Corrigé de l'Examen d'Algèbre 2

Exercices 3, 4 et 5

Janvier 2026

Exercice 3 : Étude du groupe affine et de ses actions

1. Structure algébrique

(a) Soit $M = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in G$. On a $\det(M) = a \times 1 - 0 \times b = a$. Puisque $a \in \mathbb{R}^*$, $\det(M) \neq 0$, donc $M \in \mathrm{GL}_2(\mathbb{R})$.

— L'élément neutre $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ appartient à G ($a = 1, b = 0$).

— Soient $M = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ et $M' = \begin{pmatrix} a' & b' \\ 0 & 1 \end{pmatrix}$ dans G.

$$MM' = \begin{pmatrix} aa' & ab' + b \\ 0 & 1 \end{pmatrix}$$

Comme $a, a' \in \mathbb{R}^*$, $aa' \in \mathbb{R}^*$. Et $ab' + b \in \mathbb{R}$. Donc $MM' \in G$.

— Inverse : $M^{-1} = \frac{1}{a} \begin{pmatrix} 1 & -b \\ 0 & a \end{pmatrix} = \begin{pmatrix} 1/a & -b/a \\ 0 & 1 \end{pmatrix} \in G$.

G est donc un sous-groupe de $\mathrm{GL}_2(\mathbb{R})$. Le groupe n'est **pas abélien**. Par exemple, pour $A = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$ et $B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, on a $AB = \begin{pmatrix} 2 & 2 \\ 0 & 1 \end{pmatrix}$ mais $BA = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}$.

(b) Cherchons le centre $Z(G)$. Soit $M = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in Z(G)$. Pour tout $X = \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} \in G$, on doit avoir $MX = XM$.

$$\begin{pmatrix} ax & ay + b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} xa & xb + y \\ 0 & 1 \end{pmatrix}$$

Cela impose $ax = xa$ (toujours vrai) et $ay + b = xb + y$. Pour que $ay + b = xb + y$ soit vrai pour *tous* $x \in \mathbb{R}^*$ et $y \in \mathbb{R}$, prenons $y = 1, x = 1 \implies a + b = b + 1 \implies a = 1$. L'équation devient $1y + b = 1b + y \implies b = b$. Cependant, si on prend $y = 0$ et $x = 2$ dans l'équation initiale avec $a = 1$: $b = 2b \implies b = 0$. Donc $Z(G) = \{I_2\}$.

(c)

i. Vérifions la distinction par conjugaison. Soit $M = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in G$ et $K = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \in H$.

$$MKM^{-1} = \begin{pmatrix} a & ak + b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1/a & -b/a \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -b + ak + b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & ak \\ 0 & 1 \end{pmatrix} \in H$$

Donc H est un sous-groupe distingué de G.

ii. $\psi(b)\psi(b') = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b+b' \\ 0 & 1 \end{pmatrix} = \psi(b+b')$. ψ est un morphisme bijectif, donc un isomorphisme de $(\mathbb{R}, +)$ vers $(H, \times)$.

(d) $\phi \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} = a$.

i. $\phi(MM') = \phi \begin{pmatrix} aa' & \dots \\ 0 & 1 \end{pmatrix} = aa' = \phi(M)\phi(M')$. C'est un morphisme. Il est surjectif car pour tout $x \in \mathbb{R}^*$, la matrice $\begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}$ est un antécédent.

ii. $\ker(\phi) = \{M \in G \mid a = 1\} = H$.

iii. **Théorème d'isomorphisme :** Soit $f : G \to G'$ un morphisme de groupes. Alors $G/\ker(f)$ est isomorphe à $\mathrm{Im}(f)$.

iv. Ici, $\mathrm{Im}(\phi) = \mathbb{R}^*$. Donc $G/H \simeq (\mathbb{R}^*, \times)$.

2. Action de groupe sur le plan

(e) $g \cdot X = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax+by \\ y \end{pmatrix}$.

(f)

i. Si $y \neq 0$. L'ordonnée de $g \cdot X$ est toujours y. L'abscisse est $x' = ax + by$. Comme a parcourt $\mathbb{R}^*$ et b parcourt $\mathbb{R}$, la valeur $ax + by$ peut prendre n'importe quelle valeur réelle (fixons $a = 1$, alors $x + by$ décrit $\mathbb{R}$ quand b varie). L'orbite est la droite horizontale d'équation $Y = y$.

ii. Pour $E_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, ici $y = 0$. L'ordonnée reste 0. L'abscisse devient $a(1) + b(0) = a$. Comme $a \in \mathbb{R}^*$, l'orbite est l'axe des abscisses privé de l'origine : $\mathbb{R}^* \times \{0\}$.

iii. Pour l'origine, $x = 0, y = 0$. $g \cdot O = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$. L'orbite est le singleton $\{(0, 0)\}$.

iv. La partition est constituée de : l'origine $\{0\}$, l'axe des abscisses privé de 0, et toutes les droites horizontales $Y = c$ pour chaque $c \neq 0$.

3. Lien géométrique

(g) Soit $\Gamma : G \to \mathrm{Aff}(\mathbb{R})$ définie par $\Gamma \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} = f_{a,b}$ où $f_{a,b}(t) = at + b$. Vérifions le morphisme : Soient $M = (a, b)$ et $M' = (a', b')$. $MM' = (aa', ab' + b)$. $\Gamma(MM') = f_{aa',ab'+b}$. D'autre part, $\Gamma(M) \circ \Gamma(M') = f_{a,b} \circ f_{a',b'}$. $(f_{a,b} \circ f_{a',b'})(t) = a(a't + b') + b = aa't + ab' + b = f_{aa',ab'+b}(t)$. C'est bien un isomorphisme (bijectif par construction des paramètres).

On considère l'ensemble G des matrices de la forme :

$$A(f,g,h) = \begin{pmatrix} 1 & f(X) & h(X,Y) \\ 0 & 1 & g(Y) \\ 0 & 0 & 1 \end{pmatrix}$$

où $f \in \mathbb{R}[X]$, $g \in \mathbb{R}[Y]$ et $h \in \mathbb{R}[X,Y]$.

1. Sous-groupe de $UT_3(\mathbb{R}(x,y))$

Pour montrer que G est un sous-groupe du groupe $UT_3(\mathbb{R}(x,y))$ des matrices triangulaires supérieures unipotentes à coefficients rationnels, nous devons vérifier trois points :

1. **Inclusion :** Les coefficients $f(X)$, $g(Y)$ et $h(X,Y)$ sont des polynômes, donc des fractions rationnelles particulières (dénominateur égal à 1). De plus, les éléments diagonaux valent 1 et la partie triangulaire inférieure est nulle. Donc $G \subset UT_3(\mathbb{R}(x,y))$.
2. **Élément neutre :** La matrice identité I_3 correspond au cas où $f = 0$, $g = 0$ et $h = 0$. Comme le polynôme nul appartient bien à $\mathbb{R}[X]$, $\mathbb{R}[Y]$ et $\mathbb{R}[X,Y]$, on a $I_3 \in G$.
3. **Stabilité par produit :** Soient $M_1 = A(f_1, g_1, h_1)$ et $M_2 = A(f_2, g_2, h_2)$ deux éléments de G. Calculons le produit :

$$\begin{aligned} M_1M_2 &= \begin{pmatrix} 1 & f_1 & h_1 \\ 0 & 1 & g_1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & f_2 & h_2 \\ 0 & 1 & g_2 \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & f_1 + f_2 & h_2 + f_1g_2 + h_1 \\ 0 & 1 & g_1 + g_2 \\ 0 & 0 & 1 \end{pmatrix} \end{aligned}$$

   Posons $f' = f_1 + f_2$, $g' = g_1 + g_2$ et $h' = h_1 + h_2 + f_1(X)g_2(Y)$. On a bien $f' \in \mathbb{R}[X]$ et $g' \in \mathbb{R}[Y]$. De plus, le produit $f_1(X)g_2(Y)$ est un polynôme en X et Y, donc $h' \in \mathbb{R}[X,Y]$. Ainsi, $M_1M_2 \in G$.
4. **Stabilité par inverse :** Soit $M = A(f,g,h) \in G$. Cherchons son inverse. On sait que l'inverse d'une matrice triangulaire unipotente est de la même forme. En résolvant $MM^{-1} = I_3$, on trouve :

$$M^{-1} = \begin{pmatrix} 1 & -f & fg - h \\ 0 & 1 & -g \\ 0 & 0 & 1 \end{pmatrix}$$

   On vérifie que $-f \in \mathbb{R}[X]$, $-g \in \mathbb{R}[Y]$ et $f(X)g(Y) - h(X,Y) \in \mathbb{R}[X,Y]$. Donc $M^{-1} \in G$.

Conclusion : G est bien un sous-groupe de $UT_3(\mathbb{R}(x,y))$.

2. Calcul du commutateur

Le commutateur de deux matrices A et B est défini par $[A,B] = ABA^{-1}B^{-1}$. Soient $A = A(f_1, g_1, h_1)$ et $B = A(f_2, g_2, h_2)$.

D'après le calcul de produit effectué précédemment :

$$AB = A(f_1 + f_2, g_1 + g_2, h_1 + h_2 + f_1g_2)$$

$$BA = A(f_2 + f_1, g_2 + g_1, h_2 + h_1 + f_2g_1)$$

On remarque que AB et BA ont les mêmes coefficients sur la diagonale et sur la sur-diagonale immédiate (positions $(1,2)$ et $(2,3)$). Ils ne diffèrent que par le terme en position $(1,3)$. Posons $\Delta = (AB)_{1,3} - (BA)_{1,3}$.

$$\Delta = (h_1 + h_2 + f_1 g_2) - (h_2 + h_1 + f_2 g_1) = f_1(X)g_2(Y) - f_2(X)g_1(Y)$$

Le commutateur $[A,B]$ est égal à $(AB)(BA)^{-1}$. Comme AB et BA ne diffèrent que par le terme $(1,3)$, leur quotient est une matrice où seule la composante $(1,3)$ est non nulle (en dehors de la diagonale). Plus précisément, si $M = \begin{pmatrix} 1 & u & w \\ 0 & 1 & v \\ 0 & 0 & 1 \end{pmatrix}$ et $M' = \begin{pmatrix} 1 & u & w' \\ 0 & 1 & v \\ 0 & 0 & 1 \end{pmatrix}$, alors $M(M')^{-1} = \begin{pmatrix} 1 & 0 & w-w' \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

Ainsi, le commutateur est :

$$[A,B] = \begin{pmatrix} 1 & 0 & f_1(X)g_2(Y) - f_2(X)g_1(Y) \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

3. Le groupe dérivé $D(G)$

Le groupe dérivé $D(G)$ est le sous-groupe engendré par les commutateurs. D'après la question précédente, tout commutateur est de la forme $A(0,0,P)$ avec $P(X,Y) = f_1(X)g_2(Y) - f_2(X)g_1(Y)$.

L'ensemble des matrices de la forme $A(0,0,h)$ constitue un sous-groupe abélien isomorphe au groupe additif des polynômes $\mathbb{R}[X,Y]$ (le produit de matrices correspond à la somme des termes h). Pour montrer que $D(G)$ est l'ensemble de toutes les matrices $A(0,0,h)$ avec $h \in \mathbb{R}[X,Y]$, il suffit de montrer que tout polynôme $h(X,Y)$ peut s'écrire comme une somme de termes de la forme $f_1 g_2 - f_2 g_1$.

Considérons un monôme quelconque $X^i Y^j$. Si l'on choisit :

— $f_1(X) = X^i$ et $g_2(Y) = Y^j$

— $f_2(X) = 0$ et $g_1(Y) = 0$

Alors le terme du commutateur est $X^i \cdot Y^j - 0 = X^i Y^j$. Ainsi, tout monôme est un commutateur. Comme tout polynôme de $\mathbb{R}[X,Y]$ est une somme finie de monômes, tout polynôme peut être engendré par des produits de commutateurs.

Conclusion : Le groupe dérivé de G est l'ensemble des matrices :

$$B = \begin{pmatrix} 1 & 0 & h(X,Y) \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{avec } h \in \mathbb{R}[X,Y].$$

4. La matrice C n'est pas un commutateur

On souhaite montrer que la matrice C définie par le polynôme $h(X,Y) = X^2 + XY + Y^2$ n'est pas un commutateur.

Raisonnement par l'absurde : Supposons que C soit un commutateur. D'après la question 2, il existerait des polynômes $f_1, f_2 \in \mathbb{R}[X]$ et $g_1, g_2 \in \mathbb{R}[Y]$ tels que :

$$X^2 + XY + Y^2 = f_1(X)g_2(Y) - f_2(X)g_1(Y)$$

Notons $g_1(Y)$ et $g_2(Y)$ sous la forme de leur développement en puissances de Y :

$$g_1(Y) = \sum_k a_k Y^k \quad \text{et} \quad g_2(Y) = \sum_k b_k Y^k$$

où a_k et b_k sont des coefficients réels.

En remplaçant ces expressions dans l'équation initiale, on obtient :

$$\begin{aligned} X^2 + XY + Y^2 &= f_1(X) \left(\sum_k b_k Y^k \right) - f_2(X) \left(\sum_k a_k Y^k \right) \\ &= \sum_k \left(b_k f_1(X) - a_k f_2(X) \right) Y^k \end{aligned}$$

Cette égalité est une égalité entre deux polynômes à deux variables. On peut identifier les coefficients des puissances de Y de chaque côté. Regardons les coefficients devant Y^0 (terme constant en Y), Y^1 et Y^2 :

— Coefficient de Y^0 (à gauche X^2) :

$$X^2 = b_0 f_1(X) - a_0 f_2(X)$$

— Coefficient de Y^1 (à gauche X) :

$$X = b_1 f_1(X) - a_1 f_2(X)$$

— Coefficient de Y^2 (à gauche 1) :

$$1 = b_2 f_1(X) - a_2 f_2(X)$$

Argument d'algèbre linéaire : Considérons l'espace vectoriel $\mathbb{R}[X]$. Soit $V = \text{Vect}(f_1, f_2)$ le sous-espace vectoriel engendré par les polynômes f_1 et f_2. Par définition, la dimension de V est au plus 2 ($\dim(V) \leq 2$).

Or, les relations ci-dessus montrent que les polynômes 1, X et X^2 sont des combinaisons linéaires de f_1 et f_2. Autrement dit :

$$\{1, X, X^2\} \subset \text{Vect}(f_1, f_2)$$

Cependant, la famille $\mathcal{F} = \{1, X, X^2\}$ est une famille libre de $\mathbb{R}[X]$. Le sous-espace engendré par $\mathcal{F}$ est donc de dimension 3.

Il est impossible qu'un espace de dimension 3 soit inclus dans un espace V de dimension au plus 2.

Conclusion : L'hypothèse de départ est fausse. Il est impossible d'écrire $X^2 + XY + Y^2$ sous la forme $f_1 g_2 - f_2 g_1$. La matrice C n'est pas un commutateur.

Exercice 5 : Les 3-Sylow de $\mathfrak{S}_6$

1. Ordre et structure abstraite

(a) $|\mathfrak{S}_6| = 6! = 720$. Décomposition en facteurs premiers : $720 = 72 \times 10 = 8 \times 9 \times 10 = 16 \times 9 \times 5 = 2^4 \cdot 3^2 \cdot 5^1$. La plus grande puissance de 3 divisant l'ordre est $3^2 = 9$. Un 3-Sylow est donc un groupe d'ordre 9.

(b) Pour avoir un élément d'ordre 9 dans $\mathfrak{S}_6$, il faudrait une permutation dont l'ordre (le ppcm des longueurs de ses cycles disjoints) soit 9. Les partitions de 6 sont : $6, 5+1, 4+2, 4+1+1, 3+3, 3+2+1$, etc. Les ppcm possibles sont : 6, 5, 4, 3. Aucun élément n'est d'ordre 9.

(c) Un groupe d'ordre p^2 (ici $3^2 = 9$) est toujours abélien. À isomorphisme près, c'est soit $\mathbb{Z}/9\mathbb{Z}$, soit $(\mathbb{Z}/3\mathbb{Z})^2$. Comme il n'y a pas d'élément d'ordre 9, ce n'est pas $\mathbb{Z}/9\mathbb{Z}$. C'est donc $(\mathbb{Z}/3\mathbb{Z})^2$.

2. Construction explicite

(a) $\sigma = (1\ 2\ 3)$ et $\tau = (4\ 5\ 6)$ sont des cycles à supports disjoints, donc ils commutent : $\sigma\tau = \tau\sigma$. L'ordre de σ est 3, l'ordre de τ est 3. Le groupe engendré $P = \langle \sigma, \tau \rangle$ est isomorphe à $\langle \sigma \rangle \times \langle \tau \rangle \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Il est d'ordre 9, c'est donc un 3-Sylow.

(b) Les 9 éléments sont :

— L'identité : e

— Supports disjoints purs (générés par σ ou τ) : $(1\ 2\ 3), (1\ 3\ 2), (4\ 5\ 6), (4\ 6\ 5)$. (4 éléments).

— Produits (générés par $\sigma\tau$) : $(1\ 2\ 3)(4\ 5\ 6), (1\ 2\ 3)(4\ 6\ 5), (1\ 3\ 2)(4\ 5\ 6), (1\ 3\ 2)(4\ 6\ 5)$. (4 éléments).

Il contient **4** éléments d'ordre 3 à support de taille 3 (les 3-cycles). Il contient **4** produits de deux 3-cycles disjoints.

3. Normalisateur et dénombrement

(a) Soit $g \in N_{\mathfrak{S}_6}(P)$. La conjugaison par g préserve la structure de cycles. Les 3-cycles de P sont ceux dont le support est E_1 ou E_2. Donc g doit envoyer l'ensemble des 3-cycles sur E_1 soit sur lui-même, soit sur l'ensemble des 3-cycles sur E_2. Cela implique $g(E_1) = E_1$ (et donc $g(E_2) = E_2$) OU $g(E_1) = E_2$ (et donc $g(E_2) = E_1$). La permutation $\gamma = (1\ 4)(2\ 5)(3\ 6)$ échange les supports et conjugue σ en τ, donc elle est dans le normalisateur.

(b)

— Si $g(E_1) = E_1$: g agit comme une permutation de E_1 et une permutation de E_2. N'importe quelle permutation de $\mathfrak{S}(E_1)$ normalise $\langle \sigma \rangle$ (car $\langle \sigma \rangle = \mathcal{A}_3 \triangleleft \mathfrak{S}_3$). Il y a $3! = 6$ choix pour E_1 et $3! = 6$ choix pour E_2. Soit $6 \times 6 = 36$ éléments.

— Si $g(E_1) = E_2$: Ces éléments sont de la forme $h \circ \gamma$ où h préserve les blocs. Il y en a autant, soit 36.

Total : $|N_{\mathfrak{S}_6}(P)| = 36 + 36 = 72$.

(c) Le nombre de Sylow est l'indice du normalisateur : $n_3 = \frac{|\mathfrak{S}_6|}{|N_{\mathfrak{S}_6}(P)|} = \frac{720}{72} = 10$.

(d) Théorèmes de Sylow : $n_3 \equiv 1 \pmod 3$. Ici $10 \equiv 1 \pmod 3$. n_3 divise $|G|/9 = 80$. 10 divise bien 80. C'est cohérent.

4. Lien avec $\mathcal{A}_6$

(a) P est engendré par des 3-cycles. Les 3-cycles sont des permutations paires (signature $(-1)^{3-1} = 1$). Donc $P \subset \mathcal{A}_6$.

(b) On cherche $n_3(\mathcal{A}_6)$. $N_{\mathcal{A}_6}(P) = N_{\mathfrak{S}_6}(P) \cap \mathcal{A}_6$. Le morphisme $N_{\mathfrak{S}_6}(P) \to \{-1, 1\}$ donné par la restriction de la signature est surjectif, donc $|N_{\mathcal{A}_6}(P)| = |N_{\mathfrak{S}_6}(P)| / 2 = 36$. Donc $n_3(\mathcal{A}_6) = \frac{|\mathcal{A}_6|}{36} = \frac{360}{36} = 10$.