

MAT35B - ALGÈBRE L3A
Premier Semestre — 2021-2022

Examen partiel

Toute réponse non justifiée ne sera pas validée.

Le barème est donné à titre indicatif et non contractuel.

1
2
3

Dans tout le sujet, pour $n \geq 1$, on note \mathbb{S}_n le groupe de permutations de $\llbracket 1, n \rrbracket$ et \mathbb{A}_n le sous-groupe alterné.

2pt

Exercice I.

- (1) Soit G un groupe et $K \triangleleft G$ un sous-groupe distingué d'indice fini. Montrer que, si $g \in G$ est d'ordre d et $\text{PGCD}(d, [G : K]) = 1$, alors $g \in K$. En déduire que si $[G : K] = 2$ et $g \in G$ est d'ordre impair, alors $g \in K$.
- (2) Montrer que le groupe alterné \mathbb{A}_4 possède 8 éléments d'ordre 3. À partir de ces résultats, démontrer que \mathbb{A}_4 n'a pas de sous-groupe d'indice 2.

Solution.

- (1) Comme K est un sous-groupe distingué de G , la projection $\pi : G \rightarrow G/K$ est un morphisme de groupes. En particulier, si $g \in G$ est d'ordre d , alors $\pi(g)$ est d'ordre qui divise d . Par ailleurs, on a aussi $\text{ord}(\pi(g)) \mid |G/K| = [G : K]$ d'après le théorème de Lagrange, et comme $\text{PGCD}(d, [G : K]) = 1$, on a finalement $\text{ord}(\pi(g)) = 1$. En conséquence $\pi(g) = 1_{G/K}$, ce qui nous dit que $g \in K$.
- Si $[G : K] = 2$, alors $\text{PGCD}(2, \text{ord}(g)) = 1$ puisque l'ordre de g est impair. D'après ce qui précède, on a donc bien $g \in K$.
- (2) Il y a $\binom{4}{3} \times 2! = 8$ cycles de longueurs 3 dans \mathbb{S}_4 qui sont tous de signature 1, i.e. dans \mathbb{A}_4 . S'il existe un sous-groupe K d'indice 2 dans \mathbb{A}_4 , alors K est distingué dans \mathbb{A}_4 (voir l'exercice 2 de la fiche 4) et K est d'ordre 6. Mais les 8 éléments d'ordre 3, qui est impair, sont tous dans K d'après la question précédente, ce qui nous donne une contradiction.

8pt

Exercice II. On note $E = \{H : H \text{ sous-groupe de } \mathbb{S}_5 \text{ et } |H| = 5\}$ l'ensemble des sous-groupes d'ordre 5 de \mathbb{S}_5 et $\text{Bij}(E)$ le groupe des bijections de E dans E . On considère l'action $\Phi : \mathbb{S}_5 \rightarrow \text{Bij}(E)$ de \mathbb{S}_5 sur E par conjugaison, i.e. $\Phi(\sigma)(H) = \sigma H \sigma^{-1}$, pour tous $\sigma \in \mathbb{S}_5$ et $H \in E$.

- (1) Pour $n \in \mathbb{N}^*$, rappeler (sans démonstration) comment calculer l'ordre de $\sigma \in \mathbb{S}_n$ à partir de sa décomposition en produit de cycles à supports deux à deux disjoints. Quelles sont les permutations conjuguées à σ dans \mathbb{S}_n ?

- (2) Quels sont les éléments d'ordre 5 dans \mathbb{S}_5 ? Combien y en a-t-il dans \mathbb{S}_5 ? Combien y en a-t-il dans un sous-groupe d'ordre 5 de \mathbb{S}_5 ?
- (3) En déduire que l'ensemble E est de cardinal 6.
- (4) Déterminer l'orbite de $H \in E$ pour l'action de \mathbb{S}_5 par conjugaison.
- (5) Que peut-on dire de $\text{Ker}(\Phi)$ et $\text{Im}(\Phi)$ et de leurs cardinaux ? Déduire de la question précédente que $\text{Ker}(\Phi) = \{\text{id}_{\llbracket 1,5 \rrbracket}\}$. Quel est l'ordre de $\text{Im}(\Phi)$ et son indice dans $\text{Bij}(E)$?
- (6) Soit $H \in E$. On note $\Sigma_H = \{f \in \text{Bij}(E) : f(H) = H\}$.
Montrer que Σ_H est un sous-groupe isomorphe à $\text{Bij}(E \setminus \{H\})$ et donc que $\Sigma_H \simeq \mathbb{S}_5$, puis que Σ_H n'est pas conjugué à $\Phi(\mathbb{S}_5)$ dans $\text{Bij}(E)$.
- (7) En déduire que le groupe symétrique \mathbb{S}_6 contient au moins 7 sous-groupes différents isomorphes à \mathbb{S}_5 .

Solution.

- (1) Si $\sigma = \gamma_1 \dots \gamma_k$ est la décomposition de σ en cycles à support deux à deux disjoints, l'ordre de σ est égal au PPCM($\text{ord}(\gamma_i) : i \in \{1, \dots, k\}$). Les permutations conjuguées à σ dans \mathbb{S}_n sont les permutations ayant une décomposition en cycles de même type.
- (2) Si $\sigma \in \mathbb{S}_5$ est d'ordre 5, il n'y a que des 5-cycles dans sa décomposition en cycles disjoints (puisque 5 est premier), et au plus un cycle dans cette décomposition puisque \mathbb{S}_5 agit sur un ensemble à 5 éléments. Il y a $4! = 24$ façons de choisir un 5-cycle dans \mathbb{S}_5 . Si H est un sous-groupe d'ordre 5 de \mathbb{S}_5 , alors tous ses éléments sont d'ordre 1 ou 5 d'après le théorème de Lagrange. Il y a donc 4 éléments d'ordre 5 dans H .
- (3) Chaque sous-groupe d'ordre 5 contient 4 éléments d'ordre 5 et les sous-groupes ne s'intersectent qu'en l'élément neutre (si deux sous-groupes contenaient un même élément d'ordre 5 alors cet élément engendre tout le sous-groupe et les deux sous-groupes sont confondus). Donc il y a $24/4 = 6$ sous-groupes d'ordre 5 dans \mathbb{S}_5 et E est de cardinal 6.
- (4) Les 5-cycles étant tous conjugués, il n'y a qu'une seule orbite pour l'action de \mathbb{S}_5 pour l'action par conjugaison sur E . Si $H \in E$, on a donc $\text{Orb}(H) = E$.
- (5) Le noyau de Φ est un sous-groupe distingué de \mathbb{S}_5 donc soit réduit à l'identité, soit égal à \mathbb{A}_5 , soit \mathbb{S}_5 tout entier. Par conséquent le cardinal de $\text{Im}(\Phi)$ est égal à $5!$, 2 ou 1 respectivement. Or, d'après la question précédente, le cardinal de $\text{Im}(\Phi)$ est au moins égal à 6 (puisque on a une application surjective de $\Phi(\mathbb{S}_5)$ dans $\text{Orb}(H)$), donc $\text{Im}(\Phi) = 5!$, d'indice 6 et le noyau est réduit à l'élément neutre. En particulier $\text{Im}(\Phi) \simeq \mathbb{S}_5$.
- (6) Il est clair que Σ_H est un sous-groupe de $\text{Bij}(E)$ (c'est le stabilisateur de H sous l'action naturelle de $\text{Bij}(E)$ sur E) et que le morphisme $f \in \Sigma_H \mapsto f|_{E \setminus H} \in \text{Bij}(E \setminus \{H\})$ est bijectif. Pour H fixé, Σ_H est donc isomorphe à \mathbb{S}_5 . Comme l'action Φ est transitive, elle ne fixe aucun élément de E , donc $\Phi(\mathbb{S}_5) \neq \Sigma_H$ pour tout $H \in E$. Enfin, si $\sigma \in \text{Bij}(E)$, alors $\sigma \Sigma_H \sigma^{-1} = \Sigma_{\sigma H}$ donc Σ_H n'est pas conjugué à $\Phi(\mathbb{S}_5)$.
- (7) Ainsi tous les stabilisateurs des éléments de E sont des sous-groupes de \mathbb{S}_6 isomorphes à \mathbb{S}_5 qui sont distincts 2 à 2 mais également distincts de $\Phi(\mathbb{S}_5) \simeq \mathbb{S}_5$. Comme E est de cardinal 6, on a bien 7 sous-groupes différents dans \mathbb{S}_6 isomorphes à \mathbb{S}_5 .

10pt

Exercice III.

Soient \mathbb{k} un corps fini à q éléments, $V = \mathbb{k}^2$ et $X = V \setminus \{\mathbf{0}_V\}$, où $\mathbf{0}_V = (0, 0)$.

(1) Justifier que pour toute matrice inversible $A \in \text{GL}_2(\mathbb{k})$ et tout vecteur $v \in V$ non nul, on a $Av \neq \mathbf{0}_V$.

On note alors $\rho : \text{GL}_2(\mathbb{k}) \times X \rightarrow X$, $(A, v) \mapsto Av$ l'action naturelle du groupe $\text{GL}_2(\mathbb{k})$ sur l'ensemble X .

(2) Montrer que l'action ρ est transitive.

(3) Déterminer le stabilisateur du vecteur $e_1 = (1, 0)$ et calculer son cardinal.

(4) En déduire que $|\text{GL}_2(\mathbb{k})| = (q^2 - 1)(q^2 - q)$.

(5) Montrer que le morphisme de groupes $\det : \text{GL}_2(\mathbb{k}) \rightarrow \mathbb{k}^*$ est surjectif et calculer le cardinal de $\text{SL}_2(\mathbb{k})$.

On considère la relation d'équivalence \sim sur X définie par

$$v \sim w \text{ si et seulement s'il existe } \lambda \in \mathbb{k}^* \text{ tel que } v = \lambda w.$$

On note $\mathbb{P}(V)$ l'ensemble quotient X / \sim et pour $v \in X$, on note $[v] = \{w \in X : w \sim v\}$ la classe d'équivalence de v .

(6) Décrire les classes d'équivalence de \sim et déterminer leur cardinal. En déduire que $|\mathbb{P}(V)| = q + 1$.

(7) Démontrer que pour tout $A \in \text{GL}_2(\mathbb{k})$, l'application $\rho(A, \cdot) : X \rightarrow X$ qui associe Av à $v \in X$ passe au quotient par \sim et définit une application $\bar{\rho}(A, \cdot) : \mathbb{P}(V) \rightarrow \mathbb{P}(V)$. Montrer en plus que $\bar{\rho}$ est une action de $\text{GL}_2(\mathbb{k})$ sur $\mathbb{P}(V)$.

(8) En déduire un morphisme de groupes $\psi : \text{GL}_2(\mathbb{k}) \rightarrow \mathbb{S}_{q+1}$.

On notera $\varphi : \text{SL}_2(\mathbb{k}) \rightarrow \mathbb{S}_{q+1}$ la restriction de ψ à $\text{SL}_2(\mathbb{k})$.

Dans la suite, on admettra le résultat « classique » suivant :

$$\{A \in \text{GL}_2(\mathbb{k}) : \bar{\rho}(A, \cdot) = \text{id}_{\mathbb{P}(V)}\} = \{\lambda I_2 : \lambda \in \mathbb{k}^*\}.$$

(9) Montrer l'isomorphisme de groupes $\text{GL}_2(\mathbb{Z}/2\mathbb{Z}) \simeq \mathbb{S}_3$.

(10) Soient $[v_1], [v_2]$ et $[v_3]$ trois éléments distincts de $\mathbb{P}(V)$.

i. Montrer qu'il existe trois vecteurs $u_1 \in [v_1], u_2 \in [v_2]$ et $u_3 \in [v_3]$ tels que $u_3 = -u_1 - u_2$. Justifier que (u_1, u_2) est une base de V .

ii. Soient f l'endomorphisme de V tel que $f(u_1) = u_2$ et $f(u_2) = u_3$ et A sa matrice dans la base canonique. Que vaut $f(u_3)$? Justifier que $A \in \text{SL}_2(\mathbb{k})$.

(11) On suppose $\mathbb{k} = \mathbb{Z}/3\mathbb{Z}$, et donc $q = 3$. À l'aide de la question précédente, montrer que $\text{Im}(\varphi)$ contient tous les 3-cycles.

(12) En déduire l'existence des isomorphismes de groupes suivants :

$$\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})/\{\pm I_2\} \simeq \mathbb{S}_4 \text{ et } \mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})/\{\pm I_2\} \simeq \mathbb{A}_4.$$

Solution.

(1) Comme A est inversible, $Av = \mathbf{0}_V$ implique $v = A^{-1}Av = \mathbf{0}_V$.

(2) Il suffit de montrer que, étant donné $v \in X$, il existe une matrice $A \in \mathrm{GL}_2(\mathbb{k})$ telle que $Ae_1 = v$. Comme v est non nul, on peut compléter (v) en une base (v, w) de V . On considère alors la matrice A dont la première colonne est v et la deuxième colonne est w . En conséquence, $Ae_1 = v$ et $Ae_2 = w$, où e_2 est le deuxième vecteur de la base canonique de V . Comme (v, w) est une base de V , A est inversible, i.e. $A \in \mathrm{GL}_2(\mathbb{k})$.

(3) On voit bien que

$$\mathrm{Stab}(e_1) = \{A \in \mathrm{GL}_2(\mathbb{k}) : Ae_1 = e_1\} = \left\{ \begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix} : d \neq 0 \right\},$$

où l'on a utilisé qu'une matrice $A \in M_2(\mathbb{k})$ est dans $\mathrm{GL}_2(\mathbb{k})$ si et seulement si son déterminant est non nul. En conséquence, $|\mathrm{Stab}(e_1)| = q(q-1)$.

(4) D'après le cours, l'orbite de e_1 est en bijection avec l'ensemble quotient $\mathrm{GL}_2(\mathbb{k})/\mathrm{Stab}(e_1)$. Comme l'action est transitive (question 2), l'orbite de e_1 est X tout entier. Par suite,

$$q^2 - 1 = |X| = |\mathrm{GL}_2(\mathbb{k})/\mathrm{Stab}(e_1)| = \frac{|\mathrm{GL}_2(\mathbb{k})|}{|\mathrm{Stab}(e_1)|} = \frac{|\mathrm{GL}_2(\mathbb{k})|}{q(q-1)},$$

(où l'on a utilisé la question précédente), ce qui implique que $|\mathrm{GL}_2(\mathbb{k})| = (q^2 - 1)(q^2 - q)$.

(5) Pour tout $a \in \mathbb{k}$ on a l'égalité $a = \det \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$, et cette matrice est dans $\mathrm{GL}_2(\mathbb{k})$ ssi $a \neq 0$, donc $\det : \mathrm{GL}_2(\mathbb{k}) \rightarrow \mathbb{k}^*$ est surjectif. Comme $\mathrm{SL}_2(\mathbb{k}) = \mathrm{Ker}(\det)$, on en déduit une bijection $\mathrm{GL}_2(\mathbb{k})/\mathrm{SL}_2(\mathbb{k}) \rightarrow \mathbb{k}^*$, d'où

$$q - 1 = |\mathbb{k}^*| = |\mathrm{GL}_2(\mathbb{k})/\mathrm{SL}_2(\mathbb{k})| = \frac{|\mathrm{GL}_2(\mathbb{k})|}{|\mathrm{SL}_2(\mathbb{k})|} = \frac{(q^2 - 1)(q^2 - q)}{|\mathrm{SL}_2(\mathbb{k})|},$$

ce qui implique que $|\mathrm{SL}_2(\mathbb{k})| = q(q^2 - 1)$.

(6) Pour tout $v \in X$, on a $[v] = \{\lambda v : \lambda \in \mathbb{k}^*\}$; il s'agit donc de la droite vectorielle $\mathrm{Vect}(v)$ privée du vecteur nul. De plus, l'application $\ell_v : \mathbb{k}^* \rightarrow [v], \lambda \mapsto \lambda v$ est bijective : en effet, la surjectivité découle de la définition de \sim , tandis que l'injectivité provient du fait que $\lambda v = \lambda' v$ équivaut à $(\lambda - \lambda')v = \mathbf{0}_V$, qui implique $\lambda = \lambda'$ puisque $v \neq \mathbf{0}_V$.

En conséquence, $\#[v] = \#(\mathbb{k}^*) = q - 1$. Comme $X = \bigsqcup_{[v] \in \mathbb{P}(V)} [v]$, on conclut que

$$q^2 - 1 = |X| = \sum_{[v] \in \mathbb{P}(V)} \#[v] = \sum_{[v] \in \mathbb{P}(V)} (q - 1) = (q - 1)\#(\mathbb{P}(V)),$$

ce qui implique que $\#(\mathbb{P}(V)) = (q^2 - 1)/(q - 1) = q + 1$.

(7) Il suffit de montrer que $[\rho(A, \lambda v)] = [\rho(A, v)]$ pour tous $v \in X$ et $\lambda \in \mathbb{k}^*$. Cela est immédiat, vu que $\rho(A, \lambda v) = A\lambda v = \lambda Av = \lambda \rho(A, v)$. En conséquence, on obtient une application $\bar{\rho} : \text{GL}_2(\mathbb{k}) \times \mathbb{P}(V) \rightarrow \mathbb{P}(V)$ qui associe $[\rho(A, v)]$ à $(A, [v])$, pour $A \in \text{GL}_2(\mathbb{k})$ et $v \in X$. Il s'agit clairement d'une action, vu que $\bar{\rho}(I_2, [v]) = [\rho(I_2, v)] = [v]$ et

$$\bar{\rho}(A, \bar{\rho}(B, [v])) = \bar{\rho}(A, [\rho(B, v)]) = [\rho(A, \rho(B, v))] = [\rho(AB, v)] = \bar{\rho}(AB, [v]),$$

pour tous $v \in X$ et $A, B \in \text{GL}_2(\mathbb{k})$.

(8) L'action $\bar{\rho} : \text{GL}_2(\mathbb{k}) \times \mathbb{P}(V) \rightarrow \mathbb{P}(V)$ induit un morphisme de groupes de $\text{GL}_2(\mathbb{k})$ dans l'ensemble $\text{Bij}(\mathbb{P}(V))$ des bijections de $\mathbb{P}(V)$ (cf. cours). Comme $\#\mathbb{P}(V) = q + 1$, les groupes $\text{Bij}(\mathbb{P}(V))$ et \mathbb{S}_{q+1} sont isomorphes, et on obtient ainsi un morphisme de groupes $\psi : \text{GL}_2(\mathbb{k}) \rightarrow \mathbb{S}_{q+1}$.

(9) Le morphisme de groupes $\psi : \text{GL}_2(\mathbb{Z}/2\mathbb{Z}) \rightarrow \mathbb{S}_3$ est injectif, vu que le noyau est, d'après le fait rappelé ci-dessus, $\{\lambda I_2 : \lambda \in \mathbb{k}^*\} = \{I_2\}$, qui est donc trivial. Comme $|\text{GL}_2(\mathbb{Z}/2\mathbb{Z})| = (2^2 - 2)(2^2 - 1) = 6 = |\mathbb{S}_3|$, le morphisme ψ est bijectif.

(10) i. Comme $[v_1] \neq [v_2]$, on a $v_1 \not\sim v_2$, donc v_1 et v_2 ne sont pas colinéaires. Ils forment donc une base de $V = \mathbb{k}^2$. Soit (λ, μ) les coordonnées de v_3 dans cette base. Alors $\lambda \neq 0$, sinon on aurait $v_3 = \mu v_2 \sim v_2$, i.e. $[v_3] = [v_2]$, ce qui donne une contradiction. Pour la même raison $\mu \neq 0$. On pose alors $u_1 = -\lambda v_1 \in [v_1]$ et $u_2 = -\mu v_2 \in [v_2]$. Ces deux vecteurs sont toujours non colinéaires donc forment une base de V . Avec $u_3 = v_3 \in [v_3]$, on trouve $u_3 = \lambda v_1 + \mu v_2 = -u_1 - u_2$.

ii. $f(u_3) = f(-u_1 - u_2) = -f(u_1) - f(u_2) = -u_2 - u_3 = -u_2 - (-u_1 - u_2) = u_1$. On en déduit que dans la base (u_1, u_2) , la matrice de f est

$$\text{Mat}_{(u_1, u_2)}(f) = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix},$$

qui a déterminant égal à 1. Donc $\det(A) = \det(f) = 1$, i.e. A appartient à $\text{SL}_2(\mathbb{k})$.

(11) Soient $[v_1], [v_2], [v_3]$ trois éléments distincts de $\mathbb{P}(V)$, qui est ici de cardinal $3 + 1 = 4$. Notons $[v_4]$ le dernier élément de $\mathbb{P}(V)$. On considère la matrice A de la question précédente associée à $[v_1], [v_2], [v_3]$, l'endomorphisme correspondant f et les trois vecteurs u_1, u_2, u_3 . On a alors $\bar{\rho}(A, [v_1]) = \bar{\rho}(A, [u_1]) = [Au_1] = [f(u_1)] = [u_2] = [v_2]$, et de même $\bar{\rho}(A, [v_2]) = [v_3]$ et $\bar{\rho}(A, [v_3]) = [v_1]$. Puisque $\bar{\rho}(A, \cdot)$ est une bijection, on a aussi $\bar{\rho}(A, [v_4]) = [v_4]$. La permutation $\bar{\rho}(A, \cdot)$ de $\mathbb{P}(V)$ est donc un 3-cycle, de support $([v_1], [v_2], [v_3])$. Comme $A \in \text{SL}_2(\mathbb{Z}/3\mathbb{Z})$, et que cela est vrai quels que soient les trois éléments distincts choisis, on en déduit que l'image de $\text{SL}_2(\mathbb{Z}/3\mathbb{Z})$ par l'application $A \mapsto \bar{\rho}(A, \cdot)$ contient tous les 3-cycles de $\text{Bij}(\mathbb{P}(V)) \simeq \mathbb{S}_4$, et finalement que c'est aussi le cas de $\text{Im}(\varphi)$.

(12) D'après le résultat admis on a $\text{Ker}(\psi) = \{\lambda I_2 : \lambda \in (\mathbb{Z}/3\mathbb{Z})^*\} = \{\pm I_2\}$, d'où par passage au quotient un morphisme de groupes injectif $\bar{\psi} : \text{GL}_2(\mathbb{Z}/3\mathbb{Z})/\{\pm I_2\} \rightarrow \mathbb{S}_4$. Or $|\text{GL}_2(\mathbb{Z}/3\mathbb{Z})/\{\pm I_2\}| = |\text{GL}_2(\mathbb{Z}/3\mathbb{Z})|/2 = (3^2 - 3)(3^2 - 1)/2 = 24 = |\mathbb{S}_4|$ donc ce morphisme est en fait bijectif.

Ensuite, par restriction $\text{Ker}(\varphi) = \text{Ker}(\psi) \cap \text{SL}_2(\mathbb{Z}/3\mathbb{Z}) = \{\pm I_2\}$ puisque $\det(I_2) = \det(-I_2) = 1$. Par passage au quotient, on a encore un morphisme de groupes injectif $\bar{\varphi} : \text{SL}_2(\mathbb{Z}/3\mathbb{Z})/\{\pm I_2\} \rightarrow \mathbb{S}_4$. D'après la question précédente $\text{Im}(\varphi)$ ($= \text{Im}(\bar{\varphi})$) contient tous les 3-cycles, et les 3-cycles engendrent \mathbb{A}_4 (cf. cours), donc $\mathbb{A}_4 \subset \text{Im}(\bar{\varphi})$. Par ailleurs $|\text{SL}_2(\mathbb{Z}/3\mathbb{Z})/\{\pm I_2\}| = |\text{SL}_2(\mathbb{Z}/3\mathbb{Z})|/2 = (3^2 - 3)(3 + 1)/2 = 12 = |\mathbb{A}_4|$. On en déduit que $\mathbb{A}_4 = \text{Im}(\bar{\varphi})$, puis que $\bar{\varphi}$ est un isomorphisme de groupes entre $\text{SL}_2(\mathbb{Z}/3\mathbb{Z})/\{\pm I_2\}$ et \mathbb{A}_4 .