Épreuve écrite de mathématiques générales

Les corps considérés dans le problème sont supposés commutatifs. Pour tout entier $n \geqslant 1$, on note $M_n(\mathbb{C})$ l'anneau des matrices carrées à n lignes et n colonnes à coefficients dans $\mathbb{C}$, $M_n(\mathbb{Z})$ le sous-anneau de $M_n(\mathbb{C})$ formé des matrices à coefficients dans $\mathbb{Z}$, et $C_n(\mathbb{Z})$ l'ensemble des vecteurs colonnes à n lignes à coefficients dans $\mathbb{Z}$.

Pour tout ensemble Z, on note $S(Z)$ le groupe des bijections de Z sur lui-même. Si X et Y sont deux ensembles, on note Y^X l'ensemble des applications de X dans Y.

I.

1) Soit A une matrice de $M_n(\mathbb{C})$.

1-a) Montrer que $A \in M_n(\mathbb{Z})$ si et seulement si, pour tout X dans $C_n(\mathbb{Z})$, on a $AX \in C_n(\mathbb{Z})$.

1-b) Soit A une matrice de $M_n(\mathbb{Z})$ dont le déterminant, noté $\det A$, est non nul et soit A^{-1} son inverse dans $M_n(\mathbb{C})$. Montrer que $A^{-1} \in M_n(\mathbb{Z})$ si et seulement si $|\det A| = 1$.

2) On munit $\mathbb{R}^n$ d'un produit scalaire noté $<,>$. Pour toute partie Y de $\mathbb{R}^n$, on note

$$Y^* = \left\{ x \in \mathbb{R}^n \;\middle|\; \forall y \in Y,\ < x, y > \in \mathbb{Z} \right\}.$$

Si $B = (v_i)_{1 \leqslant i \leqslant n}$ est une base de $\mathbb{R}^n$, on note

$$L_B = \left\{ \sum_{i=1}^{n} m_i v_i \;\middle|\; (m_1, \ldots, m_n) \in \mathbb{Z}^n \right\}$$

le sous-groupe additif de $(\mathbb{R}^n, +)$ engendré par B ; de plus, on note G_B la matrice de $<,>$ dans la base B, c'est-à-dire la matrice symétrique définie positive dont le (i,j)-ième coefficient vaut $< v_i, v_j >$.

2-a) Soit $x \in \mathbb{R}^n$. Montrer que $x \in L_B^*$ si et seulement s'il existe $X \in C_n(\mathbb{Z})$ tel que $G_B^{-1} X$ est le vecteur colonne formé des composantes de x dans la base B.

2-b) On suppose que $L_B \subset L_B^*$. Montrer que $G_B \in M_n(\mathbb{Z})$, et que $\det G_B = 1$ si et seulement si $L_B^* = L_B$.

3) On note $(e_i)_{1 \leqslant i \leqslant n}$ la base canonique de $\mathbb{R}^n$ et $(e_i^*)_{1 \leqslant i \leqslant n}$ sa base duale. Soit L un sous-groupe du groupe additif $(\mathbb{R}^n, +)$, tel que $2\mathbb{Z}^n \subset L \subset \mathbb{Z}^n$. Pour $1 \leqslant i \leqslant n$, on pose $L_i = L \cap F_i$, où F_i est le sous-espace vectoriel de $\mathbb{R}^n$ engendré par $\{e_i, \ldots, e_n\}$.

3-a) Montrer que, pour tout i, $1 \leqslant i \leqslant n$, il existe $a_i \in \{1, 2\}$, tel que $e_i^*(L_i) = a_i \mathbb{Z}$.

3-b) Pour $1 \leqslant i \leqslant n$, soit $u_i \in L_i$ tel que $e_i^*(u_i) = a_i$. Montrer que $(u_i)_{1 \leqslant i \leqslant n}$ engendre L et est une base de $\mathbb{R}^n$.

4) Soit C un $\mathbb{Z}/2\mathbb{Z}$-sous-espace vectoriel de $(\mathbb{Z}/2\mathbb{Z})^n$, et $L = \rho^{-1}(C)$, où ρ est l'application de $\mathbb{Z}^n$ sur $(\mathbb{Z}/2\mathbb{Z})^n$ définie par $\rho(m_1, \ldots, m_n) = (\tilde{m}_1, \ldots, \tilde{m}_n)$, $\tilde{m}$ étant la classe de m modulo 2.

Dans cette question, le produit scalaire $<,>$ est défini par $< x, y >= \dfrac{1}{2} \displaystyle\sum_{i=1}^{n} x_i y_i$, pour tout couple de vecteurs $x = (x_1 \ldots, x_n)$ et $y = (y_1, \ldots, y_n)$ de $\mathbb{R}^n$. De plus, on munit $(\mathbb{Z}/2\mathbb{Z})^n$ de

la forme bilinéaire non dégénérée, définie, pour tout couple de vecteurs $x = (x_1 \dots, x_n)$ et $y = (y_1, \dots, y_n)$ de $(\mathbb{Z}/2\mathbb{Z})^n$, par $x.y = \sum_{i=1}^{n} x_i y_i$.

4-a) Montrer qu'il existe une base B de $\mathbb{R}^n$ engendrant L, et que $L^* = \rho^{-1}(C^\perp)$, où $C^\perp$ est l'orthogonal de C relativement à la forme bilinéaire définie ci-dessus.

4-b) On suppose que $C \subset C^\perp$. Montrer que G_B est à coefficients entiers, et que $\det G_B = 1$ si et seulement si $C = C^\perp$.

II.

1) Soit K un corps, A un K-espace affine de dimension finie $r \geqslant 3$, et F le sous-espace vectoriel de K^A formé des fonctions affines $f : A \to K$.

1-a) Montrer que F est de dimension $r + 1$.

1-b) Soit $G_{aff}(A)$ le groupe affine de A, c'est-à-dire le groupe des applications affines bijectives de A dans lui-même. Montrer que $G_{aff}(A) = \{\sigma \in S(A) \mid \forall f \in F,\ f \circ \sigma \in F\}$.

2) On suppose ici que K est un corps fini et on note q son nombre d'éléments. Soit $\cdot$ la forme bilinéaire non dégénérée sur K^A définie, pour $f, g \in K^A$, par $f \cdot g = \sum_{x \in A} f(x)g(x)$. On note $F^\perp$ l'orthogonal de F relativement à cette forme bilinéaire.

2-a) Soit $f \in F$, non constante. Montrer que, pour tout $a \in K$, l'ensemble $f^{-1}(\{a\})$ a q^{r-1} éléments.

2-b) Montrer que $F \subset F^\perp$, et que $F = F^\perp$ si et seulement si $q = 2$ et $r = 3$.

3) Dans cette question, on suppose que $K = \mathbb{Z}/2\mathbb{Z}$ et que A est l'espace affine K^3, dont on numérote les points par $P_0 = (0, 0, 0)$, $P_1 = (1, 0, 0)$, $P_2 = (1, 1, 0)$, $P_3 = (0, 1, 1)$, $P_4 = (1, 0, 1)$, $P_5 = (0, 1, 0)$, $P_6 = (0, 0, 1)$ et $P_7 = (1, 1, 1)$.
Soit $\varphi : K^A \to K^8$ l'application linéaire bijective définie par $f \mapsto (f(P_0), f(P_1), \dots, f(P_7))$ et H le sous-espace vectoriel de K^8 égal à $\varphi(F)$.

3-a) Combien H possède-t-il d'éléments ayant exactement 4 composantes non nulles ?

3-b) Montrer qu'une base de H est

$$\{(1,1,1,1,1,1,1,1), (0,1,1,0,1,0,0,1), (0,0,1,1,0,1,0,1), (0,0,0,1,1,0,1,1)\}.$$

4) On utilise dans cette question les notations de la question I-4. On suppose que $n = 8$ et $C = H$.

4-a) Montrer que : $\inf\{< x, x > \mid x \in L - \{0\}\} = 2$.

4-b) Combien L possède-t-il d'éléments x tels que $< x, x >= 2$?

4-c) Déduire de ce qui précède

i) L'existence d'une matrice symétrique définie positive dans $M_8(\mathbb{Z})$, de déterminant 1 et dont les termes diagonaux sont pairs.

ii) L'existence d'une base B de l'espace euclidien usuel $\mathbb{R}^8$, possédant la propriété suivante : soit S l'ensemble des boules fermées de rayon 1 (pour la norme euclidienne) centrées en les points de L_B. Les éléments de S sont deux à deux d'intérieurs disjoints, et chaque élément de S est tangent[5] à 240 autres.

[5] deux boules fermées sont dites tangentes si la distance de leurs centres est égale à la somme de leurs rayons.

Dans la suite du problème, k désigne un corps de caractéristique différente de 2, $Q = \{x \in k \mid \exists y \in k - \{0\}, x = y^2\}$ l'ensemble de ses carrés non nuls, et $X = \mathbb{P}^1(k) = k \cup \{\infty\}$ la droite projective sur k. On rappelle que l'application $\alpha :\ \mathrm{GL}_2(k) \to S(X)$ qui à $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ associe l'homographie $\alpha(M) :\ x \mapsto \dfrac{ax+b}{cx+d}$ est un morphisme de groupes. On note $\mathrm{Ker}\,(\alpha)$ son noyau, c'est-à-dire $\alpha^{-1}(\{\mathrm{id_X}\})$.
On rappelle également que, si $c = 0$, on a $\alpha(M)(\infty) = \infty$, et que, si $c \neq 0$, $\alpha(M)(\infty) = \dfrac{a}{c}$ et $\alpha(M)\left(-\dfrac{d}{c}\right) = \infty$.
On note $\mathrm{SL}_2(k)$ le sous-groupe de $\mathrm{GL}_2(k)$ formé des matrices de déterminant 1 et $N = \mathrm{PSL}_2(k)$ l'image de $\mathrm{SL}_2(k)$ par α.

III. 1-a) Montrer que $\mathrm{SL}_2(k) \cap \mathrm{Ker}\,(\alpha) = \{-I_2,\, I_2\}$, où $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

1-b) Soit $M \in \mathrm{GL}_2(k)$; montrer que $\alpha(M) \in N$ si et seulement si $\det(M) \in Q$.

2) Si k est un corps fini à q éléments, calculer le nombre d'éléments de N en fonction de q.

3) Montrer que les homographies $x \mapsto h_i(x) = ix$ (pour $i \in Q$), $x \mapsto t_j(x) = x + j$ (pour $j \in k$) et $x \mapsto w(x) = -\dfrac{1}{x}$ appartiennent à N et l'engendrent.

4) Soit f un élément d'ordre 2 de N.

4-a) Montrer que f est conjugué dans N à une homographie de la forme $x \mapsto w_i(x) = -\dfrac{i}{x}$, avec $i \in Q$.

4-b) Montrer que si k a au moins cinq éléments, il existe un conjugué g de f dans N ne commutant pas avec f (on pourra calculer $t_a \circ w_i \circ t_a^{-1}$).

5) Soit A un $\mathbb{Z}/2\mathbb{Z}$-espace affine de direction $\overrightarrow{A}$ et $G_{aff}(A)$ son groupe affine.

5-a) Montrer que, si P est un sous-groupe de $G_{aff}(A)$ ne contenant pas de translation différente de l'application identique, alors P est isomorphe à un sous-groupe de $\mathrm{GL}\big(\overrightarrow{A}\big)$.

5-b) On suppose que k a au moins cinq éléments. Montrer que, si N est isomorphe à un sous-groupe de $G_{aff}(A)$, il est isomorphe à un sous-groupe de $\mathrm{GL}\big(\overrightarrow{A}\big)$.

IV. On note $\mathbf{1} :\ X \to \mathbb{Z}/2\mathbb{Z}$ la fonction constante égale à 1, $\mathbf{0} :\ X \to \mathbb{Z}/2\mathbb{Z}$ la fonction nulle, on note $-Q = \{-x \mid x \in Q\}$ et on suppose que k vérifie la propriété $(*)$ suivante :

$(*)$ *$k - \{0\}$ est l'union disjointe de Q et $-Q$.*

1) Montrer que, si k a q éléments, l'hypothèse $(*)$ est équivalente à $q \equiv -1 \mod 4$.

On note $u :\ X \to \mathbb{Z}/2\mathbb{Z}$ l'application qui vaut 1 si $x \in Q \cup \{\infty\}$ et 0 sinon. Pour tout élément $r \in k$, on pose $u_r = u \circ t_r$.

2-a) Montrer que, pour tout $i \in Q$ et $r \in k$, on a $u_r \circ h_i = u_{r/i}$.

2-b) Montrer que $u + u \circ w = \mathbf{1}$, puis que $u + u_{w(r)} + u_r \circ w = \begin{cases} \mathbf{1} & \text{si } r \in Q \\ \mathbf{0} & \text{si } r \in -Q \end{cases}$.

2-c) On suppose que k est un corps fini. Montrer que $\sum_{r\in k} u_r = \mathbf{1}$.

Soit R le sous-espace vectoriel de $(\mathbb{Z}/2\mathbb{Z})^X$ engendré par les fonctions u_r, $r \in k$. Montrer que

$$\mathrm{PSL}_2(k) \subset \big\{\sigma \in S(X) \;\big|\; \forall f \in R,\ f\circ\sigma \in R\big\}.$$

3) On suppose ici que $k = \mathbb{Z}/7\mathbb{Z}$. Soit $\psi :\ (\mathbb{Z}/2\mathbb{Z})^X \to (\mathbb{Z}/2\mathbb{Z})^8$ l'application linéaire bijective définie par

$$f \mapsto \Big(f\big(\overline{0}\big), f\big(\overline{1}\big), f\big(\overline{2}\big), f\big(\overline{3}\big), f\big(\overline{4}\big), f\big(\overline{5}\big), f\big(\overline{6}\big), f\big(\infty\big)\Big),$$

où, pour tout entier $x \in \mathbb{Z}$, $\overline{x}$ est la classe de x modulo 7.

3-a) Montrer que $\psi(R) = H$, où H est le sous-espace vectoriel de $(\mathbb{Z}/2\mathbb{Z})^8$ défini en II.3.

3-b) En déduire que $\mathrm{PSL}_2(\mathbb{Z}/7\mathbb{Z})$ est isomorphe à $\mathrm{GL}_3(\mathbb{Z}/2\mathbb{Z})$.

Corrigé

I.

1-a) Soit $\{E_1, \ldots, E_n\}$ la base canonique de $C_n(\mathbb{C})$. Les éléments de $C_n(\mathbb{Z})$ sont les combinaisons linéaires à coefficients dans $\mathbb{Z}$ des E_i. Par suite, dire que, pour tout $X \in C_n(\mathbb{Z})$, $AX \in C_n(\mathbb{Z})$ équivaut à dire que, pour $1 \leqslant i \leqslant n$, $AE_i \in C_n(\mathbb{Z})$. Comme les AE_i sont les vecteurs colonnes de A, ceci équivaut à $A \in M_n(\mathbb{Z})$.

1-b) Si $A \in M_n(\mathbb{Z})$, il en est de même de sa transposée. Donc, si $|\det A| = 1$, $A^{-1} \in M_n(\mathbb{Z})$. Réciproquement, si A et A^{-1} sont dans $M_n(\mathbb{Z})$, alors $\det A$ et $\det(A^{-1})$ sont dans $\mathbb{Z}$, et de produit 1, ce qui implique $|\det A| = 1$.

2-a) $x = \sum x_i v_i \in L_B^*$ si et seulement si, pour tout $v_j \in B$, on a $< x, v_j > \in \mathbb{Z}$, soit $\sum_i x_i < v_i, v_j > \in \mathbb{Z}$; si X est le vecteur colonne dont la j-ième composante est $\sum_i x_i < v_i, v_j >$, et si U est le vecteur colonne dont les composantes sont les x_i, ceci équivaut à dire que $X = G_B U$ est dans $C_n(\mathbb{Z})$, qui est la propriété demandée.

2-b) Soit $L_B \subset L_B^*$; pour tous (i, j), on a $< v_i, v_j > \in \mathbb{Z}$, i.e. $G_B \in M_n(\mathbb{Z})$. Comme G_B est la matrice d'une forme définie positive, son déterminant est positif. Donc, d'après successivement $1-b), 1-a)$ et $2-a)$, on a $\det G_B = 1 \Leftrightarrow G_B^{-1} \in M_n(\mathbb{Z}) \Leftrightarrow \forall X \in M_n(\mathbb{Z})$, $G_B^{-1} X \in \mathbb{C}_n(\mathbb{Z}) \Leftrightarrow L_B^* \subset L_B \Leftrightarrow L_B = L_B^*$.

3-a) Comme $L \subset \mathbb{Z}^n$, on a $e_i^*(L_i) \subset \mathbb{Z}$ pour $1 \leqslant i \leqslant n$. Comme e_i^* est un morphisme de groupe additif, $e_i^*(L_i)$ est un sous-groupe de $\mathbb{Z}$, et il existe $a_i \in \mathbb{N}$ tel que $e_i^*(L_i) = a_i\mathbb{Z}$. Or $2e_i$ est un élément de L_i, donc $2 = e_i^*(2e_i)$ est un multiple de a_i, qui vaut donc 1 ou 2.

3-b) Soit $v \in L = L_1$. Soit $x_1 \in \mathbb{Z}$ tel que $e_1^*(x) = x_1 a_1$, et posons $v_2 = v - x_1 u_1$. Comme $e_1^*(v_2) = 0$, v_2 est un élément de L_2. On définit ainsi une suite $(v_k)_{k=1,\ldots,n}$, où $v_k \in L_k$, $v_1 = v$, et où $v_{k+1} = v_k - x_k u_k$, avec $x_k = (e_k^*(v_k)/a_k)$. Comme $v_n = x_n u_n$, on a alors $v = \sum_{i=1}^{n} x_i u_i$.

L'espace vectoriel engendré par les (u_i) contient les vecteurs $2e_i$, et est donc égal à $\mathbb{R}^n$. 4-a) Comme $\rho^{-1}(\{0\}) = 2\mathbb{Z}^n$ et que $\rho^{-1}((\mathbb{Z}/2\mathbb{Z})^n) = \mathbb{Z}^n$, on a $2\mathbb{Z}^n \subset L \subset \mathbb{Z}^n$, et d'après $3-b)$ il existe une base de $\mathbb{R}^n$ engendrant L. Soit $y = (y_i) \in L^*$; comme, pour tout i, $2e_i \in L$, on a $y_i \in \mathbb{Z}$, et donc $L^* \subset \mathbb{Z}^n$. De plus, $y \in L^*$ si et seulement si, pour tout $x \in L$, $< x, y > \in \mathbb{Z}$, soit $\sum x_i y_i \in 2\mathbb{Z}$, soit $\rho(x).\rho(y) = 0$, soit $\rho(y) \in C^\perp$.

4-b) $C \subset C^\perp \Rightarrow L = \rho^{-1}(C) \subset \rho^{-1}(C^\perp) = L^*$. D'après $2-b)$, $\det G_B = 1$ si et seulement si $L = L^*$, i.e. $\rho^{-1}(C) = \rho^{-1}(C^\perp)$, soit, ρ étant surjective, $C = C^\perp$.

II.

Pour traiter les questions 1 et 2 de cette partie, on choisit un repère affine de A, et on note $(x_1, \ldots, x_r)$ les applications coordonnées d'un point $P \in A$ dans ce repère.

1-a) Toute fonction affine sur A s'écrit de façon unique $P \mapsto \sum a_i x_i(P) + c$, où les a_i et c sont des éléments de K. Une base de F est donc formée des $r+1$ fonctions $\{1, x_1, \ldots, x_r\}$, et F est de dimension $r+1$.

1-b) Si σ est affine, sa composée avec toute fonction affine est affine ; réciproquement, soit $\sigma \in K^A$, telle que, pour toute $f \in F$, $f \circ \sigma \in F$. Si l'on prend pour f les fonctions coordonnées x_i, ceci implique les fonctions coordonnées $x_i \circ \sigma$ sont des fonctions affines, ce qui équivaut au fait que σ est une application affine.

2-a) Soit $f : A \to K$ non constante ; elle est alors surjective, et la direction de $\operatorname{Ker} f$ est un hyperplan vectoriel H, qui a donc q^{r-1} éléments. Soit $a \in K$, et $P \in A$ tel que $f(P) = a$; comme $f^{-1}(\{a\}) = P + H$, on en déduit le résultat.

2-b) Soient $l, m \in F$. Comme $\dim A \geqslant 3$, il existe $\vec{v} \neq 0$ dans $\operatorname{Ker} \vec{l} \cap \operatorname{Ker} \vec{m}$. Soit $n \in F$ tel que $\vec{n}(\vec{v}) = 1$. Alors $\sum_{P \in A} (lmn)(P) = \sum_P (lmn)(P + \vec{v}) = \sum_P (lmn)(P) + \sum_P (lm)(P)$, d'où $\sum_P (lm)(P) = 0$, et $F \subset F^\perp$.

Puisque $F \subset F^\perp$, la condition $F = F^\perp$ équivaut à $2 \dim F = \dim K^A$, soit $q^r = 2(r+1)$. Comme $q \geqslant 2$ et $r \geqslant 3$, on a $2(r+1) \geqslant 2^r = (1+1)^r > 1 + r + r(r-1)/2$, soit $r(r-3) < 2$, et donc $r = 3$. Donc $q^3 = 8$, et $q = 2$.

3-a) Si $f = 0$ (resp. $f = 1$), $\varphi(f)$ est le vecteur nul (resp. le vecteur (11111111)). Sinon, f est non constante. D'après $2 - a$), $\operatorname{Card} f^{-1}(\{1\}) = 4$, et $\varphi(f)$ a donc exactement 4 composantes non nulles. Comme $\operatorname{Card} F = q^{r+1} = 16$, H a donc 14 vecteurs ayant exactement 4 composantes $\neq 0$.

3-b) Le système de vecteurs cité est l'image par φ de la base $\{1, x_1, x_2, x_3\}$ de F, et est donc une base de H.

4-a) et 4-b) Soit $x \in L$, non nul. Si $\rho(x) = (11111111)$, on a $< x, x > \geqslant 8/2 = 4$. Si $\rho(x) = 0$, l'un des x_i est pair et non nul, donc $< x, x > \geqslant 2^2/2 = 2$, et $< x, x > = 2$ si et seulement si il a une composante de valeur absolue 2 et les autres nulles, soit $2 \times 8 = 16$ vecteurs. Si $\rho(x)$ est l'un des 14 vecteurs de C ayant 4 composantes non nulles, on a $< x, x > \geqslant (4 \times 1^2)/2 = 2$, et $< x, x > = 2$ si et seulement si x_i pair implique $x_i = 0$, et $x_i \equiv 1 \mod 2$ implique $|x_i| = 1$, d'où $2^4 \times 14 = 224$ vecteurs. D'où au total $224 + 16 = 240$ vecteurs de L tels que $< x, x > = 2$.

4-c-i) D'après $II - 2 - b$), $C = C^\perp$, donc d'après $I - 4 - b$) il existe une base B de $\mathbb{R}^8$ engendrant L telle que la matrice G_B est définie positive, à coefficients entiers, de déterminant 1. Enfin, si $x = (x_1, \ldots, x_8) \in L$, le nombre de x_i impairs est $0, 4$ ou 8, donc $\sum x_i^2 \equiv 0 \mod 4$, et $< x, x >$ est pair pour tout $x \in L$.

4-c-ii) d'après ce qui précède, si $P \in L_B$, pour tout $Q \in L_B$ distinct de P, on a $d(P, Q) = ||P - Q|| \geqslant 2$, et il existe exactement 240 tels points Q tels que $d(P, Q) = 2$, ce qui équivaut à l'assertion de l'énoncé sur les sphères.

III.

1-a) Soit $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(k)$ telle que $M \in \operatorname{Ker}\alpha$, i.e. telle que $f = \alpha(M) = \mathrm{Id}_X$. Les égalités $f(\infty) = \infty, f(0) = 0$ et $f(1) = 1$ impliquent $c = 0, b = 0$ et $a+b = c+d$, soit $M = aI_2$, $a \in k^*$. Comme réciproquement toute matrice de cette forme appartient à $\operatorname{Ker}\alpha$, on en déduit que $\operatorname{Ker}\alpha = k^*I_2$. De plus, une matrice aI_2 est dans $\mathrm{SL}_2(k)$ si son déterminant vaut 1, i.e. $a^2 = 1$, d'où le résultat.

1-b) Soit $(M, M') \in \mathrm{GL}_2(k) \times \mathrm{SL}_2(k)$ vérifiant $\alpha(M) = \alpha(M')$. D'après ce qui précède, ceci équivaut à l'existence d'un $\lambda \in k^*$ tel que $M = \lambda M'$; s'il existe un tel λ, on a $\det M = \lambda^2$, et $\det M \in Q$. Réciproquement, si $\det M \in Q$, il existe $\lambda \in k^*$ tel que $\det M = \lambda^2$, et $M' = \dfrac{1}{\lambda}M$ est un élément de $\mathrm{SL}_2(k)$, cqfd.

2) Le cardinal n de $\mathrm{SL}_2(k)$ est égal à celui des quadruplets $\{a, b, c, d\} \in k^4$ tels que $ad - bc = 1$; le cas $a = 0$ donne $(q-1)q$ quadruplets ; si $a \neq 0$, chacun des q^2 couples $(b, c) \in k^2$ donne un quadruplet, d'où finalement $n = q(q-1) + (q-1)q^2 = q(q^2-1)$. D'après $1-a)$, N a donc $q(q^2-1)/2$ éléments.

3) On vérifie immédiatement que les h_i, t_i et w sont des éléments de N. Soit $f : x \mapsto \dfrac{ax+b}{cx+d} \in N$. Si $c = 0$, d est $\neq 0$, et $f = h_{a/d} \circ t_{b/a}$; comme $ad - bc = ad$ est un carré, il en est de même de $a/d = ad/d^2$, et f est dans le groupe engendré par les h_i, $i \in Q$, et les t_i. Si $c \neq 0$, on peut écrire $f(x) = \dfrac{a}{c} - \dfrac{ad-bc}{c(cx+d)}$. Donc $f = t_{a/c} \circ h_{(ad-bc)/c^2} \circ t_{d/c}$. Comme $ad - bc$ est un carré, il en est de même de $(ad-bc)/c^2$, d'où le résultat.

4-a) Comme $f \neq \mathrm{Id}_X$, il existe $a \neq b \in X$ tels que $f(a) = b$ (et donc $f(b) = a$). On peut supposer $a \in k$. Soit $h \in N$ définie par $h = t_{-a}$ si $b = \infty$ et par $h(x) = \dfrac{1}{a-b}\dfrac{x-a}{x-b}$ sinon. On a $h(a) = 0$ et $h(b) = \infty$, donc $g = h \circ f \circ h^{-1}$ est une involution conjuguée de f par un élément de N ; elle vérifie $g(\infty) = 0$, $g(0) = \infty$, et est donc de la forme $x \mapsto r/x$; comme $h \in N$, $-r \in Q$, cqfd.

4-b) f étant conjugué à un w_i, il suffit de montrer qu'il existe un conjugué de w_i dans N ne commutant pas avec w_i ; soit $a \in k$, $i \in Q$, et $s = t_a \circ w_i \circ t_a^{-1}$. On a $s \circ w_i(0) = a$ et $w_i \circ s(0) = \dfrac{-ia}{i+a^2}$, donc si s et w_i commutent, $a(a^2+2i) = 0$; comme k a au moins 4 éléments, il existe $a \in k$ tel que $t_a \circ w_i \circ t_a^{-1}$ ne commute pas avec w_i.

5-a) Si $\mu : G_{aff}(A) \to \mathrm{GL}(\vec{A})$ est l'homomorphisme de groupe qui associe à tout élément de $G_{aff}(A)$ son application linéaire associée, $\operatorname{Ker}\mu$ est le sous-groupe T des translations de A ; par suite, si $P \cap T = \{\mathrm{Id}_A\}$, la restriction de μ à P est injective, et P est isomorphe au sous-groupe $\mu(P)$ de $\mathrm{GL}(\vec{A})$.

5-b) Soit M un sous-groupe de $G_{aff}(A)$ isomorphe à N. Supposons qu'il existe $t \in M \cap T$, $t \neq \mathrm{Id}_A$. Cette translation est d'ordre 2 ; d'après $4-b)$, il existe $g \in M$ tel que gtg^{-1} ne commute pas avec t ; T étant commutatif et distingué dans $G_{aff}(A)$, gtg^{-1} est une translation, et commute avec t, d'où une contradiction. Par suite, d'après $5-a)$, M, et donc N, est isomorphe à un sous-groupe de $\mathrm{GL}(\vec{A})$.

IV.

1) Il est clair que $Q = -Q$ équivaut à $-1 \in Q$, i.e. à l'existence d'un élément d'ordre 4 dans k^*. Si k est fini d'ordre q, comme k^* est cyclique, ceci équivaut à $q - 1 = \operatorname{Card} k^* \equiv 0 \mod 4$, et donc $(*) \Leftrightarrow q \equiv 3 \mod 4$.

2-a) Notons $\overline{Q} = Q \cup \{+\infty\}$. Si $i \in Q$, on a $h_i(\overline{Q}) = \overline{Q}$. Donc $u = u \circ h_i$; comme $t_r \circ h_i = h_i \circ t_{r/i}$ pour tout $r \in k$, on a donc $u_r \circ h_i = u_{r/i}$.

2-b) On a $w(Q) = -Q = k^* - Q$, et $w(\infty) = 0$, donc $w(\overline{Q}) = X - \overline{Q}$, d'où $u + u \circ w = \mathbf{1}$.
Posons $v_r = u + u_{w(r)} + u_r \circ w$. On vérifie immédiatement que $v_r(0) = v_r(\infty) = u(r)$. Soit $x \in k^*$; posons $t = rx - 1$; alors $v_r(x) = u(x) + u(\frac{t}{r}) + u(\frac{t}{x})$. Si $rx \in Q$, $u(\frac{t}{r}) = u(\frac{t}{x})$, et $v_r(x) = u(x) = u(r)$. Si $rx \neq Q$, alors $t \neq 0$, et on a $u(\frac{t}{r}) \neq u(\frac{t}{x})$, d'où $v_r(x) = 1 + u(x) = u(r)$, d'où le résultat.

2-c) Soit $q = \operatorname{Card} k$, et $x \in X$; d'abord, on a $\sum u_r(\infty) = q = 1.$; ensuite, comme $r \mapsto x + r$ est une bijection de k sur lui-même, on a $\sum_{r \in k} u_r(x) = \sum_{r \in k} u(x + r) = \sum_{r \in k} u(r) = \operatorname{Card} Q \times 1.$
D'après 1), $\operatorname{Card} Q = (q-1)/2 \equiv 1 \mod 2$, et $\sum u_r = \mathbf{1}$.
Ceci prouve que $\mathbf{1} \in R$; donc, d'après $2 - b$, pour tout $r \in k = \{0\} \cup Q \cup -Q$, $u_r \circ w \in R$.
Comme, pour tout $i \in Q$, $u_r \circ h_i = u_{r/i} \in R$, et que, pour tout $i \in k$, $u_r \circ t_i = u_{r+i} \in R$, on en déduit que pour tout $g \in N$, $u_r \circ g \in R$, et donc que pour tout $f \in R$, $f \circ g \in R$.

3-a) Soit $V = \{v_1, \ldots, v_7\}$ l'image par ψ du système générateur de R égal à $\{\mathbf{1}, u, u_1, u_2, u_3, u_4, u_5\}$.
On a $V = \{(11111111), (01101001), (00110101), (00011011), (10001101), (01000111), (10100011)\}$.
Comme $v_5 = v_1 + v_2 + v_4, v_6 = v_2 + v_3 + v_4, v_7 = v_1 + v_2 + v_3$, on a bien $\psi(R) = H$.

3-b) Soit A comme dans $II - 3$, $\tau : A \to X$ la bijection définie par $\tau(P_7) = \infty$ et $\tau(P_i) = \overline{i}$ pour $0 \leqslant i \leqslant 6$, et $\lambda : S(X) \to S(A)$ l'isomorphisme de groupes défini par $g \mapsto \tau^{-1} g \tau$.
Si $N = \mathrm{PSL}_2(\mathbb{Z}/7\mathbb{Z})$, et si $\tilde{N} = \lambda(N)$, d'après $2 - c)$ et $II - 1 - b)$, $\tilde{N}$ est un sous-groupe de $G_{aff}(A)$, et donc, d'après $III - 5 - b)$, est isomorphe à un sous-groupe de $\mathrm{GL}_3(\mathbb{Z}/2\mathbb{Z})$.
D'après $III - 2$, $\operatorname{Card} N = 168$; il suffit donc pour terminer de montrer qu'il en est de même de $\mathrm{GL}_3(\mathbb{Z}/2\mathbb{Z})$, i.e. de l'ensemble des bases (x_1, x_2, x_3) de $(\mathbb{Z}/2\mathbb{Z})^3$. Or x_1 est l'un quelconque des 7 vecteurs non nuls de $E = (\mathbb{Z}/2\mathbb{Z})^3$, x_2 est l'un des $8 - 2 = 6$ vecteurs de E non colinéaire à x_1, et x_3 est l'un des $8 - 4 = 4$ vecteurs de E n'appartenant pas au plan $\{x_1, x_2\}$; le nombre de bases de $(\mathbb{Z}/2\mathbb{Z})^3$ est donc $7 \times 6 \times 4 = 168$.

Rapport des correcteurs

Le problème donnait deux applications de la théorie des codes correcteurs :

1) L'existence du réseau E_8 et de la matrice entière unimodulaire associée, (parties I et II), à partir du code de Hamming étendu de longueur 8,

2) L'isomorphisme entre les groupes simples $\mathrm{PSL}_2(\mathbf{F}_7)$ et $\mathrm{GL}_3(\mathbf{F}_2)$ (parties III et IV), déduit de l'isomorphisme entre le code de Hamming binaire de longueur 7 et le code binaire des résidus quadratiques modulo 7.

Le problème a été terminé (à une ou deux questions près) par quatre candidats.

Il n'y a eu que deux copies blanches. La plupart des candidats ont correctement traité les premières questions de la partie I, et une partie non négligeable des candidats admissibles a traité avec succès plusieurs questions des parties III et IV.

Néanmoins, la partie II a révélé de sérieuses lacunes en gómétrie affine : même la première question de la partie II a posé de sérieux problèmes. Dans la seconde question, de nombreux candidats ont affirmé que les éléments de F sont des bijections, et très peu ont correctement résolu la question.

Parmi les omissions les plus fréquentes, remarquons celles qui consistaient, dans la question $I-4-a$, à ne pas vérifier que $L^\perp \subset \mathbf{Z}^n$, ou encore, dans la question suivante, à ne pas évoquer la surjectivité de ρ.

La plupart des candidats n'a pas correctement traité la question $I-3-a$, n'ayant pas remarqué que $e_i^*(L_i)$ est un sous-groupe de $\mathbf{Z}$.

La question $II-3-b$ a en général été mal traitée, les candidats vérifiant l'indépendance des quatre vecteurs, mais oubliant de montrer leur appartenance à H.

Dans la question $III-1-a$, de nombreux candidats ont implicitement identifié un polynôme à la fonction polynomiale associée.

Les deux questions du problème ayant posé les plus de difficultés aux candidats ont été la question $II-2-b$ et surtout, et de loin, la question $III-4-a$.

Enfin, plusieurs candidats, ne tenant pas compte de la ponctuation, ont lu

"Montrer que $G_B \in M_n(\mathbf{Z})$ et que $\det G_B = 1$ si et seulement si $L_B^* = L_B$". En fait, pour la plupart, ils ont donné les bons arguments pour résoudre la question, et n'ont pas été pénalisés. Mais mieux vaut lire attentivement les questions !
