Mathématiques générales 2005 - Corrigé

Michel Coste

1er avril 2005

Partie I

1. (a) Si $A \in M_n(\mathbb{Z})$ alors pour tout $X \in C_n(\mathbb{Z})$ on a $AX \in C_n(\mathbb{Z})$. On obtient la réciproque en remarquant que la i-ème colonne de A est Ae_i, où e_i est le i-ème vecteur-colonne de la base canonique.

   (b) Si A^{-1} appartient à $M_n(\mathbb{Z})$, alors $\det(A)$ et $\det(A^{-1})$ sont tous les deux entiers et l'égalité $\det(A)\det(A^{-1}) = 1$ entraîne $|\det(A)| = 1$. Réciproquement si $|\det(A)| = 1$, alors A^{-1}, qui est la transposée de la matrice des cofacteurs de A divisée par $\det(A)$, est à coefficients entiers.

2. Il est bon de remarquer que $x \in L_B^*$ si et seulement si $\langle v_i, x\rangle \in \mathbb{Z}$ pour $i = 1, \dots, n$.

   (a) Soit Λ le vecteur colonne des coordonnées λ_j de x dans la base B. Alors $x \in L_B^*$ si et seulement si $\sum_{j=1}^n \langle v_i, v_j\rangle \lambda_j \in \mathbb{Z}$ pour $i = 1, \dots, n$, c.-à-d. si et seulement si $G_B\Lambda \in C_n(\mathbb{Z})$. Puisque G_B est inversible dans $M_n(\mathbb{C})$, ceci revient à dire qu'il existe $X \in C_n(\mathbb{Z})$ tel que $G_B^{-1}X$ soit le vecteur colonne des coordonnées de x dans la base B.

   (b) Avec les notations qui précèdent, $x \in L_B$ si et seulement si $\Lambda \in C_n(\mathbb{Z})$.
   D'après la question précédente, on a $L_B \subset L_B^*$ si et seulement si $G_B\Lambda \in C_n(\mathbb{Z})$ pour tout $\Lambda \in C_n(\mathbb{Z})$. Ceci équivaut à $G_B \in M_n(\mathbb{Z})$ d'après 1.(a).
   On a $L_B^* \subset L_B$ si et seulement si, d'après 2.(a), $G_B^{-1}X \in C_n(\mathbb{Z})$ pour tout $X \in C_n(\mathbb{Z})$. Ceci équivaut à $G_B^{-1} \in M_n(\mathbb{Z})$.
   On a donc $L_B = L_B^*$ si et seulement si $G_B \in M_n(\mathbb{Z})$ et $|\det(G_B)| = 1$, d'après 1.(b). Comme G_b est symétrique définie positive, son déterminant est strictement positif et $|\det(G_B)| = 1$ équivaut à $\det(G_B) = 1$.

3. Rappelons que $e_i^*(x)$ est la i-ème composante de x.

   (a) Puisque $2\mathbb{Z}^n \subset L \subset \mathbb{Z}^n$, $e_i^*(L_i)$ est un sous-groupe additif de $\mathbb{R}$ qui vérifie $2\mathbb{Z} \subset e_i^*(L_i) \subset \mathbb{Z}$. Donc $e_i^*(L_i)$ est $\mathbb{Z}$ ou $2\mathbb{Z}$.

   (b) Montrons par récurrence descendante sur k que $(u_i)_{k\le i\le n}$ engendre L_l et est une base de F_k. Pour $k = n$ c'est clair car e_k^* induit un isomorphisme de F_k sur $\mathbb{R}$. Supposons maintenant $1 \le k < n$ et que la propriété est vraie pour $k+1$.
   Si $x \in L_k$, il existe un entier m_k tel que $e_k^*(x) = m_k a_k$, et donc $x - m_k u_k \in L_{k+1}$. D'après l'hypothèse de récurrence, il existe des entiers $m_{k+1}, \dots, m_n$ tels que $x - m_k u_k = \sum_{i=k+1}^n m_i u_i$. Donc, $(u_i)_{k\le i\le n}$

engendre L_k. Comme $e_k^*(u_k) \neq 0$ et $e_k^*(u_i) = 0$ pour $k < i \leq n$, u_k n'est pas combinaison linéaire des $(u_i)_{k<i\leq n}$; avec l'hypothèse de récurrence ceci entraîne que la famille $(u_i)_{k\leq i\leq n}$ est libre, et donc une base de F_k qui est de dimension $n-k+1$.

4. Remarquons que L est un sous-groupe additif de $\mathbb{R}^n$ qui vérifie $2\mathbb{Z}^n \subset L \subset \mathbb{Z}^n$. Ceci entraîne que $L^* \subset \mathbb{Z}^n$; en effet, si e_i est le i-ème vecteur de la base canonique de $\mathbb{R}^n$, alors $2e_i \in L$ et $\langle x, 2e_i\rangle = x_i$.
   (a) La question 3.(b) nous fournit une base B de $\mathbb{R}^n$ engendrant L. On a déjà dit que $L^* \subset \mathbb{Z}^n$. Un élément $x \in \mathbb{Z}^n$ est dans L^* si et seulement si $\langle x, y\rangle \in \mathbb{Z}$ pour tout $y \in \rho^{-1}(C)$, c.-à-d. si et seulement si $\sum_{i=1}^n x_i y_i \in 2\mathbb{Z}$ pour tout $y = (y_1, \ldots, y_n)$ tel que $\rho(y) \in C$. Ceci équivaut à dire que $\rho(x) \cdot z = 0$ pour tout $z \in C$, ou encore que $\rho(x) \in C^\perp$. On a montré $L^* = \rho^{-1}(C^\perp)$.
   (b) Puisque $L = \rho^{-1}(C)$ et $L^* = \rho^{-1}(C^\perp)$ et que ρ est surjective, on a $C \subset C^\perp$ si et seulement si $L \subset L^*$, et $C = C^\perp$ si et seulement si $L = L^*$. L'application de 2.(b) à $L = L_B$ montre que G_B est à coefficients entiers si et seulement si $C \subset C^\perp$ et que dans ce cas $C = C^\perp$ si et seulement si $\det G_B = 1$.

Partie II

1. (a) Soit $\vec{A}$ l'espace vectoriel sous-jacent à A et notons $\vec{f}$ l'application linéaire $\vec{A} \to K$ définie par $\vec{f}(\overrightarrow{PQ}) = f(Q) - f(P)$. L'application $f \mapsto \vec{f}$ est une application linéaire surjective de F sur le dual de $\vec{A}$, qui est de dimension r. Le noyau de cette application est le sous-espace vectoriel des fonctions constantes de A dans K, qui est de dimension 1. Donc F est de dimension $r+1$.
   (b) La composée de deux fonctions affines est affine, donc si $\sigma \in G_{\text{aff}}(A)$ et $f \in F$, alors $f \circ \sigma \in F$.
   Réciproquement, soit $\sigma \in S(A)$ tel que $f \circ \sigma \in F$ pour tout $f \in F$. Fixons $P \in A$. Pour tout $f \in F$, l'application
$$\begin{array}{ccc} \vec{A} & \longrightarrow & K \\ \overrightarrow{PQ} & \longmapsto & \overrightarrow{(f\circ\sigma)}(\overrightarrow{PQ}) = \vec{f}(\overrightarrow{\sigma(P)\sigma(Q)}) \end{array}$$
   est linéaire. Comme les $\vec{f}$ parcourent tout le dual de $\vec{A}$ quand f parcourt F, ceci entraîne que l'application
$$\begin{array}{ccc} \vec{A} & \longrightarrow & \vec{A} \\ \overrightarrow{PQ} & \longmapsto & \overrightarrow{\sigma(P)\sigma(Q)} \end{array}$$
   est linéaire. Donc σ est affine. Comme par hypothèse σ est bijective, c'est un élément de $G_{\text{aff}}(A)$.

2. (a) Puisque $f : A \to K$ est affine non constante, elle est surjective. Donc $f^{-1}(\{a\})$ est non vide, et c'est un sous-espace affine de A dirigé par le noyau de la forme linéaire non nulle $\vec{f}$. Ce noyau est de dimension $r-1$ sur K et a donc q^{r-1} éléments. Par conséquent $f^{-1}(\{a\})$ a q^{r-1} éléments.

(b) Nous avons vu à la question précédente que si $f : A \to K$ est une fonction affine non constante, $f^{-1}(\{a\})$ est un sous-espace affine de A de dimension $r-1$. Bien sûr, si f est constante alors $f^{-1}(\{a\})$ est soit vide soit A tout entier. Donc, si f et g sont deux éléments de F et $(a,b) \in K^2$, alors l'ensemble $F(a,b) = f^{-1}(\{a\}) \cap g^{-1}(\{b\})$ est soit vide, soit un sous-espace affine de A de dimension au moins $r-2$. Si on note $|F(a,b)|$ son nombre d'éléments, on a donc $|F(a,b)| = 0$ ou q^k, avec $k \geq r-2$. Comme $r \geq 3$, $|F(a,b)|$ est toujours divisible par q. On en déduit que

$$f \cdot g = \sum_{x \in A} f(x)g(x) = \sum_{(a,b) \in K^2} |F(a,b)|ab = 0 \; .$$

Ceci montre que $F \subset F^\perp$.
L'espace vectoriel K^A est de dimension égale au nombre d'éléments de A, soit q^r. Comme F est de dimension $r+1$, son orthogonal $F^\perp$ est de dimension $q^r - r - 1$ (la forme bilinéaire est non dégénérée, dit l'énoncé). Vu que $F \subset F^\perp$, on a l'égalité $F = F^\perp$ si et seulement si $q^r = 2(r+1)$. Pour $q = 2$, on a $2^3 = 2(2+1)$ et $2^r > 2(r+1)$ dès que $r \geq 4$. Pour $q > 2$ et $r \geq 3$, on a $q^r > 2^r \geq 2(r+1)$. En conclusion, on a $F = F^\perp$ si et seulement si $q = 2$ et $r = 3$.

3. (a) D'après la question 2.(a), une fonction affine non constante de $(\mathbb{Z}/2\mathbb{Z})^3$ dans $\mathbb{Z}/2\mathbb{Z}$ prend quatre fois la valeur 0 et quatre fois la valeur 1. Le nombre d'éléments de H ayant exactement quatre composantes non nulles est donc le nombre de fonctions affines non constantes de $(\mathbb{Z}/2\mathbb{Z})^3$ dans $\mathbb{Z}/2\mathbb{Z}$, soit $2^4 - 2 = 14$.

(b) On remarque qu'une application $f : (\mathbb{Z}/2\mathbb{Z})^3 \to \mathbb{Z}/2\mathbb{Z}$ est linéaire si et seulement si $f^{-1}(0)$ est soit $(\mathbb{Z}/2\mathbb{Z})^3$ entier, soit un hyperplan vectoriel de celui-ci ; donc f est affine si et seulement si f est constante ou $f^{-1}(0)$ est un hyperplan affine de $(\mathbb{Z}/2\mathbb{Z})^3$. Ceci permet de vérifier facilement que les quatre éléments

$$(1,1,1,1,1,1,1,1),\ (0,1,1,0,1,0,0,1),\ (0,0,1,1,0,1,0,1),\ (0,0,0,1,1,0,1,1)$$

sont dans H. Comme ils sont visiblement linéairement indépendants (matrice échelonnée) et que H est de dimension 4, ils forment une base de H.

4. (a) Les éléments de H autres que $(0,0,0,0,0,0,0,0)$ et $(1,1,1,1,1,1,1,1)$ ont exactement quatre composantes égales à 1 et quatre composantes nulles. Donc un élément x de L a
– ou bien huit composantes paires,
– ou bien huit composantes impaires,
– ou bien quatre composantes impaires et quatre composantes paires.
Or le carré d'un nombre impair est congru à 1 modulo 4, et le carré d'un nombre pair congru à 0. Donc, la somme des carrés des composantes d'un élément de L est toujours divisible par quatre. Ainsi pour tout x dans $L \setminus \{0\}$, $\langle x, x\rangle$ est un entier strictement positif pair. Pour $x = (0,1,1,0,1,0,0,1)$, qui relève le deuxième élément de la base de H décrite ci-dessus, on a $\langle x, x\rangle = 2$. Donc

$$\inf\{\langle x, x\rangle \mid x \in L \setminus \{0\}\} = 2 \; .$$

(b) Un élément x de $\mathbb{Z}^8$ vérifie $\langle x, x\rangle = 2$ si et seulement si
- ou bien il a quatre composantes de valeur absolue 1 et quatre composantes nulles,
- ou bien il a une composante de valeur absolue 2 et toutes les autres nulles.

Chacun des quatorze éléments de H ayant exactement quatre composantes non nulles se relève en $2^4 = 16$ éléments du premier type (choisir quatre signes), et l'élément nul de H se relève en 16 éléments du second type. Donc L possède $(14 \times 16) + 16 = 240$ éléments x tels que $\langle x, x\rangle = 2$.

(c) On applique la question I-4 avec $C = H$. D'après le 2.(b), on a bien $H = H^\perp$. On choisit une base B de $\mathbb{R}^8$ engendrant L.

i. D'après I-4.(b), la matrice G_B est symétrique définie positive, à coefficients entiers, et $\det(G_B) = 1$. De plus, d'après l'argument du 4.(a), tous ses coefficients diagonaux sont pairs.

ii. D'après 4.(a), deux points distincts de L_B sont à une distance au moins égale à 2 (la distance est de la forme $2\sqrt{n}$, avec n entier strictement positif). Ceci montre que les éléments de S sont deux à deux d'intérieurs disjoints. D'après 4.(b), il y a dans $L_B \setminus \{0\}$ 240 éléments à la distance exactement 2 de l'origine. Ceci montre que chaque élément de S est tangent à 240 autres (on peut toujours se ramener à l'origine par translation d'un vecteur de L_B).

Partie III

1. (a) Les matrices I_2 et $-I_2$ sont clairement dans $\mathrm{SL}_2(k) \cap \ker(\alpha)$. Réciproquement, si $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est dans $\mathrm{SL}_2(k) \cap \ker(\alpha)$, alors $\alpha(M)(\infty) = \infty$ impose $c = 0$, $\alpha(M)(0) = 0$ impose $b = 0$, et en conséquence $\alpha(M)(1) = 1$ impose $a = d$. La condition $\det(M) = 1$ impose alors $a = d = \pm 1$.

   (b) Une petite variante du raisonnement précédent montre que $\ker(\alpha) = \{yI_2 \mid y \in k \setminus \{0\}\}$. Donc $\alpha(M) \in \mathrm{PSL}_2(k)$ si et seulement s'il existe $y \in k \setminus \{0\}$ tel que $y^{-1}M \in \mathrm{SL}_2(k)$, c.-à-d. si et seulement si $\det(M) \in Q$.

2. Le sous-groupe Q du groupe multiplicatif $k \setminus \{0\}$ est l'image de l'homomorphisme $y \mapsto y^2$ de ce groupe dans lui-même. Le noyau de cet homomorphisme est l'ensemble des solutions de $y^2 = 1$, soit $\{1, -1\}$ puisque k est de caractéristique $\neq 2$. Donc Q est un sous groupe de $k \setminus \{0\}$ d'indice 2. Comme $\det : \mathrm{GL}_2(k) \to k \setminus \{0\}$ est un homomorphisme surjectif et que $k \setminus \{0\}$ est d'ordre $q - 1$, le sous-groupe $\mathrm{SL}_2(k) = \ker(\det)$ est d'indice $q - 1$ dans $\mathrm{GL}_2(k)$. Or $\mathrm{GL}_2(k)$ est d'ordre $(q^2 - 1)(q^2 - q)$ (pour choisir une matrice inversible de $M_2(k)$, on choisit une première colonne non nulle puis une deuxième colonne non colinéaire à la première). Donc l'ordre de $\mathrm{SL}_2(k)$ est $q(q^2 - 1)$. Comme $\mathrm{PSL}_2(k) = \alpha(\mathrm{SL}_2(k))$ et que $\mathrm{SL}_2(k) \cap \ker(\alpha)$ est d'ordre 2, l'ordre de $\mathrm{PSL}_2(k)$ est $q(q^2 - 1)/2$.

3. Les homographies h_{y^2} (pour $y \in k \setminus \{0\}$), t_j et w sont les images par α de $\begin{pmatrix} y & 0 \\ 0 & y^{-1} \end{pmatrix}$, $\begin{pmatrix} 1 & j \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ respectivement, et ces matrices sont dans $\mathrm{SL}_2(k)$. Donc les h_{y^2}, t_j et w sont dans $\mathrm{PSL}_2(k)$. Il est connu que $\mathrm{SL}_2(k)$ est engendré par les transvections $\begin{pmatrix} 1 & j \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & 0 \\ \ell & 1 \end{pmatrix}$ pour $j, \ell \in k$. Donc $\mathrm{PSL}_2(k)$, qui est l'image homomorphe de $\mathrm{SL}_2(k)$, est engendré par les homographies $x \mapsto t_j(x) = x + j$ et $x \mapsto s_\ell(x) = x/(\ell x+1)$. Comme $s_\ell = w \circ t_{-\ell} \circ w$, on voit que $\mathrm{PSL}_2(k)$ est aussi engendré par les t_j et w. On peut remarquer que les h_{y^2} sont superflus.

4. (a) On a $f^2 = \mathrm{Id}$ et $f \neq \mathrm{Id}$. Donc il existe $a \in \mathbb{P}^1(k)$ tel que $f(a) = b \neq a$, et $f(b) = a$. Soit h une homographie qui envoie a sur 0 et b sur ∞, et qui est dans $\mathrm{PSL}_2(k)$. Si a et b sont dans k, on peut prendre $h : x \mapsto (a-b)(x-a)/(x-b)$. Si $a = \infty$, on peut prendre $h : x \mapsto -1/(x-b)$. Enfin, si $b = \infty$, on peut prendre $h : x \mapsto x - a$. On vérifie que ces homographies sont dans $\mathrm{PSL}_2(k)$ (en utilisant 1.(b) pour la première). Alors $h \circ f \circ h^{-1}$ est dans $\mathrm{PSL}_2(k)$ et envoie 0 sur ∞ et vice-versa. Il existe donc $c \in k \setminus \{0\}$ tel que $h \circ f \circ h^{-1}(x) = c/x$. D'après 1.(b), on a $c = -i$ avec $i \in Q$. Donc f est conjugué dans $\mathrm{PSL}_2(k)$ à $w_i : x \mapsto -i/x$ avec $i \in Q$.

   (b) Puisque f est conjugué à w_i, il suffit de trouver un conjugué de w_i qui ne commute pas avec w_i. Choisissons $a \in k$ telque $a^2 \neq -2i$ et $a \neq 0$; si k a au moins cinq éléments, on peut surement le faire. Alors $t_a \circ w_i \circ t_a^{-1} \circ w_i(\infty) = \dfrac{i}{a} + a$, tandis que $w_i \circ t_a \circ w_i \circ t_a^{-1}(\infty) = -\dfrac{i}{a}$. Avec le choix fait pour a, ceci montre que w_i ne commute pas avec son conjugué $t_a \circ w_i \circ t_a^{-1}$.

5. (a) L'homomorphisme $f \mapsto \vec{f}$ de $G_{\mathrm{aff}}(A)$ sur $\mathrm{GL}(\vec{A})$ a pour noyau le sous-groupe des translations. Puisque l'intersection de P avec ce noyau est réduite à l'identité, cet homomorphisme induit un isomorphisme de P sur son image, qui est un sous-groupe de $\mathrm{GL}(\vec{A})$.

   (b) Remarquons d'abord que puisque $\vec{A}$ est un $\mathbb{Z}/2\mathbb{Z}$-espace vectoriel, toute translation de A différente de l'identité est d'ordre 2. Soit P un sous-groupe de $G_{\mathrm{aff}}(A)$ isomorphe à $\mathrm{PSL}_2(k)$. Si P contenait une translation τ différente de l'identité, alors d'après 4.(b) il y aurait un conjugué de τ dans P qui ne commuterait pas avec τ. Or un conjugué d'une translation dans le groupe affine est une translation, et deux translations commutent. On aboutit ainsi à une contradiction. Donc P ne contient pas de translation autre que l'identité. D'après le (a), P et aussi $\mathrm{PSL}_2(k)$ est isomorphe à un sous-groupe de $\mathrm{GL}(\vec{A})$.

Partie IV

1. Puisque $-Q$ est la classe de -1 modulo le sous-groupe Q d'indice 2 de $k \setminus \{0\}$, ce dernier est l'union disjointe de Q et $-Q$ si et seulement si -1 n'est pas un carré dans k.
   Les $q-1$ éléments de $k \setminus \{0\}$ sont les racines de $X^{q-1} - 1$ dans k. Comme $X^4 - 1 = (X-1)(X+1)(X^2+1)$, -1 est un carré dans k si et seulement

si X^4-1 a quatre racines (forcément non nulles et distinctes) dans k, c.-à-d. si et seulement si X^4-1 divise $X^{q-1}-1$ dans $k[X]$. Ceci a lieu si et seulement si 4 divise $q-1$ (en effet le reste dans la division euclidienne est X^r-1, où r est le reste de la division de $q-1$ par 4), autrement dit si et seulement si $q \equiv 1 \bmod 4$. Comme q est impair, -1 n'est pas un carré dans k si et seulement si $q \equiv -1 \bmod 4$.

2. (a) On a $u_r \circ h_i(x) = u(ix+r) = u(i(x+(r/i))) = u(x+(r/i))$, où la dernière égalité est vérifiée parce que $i \in Q$ (ceci vaut aussi pour $x=\infty$). Donc $u_r \circ h_i = u_{r/i}$.

   (b) Remarquons que $x \in k \setminus \{0\}$ appartient à Q si et seulement si $w(x) = -1/x = (1/x)^2(-x)$ appartient à $-Q$. Par ailleurs w échange 0 et ∞. D'après l'hypothèse (*), on a donc $u(w(x)) = 1-u(x)$ pour tout $x \in \mathbb{P}^1(k)$, c.-à-d. $u + u \circ w = \mathbf{1}$.
   Remarquons que si x et y sont dans $k \setminus \{0\}$, alors $u(xy) = 1+u(x)+u(y)$ et $u(1/x) = u(x)$. Soient x et r dans $k \setminus \{0\}$. Alors

$$\begin{aligned}(u+u_{w(r)}+u_r \circ w)(x) &= u(x)+u(x-(1/r))+u((-1/x)+r) \\ &= u(x)+u((xr-1)/r)+u((xr-1)/x)\ .\end{aligned}$$

   Si $xr=1$, cette dernière quantité vaut $u(x)+0+0 = u(x) = u(r)$. Si $xr \neq 1$, elle vaut $u(x)+(1+u(xr-1)+u(r))+(1+u(xr-1)+u(x)) = u(r)$.
   Calculons

$$(u+u_{w(r)}+u_r \circ w)(0) = u(0)+u(-1/r)+u(\infty) = 0+(1+u(r))+1 = u(r)\ .$$

   Enfin, calculons

$$(u+u_{w(r)}+u_r \circ w)(\infty) = u(\infty)+u(\infty)+u(r) = u(r)\ .$$

   On a montré que $u+u_{w(r)}+u_r \circ w$ est la fonction constante égale à $u(r)$, soit $\mathbf{1}$ si $r \in Q$ et $\mathbf{0}$ si $r \in -Q$.

   (c) On suppose que k a q éléments, avec $(q-1)/2$ impair d'après l'hypothèse (*) et 1.
   Si $x \in k$, alors

$$\sum_{r \in k} u_r(x) = \sum_{r \in k} u(x+r) = \sum_{r \in k} u(r) = \sum_{r \in Q} 1 = 1\ ,$$

   la dernière égalité ayant lieu puisque Q a $(q-1)/2$ éléments, ce qui est un nombre impair. Par ailleurs $\sum_{r \in k} u_r(\infty) = \sum_{r \in k} 1 = 1$ puisque q est impair. Donc $\sum_{r \in k} u_r = \mathbf{1}$.
   La question III-3 nous donne une partie génératrice de $\mathrm{PSL}_2(k)$. Pour montrer que pour tout $\sigma \in \mathrm{PSL}_2(k)$ et tout $r \in k$, $u_r \circ \sigma$ est dans R, il suffit de le vérifier pour tout σ dans cette partie. Si σ est un t_s, c'est vrai parce que $u_r \circ t_s = u_{r+s}$. Si σ est un h_i, la vérification a été faite en 2.(a). Si σ est w, on a $u_r \circ w$ égal à $\mathbf{1}+u_0$ si $r=0$ (remarquez que $u_0 = u$), à $\mathbf{1}+u_0+u_{w(r)}$ si $r \in Q$ et à $u_0+u_{w(r)}$ si $r \notin Q$; on n'a fait ici que transcrire les résultats de 2.(b). Comme on a vu au début de cette question que $\mathbf{1} \in R$, on a bien $u_r \circ w \in R$ pour tout $r \in k$.

3. Remarquons déjà que $\mathbb{Z}/7\mathbb{Z}$ est un corps fini qui vérifie l'hypothèse (*). On utilise ici les notations de la question II-3. On notera (b_1, b_2, b_3, b_4) la base de H définie en II-3.(b). Soit $\theta : (\mathbb{Z}/2\mathbb{Z})^3 \to \mathbb{P}^1(\mathbb{Z}/7\mathbb{Z})$ la bijection définie par $\theta(P_i) = \bar{i}$ pour $i = 0, \ldots, 6$ et $\theta(P_7) = \infty$. Si f est une application de $\mathbb{P}^1(\mathbb{Z}/7\mathbb{Z})$ dans $\mathbb{Z}/2\mathbb{Z}$, alors $\psi(f) = \varphi(f \circ \theta)$. Rappelons que H est l'image par φ du $\mathbb{Z}/2\mathbb{Z}$-espace vectoriel des fonctions affines de $(\mathbb{Z}/2\mathbb{Z})^3$ dans $\mathbb{Z}/2\mathbb{Z}$.

   (a) Vérifions d'abord que $\psi(R) \subset H$. Ceci revient, d'après ce qui précède, à vérifier que pour tout $f \in R$, $f \circ \theta$ est une fonction affine de $(\mathbb{Z}/2\mathbb{Z})^3$ dans $\mathbb{Z}/2\mathbb{Z}$. Il suffit de le faire pour $f = u_{\bar{i}}$ avec $i = 0, \ldots 6$. Remarquons que $u_{\bar{i}} = u \circ t_{\bar{i}} = u \circ (t_{\bar{1}})^i$. Il suffit donc de vérifier que la fonction $u \circ \theta$ est affine, et que la bijection $\theta^{-1} \circ t_{\bar{1}} \circ \theta$ de $(\mathbb{Z}/2\mathbb{Z})^3$ dans lui-même est affine.
   Les éléments de Q sont ici $\bar{1}, \bar{2}, \bar{4}$. On voit alors immédiatement sur la définition des points $P_0, ..., P_7$ que $u \circ \theta$ est la forme linéaire première coordonnée. On remarque aussi que $\psi(u) = b_2$.
   La permutation $\theta^{-1} \circ t_{\bar{1}} \circ \theta$ est le cycle $(P_0, P_1, P_2, P_3, P_4, P_5, P_6)$. On vérifie sans difficulté que c'est la bijection affine donnée par

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} \longmapsto \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$$

   Pour montrer $\psi(R) = H$, il reste maintenant à voir que $b_i \in \psi(R)$ pour $i = 1, 2, 3, 4$. On a $b_1 = \psi(\mathbf{1}) \in \psi(R)$ d'après 2.(c) et on a vu que $b_2 = \psi(u)$. On remarque que b_3 et b_4 s'obtiennent à partir de b_2 en permutant cycliquement les sept premères coordonnées. Donc $b_3 = \psi(u \circ t_{\bar{1}}^{-1}) = \psi(u_{\bar{6}})$ et $b_4 = \psi(u \circ t_{\bar{2}}^{-1}) = \psi(u_{\bar{5}})$. On a bien montré $\psi(R) = H$.

   (b) On vient de vérifier que $f \mapsto f \circ \theta$ réalise un isomorphisme de R sur l'espace vectoriel des fonctions affines de $(\mathbb{Z}/2\mathbb{Z})^3$ dans $\mathbb{Z}/2\mathbb{Z}$. Considérons maintenant l'isomorphisme $\Gamma : \sigma \mapsto \theta^{-1} \circ \sigma \circ \theta$ de $S(\mathbb{P}^1(\mathbb{Z}/7\mathbb{Z}))$ sur $S((\mathbb{Z}/2\mathbb{Z})^3)$. D'après 2.(c), si $\sigma \in \mathrm{PSL}_2(\mathbb{Z}/7\mathbb{Z})$, alors $f \circ \sigma \in R$ pour tout $f \in R$. Ceci entraîne que pour toute fonction affine g de $(\mathbb{Z}/2\mathbb{Z})^3$ dans $\mathbb{Z}/2\mathbb{Z}$, on a $g \circ \Gamma(\sigma)$ affine, et donc $\Gamma(\sigma) \in G_{\mathrm{aff}}((\mathbb{Z}/2\mathbb{Z})^3)$ d'après II-1.(b). Ainsi Γ induit un isomorphisme de $\mathrm{PSL}_2(\mathbb{Z}/7\mathbb{Z})$ sur un sous-groupe de $G_{\mathrm{aff}}((\mathbb{Z}/2\mathbb{Z})^3)$. D'après III-5.(b), on en déduit que $\mathrm{PSL}_2(\mathbb{Z}/7\mathbb{Z})$ est isomorphe à un sous-groupe de $\mathrm{GL}_3(\mathbb{Z}/2\mathbb{Z})$. Le nombre d'éléments du premier groupe est

$$7 \times (7^2 - 1)/2 = 7 \times 24$$

   d'après III-2. Le nombre d'éléments du deuxième groupe est

$$(8 - 1) \times (8 - 2) \times (8 - 4) = 7 \times 24$$

   (choisir un premier vecteur colonne non nul, puis un deuxième qui n'est pas dans la droite engendrée par le premier, puis un troisième qui n'est pas dans le plan engendré par les deux premiers). Les deux groupes sont donc isomorphes.