminus \{1\}\right).$$

Or, $\text{Card}\left(rHr^{-1} \setminus \{1\}\right) = |H| - 1$, pour tout $r \in \mathcal{R}$ et, par ailleurs, $\text{Card}\,\mathcal{R} = [G : H] = \frac{|G|}{|H|}$, ce qui entraîne que $\sum_{r\in\mathcal{R}} \text{Card}\left(rHr^{-1} \setminus \{1\}\right) = \frac{|G|}{|H|}(|H| - 1)$. En remarquant que $\bigcup_{g\in G}\left(gHg^{-1} \setminus \{1\}\right) = \left(\bigcup_{g\in G} gHg^{-1}\right) \setminus \{1\}$, l'inégalité de Jordan est démontrée.

2.5) Si $H \neq G$, alors $[G : H] \geq 2$ et donc, d'après l'inégalité de Jordan, le cardinal de la réunion des conjugués de H est inférieur ou égal à $|G| - 2 + 1 = |G| - 1$, ce qui montre que cette réunion n'emplit pas G tout entier.

2.2 L'inégalité de Jordan est optimale

Soient $\mathbb{F}$ un corps fini de cardinal q et $\mathbb{F}^\times$ son groupe multiplicatif. Pour tous $(a,b) \in \mathbb{F}^\times \times \mathbb{F}$, on note $g_{a,b}$ l'application

$$\begin{array}{rccc} g_{a,b} : & \mathbb{F} & \longrightarrow & \mathbb{F} \\ & x & \longmapsto & ax+b. \end{array}$$

On note aussi $G = \{g_{a,b},\ a \in \mathbb{F}^\times,\ b \in \mathbb{F}\}$.

2.6) Si $x, y \in \mathbb{F}$, alors $y = ax + b$ si, et seulement si $x = \frac{y}{a} - \frac{b}{a}$. Ainsi, $g_{a,b}$ est bijective et $g_{a,b}^{-1} = g_{\frac{1}{a},-\frac{b}{a}}$.

2.7) G n'est évidemment pas vide ; d'ailleurs, $\mathrm{id}_{\mathbb{F}} = g_{1,0}$. Le calcul précédent montre que G est stable par passage à l'inverse. Enfin, $g_{a,b} \circ g_{c,d} = g_{ac,ad+b}$ (calcul immédiat), ce qui montre que G est stable pour la composition. On a montré que G est un sous-groupe de $\mathfrak{S}_{\mathbb{F}}$.
Pour calculer l'ordre de G, il s'agit de savoir à quelle condition on peut avoir $g_{a,b} = g_{c,d}$. Or, $g_{a,b} = g_{c,d}$ si, et seulement si $ax + b = cx + d$, pour tout $x \in \mathbb{F}$; pour $x = 0$, cela impose que $b = d$; ensuite, pour $x = 1$, on obtient que $a = c$. On a montré que $g_{a,b} = g_{c,d}$ si, et seulement si $a = c$ et $b = d$.
Il ne reste plus qu'à calculer l'ordre de G :

$$|G| = \mathrm{Card}\left\{(a,b), a \in \mathbb{F}^\times,\ b \in \mathbb{F}\right\} = q(q-1).$$

2.8) Les formules immédiates $h_a h_b = h_{ab}$ et $(h_a)^{-1} = h_{\frac{1}{a}}$ montrent que H est un sous-groupe de G. De même, T est un sous-groupe de G puisque $t_a t_b = t_{a+b}$ et $(t_a)^{-1} = t_{-a}$.

2.9) La formule immédiate $t_b h_a t_b^{-1} = g_{a,b(1-a)}$ montre que H n'est pas distingué, à moins que $\mathbb{F} = \mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ auquel cas H est réduit à $\{\mathrm{id}_{\mathbb{F}}\}$.
La formule $g_{a,b} = t_b h_a$ montre que G est engendré par H et T. Ainsi, la formule $h_a t_b h_a^{-1} = t_{ab}$ suffit à montrer que T est un sous-groupe normal de G.

2.10) On suppose que $t_b H t_b^{-1}$ et $t'_b H t'^{-1}_b$ ont un élément commun non trivial. Soient donc $a, a' \in \mathbb{F} \setminus \{0,1\}$ tels que $t_b h_a t_b^{-1} = t'_b h_{a'} t'^{-1}_b$, ce qui s'écrit encore $g_{a,b(1-a)} = g_{a',b'(1-a')}$. Alors, $a = a'$ et $(b'-b)(1-a) = 0$. Comme $a \neq 1$, cela entraîne que $b = b'$, ce qu'il fallait démontrer.

2.11) On note $u = \mathrm{Card}\left(\bigcup_{g\in G} gHg^{-1}\right)$. D'un côté, puisque $[G : H] = q$, la formule de Jordan montre que

$$u \leq |G| - [G:H] + 1 = q(q-1) - q + 1 = (q-1)^2.$$

De l'autre, $u \geq \mathrm{Card}\left(\bigcup_{t\in T} tHt^{-1}\right)$. La question précédente montre que l'union $\bigcup_{t\in T}\left(tHt^{-1} \setminus \{1\}\right)$ est disjointe. Ainsi,

$$u \geq 1 + \sum_{t\in T}\left(\left|tHt^{-1}\right| - 1\right) = 1 + q(q-2) = (q-1)^2.$$

En regroupant les deux inégalités sur u, on obtient que

$$u = (q-1)^2 = \mathrm{Card}\left(\bigcup_{g\in G} gHg^{-1}\right) = |G| - [G:H] + 1,$$

QED.

UVSQ 2023/2024
Licence de sciences et technologie, santé
LSMA610 (groupes et géométrie)
22 mars 2024

Examen partiel

– durée : une heure et demie –

— Bon, il faut l'écrire : aucun document ni aucun instrument électronique n'est autorisé pour cette épreuve —

1 Six-cycles de $\mathfrak{S}_6$ [4 points]

Montrer que le groupe $\mathfrak{S}_6$ des permutations de $\{1,2,3,4,5,6\}$ est engendré par ses 6-cycles.

2 Affines [8 points]

Soient $\mathbb{F}$ un corps (commutatif) et V un espace vectoriel sur $\mathbb{F}$. On note comme toujours $\mathfrak{S}_V$ le groupe des permutations de V et $\mathrm{GL}(V)$ le sous-groupe de $\mathfrak{S}_V$ formé des permutations linéaires de V. Pour tout $v \in V$, on note t_v la *translation de vecteur* v, qui est définie par

$$\forall w \in V,\ t_v(w) = v + w.$$

Une remarque : chacun verra du premier coup d'œil qu'hormis l'identité, une translation n'est jamais linéaire. On note $T(V)$ l'ensemble des translations de V.

2.1) Préliminaire
Soient G un groupe, N et Q deux sous-groupes de G. On suppose que N est distingué. Montrer que l'ensemble

$$NQ = \{nq,\ (n,q) \in N \times Q\}$$

est un sous-groupe de G.

2.2) Montrer que $T(V)$ est un sous-groupe de $\mathfrak{S}_V$ isomorphe au groupe additif $(V,+)$.

2.3) On note $\mathrm{GA}(V)$ le sous-groupe de $\mathfrak{S}_V$ engendré par $T(V)$ et $\mathrm{GL}(V)$. Montrer que $T(V)$ est un sous-groupe distingué de $\mathrm{GA}(V)$.

2.4) Montrer que $\mathrm{GA}(V) = \{t \circ f,\ t \in T(V),\ f \in \mathrm{GL}(V)\}$.

2.5) L'écriture $t \circ f$ d'un élément de $\mathrm{GA}(V)$ comme composée d'une translation et d'un automorphisme linéaire est-elle unique ?

2.6) Montrer que si p est un nombre premier, le groupe $\mathfrak{S}_p$ des permutations de $\{1,\ldots,p\}$ contient un sous-groupe d'ordre $p(p-1)$.

3 Conjugués vs isomorphes [8 points]

Pour tout entier naturel non nul, on note $\mathfrak{S}_n$ le groupe des permutations de l'ensemble $\{1,\ldots n\}$ et $\mathfrak{A}_n$ son sous-groupe des permutations paires.

3.1) On note

$$F = \{\sigma \in \mathfrak{S}_6,\ \sigma(5) = 5 \text{ et } \sigma(6) = 6\}.$$

C'est évidemment un sous-groupe de $\mathfrak{S}_6$, on ne demande pas de montrer cela.

(i) Montrer que $\{1,2,3,4\}$ est stable par tout élément de F.

(ii) Expliciter un isomorphisme de groupes entre F et $\mathfrak{S}_4$.

3.2) On note $I : \mathfrak{S}_6 \to \{0,1\}$ la fonction indicatrice du complémentaire de $\mathfrak{A}_6$ dans $\mathfrak{S}_6$. Autrement dit,

$$\forall \sigma \in \mathfrak{S}_6,\ I(\sigma) = \begin{cases} 0 \text{ si } \sigma \in \mathfrak{A}_6 \\ 1 \text{ si } \sigma \notin \mathfrak{A}_6. \end{cases}$$

On note également

$$G = \left\{ \sigma \circ (56)^{I(\sigma)},\ \sigma \in F \right\},$$

où (56) désigne comme d'habitude la transposition de $\mathfrak{S}_6$ qui échange les nombres 5 et 6.

(i) Montrer que $I(\sigma\tau) = I(\sigma) + I(\tau)$ [mod 2] pour tous $\sigma, \tau \in \mathfrak{S}_6$.

(ii) Montrer que G est un sous-groupe de $\mathfrak{S}_6$.

(iii) L'application

$$\begin{array}{rccc} \Phi : & F & \longrightarrow & G \\ & \sigma & \longmapsto & \sigma \circ (56)^{I(\sigma)} \end{array}$$

est-elle un isomorphisme de groupes ?

3.3) Les groupes F et G sont-ils conjugués dans $\mathfrak{S}_6$?

3.4) [Hors barème] Prolonger ce qui précède en montrant que pour tout $n \geq 2$, le groupe $\mathfrak{S}_{n+2}$ contient au moins deux classes de conjugaison de sous-groupes isomorphes à $\mathfrak{S}_n$.

UVSQ 2023/2024
Licence de sciences et technologie, santé
LSMA610 (groupes et géométrie)
22 mars 2024

Examen partiel : un corrigé succinct

1 Six-cycles de $\mathfrak{S}_6$

On note S le sous-groupe de $\mathfrak{S}_6$ engendré par les 6-cycles. Le conjugué d'un 6-cycle est un 6-cycle. Donc S est un sous-groupe distingué de $\mathfrak{S}_6$. Or, les sous-groupes distingués de $\mathfrak{S}_6$ sont le groupe trivial, le groupe alterné $\mathfrak{A}_6$ et $\mathfrak{S}_6$. Puisque S contient les 6-cycles, il n'est pas trivial. Comme les 6-cycles sont des permutations impaires, S n'est pas contenu dans $\mathfrak{A}_6$. Donc $S = \mathfrak{S}_6$.

2 Affines

2.1) L'ensemble NQ, bien sûr, n'est pas vide. Soient $n, n' \in N$ et $q, q' \in Q$. Puisque N est normal, soit $n'' \in N$ tel que $qn' = n''q$. Alors, $nqn'q' = (nn'')(qq')$, ce qui montre que NQ est stable pour la loi de G. Par ailleurs, toujours par normalité de N, soit $n''' \in N$ tel que $q^{-1}n^{-1} = n'''q^{-1}$; alors, $(nq)^{-1} = q^{-1}n^{-1} = n'''q^{-1} \in NQ$: on a montré que NQ est stable par passage à l'inverse. Tout cela suffit à prouver que NQ est un sous-groupe de G.

2.2) Un calcul immédiat montre que $t_v \circ t_w = t_{v+w}$, pour tous $v, w \in V$. En particulier, t_v est bijective et $(t_v)^{-1} = t_{-v}$. Ainsi, $T(V)$ est contenu dans $\mathfrak{S}_V$ et en est un sous-groupe. En outre, la même formule montre que l'application $(V, +) \to (T(V), \circ)$, $v \mapsto t_v$ est un homomorphisme de groupes. On montre que ce dernier est bijectif par exemple en exhibant sa réciproque : c'est $T(V) \to V$, $t \mapsto t(0)$.

2.3) Par le théorème de caractérisation des sous-groupes engendrés, puisque $\mathrm{GA}(V)$ est engendré par $T(V)$ et $\mathrm{GL}(V)$, tout élément de $\mathrm{GA}(V)$ est un produit d'éléments de $T(V)$ et d'éléments de $\mathrm{GL}(V)$. Conjuguer une translation par un tel produit revient donc à la conjuguer successivement par des translations et des éléments de $\mathrm{GL}(V)$. Or, conjuguer une translation par une translation donne encore une translation (d'ailleurs, cela ne produit rien puisque les translations commutent). Il suffit ainsi, pour montrer que $T(V)$ est distingué dans $\mathrm{GA}(V)$, de montrer que le conjugué d'une translation par une application linéaire est encore une translation.
Soient donc $v \in V$ et $f \in \mathrm{GL}(V)$. Alors, pour tout $w \in V$, $ft_vf^{-1}(w) = f\left(f^{-1}(w) + v\right) = f\left(f^{-1}(w)\right) + f(v) = w + f(v)$. Cela montre que $ft_vf^{-1} = t_{f(v)} \in T(V)$ et donc que $T(V)$ est un sous-groupe normal de $GA(V)$.

2.4) On note $\mathcal{G} = \{t \circ f,\ t \in T(V),\ f \in \mathrm{GL}(V)\}$. Avec les notations de la question **2.1)**, $\mathcal{G} = T(V)\,\mathrm{GL}(V)$; toujours grâce à la question **2.1)**, ce dernier est donc un sous-groupe de $\mathrm{GA}(V)$ puisque $T(V)$ est distingué dans $\mathrm{GA}(V)$. Ainsi, $\mathcal{G}$ est un sous-groupe de $\mathrm{GA}(V)$ qui contient (évidemment) $T(V)$ et $\mathrm{GL}(V)$; par minimalité des sous-groupes engendrés, $\mathcal{G}$ contient $\mathrm{GA}(V)$ tout entier. Donc $\mathcal{G} = \mathrm{GA}(V)$.

2.5) On suppose que $t_1f_1 = t_2f_2$ où $t_1, t_2 \in T(V)$ et $f_1, f_2 \in \mathrm{GL}(V)$. Alors, $t_2^{-1}t_1 = f_2f_1^{-1}$ est à la fois une translation et une application linéaire : c'est l'identité de V, ce qui montre que $t_1 = t_2$ et $f_1 = f_2$. La réponse est oui.

2.6) Puisque p est premier, l'anneau $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ est un corps. On prend pour V la droite vectorielle $\mathbb{F}_p$ sur le corps $\mathbb{F}_p$. Son groupe $\mathrm{GA}(\mathbb{F}_p)$ jouit de l'existence et de l'unicité de l'écriture de ses éléments vues en **2.4)** et **2.5)**. Donc l'ordre de $\mathrm{GA}(\mathbb{F}_p)$ est les produit des ordres de $T(\mathbb{F}_p)$ et de $\mathrm{GL}(\mathbb{F}_p)$. Or, ces derniers sont respectivement p et $p-1$. Donc $|\mathrm{GA}(\mathbb{F}_p)| = p(p-1)$, ce qu'il fallait démontrer.

[Pour aller plus loin : si p est un nombre premier et d un entier naturel non nul, le groupe $\mathfrak{S}_{p^d}$ contient un sous-groupe d'ordre $p^d(p^d-1)$. Appliquer ce qui précède en considérant le corps $\mathbb{F}_{p^d}$ comme droite vectorielle sur lui-même. Ce résultat ne s'étend pas à tous les entiers : il est faux que $\mathfrak{S}_n$ contient toujours un sous-groupe d'ordre $n(n-1)$. Par exemple, c'est faux pour $\mathfrak{S}_6$ qui ne contient pas de sous-groupe d'ordre 30. Pour voir cela, on peut montrer, avec théorie de Sylow par exemple, qu'un groupe d'ordre 30 contient toujours un élément d'ordre 15 — il n'y a que quatre groupes d'ordre 30 qui sont le cyclique, D_{30}, $\mathbb{Z}/3\mathbb{Z} \times D_{10}$ et $\mathbb{Z}/5\mathbb{Z} \times D_6$ où D_{2n} est le groupe diédral d'ordre $2n$ — alors que $\mathfrak{S}_6$ lui-même n'en a pas.]

3 Conjugués vs isomorphes [8 points]

3.1) (i) Soit $\sigma \in F$. Puisque σ est injectif, l'image de $\{1,2,3,4\}$ ne contient pas 5 et 6 qui sont respectivement les images de 5 et 6. Donc $\sigma(\{1,2,3,4\}) \subseteq \{1,2,3,4\}$ — il y a même égalité puisque $\{1,2,3,4\}$ est un ensemble fini.

(ii) Si $\sigma \in F$, la restriction de σ à $\{1,2,3,4\}$ induit une permutation de $\{1,2,3,4\}$ que l'on note $\widetilde{\sigma} \in \mathfrak{S}_4$: pour tout $k \in \{1,2,3,4\}$, $\widetilde{\sigma}(k) = \sigma(k)$. Inversement, tout élément τ de $\mathfrak{S}_4$ se prolonge en un élément $\widehat{\tau}$ de F en fixant 5 et 6 : si $k \in \{1,2,3,4\}$, $\widehat{\tau}(k) = \tau(k)$ et si $k \in \{5,6\}$, $\widehat{\tau}(k) = k$. Que $F \to \mathfrak{S}_4$, $\sigma \to \widetilde{\sigma}$ soit un homomorphisme de groupes est parfaitement élémentaire. Que les applications $\sigma \mapsto \widetilde{\sigma}$ et $\tau \mapsto \widehat{\tau}$ soient des bijections réciproques l'une de l'autre ne l'est pas moins. Ainsi, $\widetilde{\cdot}$ est un isomorphisme de groupes entre F et $\mathfrak{S}_4$.

3.2) (i) Soient $s,t \in \mathfrak{S}_6$. Si s et t sont paires, st l'est aussi et $I(st) = 0 = I(s) + I(t)$. Si s est paire et t impaire, st est impaire et $I(st) = 1 = I(s) + I(t)$. Enfin, si s et t sont impaires, st est paire et $I(st) = 0$ alors que $I(s) + I(t) = 2 = 0$ [mod 2]. Dans tous les cas, $I(st) = I(s) + I(t)$ [mod 2].

(ii) Si $\sigma \in F$, son support est disjoint de celui de la transposition (56) si bien que σ et (56) commutent. Soient s et t dans F. Alors, $s(56)^{I(s)}t(56)^{I(t)} = st(56)^{I(s)+I(t)}$. Mais puisque (56) est d'ordre 2, d'après la question précédente, $(56)^{I(s)+I(t)} = (56)^{I(st)}$. Ainsi, $s(56)^{I(s)}t(56)^{I(t)} = st(56)^{I(st)} \in G$: on a montré que G est stable pour la composition. Enfin, l'inverse de $s(56)^{I(s)}$ est $(56)^{-I(s)}s^{-1} = s^{-1}(56)^{I\left(s^{-1}\right)} \in G$, la dernière égalité venant du fait que $I(1) = 0$, et donc que $I\left(s^{-1}\right) + I(s) = 0$ [2] : on a montré que G est stable pour le passage à l'inverse. Comme G est évidemment non vide, tout cela suffit à prouver que G est un sous-groupe de $\mathfrak{S}_6$.

(iii) Le calcul précédent montre aussi que Φ est un homomorphisme de groupes. Par définition de G, il est surjectif. Si s est dans son noyau, alors $s = (56)^{I(s)}$; Le support de s est ainsi dans l'intersection de $\{1,2,3,4\}$ et de $\{5,6\}$: il est vide, ce qui signifie que $s = 1$. on a prouvé que Φ est injectif : la réponse est oui.

3.3) Par construction, G est un sous-groupe de $\mathfrak{A}_6$; donc tous ses conjugués sont aussi des sous-groupes de $\mathfrak{A}_6$. Or, ce n'est pas le cas de F qui contient par exemple la transposition (12). Donc F et G ne sont pas conjugués dans $\mathfrak{S}_6$.

3.4) Toute la construction précédente s'étend à $\mathfrak{S}_{n+2}$ en notant $F \simeq \mathfrak{S}_n$ le fixateur de $n+1$ et $n+2$ dans $\mathfrak{S}_{n+2}$ et G le sous-groupe de $\mathfrak{S}_{n+2}$ obtenu à partir de F en compensant la négativité des éléments de F par composition par la transposition $(n+1, n+2)$. Là encore, F et G sont isomorphes alors que G est un sous-groupe de $\mathfrak{A}_{n+2}$, l'empêchant d'être conjugué à F.

UVSQ 2024/2025
Licence de sciences et technologie, santé
LSMA610 (groupes et géométrie)
21 mars 2025

Examen partiel

– durée : une heure sept minutes et trente secondes –

— Bon, il faut l'écrire : aucun document ni aucun instrument électronique n'est autorisé pour cette épreuve —

1 Ce qu'engendrent une transposition et un 4-cycle [11 points]

Pour tout entier naturel non nul, on note $\mathfrak{S}_n$ le groupe symétrique de l'ensemble $\{1, 2, \ldots, n\}$. Si $1 \leq k \leq n$ et si $a_1, \ldots, a_k$ sont k éléments distincts de $\{1, 2, \ldots, n\}$, on note $(a_1, \ldots, a_k)$ le k-cycle de $\mathfrak{S}_n$ habituel.

On pourra utiliser le résultat suivant, exercice du cours : *pour tout $n \geq 2$, le groupe $\mathfrak{S}_n$ est engendré par les $n-1$ transpositions* $(12), (23), \cdots, (n-1, n)$.

1.1) Soit A le sous-groupe de $\mathfrak{S}_4$ engendré par la transposition (12) et le 4-cycle (1234). Montrer que A contient les transpositions (23) et (34). En déduire que $A = \mathfrak{S}_4$.

1.2) Soit B le sous-groupe de $\mathfrak{S}_4$ engendré par la transposition (12) et le 4-cycle (1324).

(i) Calculer la décomposition du produit (12)(1324) en produit de cycles à supports disjoints.

(ii) On note $K = \{1, (12)(34), (13)(24), (14)(23)\}$ le groupe de Klein. Montrer que K est un sous-groupe distingué de B.

(iii) Montrer que les classes de (12) et de (1324) dans le groupe-quotient B/K sont inverses l'une de l'autre.

(iv) En déduire que B est d'ordre 8.

1.3) Soit C le sous-groupe de $\mathfrak{S}_5$ engendré par la transposition (12) et le 4-cycle (2345). Montrer que $C = \mathfrak{S}_5$.

1.4) Soit D le sous-groupe de $\mathfrak{S}_6$ engendré par la transposition (12) et le 4-cycle (3456).

(i) Montrer que D est un groupe abélien, isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

(ii) Le groupe D est-il cyclique ?

1.5) Déduire soigneusement des questions précédentes que lorsque $n \geq 6$, le sous-groupe de $\mathfrak{S}_n$ engendré par une transposition et un 4-cycle est soit d'ordre 8, soit isomorphe à $\mathfrak{S}_4$, soit isomorphe à $\mathfrak{S}_5$.

1.6) Les groupes B et D, tous les deux d'ordre 8, sont-ils isomorphes ?

2 Centralisateurs dans SL_2 [9 points]

On note $\mathrm{GL}(2, \mathbb{C})$ le groupe multiplicatif des matrices à deux lignes et deux colonnes, à coefficients complexes, inversibles. On note aussi $\mathrm{SL}(2, \mathbb{C})$ son sous-groupe des matrices de déterminant 1. On note I_2 le neutre de $\mathrm{GL}(2, \mathbb{C})$. Pour tout $M \in \mathrm{SL}(2, \mathbb{C})$, on note $Z(M)$ le *centralisateur* de M dans $\mathrm{SL}(2, \mathbb{C})$, à savoir

$$Z(M) = \{N \in \mathrm{SL}(2, \mathbb{C}),\ MN = NM\}.$$

2.1) Montrer que $Z(M)$ est un sous-groupe de $\mathrm{SL}(2, \mathbb{C})$, pour tout $M \in \mathrm{SL}(2, \mathbb{C})$.

2.2) Montrer que pour tout $M \in \mathrm{SL}(2, \mathbb{C})$ et pour tout $P \in \mathrm{GL}(2, \mathbb{C})$, on a l'égalité

$$Z\left(PMP^{-1}\right) = PZ(M)P^{-1}.$$

2.3) [Question bonus, hors barème, dont on pourra utiliser le résultat]
Montrer que tout élément de $\mathrm{SL}(2,\mathbb{C})$ est semblable à une matrice de l'une des cinq formes suivantes :

$$\pm I_2,\ \pm\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix},\ \begin{pmatrix}a & 0\\ 0 & 1/a\end{pmatrix} \text{ où } a\in\mathbb{C}\setminus\{-1,0,1\}$$

— on pourra raisonner sur le polynôme caractéristique.

2.4) Montrer que le centralisateur de $T=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$ est $Z(T)=\left\{\pm\begin{pmatrix}1 & \alpha\\ 0 & 1\end{pmatrix},\ \alpha\in\mathbb{C}\right\}$.

2.5) Soit $a\in\mathbb{C}\setminus\{0\}$. Calculer le centralisateur de $\begin{pmatrix}a & 0\\ 0 & 1/a\end{pmatrix}$.

2.6) On note $\mathbb{C}$ le groupe additif $(\mathbb{C},+)$ et $\mathbb{C}^\times$ le groupe multiplicatif $(\mathbb{C}\setminus\{0\},\times)$. On note aussi $S=\begin{pmatrix}i & 0\\ 0 & -i\end{pmatrix}$.
Montrer que $Z(T)$ est isomorphe au groupe $\mathbb{Z}/2\mathbb{Z}\times\mathbb{C}$ et que $Z(S)$ est isomorphe à $\mathbb{C}^\times$.

2.7) Déduire des questions précédentes que $Z(M)$ est un groupe abélien, pour tout $M\in\mathrm{SL}(2,\mathbb{C})\setminus\{-I_2,I_2\}$.

UVSQ 2024/2025
Licence de sciences et technologie, santé
LSMA610 (groupes et géométrie)
21 mars 2025

Examen partiel : un corrigé succinct

1 Ce qu'engendrent une transposition et un 4-cycle [11 points]

1.1) On note $c = (1234) \in \mathfrak{S}_4$. Le groupe A contient $c(12)c^{-1} = (23)$ et $c^2(12)c^{-2} = (34)$. Il contient donc le sous-groupe de $\mathfrak{S}_4$ engendré par les transpositions (12), (23) et (34) qui est $\mathfrak{S}_4$ lui-même. Donc $A = \mathfrak{S}_4$.

1.2) (i) Calcul immédiat : $(12)(1324) = (13)(24)$.

(ii) Le calcul précédent montre que $(13)(24) \in B$. En conjuguant ce dernier par (12), on obtient (14)(23) ; donc $(14)(23) \in B$. Comme (13)(24) et (14)(23) engendrent K, cela montre que K est un sous-groupe de B. Enfin, K est un sous-groupe distingué de $\mathfrak{S}_4$, donc de B.

(iii) Puisque $K \lhd B$, on a un groupe-quotient B/K. Puisque $(12)(1324) = (13)(24) \in K$, le produit des classes de (12) et de (1324) est trivial dans le quotient B/K.

(iv) Puisque B est engendré par (12) et (1324), il est aussi engendré par (12) et $(12)(1324)$. Ainsi, B est engendré par (12) et par un élément de K, ce qui entraîne que la classe de (12) dans le quotient B/K engendre B/K ; en outre, cette classe est d'ordre 2 puisque (12) est d'ordre 2 dans B et puisque $(12) \notin K$. Ainsi, le groupe B/K est d'ordre 2. Comme K est d'ordre 4, cela entraîne que B est d'ordre 8.

1.3) Le groupe C contient le 5-cycle $d = (12)(2345) = (12345)$ Ainsi, C contient les conjugués de (12) par les d^k, $0 \leq k \leq 3$, à savoir les transpositions (12), (23), (34), (45). Donc C contient le groupe que ces quatre transpositions engendrent : $C = \mathfrak{S}_5$.

1.4) (i) On note $e = (3456) \in \mathfrak{S}_6$. Puisque leurs supports sont disjoints, les permutations $t = (12)$ et e commutent. Cela montre immédiatement que le groupe $D = \langle t, e \rangle$ est abélien. En outre, puisque t est d'ordre 2 et e d'ordre 4, la caractérisation des sous-groupes (abéliens) engendrés montre que $D = \left\{ t^a e^b,\ a \in \{0,1\},\ 0 \leq b \leq 3 \right\}$. En outre, puisque les supports de t et de e sont disjoints, l'écriture sous la forme $t^a e^b$ avec $a \in \{0,1\}$ et $0 \leq b \leq 3$ est unique puisque c'est *la* décomposition de ce produit en cycles à supports disjoints. Cela montre que $|D| = 8$.

Enfin, le théorème de décomposition des groupes abéliens finis en facteurs invariants (ou en composantes primaires) montre que tout sous-groupe abélien d'ordre 8 est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^3$, à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ ou à $\mathbb{Z}/8\mathbb{Z}$. Comme D contient un élément d'ordre 4 (e, par exemple), il n'est pas isomorphe à $(\mathbb{Z}/2\mathbb{Z})^3$. Comme D n'a pas d'élément d'ordre 8, il n'est pas isomorphe à $\mathbb{Z}/8\mathbb{Z}$. Donc il est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

NB : on pouvait aussi montrer directement que l'application $\mathbb{Z} \times \mathbb{Z} \to D$, $(a,b) \mapsto t^a e^b$ est un homomorphisme de groupes qui induit un isomorphisme de groupes $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \to D$.

(ii) On l'a déjà dit : la décomposition des éléments de D sous la forme $t^a e^b$ montre que les éléments de D sont d'ordre 1, 2 ou 4. Comme D est d'ordre 8, il n'est donc pas cyclique.
On peut aussi invoquer le théorème d'unicité des facteurs invariants qui assure notamment que $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/8\mathbb{Z}$ ne sont pas isomorphes.

1.5) Soit $n \geq 6$ et G un sous-groupe de $\mathfrak{S}_6$ engendré par une transposition τ et un 4-cycle σ. Quitte à conjuguer G (ou à renuméroter l'ensemble $\{1, 2, \ldots, n\}$, ce qui revient au même), on peut supposer que $\tau = (12)$. On raisonne alors sur l'intersection des supports de τ et de σ. On note S le support de σ.

Si $S \cap \{1,2\} = \emptyset$, quitte à conjuguer G, on peut supposer que $\sigma = (3456)$. Alors, $G = D$ est d'ordre 8.

Si l'intersection de S et de $\{1,2\}$ est un singleton, quitte à conjuguer G, on peut supposer que $S \cap \{1,2\} = \{2\}$ et que $\sigma = (2345)$. Alors, $G = C \simeq \mathfrak{S}_5$.

Enfin, si $\{1,2\} \subseteq S$, deux cas se présentent.
• Ou bien 1 et 2 sont consécutifs dans l'écriture de σ (ce qui signifie que $2 = \sigma(1)$ ou que $2 = \sigma^3(1)$), alors, quitte à conjuguer G, on peut supposer que $\sigma = (1234)$. Alors, $G = A \simeq \mathfrak{S}_4$.
• Ou bien 1 et 2 en sont pas consécutifs dans l'écriture de σ (ce qui signifie que $2 = \sigma^2(1)$), alors, quitte à conjuguer G, on peut supposer que $\sigma = (1324)$. Alors, $G = B$ est d'ordre 8.

On a montré que G est soit d'ordre 8, soit isomorphe à $\mathfrak{S}_4$, soit isomorphe à $\mathfrak{S}_5$.

1.6) Les groupes B et D ne sont pas isomorphes car D est abélien alors que (12) et (1324), qui sont dans B, ne commutent pas : $(12)(1324) = (13)(24)$ alors que $(1324)(12) = (14)(23)$.

2 Centralisateurs dans SL_2 [9 points]

2.1) Soit $M \in \mathrm{SL}(2,\mathbb{C})$. Puisque I_2 est évidemment dans $Z(M)$ qui n'est donc pas vide, il suffit de montrer que $Z(M)$ est stable pour la multiplication des matrices et par le passage à l'inverse. Soient $P, Q \in Z(M)$. D'une part, $(PQ)M = P(QM) = P(MQ) = (PM)Q = (MP)Q = M(PQ)$, ce qui prouve que $PQ \in Z(M)$. D'autre part, en multipliant l'égalité $PM = MP$ par P^{-1} à droite et à gauche, on obtient que $MP^{-1} = P^{-1}M$, ce qui prouve que $P^{-1} \in Z(M)$.

2.2) Soient $M \in \mathrm{SL}(2,\mathbb{C})$ et $P \in \mathrm{GL}(2,\mathbb{C})$. Alors, c'est une première remarque, $PMP^{-1} \in \mathrm{SL}(2,\mathbb{C})$, ce qui donne du sens à la question.
• D'une part, soit $Q \in Z\left(PMP^{-1}\right)$. Alors,

$$\left(P^{-1}QP\right)M = P^{-1}Q\left(PMP^{-1}\right)P = P^{-1}\left(PMP^{-1}\right)QP = M\left(P^{-1}QP\right).$$

Cela montre que $P^{-1}QP \in Z(M)$ ce qui implique, en multipliant par P à gauche et par P^{-1} à droite, que $Q \in PZ(M)P^{-1}$. On a prouvé l'inclusion $Z\left(PMP^{-1}\right) \subseteq PZ(M)P^{-1}$.
• D'autre part, soit $Q \in Z(M)$. Alors,

$$\left(PQP^{-1}\right)\left(PMP^{-1}\right) = P(QM)P^{-1} = P(MQ)P^{-1} = \left(PMP^{-1}\right)\left(PQP^{-1}\right).$$

Cela montre que $PQP^{-1} \in Z\left(PMP^{-1}\right)$. On a prouvé l'inclusion $Z\left(PMP^{-1}\right) \supseteq PZ(M)P^{-1}$.

NB : à vrai dire, dans le langage des actions de groupes, c'est une application directe du cours. En effet, $Z(M)$ est le groupe d'isotropie M sous de l'action de $\mathrm{GL}(2,\mathbb{C})$ sur $\mathrm{SL}(2,\mathbb{C})$ par conjugaison. Vu sous cet angle, il suffit d'appliquer la proposition qui affirme que deux éléments d'une même orbite ont des sous-groupes d'isotropie conjugués : avec les notations présentes, $Z\left(PMP^{-1}\right) = \mathrm{GL}(2,\mathbb{C})_{P\cdot M} = P\,\mathrm{GL}(2,\mathbb{C})_M\,P^{-1} = PZ(M)P^{-1}$.

2.3) [Question bonus, hors barème, dont on pourra utiliser le résultat]
Le polynôme caractéristique d'une matrice $M \in \mathrm{SL}(2,\mathbb{C})$ est $\chi_M(X) = X^2 - \mathrm{Tr}(M)X + 1$, où $\mathrm{Tr}(M)$ désigne la trace de M. Le discriminant de ce polynôme est $\mathrm{Tr}(M)^2 - 4$.
Si la trace de M est différente de ± 2, ce polynôme a deux racines distinctes ; M est alors diagonalisable, semblable à une matrice diagonale de déterminant 1 à valeurs propres distinctes, c'est-à-dire à une matrice du type $\begin{pmatrix} a & 0 \\ 0 & 1/a \end{pmatrix}$ avec $a \in \mathbb{C} \setminus \{-1, 0, 1\}$. Si la trace de M est 2, alors 1 est valeur propre double. Si M est diagonalisable, elle est égale à I_2. Sinon, elle est semblable à $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$; en effet, elle est trigonalisable puisque χ_M est scindé ($\mathbb{C}$ est algébriquement clos), donc semblable à une matrice $\begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix}$ avec $z \neq 0$, qui est elle-même semblable à T — conjuguer par exemple T par la matrice diagonale $\mathrm{diag}(z, 1)$. De même, si la trace de M est -2, alors $M = -I_2$ ou M est semblable à $-T$.

2.4) On peut faire un calcul direct : $M = \begin{pmatrix} x & z \\ y & t \end{pmatrix}$ est dans le centralisateur de T si, et seulement si $MT = TM$, c'est-à-dire si, et seulement si les coefficients de M sont solution du système linéaire vérifient $y = 0$ et $x = t$. La condition $\det(M) = 1$ ajoute alors que $x = t = \pm 1$, ce qui montre le résultat.

2.5) On fait encore un calcul direct : $M = \begin{pmatrix} x & z \\ y & t \end{pmatrix}$ est dans le centralisateur de $A = \begin{pmatrix} a & 0 \\ 0 & 1/a \end{pmatrix}$ si, et seulement si x, y, z et t vérifient $\left(a^2 - 1\right)y = \left(a^2 - 1\right)z = 0$. Si $a \notin \{-1, 1\}$, cela impose que $y = z = 0$ et donc que M soit diagonale. Si au contraire $a = \pm 1$, alors $A = \pm I_2$ est dans le centre de $\mathrm{SL}(2,\mathbb{C})$.

Conclusion : si $a = \pm 1$, alors $Z(A) = \mathrm{SL}(2,\mathbb{C})$. Si $a \notin \{\pm 1\}$, alors $Z(A) = \left\{ \begin{pmatrix} x & 0 \\ 0 & 1/x \end{pmatrix},\ x \in \mathbb{C},\ x \neq 0 \right\}$ est le groupe des matrices diagonales de $\mathrm{SL}(2,\mathbb{C})$.

2.6) (i) On a vu plus haut que $Z(T) = \left\{ \pm \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix},\ \alpha \in \mathbb{C} \right\}$.

Le calcul général et célébrissime $\begin{pmatrix}1 & \alpha\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & \beta\\ 0 & 1\end{pmatrix}=\begin{pmatrix}1 & \alpha+\beta\\ 0 & 1\end{pmatrix}$ montre d'une part que l'ensemble $\mathcal{T}=\left\{\begin{pmatrix}1 & \alpha\\ 0 & 1\end{pmatrix},\ \alpha\in\mathbb{C}\right\}$ est un sous-groupe de $\mathrm{SL}\,(2,\mathbb{C})$, et d'autre part que l'application

$$\begin{array}{ccc}(\mathbb{C},+) & \longrightarrow & (\mathcal{T},\times)\\ \alpha & \longmapsto & \begin{pmatrix}1 & \alpha\\ 0 & 1\end{pmatrix}\end{array}$$

est un isomorphisme de groupes. Il en résulte que l'application

$$\begin{array}{ccc}\{-1,1\}\times\mathbb{C} & \longrightarrow & Z(T)\\ ((-1)^n,\alpha) & \longmapsto & (-1)^n\begin{pmatrix}1 & \alpha\\ 0 & 1\end{pmatrix}\end{array}$$

est également un isomorphisme de groupes. Puisque les groupes $\mathbb{Z}/2\mathbb{Z}$ et $\{-1,1\}=\mathbb{U}_2$ sont isomorphes, on a montré le résultat.

(ii) On a vu plus haut que $Z(S)=\left\{\begin{pmatrix}\alpha & 0\\ 0 & 1/\alpha\end{pmatrix},\ \alpha\in\mathbb{C},\ \alpha\neq 0\right\}$. Alors, l'application

$$\begin{array}{ccc}(\mathbb{C}^\times,\times) & \longrightarrow & Z(S)\\ \alpha & \longmapsto & \begin{pmatrix}\alpha & 0\\ 0 & 1/\alpha\end{pmatrix}\end{array}$$

est un isomorphisme de groupes, la preuve en est immédiate.

2.7) Si deux matrices M et N sont semblables, alors leurs centralisateurs sont conjugués — c'est la question **2.2)** — donc isomorphes. Or, toute matrice de $\mathrm{SL}\,(2,\mathbb{C})$ est semblable à T où à une matrice diagonale à valeurs propres distinctes— c'est la question **2.2)** —, dont les centralisateurs sont abéliens — c'est la question **2.6)**. On en conclut que toute matrice non centrale de $\mathrm{SL}\,(2,\mathbb{C})$ a une centralisateur abélien.

UVSQ 2022/2023
Licence de sciences et technologie, santé
LSMA610 (groupes et géométrie)
16 mai 2023

Examen

(durée : deux heures)

1 Question de cours [4 points]

Soit n un entier naturel non nul.
Démontrer que le groupe spécial linéaire $\mathrm{SL}(n,\mathbb{C})$ est un sous-groupe distingué du groupe linéaire $\mathrm{GL}(n,\mathbb{C})$ et que le groupe quotient $\mathrm{GL}(n,\mathbb{C})/\mathrm{SL}(n,\mathbb{C})$ est isomorphe au groupe multiplicatif $\mathbb{C}^\times$.

2 Automorphismes du groupe $\mathrm{SL}(2,\mathbb{F}_3)$ [16 points]

On note $\mathbb{F}_3$ le corps à trois éléments $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$.

On note aussi selon l'usage $\mathrm{GL}(2,\mathbb{F}_3)$ le groupe des matrices carrées 2×2 à coefficents dans $\mathbb{F}_3$ inversibles et $\mathrm{SL}(2,\mathbb{F}_3)$ son sous-groupe des matrices dont le déterminant égale 1.

Si G est un groupe, un *automorphisme* de G est un homomorphisme de groupes $G \to G$ bijectif. L'ensemble des automorphismes de G est un sous-groupe du groupe des permutations de G, que l'on notera $\mathrm{Aut}(G)$.

L'objet de cette partie consiste à montrer que $\mathrm{Aut}(\mathrm{SL}(2,\mathbb{F}_3))$ *est isomorphe au groupe symétrique* $\mathfrak{S}_4$.

On rappelle ici l'énoncé des théorèmes de Sylow.

Premier théorème de Sylow
Pour tout nombre premier p, tout groupe fini contient au moins un p-Sylow.

Deuxième théorème de Sylow
Soient G un groupe fini et p un nombre premier. Alors, tout p-sous-groupe de G est contenu dans un p-Sylow et les p-Sylow de G sont conjugués.

Troisième théorème de Sylow
Soient G un groupe fini et p un nombre premier. Alors, le nombre de p-Sylow de G divise l'ordre de G et est congru à 1 modulo p.

2.1) **Question de cours :** quel est l'ordre de $\mathrm{SL}(2,\mathbb{F}_3)$?

2.2) On note $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $U = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$. Calculer l'ordre de T et l'ordre de U dans $\mathrm{SL}(2,\mathbb{F}_3)$.

On admet, c'est une conséquence du cours sur le groupe modulaire, que T *et* U *engendrent* $\mathrm{SL}(2,\mathbb{F}_3)$.

2.3) Déduire de la question précédente que le nombre de 3-Sylow de $\mathrm{SL}(2,\mathbb{F}_3)$ est 4. On note $\mathcal{S}_3$ l'ensemble des 3-Sylow de $\mathrm{SL}(2,\mathbb{F}_3)$.

2.4) Montrer que l'image d'un 3-Sylow de $\mathrm{SL}(2,\mathbb{F}_3)$ par un automorphisme de $\mathrm{SL}(2,\mathbb{F}_3)$ est encore un 3-Sylow de $\mathrm{SL}(2,\mathbb{F}_3)$. En déduire une action du groupe $\mathrm{Aut}(\mathrm{SL}(2,\mathbb{F}_3))$ sur $\mathcal{S}_3$. On notera

$$\Phi : \mathrm{Aut}(\mathrm{SL}(2,\mathbb{F}_3)) \longrightarrow \mathfrak{S}_{\mathcal{S}_3}$$

l'homomorphisme de groupes induit par cette action.

2.5) Montrer que les 3-Sylow de $\mathrm{SL}(2,\mathbb{F}_3)$ sont

$$S_1 = \langle T \rangle \ , \ S_2 = \langle U \rangle \ , \ S_3 = \left\langle UTU^{-1} \right\rangle \text{ et } S_4 = \left\langle U^2TU^{-2} \right\rangle.$$

2.6) Montrer que si $g \in \ker \Phi$, alors $g(T) \in \left\{T, T^2\right\}$ et $g(U) \in \left\{U, U^2\right\}$.

2.7) Calculer l'ordre de TU et celui de TU^2.

2.8) Déduire des questions précédentes que Φ est injectif.

2.9) On note $A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \in \mathrm{GL}\,(2, \mathbb{F}_3)$. Calculer les conjugués de S_1, S_2, S_3 et S_4 par A et en déduire que l'image de Φ contient une permutation impaire.

2.10) **Question de cours :** quel est le centre de $\mathrm{SL}\,(2, \mathbb{F}_3)$?

2.11) Soit G un groupe. Expliciter un isomorphisme entre le groupe des isomorphismes intérieurs de G et le groupe-quotient $G/Z(G)$ de G par son centre $Z(G)$.

2.12) Montrer que l'image de Φ contient le groupe alterné $\mathfrak{A}_{\mathcal{S}_3}$.

2.13) Déduire de tout ce qui précède que Φ est surjectif.

2.14) Montrer que $\mathrm{Aut}\,(\mathrm{SL}\,(2, \mathbb{F}_3))$ est isomorphe au groupe symétrique $\mathfrak{S}_4$.

UVSQ 2022/2023
Licence de sciences et technologie, santé
LSMA610 (groupes et géométrie)
16 mai 2023

Examen : un corrigé succinct

1 Question de cours

2 Automorphismes du groupe $\mathrm{SL}(2,\mathbb{F}_3)$

2.1) $|\mathrm{SL}(2,\mathbb{F}_3)| = \left(3^2-1\right)\left(3^2-3\right)/(3-1) = 24$.

2.2) On calcule : $T^2 = \begin{pmatrix}1 & 2\\ 0 & 1\end{pmatrix}$, $U^2 = \begin{pmatrix}1 & 0\\ 2 & 1\end{pmatrix}$ et $T^3 = U^3 = I_2$. Donc T et U sont d'ordre 3.

2.3) D'après le troisième théorème de Sylow, le nombre de 3-Sylow de $\mathrm{SL}(2,\mathbb{F}_3)$ est congru à 1 modulo 3 et divise 24, donc divise 8 : ce nombre est 1 ou 4. Or, les 3-Sylow sont d'ordre 3 et la question précédente montre que les groupes engendrés par T et U sont deux 3-Sylow distincts. Puisque ce n'est pas 1, le nombre de 3-Sylow est donc 4.

2.4) Un sous-groupe de $\mathrm{SL}(2,\mathbb{F}_3)$ en est un 3-Sylow si, et seulement s'il est d'ordre 3. Or, l'image d'un sous-groupe par un automorphisme est un sous-groupe de même ordre puisque ces deux groupes sont isomorphes. Donc l'image d'un 3-Sylow de $\mathrm{SL}(2,\mathbb{F}_3)$ par un automorphisme de $\mathrm{SL}(2,\mathbb{F}_3)$ est encore un 3-Sylow de $\mathrm{SL}(2,\mathbb{F}_3)$.
L'application $\mathrm{Aut}(\mathrm{SL}(2,\mathbb{F}_3)) \times \mathcal{S}_3 \to \mathcal{S}_3$, $(f,S) \mapsto f\cdot S = f(S)$ définit évidemment une action (à gauche) du groupe $\mathrm{Aut}(\mathrm{SL}(2,\mathbb{F}_3))$ sur $\mathcal{S}_3$: c'en est l'action *naturelle*.

2.5) On calcule : $S_1 = \left\{1, \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}, \begin{pmatrix}1 & -1\\ 0 & 1\end{pmatrix}\right\}$, $S_2 = \left\{1, \begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}, \begin{pmatrix}1 & 0\\ -1 & 1\end{pmatrix}\right\}$, $S_3 = \left\{1, \begin{pmatrix}0 & 1\\ -1 & -1\end{pmatrix}, \begin{pmatrix}-1 & -1\\ 1 & 0\end{pmatrix}\right\}$ et $S_4 = \left\{1, \begin{pmatrix}-1 & 1\\ -1 & 0\end{pmatrix}, \begin{pmatrix}0 & -1\\ 1 & -1\end{pmatrix}\right\}$. Ces quatre groupes d'ordre 3 sont manifestement distincts : ce sont *les* 3-Sylow de $\mathrm{SL}(2,\mathbb{F}_3)$.

2.6) Si $g \in \ker\Phi$, alors g laisse les deux 3-Sylow S_1 et S_2 invariants — les deux autres 3-Sylow aussi, du reste. Donc $g(T)$ est un élément d'ordre 3 de S_1 : c'est T ou T^2. De même, $g(U) \in \left\{U, U^2\right\}$.

2.7) On calcule : $TU = \begin{pmatrix}-1 & 1\\ 1 & 1\end{pmatrix}$ et $(TU)^2 = -I_2$. Donc TU est d'ordre 4.
Ensuite, $TU^2 = \begin{pmatrix}0 & 1\\ -1 & 1\end{pmatrix}$, $(TU^2)^2 = \begin{pmatrix}-1 & 1\\ -1 & 0\end{pmatrix}$ et $(TU^2)^3 = -I_2$. Donc TU^2 est d'ordre 6.

2.8) Soit $g \in \ker\Phi$. Le résultat de la question **2.6)** aboutit à quatre possibilités :

$$(g(T), g(U)) \in \left\{(T,U), (T,U^2), (T^2,U), (T^2,U^2)\right\}.$$

Si $g(T) = T$ et $g(U) = U^2$, alors $g(TU) = TU^2$ ce qui est impossible puisque TU et TU^2 n'ont pas le même ordre.
Si $g(T) = T^2$ et $g(U) = U$, alors $g(TU^2) = T^2U^2 = T^{-1}U^{-1} = (UT)^{-1}$ ce qui est impossible puisque TU^2 et UT n'ont pas le même ordre — noter que UT et TU, qui sont conjugués puisque $TU = U^{-1}(UT)U$, ont le même ordre.
Si $g(T) = T^2$ et $g(U) = U^2$, alors $g(UTU^{-1}) = g(UTU^2) = U^2T^2U = \left(U^{-1}TU\right)^2$ ce qui entraîne que g échange les 3-Sylow S_3 et S_4, contredisant le fait que g soit dans le noyau de Φ.
On déduit de cela que g fixe T et U, ce qui implique que $g = \mathrm{id}_{\mathrm{SL}(2,\mathbb{F}_3)}$ puisque T et U engendrent $\mathrm{SL}(2,\mathbb{F}_3)$.
On a montré que Φ est injectif.

Noter que beaucoup d'autres arguments faisaient aussi l'affaire, dans cette question.

2.9) On calcule : $ATA^{-1} = U \in S_2$, $AUA^{-1} = \begin{pmatrix}0 & 1\\ -1 & -1\end{pmatrix} \in S_3$, $A(UTU^{-1})A^{-1} = \begin{pmatrix}0 & -1\\ 1 & -1\end{pmatrix} \in S_4$ et $A(U^{-1}TU)A^{-1} = T^2 \in S_1$. Cela montre que la conjugaison par A, qui est un automorphisme de $\mathrm{SL}(2,\mathbb{F}_3)$, a le 4-cycle (S_1, S_2, S_3, S_4) pour image par Φ. Par ailleurs, un 4-cycle est une permutation impaire.

2.10) Le centre de $\mathrm{SL}(2,\mathbb{F}_3)$ est le groupe $\{\pm I_2\}$ de ses homothéties.

2.11) Pour tout $g \in G$, on note $i_g : G \to G$ la conjugaison par g : $i_g(h) = ghg^{-1}$, pour tout $h \in G$. Alors, l'application $G \to \mathrm{Aut}(G)$, $g \mapsto i_g$ est un homomorphisme de groupes dont l'image est le groupe $\mathrm{Int}(G)$ des automorphismes intérieurs et dont le noyau est le centre $Z(G)$ de G. Le premier théorème d'isomorphisme pour les groupes assure alors que $G/Z(G) \simeq \mathrm{Int}(G)$.

2.12) Le groupe $\mathrm{Int}(\mathrm{SL}(2,\mathbb{F}_3))$ est isomorphe à $\mathrm{SL}(2,\mathbb{F}_3)/\{\pm I_2\}$ qui est d'ordre 12. Puisque Φ est injectif, l'image de $\mathrm{Int}(\mathrm{SL}(2,\mathbb{F}_3))$ par Φ est donc sous-groupe d'ordre 12 — donc d'indice 2, donc distingué — de $\mathfrak{S}_{\mathcal{S}_3}$: ce groupe est le groupe alterné $\mathfrak{A}_{\mathcal{S}_3}$ puisque ce dernier est l'unique sous-groupe d'indice 2 de $\mathfrak{S}_{\mathcal{S}_3}$.

2.13) L'image de Φ est un sous-groupe de $\mathfrak{S}_{\mathcal{S}_3}$ qui contient le groupe alterné $\mathfrak{A}_{\mathcal{S}_3}$ et une permutation impaire : c'est $\mathfrak{S}_{\mathcal{S}_3}$ tout entier, ce qui montre que Φ est surjectif.

2.14) Φ est un isomorphisme entre $\mathrm{Aut}(\mathrm{SL}(2,\mathbb{F}_3))$ et $\mathfrak{S}_{\mathcal{S}_3}$. Comme $\mathcal{S}_3$ est de cardinal 4, le groupe $\mathfrak{S}_{\mathcal{S}_3}$ est isomorphe à $\mathfrak{S}_4$. Donc $\mathrm{Aut}(\mathrm{SL}(2,\mathbb{F}_3))$ et $\mathfrak{S}_4$ sont isomorphes.

UVSQ 2023/2024
Licence de sciences et technologie, santé
LSMA610 (groupes et géométrie)
17 mai 2024

Examen

– durée : deux heures –

— *Bon, il faut l'écrire : aucun document ni aucun instrument électronique n'est autorisé pour cette épreuve* —

1 Sur les 7-Sylow du groupe $\mathfrak{S}_7$ [7 points]

On note $\mathfrak{S}_7$ le groupe des permutations de $\{1,2,3,4,5,6,7\}$.

1.1) Calculer l'ordre commun à tous les 7-Sylow de $\mathfrak{S}_7$.

1.2) Montrer que tout 7-cycle de $\mathfrak{S}_7$ est dans un unique 7-Sylow.

1.3) Combien $\mathfrak{S}_7$ contient-il de 7-cycles ?

1.4) En utilisant ce qui précède, calculer le nombre de 7-Sylow de $\mathfrak{S}_7$.

1.5) On fait agir $\mathfrak{S}_7$ par conjugaison sur l'ensemble de ses 7-Sylow. Dire quel théorème du cours permet d'affirmer que cette action n'a qu'une seule orbite et calculer l'ordre du groupe d'isotropie du 7-Sylow qui contient le 7-cycle (1234567).

1.6) Montrer que si p est un nombre premier, $(p-2)! = 1 \mod (p)$, et que le groupe symétrique $\mathfrak{S}_p$ admet toujours un sous-groupe d'ordre $p(p-1)$.

2 Groupe dérivé de $\mathrm{SL}(2,\mathbb{Z})$ [13 points]

On note $\Gamma = \mathrm{SL}(2,\mathbb{Z})$ le groupe des matrices 2×2 à coefficients entiers dont le déterminant égale 1. Si x et y sont deux matrices de Γ, on note

$$[x,y] = xyx^{-1}y^{-1}$$

le *commutateur* de x et y. On note aussi $D(\Gamma)$ le groupe dérivé de Γ, qui est le sous-groupe de Γ engendré par ses commutateurs.

— *Les deux matrices* $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ *et* $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ *engendrent* Γ *; c'est un résultat du cours, on le redit ici.* —

2.1) On note $R = ST = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$. Calculer l'ordre de S et l'ordre de R.

2.2) Montrer que le groupe Γ est engendré par S et R.

2.3) En déduire que l'image de tout homomorphisme de groupes $\Gamma \longrightarrow \mathbb{C}^\times$ est incluse dans le groupe $\mathbb{U}_{12}$ des racines douzièmes de l'unité.

2.4) On note A et B les deux matrices de Γ

$$A = [S,R] = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \quad \text{et} \quad B = [S^{-1},R^{-1}] = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}.$$

Montrer que le sous-groupe $\langle A,B\rangle$ de Γ engendré par A et B est inclus dans $D(\Gamma)$.

2.5) Montrer que $\langle A,B\rangle$ est un sous-groupe distingué de Γ.
[Pas si simple ! On pourra par exemple montrer, au cours du calcul, que $RAR^{-1} = A^{-1}B$.]

2.6) Montrer que $AST^3 = B$. En déduire que $\Gamma = \langle A,B,T\rangle$.

2.7) Montrer que le groupe quotient $\Gamma/\langle A, B\rangle$ est monogène.

2.8) Montrer que si G est un groupe dont on note $D(G)$ le groupe dérivé et si H est un sous-groupe distingué de G dont le quotient G/H est abélien, alors $D(G) \subseteq H$.
[On pourra considérer l'image de $D(G)$ par la projection canonique $G \to G/H$.]

2.9) En déduire que $D(\Gamma) = \langle A, B\rangle$.

2.10) Montrer que $\left[A, B^{-1}\right] = -T^6$. En admettant que le centre de $D(\Gamma)$ est trivial[♪], en déduire que le quotient $\Gamma/D(\Gamma)$ est isomorphe à $\mathbb{U}_{12}$.

[♪] C'est, par exemple, une conséquence du fait que $D(\Gamma)$ est un groupe *libre* à 2 générateurs A et B.

UVSQ 2023/2024
Licence de sciences et technologie, santé
LSMA610 (groupes et géométrie)
17 mai 2024

Examen : un corrigé succinct

1 Sur les 7-Sylow du groupe $\mathfrak{S}_7$

1.1) Puisque 7 est premier, il ne divise par 6! (lemme d'Euclide). Donc la 7-valuation de 7! est 1, ce qui montre que les 7-Sylow de $\mathfrak{S}_7$ sont d'ordre 7.

1.2) Soit c un 7-cycle de $\mathfrak{S}_7$. Alors, le groupe $\langle c\rangle$ engendré par c est cyclique d'ordre 7 : c'est un 7-Sylow. Inversement, si S est un 7-Sylow contenant c, il contient $\langle c\rangle$; puisque ces deux groupes ont le même ordre fini, $S = \langle c\rangle$. Donc $\langle c\rangle$ est l'unique 7-Sylow qui contient c.

1.3) Tout 7-cycle s'écrit de manière unique sous la forme $(1a_1a_2a_3a_4a_5a_6)$ où $(a_1a_2a_3a_4a_5a_6)$ est un 6-uplet d'éléments distincts de $\{2,3,4,5,6,7\}$. Ainsi, le nombre de 7-cycles de $\mathfrak{S}_7$ est 6!.

1.4) Le nombre 7 est premier. Chaque 7-Sylow, puisqu'il est cyclique d'ordre 7, est donc constitué de l'identité et de six 7-cycles distincts : les 7-cycles se répartissent dans les 7-Sylow par groupes de 6. Ainsi, le nombre de 7-Sylow est $\frac{6!}{6} = 5!$.

1.5) L'un des théorèmes de Sylow assure que tous les p-Sylow d'un groupe sont conjugués. En termes d'actions de groupes, cela signifie que l'action par conjugaison du groupe sur ses p-Sylow est transitive, ou encore qu'elle n'a qu'une seule orbite. C'est cela qu'on applique au groupe $\mathfrak{S}_7$.
L'ordre de $\mathfrak{S}_7$ est le produit du cardinal de l'unique orbite et de l'ordre commun au groupe d'isotropie de n'importe quel 7-Sylow. Donc l'ordre commun aux groupes d'isotropie des 7-Sylow— dont celui du 7-Sylow de (1234567) — est $\frac{7!}{5!} = 7\times 6 = 42$.

1.6) Tout ce qui précède est encore valide si on remplace 7 par n'importe quel nombre premier p : le nombre de p-Sylow de $\mathfrak{S}_p$ est $(p-2)!$ et les groupes d'isotropie de l'action de $\mathfrak{S}_p$ par conjugaison sur ses p-Sylow sont d'ordre $\frac{p!}{(p-2)!} = p(p-1)$. Donc $\mathfrak{S}_p$ admet des sous-groupes d'ordre $p(p-1)$. En outre, puisque le nombre de p-Sylow de $\mathfrak{S}_p$ est $(p-2)!$, le troisième théorème de Sylow assure que ce nombre vaut 1 modulo p, ce qu'il fallait démontrer.

[Pour aller plus loin : si G est un sous-groupe d'ordre $p(p-1)$ de $\mathfrak{S}_p$, alors le troisième théorème de Sylow montre que G contient un unique p-Sylow, engendré par n'importe lequel de ses p-cycles c. En particulier, $\langle c\rangle$ est distingué dans G. Alors, le normalisateur de $\langle c\rangle$ dans $\mathfrak{S}_p$ est d'ordre $p(p-1)$ et contient G : ces deux groupes de même ordre fini sont donc égaux. On a montré que tout sous-groupe d'ordre $p(p-1)$ de $\mathfrak{S}_p$ est le normalisateur d'un p-cycle (ou plutôt du sous-groupe qu'il engendre).]

2 Groupe dérivé de $\mathrm{SL}(2,\mathbb{Z})$

2.1) On calcule. On trouve $S^2 = R^3 = -I_2$. Cela suffit à montrer que l'ordre de S est 4 et que l'ordre de R est 6.

2.2) Puisque S et $R = ST$ sont dans $\langle S,T\rangle$, par minimalité des sous-groupes engendrés, $\langle S,R\rangle \subseteq \langle S,T\rangle$. De même, puisque S et $T = S^{-1}R \in \langle S,R\rangle$, on a l'inclusion inverse $\langle S,T\rangle \subseteq \langle S,R\rangle$. On a montré que $\langle S,R\rangle = \langle S,T\rangle$. Puisque par ailleurs $\Gamma = \langle S,T\rangle$ — c'est rappelé dans l'énoncé —, $\Gamma = \langle S,R\rangle$.

2.3) Soit $f : \Gamma \longrightarrow \mathbb{C}^\times$ un homomorphisme de groupes. Puisque Γ est engendré par S et R dont les ordres sont 4 et 6 respectivement, l'image $\mathrm{im}(f)$ est engendrée par $\langle f(S)\rangle$ et $\langle f(R)\rangle$ qui sont des sous-groupes de $\mathbb{U}_4$ et de $\mathbb{U}_6$ respectivement. Or, les sous-groupes $\mathbb{U}_4$ et de $\mathbb{U}_6$ de $\mathbb{C}^\times$, qui sont tous les deux des sous-groupes de $\mathbb{U}_{12}$, engendrent un sous-groupe de $\mathbb{U}_{12}$. Donc $\mathrm{im}(f)$ est un sous-groupe de $\mathbb{U}_{12}$.

2.4) A et B sont des commutateurs. Donc le sous-groupe de Γ qu'ils engendrent est inclus dans le groupe engendré par les commutateurs de Γ, qui est le groupe dérivé $D(\Gamma)$.

2.5) Puisque les générateurs S et R de Γ sont d'ordres finis, il suffit de montrer que $\langle A,B\rangle$ est stable par la conjugaison par S et R — autrement dit, il est inutile de tester la conjugaison par $S^{-1} = S^3$ et par $R^{-1} = R^5$. Par

ailleurs, par caractérisation des sous-groupes engendrés, il suffit de montrer que les conjugués de A et de B par S et R sont dans $\langle A, B\rangle$. Il y a ainsi quatre calculs à faire :
(i) $SAS^{-1} = S \cdot SRS^{-1}R^{-1} \cdot S^{-1} = -RS^{-1}R^{-1} \cdot S^{-1} = RSR^{-1} \cdot S^{-1} = [R, S] = [S, R]^{-1} = A^{-1}$, les différentes expressions de cette matrice venant du fait que $S^2 = -I_2$, ou encore que $S^{-1} = S^3 = -S$. Cela montre que $SAS^{-1} \in \langle A, B\rangle$.
(ii) $RAR^{-1} = R \cdot SRS^{-1}R^{-1} \cdot R^{-1} = RSRSR$ alors que $A^{-1}B = RSR^{-1}S^{-1} \cdot S^{-1}R^{-1}SR = -RSR^{-2}SR = RSRSR$, les différentes expressions de cette matrice venant du fait que $R^{-1} = -R^2$, ou encore que $R^{-2} = -R$. Cela montre que $RAR^{-1} = A^{-1}B \in \langle A, B\rangle$.
(iii) $SBS^{-1} = S \cdot S^{-1}R^{-1}SR \cdot S^{-1} = R^{-1}SRS^{-1} = (-1)^2 \left[R^{-1}, S^{-1}\right] = B^{-1}$. Cela montre que $SBS^{-1} \in \langle A, B\rangle$.
(iv) $RBR^{-1} = R \cdot S^{-1}R^{-1}SR \cdot R^{-1} = RS^{-1}R^{-1}S = (-1)^2 [R, S] = A^{-1}$. Cela montre que $RBR^{-1} \in \langle A, B\rangle$.
On a montré que le sous-groupe $\langle A, B\rangle$ de Γ est normal.

NB : on pouvait bien sûr mener ces calculs autrement.

2.6) $AST^3 = SRS^{-1}R^{-1} \cdot S \cdot \left(S^{-1}R\right)^3 = SRS^{-1}\left(R^{-1}S \cdot S^{-1}R\right)S^{-1}RS^{-1}R = SRS^{-2}RS^{-1}R = -SR^2S^{-1}R = SR^{-1}S^{-1}R = (-1)^2\left[S^{-1}, R^{-1}\right] = B$, en utilisant à nouveau, dans cet ordre, les relations $S^2 = -I_2$, $R^2 = -R^{-1}$ et $S^{-1} = -S$ — là encore, on pouvait faire un calcul matriciel direct, fastidieux mais sans histoire.

En particulier, $S = A^{-1}BT^{-3} \in \langle A, B, T\rangle$. Comme en outre $T \in \langle A, B, T\rangle$, par minimalité des sous-groupes engendrés, cela montre que $\Gamma = \langle S, T\rangle \subseteq \langle A, B, T\rangle$. Par ailleurs, $\langle A, B, T\rangle \subseteq \Gamma$, ce qui montre que $\Gamma = \langle A, B, T\rangle$.

2.7) Par caractérisation des sous-groupes engendrés, tout élément de Γ est un produit d'éléments de l'ensemble $\left\{A, A^{-1}, B, B^{-1}, T, T^{-1}\right\}$. Puisque les classes de $A^{\pm 1}$ et de $B^{\pm 1}$ sont triviales dans le groupe-quotient $\Gamma/\langle A, B\rangle$, toute classe modulo $\langle A, B\rangle$ d'un élément de Γ est représentée par un produit de l'ensemble $\left\{T, T^{-1}\right\}$. Cela montre que tout élément de $\Gamma/\langle A, B\rangle$ est une puissance de la classe de T, ce qui prouve que $\Gamma/\langle A, B\rangle$ est monogène.

En d'autres mots, $\langle A, B, T\rangle / \langle A, B\rangle = \left\langle \overline{T}\right\rangle$ — notations évidentes.

2.8) Dans les conditions de l'énoncé, soit $p : G \longrightarrow G/H$ la projection canonique. Alors, si $x, y \in G$, $p([x, y]) = [p(x), p(y)] = 1_{G/H}$ puisque G/H est abélien. Ainsi, tout commutateur est dans $\ker(p) = H$ et donc, par minimalité des sous-groupes engendrés, $D(G) \subseteq H$.

2.9) Puisqu'il est monogène, le groupe-quotient $\Gamma/\langle A, B\rangle$ est abélien. La question précédente montre alors que $D(\Gamma) \subseteq \langle A, B\rangle$. Par ailleurs, la question **2.4)** montrait l'inclusion inverse.

2.10) On calcule : $\left[A, B^{-1}\right] = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} -1 & -6 \\ 0 & -1 \end{pmatrix} = -T^6$.

Ainsi, puisque $-T^6$ est un commutateur, sa classe modulo $D(\Gamma) = \langle A, B\rangle$ est triviale. Cela montre que l'ordre de la classe de T dans $\Gamma/D(\Gamma)$ divise 12. Puisque cette classe engendre $\Gamma/D(\Gamma)$, il suffit de montrer que cet ordre est 12 exactement pour montrer que $\Gamma/D(\Gamma)$ est cyclique d'ordre 12, donc isomorphe à $\mathbb{U}_{12}$.

Or, $-I_2 \notin D(\Gamma)$ puisqu'il est dans le centre de Γ — ce serait un élément non trivial du centre de $D(\Gamma)$ ce qui est impossible selon l'énoncé admis dans l'énoncé. Donc $T^6 \notin D(\Gamma)$, ce qui finit de montrer que la classe de T est d'ordre 12 dans $\Gamma/D(\Gamma)$.

UVSQ 2024/2025
Licence de sciences et technologie, santé
LSMA610 (groupes et géométrie)
16 mai 2025

Examen

(durée : deux heures)

— Bon, il faut l'écrire : aucun document ni aucun instrument électronique n'est autorisé pour cette épreuve —

1 Il n'y a pas de groupe simple d'ordre 15309 [6 points]

Soit G un groupe d'ordre $15309 = 3^7 \times 7$.

1.1) Montrer que le nombre de 3-sous-groupes de Sylow de G est inclus dans l'ensemble $\{1, 7\}$.

1.2) On suppose que G est simple et a sept 3-sous-groupes de Sylow. Montrer avec soin comment l'action de G par conjugaison sur l'ensemble de ses 3-sous-groupes de Sylow induit un homomorphisme injectif de groupes $G \longrightarrow \mathfrak{S}_7$. Comparer les ordres de G et de $\mathfrak{S}_7$ et conclure à une contradiction.

1.3) Montrer qu'il n'y a pas de groupe simple d'ordre 15309.

2 Commutateurs orthogonaux [14 points]

2.1 Carrés et commutateurs

Si G est un groupe, on note $D(G)$ son groupe dérivé et $C(G)$ et le sous-groupe de G engendré par ses carrés :

$$D(G) = \left\langle \left\{ xyx^{-1}y^{-1},\ (x,y) \in G^2 \right\} \right\rangle$$
et
$$C(G) = \left\langle \left\{ x^2,\ x \in G \right\} \right\rangle$$

2.1) Montrer que $C(G)$ et $D(G)$ sont des sous-groupes distingués de G.

2.2) Montrer que le groupe quotient $G/C(G)$ n'a que des éléments d'ordre 1 ou 2. En déduire que $G/C(G)$ est abélien et que, lorsqu'il est fini, il est isomorphe à un groupe produit de la forme $(\mathbb{Z}/2\mathbb{Z})^r$ où $r \in \mathbb{N}$.

2.3) En considérant la projection canonique $G \longrightarrow G/C(G)$, montrer que $D(G) \subseteq C(G)$.

2.4) Montrer que si un groupe G est engendré par ses éléments d'ordre 2, alors $D(G) = C(G)$.

2.2 Sur le groupe $\mathrm{SO}(3, \mathbb{F}_5)$

On note $\mathbb{F}_5$ le corps $\mathbb{Z}/5\mathbb{Z}$. Selon l'usage, on note aussi $\mathrm{O}(3, \mathbb{F}_5)$ le sous-groupe de $\mathrm{GL}(3, \mathbb{F}_5)$ formé des matrices orthogonales et $\mathrm{SO}(3, \mathbb{F}_5)$ son sous-groupe des matrices orthogonales de déterminant 1 :

$$\mathrm{O}(3, \mathbb{F}_5) = \left\{ A \in \mathrm{GL}(3, \mathbb{F}_5),\ {}^tA = A^{-1} \right\} \text{ et } \mathrm{SO}(3, \mathbb{F}_5) = \left\{ A \in \mathrm{O}(3, \mathbb{F}_5),\ \det(A) = 1 \right\}.$$

On note également V le $\mathbb{F}_5$-espace vectoriel des vecteurs-colonne à 3 lignes et à coefficients dans $\mathbb{F}_5$. On note enfin q la forme quadratique standard sur V et $\langle \cdot | \cdot \rangle$ sa forme polaire, définies par : $\forall (x,y,z) \in (\mathbb{F}_5)^3$, $\forall (x',y',z') \in (\mathbb{F}_5)^3$,

$$q\begin{pmatrix} x \\ y \\ z \end{pmatrix} = x^2 + y^2 + z^2 \text{ et } \left\langle \begin{pmatrix} x \\ y \\ z \end{pmatrix} \middle| \begin{pmatrix} x' \\ y' \\ z' \end{pmatrix} \right\rangle = xx' + yy' + zz'.$$

Si v et w sont dans V, on dit que v est *unitaire* lorsque $q(v) = 1$ et que v et w sont *orthogonaux* lorsque $\langle v | w \rangle = 0$.

On admettra — c'est élémentaire — que pour toute $A \in \mathrm{GL}(3, \mathbb{F}_5)$, les assertions suivantes sont équivalentes :

(i) A est orthogonale

(ii) $q(Av) = q(v)$, pour tout $v \in V$

(iii) les vecteurs-colonne de A sont unitaires et deux à deux orthogonaux.

Par exemple, si on note

$$D_2 = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix},\ R = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix},\ P = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix},\ T = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ et } M = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix},$$

alors D_2, R, P, $-T$ et $-M$ sont dans $\mathrm{SO}(3, \mathbb{F}_5)$.

Pour finir, on admet — c'est un calcul élémentaire — que les vecteurs unitaires de V sont ceux de la liste suivante :

$$\pm {}^t(1,0,0),\ \pm {}^t(0,1,0),\ \pm {}^t(0,0,1), {}^t(\pm 2, \pm 1, \pm 1),\ {}^t(\pm 1, \pm 2, \pm 1),\ \text{et}\ {}^t(\pm 1, \pm 1, \pm 2).$$

2.5) On note $e_1 = {}^t(1,0,0)$. On note aussi

$$S = \{A \in \mathrm{SO}(3, \mathbb{F}_5),\ \exists x \in \mathbb{F}_5,\ Ae_1 = xe_1\}$$

et

$$F = \{A \in \mathrm{SO}(3, \mathbb{F}_5),\ Ae_1 = e_1\}.$$

On admettra — c'est un calcul élémentaire — que S est le sous-groupe de $\mathrm{SO}(3, \mathbb{F}_5)$ engendré par D_2 et R.

(i) Montrer que le groupe engendré par R est distingué dans S.

(ii) En déduire l'ordre de S.

(iii) Faire la liste des éléments de S et en déduire que F est le sous-groupe de S engendré par R.

2.6) Montrer que l'action naturelle de $\mathrm{GL}(3, \mathbb{F}_5)$ sur V induit une action transitive de $\mathrm{SO}(3, \mathbb{F}_5)$ sur l'ensemble des vecteurs unitaires de V.

2.7) En déduire que $|\mathrm{SO}(3, \mathbb{F}_5)| = 120$.

2.8) On admet encore — c'est un calcul élémentaire — que $S = \left\{A \in \mathrm{SO}(3, \mathbb{F}_5),\ AR^2 = R^2A\right\}$. Montrer que $\mathrm{SO}(3, \mathbb{F}_5)$ contient exactement 15 matrices d'ordre 2 conjuguées à R^2.

2.9) On admet enfin — c'est un calcul élémentaire — que le groupe des matrices de $\mathrm{SO}(3, \mathbb{F}_5)$ qui commutent avec P est le sous-groupe de $\mathrm{SO}(3, \mathbb{F}_5)$ engendré par P et $-M$. Démontrer que ce groupe est isomorphe à $\mathbb{Z}/6\mathbb{Z}$ et en déduire le nombre de matrices de $\mathrm{SO}(3, \mathbb{F}_5)$ qui sont conjuguées à P.

2.10) On admet — ce n'est pas si simple — que $-M \in \mathrm{SO}(3, \mathbb{F}_5) \setminus D(\mathrm{SO}(3, \mathbb{F}_5))$. On admet enfin — c'est à la fois classique et élémentaire — que $\mathrm{SO}(3, \mathbb{F}_5)$ est engendré par ses éléments d'ordre 2.

(i) Montrer que l'ordre du groupe $\mathrm{SO}(3, \mathbb{F}_5)/D(\mathrm{SO}(3, \mathbb{F}_5))$ est dans l'ensemble $\{2, 4, 8\}$.

(ii) Montrer que P est dans $D(\mathrm{SO}(3, \mathbb{F}_5))$.

(iii) En déduire[♪] que $\mathrm{SO}(3, \mathbb{F}_5)/D(\mathrm{SO}(3, \mathbb{F}_5)) \simeq \mathbb{Z}/2\mathbb{Z}$.

[♪] La situation est bien différente du cas réel puisque $\mathrm{SO}(3, \mathbb{R})$ est simple, égal à son groupe des commutateurs.

UVSQ 2024/2025
Licence de sciences et technologie, santé
LSMA610 (groupes et géométrie)
16 mai 2025

Examen : un corrigé succinct

1 Il n'y a pas de groupe simple d'ordre 15309

1.1) Selon le troisième théorème de Sylow, le nombre de 3-sous-groupes de Sylow de G vaut 1 modulo 3 et divise 7. Ce nombre est donc 1 ou 7.

1.2) Sous l'hypothèse de l'énoncé, soit $\mathcal{S}$ l'ensemble des sept 3-Sylow de G. Puisque le conjugué d'un 3-Sylow de G est encore un 3-Sylow de G, la conjugaison des sous-groupes définit une action à gauche sur $\mathcal{S}$. Cette action induit un homomorphisme de groupes

$$\varphi : G \longrightarrow \mathfrak{S}_{\mathcal{S}} \simeq \mathfrak{S}_7.$$

Puisque G est simple et puisque $\ker\varphi$ en est un sous-groupe normal, $\ker\varphi \in \{\{1\}, G\}$. Demander que $\ker\varphi = G$ revient à demander que $gSg^{-1} = S$, pour tout $S \in \mathcal{S}$ et pour tout $g \in G$, ce qui contredirait le fait que tous les 3-Sylow de G sont conjugués — c'est un des théorèmes de Sylow. Ainsi, φ est injectif.
Or, $|G| = 15309 > |\mathfrak{S}_7| = 7! = 5040$. Donc il n'y a pas d'application injective $G \mapsto \mathfrak{S}_7$. On déduit de tout cela qu'il n'y a pas de groupe simple d'ordre 15309 ayant sept 3-Sylow.

1.3) Par l'absurde, on suppose que G est un groupe simple d'ordre 15309. La question précédente montre que le nombre de ses 3-Sylow n'est pas 7. La première question impose donc que ce nombre soit 1. Mais puisque tout conjugué d'un 3-Sylow est encore un 3-Sylow (deux sous-groupes conjugués ont le même ordre), cela oblige l'unique 3-Sylow de G à être distingué, ce qui contredit la simplicité de G. On a montré que l'hypothèse de l'existence d'un groupe simple d'ordre 15309 ne tient pas, ce qu'il fallait démontrer.

2 Commutateurs orthogonaux

2.1 Carrés et commutateurs

2.1) La formule générale $z(xy)z^{-1} = \left(zxz^{-1}\right)\left(zyz^{-1}\right)$ montre que le conjugué d'un commutateur est un commutateur et que le conjugué d'un carré est encore un carré. Cela suffit à montrer que $D(G)$ et $C(G)$ sont des sous-groupes normaux de G.

2.2) Si $x \in G$, la classe de x^2 est triviale dans le groupe quotient $G/C(G)$. La classe de x est donc d'ordre 1 (lorsque x est lui-même un produit de carrés dans G) ou 2.

Dans un groupe quelconque, il suffit que tout élément soit d'ordre 1 ou 2 pour que ledit groupe soit abélien. C'est l'objet d'un exercice de la liste de TD. L'argument repose par exemple sur le fait que tout élément égale son inverse, et donc que $xy = (xy)^{-1} = y^{-1}x^{-1} = yx$, pour tous x et y.

Lorsque G est fini, le quotient est un groupe abélien fini dont tous les éléments non triviaux sont d'ordre 2. Ses facteurs invariants sont nécessairement de la forme $(2, 2, \ldots, 2)$, puisqu'un groupe abélien fini ayant un facteur invariant $d \neq 2$ contient toujours un élément d'ordre d.

[On peut aussi de passer du théorème de structure des groupes abéliens finis en remarquant que la loi externe $(n, x) \in \mathbb{Z} \times G/C(G) \mapsto nx \in G/C(G)$ induit une structure de $\mathbb{Z}/2\mathbb{Z}$-espace vectoriel sur $G/C(G)$. Si d est la dimension — nécessairement finie puisque $G/C(G)$ est fini — de cet espace vectoriel, le choix d'une base montre que cet espace est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^d$. En particulier, son cardinal est 2^d.]

2.3) Puisque le groupe $G/C(G)$ est abélien, tout commutateur appartient au noyau de la projection canonique $G \to G/C(G)$; or, ce noyau est précisément $C(G)$. Donc $D(G)$ est un sous-groupe $C(G)$.
[On peut aussi voir cela brutalement en remarquant que $xyx^{-1}y^{-1} = x^2\left(x^{-1}y\right)^2 y^{-2}$.]

2.4) Compte tenu de la question précédente, il suffit de montrer que tout carré de G est un produit de commutateurs. Soit $x = a_1 \ldots a_n \in G$, où les a_k sont des éléments d'ordre 2 de G. Alors, on montre par récurrence sur n que x^2 est un produit de commutateurs. Si $n = 2$, alors $x^2 = a_1a_2a_1^{-1}a_2^{-1} \in D(G)$. Si $n \geq 3$, alors, en notant $y = a_2 \ldots a_n$, dont

le carré est dans $D(G)$ par récurrence, on obtient $x^2 = a_1 y a_1 y = \left(a_1 y a_1^{-1} y^{-1}\right) y^2 \in D(G)$. Ainsi, tout carré est dans $D(G)$, ce qui montre — par minimalité des sous-groupes engendrés — que $C(G) \subseteq D(G)$.

2.2 Sur le groupe $\mathrm{SO}(3, \mathbb{F}_5)$

2.5) (i) On peut d'abord noter que R^2 est la matrice diagonale $\mathrm{diag}(1, -1, -1)$ et donc que R est d'ordre 4.
On calcule : $D_2 R D_2^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix} = R^3 \in \langle R \rangle$. Puisque S est engendré par D_2 et R et puisque D_2 est d'ordre fini, cela montre que $\langle R \rangle \triangleleft S$.

(ii) On considère la composée $\langle D_2 \rangle \to S \to S/\langle R \rangle$ de la projection canonique $S \to S/\langle R \rangle$ et de l'inclusion $\langle D_2 \rangle \to S$. Puisque $S = \langle R, D_2 \rangle$, en vertu de la caractérisation des sous-groupes engendrés, cette composée est surjective ; en outre, $\langle D_2 \rangle \cap \langle R \rangle = \{I_3\}$ — c'est immédiat —, ce qui implique que ladite composée est également injective. Ainsi, $S/\langle R \rangle$ est isomorphe au sous-groupe engendré par D_2. Puisque D_2 est (évidemment) d'ordre 2, l'indice de $\langle R \rangle$ dans S est 2. Puisque l'ordre de $\langle R \rangle$ est 4, cela montre que $|S| = 8$.
[On ne le demandait pas, mais S est un groupe diédral d'ordre 8.]

(iii) Les huit éléments de S sont I_2, R, R^2, R^3, D_2, $RD_2 = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$, $R^2 D_2 = \mathrm{diag}(-1, -1, 1)$ et $R^3 D_2 = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{pmatrix}$. Parmi ces matrices seules les puissances de R ont un coefficient 1 en haut à gauche, ce qui montre que $F = \langle R \rangle$.

2.6) L'action naturelle est celle du produit matriciel : si $A \in \mathrm{GL}(3, \mathbb{F}_5)$ et $v \in V$, $A \cdot v = Av$. Si $A \in \mathrm{SO}(3, \mathbb{F}_5)$ et si v est unitaire, alors $q(Av) = q(v) = 1$, ce qui montre que $A \cdot v$ est encore unitaire. L'action naturelle de $\mathrm{GL}(3, \mathbb{F}_5)$ sur V induit donc une action de $\mathrm{SO}(3, \mathbb{F}_5)$ sur l'ensemble des vecteurs unitaires de V.

Il reste à montrer que cette action est transitive. On montre pour cela que pour tout vecteur unitaire $v \in V$, il existe $A \in \mathrm{SO}(3, \mathbb{F}_5)$ tel que $Ae_1 = v$, où $e_1 = {}^t(1, 0, 0)$, ce qui suffit à montrer la transitivité. Il suffit pour de trouver une matrice A de $\mathrm{SO}(3, \mathbb{F}_5)$ dont la première colonne soit v, puisqu'alors, $Ae_1 = v$ — ce qui est à vrai dire plus facile à comprendre qu'à écrire.
Si $v = e_1$, alors $A = I_3$ convient. Si $v = -e_1$, alors $A = D_2$ convient. De même, si $v = e_2 = {}^t(0, 1, 0)$, prendre par exemple $A = P$ et si $v = -e_2$, prendre $A = -T$. Enfin, si $v = e_3 = {}^t(0, 0, 1)$, prendre $A = P^2$ et si $v = -e_3$, prendre $A = -PT$ — attention aux déterminants de ces matrices. Voilà pour les six premiers vecteurs unitaires.
Restent les vingt-quatre autres. Par exemple, pour illustrer ce qui suit, si $v = {}^t(2, 1, 1)$, la matrice $A = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 1 & 2 \\ 1 & 2 & 1 \end{pmatrix} = M \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$ convient — on a permuté les deux dernières colonnes de M pour obtenir une matrice de déterminant 1.
On peut aussi prendre $A = \begin{pmatrix} 2 & 1 & -1 \\ 1 & 2 & -1 \\ 1 & 1 & -2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix} M$ — on a inversé le signe du déterminant de M en changeant du signe de sa dernière colonne.
On écrit cela (mais on n'exigeait pas tant de précision sur une copie, à vrai dire). Soient $\varepsilon, \zeta, \eta \in \{-1, 1\}$. Si $v = {}^t(2\varepsilon, \zeta, \eta)$, alors la matrice orthogonale $\begin{pmatrix} 2\varepsilon & \varepsilon & \varepsilon \\ \zeta & 2\zeta & \zeta \\ \eta & \eta & 2\eta \end{pmatrix} = \begin{pmatrix} \varepsilon & 0 & 0 \\ 0 & \zeta & 0 \\ 0 & 0 & \eta \end{pmatrix} M$ envoie bien e_1 sur v, mais son déterminant vaut $-\varepsilon\zeta\eta$. Si ce déterminant égale 1, on prend pour A cette matrice. S'il égale -1, permuter les deux dernières colonnes de cette matrice ; la matrice obtenue reste orthogonale, envoie encore e_1 sur v mais est cette fois dans $\mathrm{SO}(3, \mathbb{F}_5)$. On procède de façon analogue si v est l'un seize vecteurs unitaires restants, savoir ${}^t(\pm 1, \pm 2, \pm 1)$ ou ${}^t(\pm 1, \pm 1, \pm 2)$.

2.7) On considère l'action de $\mathrm{SO}(3, \mathbb{F}_5)$ sur les 30 vecteurs unitaires que l'énoncé fournit — les compter, simplement, pour obtenir ce nombre. La question précédente montre qu'il n'y a qu'une seule orbite. La question d'encore avant

montre que l'ordre commun des groupes d'isotropie de cette action, qui est l'ordre de F, est 4. La formule des classes montre alors que l'ordre de $\mathrm{SO}(3,\mathbb{F}_5)$ est $4 \times 30 = 120$.

2.8) On considère l'action de $\mathrm{SO}(3,\mathbb{F}_5)$ sur lui-même par conjugaison. On cherche le cardinal de l'orbite de R^2, qui est sa classe de conjugaison dans $\mathrm{SO}(3,\mathbb{F}_5)$. Selon l'énoncé, le groupe d'isotropie de R^2 est S, dont l'ordre est 8. On en déduit *via* la formule des classes que le cardinal de l'orbite cherché est $\frac{120}{8} = 15$.

2.9) Les matrices P et $-M$ sont respectivement d'ordres 3 et 2. En outre, elles commutent, comme l'assure l'énoncé (on peut aussi faire le calcul, très simple). Elles engendrent donc un groupe cyclique d'ordre 6 — dont le produit $-PM$ est un générateur. Ainsi, $\langle P, -M\rangle \simeq \mathbb{Z}/6\mathbb{Z}$.
On reprend l'action de $\mathrm{SO}(3,\mathbb{F}_5)$ sur lui-même par conjugaison. On considère cette fois l'orbite de P dont le groupe d'isotropie est d'ordre 6. Selon la formule des classes, sa classe de conjugaison a exactement $\frac{120}{6} = 20$ éléments.

2.10) (i) Puisque $\mathrm{SO}(3,\mathbb{F}_5)$ est engendré par ses éléments d'ordre 2, la partie **2.2** assure que $D(\mathrm{SO}(3,\mathbb{F}_5)) = C(\mathrm{SO}(3,\mathbb{F}_5))$, et donc que le quotient $\mathrm{SO}(3,\mathbb{F}_5)/D(\mathrm{SO}(3,\mathbb{F}_5))$ est de la forme $(\mathbb{Z}/2\mathbb{Z})^r$ où $r \geq 0$.
D'une part, l'indice d'un sous-groupe de $\mathrm{SO}(3,\mathbb{F}_5)$, qui est d'ordre $2^3 \times 3 \times 5$, divise ce nombre. Donc $r \leq 3$. D'autre part, $r \geq 1$ puisque $-M$ n'est pas dans le groupe dérivé de $\mathrm{SO}(3,\mathbb{F}_5)$. Il reste les cas $r \in \{1,2,3\}$.

(ii) Puisque P est d'ordre 3, on peut écrire $P = P^4 = \left(P^2\right)^2$, ce qui montre que P est dans $C(\mathrm{SO}(3,\mathbb{F}_5)) = D(\mathrm{SO}(3,\mathbb{F}_5))$.

(iii) Puisque P est dans le groupe dérivé qui est normal, tous ses conjugués sont aussi dans le groupe dérivé : $D(\mathrm{SO}(3,\mathbb{F}_5))$ contient les 20 éléments de la classe de conjugaison de P. Par ailleurs, de façon analogue, $D(\mathrm{SO}(3,\mathbb{F}_5))$ contient les 15 éléments de la classe de conjugaison de R^2 puisque ce dernier est un carré, donc un élément du groupe dérivé. Ainsi, puisque ces deux classes sont disjointes (elles sont distinctes), l'ordre du groupe $D(\mathrm{SO}(3,\mathbb{F}_5))$ est supérieur ou égal à $20 + 15 = 35$, donc strictement supérieur à $30 = \frac{120}{4}$. On en déduit que l'indice de ce groupe dérivé est strictement inférieur à 4, ce qui montre, compte tenu du (i) ci-dessus, que l'ordre du groupe quotient $\mathrm{SO}(3,\mathbb{F}_5)/D(\mathrm{SO}(3,\mathbb{F}_5))$ est 2, ce qu'il fallait démontrer.

[En poussant davantage l'étude, on montrerait le groupe dérivé $D(\mathrm{SO}(3,\mathbb{F}_5))$ est simple d'ordre 60, donc isomorphe au groupe alterné $\mathfrak{A}_5$.]

UVSQ 2022/2023
Licence de sciences et technologie, santé
LSMA610 (groupes et géométrie)
9 mai 2023

Contrôle continu : épreuve de remplacement

(durée : une heure et demie)

1 Ordre ou indice premier [4 points]

Soient G un groupe fini et p un nombre premier.

1.1) Un sous-groupe d'ordre p de G est-il nécessairement abélien ?

1.2) Un sous-groupe d'indice p de G est-il nécessairement distingué ?

2 Déterminant positif [4 points]

Soit n un entier naturel non nul. On note $\mathrm{GL}_+(n,\mathbb{R})$ l'ensemble des matrices de $\mathrm{GL}(n,\mathbb{R})$ dont le déterminant est strictement positif.

2.1) Montrer que $\mathrm{GL}_+(n,\mathbb{R})$ est un sous-groupe distingué de $\mathrm{GL}(n,\mathbb{R})$.

2.2) Montrer que le quotient $\mathrm{GL}(n,\mathbb{R})/\mathrm{GL}_+(n,\mathbb{R})$ est un groupe abélien et calculer son ordre.

3 Ordre maximal dans $\mathrm{GL}(n,\mathbb{F}_q)$ [12 points]

On note $\mathbb{F}_7$ le corps $\mathbb{F}_7 = \mathbb{Z}/7\mathbb{Z}$.
On note également $\mathcal{M}_2(\mathbb{F}_7)$ l'espace des matrices carrées 2×2 à coefficients dans $\mathbb{F}_7$ et $\mathrm{GL}(2,\mathbb{F}_7)$ le groupe de ces matrices qui sont inversibles.

L'objet de cette partie consiste à montrer que $\mathrm{GL}(2,\mathbb{F}_7)$ *contient un élément d'ordre* $7^2-1=48$ *et que tout élément de* $\mathrm{GL}(2,\mathbb{F}_7)$ *a un ordre inférieur ou égal à* 48[♪].

3.1) Décomposer le cardinal de $\mathcal{M}_2(\mathbb{F}_7)$ et l'ordre du groupe $\mathrm{GL}(2,\mathbb{F}_7)$ en produits de facteurs premiers.

3.2) Soit $g\in\mathcal{M}_2(\mathbb{F}_7)$. En faisant la division euclidienne de tout $P\in\mathbb{F}_7[X]$ par le polynôme caractéristique de g et en utilisant le théorème de Cayley-Hamilton, montrer que le cardinal du sous-ensemble

$$\{P(g),\ P\in\mathbb{F}_7[X]\}$$

de $\mathcal{M}_2(\mathbb{F}_7)$ est inférieur ou égal à 49.

3.3) Soit $g\in\mathrm{GL}(2,\mathbb{F}_7)$. En considérant l'ensemble $\{g^k,\ k\in\mathbb{N}\}$, montrer que l'ordre de g est au plus 48.

3.4) Soit $\gamma=\begin{pmatrix}0&-3\\1&-1\end{pmatrix}\in\mathrm{GL}(2,\mathbb{F}_7)$. Calculer γ^8. En déduire soigneusement l'ordre de γ dans $\mathrm{GL}(2,\mathbb{F}_7)$.

3.5) Montrer que l'ordre maximal d'un élément de $\mathrm{GL}(2,\mathbb{F}_7)$ est 7^2-1.

3.6) Est-il vrai que l'ordre de tout élément de $\mathrm{GL}(2,\mathbb{F}_7)$ divise 48 ?

[♪] Ce résultat se généralise en remplaçant $\mathbb{F}_7$ par n'importe quel corps fini $\mathbb{F}_q$ et $\mathrm{GL}(2,\mathbb{F}_7)$ par $\mathrm{GL}(n,\mathbb{F}_q)$, $n\geqslant 1$.

UVSQ 2022/2023
Licence de sciences et technologie, santé
LSMA610 (groupes et géométrie)
9 mai 2023

Epreuve de remplacement : un corrigé succinct

1 Ordre ou indice premier

1.1) Tout groupe fini dont l'ordre est un nombre premier p est cyclique. En effet, tout élément non neutre d'un tel groupe engendre un sous-groupe dont l'ordre divise p mais n'est pas 1 : cet ordre est p. Ainsi, ledit élément engendre le groupe tout entier qui est donc cyclique, dont abélien : la réponse est oui.

1.2) Le groupe engendré par la transposition (12) est un sous-groupe non distingué d'indice 3 dans $\mathfrak{S}_3$: la réponse est non.

2 Déterminant positif

2.1) L'application $f : \mathrm{GL}(n,\mathbb{R}) \to \{\pm 1\}$, $M \mapsto \frac{\det M}{|\det M|}$ est un homomorphisme de groupes dont le noyau est $\mathrm{GL}_+(n,\mathbb{R})$. Cela montre à la fois que $\mathrm{GL}_+(n,\mathbb{R})$ est un sous-groupe de $\mathrm{GL}(n,\mathbb{R})$ et qu'il est normal.

2.2) L'homomorphisme f est surjectif. En effet, la matrice diagonale $\mathrm{diag}(-1,1,\dots 1)$ a -1 pour déterminant. Ainsi, le premier théorème d'isomorphisme appliqué à f montre que $\mathrm{GL}(n,\mathbb{R})/\mathrm{GL}_+(n,\mathbb{R})$ est isomorphe au groupe multiplicatif $\{\pm 1\}$, qui est cyclique (donc abélien) d'ordre 2.

3 Ordre maximal dans $\mathrm{GL}(n,\mathbb{F}_q)$

3.1) Le cardinal de $\mathcal{M}_2(\mathbb{F}_7)$ est $7^{2^2} = 7^4$. L'ordre de $\mathrm{GL}(2,\mathbb{F}_7)$ est $(7^2-1)(7^2-7) = 48\times 42 = 2^5\times 3^2\times 7$.

3.2) Soient $P \in \mathbb{F}_7[X]$ et χ_g le polynôme caractéristique de g qui est de degré 2. On fait la division euclidenne de P par χ_g sur le corps $\mathbb{F}_7$: soient $Q \in \mathbb{F}_7[X]$ et $a,b \in \mathbb{F}_7$ tels que $P = Q\chi_g + aX + b$. Le théorème de Cayley-Hamilton assure que $\chi_g(g)$ est la matrice nulle, ce qui entraîne, en spécialisant par g, que $P(g) = ag + b$. Comme le cardinal de $\left\{(a,b), a,b \in \mathbb{F}^7\right\} = (\mathbb{F}_7)^2$ est $7^2 = 49$, cela montre que $\#\{P(g),\ P \in \mathbb{F}_7[X]\} \leqslant 49$.

3.3) On note O_2 la matrice nulle de $\mathcal{M}_2(\mathbb{F}_7)$. Puisque g est inversible, aucun des g^k n'est O_2. Comme $O_2 \in \{P(g),\ P \in \mathbb{F}_7[X]\}$, cela montre que $\#\left\{g^k,\ k \in \mathbb{N}\right\} \leqslant 49 - 1 = 48$. Cela montre qu'au moins deux éléments de l'ensemble $\left\{g^k, 0 \leqslant k \leqslant 48\right\}$ sont égaux : soient p et q deux entiers tels que $0 \leqslant p < q \leqslant 48$ tels que $g^p = g^q$. Alors, puisque g est inversible, $g^{q-p} = I_2$, ce qui montre que l'ordre de g est inférieur ou égal à $q - p \in \{1,\dots,48\}$.

3.4) On calcule : $\gamma^2 = \begin{pmatrix} -3 & 3 \\ -1 & -2 \end{pmatrix}$, $\gamma^4 = \begin{pmatrix} -1 & -1 \\ -2 & 1 \end{pmatrix}$ et $\gamma^8 = 3I_2$. On continue : $\gamma^{16} = 2I_2$, $\gamma^{24} = -I_2$ et $\gamma^{48} = I_2$. Donc l'ordre de g divise $48 = 2^4\times 3$, mais ne divise ni $24 = \frac{48}{2}$ ni $16 = \frac{48}{3}$: c'est 48.

3.5) Tout élément de $\mathrm{GL}(2,\mathbb{F}_7)$ est d'ordre inférieur ou égal à l'ordre de g qui est 48. Donc l'ordre maximal d'un élément de $\mathrm{GL}(2,\mathbb{F}_7)$ est $48 = 7^2 - 1$.

3.6) L'ordre de $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}(2,\mathbb{F}_7)$ est 7 : la réponse est non puisque 7 ne divise pas 48. Sans être aussi explicite, on peut argumenter que $\mathrm{GL}(2,\mathbb{F}_7)$ a au moins un 7-Sylow, qui est cyclique d'ordre 7 ; cela montre que $\mathrm{GL}(2,\mathbb{F}_7)$ des éléments d'ordre 7 (contient au moins six).

UVSQ 2023/2024
Licence de sciences et technologie, santé
LSMA610 (groupes et géométrie)
7 mai 2024

Contrôle continu : épreuve de remplacement

(durée : une heure et demie)

— *Bon, il faut l'écrire : aucun document ni aucun instrument électronique n'est autorisé pour cette épreuve* —

Chacun sait, mais on le redit ici, que le nombre π est transcendant, ce qui signifie qu'il n'est racine d'aucun polynôme non nul à coefficients entiers.

1 Action ? [6 points]

On donne ci-dessous deux ensembles G et X, une loi de composition interne sur G que l'on note $\star$ et une application α définie sur $G \times X$. Si l'on veut, lorsque $g \in G$ et $x \in X$, on pourra noter $\alpha(g,x) = g \cdot x$. Dans chaque cas, en justifiant rapidement mais proprement, dire si α est une action à gauche du groupe G sur l'ensemble X.

1.1) $G = \mathbb{N}$, X est l'ensemble des nombres complexes de module 1, $\star$ est l'addition dans $\mathbb{N}$ et $\alpha(n,z) = z^n$.

1.2) $G = \mathrm{End}\left(\mathbb{R}^2\right)$ est l'ensemble des applications linéaires de $\mathbb{R}^2$ dans lui-même, $\star$ est l'addition dans $\mathrm{End}\left(\mathbb{R}^2\right)$, X est l'ensemble des droites vectorielles de $\mathbb{R}^2$ et $\alpha(f,D) = f(D)$ qui est l'image par l'endomorphisme f de la droite D.

1.3) $G = X = \mathfrak{S}_8$ est l'ensemble des bijections de $\{1,\dots,8\}$ dans lui-même, $\star$ est la composition des applications et $\alpha(g,x) = gxg^{-1}x^{-1} = g \circ x \circ g^{-1} \circ x^{-1}$.

1.4) $G = \mathfrak{S}_8$ est l'ensemble des bijections de $\{1,\dots,8\}$ dans lui-même, $\star$ est la composition des applications, X est l'ensemble des 5-Sylow de G et $\alpha(\sigma,S) = \sigma S = \{\sigma \circ s,\ s \in S\}$ est la classe à gauche de la permutation σ modulo le 5-Sylow S de $\mathfrak{S}_8$.

2 Autour du Klein [4 points]

On note K le sous-groupe de Klein du groupe symétrique $\mathfrak{S}_4$; il est engendré par les produits de transpositions à supports disjoints et est isomorphe au groupe produit $(\mathbb{Z}/2\mathbb{Z})^2$ — c'est dans le cours.

2.1) Montrer que le groupe-quotient du groupe alterné $\mathfrak{A}_4$ par K est isomorphe à $\mathbb{Z}/3\mathbb{Z}$.

2.2) Montrer que le groupe-quotient du groupe symétrique $\mathfrak{S}_4$ par K est isomorphe au groupe symétrique $\mathfrak{S}_3$.

2.3) Est-il vrai que $\mathfrak{A}_4$ est isomorphe au groupe produit $(\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})^2$?

2.4) Est-il vrai que $\mathfrak{S}_4$ est isomorphe au groupe produit $\mathfrak{S}_3 \times (\mathbb{Z}/2\mathbb{Z})^2$?

3 Quand le quotient par le centre est abélien [4 points]

Soient G un groupe et $Z(G)$ son centre. On note $D(G)$ le groupe dérivé de G, qui est le sous-groupe de G engendré par ses commutateurs. Démontrer que le groupe-quotient $G/Z(G)$ est abélien si, et seulement si $D(G) \subseteq Z(G)$.

4 Sous-groupes de type fini de $\mathbb{R}$ [6 points]

4.1) Montrer que le sous groupe de $(\mathbb{R},+)$ engendré par 1 et $\sqrt{2}$ est isomorphe à $\mathbb{Z}^2$.

4.2) Le sous-groupe de $(\mathbb{R},+)$ engendré par 1, $\sqrt{2}$ et $\sqrt{3}$ est (évidemment) un groupe abélien de type fini. Quel est son rang ? Quels sont ses facteurs invariants ?

4.3) Montrer que pour tout $r \in \mathbb{N}$, le groupe additif $\mathbb{R}$ contient un sous-groupe abélien libre de rang r.

UVSQ 2023/2024
Licence de sciences et technologie, santé
LSMA610 (groupes et géométrie)
7 mai 2024

Contrôle continu : épreuve de remplacement — un corrigé succinct —

1 Action ? [6 points]

1.1) G n'est (même) pas un groupe : la réponse est non.

1.2) Si $f \in \mathrm{End}\left(\mathbb{R}^2\right)$ n'est pas inversible et si D est une droite de $\mathbb{R}^2$ contenue dans le noyau de f, alors $f(D) = (0)$: ce n'est pas une droite. Dans ces conditions, $D \in X$ mais $f \cdot D \notin X$: ce n'est pas une action, la réponse est non.

1.3) Si x est une permutation non triviale de $\{1, \ldots, 8\}$, alors $\mathrm{id} \cdot x = \mathrm{id} \neq x$. Donc ce n'est pas une action : la réponse est non.

1.4) Si $\sigma \in \mathfrak{S}_8$ et si S est un 5-Sylow de $\mathfrak{S}_8$, alors σS n'est un sous-groupe de $\mathfrak{S}_8$ que si $\sigma \in S$. Par exemple, si σ est une transposition, elle n'est dans aucun 5-Sylow (un 5-Sylow n'a aucun élément d'ordre 2) et si S est n'importe quel 5-Sylow, σS n'est (même) pas un sous-groupe de $\mathfrak{S}_8$, donc pas un 5-Sylow. La réponse est non : ce n'est pas une action.

2 Autour du Klein [4 points]

2.1) Le groupe K est d'ordre 4, distingué dans $\mathfrak{A}_4$ qui est d'ordre 12. Donc $\mathfrak{A}_4/K$ est un groupe d'ordre $\frac{12}{4} = 3$ qui est un nombre premier : il est donc cyclique, isomorphe à $\mathbb{Z}/3\mathbb{Z}$.

2.2) Le groupe K est distingué dans $\mathfrak{S}_4$ qui est d'ordre 24. Donc le groupe-quotient $\mathfrak{S}_4/K$ est d'ordre $\frac{24}{4} = 6$. Il est donc isomorphe à $\mathfrak{S}_3$ ou à $\mathbb{Z}/6\mathbb{Z}$ (il n'y a que deux classes d'isomorphismes de groupes d'ordre 6). Or, tout élément de $\mathfrak{S}_4$ est d'ordre 1, 2, 3 ou 4. Donc $\mathfrak{S}_4/K$ n'a pas d'élément d'ordre 6. Il en résulte que $\mathfrak{S}_4/K \simeq \mathfrak{S}_3$.

2.3) Le groupe $(\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})^2$ est abélien, pas $\mathfrak{A}_4$. La réponse est non.

2.4) Le centre de $\mathfrak{S}_4$ est trivial alors que celui de $\mathfrak{S}_3 \times (\mathbb{Z}/2\mathbb{Z})^2$ contient $\{\mathrm{id}\} \times (\mathbb{Z}/2\mathbb{Z})^2$. La réponse est non.

3 Quand le quotient par le centre est abélien [4 points]

On note $Z = Z(G)$ pour plus de simplicité. On note aussi $[x, y] = x^{-1}y^{-1}xy$ qui est un commutateur. Par définition, le groupe $D(G)$ est le sous-groupe de G engendré par $\left\{[x, y],\ (x, y) \in G^2\right\}$.

La loi du groupe-quotient G/Z est donnée par la formule $xZ \cdot yZ = xyZ$, pour tous $x, y \in G$. Dire que G/Z est abélien signifie donc que pour tous $x, y \in G$, on a $xyZ = yxZ$, ce qui équivaut à $yx \in xyZ$, ou encore à $y^{-1}x^{-1}yx \in Z$. Autrement dit, G/Z est abélien si, et seulement si tout commutateur de G est dans Z, ce qui équivaut encore à l'inclusion $D(G) \subseteq Z$. C'est cela qu'il fallait démontrer.

4 Sous-groupes de type fini de $\mathbb{R}$ [6 points]

4.1) Soit $f : \mathbb{Z}^2 \to \left\langle 1, \sqrt{2} \right\rangle$ l'applicaiton définie par $f(m, n) = m + n\sqrt{2}$. Cette application est (évidemment) un homomorphisme de groupes. Il est surjectif par caractérisation des sous-groupes engendrés. Par ailleurs, si $(m, n) \in \ker f$, alors $m + n\sqrt{2} = 0$ ce qui impose que $m = n = 0$ puisque $\sqrt{2}$ est irrationnel. Donc f est injectif : c'est un isomorphisme de groupes.

4.2) On note $G = \langle 1, \sqrt{2}, \sqrt{3} \rangle$, sous-groupe de $\mathbb{R}$. En raisonnant comme précédemment, il suffit de montrer que toute relation linéaire $a + b\sqrt{2} + c\sqrt{3} = 0$ à coefficients entiers a, b, c est nécéssairement triviale pour montrer que G est isomorphe à $\mathbb{Z}^3$.
Soient ainsi $a, b, c \in Z$ tels que $a + b\sqrt{2} + c\sqrt{3} = 0$. Alors, $a^2 = \left(b\sqrt{2} + c\sqrt{3}\right)^2 = 2b^2 + 3c^2 + 2bc\sqrt{6}$. Comme $\sqrt{6}$ est irrationnel, cela impose que $bc = 0$ et $a^2 - 2b^2 - 3c^2 = 0$. Si $b = 0$, alors $a^2 = 3c^2$ ce qui impose que $a = c = 0$ puisque $\sqrt{3}$ est irrationnel. Si $c = 0$, alors $a^2 = 2b^2$ ce qui impose que $a = b = 0$ puisque $\sqrt{2}$ est irrationnel. On a montré que nécessairement, $a = b = c = 0$, ce qui finit de démontrer que $G \simeq \mathbb{Z}^3$.
Ainsi, le rang du groupe abélien fini G est 3 et sa composante de torsion, comme celle de tout sous-groupe de $\mathbb{R}$, est nulle : G n'a pas de facteurs invariants.

4.3) Soit $r \in \mathbb{N}$, $r \geqslant 1$. Alors, puisque π est transcendant, la famille $\left\{1, \pi, \pi^2, \ldots, \pi^{r-1}\right\}$ est libre sur $\mathbb{Z}$. Donc le sous-groupe abélien fini $\left\langle 1, \pi, \pi^2, \ldots, \pi^{r-1} \right\rangle$ est un sous-groupe abélien libre de rang r de $\mathbb{R}$.

UVSQ 2024/2025
Licence de sciences et technologie, santé
LSMA610 (groupes et géométrie)
12 mai 2025

Contrôle continu : épreuve de remplacement

(durée : une heure et demie)

— Bon, il faut l'écrire : aucun document ni aucun instrument électronique n'est autorisé pour cette épreuve —

1 Conjugaison dans $\mathrm{SL}(3,\mathbb{F}_2)$ [10 points]

On note $\mathbb{F}_2$ le corps $\mathbb{Z}/2\mathbb{Z}$.

1.1) Quel est l'ordre du groupe $\mathrm{SL}(3,\mathbb{F}_2)$?

1.2) On note $P = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \in \mathrm{SL}(3,\mathbb{F}_2)$. Montrer que P et P^2 sont conjuguées dans $\mathrm{SL}(3,\mathbb{F}_2)$.

[On pourra par exemple interpréter P comme une permutation des vecteurs de la base canonique de $(\mathbb{F}_2)^3$.]

1.3) Calculer l'ordre des 3-sous-groupes de Sylow de $\mathrm{SL}(3,\mathbb{F}_2)$. En déduire que tous les éléments d'ordre 3 de $\mathrm{SL}(3,\mathbb{F}_2)$ sont conjugués.

1.4) Soit S l'ensemble des matrices triangulaires supérieures de $\mathrm{SL}(3,\mathbb{F}_2)$:

$$S = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix},\ (a,b,c) \in (\mathbb{F}_2)^3 \right\}$$

C'est un sous-groupe de $\mathrm{SL}(3,\mathbb{F}_2)$, on ne demande pas de montrer ce résultat très classique. Montrer que S est un 2-sous-groupes de Sylow de $\mathrm{SL}(3,\mathbb{F}_2)$.

1.5) On note R la matrice de $\mathrm{SL}(3,\mathbb{F}_2)$ suivante :

$$R = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

Calculer l'ordre de R. En déduire la liste explicite des éléments d'ordre 2 de S et celle de ses éléments d'ordre 4.

1.6) Montrer que tous les éléments d'ordre 4 de $\mathrm{SL}(3,\mathbb{F}_2)$ sont conjugués.

1.7) On note A et B les matrices de $\mathrm{SL}(3,\mathbb{F}_2)$ suivantes (ce sont des matrices compagnon) :

$$A = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \text{ et } B = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}.$$

On admet — c'est un calcul élémentaire — que A et B sont d'ordre 7. Calculer les polynômes caractéristiques de A et de B. En déduire que tous les éléments non triviaux du groupe engendré par A ne sont pas conjugués.

2 Semi-stabilité par conjugaison [10 points]

On note t et u les deux matrices $t = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ et $u = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$, et G le sous-groupe de $\mathrm{SL}(2,\mathbb{Z})$ qu'elles engendrent. On note I_2 l'élément neutre de $\mathrm{SL}(2,\mathbb{Z})$.

2.1) Calculer l'ordre de t et l'ordre de u dans G.

2.2) On note H le sous-groupe de G engendré par $\{t^n u t^{-n},\ n \in \mathbb{N} \setminus \{0\}\}$: avec la notation habituelle,

$$H = \left\langle t^n u t^{-n},\ n \geq 1 \right\rangle.$$

Montrer soigneusement que H est la réunion de $\{I_2\}$ et de l'ensemble

$$\Big\{ t^{m_0} u^{n_0} t^{m_1} u^{n_1} \dots t^{m_p} u^{n_p} t^{m_{p+1}},\ p \in \mathbb{N},\ (m_0, \dots, m_{p+1}, n_0, \dots, n_p) \in (\mathbb{Z} \setminus \{0\})^{2p+3},\ m_0 \geq 1,\ m_{p+1} \leq -1,\ \sum_{k=0}^{p+1} m_k = 0 \Big\}.$$

2.3) Montrer que $tHt^{-1} \subseteq H$.

L'objet de la suite de cette partie consiste à montrer que $t^{-1}Ht \not\subseteq H$.

2.4) On fait agir G sur l'ensemble $\mathcal{M}_{2,1}$ des vecteurs-colonne de dimension 2 à coefficients réels par l'action naturelle donnée par le produit matriciel :

$$\forall g = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in G,\ \forall v = \begin{pmatrix} x \\ y \end{pmatrix} \in \mathcal{M}_{2,1},\ g \cdot v = \begin{pmatrix} ax + cy \\ bx + dy \end{pmatrix}.$$

On note A et B les parties de $\mathcal{M}_{2,1}$ définies par

$$A = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathcal{M}_{2,1},\ |x| > |y| > 0 \right\} \quad \text{et} \quad B = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathcal{M}_{2,1},\ |y| > |x| > 0 \right\}.$$

Dessiner A et B.

2.5) Montrer que $t^n \cdot B \subseteq A$ et $u^n \cdot A \subseteq B$, pour tout $n \in \mathbb{Z} \setminus \{0\}$.

2.6) Montrer que $h \cdot B \subseteq A$, pour tout $h \in H \setminus \{I_2\}$.

2.7) En déduire que $u \notin H$.

2.8) Montrer que $t^{-1}Ht \not\subseteq H$.

UVSQ 2024/2025
Licence de sciences et technologie, santé
LSMA610 (groupes et géométrie)
12 mai 2025

Epreuve de remplacement : un corrigé succinct

1 Conjugaison dans $\mathrm{SL}(3,\mathbb{F}_2)$

1.1) C'est du cours : $|\mathrm{SL}(3,\mathbb{F}_2)| = \left(2^3-1\right)\left(2^3-2\right)\left(2^3-2^2\right) = 2^3\times 3\times 7 = 168$.
[Noter que puisque $\mathbb{F}_2$ n'a qu'un seul inversible, $\mathrm{SL}(3,\mathbb{F}_2) = \mathrm{GL}(3,\mathbb{F}_2)$.]

1.2) Un peu d'heurisitique, comme suggéré par l'énoncé : P est la matrice de la permutation (123) des trois vecteurs de la base canonique de $\mathbb{F}_2^3$, et $P^2 = \begin{pmatrix}0&1&0\\0&0&1\\1&0&0\end{pmatrix}$ est celle du 3-cycle $(123)^2 = (132)$. Du côté des permutations, la formule de conjugaison des cycles fournit $(132) = (23)(123)(23)^{-1}$.
Enfin, la matrice de la transposition (23) sur la base canonique de $\mathbb{F}_2^3$ est $\begin{pmatrix}1&0&0\\0&0&1\\0&1&0\end{pmatrix} \in \mathrm{SL}(3,\mathbb{F}_2)$. Ainsi,

$$P^2 = \begin{pmatrix}1&0&0\\0&0&1\\0&1&0\end{pmatrix} P \begin{pmatrix}1&0&0\\0&0&1\\0&1&0\end{pmatrix}^{-1}.$$

Toute personne sceptique est invitée à vérifier ce calcul ☺.

1.3) Puisque l'ordre de $\mathrm{SL}(3,\mathbb{F}_2)$ est $2^3\times 3\times 7$, ses 3-Sylow sont d'ordre 3 — donc cycliques. Le groupe engendré par P est cyclique d'ordre 3. C'est donc un 3-Sylow de $\mathrm{SL}(3,\mathbb{F}_2)$. Soit alors g un élément d'ordre 3 de $\mathrm{SL}(3,\mathbb{F}_2)$. Selon le second théorème de Sylow, g est contenu dans un 3-Sylow (qu'il engendre, par ailleurs). Mais comme les 3-Sylow sont tous conjugués, g est conjugué à un élément d'ordre 3 de $\langle P\rangle$, c'est-à-dire à P ou à P^2. Mais comme on a montré que P et P^2 sont conjugués, cela finit de démontrer que g est conjugué à P : tous les éléments d'ordre 3 de $\mathrm{SL}(3,\mathbb{F}_2)$ sont donc conjugués.

1.4) Les choix de a, b et c étant arbitraires, l'ordre de S est (évidemment) $2^3 = 8$. Par ailleurs, les 2-Sylow de $\mathrm{SL}(3,\mathbb{F}_2)$ sont d'ordre 2^3 puisque l'ordre de ce groupe est $2^3\times 3\times 7$. Donc S est un 2-Sylow de $\mathrm{SL}(3,\mathbb{F}_2)$.

1.5) On calcule : $R^2 = \begin{pmatrix}1&0&1\\0&1&0\\0&0&1\end{pmatrix}$ et $R^4 = I_3$, ce qui montre que l'ordre de R est 4. Ainsi, R^3 est également d'ordre 4, puisque 3 et 4 sont étrangers. Hormis I_3 qui est d'ordre 1, il reste les quatre matrices

$$\begin{pmatrix}1&1&0\\0&1&0\\0&0&1\end{pmatrix},\ \begin{pmatrix}1&0&0\\0&1&1\\0&0&1\end{pmatrix},\ \begin{pmatrix}1&1&1\\0&1&0\\0&0&1\end{pmatrix}\ \text{et}\ \begin{pmatrix}1&0&1\\0&1&1\\0&0&1\end{pmatrix}$$

qui sont toutes d'ordre 2 comme le montre un calcul immédiat. [En passant, cela montre que S est un groupe diédral.]

1.6) Puisque tous les 2-Sylow sont conjugués, il suffit de montrer que les deux élements d'ordre 4 de S, savoir R et R^3, sont conjugués. Pour cela, on peut faire un calcul direct comme par exemple

$$R^3 = \begin{pmatrix}1&1&0\\0&1&1\\0&0&1\end{pmatrix} = \begin{pmatrix}1&0&1\\0&1&1\\0&0&1\end{pmatrix} R \begin{pmatrix}1&0&1\\0&1&1\\0&0&1\end{pmatrix}^{-1},$$

ou raisonner sur le polynôme caractéristique et le polynôme minimal (deux matrices de dimension 3 ayant même polynôme caractéristique (scindé) et même polynôme minimal sont semblables).

1.7) On calcule ces polynômes caractéristiques : $\chi_A(X) = X^3 + X + 1$, $\chi_B(X) = X^3 + X^2 + 1$. Puisque ces deux polynômes sont distincts, A et B ne sont pas semblables, donc ne sont pas conjuguées dans $\mathrm{SL}(3, \mathbb{F}_2)$. Puisque B est d'ordre 7, elle est dans un 7-Sylow de $\mathrm{SL}(3, \mathbb{F}_2)$. Or, les 7-Sylow sont d'ordre 7, tous conjugués au groupe engendré par A. Donc il existe un élément de $\langle A \rangle$ qui est conjugué à B, ce dernier n'étant pas conjugué à A. Il n'est donc pas vrai que tous les éléments d'ordre 7 de $\langle A \rangle$ sont conjugués dans $\mathrm{SL}(3, \mathbb{F}_2)$.
[Pour aller un peu plus loin : $\mathrm{SL}(3, \mathbb{F}_2)$ contient deux classes de conjugaison d'éléments d'ordre 7.]

2 Semi-stabilité par conjugaison

2.1) Pour tout $n \in \mathbb{Z}$, $t^n = \begin{pmatrix} 1 & 2n \\ 0 & 1 \end{pmatrix}$ et $u^n = \begin{pmatrix} 1 & 0 \\ 2n & 1 \end{pmatrix}$, ce qui montre que t et u sont d'ordre infini.

2.2) On note $\mathcal{E}$ l'ensemble

$$\mathcal{E} = \{I_2\} \cup \Bigg\{ t^{m_0} u^{n_0} t^{m_1} u^{n_1} \dots t^{m_p} u^{n_p} t^{m_{p+1}},\ p \in \mathbb{N}, \\ (m_0, \dots, m_{p+1}, n_0, \dots, n_p) \in (\mathbb{Z} \setminus \{0\})^{2p+3}, \\ m_0 \geq 1,\ m_{p+1} \leq -1,\ \sum_{k=0}^{p+1} m_k = 0 \Bigg\}.$$

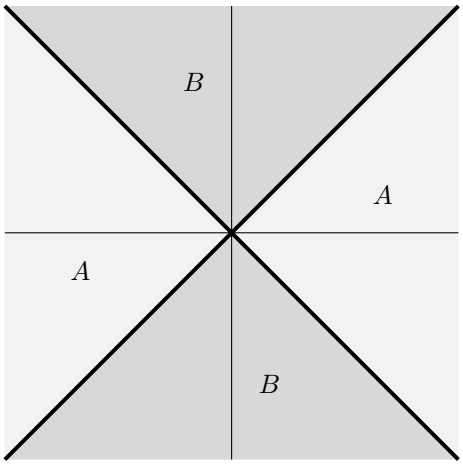
Il s'agit de montrer que $H = \mathcal{E}$.
On montre d'abord que $\mathcal{E}$ est un sous-groupe de G. Pour commencer, $\mathcal{E}$ n'est (évidemment) pas vide. Ensuite, soient $x = t^{m_0} u^{n_0} t^{m_1} u^{n_1} \dots t^{m_p} u^{n_p} t^{m_{p+1}}$ et $y = t^{r_0} u^{s_0} t^{r_1} u^{s_1} \dots t^{r_q} u^{s_q} t^{r_{q+1}}$ deux élements de $\mathcal{E}$, où $p, q \in \mathbb{N}$, les m_k, les n_k, les r_k et les s_k sont des entiers non nuls, $m_0 \geq 1$, $r_0 \geq 1$, $m_{p+1} \leq -1$, $s_{q+1} \leq -1$, et $\sum_{k=0}^{p+1} m_k = 0 = \sum_{k=0}^{q+1} r_k = 0$.
D'une part, $x^{-1} = t^{-m_{p+1}} u^{-n_p} t^{-m_p} u^{-n_{p-1}} \dots t^{-m_1} u^{-n_0} t^{-m_0}$, avec $-m_{p+1} \geq 1$, $-m_0 \leq -1$, les entiers $-n_k$ et $-m_k$ sont encore non nuls et enfin la somme des puissances de t dans cette écriture de x^{-1} s'écrit $\sum_{k=0}^{p+1} (-m_k) = -\sum_{k=0}^{p+1} m_k = 0$. Cela montre que $x^{-1} \in \mathcal{E}$.
D'autre part, $xy = t^{m_0} u^{n_0} t^{m_1} u^{n_1} \dots t^{m_p} u^{n_p} t^{m_{p+1}} t^{r_0} u^{s_0} t^{r_1} u^{s_1} \dots t^{r_q} u^{s_q} t^{r_{q+1}}$. Les entiers qui apparaissent en puissances de t ou de u sont encore non nuls, le premier d'entre eux est $m_0 \geq 1$, le dernier est $r_{q+1} \leq -1$ et la somme des puissances de t vaut $\sum_{k=0}^{p+1} m_k + \sum_{k=0}^{q+1} r_k = 0 + 0 = 0$. Cela montre que $xy \in \mathcal{E}$.
Ainsi, $\mathcal{E}$ est un sous-groupe de G.
Si $n \geq 1$, alors $t^n u t^{-n}$ est dans $\mathcal{E}$ — prendre $p = 0$, $m_0 = n$ et $m_1 = -n$. Ainsi, le groupe $\mathcal{E}$ contient un système de générateurs de H, donc il contient H. Inversement, il s'agit de montrer que tout élément de $\mathrm{SL}(2, \mathbb{Z})$ de la forme $t^{m_0} u^{n_0} t^{m_1} u^{n_1} \dots t^{m_p} u^{n_p} t^{m_{p+1}}$ — avec les hypothèses de la définition de $\mathcal{E}$ — est dans H, autrement dit que cet élément est un produit de $t^m u^n t^{-m} = (t^m u t^{-m})^n$, où $m \geq 1$ et $n \in \mathbb{Z} \setminus \{0\}$. Or, cela se voit sur l'écriture

$$\begin{aligned} t^{m_0} u^{n_0} t^{m_1} u^{n_1} \dots t^{m_p} u^{n_p} t^{m_{p+1}} &= \left(t^{m_0} u^{n_0} t^{m_1} u^{n_1} \dots t^{m_{p-1}} u^{n_{p-1}}\right) t^{m_p} u^{n_p} t^{m_{p+1}} \\ &= \left(t^{m_0} u^{n_0} t^{-m_0}\right) \left(t^{m_0+m_1} u^{n_1} t^{-m_0-m_1}\right) \dots \left(t^{m_0+m_1+\dots+m_p} u^{n_p} t^{-m_0-m_1-\dots-m_p}\right), \end{aligned}$$

l'égalité étant assurée par l'hypothèse $m_0 + m_1 + \dots + m_p = -m_{p+1}$ — la validité de l'écriture se montre par récurrence sur p *via* l'argument ci-dessus. Ainsi, on a montré que $\mathcal{E} \subseteq H$, ce qui finit de démontrer que $H = \mathcal{E}$.

2.3) Puisque H est engendré par les $t^n u t^{-n}$ où $n \geq 1$, il suffit de montrer que le conjugué par t de $t^n u t^{-n}$ est encore dans H, ce qui est évident puisque $t\left(t^n u t^{-n}\right) t^{-1} = t^{n+1} u t^{-n-1}$.

2.4)



2.5) On calcule : $t^n \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x+2ny \\ y \end{pmatrix}$ et $u^n \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ 2nx+y \end{pmatrix}$, pour tous $x, y \in \mathbb{R}$ et pour tout $n \in \mathbb{Z}$.
On suppose que $n \neq 0$ et que $\begin{pmatrix} x \\ y \end{pmatrix} \in B$. Alors, $|y| > |x| > 0$, et

$$|x+2ny| \geq 2|ny| - |x| = (2|n|-1)\,|y| + (|y|-|x|) > (2|n|-1)\,|y| \geq |y|$$

la dernière inégalité étant garantie par le fait que $|n| \geq 1$. Cela montre que $t^n \cdot \begin{pmatrix} x \\ y \end{pmatrix} \in A$. De la même façon, si $n \neq 0$ et si $\begin{pmatrix} x \\ y \end{pmatrix} \in A$, alors

$$|2nx+y] \geq (2|n|-1)\,|x| + (|x|-|y|) > |x|,$$

ce qui montre que $u^n \cdot \begin{pmatrix} x \\ y \end{pmatrix} \in B$.

2.6) Soit $h \in H$, $h \neq I_2$. Alors, l'écriture de h sous la forme d'un produit de la question **1.2** combinée avec la question **1.5** montre (par récurrence sur p) que $h \cdot B \subseteq A$.

2.7) On suppose que $u \in H$. Alors, $u^2 \in H$. D'une part, comme $u^2 \neq I_2$ (u est d'ordre infini), cela implique que $u^2 \cdot B \subseteq A$. D'autre part, $u^2 \cdot B = u \cdot (u \cdot B) \subseteq u \cdot A \subseteq B$, la première inclusion venant du fait que $u \in H \setminus \{I_2\}$ et donc que $u \cdot B \subseteq A$, la second venant de la question **2.5)**. Or, $A \cap B = \emptyset$: l'hypothèse "$u \in H$" ne tient pas. On a montré que $u \notin H$.
Autre raisonnement possible : ${}^t(1,2) \in B$ et $u \cdot {}^t(1,2) = {}^t(1,4) \in B$ et $A \cap B = \emptyset$. Donc $u \notin H$.

2.8) Bien sûr, $h = tut^{-1} \in H$, cela résulte de la définition de H. En revanche, $t^{-1}ht = u \notin H$. Et voilà.

UVSQ 2022/2023
Licence de sciences et technologie, santé
LSMA610 (groupes et géométrie)
29 juin 2023

Examen

(durée : deux heures)

1 Extension centrale ? [4 points]

1.1) Montrer que si deux groupes sont isomorphes, leurs centres sont également isomorphes.

1.2) Le groupe $\mathrm{GL}(3,\mathbb{C})$ est-il isomorphe au produit direct $\mathbb{C}^\times \times \mathrm{SL}(3,\mathbb{C})$, où $\mathbb{C}^\times$ désigne le groupe multiplicatif des nombres complexes non nuls ?

2 Un peu de Pauli [8 points]

On note $\mathcal{P}$ le sous-groupe de $\mathrm{GL}(2,\mathbb{C})$ engendré par les trois matrices

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \text{ et } \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

2.1) Calculer les ordres de σ_1, σ_2 et σ_3.

2.2) Calculer $\sigma_1\sigma_2\sigma_3$ et en déduire que iI_2 est dans le centre de $\mathcal{P}$. On note H le sous-groupe de $\mathcal{P}$ engendré par iI_2.

2.3) Montrer que le groupe-quotient $\mathcal{P}/H$ est engendré par les classes modulo H de σ_1 et σ_3.

2.4) En déduire que $\mathcal{P}/H$ est un groupe abélien d'ordre 4 et calculer ses facteurs invariants.

2.5) Montrer que $\mathcal{P}$ est un groupe fini et calculer son ordre.

2.6) On note $\mathcal{Q} = \mathcal{P} \cap \mathrm{SL}(2,\mathbb{C})$. Calculer l'indice $[\mathcal{P} : \mathcal{Q}]$ et montrer que tout élément de $\mathcal{P}$ s'écrit de manière unique sous la forme $i^\varepsilon q$ où $\varepsilon \in \{0,1\}$ et où $q \in \mathcal{Q}$.

2.7) Montrer que $\mathcal{Q}$ n'est pas abélien et qu'il contient au moins trois éléments d'ordre 4.

Cela suffit à démontrer que $\mathcal{Q}$ est isomorphe au groupe quaternionique $\mathbb{H}_8$, mais on ne demande pas de prouver cela.

3 Pas de gros symétrique dans l'alterné [8 points]

Soit n un entier naturel supérieur ou égal à 2. On note $\mathfrak{S}_n$ le groupe symétrique de n objets et $\mathfrak{A}_n$ son sous-groupe des permutations paires.

On cherche à montrer que le groupe alterné $\mathfrak{A}_{n+1}$ ne contient aucun sous-groupe isomorphe à $\mathfrak{S}_n$.

3.1) Montrer que $\mathfrak{A}_4$ n'a pas de sous-groupe isomorphe à $\mathfrak{S}_3$.

3.2) Montrer, par des considérations d'ordres, que si $\mathfrak{A}_{n+1}$ contient un sous-groupe isomorphe à $\mathfrak{S}_n$, alors n est nécessairement impair.

3.3) Soit m un entier supérieur ou égal à 3. On suppose que G est un sous-groupe de $\mathfrak{A}_{2m}$ isomorphe à $\mathfrak{S}_{2m-1}$.

(i) On note $(\mathfrak{A}_{2m}/G)_g$ l'ensemble des classes à gauches modulo G des éléments de $\mathfrak{A}_{2m}$. Calculer le cardinal de $(\mathfrak{A}_{2m}/G)_g$ en fonction de m.

(ii) On fait agir $\mathfrak{A}_{2m}$ sur $(\mathfrak{A}_{2m}/G)_g$ par translation à gauche et on note $\varphi : \mathfrak{A}_{2m} \to \mathfrak{S}_m$ l'homomorphisme de groupes que cette action induit. Montrer que φ est nécessairement injectif.

3.4) Déduire de ce qui précède que $\mathfrak{A}_{n+1}$ n'a pas de sous-groupe isomorphe à $\mathfrak{S}_n$.

UVSQ 2022/2023
Licence de sciences et technologie, santé
LSMA610 (groupes et géométrie)
29 juin 2023

Examen : un corrigé succinct

1 Extension centrale ?

1.1) Soit $f : G \to G'$ un isomorphisme de groupes. On note respectivement Z et Z' les centres des groupes G et G'. Si $z \in Z$ et si $g' \in G'$, en notant $g = f^{-1}(g')$, il vient $f(z)g' = f(zg) = f(gz) = g'f(z)$, ce qui montre que $f(z)$ est dans Z', et ainsi que $f(Z)$ est un sous-groupe de Z'. En appliquant ce résultat à f^{-1} qui est aussi un isomorphisme de groupes, on obtient que $f^{-1}(Z')$ est un sous-groupe de Z ; par image par f, on en déduit que Z' est un sous-groupe de $f(Z)$. On a montré que $f(Z) = Z'$. Ainsi, la restriction de f à Z a Z' pour image, ce qui montre que Z et Z' sont isomorphes.

1.2) Le centre de $\mathrm{GL}(3,\mathbb{C})$ est le groupe $\mathbb{C}^\times I_3 \simeq \mathbb{C}^\times$, alors que celui de $\mathbb{C}^\times \times \mathrm{SL}(3,\mathbb{C})$ est le produit des centres, savoir $\mathbb{C}^\times I_3 \times \mathbb{U}_3 I_3 \simeq \mathbb{C}^\times \times \mathbb{U}_3$ où $\mathbb{U}_3 = \langle \exp\left(\frac{2i\pi}{3}\right)\rangle$ est le groupe des racines complexes cubiques de l'unité. Or, les groupes $\mathbb{C}^\times$ et $\mathbb{C}^\times \times \mathbb{U}_3$ ne sont pas isomorphes puisque le premier a deux éléments d'ordre 3 (les éléments de $\mathbb{U}_3 \setminus \{1\}$) alors que le second en a huit (tous les éléments de $\mathbb{U}_3^2 \setminus \{1\}$).

2 Un peu de Pauli

Dans $\mathrm{GL}(2,\mathbb{C})$, on note $\mathcal{P}$ le groupe engendré par les trois matrices

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \text{ et } \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

2.1) On calcule (à peine tellement c'est visible) : $\sigma_1^2 = I_2$, $\sigma_2^2 = I_2$ et $\sigma_3^2 = I_2$. Ainsi, les σ_k sont tous d'ordre 2.

2.2) On calcule encore : $\sigma_1\sigma_2\sigma_3 = iI_2$, qui est à la fois dans $\mathcal{P}$ et dans le centre de $\mathrm{GL}(2,\mathbb{C})$, donc dans le centre de $\mathcal{P}$.

2.3) Dans $\mathcal{P}/H$, en notant $\overline{g}$ la classe modulo H d'un élément de $\mathcal{P}$, on a la relation $\overline{\sigma_1} \cdot \overline{\sigma_2} \cdot \overline{\sigma_3} = 1$, ce qui montre que $\overline{\sigma_2} = \overline{\sigma_1}^{-1} \cdot \overline{\sigma_3}^{-1} = \overline{\sigma_1} \cdot \overline{\sigma_3}$ est dans le sous-groupe de $\mathcal{P}/H$ engendré par $\overline{\sigma_1}$ et $\overline{\sigma_3}$. Puisque $\mathcal{P}/H$ est (évidemment) engendré par $\overline{\sigma_1}$, $\overline{\sigma_2}$ et $\overline{\sigma_3}$, il est engendré par les seuls $\overline{\sigma_1}$ et $\overline{\sigma_3}$.

2.4) $\overline{\sigma_1}$ et $\overline{\sigma_3}$ sont d'ordre 2 ; en outre, un calcul élémentaire montre que $\sigma_1\sigma_3 = -\sigma_1\sigma_3 = (iI_2)^2 \sigma_1\sigma_3$, ce qui implique que $\overline{\sigma_1} \cdot \overline{\sigma_3} = \overline{\sigma_3} \cdot \overline{\sigma_1}$. Ainsi, $\mathcal{P}/H$ est un groupe abélien engendré par deux éléments d'ordre 2 : il est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$. Il a deux facteurs invariants qui sont $(2,2)$.

2.5) Les groupes $\mathcal{P}/H$ et H sont tous les deux finis d'ordre 4. Donc $\mathcal{P}$ est fini d'ordre $|\mathcal{P}| = |H| \times [\mathcal{P} : H] = 4 \times 4 = 16$.

2.6) Le déterminant $\det : \mathcal{P} \to \mathbb{C}^\times$ est un homomorphisme de groupes dont le noyau est $\mathcal{Q}$. En outre, les déterminants des trois σ_k sont tous égaux à -1, ce qui montre que l'image de $\mathcal{P}$ par det est le sous-groupe $\{-1,1\}$ de $\mathbb{C}^\times$. Cela montre que $[\mathcal{P} : \mathcal{Q}] = 2$ — et donc que $\mathcal{Q}$ est d'ordre 8.

L'homothétie iI_2 est dans $\mathcal{P}$ et son déterminant est -1. Ainsi, si $g \in \mathcal{P} \setminus \mathcal{Q}$, alors $(iI_2)^3 \cdot g = -ig$ est dans $\mathcal{Q}$, ce qui montre que $\mathcal{P}$ est l'union disjointe $\mathcal{P} = \mathcal{Q} \cup i\mathcal{Q}$.

Enfin, l'unicité : si $i^\varepsilon q = i^{\varepsilon'} q'$ (notations évidentes), alors, en passant au déterminant, il vient $(-1)^\varepsilon = (-1)^{\varepsilon'}$ ce qui impose $\varepsilon = \varepsilon'$ puisque ces deux nombres sont dans $\{0,1\}$. On en déduit alors que $q = q'$.

2.7) On a vu que $\sigma_1\sigma_2 = i\sigma_3$. Alors, $i\sigma_1$ et $i\sigma_2$ sont dans $\mathcal{Q}$ et vérifient $(i\sigma_1)(i\sigma_2) = -\sigma_1\sigma_2 = -i\sigma_3$ alors que $(i\sigma_2)(i\sigma_1) = -\sigma_2\sigma_1 = i\sigma_3$. Cela montre que $\mathcal{Q}$ n'est pas abélien. Enfin, tous les $i\sigma_k \in \mathcal{Q}$ sont d'ordre 4.

Pour conclure : le groupe $\mathcal{Q}$ est non abélien d'ordre 8. Donc c'est le groupe diédral D_4 ou le groupe quaternionique $\mathbb{H}_8$. Comme il a au moins trois éléments d'ordre 4, il est isomorphe à $\mathbb{H}_8$, puisque D_4 n'a que deux éléments d'ordre 4 — alors que $\mathbb{H}_8$ en a six.

3 Pas de gros symétrique dans l'alterné

3.1) Si G était un sous-groupe G de $\mathfrak{A}_4$ isomorphe à $\mathfrak{S}_3$, alors l'indice de G dans $\mathfrak{A}_4$ serait 2. Donc G serait distingué dans $\mathfrak{A}_4$. Or, les seuls sous-groupes distingués de $\mathfrak{A}_4$ sont d'ordres 1, 4 et 12 alors que G est d'ordre 6. Il n'y a donc pas de tel G.

3.2) Si $\mathfrak{A}_{n+1}$ — qui est d'ordre $\frac{(n+1)!}{2}$ — contient un sous-groupe d'ordre $n!$, alors, $n!$ divise $\frac{(n+1)!}{2}$ ce qui oblige $\frac{n+1}{2}$ à être un nombre entier. Donc n est impair.

3.3) (i) $\#\left(\mathfrak{A}_{2m}/G\right)_g = \frac{|\mathfrak{A}_{2m}|}{|G|} = \frac{(2m)!}{2(2m-1)!} = m$.

(ii) Puisque $m \geqslant 3$, le groupe $\mathfrak{A}_{2m}$ est simple. Donc φ est constant ou injectif. Or, que φ soit constant signifie que $\sigma\tau G = \tau G$ pour tout $\sigma, \tau \in \mathfrak{A}_{2m}$, ce qui équivaut à $G = \mathfrak{A}_{2m}$. Comme les deux groupes G et $\mathfrak{A}_{2m}$ n'ont pas le même ordre, φ n'est pas constant. Donc il est injectif.

3.4) On suppose que $\mathfrak{A}_{n+1}$ a un sous-groupe G isomorphe à $\mathfrak{S}_n$, où $n \geqslant 2$. D'après **2)**, n est impair. Soit alors $m \geqslant 2$ tel que $n = 2m - 1$. Si $m \geqslant 3$, la question **3)** assure que $|\mathfrak{A}_{2m}|$ divise $|\mathfrak{S}_m|$, c'est-à-dire que $\frac{(2m)!}{2}$ divise $m!$, ce qui est faux puisque $\frac{(2m)!}{2} = m(2m-1)! > m!$. Donc $m = 2$ et G est un sous-groupe de $\mathfrak{A}_4$ isomorphe à $\mathfrak{S}_3$, ce qu'interdit la question **1)**. Il n'y donc aucun sous-groupe de $\mathfrak{A}_{n+1}$ qui soit isomorphe à $\mathfrak{S}_n$, dès que $n \geqslant 2$ (pour $n = 1$, il n'y a pas grand chose à dire).

UVSQ 2023/2024
Licence de sciences et technologie, santé
LSMA610 (groupes et géométrie)
28 juin 2024

Examen

– durée : deux heures –

— Bon, il faut l'écrire : aucun document ni aucun instrument électronique n'est autorisé pour cette épreuve —

1 Alors, cyclique ou non ? [3 points]

Un groupe abélien d'ordre 1003 est-il nécessairement cyclique ?

2 Un peu de $\mathfrak{S}_7$ [5 points]

On note $\mathfrak{S}_7$ le groupe des permutations de $\{1,2,3,4,5,6,7\}$.

2.1) Les éléments d'ordre 3 de $\mathfrak{S}_7$ sont-ils tous conjugués ?

2.2) Les éléments d'ordre 4 de $\mathfrak{S}_7$ sont-ils tous conjugués ?

2.3) Quel sous-groupe de $\mathfrak{S}_7$ les 7-cycles engendrent-ils ?

3 Classes de congruence de matrices symétriques [12 points]

On note $\mathcal{M}_2(\mathbb{F}_3)$ l'ensemble des matrices à 2 lignes et 2 colonnes et à coefficients dans le corps $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$. On note $\mathcal{S}$ l'ensemble des matrices symétriques de $\mathcal{M}_2(\mathbb{F}_3)$ et $G = \mathrm{GL}(2,\mathbb{F}_3)$ le groupe des matrices inversibles de $\mathcal{M}_2(\mathbb{F}_3)$. Si $M \in \mathcal{M}_2(\mathbb{F}_3)$, on note ${}^tM$ la transposée de M. Enfin, pour toute $M \in \mathcal{M}_2(\mathbb{F}_3)$ et pour toute $P \in G$, on note

$$P \cdot M = PM{}^tP.$$

3.1) Montrer que l'application

$$\begin{array}{ccc} G \times \mathcal{S} & \longrightarrow & \mathcal{S} \\ (P, M) & \longmapsto & P \cdot M \end{array} \qquad (1)$$

définit une action à gauche de G sur $\mathcal{S}$.

3.2) Calculer le cardinal de $\mathcal{S}$ et l'ordre de G.

3.3) Pour toute $S \in \mathcal{S}$, on appelle *classe de congruence de* S l'orbite de S sous l'action de G définie par (1). Montrer que deux matrices d'une même classe de congruence ont le même rang.

3.4) (i) Dans $\mathbb{F}_3$, résoudre l'équation $x^2 + y^2 = 1$ dont x et y sont les inconnues.

(ii) Calculer le groupe d'isotropie de I_2 sous l'action (1) et en déduire que la classe de congruence de I_2 contient 6 éléments.

3.5) On note $D = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \in \mathcal{S}$.

(i) Dans $\mathbb{F}_3$, résoudre l'équation $x^2 - y^2 = 1$ dont x et y sont les inconnues.

(ii) Calculer le groupe d'isotropie de D sous l'action (1) et en déduire le cardinal de la classe de congruence de D.

3.6) Calculer le groupe d'isotropie de $R = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in \mathcal{S}$ et le cardinal de la classe de congruence de R.

3.7) Montrer que les orbites de R et de $-R$ sont distinctes.

3.8) On dit que deux matrices A et B sont *congruentes* lorsqu'il existe une matrice inversible P telle que $B = PA{}^tP$. Démontrer soigneusement que toute matrice symétrique de $\mathcal{M}_2(\mathbb{F}_3)$ est congruente à l'une exactement des cinq matrices de la liste :

$$O_2,\ I_2,\ R,\ -R,\ D$$

où on a noté O_2 la matrice nulle de $\mathcal{M}_2(\mathbb{F}_3)$.

3.9) (i) Est-il vrai que deux matrices de rang 2 de $\mathcal{S}$ sont toujours congruentes ?

(ii) Est-il vrai que toute matrice de rang 1 de $\mathcal{S}$ est congruente à R ou à $-R$?

(iii) Combien $\mathcal{S}$ contient-il de matrices inversibles ?

UVSQ 2023/2024
Licence de sciences et technologie, santé
LSMA610 (groupes et géométrie)
28 juin 2024

Examen : un corrigé succinct

1 Alors, cyclique ou non ?

On décompose 1003 en facteurs premiers : $1003 = 17 \times 59$, les deux nombres 17 et 59 étant premiers (ça, c'est pas dur). Soit G un groupe abélien d'ordre 1003. Puisqu'aucun des nombres premiers de la factorisation de 1003 n'apparaît avec une valuation supérieur ou égale à 2, G ne peut pas avoir plus d'un facteur invariant. Donc G est cyclique et la réponse est oui.

[Evidemment, de la même manière, si p et q sont deux nombres premiers distincts, tout groupe abélien d'ordre pq est cyclique.]

2 Un peu de $\mathfrak{S}_7$

2.1) Le 3-cycle (123) et le produit des deux 3-cycles à supports disjoints (123)(456) sont tous les deux d'ordre 3 sans être conjugués : la réponse est non.

2.2) Le 4-cycle (1234) et le produit (12)(3456) sont tous les deux d'ordre 4 sans être conjugués : la réponse est non.

2.3) Un 7-cycle est une permutation paire. Les 7-cycles engendrent donc un sous-groupe du groupe alterné $\mathfrak{A}_7$. Puisque le conjugué d'un 7-cycle est encore un 7-cycle, les 7-cycles engendrent un sous-groupe distingué de $\mathfrak{A}_7$. Or, $\mathfrak{A}_7$ est simple. Le sous-groupe qu'engendrent les 7-cycles, puisqu'il n'est (évidemment) pas trivial, est donc $\mathfrak{A}_7$.

3 Classes de congruence de matrices symétriques

3.1) D'abord, si $P \in G$ et $M \in \mathcal{S}$, alors ${}^t(P \cdot M) = {}^t\left(PM{}^tP\right) = P{}^tM{}^tP = PM{}^tP = P \cdot M$, la dernière égalité venant du fait que M est symétrique. Cela montre que $P \cdot M \in \mathcal{S}$. Evidemment, $I_2 \cdot M = M$, pour toute $M \in \mathcal{S}$. Enfin, si $P, Q \in G$ et $M \in \mathcal{S}$, alors $P \cdot (Q \cdot M) = P\left(QM{}^tQ\right){}^tP = (PQ)M{}^t(PQ) = (PQ) \cdot M$. On a montré qu'on a affaire à une action à gauche de G sur $\mathcal{S}$.

3.2) Evidemment, $\operatorname{Card}\mathcal{S} = 3^3 = 27$ (libre choix des coefficients diagonaux et d'un coefficient anti-diagonal) et selon le cours, $|G| = (9-1) \times (9-3) = 48$.

3.3) Si P est inversibles, alors ${}^tP$ l'est aussi. Donc le rang de $PM{}^tP$ est le rang de M, puisque ces deux matrices sont équivalentes — si on en doute, on peut voir cela en interprétant ces matrices comme des endomorphismes de $(\mathbb{F}_3)^2$, *via* sa base canonique ; en ces termes, P et ${}^tP$ sont des isomorphismes, ce qui entraîne que les images de M et de $M{}^tP$ ont la même dimension, et que les images de $M{}^tP$ et de $PM{}^tP$ ont également la même dimension.

3.4) (i) On suppose que $x, y \in \mathbb{F}_3$ vérifient $x^2 + y^2 = 1$. Si $x = 0$, alors $y = \pm 1$; si $x = \pm 1$, alors $y = 0$. Cela montre que toute solution est dans l'ensemble $\{(0, \pm 1), (\pm 1, 0)\}$. Inversement, ces quatre couples sont évidemment des solutions de l'équation, que l'on a ainsi résolue.

(ii) Soit $P = \begin{pmatrix} x & z \\ y & t \end{pmatrix}$ une matrice du groupe d'isotropie de I_2, ce qui signifie que $P{}^tP = I_2$ (dans le jargon, P est une matrice *orthogonale* dans le corps $\mathbb{F}_3$). On effectue le produit : $P \in G_{I_2}$ si, et seulement si $x^2 + z^2 = 1 = y^2 + t^2$ et $xz + yt = 0$. Au vu de la question précédente, on obtient le groupe d'ordre 8

$$G_{I_2} = \left\{ \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}, \begin{pmatrix} 0 & \pm 1 \\ \pm 1 & 0 \end{pmatrix} \right\}.$$

Enfin, puisque G est d'ordre 48, l'orbite de I_2 sous l'action de G sur $\mathcal{S}$, qui est exactement la classe de congruence de I_2, contient $\frac{|G|}{|G_{I_2}|} = \frac{48}{8} = 6$ éléments. [Pour aller plus loin : le groupe G_{I_2} est le groupe diédral d'ordre 8.]

3.5) (i) On suppose que $x, y \in \mathbb{F}_3$ vérifient $x^2 - y^2 = 1$. Comme -1 n'est pas un carré dans $\mathbb{F}_3$, alors $x \neq 0$. Donc $x^2 = 1$ et $y = 0$. On a montré que les solutions de $x^2 - y^2 = 1$ sont les deux couples $(\pm 1, 0)$.

(ii) $P = \begin{pmatrix} x & z \\ y & t \end{pmatrix} \in G_D$ si, et seulement si $x^2 - z^2 = 1 = t^2 - y^2$ et $xy = zt$. On résout ce système au regard de la question précédente. On trouve que

$$G_D = \left\{ \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix} \right\}$$

est un groupe à 4 éléments — isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$ puisqu'il n'a pas d'élément d'ordre 4. Cela montre que la classe de congruence de D, qui est exactement l'orbite $G \cdot D$, contient $\frac{48}{4} = 12$ éléments.

3.6) $P = \begin{pmatrix} x & z \\ y & t \end{pmatrix} \in G_R$ si, et seulement si $x^2 = 1$ et $xy = y^2 = 0$. Cela montre que G_R est formé de toutes les matrices trigonales supérieures de G :

$$G_R = \left\{ \begin{pmatrix} x & z \\ 0 & t \end{pmatrix},\ x, t \neq 0 \right\}.$$

On compte : l'ordre de G_R est $2 \times 2 \times 3 = 12$, ce qui montre que la classe de congruence de R contient $\frac{48}{12} = 4$ éléments.

3.7) On suppose que $P = \begin{pmatrix} x & z \\ y & t \end{pmatrix} \in G$ vérifie $P \cdot R = -R$. Alors, $x^2 = -1$, ce qui est impossible dans $\mathbb{F}_3$. Ainsi, R et $-R$ ne sont pas dans la même classe de congruence.

3.8) Puisque (évidemment) $P \cdot (-R) = -P \cdot R$, les deux matrices symétriques R et $-R$ ont le même groupe d'isotropie à 12 éléments. Donc l'orbite de $-R$ a aussi 4 éléments — distincts de ceux de l'orbite de R, selon la question précédente.
Ainsi, $\mathcal{S}$, qui a 27 éléments, contient les 5 orbites distinctes de cardinaux respectifs 1 (pour l'orbite de O_2), 4 (pour l'orbite de R), 4 (pour l'orbite de $-R$), 6 (pour l'orbite de I_2) et 12 (pour l'orbite de D). Comme $27 = 1+4+4+6+12$, il n'y a pas d'autre orbite que ces cinq-là, ce qui démontre le résultat.

3.9) (i) I_2 et D sont symétriques, de rang 2 et ne sont pas congruentes : la réponse est non.

(ii) Les matrices d'une même classe de congruence ont le même rang (question **3.3)**). Parmi les cinq représentantes trouvées de classes de congruence, seules les matrices R et $-R$ sont de rang 1. Donc toute matrice de rang 1 est dans la classe de R ou dans celle de $-R$ (il y en 8 en tout) : la réponse est oui.

(iii) Les matrices symétriques inversibles sont celles dont le rang est 2 : ce sont les matrices des classes de congruence de I_2 et de D. Il y en a donc $6 + 12 = 18$.

UVSQ 2024/2025
Licence de sciences et technologie, santé
LSMA610 (groupes et géométrie)
27 juin 2025

Examen

(durée : deux heures)

— Bon, il faut l'écrire : aucun document ni aucun instrument électronique n'est autorisé pour cette épreuve —

1 Un sous-groupe de $\mathrm{GL}(2,\mathbb{F}_3)$ [6 points]

On note $\mathbb{F}_3$ le corps $\mathbb{Z}/3\mathbb{Z}$. Dans le groupe linéaire $\mathrm{GL}(2,\mathbb{F}_3)$, on note

$$r = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{et} \quad s = \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix}.$$

On note R (*resp.* S) le sous-groupe de $\mathrm{GL}(2,\mathbb{F}_3)$ engendré par r (*resp.* s) et G le sous-groupe engendré par $\{r,s\}$.

1.1) Calculer avec soin l'ordre de R et celui de S.

1.2) Montrer que $R \lhd G$ et que $R \cap S$ est le groupe trivial.

1.3) En déduire soigneusement l'ordre de G.

[On pourra montrer que l'ensemble des $\rho\sigma$ où $\rho \in R$ et $\sigma \in S$ est un sous-groupe de G et raisonner dessus.]

1.4) Quel est l'indice de G dans $\mathrm{GL}(2,\mathbb{F}_3)$?

2 Action doublement transitive [14 points]

Lorsqu'un groupe G agit (à gauche) sur un ensemble X à au moins 2 éléments, on dit que l'action est *doublement transitive* lorsque

$$\forall (x,y,z,t) \in X^4,\ x \neq y \text{ et } z \neq t \implies \exists g \in G,\ g \cdot x = z \text{ et } g \cdot y = t.$$

On dit aussi que G *agit doublement transitivement* sur X.

2.1) Montrer que l'action naturelle du groupe alterné $\mathfrak{A}_4$ sur $\{1,2,3,4\}$ est doublement transitive.

2.2) Soit G un groupe fini agissant doublement transitivement sur un ensemble fini X de cardinal $n \geq 2$. On considère l'action naturelle de G sur X^2, définie par

$$\forall g \in G,\ \forall (x,y) \in X^2,\ g \cdot (x,y) = (g \cdot x, g \cdot y)$$

— on ne demande pas montrer que c'est une action, c'est élémentaire. Montrer que cette action admet exactement deux orbites, qui sont la diagonale $D = \{(x,x),\ x \in X\}$ et son complémentaire $X^2 \setminus D$. En déduire que l'ordre de G est un multiple de $n(n-1)$.

2.3) Soient q la puissance d'un nombre premier et $\mathbb{F}_q$ "le" corps à q éléments, dont on note $\mathbb{F}_q^\times$ le groupe des inversibles. Pour tout $(a,b) \in \mathbb{F}_q^\times \times \mathbb{F}_q$, on note $f_{a,b}$ l'application affine

$$\begin{array}{rccc} f_{a,b}: & \mathbb{F}_q & \longrightarrow & \mathbb{F}_q \\ & x & \longmapsto & ax+b. \end{array}$$

On note aussi $\mathcal{A} = \left\{f_{a,b},\ a \in \mathbb{F}_q^\times,\ b \in \mathbb{F}_q\right\}$; c'est un sous-groupe du groupe $\mathfrak{S}_{\mathbb{F}_q}$ des permutations de $\mathbb{F}_q$, on ne demande pas de démontrer ce fait élémentaire.

(i) Calculer l'ordre de $\mathcal{A}$.

(ii) Montrer que l'action naturelle de $\mathcal{A}$ sur $\mathbb{F}_q$ — définie par $f \cdot x = f(x)$ pour tous $f \in \mathcal{A}$ et $x \in \mathbb{F}_q$ —, est doublement transitive.

(iii) Montrer que les éléments de $\mathcal{A} \setminus \left\{\mathrm{id}_{\mathbb{F}_q}\right\}$ sont de deux types : ceux qui fixent exactement un élément de $\mathbb{F}_q$ d'un côté, ceux qui ne fixent aucun élément de $\mathbb{F}_q$ de l'autre.

La suite de cette partie consiste à montrer que si un groupe d'ordre $n^2 - n$ agit doublement transitivement sur un ensemble à n éléments, alors n est nécessairement la puissance d'un nombre premier.

2.4) ***Pour toute la suite*, soient n un entier naturel, G un groupe fini d'ordre $n^2 - n$ et X un ensemble à n éléments sur lequel G agit doublement transitivement** — on notera que $n \geq 2$, nécessairement.

Montrer que l'action de G sur X est transitive, et en déduire que pour tout $x \in X$, le groupe d'isotropie

$$G_x = \{g \in G,\ g \cdot x = x\}$$

est d'ordre $n - 1$.

2.5) Comme dans la question **2.2)**, on considère l'action naturelle de G sur X^2, qui admet exactement deux orbites, à savoir la diagonale D et $X^2 \setminus D$. Démontrer que le groupe d'isotropie de tout élément de $X^2 \setminus D$ est trivial et en déduire que G est partitionné en ses trois sous ensembles suivants :

- $\{1\}$
- l'ensemble des éléments de G qui fixent un unique point de X
- l'ensemble des éléments de G qui ne fixent aucun point de X.

On note Γ la réunion de $\{1\}$ et des éléments de G qui ne fixent aucun point de X.

2.6) En calculant de deux façons le cardinal de l'ensemble $\{(g, x) \in G \times X,\ g \cdot x = x\}$, montrer que Γ a n éléments.

2.7) Pour tout $g \in G$, on note $\mathrm{CONJ}_G(g)$ sa classe de conjugaison dans G et $C_G(g)$ son centralisateur, défini comme d'habitude par

$$C_G(g) = \{h \in G,\ hg = gh\}.$$

Soit $\gamma \in \Gamma \setminus \{1\}$. Montrer que γ ne commute avec aucun élément de $G \setminus \Gamma$ et qu'il n'est conjugué à aucun élément de $G \setminus \Gamma$. En déduire que

$$C_G(\gamma) = \Gamma \quad \text{et} \quad \mathrm{CONJ}_G(\gamma) = \Gamma \setminus \{1\}.$$

2.8) Déduire de la question précédente les trois assertions suivantes :

- Γ est un sous-groupe de G
- Γ est abélien, d'ordre n
- $\Gamma \triangleleft G$.

2.9) Montrer que n est la puissance d'un nombre premier.

UVSQ 2024/2025
Licence de sciences et technologie, santé
LSMA610 (groupes et géométrie)
27 juin 2025

Examen : un corrigé succinct

1 Un sous-groupe de $\mathrm{GL}(2,\mathbb{F}_3)$

1.1) On calcule : $s^2 = I_2$ alors que $s \neq I_2$; donc l'ordre de $S = \langle s \rangle$ est 2. En calculant encore, $r^2 = \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}$, $r^3 = \begin{pmatrix} 0 & -1 \\ -1 & 1 \end{pmatrix}$ et $r^4 = -I_2$. Ainsi, l'ordre de $R = \langle r \rangle$ divise 8 mais n'est ni 1, ni 2 ni 4 : c'est 8.

1.2) Puisque $G = \langle \{r, s\} \rangle$ et puisque s est d'ordre fini, il suffit de montrer que le conjugué de r par s est une puissance de r. On fait le calcul : $srs^{-1} = srs = r^3 \in R$. Cela montre que $R \triangleleft G$.

La matrice s est d'ordre 2. L'unique élément d'ordre 2 du groupe $R = \langle r \rangle$, qui est cyclique d'ordre 8, est $r^4 = -I_2 \neq s$. Comme $S = \{I_2, s\}$, cela montre que $R \cap S = \{I_2\}$.

1.3) On note $RS = \{\rho\sigma,\ \rho \in R,\ \sigma \in S\}$. Puisque $R \triangleleft G$, l'ensemble RS forme un sous-groupe de $\langle R \cup S \rangle$ — c'est un résultat classique, traité en TD, basé par exemple sur les égalités $\rho\sigma\rho'\sigma' = \rho\left(\sigma\rho'\sigma^{-1}\right)(\sigma\sigma')$ et $(\rho\sigma)^{-1} = \sigma^{-1}\rho^{-1} = \rho^{-1}\left(\rho\sigma^{-1}\rho^{-1}\right)$ — notations évidentes. En outre, puisque $R \cap S = \{1\}$, l'écriture d'un élément de RS sous la forme $\rho\sigma$ est unique, ce qui montre que $|RS| = |R| \times |S| = 16$. Enfin, d'une part, R et S sont (évidemment) dans le groupe RS et donc, par minimalité des sous-groupes engendrés, $G \subseteq RS$. D'autre part, par stabilité du produit dans G, l'inclusion $RS \subseteq G$ est immédiate. On a montré que $G = RS$, ce qui prouve que $|G| = 16$.

1.4) L'ordre de $\mathrm{GL}(2,\mathbb{F}_3)$ est $\left(3^2-1\right)\left(3^2-3\right) = 48$ et celui de G est 16. Donc $[\mathrm{GL}(2,\mathbb{F}_3) : G] = \frac{48}{16} = 3$.

2 Action doublement transitive

2.1) Par transitivité de l'action, il suffit de montrer que pour tous $a, b \in \{1,2,3,4\}$ distincts, il existe $\sigma \in \mathfrak{A}_4$ tel que $\sigma(1) = a$ et $\sigma(2) = b$. Si $\{a,b\} = \{1,2\}$, il suffit de prendre $\sigma = 1$ lorsque $a = 1$ ou $\sigma = (12)(34)$ lorsque $a = 2$. Si $\#\{a,b\} \cap \{1,2\} = 1$, quitte à renuméroter, on peut supposer que $a = 1$ et $b = 3$; alors, $\sigma = (234)$ convient. Enfin, si $\{a,b\} = \{3,4\}$, la permutation $(1a)(2b)$ est paire, donc convient. On a montré que l'action est 2-transitive.

2.2) Puisque l'action est 2-transitive, elle est (évidemment) transitive. Donc tous les éléments de la diagonale D sont dans une même orbite. Par ailleurs, dire que l'action est 2-transitive équivaut à dire que les éléments de $X^2 \setminus D$ sont tous dans une même orbite de l'action de G sur X^2. Par ailleurs, si $g \in G$, si x, y et z sont dans X et si $y \neq z$, alors $g \cdot (x,x) = (g \cdot x, g \cdot x) \neq (y,z)$, ce qui montre qu'un élément de D et un élément de $X^2 \setminus D$ ne sont pas dans une même orbite. Cela démontre que l'action a exactement deux orbites : D et $X^2 \setminus D$.

Le cardinal de l'orbite $X^2 \setminus D$ est (évidemment) $n^2 - n$. Mais le cardinal d'une orbite divise toujours l'ordre du groupe qui agit, ce qu'il fallait démontrer.

2.3) (i) Si $f_{a,b} = f_{c,d}$, alors $a = c$ et $b = d$ (calcul élémentaire, évaluer en 0 puis en 1). Ainsi, l'application $\mathbb{F}_q^\times \times \mathbb{F}_q \to \mathcal{A}$, $(a,b) \mapsto f_{a,b}$ est une bijection. Donc l'ordre de $\mathcal{A}$ est $q(q-1)$.

(ii) Soient $x, y, z, t \in \mathbb{F}_q$, avec $x \neq y$ et $z \neq t$. On cherche $(a,b) \in \mathbb{F}_q^\times \times \mathbb{F}_q$ tel que $f_{a,b}(x) = z$ et $f_{a,b}(y) = t$, ce qui revient à résoudre le système

$$\begin{cases} xa + b = z \\ ya + b = t \end{cases}$$

dont les inconnues sont a et b. Le déterminant de ce système est $x - y$ qui est non nul puisque $x \neq y$: le système est de Cramer et admet donc une unique solution dans $\mathbb{F}_q^2$. En particulier, $a = \frac{z-t}{x-y} \neq 0$ puisque $z \neq t$. Cela montre que l'action naturelle de $\mathcal{A}$ sur $\mathbb{F}_q$ est doublement transitive.

(iii) Soit $(a,b) \in \mathbb{F}_q^\times \times \mathbb{F}_q$. Si $(a,b) = (1,0)$, alors $f_{a,b} = \mathrm{id}_{\mathbb{F}_q}$. Si $a = 1$ et $b \neq 0$, alors $f_{a,b} : x \mapsto x + b$ n'a (évidemment) aucun point fixe. Enfin, si $a \neq 1$, alors $f_{a,b}$ admet (évidemment) $\frac{b}{1-a}$ comme unique point fixe. On a disjoint tous les cas, c'est ce qu'il fallait démontrer.

2.4) Si x et y sont deux éléments distincts de X, la double transitivité garantit qu'il existe $g \in G$ tel que $g \cdot (x,y) = (y,x)$. En particulier, $g \cdot x = y$, ce qui montre que l'action est transitive (on a déjà utilisé ce fait en le considérant comme évident, ☺). Alors, si $x \in X$, l'orbite $G \cdot x$ de x sous l'action de G est X tout entier, dont le cardinal est n. Ainsi, $|G_x| = \frac{|G|}{\#(G \cdot x)} = \frac{n^2-n}{n} = n-1$.

2.5) Si $(x,y) \in X^2 \setminus D$, son orbite sous l'action de G est $X^2 \setminus D$ tout entier, dont le cardinal est $n^2 - n = |G|$. Donc l'ordre de son groupe d'isotropie est $\frac{|G|}{n^2-n} = 1$, ce qu'il fallait démontrer.

On suppose que $g \in G$ fixe au moins deux points distincts x et y de X. Alors, g est dans le groupe d'isotropie de $(x,y) \in X^2 \setminus D$ pour l'action de G sur X^2 ; comme ce groupe est trivial, $g = 1$. Cela démontre le partitionnement de G de l'énoncé.

2.6) Comme dans le cours lors de la preuve du théorème de Burnside — que l'on peut aussi utiliser directement ici, par ailleurs —, on calcule le cardinal de la variété d'incidence $\mathcal{I} = \{(g,x) \in G \times X,\ g \cdot x = x\}$. Pour chaque $x \in X$, le nombre de $(g,x) \in \mathcal{I}$ est l'ordre de G_x, à savoir $n-1$. Donc le cardinal de $\mathcal{I}$ est $n(n-1)$. De l'autre côté, selon la question **2.5)**, pour chaque $g \in G$, le nombre de $(g,x) \in \mathcal{I}$ est n si $g = 1$, 0 si $g \in \Gamma \setminus \{1\}$ et 1 si $g \in G \setminus \Gamma$; il en résulte que le cardinal de $\mathcal{I}$ est

$$\#\mathcal{I} = \sum_{g \in G} \#\{x \in X,\ g \cdot x = x\} = \left(\sum_{g=1} + \sum_{g \in \Gamma \setminus \{1\}} + \sum_{g \in G \setminus \Gamma} \right) \#\{x \in X,\ g \cdot x = x\} = n + \#(G \setminus \Gamma).$$

En regroupant ces deux calculs, on obtient $n^2 - n = n + \left(n^2 - n - \#\Gamma\right)$, ce qui s'écrit encore $\#\Gamma = n$.

2.7) Soit $g \in G \setminus \Gamma$. Soit alors x l'unique élément de X tel que $g \cdot x = x$ (question **2.5)**). On suppose, par l'absurde, que $\gamma g = g\gamma$. Alors, $\gamma g \cdot x = \gamma \cdot x = g\gamma \cdot x$, ce qui montre que $\gamma \cdot x$ est un point fixe de g, qui égale donc x par unicité (question **2.5)**). Cela contredit le fait que γ ne fixe aucun point de X : l'hypothèse que γ et g commutent ne tient pas.

Si $g \in G \setminus \Gamma$, alors g fixe un (unique) élément $x \in X$ (question **2.5)**). Donc $g \in G_x$. Mais alors, si $h \in G$, alors hgh^{-1} fixe $h \cdot x$ et n'est pas le neutre de G, ce qui l'empêche d'être dans Γ (question **2.5)**). Donc g n'est conjugué à aucun élément de Γ, donc n'est pas conjugué à γ.

Il en résulte à la fois que $C_G(\gamma) \subseteq \Gamma$ et que $\mathrm{CONJ}_G(\gamma) \subseteq \Gamma \setminus \{1\}$. Comme $|C_G(\gamma)| \times \#\,\mathrm{CONJ}_G(\gamma) = |G| = n(n-1)$ et $\#\Gamma = n$, cela entraîne que $|C_G(\gamma)| = n$ et que $\#\,\mathrm{CONJ}_G(\gamma) = n-1$ et donc que $C_G(\gamma) = \Gamma$ et $\mathrm{CONJ}_G(\gamma) = \Gamma \setminus \{1\}$, ce qu'il fallait démontrer.

2.8) Puisque Γ est un centralisateur, c'est un sous-groupe de G. Son ordre est n, c'est la question **2.6)**. Si $\gamma \in \Gamma \setminus \{1\}$, alors Γ est le centralisateur de γ dans G — c'est la question précédente ; donc γ est dans le centre de Γ. Comme cela est vrai pour tout $\gamma \in \Gamma \setminus \{1\}$, cela montre que Γ est abélien. Enfin, selon la question précédente, $\Gamma \setminus \{1\}$ est une classe de conjugaison de G ; cela montre que $\Gamma \triangleleft G$.

2.9) Soient p et q deux nombres premiers divisant n. Alors, ils divisent l'ordre de Γ. Donc il existe au moins un p-Sylow et au moins un q-Sylow de Γ. Donc il existe au moins un élément d'ordre p^α et au moins un élément d'ordre q^β dans Γ, pour certains $\alpha, \beta \geq 1$. Mais comme tous les éléments de $\Gamma \setminus \{1\}$ ont le même ordre (ils sont conjugués), $p = q$. Donc Γ est un p-groupe, et n une puissance de p.

NB : sachant que Γ est un groupe abélien fini d'ordre n dont tous les éléments non triviaux ont le même ordre (ils sont conjugués dans G), on peut aussi utiliser le théorème de structure des groupes abéliens finis pour conclure. Ou même conclure sans ce théorème de structure en raisonnant directement sur les ordres des éléments d'un groupe abélien fini.

UVSQ 2025/2026
Licence de sciences et technologie, santé
LSMA610 (groupes et géométrie)
20 mars 2026

Examen partiel

– durée : une heure et demie –

Bon, il faut l'écrire : aucun document ni aucun instrument électronique n'est autorisé pour cette épreuve

1 Sous-groupe caractéristique [6 points]

Si H est un sous-groupe d'un groupe G, on dit que H est un *sous-groupe caractéristique* de G lorsque $\sigma(H) \subseteq H$, pour tout automorphisme σ de G.

1.1) Montrer que tout sous-groupe caractéristique est distingué.

1.2) En considérant le groupe produit $(\mathbb{Z}/2\mathbb{Z})^2$, exhiber un exemple de sous-groupe distingué non caractéristique.

1.3) Montrer avec soin que si G est un groupe et si $D(G)$ est son groupe dérivé[♪], alors $D(G)$ est un sous-groupe caractéristique de G.

1.4) Trouver un exemple de sous-groupes de H et K du groupe $\mathfrak{S}_4$ des permutations de 4 objets tels que $H \triangleleft K$, $K \triangleleft G$, mais H n'est pas distingué dans $\mathfrak{S}_4$.

1.5) Soient G un groupe, et H et K deux sous-groupes de G. Est-il vrai que si H est un sous-groupe caractéristique de K et si K est un sous-groupe distingué de G, alors H est aussi un sous-groupe distingué de G ?

2 Un groupe arithmétique [5 points]

On note $\Gamma = \mathrm{SL}(2, \mathbb{Z})$ le groupe multiplicatif des matrices carrées de taille 2 dont le déterminant égale 1. Si $M = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in \Gamma$, on note

$$\overline{M} = \begin{pmatrix} \overline{a} & \overline{c} \\ \overline{b} & \overline{d} \end{pmatrix}$$

où $\overline{x}$ désigne la classe modulo 7 du nombre entier x.

2.1) Montrer que l'application $M \mapsto \overline{M}$ définit un homomorphisme de groupes de Γ sur $\mathrm{SL}(2, \mathbb{Z}/7\mathbb{Z})$.

2.2) On note

$$\Gamma(7) = \left\{ \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in \Gamma,\ a \equiv d \equiv 1\ [7] \text{ et } b \equiv c \equiv 0\ [7] \right\}.$$

Montrer que $\Gamma(7)$ est un sous-groupe distingué de Γ.

2.3) Calculer le cardinal de $\Gamma(7)$. En admettant que $\mathrm{SL}(2, \mathbb{Z}/7\mathbb{Z})$ est engendré par les classes modulo 7 des matrices $S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ et $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, calculer l'indice de $\Gamma(7)$ dans Γ.

[♪] C'est le sous-groupe de G engendré par ses commutateurs, on le redit ici.

3 A propos de permutations [9 points]

Pour tout entier naturel non nul n, comme c'est l'usage, on note $\mathfrak{S}_n$ le groupe symétrique de l'ensemble $\{1, \ldots, n\}$ et $\mathfrak{A}_n$ son groupe alterné.

3.1 Les 3-cycles consécutifs engendrent $\mathfrak{A}_n$

3.1.1) Montrer que les 3-cycles (123) et (234) engendrent le groupe $\mathfrak{A}_4$.

3.1.2) Montrer que pour tout $n \geq 3$, le groupe $\mathfrak{A}_{n+1}$ est engendré par $\mathfrak{A}_n$ et le 3-cycle $(n-1, n, n+1)$.

3.1.3) En déduire que pour tout $n \geq 3$, le groupe $\mathfrak{A}_n$ est engendré par les 3-cycles *consécutifs*

$$(123),\ (234), \ldots, (n-2, n-1, n).$$

3.2 Ce qu'engendrent (12345) et $(135)(246)$

On note G le sous-groupe de $\mathfrak{S}_6$ engendré par les permutations $c = (12345)$ et $t = (135)(246)$.

3.2.1) Justifier que G est un sous-groupe de $\mathfrak{A}_6$, en précisant soigneusement quelle(s) propriété(s) des sous-groupes engendrés intervien(nen)t dans l'argumentation apportée.

3.2.2) Quels sont les ordres de c et t ?

3.2.3) Calculer t^2c^2.

3.2.4) En utilisant la formule de conjugaison des cycles, en déduire que les 3-cycles (126) et (236) sont dans G.

3.2.5) Déduire de la question précédente que $(123) \in G$.

3.2.6) Montrer que G contient aussi les 3-cycles (234) et (345).

3.2.7) En utilisant le résultat de **3.1**, en déduire que $G = \mathfrak{A}_6$. Ecrire son ordre en base 10.

[Pour aller plus loin : le sous-groupe de $\mathfrak{A}_6$ engendré par (12345) et $(136)(254)$, lui, est beaucoup plus petit puisqu'il est d'ordre 60, isomorphe à $\mathfrak{A}_5$. Mais c'est une autre histoire, passionnante bien qu'un peu plus longue...]

UVSQ 2025/2026
Licence de sciences et technologie, santé
LSMA610 (groupes et géométrie)
20 mars 2026

Examen partiel : un corrigé succinct

1 Sous-groupe caractéristique

1.1) Soit G un groupe. Si $g \in G$, l'application $G \to G$, $h \mapsto ghg^{-1}$ est (évidemment) un automorphisme de G. Si un sous-groupe de G est caractéristique, il est en particulier invariant par tous les automorphismes de cette forme, ce qui signifie qu'il est normal.

1.2) L'application $j : (\mathbb{Z}/2\mathbb{Z})^2 \to (\mathbb{Z}/2\mathbb{Z})^2$, $(x, y) \mapsto (y, x)$ est (évidemment) un automorphisme de $(\mathbb{Z}/2\mathbb{Z})^2$. Comme $(\mathbb{Z}/2\mathbb{Z})^2$ est abélien, son sous-groupe engendré par $(1, 0)$, comme tous les autres sous-groupes, est distingué. Pourtant, il n'est pas invariant par j : ce n'est pas un sous-groupe caractéristique.

1.3) Soit $\sigma \in \mathrm{Aut}(G)$.

Si A est une partie (quelconque) de G, alors $\sigma(A)$ est (évidemment) contenue dans le sous-groupe $\sigma(\langle A\rangle)$; par minimalité des sous-groupes engendrés, cela implique que $\langle\sigma(A)\rangle \subseteq \sigma(\langle A\rangle)$. Inversement, par caractérisation des sous-groupes engendrés, puisque tout élément de $\langle A\rangle$ est un produit $\alpha_1^{\pm 1} \dots \alpha_n^{\pm 1}$ où les α_k sont des éléments de A, son image par σ est un produit $\sigma(\alpha_1)^{\pm 1} \dots \sigma(\alpha_n)^{\pm 1}$ qui est ainsi dans $\langle\sigma(A)\rangle$: on a montré que $\langle\sigma(A)\rangle \supseteq \sigma(\langle A\rangle)$. Conclusion : pour toute partie A de G, on a $\sigma(\langle A\rangle) = \langle\sigma(A)\rangle$.

On applique cela dans le cas où A est l'ensemble des commutateurs de G. Or, si $x, y \in G$, alors $\sigma\left(xyx^{-1}y^{-1}\right) = \sigma(x)\,\sigma(y)\,\sigma(x)^{-1}\,\sigma(y)^{-1}$ est encore un commutateur de G. Donc $\sigma(D(G)) = D(\sigma(G)) = D(G)$: le groupe dérivé est caractéristique.

1.4) Prendre par exemple $H = \langle(12)(34)\rangle$ et $K = \langle(12)(34), (13)(24)\rangle$ — c'est le groupe de Klein.

1.5) Soit $g \in G$. On note i_g l'application $G \to G$ définie par $i_g(\gamma) = g\gamma g^{-1}$; c'est un automorphisme (*intérieur*) de G. Puisque K est distingué dans G, la restriction de i_g à K définit un automorphisme de K — non intérieur si $g \notin K$. Puisque H est un sous-groupe caractéristique de K, cela entraîne que H est stable par i_g, c'est-à dire que $gHg^{-1} \subseteq H$. L'arbitraire sur g montre ainsi que $H \triangleleft G$: la réponse est *oui*.

2 Un groupe arithmétique

2.1) Puisque la projection canonique $\mathbb{Z} \to \mathbb{Z}/7\mathbb{Z}$, $x \mapsto \overline{x}$ est un homomorphisme d'anneaux,

$$\overline{\begin{pmatrix} a & c \\ b & d \end{pmatrix}\begin{pmatrix} a' & c' \\ b' & d' \end{pmatrix}} = \begin{pmatrix} \overline{aa'+cb'} & \overline{ac'+cd'} \\ \overline{ba'+db'} & \overline{bc'+dd'} \end{pmatrix} = \begin{pmatrix} \overline{a}\,\overline{a'}+\overline{c}\,\overline{b'} & \overline{a}\,\overline{c'}+\overline{c}\,\overline{d'} \\ \overline{b}\,\overline{a'}+\overline{d}\,\overline{b'} & \overline{b}\,\overline{c'}+\overline{d}\,\overline{d'} \end{pmatrix} = \begin{pmatrix} \overline{a} & \overline{c} \\ \overline{b} & \overline{d} \end{pmatrix}\begin{pmatrix} \overline{a'} & \overline{c'} \\ \overline{b'} & \overline{d'} \end{pmatrix} = \overline{\begin{pmatrix} a & c \\ b & d \end{pmatrix}} \times \overline{\begin{pmatrix} a' & c' \\ b' & d' \end{pmatrix}}$$

d'une part, et d'autre part

$$\det \overline{\begin{pmatrix} a & c \\ b & d \end{pmatrix}} = \det \begin{pmatrix} \overline{a} & \overline{c} \\ \overline{b} & \overline{d} \end{pmatrix} = \overline{a}\,\overline{d} - \overline{b}\,\overline{c} = \overline{ad-bc} = \overline{1},$$

pour tous $a, b, c, d, a', b', c', d' \in \mathbb{Z}$. C'est cela qu'il fallait démontrer.

2.2) Le neutre du groupe $\mathrm{SL}(2, \mathbb{Z}/7\mathbb{Z})$ est $\begin{pmatrix} \overline{1} & \overline{0} \\ \overline{0} & \overline{1} \end{pmatrix}$. Ainsi, $\Gamma(7)$ est le noyau de l'homomorphisme de groupes $p : \mathrm{SL}(2, \mathbb{Z}) \to \mathrm{SL}(2, \mathbb{Z}/7\mathbb{Z})$, $M \mapsto \overline{M}$ de la question précédente. Cela montre à la fois que $\Gamma(7)$ est un sous-groupe de Γ, et aussi qu'il est normal.

2.3) Le groupe $\Gamma(7)$ est infini, puisqu'il contient la suite de matrices $\begin{pmatrix} 1 & 7n \\ 0 & 1 \end{pmatrix}$, $n \in \mathbb{N}$. Par ailleurs, il est au plus dénombrable puisque $\mathrm{SL}(2, \mathbb{Z})$, sous-ensemble de l'ensemble $\mathcal{M}_2(\mathbb{Z})$ qui est (évidemment) dénombrable, est lui-même (au plus) dénombrable. Ainsi, le cardinal de $\Gamma(7)$ est celui de $\mathbb{N}$: il est infini et dénombrable.

Par ailleurs, $\mathrm{SL}(2,\mathbb{Z})$ est engendré par S et T — c'est du cours. Le fait admis que $\mathrm{SL}(2,\mathbb{Z}/7\mathbb{Z})$ soit engendré par les classes modulo 7 de ces deux matrices montre que p est une surjection. Alors, puisque $\mathbb{Z}/7\mathbb{Z}$ est un corps (7 est premier),

$$[\Gamma : \Gamma(7)] = |\mathrm{SL}(2,\mathbb{Z}/7\mathbb{Z})| = \left(7^2-1\right)\left(7^2-7\right)/6 = 7\times 48 = 336.$$

Ce dernier calcul peut se faire en posant la multiplication comme à l'école élémentaire, ou en faisant de faciles multiplications par 2 successives : $7\times 48 = 7\times 3\times 2^4 = 21\times 16 = 42\times 2^3 = 84\times 2^2 = 168\times 2 = 336$.

3 A propos de permutations

3.1 Les 3-cycles consécutifs engendrent $\mathfrak{A}_n$

3.1.1) Là, on peut tout faire à la main. Un dénombrement élémentaire montre que les huit 3-cycles de $\mathfrak{A}_4$ sont (123), (124), (134), (234) et leurs carrés. Or, la formule de conjugaison des cycles montre que $(134) = (234)(123)(234)^{-1}$ et que $(124) = (123)^2(234)(123)^{-2}$ sont des produits des seuls 3-cycles (123) et (234) — ce qui est donc aussi vrai de leurs carrés. Comme les 3-cycles engendrent $\mathfrak{A}_4$, on a montré que (123) et (234) suffisent à engendrer $\mathfrak{A}_4$.

3.1.2) Le cas $n = 3$ vient d'être traité ; on suppose $n \geq 4$. Puisque les 3-cycles sont des permutations paires, le groupe G_n engendré par $\mathfrak{A}_n$ et $(n-1, n, n+1)$ est un sous-groupe de $\mathfrak{A}_{n+1}$. En outre, puisque $\mathfrak{A}_{n+1}$ est engendré par ses 3-cycles, il suffit de montrer que les 3-cycles dont le support contient $n+1$ sont dans G_n pour montrer que $G_n = \mathfrak{A}_{n+1}$. Or, si a et b sont deux éléments distincts de $\{1,\dots,n\}$, il existe une permutation paire $\sigma \in \mathfrak{A}_n$ qui envoie $n-1$ sur a et n sur b — raisonner comme pour montrer que les 3-cycles du groupe alterné $\mathfrak{A}_n$ sont tous conjugués dans $\mathfrak{A}_n$ lorsque $n \geq 5$: prendre d'abord $\tau \in \mathfrak{S}_n$ qui envoie $n-1$ sur a et n sur b — il en existe évidemment. Si τ est paire, on prend $\sigma = \tau$; si τ est impaire, on prend $\sigma = \tau\cdot(n-3, n-2)$ qui est paire et envoie encore $n-1$ sur a et n sur b — noter qu'on utilise ici que $n \geq 4$. Alors, $\sigma(n-1, n, n+1)\sigma^{-1} = (a, b, n+1)$, ce qui montre que $(a, b, n+1) \in G_n$.

3.1.3) On procède par récurrence sur n. Si $n = 3$, c'est fait au **3.1**. On suppose que $n \geq 4$ et que $\mathfrak{A}_{n-1}$ est engendré par ses 3-cycles consécutifs (c'est l'hypothèse de récurrence). Alors, le sous-groupe de $\mathfrak{A}_n$, qui est engendré par $\mathfrak{A}_{n-1}$ et $(n-2, n-1, n)$ selon la question précédente, est aussi engendré par (123), $(234), \dots, (n-2, n-1, n)$, ce qu'il fallait démontrer.

3.2 Ce qu'engendrent (12345) et (135)(246)

3.2.1) Les permutations c et t sont paires. Ainsi, le groupe $\mathfrak{A}_6$, qui contient c et t, contient aussi le groupe qu'ils engendrent (cela résulte de la minimalité des sous-groupes engendrés, ou encore directement de la définition du sous-groupe engendré).

3.2.2) Un calcul immédiat montre que l'ordre de c est 5 et que celui de t est 3.

3.2.3) On calcule. On trouve $t^2c^2 = (456)$.

3.2.4) Bien sûr, $t^2c^2 \in G$. En conjugant par une puissance de c, on trouve encore un élément de G. Ainsi, $c^2\left(t^2c^2\right)c^{-2} = (126) \in G$ et $c^3\left(t^2c^2\right)c^{-3} = (236) \in G$.

3.2.5) On fait juste le produit : $(123) = (126)(236) \in G$.

3.2.6) On conjugue encore par c et c^2 qui sont dans G. On obtient $c(123)c^{-1} = (234) \in G$ et $c^2(123)c^{-2} = (345) \in G$.

3.2.7) Les questions précédentes montrent que G contient tous les 3-cycles consécutifs de $\mathfrak{A}_6$, qui engendrent $\mathfrak{A}_6$. Donc $G = \mathfrak{A}_6$. En particulier, $|G| = 6!/2 = 360$.

[Pour aller plus loin : le sous-groupe de $\mathfrak{A}_6$ engendré par (12345) et (136)(254), lui, est beaucoup plus petit puisqu'il est d'ordre 60, isomorphe à $\mathfrak{A}_5$. Mais c'est une autre histoire, passionnante bien qu'un peu plus longue...]

UVSQ 2025/2026
Licence de sciences et technologie, santé
LSMA610 (groupes et géométrie)
7 mai 2026

Contrôle continu : épreuve de remplacement

(durée : une heure et demie)

— Bon, il faut l'écrire : aucun document ni aucun instrument électronique n'est autorisé pour cette épreuve —

1 Intérieurs [4 points]

Soit G un groupe. Montrer que le groupe des automorphismes intérieurs de G est isomorphe au quotient de G par son centre.

2 Déterminant modulo un sous-groupe multiplicatif du corps [4 points]

Soit n un entier naturel non nul. Soient $\mathbb{F}$ un corps commutatif et G un sous-groupe du groupe multiplicatif $\mathbb{F}^\times$.

2.1) On note

$$S(G) = \{M \in \mathrm{GL}(n, \mathbb{F}),\ \det(M) \in G\}.$$

Montrer que $S(G)$ est un sous-groupe distingué du groupe linéaire $\mathrm{GL}(n, \mathbb{F})$.

2.2) Montrer que les deux groupes quotient $\mathrm{GL}(n, \mathbb{F})/S(G)$ et $\mathbb{F}^\times/G$ sont isomorphes.

3 Ce qu'engendrent (12345) et $(136)(254)$ [12 points]

Pour tout entier naturel non nul n, comme c'est l'usage, on note $\mathfrak{S}_n$ le groupe symétrique de l'ensemble $\{1, \ldots, n\}$ et $\mathfrak{A}_n$ son groupe alterné. On note G le sous-groupe de $\mathfrak{A}_6$ engendré par le 5-cycle c et le produit de 3-cycles t définis par

$$c = (12345) \text{ et } t = (136)(254).$$

— L'objet de cette partie est de montrer que G est isomorphe au groupe $\mathfrak{A}_5$ —

3.1) Calculer la décomposition de $a = c^2t$ en produit de cycles à supports disjoints, ainsi que celle de $b = tctct^2$.

3.2) Montrer que le groupe engendré par a et b est un sous-groupe de G isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$.

3.3) On note $P_1, \ldots, P_5$ les cinq partitions de $\{1, 2, 3, 4, 5, 6\}$ suivantes :

$$P_1 = \{\{1, 2\}, \{3, 5\}, \{4, 6\}\}$$
$$P_2 = \{\{1, 3\}, \{2, 6\}, \{4, 5\}\}$$
$$P_3 = \{\{1, 4\}, \{2, 3\}, \{5, 6\}\}$$
$$P_4 = \{\{1, 5\}, \{2, 4\}, \{3, 6\}\}$$
$$P_5 = \{\{1, 6\}, \{2, 5\}, \{3, 4\}\}$$

et $\mathcal{P} = \{P_1, P_2, P_3, P_4, P_5\}$. Montrer que l'action naturelle de $\mathfrak{S}_6$ sur les triplets de paires d'éléments distincts de $\{1, 2, 3, 4, 5, 6\}$ induit une action du groupe G sur l'ensemble $\mathcal{P}$.

3.4) On note

$$\varphi : G \to \mathfrak{S}_5$$

l'homomorphisme de groupes induit par l'action de G sur $\mathcal{P}$ définie à la question précédente, *via* la numérotation des éléments de $\mathcal{P}$. Montrer que $\varphi(c)$ est le 5-cycle $(\mathcal{P}_1, \mathcal{P}_3, \mathcal{P}_5, \mathcal{P}_2, \mathcal{P}_4)$ et que $\varphi(t)$ est le 3-cycle $(\mathcal{P}_2, \mathcal{P}_4, \mathcal{P}_5)$. En déduire que l'image de φ est un sous-groupe du groupe alterné $\mathfrak{A}_5$.

3.5) Montrer que G est isomorphe à $\mathfrak{A}_5$.

3.6) Trouver le nombre de 2-sous-groupes de Sylow de G. Expliciter tous les éléments de l'un quelconque de ces 2-Sylow.

UVSQ 2025/2026
Licence de sciences et technologie, santé
LSMA610 (groupes et géométrie)
7 mai 2026

Epreuve de remplacement : un corrigé succinct

1 Intérieurs

C'est presque du cours. Pour tout $\gamma \in G$, on note $i_\gamma : G \to G$, $g \mapsto \gamma g \gamma^{-1}$, qui est — c'est immédiat — un endomorphisme de groupe. Un calcul non moins immédiat montre que $i_1 = \mathrm{id}_G$ et que $i_{\gamma\delta} = i_\gamma \circ i_\delta$. Cela montre à la fois que les i_γ sont des automorphismes de G — la réciproque de i_γ est $i_{\gamma^{-1}}$ — et que l'application $i : G \to \mathrm{Aut}(G)$, $\gamma \mapsto i_\gamma$ est un homomorphisme de groupes. L'image de i est, par définition, le sous-groupe $\mathrm{Int}(G)$ des automorphismes intérieurs de G. Le noyau de G est le centre $Z(G)$ de G — calcul immédiat. Le premier théorème d'isomorphisme appliqué à i induit alors un isomorphisme de groupes $G/Z(G) \simeq \mathrm{Int}(G)$, ce qu'il fallait démontrer.

2 Déterminant modulo un sous-groupe multiplicatif du corps

2.1) L'application déterminant $\det : \mathrm{GL}(n, \mathbb{F}) \to \mathbb{F}^\times$ est un homomorphisme de groupes. Par ailleurs, le groupe $\mathbb{F}^\times$ est abélien ce qui induit une structure canonique de groupe quotient $\mathbb{F}^\times/G$ — tous les sous-groupes de $\mathbb{F}^\times$ sont normaux. On compose det à gauche par la surjection canonique $\mathrm{can} : \mathbb{F}^\times \to \mathbb{F}^\times/G$, ce qui fournit un homomorphisme de groupes

$$\varphi = \mathrm{can} \circ \det : \mathrm{GL}(n, \mathbb{F}) \to \mathbb{F}^\times/G$$

dont le noyau est, par définition, $S(G)$. Cela montre à la fois que $S(G)$ est un sous-groupe de $\mathrm{GL}(n, \mathbb{F})$ et qu'il est distingué.

2.2) Au vu de la question précédente et en vertu du premier théorème d'isomorphisme, il suffit de montrer que φ est surjectif pour conclure. Or, can est (bien sûr) une surjection, et $\det : \mathrm{GL}(n, \mathbb{F}) \to \mathbb{F}^\times$ aussi puisque pour tout $x \in \mathbb{F}^\times$, la matrice $\mathrm{diag}(x, 1, \ldots, 1)$ (notation évidente) est un antécédent de x par det. Ainsi, φ est surjectif, comme composé de deux surjections.

3 Ce qu'engendrent (12345) et $(136)(254)$

3.1) On calcule. On trouve $a = (15)(36)$ et $b = (15)(24)$.

3.2) Un calcul immédiat montre que $ab = (24)(36)$. Les trois transpositions (15), (24) et (36) commutent, ce qui montre que a, b et ab commutent et sont toutes d'ordre 2. Le groupe $\langle a, b\rangle = \{1, a, b, ab\}$ est donc abélien d'ordre 4 à éléments d'ordres 1 ou 2 : ses facteurs invariants sont nécessairement $(2, 2)$, ce qu'il fallait démontrer.

3.3) Puisque c et t engendrent G, il suffit de montrer que $\mathcal{P}$ est stable par ces deux permutations pour montrer que l'action naturelle de $\mathfrak{S}_6$ sur les paires d'éléments distincts de $\{1, \ldots, 6\}$ induit une action de G sur $\mathcal{P}$. Or, par un calcul immédiat, on obtient $c \cdot \mathcal{P}_1 = \mathcal{P}_3$, $c \cdot \mathcal{P}_2 = \mathcal{P}_4$, $c \cdot \mathcal{P}_3 = \mathcal{P}_5$, $c \cdot \mathcal{P}_4 = \mathcal{P}_1$ (et $c \cdot \mathcal{P}_5 = \mathcal{P}_2$) d'une part, et d'autre part, $t \cdot \mathcal{P}_1 = \mathcal{P}_1$, $t \cdot \mathcal{P}_2 = \mathcal{P}_4$, $t \cdot \mathcal{P}_3 = \mathcal{P}_3$, $t \cdot \mathcal{P}_4 = \mathcal{P}_5$ (et $t \cdot \mathcal{P}_5 = \mathcal{P}_2$). Cela montre que $c \cdot \mathcal{P} = \mathcal{P}$ et que $t \cdot \mathcal{P} = \mathcal{P}$, et donc que $G = \langle c, t\rangle$ agit sur $\mathcal{P}$, par restriction de l'action naturelle de $\mathfrak{S}_6$ sur les triplets de paires d'éléments distincts de $\{1, 2, 3, 4, 5, 6\}$.

3.4) Le calcul de la question précédente montre que $\varphi(c) = (\mathcal{P}_1, \mathcal{P}_3, \mathcal{P}_5, \mathcal{P}_2, \mathcal{P}_4) = (13524)$ et que $\varphi(t) = (\mathcal{P}_2, \mathcal{P}_4, \mathcal{P}_5) = (245)$. Ces deux cycles sont des permutations paires qui engendrent l'image de φ puisque c et t engendrent G. Donc cette image est incluse dans $\mathfrak{A}_5$.

3.5) Soit $g \in \ker\varphi$. Puisque $g \cdot \mathcal{P}_1 = \mathcal{P}_1$, $g(1) \in \{1, 2\}$. Mais g fixe aussi $\mathcal{P}_2$; donc $g(1) \in \{1, 3\}$. Cela implique que g fixe 1. De la même façon, g fixe tous les éléments de $\{1, \ldots, 6\}$, ce qui signifie que $g = 1$: on a montré que φ est injectif.

Pour montrer que φ est surjectif, il suffit de montrer que $\varphi(c) = (13524)$ et $\varphi(t) = (245)$ engendrent $\mathfrak{A}_5$. En conjuguant par (1435), cela revient à montrer que $\kappa = (12345)$ et $\tau = (123)$ engendrent $\mathfrak{A}_5$. Or, conjuguer τ par les puissances

de κ montre que le groupe engendré par τ et κ contient le groupe engendré par les 3-cycles (123), (234) et (345) qui, c'est notoire aussi, engendrent $\mathfrak{A}_5$.

3.6) Le groupe G est isomorphe à $\mathfrak{S}_5$. Comme pour ce dernier, ses 2-Sylow sont d'ordre 4 et sont au nombre de 5 — pour chaque $k \in \{1,2,3,4,5\}$, le groupe de Klein de $\mathfrak{S}_{\{1,2,3,4,5\}\setminus\{k\}}$ est un 2-Sylow de $\mathfrak{A}_5$, et tous sont de cette forme. Les cinq 2-Sylow de G sont donc des sous-groupes d'ordre 4 — formés d'éléments d'ordres 1 ou 2. Le groupe engendré par a et b de la question **2)** en est un :

$$\langle a, b\rangle = \{1, (15)(24), (15)(36), (24)(36)\}\,.$$

Dans l'action de G sur $\mathcal{P}$, c'est le fixateur de $\mathcal{P}_4$.

UVSQ 2025/2026
Licence de sciences et technologie, santé
LSMA610 (groupes et géométries)
20 mai 2026

Examen

– durée : deux heures –

Bon, il faut l'écrire : aucun document ni aucun instrument électronique n'est autorisé pour cette épreuve

1 Affine-Frobenius [6 points]

On note $\mathbb{F}_4$ "le" corps à 4 éléments. On redit ici que la caractéristique de $\mathbb{F}_4$ est 2 et que le groupe multiplicatif $\mathbb{F}_4^\times$ est cyclique d'ordre 3. Pour tout $a \in \mathbb{F}_4^\times$, pour tout $\varepsilon \in \{0,1\}$ et pour tout $b \in \mathbb{F}_4$, on note $A_{a,\varepsilon,b}$ l'application $\mathbb{F}_4 \to \mathbb{F}_4$ définie par la formule

$$\forall x \in \mathbb{F}_4,\ A_{a,\varepsilon,b}(x) = ax^{2^\varepsilon} + b.$$

1.1) Montrer que $(X+Y)^2 = X^2 + Y^2$ dans $\mathbb{F}_4[X,Y]$, et que $x^4 = x$ pour tout $x \in \mathbb{F}_4$.

1.2) Montrer que, pour tous $a, c \in \mathbb{F}_4^\times$, pour tous $\varepsilon, \zeta \in \{0,1\}$ et pour tous $b, d \in \mathbb{F}_4$, on a la formule

$$A_{a,\varepsilon,b} \circ A_{c,\zeta,d} = A_{ac^{2^\varepsilon}, 1-\delta_{\varepsilon,\zeta}, ad^{2^\varepsilon}+b}$$

où δ est le symbole de Kronecker :

$$\delta_{\varepsilon,\zeta} = \begin{cases} 1 \text{ si } \varepsilon = \zeta \\ 0 \text{ si } \varepsilon \neq \zeta. \end{cases}$$

1.3) En déduire que l'ensemble

$$\mathrm{AF}(\mathbb{F}_4) = \left\{ A_{a,\varepsilon,b},\ a \in \mathbb{F}_4^\times,\ \varepsilon \in \{0,1\},\ b \in \mathbb{F}_4 \right\}$$

est un sous-groupe du groupe des permutations de $\mathbb{F}_4$.

1.4) Montrer que l'application

$$\begin{array}{ccc} \mathbb{F}_4^\times \times \{0,1\} \times \mathbb{F}_4 & \longrightarrow & \mathrm{AF}(\mathbb{F}_4) \\ (a,\varepsilon,b) & \longmapsto & A_{a,\varepsilon,b} \end{array}$$

est injective.

1.5) Déduire des questions précédentes que le groupe $\mathrm{AF}(\mathbb{F}_4)$ est isomorphe au groupe symétrique $\mathfrak{S}_4$.

2 Produit ensembliste [4 points]

Soient G un groupe fini, H et K deux sous-groupes de G dont les ordres sont premiers entre eux. On suppose que H est un sous-groupe distingué de G. Montrer, dans ces conditions, que le produit ensembliste

$$HK = \{hk,\ h \in H,\ k \in K\}$$

est un sous-groupe de G, d'ordre $|H| \times |K|$.

3 Normaliser les 5-Sylow de $\mathfrak{S}_5$ [10 points]

On note $\mathfrak{S}_5$ le groupe symétrique de l'ensemble $\{1,\dots,5\}$. Si H est un sous-groupe de $\mathfrak{S}_5$, on note

$$N(H) = \left\{\sigma \in \mathfrak{S}_5,\ \sigma H \sigma^{-1} \subseteq H\right\}.$$

son *normalisateur*, qui est (c'est immédiat) un sous-groupe de $\mathfrak{S}_5$ contenant H.

3.1 Normalisateurs des 5-Sylow de $\mathfrak{S}_5$

Avec les notations habituelles, on note c et q les cycles de $\mathfrak{S}_5$ suivants :

$$c = (1,2,3,4,5) \text{ et } q = (1,2,4,3).$$

3.1) Donner un exemple de 5-Sylow de $\mathfrak{S}_5$ — en justifiant que c'en est un, bien entendu.

3.2) On note C le sous-groupe de $\mathfrak{S}_5$ engendré par c. Montrer que $qcq^{-1} \in C$.

3.3) En déduire soigneusement que le sous-groupe de $\mathfrak{S}_5$ engendré par c et q est d'ordre 20. Est-il abélien ?
[On pourra s'il l'on veut appuyer son raisonnement sur le résultat de la partie **2**.]

3.4) On note

$$N = N(C)$$

le normalisateur de C dans $\mathfrak{S}_5$. Calculer le nombre de 5-Sylow de $\mathfrak{S}_5$. En faisant agir $\mathfrak{S}_5$ sur l'ensemble de ses 5-Sylow par conjugaison, en déduire l'ordre de N.

3.5) Montrer que N est engendré par c et q.

3.6) Montrer que si S est n'importe quel 5-Sylow de $\mathfrak{S}_5$, son normalisateur $N(S)$ est isomorphe à N.

3.2 Intersections deux à deux des normalisateurs des 5-Sylow de $\mathfrak{S}_5$

3.7) On note $\mathcal{S}_5$ l'ensemble des 5-Sylow de $\mathfrak{S}_5$ et $\mathcal{Q}$ l'ensemble des 4-cycles de $\mathfrak{S}_5$. Si $(S,\tau) \in \mathcal{S}_5 \times \mathcal{Q}$, on dit que τ *normalise* S lorsque $\tau S \tau^{-1} \subseteq S$. Montrer que deux 4-cycles quelconques de $\mathfrak{S}_5$ normalisent le même nombre de 5-Sylow de $\mathfrak{S}_5$.

3.8) En comptant de deux façons le cardinal de l'ensemble

$$\mathcal{E} = \{(S,\tau) \in \mathcal{S}_5 \times \mathcal{Q},\ \tau \text{ normalise } S\},$$

montrer que tout 4-cycle de $\mathfrak{S}_5$ normalise exactement deux 5-Sylow de $\mathfrak{S}_5$.

3.9) En considérant l'application qui à un 4-cycle de $\mathfrak{S}_5$ associe la paire de 5-Sylow qu'il normalise, montrer que si S et T sont deux 5-Sylow distincts quelconques de $\mathfrak{S}_5$, l'intersection de leurs normalisateurs $N(S) \cap N(T)$ est un groupe cyclique d'ordre 4.

UVSQ 2025/2026
Licence de sciences et technologie, santé
LSMA610 (groupes et géométries)
20 mai 2026

Examen : un corrigé succinct

1 Affine-Frobenius

1.1) Dans $\mathbb{F}_4[X,Y]$, on a $2=0$ puisque la caractéristique de $\mathbb{F}_4$ — et donc de $\mathbb{F}_4[X,Y]$ — est 2. Alors, $(X+Y)^2 = X^2+2XY+Y^2 = X^2+Y^2$. En outre, puisque $\mathbb{F}_4^\times$ est d'ordre 3, le théorème de Lagrange assure que tout élément non nul x de $\mathbb{F}_4$ vérifie $x^3=1$, et donc que $x^4=x$. Puisque $0^4=0$, l'égalité est vraie sur $\mathbb{F}_4$ tout entier.

Commentaire post-correction
Attention à ne pas se laisser tenter par l'erreur — hélas fréquente — qui consiste à croire que les quatre éléments de $\mathbb{F}_4$ sont 0, 1, 2 et 3, ce qui reviendrait à croire que le groupe additif de $\mathbb{F}_4$ est cyclique alors qu'il ne contient que des éléments d'ordre 1 ou 2 : ce groupe additif est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$. Puisque la caractéristique est 2, dans le corps $\mathbb{F}_4$, on a $2=0$ et $3=1$. Une façon standard de représenter l'unique structure de corps à quatre éléments consiste à considérer la structure d'anneau quotient $\mathbb{Z}/2\mathbb{Z}[X]/\big(X^2+X+1\big)$. Puisque le polynôme X^2+X+1 est irréductible sur $\mathbb{Z}/2\mathbb{Z}$ et puisque $\mathbb{Z}/2\mathbb{Z}[X]$ est principal, cet anneau est un corps, dont les éléments sont (les classes modulo X^2+X+1 de) 0, 1, X et $X+1$. Les seuls produits non évidents sont $X^2=X+1$, $(X+1)^2=X$ et $X(X+1)=1$. On voit ici la structure de groupe cyclique de $F_4^\times = \langle X\rangle$.

1.2) On calcule les composées. Pour tout $x\in\mathbb{F}_4$,

$$A_{a,\varepsilon,b}\circ A_{c,\zeta,d}(x) = a\left(cx^{2^\zeta}+d\right)^{2^\varepsilon}+b = ac^{2^\varepsilon}x^{2^{\varepsilon+\zeta}}+ad^{2^\varepsilon}+b.$$

Or, $x^4=x$ pour tout $x\in\mathbb{F}_4$, ce qui montre que $x^{2^{\varepsilon+\zeta}}=x$ si $\varepsilon=\zeta$, et que $x^{2^{\varepsilon+\zeta}}=x^2$ si $\varepsilon\neq\zeta$. Ainsi, $A_{a,\varepsilon,b}\circ A_{c,\zeta,d} = A_{ac^{2^\varepsilon},0,ad^{2^\varepsilon}+b}$ si $\varepsilon=\zeta$, et $A_{a,\varepsilon,b}\circ A_{c,\zeta,d} = A_{ac^{2^\varepsilon},1,ad^{2^\varepsilon}+b}$ si $\varepsilon\neq\zeta$, ce qu'il fallait démontrer.

1.3) La formule de la question précédente montre que $\mathrm{AF}(\mathbb{F}_4)$ est stable pour la composition. Elle montre aussi que $A_{a,0,b}\circ A_{a^2,0,ba^2} = A_{a^2,0,ba^2}\circ A_{a,0,b} = A_{1,0,0} = \mathrm{id}_{\mathbb{F}_4}$ et que $A_{a,1,b}\circ A_{a,1,ab^2} = A_{a,1,ab^2}\circ A_{a,1,b} = A_{1,0,0} = \mathrm{id}_{\mathbb{F}_4}$, ce qui montre à la fois que les $A_{a,\varepsilon,b}$ sont des permutations de $\mathbb{F}_4$ et que leurs réciproques sont encore dans $\mathrm{AF}(\mathbb{F}_4)$. Tout cela montre que $\mathrm{AF}(\mathbb{F}_4)$ est un sous-groupe de $\mathfrak{S}_{\mathbb{F}_4}$.

NB : montrer directement que les $A_{a,\varepsilon,b}$ sont des permutations de $\mathbb{F}_4$ et calculer leurs inverses en résolvant les équations $ax+b=y$ et $ax^2+b=y$ se fait en deux coups de cuillère à pot. On trouve si l'on veut la formule générale de l'inverse : $(A_{a,\varepsilon,b})^{-1} = A_{a^{2^{1-\varepsilon}},\varepsilon,(a^2b)^{2^\varepsilon}} = A_{a^{-2^\varepsilon},\varepsilon,(a^2b)^{2^\varepsilon}}$.

1.4) Avec des notations évidentes, on suppose que $A_{a,\varepsilon,b}=A_{c,\zeta,d}$, ce qui signifie que pour tout $x\in\mathbb{F}_4$,

$$ax^{2^\varepsilon}+b = cx^{2^\zeta}+d.$$

Spécialiser en $x=0$ puis en $x=1$ conduit aux égalités $b=d$ et $a=c$ qui, puisque $a\neq 0$, impose que $x^{2^\varepsilon}=x^{2^\zeta}$, pour tout $x\in\mathbb{F}_4$. Alors, si ω est un générateur du groupe $\mathbb{F}_4^\times$, cela conduit à $\omega^{2^\varepsilon}=\omega^{2^\zeta}$. Comme 2^ε et 2^ζ sont dans l'ensemble $\{1,2\}$ et puisque ω est d'ordre 3, cela nécessite que $2^\varepsilon=2^\zeta$, et donc que $\varepsilon=\zeta$. On a montré l'injectivité demandée.

1.5) La question précédente montre que l'écriture des éléments de $\mathrm{AF}(\mathbb{F}_4)$ sous la forme $A_{a,\varepsilon,b}$ est unique, et donc que l'ordre du groupe $\mathrm{AF}(\mathbb{F}_4)$ est celui de $\mathbb{F}_4^\times\times\{0,1\}\times\mathbb{F}_4$, assavoir $3\times 2\times 4 = 24$. Les deux groupes finis $\mathrm{AF}(\mathbb{F}_4)$ et $\mathfrak{S}_{\mathbb{F}_4}$ sont inclus l'un dans l'autre et de même ordre : ils sont égaux. Enfin, puisque le cardinal de $\mathbb{F}_4$ est 4, les groupes $\mathfrak{S}_{\mathbb{F}_4}$ et $\mathfrak{S}_4$ sont isomorphes. On a montré que $\mathrm{AF}(\mathbb{F}_4)\simeq\mathfrak{S}_4$.

2 Produit ensembliste

Soient $h,h'\in H$ et $k,k'\in K$. Puisque $H\triangleleft G$, soit $h''\in H$ tel que $kh'=h''k$. Alors, $hkh'k' = (hh'')(kk')\in HK$. De même, $(hk)^{-1}=k^{-1}h^{-1} = \big(k^{-1}h^{-1}k\big)k^{-1}\in HK$. Cela montre que HK est un sous-groupe de G — la non vacuité de HK est évidente.

En outre, la condition sur les ordres de H et K impose l'unicité de l'écriture sous la forme hk des éléments de HK. En effet, si $hk=h'k'$ (notations évidentes), alors $h^{-1}h' = kk'^{-1}\in H\cap K$; or, $H\cap K$ est à la fois un sous-groupe de H et un sous-groupe de K, ce qui impose, grâce au théorème de Lagrange, que son ordre divise les entiers premiers entre eux $|H|$ et $|K|$: le groupe $H\cap K$ est trivial. Ainsi, $h^{-1}h'=1$ et $kk'^{-1}=1$, *i.e.* $h=h'$ et $k=k'$.

L'unicité de l'écriture sous la forme hk montre que l'application $H \times K \to HK$, $(h,k) \mapsto hk$ est une bijection. Ainsi, $|HK| = |H| \times |K|$.

3 Normaliser les 5-Sylow de $\mathfrak{S}_5$

3.1 Normalisateurs des 5-Sylow de $\mathfrak{S}_5$

3.1) L'ordre de $\mathfrak{S}_5$ est $5! = 5 \times 24$. Comme 24 n'est pas multiple de 5, les 5-Sylow de $\mathfrak{S}_5$ sont ses sous-groupes d'ordre 5. Par exemple, le 5-cycle (12345) engendre un 5-Sylow de $\mathfrak{S}_5$ — c'est le sous-groupe C de la question suivante.

3.2) On calcule *via* la formule de conjugaison des cycles : $qcq^{-1} = (24135) = (13524) = c^2 \in C$.

3.3) On note $Q = \langle q \rangle$ et $G = \langle q, c \rangle = \langle C, Q \rangle$. La question précédente montre que $C \triangleleft G$. En utilisant le résultat de la partie **2**, on obtient que le produit ensembliste CQ est un sous-groupe de G. Comme C et Q sont — évidemment — des sous-groupes de CQ, on en déduit, par minimalité des sous-groupes engendrés, que G est inclus dans CQ, et donc que $G = CQ$. Enfin, puisque $|C| = 5$ et $|Q| = 4$ sont étrangers, la partie **2** montre que $|G| = 4 \times 5 = 20$.

Puisque $qcq^{-1} = c^2 \neq c$, le groupe G n'est pas abélien.

3.4) Chaque 5-Sylow de $\mathfrak{S}_5$ contient exactement quatre 5-cycles en plus de 1. En outre, l'intersections de deux 5-Sylow distincts est triviale puisque 5 est un nombre premier — un groupe d'ordre premier n'a pas de sous-groupe propre, conséquence du théorème de Lagrange. Ainsi, le nombre de 5-Sylow de $\mathfrak{S}_5$ est le quart du nombre de ses 5-cycles, assavoir $\frac{1}{4} \times 24 = 6$.

NB : pour calculer ce nombre n_5, on peut aussi utiliser le troisième théorème de Sylow qui impose que $n_5 \in \{1, 6\}$. Comme $\mathfrak{S}_5$ n'a pas de sous-groupe distingé d'ordre 5 — cela vient de la simplicité de $\mathfrak{A}_5$ —, nécessairement, $n_5 = 6$.

On fait agir $\mathfrak{S}_5$ sur l'ensemble de ses 5-Sylow par conjugaison. Le troisième théorème de Sylow assure qu'il n'y a qu'une seule orbite, dont le cardinal est donc 6. Les groupes d'isotropie ont ainsi pour ordre (commun) $\frac{5!}{6} = 20$. Or, $N = N(C)$ est précisément le groupe d'isotropie de C sous l'action considérée. On a montré que $|N| = 20$.

3.5) Les permutations q et c sont dans N — question **3.2)** ; par minimalité des sous-groupes engendrés, il en résulte que $\langle c, q \rangle \subseteq N$. Or, $\langle c, q \rangle$ et N sont deux groupes finis de même ordre. On en déduit que $N = \langle c, q \rangle$.

3.6) Soient S et T deux 5-Sylow de $\mathfrak{S}_5$. Le premier théorème de Sylow assure que S et T sont conjugués : soit $\pi \in \mathfrak{S}_5$ tel que $S = \pi T \pi^{-1}$. Alors, $N(S) = \pi N(T) \pi^{-1}$. En effet, si $n \in N(T)$, alors $\left(\pi n \pi^{-1}\right) S \left(\pi n \pi^{-1}\right)^{-1} = \pi n T n^{-1} \pi^{-1} = \pi T \pi^{-1} = S$; cela montre que $N(S) \supseteq \pi N(T) \pi^{-1}$. En raisonnant de même en échangeant T et S, il en résulte que $N(S) = \pi N(T) \pi^{-1}$.

Ainsi, si S est un 5-Sylow de $\mathfrak{S}_5$, les groupes $N(S)$ et $N = N(C)$ sont conjugués, donc isomorphes.

3.2 Intersections deux à deux des normalisateurs des 5-Sylow de $\mathfrak{S}_5$

3.7) Soient σ et τ deux 4-cycles de $\mathfrak{S}_5$. Comme les 4-cycles de $\mathfrak{S}_5$ sont tous conjugués, soit $\pi \in \mathfrak{S}_5$ tel que $\tau = \pi \sigma \pi^{-1}$. Alors, l'application $S \mapsto \pi S \pi^{-1}$ est une bijection de l'ensemble des 5-Sylow de $\mathfrak{S}_5$ que σ normalise sur l'ensemble des 5-Sylow de $\mathfrak{S}_5$ que τ normalise. En effet, si $\sigma S \sigma^{-1} = S$, alors $\tau \left(\pi S \pi^{-1}\right) \tau^{-1} = \pi \sigma S \sigma^{-1} \pi^{-1} = \pi S \pi^{-1}$ et l'application $T \mapsto \pi^{-1} T \pi$ est — évidemment — la bijection réciproque. Les deux ensembles cherchés sont en bijection : ils ont le même cardinal.

3.8) Pour tout $S \in \mathcal{S}_5$, le nombre de 4-cycles qui normalisent S est le nombre de 4-cycles de $N(S)$. Puisque $N(S)$ et N sont conjugués, c'est aussi le nombre de 4-cycles de N. Or, les 2-Sylow de N sont cycliques d'ordre 4 (le 4-cycle q est dans l'un d'entre eux). Ils contiennent donc tous exactement deux 4-cycles. Par ailleurs, le nombre de 2-sylow de N, qui est d'ordre 20, divise 5 et est impair. Or, le 2-Sylow $\langle q \rangle$ de N n'est pas normal puisque la formule de conjugaison des cycles assure que $cqc^{-1} = (2354) \notin \langle q \rangle$. Donc le nombre de 2-Sylow de N est 5. Par conséquent, le nombre de 4-cycles qui normalisent S est $5 \times 2 = 10$. On en déduit, puisque $\#\mathcal{S}_5 = 6$, que $\#\mathcal{E} = 6 \times 10 = 60$.

D'autre part, en s'appuyant sur la question précédente, on note N le nombre de 5-Sylow de $\mathfrak{S}_5$ que n'importe quel 4-cycle normalise. Alors, puisque le nombre de 4-cycles de $\mathfrak{S}_5$ est $5 \times 3! = 30$, on en déduit que $\#\mathcal{E} = 30N$.

Des deux façons de compter le cardinal de $\mathcal{E}$, on déduit que $30N = 60$, c'est-à-dire que $N = 2$, ce qu'il fallait démontrer.

3.9) Soit $\mathcal{P}$ l'ensemble des paires de 5-Sylow de $\mathfrak{S}_5$. Soit $\varphi : \mathcal{Q} \to \mathcal{P}$ l'application qui à un 4-cycle de $\mathfrak{S}_5$ associe la paire de 5-Sylow qu'il normalise.
Soit $\{S, T\} \in \mathcal{P}$ ayant une fibre non vide, c'est-à-dire tel qu'il existe un 4-cycle q tel que $\langle q \rangle \subseteq N(S) \cap N(T)$. Alors, le théorème de Lagrange assure que l'ordre du groupe $N(S) \cap N(T)$ est un multiple de 4. Mais $N(S) \cap N(T)$ est un sous-groupe de $N(S)$; or, $|N| = |N(S)| = 20 = 4 \times 5$, ce qui entraîne que tout sous-groupe de $N(S)$ dont l'ordre est un

multiple de 4 est d'ordre 4, à moins d'être $N(S)$ lui-même. Comme $N(S) \neq N(T)$, on en déduit que $\langle q \rangle = N(S) \cap N(T)$. En particulier, $N(S) \cap N(T)$ contient exactement 2 éléments de $\mathcal{Q}$ qui sont q et q^3 : lorsque la fibre par φ d'un élément de $\mathcal{P}$ n'est pas vide, elle est de cardinal 2.

Ainsi, le théorème des bergers assure que l'image de φ a $\frac{30}{2} = 15$ éléments. Comme $\#\mathcal{P} = \binom{6}{2} = 15$, cela montre que φ est surjective, et donc que l'intersection des normalisateurs de deux 5-Sylow quelconques de $\mathfrak{S}_5$ est un groupe cyclique d'ordre 4.