Groupe linéaire, simplicité : correction

Exercice 1. Une matrice $M \in M_n(\mathbf{F}_q)$ est inversible si et seulement si les vecteurs colonnes forment une base. Il suffit pour cela que le premier vecteur soit non nul, que le deuxième ne soit pas colinéaire au premier, que le troisième n'appartienne pas au plan engendré par les deux premiers, etc. On obtient donc

$$|\mathrm{GL}_n(\mathbf{F}_q)| = (q^n-1)(q^n-q)\cdots(q^n-q^{n-1}) = q^{n(n-1)/2}(q^n-1)(q^{n-1}-1)\cdots(q-1).$$

$\mathrm{SL}_n(\mathbf{F}_q)$ est le noyau du morphisme surjectif $\mathrm{GL}_n(\mathbf{F}_q) \to \mathbf{F}_q^\times$. Puisque $|\mathbf{F}_q^\times| = q-1$, on a

$$|\mathrm{SL}_n(\mathbf{F}_q)| = \frac{|\mathrm{GL}_n(\mathbf{F}_q)|}{q-1} = q^{n(n-1)/2}(q^n-1)(q^{n-1}-1)\cdots(q^2-1).$$

$\mathrm{PGL}_n(\mathbf{F}_q)$ est le quotient de $\mathrm{GL}_n(\mathbf{F}_q)$ par son centre. D'après le cours, celui-ci est constitué des matrices scalaires $\lambda \mathrm{I}_n$ ($\lambda \in \mathbf{F}_q^\times$), qui forment un ensemble de cardinal $q-1$. On obtient donc le même cardinal

$$|\mathrm{PGL}_n(\mathbf{F}_q)| = \frac{|\mathrm{GL}_n(\mathbf{F}_q)|}{q-1} = q^{n(n-1)/2}(q^n-1)(q^{n-1}-1)\cdots(q^2-1).$$

Il est également vrai que les matrices de $\mathrm{SL}_n(\mathbf{F}_q)$ sont centrales si et seulement si elles sont scalaires (une matrice dans le centre de $\mathrm{SL}_n(\mathbf{F}_q)$ doit commuter avec toutes les matrices de transvection $1+e_{i,j}$ ($i \neq j$), ce qui revient à commuter avec les matrices $e_{i,j}$; le calcul montre alors que la matrice est scalaire). Les matrices scalaires de $\mathrm{SL}_n(\mathbf{F}_q)$ sont les $\lambda \mathrm{I}_n$, avec λ racine n-ième de l'unité.
Remarque importante. Outre le fait que cette remarque va nous permettre de dénombrer $\mathrm{PSL}_n(\mathbf{F}_q)$, il convient de noter que le fait que $\mathrm{Z}(\mathrm{SL}_n(\mathbf{F}_q)) = \mathrm{SL}_n(\mathbf{F}_q) \cap \mathrm{Z}(\mathrm{GL}_n(\mathbf{F}_q))$ entraîne que $\mathrm{PSL}_n(\mathbf{F}_q)$ est naturellement un sous-groupe (distingué) de $\mathrm{PGL}_n(\mathbf{F}_q)$.
Il s'agit donc maintenant de dénombrer l'ensemble $\mu_n(\mathbf{F}_q)$ des racines n-ièmes de l'unité dans $\mathbf{F}_q$. Nous allons montrer que son cardinal est $d = \mathrm{pgcd}(n, q-1)$ (c'est en fait un résultat général : il y a $\mathrm{pgcd}(r,s)$ éléments d'ordre divisant r dans un groupe cyclique d'ordre s).
En effet, soit u et v tels que $d = u(q-1)+vn$. Si $x \in \mu_n(\mathbf{F}_q)$, alors $x^n = 1$, et donc $x^d = (x^n)^v (x^{q-1})^u = 1$. Inversement, si $x^d = 1$, alors $x^n = 1$. Donc on a égalité entre $\mu_n(\mathbf{F}_q)$ et $\mu_d(\mathbf{F}_q)$. Mais le polynôme $\mathrm{X}^{q-1}-1$ est déjà scindé et à racines simples sur $\mathbf{F}_q$, donc on peut en dire autant de X^d-1 qui en est un diviseur. Bref, $|\mu_n(\mathbf{F}_q)| = |\mu_d(\mathbf{F}_q)| = d$.
On a donc

$$|\mathrm{PSL}_n(\mathbf{F}_q)| = \left|\frac{\mathrm{PSL}_n(\mathbf{F}_q)}{\mathrm{Z}(\mathrm{PSL}_n(\mathbf{F}_q))}\right| = \frac{|\mathrm{SL}_n(\mathbf{F}_q)|}{\mathrm{pgcd}(q-1,n)} = q^{n(n-1)/2}\frac{(q^n-1)(q^{n-1}-1)\cdots(q^2-1)}{\mathrm{pgcd}(q-1,n)}.$$

Exercice 2. Soit G un sous-groupe distingué de $\mathrm{SL}_n(\mathrm{K})$, distinct de $\mathrm{SL}_n(\mathrm{K})$. On peut considérer l'application canonique $\varphi : \mathrm{SL}_n(\mathrm{K}) \longrightarrow \mathrm{PSL}_n(\mathrm{K})$ qui est surjective, donc $\varphi(\mathrm{G})$ est distingué dans $\mathrm{PSL}_n(\mathrm{K})$. Puisque $\mathrm{PSL}_n(\mathrm{K})$ est simple, c'est donc que $\varphi(\mathrm{G})$ est trivial ou est $\mathrm{PSL}_n(\mathrm{K})$ tout entier. Montrons que ce dernier cas ne peut pas se produire. Si $\varphi(\mathrm{G}) = \mathrm{PSL}_n(\mathrm{K})$, alors G contient un antécédent de $\left[\begin{pmatrix} 1 & 0 & & 0 \\ & \ddots & 0 & 0 \\ & & 1 & 1 \\ & & & 1 \end{pmatrix}\right]$, qui est nécessairement de la forme $\lambda \begin{pmatrix} 1 & 0 & & 0 \\ & \ddots & 0 & 0 \\ & & 1 & 1 \\ & & & 1 \end{pmatrix}$ avec $\lambda \in \mu_n(\mathrm{K})$.

Élevons alors cette matrice à la puissance $d = \text{pgcd}(n, q-1)$, ce qui donne $\begin{pmatrix} 1 & 0 & & 0 \\ & \ddots & 0 & 0 \\ & & 1 & d \\ & & & 1 \end{pmatrix}$. Ce dernier élément est une transvection (car $d \neq 0$ dans K), et puisque toutes les transvections sont conjuguées dans $\text{SL}_n(\text{K})$ et que G est distingué, c'est que G contient toutes les transvections. Or, les transvections engendrent $\text{SL}_n(\text{K})$, donc $\text{G} = \text{SL}_n(\text{K})$. Ainsi, $\varphi(\text{G})$ est réduit à l'élément neutre, et donc G est inclus dans le centre de $\text{SL}_n(\text{K})$, et donc de la forme $\{\lambda \text{I}_n, \lambda \in \text{T}\}$, où T est un sous-groupe de racines de l'unité de $\text{K}^\times$. Or, on sait que pour un corps fini, $\text{K}^\times$ est cyclique, de même que tous ses sous-groupes.

Exercice 3.

1. L'action de $\text{GL}_2(\text{K})$ sur K^2 est linéaire, donc elle envoie droite vectorielle sur droite vectorielle : on a donc bien une action de $\text{GL}_2(\text{K})$ sur $\mathscr{D}(\text{K})$.

   Le noyau de cette action est le sous-groupe des éléments de $\text{GL}_2(\text{K})$ stabilisant toute droite. Il s'agit donc des homothéties, à cause du résultat classique suivant.

   Lemme. Soit $\varphi \in \text{GL}_2(\text{K})$ envoyant tout vecteur x sur un vecteur colinéaire. Alors φ est une homothétie.

   Preuve. En utilisant l'hypothèse sur les deux vecteurs de la base canonique, on obtient l'existence de scalaires non nuls λ, μ tels que $\varphi(e_1) = \lambda e_1$ et $\varphi(e_2) = \mu e_2$, c'est-à-dire tels que la matrice de φ dans la base canonique soit $\text{diag}(\lambda, \mu)$.

   On applique alors le résultat à $e_1 + e_2$: il existe un scalaire $\nu \neq 0$ tel que $\varphi(e_1+e_2) = \nu(e_1+e_2)$. On a donc

   $$\nu e_1 + \nu e_2 = \varphi(e_1+e_2) = \varphi(e_1) + \varphi(e_2) = \lambda e_1 + \mu e_2,$$

   ce qui entraîne $\lambda = \mu = \nu$, et φ est une homothétie.

   Par passage au quotient on obtient donc bien une action fidèle de $\text{PGL}_2(\text{K})$ sur $\mathscr{D}(\text{K})$.

2. Pour obtenir l'expression donnée dans l'énoncé, il suffit maintenant de regarder l'action d'une matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{GL}_2(\text{K})$ sur les droites D_x.

   Si $x \in \text{K}$, $\text{D}_x = \text{Vect}\begin{pmatrix} x \\ 1 \end{pmatrix}$. On a donc

   $$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \text{D}_x = \text{Vect}\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} x \\ 1 \end{pmatrix} = \text{Vect}\begin{pmatrix} ax+b \\ cx+d \end{pmatrix} = \begin{cases} \text{Vect}\begin{pmatrix} \frac{ax+b}{cx+d} \\ 1 \end{pmatrix} = \text{D}_{\frac{ax+b}{cx+d}} & \text{si } cx+d \neq 0\,; \\ \text{Vect}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \text{D}_\infty & \text{si } cx+d = 0. \end{cases}$$

   De même,

   $$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \text{D}_\infty = \text{Vect}\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \text{Vect}\begin{pmatrix} a \\ c \end{pmatrix} = \begin{cases} \text{Vect}\begin{pmatrix} a/c \\ 1 \end{pmatrix} = \text{D}_{a/c} & \text{si } c \neq 0\,; \\ \text{Vect}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \text{D}_\infty & \text{si } c = 0. \end{cases}$$

   Cela donne bien l'expression voulue pour l'action de $\text{PGL}_2(\text{K})$ sur $\text{K} \sqcup \{\infty\}$.

   Remarque. On pourrait définir l'action par cette formule (et c'est ce que l'on fait parfois), mais il y a alors un certain nombre de choses (faciles mais impliquant des disjonctions de

cas un peu pénibles) à vérifier pour être sûr que l'on obtient bien une action. Il est plus satisfaisant de voir dans ces formules l'expression en coordonnées d'une action naturelle.

3. On va utiliser une méthode assez naturelle pour montrer la 3-transitivité : on se fixe trois éléments privilégiés, disons ∞, 0 et 1 dans $\mathrm{K}\sqcup\{\infty\}$.

   La transitivité de l'action revient à l'existence, pour tout $p\in\mathrm{K}\sqcup\{\infty\}$, d'un élément g tel que $g\cdot p=\infty$ (si p et q sont des points quelconques, que $g\cdot p=\infty$ et que $h\cdot q=\infty$, l'élément $h^{-1}g$ envoie bien p sur q).

   Maintenant, la 2-transitivité est équivalente à la conjonction de deux propriétés :
   – Étant donné $p\in\mathrm{K}\sqcup\{\infty\}$, il existe un élément $g\in\mathrm{PGL}_2(\mathrm{K})$ envoyant p sur ∞ ;
   – Étant donné $q\neq\infty$, il existe un élément $h\in\mathrm{Stab}(\infty)$ envoyant q sur 0.

   En effet, ces deux propriétés sont clairement plus faibles que la 2-transitivité de l'action, mais, ensemble, elles l'impliquent : si (p,q) est une paire de points distincts, que g envoie p sur ∞ et que h envoie $g\cdot p$ sur 0 tout en fixant ∞, la composition hg envoie bien (p,q) sur $(\infty,0)$.

   Ainsi, pour démontrer la 3-transitivité de l'action, on va démontrer :
   – Étant donné $p\in\mathrm{K}\sqcup\{\infty\}$, il existe un élément $g\in\mathrm{PGL}_2(\mathrm{K})$ envoyant p sur ∞ ;
   – Étant donné $q\neq\infty$, il existe un élément $h\in\mathrm{Stab}(\infty)$ envoyant q sur 0.
   – Étant donné $r\notin\{\infty,0\}$, il existe un élément $k\in\mathrm{Stab}(\infty,0)=\mathrm{Stab}(\infty)\cap\mathrm{Stab}(0)$ envoyant r sur 1.

   Faisons-le :
   – Soit $p\in\mathrm{K}\sqcup\{\infty\}$. Si $p=\infty$, il n'y a rien à faire. Sinon, $p\in\mathrm{K}$ et l'homographie $x\mapsto\dfrac{1}{x-p}$ correspondant à la classe $\begin{bmatrix}0&1\\1&-p\end{bmatrix}$ envoie p sur ∞.
   – Le stabilisateur de ∞ est l'ensemble des homographies $x\mapsto\dfrac{ax+b}{cx+d}$ pour lesquelles $c=0$. Il s'agit donc du groupe affine
   $$\mathrm{Stab}(\infty)=\{x\mapsto \mathrm{A}x+\mathrm{B}\,|\,\mathrm{A}\neq 0\}.$$
   En particulier, la translation $x\mapsto x-q$ fixe ∞ et envoie $x\in\mathrm{K}$ quelconque sur 0.
   – Le stabilisateur de ∞ et de 0 est l'ensemble des transformations affines du type précédent fixant 0. Il s'agit donc des homothéties $x\mapsto \mathrm{A}x$, $\mathrm{A}\neq 0$. En particulier, la transformation $x\mapsto r^{-1}x$ envoie $r\notin\{\infty,0\}$ sur 1 (et c'est la seule).

   On a donc montré la 3-transitivité. En outre, on voit que seule l'identité fixe à la fois ∞, 0 et 1 ; cela montre l'*exacte* 3-transitivité : si g et h sont deux éléments envoyant p_1,p_2,p_3 sur p_1',p_2',p_3' et que k envoie p_1,p_2,p_3 sur $\infty,0,1$, l'élément $g^{-1}h$ fixe les p_i, donc l'élément $k(g^{-1}h)k^{-1}$ fixe ∞, 0 et 1. Il s'ensuit $kg^{-1}hk^{-1}=1$, donc $g=h$.

   Remarque. En explicitant la preuve que l'on vient de donner, on voit que l'unique homographie envoyant $p,q,r\in\mathrm{K}$ sur $\infty,0,1$ est
   $$x\mapsto\frac{r-p}{r-q}\Big/\frac{x-p}{x-q},$$
   mais l'intérêt de notre preuve « par étapes » est de limiter au minimum les calculs (en outre, cette expression n'a un sens que si $p,q,r\in\mathrm{K}$, le cas où l'un des trois vaut ∞ devant être traité à la main).

4. Si $\mathrm{K}=\mathbf{F}_2$, le fait que $\mathbf{F}_2^\times$ soit le groupe trivial rend les égalités $\mathrm{GL}_2(\mathbf{F}_2)=\mathrm{SL}_2(\mathbf{F}_2)=\mathrm{PGL}_2(\mathbf{F}_2)=\mathrm{PSL}_2(\mathbf{F}_2)$ évidentes. D'après ce qui précède, ce groupe agit fidèlement et exactement 3-transitivement sur $\mathbf{F}_2\sqcup\{\infty\}$, qui a 3 éléments. Cela entraîne que le morphisme $\mathrm{PGL}_2(\mathbf{F}_2)\to\mathfrak{S}(3)$ défini par l'action est un isomorphisme (il est injectif par fidélité et surjectif par 3-transitivité).

Si $\mathrm{K} = \mathbf{F}_3$, la question précédente montre que $\mathrm{PGL}_2(\mathbf{F}_3)$ agit 3-transitivement sur $\mathbf{F}_3 \sqcup \{\infty\}$, qui a quatre éléments. L'action est alors nécessairement 4-transitive : si (p,q,r,s) et (p',q',r',s') sont des quadruplets d'éléments distincts, l'élément envoyant (p,q,r) sur (p',q',r') envoie nécessairement l'unique élément restant, r, sur l'unique élément restant, r', ce qui montre la 4-transitivité (plus généralement, une action n-transitive sur un ensemble à $n+1$ éléments est automatiquement $(n+1)$-transitive). Pour la même raison que précédemment, on obtient un isomorphisme $\mathrm{PGL}_2(\mathbf{F}_3) \to \mathfrak{S}(4)$.

Puisqu'il y a 2 racines carrées de l'unité dans $\mathbf{F}_3$, $\mathrm{PSL}_2(\mathbf{F}_3)$ a 12 éléments. C'est donc un sous-groupe d'indice 2 de $\mathrm{PGL}_2(\mathbf{F}_3) \simeq \mathfrak{S}(4)$, ce qui entraîne $\mathrm{PSL}_2(\mathbf{F}_3) \simeq \mathfrak{A}(4)$.

Remarque. On a vu en cours que $\mathrm{PSL}_2(\mathbf{F}_2) \simeq \mathfrak{S}(3)$ et $\mathrm{PSL}_2(\mathbf{F}_3) \simeq \mathfrak{A}(4)$ sont les seuls $\mathrm{PSL}_n(\mathrm{K})$ qui ne soient pas simples.

Si $\mathrm{K} = \mathbf{F}_4$, $\mathrm{PGL}_2(\mathbf{F}_4)$ (et donc $\mathrm{PSL}_2(\mathbf{F}_4)$) agit fidèlement sur l'ensemble $\mathbf{F}_4 \sqcup \{\infty\}$, qui a 5 éléments. On obtient donc un morphisme

$$\varphi : \mathrm{PSL}_2(\mathbf{F}_4) \to \mathfrak{S}(5).$$

Si $\varepsilon : \mathfrak{S}(5) \to \{\pm 1\}$ est le morphisme signature, la simplicité de $\mathrm{PSL}_2(\mathbf{F}_4)$ entraîne que $\varepsilon \circ \varphi : \mathrm{PSL}_2(\mathbf{F}_4) \to \{\pm 1\}$ soit un morphisme trivial (par simplicité, son noyau est $\{1\}$ – ce qui est exclu car il est hors de question que $\mathrm{PSL}_2(\mathbf{F}_4)$ s'injecte dans un groupe d'ordre 2 ou $\mathrm{PSL}_2(\mathbf{F}_4)$ lui-même).

Le morphisme φ induit donc un morphisme

$$\varphi : \mathrm{PSL}_2(\mathbf{F}_4) \to \mathfrak{A}(5).$$

La fidélité de l'action montre en outre que ce morphisme est injectif. Comme les deux groupes en présence ont 60 éléments, c'est un isomorphisme.

Remarque. Signalons d'autres isomorphismes exceptionnels, plus délicats à démontrer.

$$\begin{aligned} \mathrm{PSL}_2(\mathbf{F}_4) \simeq \mathrm{PSL}_2(\mathbf{F}_5) \simeq \mathfrak{A}(5), \qquad & \mathrm{PGL}_2(\mathbf{F}_5) \simeq \mathfrak{S}(5) \\ \mathrm{PSL}_2(\mathbf{F}_7) \simeq \mathrm{PSL}_3(\mathbf{F}_3) = \mathrm{GL}_3(\mathbf{F}_2) \qquad & \mathrm{PSL}_2(\mathbf{F}_9) \simeq \mathfrak{A}(6) \\ \mathrm{GL}_4(\mathbf{F}_2) = \mathrm{PSL}_4(\mathbf{F}_2) \simeq \mathfrak{A}(8). & \end{aligned}$$

5. Attention ! L'énoncé distribué en TD ne mentionnait pas l'hypothèse K **fini.**
   On a déjà montré (à la question 3) que $\mathrm{Stab}(0,\infty) = \{x \mapsto \lambda x \,\big|\, \lambda \in \mathrm{K}^\times\}$.
   D'après ce que l'on a démontré à la question 3, le sous-groupe $\langle x \mapsto x+1, x \mapsto 1/x\rangle$, qui contient toutes les transformations du type $x \mapsto \frac{1}{x-p}$ et du type $x \mapsto x-q$ (c'est là qu'on utilise l'hypothèse de finitude de K), agit 2-transitivement sur $\mathrm{K} \sqcup \{\infty\}$.
   En particulier, si $g \in \mathrm{PGL}_2(\mathrm{K})$, on peut trouver $h \in \langle x \mapsto x+1, x \mapsto 1/x\rangle$ tel que $h \cdot 0 = g \cdot 0$ et $h \cdot \infty = g \cdot \infty$.
   L'élément $g^{-1}h = k$ appartient donc à $\mathrm{Stab}(0,\infty)$. Cela entraîne que k est de la forme $x \mapsto \lambda x$, et donc que $g \in \langle x \mapsto x+1, x \mapsto 1/x, x \mapsto \lambda x\rangle$.
6. Essentiellement le seul problème à régler pour adapter cette méthode de preuve à $\mathrm{PSL}_2(\mathrm{K})$ est que l'homographie $x \mapsto 1/x$ n'appartient pas nécessairement à $\mathrm{PSL}_2(\mathrm{K})$ (en fait, $x \mapsto 1/x \in \mathrm{PSL}_2(\mathrm{K})$ si et seulement si -1 est un carré dans K). Mais $x \mapsto -1/x$, correspondant à la matrice $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ peut jouer le même rôle : on voit que $\langle x \mapsto -1/x, x \mapsto x+1\rangle$ agit 2-transitivement sur $\mathrm{K} \sqcup \{\infty\}$, et que

$$\mathrm{Stab}_{\mathrm{PSL}_2(\mathrm{K})}(0,\infty) = \mathrm{Stab}_{\mathrm{PGL}_2(\mathrm{K})}(0,\infty) \cap \mathrm{PSL}_2(\mathrm{K}) = \{x \mapsto \lambda x \,|\, \lambda \text{ est un carré dans K}\}.$$

   On obtient donc un système de générateurs pour $\mathrm{PSL}_2(\mathrm{K})$ constitué de l'inversion $x \mapsto -1/x$, de la translation $x \mapsto x+1$ et des homothéties $x \mapsto \lambda x$ dont le rapport λ est un carré.

Exercice 4.

1. D'après le théorème chinois, si $n = n_1 n_2$ est la décomposition de n en produit de deux nombres premiers entre eux, on a un isomorphisme d'anneaux $\mathbf{Z}/n\mathbf{Z} \simeq \mathbf{Z}/n_1\mathbf{Z} \times \mathbf{Z}/n_2\mathbf{Z}$. Cela implique un isomorphisme

$$\mathrm{SL}_2(\mathbf{Z}/n\mathbf{Z}) \simeq \mathrm{SL}_2(\mathbf{Z}/n_1\mathbf{Z}) \times \mathrm{SL}_2(\mathbf{Z}/n_2\mathbf{Z}).$$

Il est donc simplement besoin de déterminer le cardinal de $\mathrm{SL}_2\left(\mathbf{Z}/p^e\mathbf{Z}\right)$, pour un nombre premier p et un exposant $e \geq 1$.
Considérons l'application

$$\begin{array}{rccc} f : & \mathrm{SL}_2\left(\mathbf{Z}/p^e\mathbf{Z}\right) & \to & \left(\mathbf{Z}/p^e\mathbf{Z}\right)^2 \\ & \begin{pmatrix} a & b \\ c & d \end{pmatrix} & \mapsto & \begin{pmatrix} a \\ c \end{pmatrix}. \end{array}$$

– Déterminons l'image de f.

$$\begin{aligned} \begin{pmatrix} a \\ c \end{pmatrix} \in f\left[\mathrm{SL}_2\left(\mathbf{Z}/p^e\mathbf{Z}\right)\right] &\Leftrightarrow \exists (b,d) \in \mathbf{Z}/p^e\mathbf{Z} : ad - bc = 1 \\ &\Leftrightarrow (a,c)_{\mathbf{Z}/p^e\mathbf{Z}} = \mathbf{Z}/p^e\mathbf{Z} \\ &\Leftrightarrow (a,c) \not\equiv (0,0) \pmod{p}. \end{aligned}$$

Justifions la dernière équivalence. Réduire modulo p un élément de $\mathbf{Z}/p^e\mathbf{Z}$ a un sens parfaitement bien défini. Évidemment, si a et c se réduisent à 0 modulo p, cela entraîne qu'ils sont tous les deux divisibles par l'élément non inversible $p \in \mathbf{Z}/p^e\mathbf{Z}$ et l'idéal qu'ils engendrent ne peut pas être $\mathbf{Z}/p^e\mathbf{Z}$ tout entier.
Réciproquement, si l'un des deux ne se réduit pas à 0 modulo p, il engendre $\mathbf{Z}/p^e\mathbf{Z}$ seul et, *a fortiori*, $(a,c)_{\mathbf{Z}/p^e\mathbf{Z}} = \mathbf{Z}/p^e\mathbf{Z}$.
L'image de f est donc constitué du complémentaire de l'ensemble $p\left(\mathbf{Z}/p^{e-1}\mathbf{Z}\right)^2$ des couples d'éléments divisibles par p. En particulier,

$$\left|f\left[\mathrm{SL}_2\left(\mathbf{Z}/p^e\mathbf{Z}\right)\right]\right| = (p^e)^2 - (p^{e-1})^2 = p^{2e}\left(1 - \frac{1}{p^2}\right).$$

– Déterminons maintenant le cardinal des images réciproques des points de l'image. Utilisons le vocabulaire des actions de groupes : $\mathrm{SL}_2\left(\mathbf{Z}/p^e\mathbf{Z}\right)$ agit sur les vecteurs de $\left(\mathbf{Z}/p^e\mathbf{Z}\right)^2$ par multiplication à gauche ; si $\begin{pmatrix} a \\ c \end{pmatrix}$ est dans l'image de f, il existe une matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2\left(\mathbf{Z}/p^e\mathbf{Z}\right)$. Les matrices dans $f^{-1}\left[\begin{pmatrix} a \\ c \end{pmatrix}\right]$ sont précisément les matrices de la forme $\mathrm{S}\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, où $\mathrm{S}\begin{pmatrix} a \\ c \end{pmatrix} = \begin{pmatrix} a \\ c \end{pmatrix}$. En résumé,

$$\begin{aligned} f^{-1}\left[\begin{pmatrix} a \\ c \end{pmatrix}\right] &= \left\{ \mathrm{S}\begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \, \mathrm{S} \in \mathrm{Stab}\begin{pmatrix} a \\ c \end{pmatrix} \right\} \\ &= \left\{ \mathrm{S}\begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \, \mathrm{S} \in \mathrm{Stab}\left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix}\right] \right\} \\ &= \left\{ \mathrm{S}\begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \, \mathrm{S} \in \begin{pmatrix} a & b \\ c & d \end{pmatrix}\left(\mathrm{Stab}\begin{pmatrix} 1 \\ 0 \end{pmatrix}\right)\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \right\}. \end{aligned}$$

En particulier,

$$\left|f^{-1}\left[\begin{pmatrix}a\\c\end{pmatrix}\right]\right| = \left|\mathrm{Stab}\begin{pmatrix}1\\0\end{pmatrix}\right| = \left|\left\{\begin{pmatrix}1 & \tau\\0 & 1\end{pmatrix} \middle| \tau \in \mathbf{Z}/p^e\mathbf{Z}\right\}\right| = p^e.$$

D'après le théorème des bergers, on a donc

$$\left|\mathrm{SL}_2\left(\mathbf{Z}/p^e\mathbf{Z}\right)\right| = p^{3e}\left(1-\frac{1}{p^2}\right).$$

Ainsi, si $n = p_1^{e_1}\cdots p_n^{e_n}$, on a

$$|\mathrm{SL}_2(\mathbf{Z}/n\mathbf{Z})| = \prod_{i=1}^{n}\left(p_i^{e_i}\right)^3\left(1-\frac{1}{p_i^2}\right) = n^3\prod_{i=1}^{n}\left(1-\frac{1}{p_i^2}\right).$$

2. Il n'y a pas grand chose à démontrer :
   - Le morphisme dét : $\mathrm{GL}_2(\mathbf{Z}/n\mathbf{Z}) \to (\mathbf{Z}/n\mathbf{Z})^\times$ a par définition $\mathrm{SL}_2(\mathbf{Z}/n\mathbf{Z})$ comme noyau.
   - Le morphisme est surjectif car, si $d \in (\mathbf{Z}/n\mathbf{Z})^\times$, $\mathrm{M} = \mathrm{diag}(1,d) \in \mathrm{GL}_2(\mathbf{Z}/n\mathbf{Z})$ et $\det \mathrm{M} = d$.
   - De fait, si $\mathrm{M} \in \mathrm{GL}_2(\mathbf{Z}/n\mathbf{Z})$, on peut poser $d = \det \mathrm{M}$. On a alors $\det\left(\mathrm{M}\,\mathrm{diag}(1,d)^{-1}\right) = 1$, ce qui implique que $\mathrm{M}\,\mathrm{diag}(1,d)^{-1} \in \mathrm{SL}_2(\mathbf{Z}/n\mathbf{Z})$ et donc que $\mathrm{M} \in \mathrm{SL}_2(\mathbf{Z}/n\mathbf{Z})\mathrm{G}_n$.

   On remarque d'ailleurs que cela démontre que $\mathrm{GL}_2(\mathbf{Z}/n\mathbf{Z})$ est isomorphe à un produit semi-direct $\mathrm{SL}_2(\mathbf{Z}/n\mathbf{Z}) \rtimes (\mathbf{Z}/n\mathbf{Z})^\times$.

Exercice 5. On va démontrer qu'il est très rare que la réduction $\mathrm{GL}_2(\mathbf{Z}) \to \mathrm{GL}_2(\mathbf{Z}/n\mathbf{Z})$ soit surjective, car $\mathbf{Z}/n\mathbf{Z}$ a beaucoup trop d'inversibles par rapport à $\mathbf{Z}$.

Lemme. La réduction $\mathrm{GL}_2(\mathbf{Z}) \to \mathrm{GL}_2(\mathbf{Z}/n\mathbf{Z})$ est surjective si et seulement si la réduction modulo n induit un morphisme surjectif $\mathbf{Z}^\times = \{\pm 1\} \to (\mathbf{Z}/n\mathbf{Z})^\times$.
Preuve. Supposons la réduction $p : \mathrm{GL}_2(\mathbf{Z}) \to \mathrm{GL}_2(\mathbf{Z}/n\mathbf{Z})$ surjective. En particulier, si $u \in (\mathbf{Z}/n\mathbf{Z})^\times$, il doit exister $\mathrm{A} \in \mathrm{GL}_2(\mathbf{Z})$ tel que $p(\mathrm{M}) = \mathrm{diag}(1,u)$. Cela entraîne que $\left[\det p(\mathrm{M})\right]_n = u$ et donc que u soit l'image d'un inversible de $\mathbf{Z}$.
Réciproquement, supposons que tout inversible de $\mathbf{Z}/n\mathbf{Z}$ soit l'image d'un inversible de $\mathbf{Z}$ modulo n. Alors toute matrice $\mathrm{diag}(1,u) \in \mathrm{GL}_2(\mathbf{Z}/n\mathbf{Z})$ est dans l'image de p. Celle-ci contient donc à la fois le sous-groupe G_n de l'exercice précédent et $\mathrm{SL}_2(\mathbf{Z}/n\mathbf{Z})$ (à cause du cours). D'après l'exercice précédent, on a donc $\mathrm{im}\, f = \mathrm{GL}_2(\mathbf{Z}/n\mathbf{Z})$.

Il reste donc à déterminer les $n \geq 2$ tels que $\{\pm 1\}$ se surjecte sur $(\mathbf{Z}/n\mathbf{Z})^\times$. Cela entraîne $\varphi(n) = \left|(\mathbf{Z}/n\mathbf{Z})^\times\right| \leq 2$, c'est-à-dire que $n \in \{2,3,4,6\}$. Réciproquement, dans ces quatre cas, les rares inversibles de $\mathbf{Z}/n\mathbf{Z}$ sont bien les images de ± 1.
La réduction $\mathrm{GL}_2(\mathbf{Z}) \to \mathrm{GL}_2(\mathbf{Z}/n\mathbf{Z})$ est donc surjective si et seulement si $n \in \{2,3,4,6\}$.