# TD6 : groupe linéaire, homographies, simplicité

Exercices ⋆ : à préparer à la maison avant le TD, seront corrigés en début de TD.
Exercices ⋆⋆ : seront traités en classe en priorité.
Exercices ⋆⋆⋆ : plus difficiles.

**Exercice 1 :** ⋆

a) Soit $K$ un corps et soit $E$ un $K$-espace vectoriel de dimension finie. Rappeler pourquoi $\mathrm{PGL}(E)$ agit fidèlement sur $\mathbb{P}(E)$.

b) Soit $q$ une puissance d'un nombre premier et $n \geq 2$. Construire un morphisme de groupes injectif canonique $\mathrm{PGL}_n(\mathbb{F}_q) \to \mathfrak{S}_N$ avec $N := \frac{q^n-1}{q-1}$.

c) Identifier les groupes $\mathrm{PGL}_n(\mathbb{F}_q)$ et $\mathrm{PSL}_n(\mathbb{F}_q)$ pour $n = 2$ et $q = 2, 3, 4, 5$.

d) Montrer que $\mathrm{PSL}_2(\mathbb{F}_5)$ est isomorphe à $\mathrm{PGL}_2(\mathbb{F}_4)$.

*Solution de l'exercice* 1.

a) voir cours.

b) La question a) assure que l'on a un morphisme de groupes injectif $\varphi : \mathrm{PGL}(\mathbb{F}_q^n) \to \mathfrak{S}(\mathbb{P}^{n-1}(\mathbb{F}_q))$. Or par définition on a $\mathbb{P}^{n-1}(\mathbb{F}_q) = (\mathbb{F}_q^n \setminus \{0\})/\mathbb{F}_q^*$, donc on déduit facilement que $|\mathbb{P}^{n-1}(\mathbb{F}_q)| = \frac{|\mathbb{F}_q^n|}{|\mathbb{F}_q^*|} = \frac{q^n-1}{q-1} =: N$. Par conséquent, on a bien un morphisme de groupes injectif

$$\varphi : \mathrm{PGL}_n(\mathbb{F}_q) \to \mathfrak{S}_N \,.$$

On peut donner une autre preuve, plus géométrique, par récurrence sur $n$ : on sait que l'espace projectif $\mathbb{P}^{n-1}(K)$ est réunion disjointe d'un espace affine de dimension $n-1$ sur $K$ (disons $K^n$) et d'un hyperplan projectif de dimension $n-2$ (i.e. isomorphe à $\mathbb{P}^{n-2}(K)$), appelé hyperplan à l'infini. On a donc $\mathbb{P}^{n-1}(K) = K^{n-1} \sqcup \mathbb{P}^{n-2}(K)$, dont on déduit par récurrence la formule suivante :

$$|\mathbb{P}^{n-1}(\mathbb{F}_q)| = q^{n-1} + q^{n-2} + \cdots + q + 1 \,.$$

c) Pour $n = 2$, le morphisme $\varphi$ de la question précédente est de la forme

$$\varphi : \mathrm{PGL}_2(\mathbb{F}_q) \to \mathfrak{S}_{q+1} \,,$$

avec $|\mathrm{PGL}_2(\mathbb{F}_q)| = (q-1)q(q+1)$ et $|\mathfrak{S}_{q+1}| = (q+1)!$.

i) Si $q = 2$ ou 3, les deux cardinaux sont égaux, ce qui assure que $\varphi$ est un isomorphisme. Donc $\mathrm{PGL}_2(\mathbb{F}_2) \cong \mathfrak{S}_3$ et $\mathrm{PGL}_2(\mathbb{F}_3) \cong \mathfrak{S}_4$. En outre, $\mathrm{PSL}_2(\mathbb{F}_2) = \mathrm{PGL}_2(\mathbb{F}_2) = \mathrm{GL}_2(\mathbb{F}_2)$, donc $\mathrm{PSL}_2(\mathbb{F}_2) \cong \mathfrak{S}_3$. On vérifie aussi que $\mathrm{PSL}_2(\mathbb{F}_3) \subset \mathrm{PGL}_2(\mathbb{F}_3)$ est un sous-groupe d'indice 2, donc $\mathrm{PSL}_2(\mathbb{F}_3) \cong \mathfrak{A}_4$.

ii) Si $q = 4$, on a $\mathrm{PSL}_2(\mathbb{F}_4) = \mathrm{PGL}_2(\mathbb{F}_4) \subset \mathfrak{S}_5$ est un sous-groupe d'indice 2, ce qui assure que $\mathrm{PSL}_2(\mathbb{F}_4) = \mathrm{PGL}_2(\mathbb{F}_4) \cong \mathfrak{A}_5$, l'unique groupe simple d'ordre 60.

iii) Si $q = 5$, les cardinaux assurent que $\mathrm{PGL}_2(\mathbb{F}_5) \subset \mathfrak{S}_6$ est un sous-groupe d'indice 6. Or un résultat classique assure qu'un tel sous-groupe est isomorphe à $\mathfrak{S}_5$ (voir TD1, exercice 20). Et $\mathrm{PSL}_2(\mathbb{F}_5) \subset \mathrm{PGL}_2(\mathbb{F}_5)$ est un sous-groupe d'indice 2, ce qui assure que $\mathrm{PGL}_2(\mathbb{F}_5) \cong \mathfrak{S}_5$ et $\mathrm{PSL}_2(\mathbb{F}_5) \cong \mathfrak{A}_5$.

d) On a vu à la question précédente que ces deux groupes sont isomorphes à $\mathfrak{A}_5$. C'est l'unique groupe (à isomorphisme près) simple d'ordre 60.

**Exercice 2 :** ⋆

a) Soit $p$ un nombre premier. Montrer que la réduction modulo $p$ des coefficients d'une matrice induit un morphisme de groupes $\mathrm{SL}_n(\mathbb{Z}) \to \mathrm{SL}_n(\mathbb{Z}/p\mathbb{Z})$ qui est surjectif.

b) Montrer que ce résultat reste vrai en remplaçant $p$ par n'importe quel entier $N \geq 2$.

c) Soit $N \geq 3$. Montrer que le noyau du morphisme de réduction $\mathrm{GL}_n(\mathbb{Z}) \to \mathrm{GL}_n(\mathbb{Z}/N\mathbb{Z})$ est sans torsion.

*Solution de l'exercice* 2.

a) Si $M \in \mathrm{SL}_n(\mathbb{Z})$, le déterminant de sa réduction modulo $p$ est encore 1 car l'expression du déterminant est la même quel que soit le corps. La réduction modulo $p$ d'un produit est bien le produit des réductions car l'expression du produit de deux matrices est la même quel que soit le corps. Donc $\mathrm{SL}_n(\mathbb{Z}) \to \mathrm{SL}_n(\mathbb{Z}/p\mathbb{Z})$ est bien défini et c'est un morphisme de groupes.
Toute matrice élémentaire $I_n + E_{ij}$ de $\mathrm{SL}_n(\mathbb{Z}/p\mathbb{Z})$ est l'image de la matrice $I_n + E_{ij} \in \mathrm{SL}_n(\mathbb{Z})$. Comme les matrices élémentaires engendrent $\mathrm{SL}_n(\mathbb{Z}/p\mathbb{Z}) = \mathrm{SL}_n(\mathbb{F}_p)$, le morphisme de réduction est surjectif.

b) Soit $N \geq 2$. On décompose $N$ en facteurs premiers : $N = \prod_{i=1}^n p_i^{\alpha_i}$, avec les $p_i$ premiers deux-à-deux distincts. Alors le lemme chinois assure que l'application naturelle de réduction

$$\mathrm{SL}_n(\mathbb{Z}/N\mathbb{Z}) \to \prod_i^n \mathrm{SL}_n(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})$$

est un isomorphisme de groupes, compatible aux morphismes naturels $\mathrm{SL}_n(\mathbb{Z}) \to \mathrm{SL}_n(\mathbb{Z}/N\mathbb{Z})$ et $\mathrm{SL}_n(\mathbb{Z}) \to \prod_i^n \mathrm{SL}_n(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})$. Cela assure, via la preuve de la question précédente, qu'il suffit de montrer que pour $p$ premier et $\alpha \geq 1$, $\mathrm{SL}_n(\mathbb{Z}/p^\alpha\mathbb{Z})$ est engendré par les matrices élémentaires. Pour cela, on adapte la démonstration du cas de $\mathrm{SL}_n(K)$, où $K$ est un corps. Soit en effet $M \in \mathrm{SL}_n(\mathbb{Z}/p^\alpha\mathbb{Z})$. Puisque le déterminant de $M$ vaut 1 modulo $p^\alpha$, le développement par rapport à la première ligne assure qu'il existe un coefficient de la première ligne de $M$ qui n'est pas divisible par $p$, donc qui est inversible dans $\mathbb{Z}/p^\alpha\mathbb{Z}$. On utilise cet élément inversible comme pivot, et la preuve du cas des corps fonctionne (récurrence sur la taille de la matrice).

c) Soit $A \in \mathrm{GL}_n(\mathbb{Z})$ d'ordre fini $r$ dans le noyau de ce morphisme. Alors $A^r = I_n$, ce qui assure que $A$ est annulée par le polynôme $X^r - 1$. Comme ce polynôme est scindé à racines simples dans $\mathbb{C}$, $A$ est diagonalisable dans $\mathbb{C}$, et ses valeurs propres $\lambda_1, \ldots, \lambda_n$ sont des racines de l'unité dans $\mathbb{C}$. Et par hypothèse, il existe une matrice $B \in \mathrm{Mat}_n(\mathbb{Z})$ telle que $A = I_n + N.B$. Un calcul simple assure que $\chi_A(X) = N^n \chi_B\left(\frac{X-1}{N}\right)$.
Donc $\chi_A(1) = N^n \chi_B(0)$, avec $\chi_B(0) \in \mathbb{Z}$. Et $\chi_A(X) = \prod_{i=1}^n (X - \lambda_i)$, donc $|\chi_A(1)| = \prod_{i=1}^n |1 - \lambda_i| \leq 2^n$. On a donc $\chi_B(0) \in \mathbb{Z}$ et $|\chi_B(0)| N^n \leq 2^n$, avec $N \geq 3$. Donc nécessairement $\chi_B(0) = 0$, donc $\chi_A(1) = 0$. Donc on peut supposer que $\lambda_1 = 1$. Donc $A$ admet un vecteur propre dans $\mathbb{Q}^n$ pour la valeur propre $\lambda_1 = 1$. Quitte à multiplier par un rationnel bien choisi, on peut supposer ce vecteur propre dans $\mathbb{Z}^n$, avec les coordonnées premières entre elles. Alors $A$ est semblable dans $\mathrm{GL}_n(\mathbb{Z})$ à une matrice de la forme

$$A \sim \begin{pmatrix} 1 & * \\ 0 & A' \end{pmatrix}$$

avec $A' \in \mathrm{GL}_{n-1}(\mathbb{Z})$. Par construction, $A'$ vérifie les mêmes hypothèses que $A$, donc $A'$ admet également 1 pour valeur propre, et on conclut par récurrence sur $n$ que $A = I_n$.

**Exercice 3 :** $\star$
On note $G := \mathrm{PSL}_3(\mathbb{F}_4)$ et $H := \mathrm{PSL}_4(\mathbb{F}_2)$.

a) Montrer que $G$ et $H$ ont même cardinal.

b) Montrer que $H$ contient deux classes de conjugaison distinctes formées d'éléments d'ordre 2.

c) Montrer que tout élément d'ordre 2 dans $G$ est la classe d'une transvection de $\mathbb{F}_4^3$.

d) Montrer que $G$ et $H$ ne sont pas isomorphes.

*Solution de l'exercice* 3.

a) On voit facilement que $G$ et $H$ sont de cardinal 20160.

b) On considère les deux matrices suivantes dans $H$ :

$$A = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \text{ et } B = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Il est clair que $A$ et $B$ sont des élément de $H$ d'ordre 2. Or $A - I_4$ est de rang 1 alors que $B - I_4$ est de rang 2, donc $A$ et $B$ ne sont pas conjugués dans $H$.

c) Soit $\overline{A} \in G$ d'ordre 2. On note $A \in \mathrm{SL}_3(\mathbb{F}_3)$ un relevé de $A$. Alors $A^2 = \alpha I_3$, avec $\alpha \in \mathbb{F}_4^*$. Donc $A$ est annulée par $X^2 - \alpha = (X - \alpha^2)^2 \in \mathbb{F}_4[X]$, ce qui assure que $A$ est trigonalisable, donc $A$ est semblable à une matrice de la forme

$$A' = \begin{pmatrix} \alpha^2 & a & b \\ 0 & \alpha^2 & c \\ 0 & 0 & \alpha^2 \end{pmatrix},$$

avec $a, b, c \in \mathbb{F}_4$ non tous nuls. On peut en outre supposer que $\alpha = 1$. La condition $A^2 = I_3$ équivaut à $ac = 0$, ce qui assure que $a = 0$ ou $c = 0$. Donc $A$ est semblable à l'une des deux matrices suivantes

$$A' = \begin{pmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ ou } \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}.$$

Donc on voit facilement qu'une telle matrice $A$ est une matrice de transvection dans $\mathrm{SL}_3(\mathbb{F}_4)$. Or en dimension $n \geq 3$, les transvections sont toutes conjuguées dans $\mathrm{SL}_n(K)$. Cela assure que $G$ admet une unique classe de conjugaison formée d'éléments d'ordre 2.

d) Puisqu'un isomorphisme de groupes envoie les classes de conjugaison sur les classes de conjugaison et respecte l'ordre des éléments, les questions b) et c) assurent que $G$ et $H$ ne sont pas isomorphes. Ce sont donc deux groupes simples non isomorphes de même cardinal. On peut montrer que 2160 est le plus petit entier $n$ tel qu'il existe deux groupes simples non isomorphes de cardinal $n$.

**Exercice 4 :** $\star\star$

Soit $K$ un corps et soit $E$ un $K$-espace vectoriel de dimension 2. Soit $\mathcal{T}$ l'ensemble des classes de conjugaisons sous $\mathrm{SL}(E)$ des transvections de $E$. On fixe une base de $E$ et, pour $a \in K^*$, on note $T_a$ la transvection de matrice $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ dans cette base.

a) Montrer que $T_a$ et $T_b$ sont conjuguées si et seulement si $ab^{-1}$ est un élément de $K^{*2}$.

b) En déduire une bijection entre $K^*/K^{*2}$ et $\mathcal{T}$.

c) Que dire de plus si $K = \mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{F}_p$ ?

*Solution de l'exercice* 4.

a) Pour toute matrice $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(K)$, pour tout $x \in K^*$, on a

$$AT_xA^{-1} = \begin{pmatrix} 1 - acx & a^2x \\ -c^2x & 1 - bc \end{pmatrix}.$$

Donc pour $x, y \in K^*$, les matrices $T_x$ et $T_y$ sont conjuguées dans $\mathrm{SL}_2(K)$ si et seulement s'il existe $a, b, d \in K$ tels que $ad = 1$ et $y = a^2x$ si et seulement s'il existe $a \in K^*$ tel que $y = a^2x$ si et seulement si $yx^{-1} \in (K^*)^2$.

b) On définit l'application $\begin{array}{ccc} \psi : K^\times & \to & \mathcal{T} \\ x & \mapsto & [T_x] \end{array}$, où $[T]$ désigne la classe de similitude de l'endomorphisme $T$. Elle est surjective car toute transvection de $E$ a pour matrice $T_y$ pour un certain $y \in K^*$, dans une base $(e_1, e_2)$ bien choisie. La question a) assure que $\psi$ passe au quotient par $(K^*)^2$ et induit la bijection souhaitée.

c) Pour $\mathbb{C}$, $\mathcal{T}$ est un singleton car tout élément est un carré ; donc toutes les transvections sont conjuguées dans $\mathrm{SL}_2(\mathbb{C})$. Pour $\mathbb{R}$ ou $\mathbb{F}_p$, $\mathcal{T}$ est un ensemble à 2 éléments. Pour $\mathbb{Q}$, $\mathcal{T}$ est infini, puisque $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ est en bijection avec l'ensemble des entiers relatifs sans facteur carré.

**Exercice 5 :** $\star\star$

Soit $n \geq 1$. On note $\mathrm{Int}(\mathfrak{S}_n)$ le sous-groupe des automorphismes intérieurs de $\mathrm{Aut}(\mathfrak{S}_n)$.

a) Soit $\phi \in \mathrm{Aut}(\mathfrak{S}_n)$ tel que $\phi$ transforme toute transposition en une transposition. Montrer que $\phi$ est intérieur.

b) Soit $\sigma \in \mathfrak{S}_n$. Déterminer le cardinal du commutant $Z(\sigma) := \{\tau \in \mathfrak{S}_n \mid \tau\sigma\tau^{-1} = \sigma\}$ de $\sigma$.

c) En déduire que si $n \neq 6$, on a $\mathrm{Int}(\mathfrak{S}_n) = \mathrm{Aut}(\mathfrak{S}_n)$.

d) Soit $n \geq 5$ tel que $\mathrm{Int}(\mathfrak{S}_n) = \mathrm{Aut}(\mathfrak{S}_n)$. Montrer que tous les sous-groupes d'indice $n$ de $\mathfrak{S}_n$ sont conjugués.

e) En utilisant les 5-Sylow de $\mathfrak{S}_5$, montrer qu'il existe un sous-groupe $H$ d'indice 6 de $\mathfrak{S}_6$ opérant transitivement sur $\{1, \ldots, 6\}$.

f) Construire géométriquement un sous-groupe $H'$ d'indice 6 dans $\mathfrak{S}_6$ vérifiant les mêmes propriétés que $H$.

g) En déduire que $\mathrm{Aut}(\mathfrak{S}_6) \neq \mathrm{Int}(\mathfrak{S}_6)$.

*Solution de l'exercice* 5.

a) On peut supposer $n \geq 4$, puisque tout automorphisme de $\mathfrak{S}_i$ pour $i \leq 3$ étant intérieur (le vérifier). Le groupe symétrique $\mathfrak{S}_n$ est engendré par les transpositions $\tau_i = (1\, i)$ pour $i \geq 2$. Puisque $\tau_i$ et $\tau_j$ ne commutent pas si $i \neq j$, les supports des transpositions $\varphi(\tau_i)$ et $\varphi(\tau_j)$ ont exactement un point en commun, que l'on notera $\alpha_1$. Comme $\varphi(\tau_i)$ a un point commun avec $\varphi(\tau_1)$, $\varphi(\tau_2)$ et $\varphi(\tau_3)$, il ne peut en tre autrement : tous ont $\alpha_1$ en commun. On écrit alors $\varphi(\tau_i) = (\alpha_1\ \alpha_i)$. On a ensuite $\{\alpha_1, \ldots, \alpha_n\} = \{1, \ldots, n\}$ par injectivité de $\varphi$. On définit alors la permutation $\alpha \in \mathfrak{S}_n$ par $\alpha(i) = \alpha_i$ pour tout $i$ : il est alors clair que $\varphi$ est la conjugaison par $\alpha$, donc $\varphi \in \mathrm{Int}(\mathfrak{S}_n)$.

b) Décomposons $\sigma$ en produit de cycles à supports disjoints, $k_1$ cycles de longueur 1, ..., $k_n$ cycles de longueur $n$, avec $n = \sum_i i k_i$. Un élément qui commute à $\sigma$ doit préserver la décomposition en cycles de $\sigma$, et donc envoyer le support d'un $k$-cycle sur celui d'un autre $k$-cycle, en respectant l'ordre cyclique du support de ces cycles, pour tout $k$. Ainsi le commutant d'un $n$-cycle de $\mathfrak{S}_n$ est-il par exemple composé des puissances de ce dernier. En mettant ceci bout à bout, on prouve que l'on a

$$|Z(\sigma)| = \prod_i k_i! i^{k_i}.$$

c) Soit $\varphi$ un automorphisme de $\mathfrak{S}_n$. Si $\tau$ est une transposition de $\mathfrak{S}_n$, $\varphi(\tau)$ est aussi d'ordre 2 et est donc un produit de $k$ transpositions à supports disjoints. Or on a $|Z(\tau)| = |Z(\varphi(\tau))|$, ce qui se réécrit $2(n-2)! = 2^k k!(n-2k)!$. Comme on a $n \neq 6$, on voit que ceci impose $k = 1$. Par la question b), $\varphi$ est alors intérieur.

d) Soit $H \subset \mathfrak{S}_n$ un sous-groupe d'indice $n$. L'action transitive de $\mathfrak{S}_n$ sur $\mathfrak{S}_n/H$ induit un morphisme de groupes $\phi : \mathfrak{S}_n \to \mathfrak{S}(\mathfrak{S}_n/H) \cong \mathfrak{S}_n$. Alors $\mathrm{Ker}(\phi)$ est un sous-groupe distingué de $\mathfrak{S}_n$, c'est donc $\{\mathrm{id}\}$, $\mathfrak{A}_n$ ou $\mathfrak{S}_n$. Puisque $\mathrm{Ker}(\phi)$ agit trivialement sur la classe de $H$ dans $\mathfrak{S}_n/H$, on a $\mathrm{Ker}(\phi) \subset H$, donc $\mathrm{Ker}(\phi) = \{\mathrm{id}\}$, i.e. $\phi$ est injective. Donc $\phi \in \mathrm{Aut}(\mathfrak{S}_n)$. Par hypothèse, il existe $\sigma \in \mathfrak{S}_n$ tel que $\phi$ soit la conjugaison par $\sigma$. Or par construction $\phi$ envoie $H$ sur le stabilisateur d'un point (la classe de $H$) dans $\mathfrak{S}(\mathfrak{S}_n/H) \cong \mathfrak{S}_n$. Enfin, dans $\mathfrak{S}_n$, il est clair que les stabilisateurs d'un point de $\{1, \ldots, n\}$ sont tous conjugués.

e) Les théorèmes de Sylow assurent que $\mathfrak{S}_5$ admet un ou six 5-Sylow. La simplicité de $\mathfrak{A}_5$ assure que $\mathfrak{S}_5$ n'admet pas de sous-groupe distingué d'ordre 5, donc $\mathfrak{S}_5$ admet exactement six 5-Sylow. Notons $X$ l'ensemble des 5-Sylow de $\mathfrak{S}_5$. L'action de $\mathfrak{S}_5$ sur $X$ par conjugaison est transitive, et induit un morphisme de groupes $\mu : \mathfrak{S}_5 \to \mathfrak{S}(X) \cong \mathfrak{S}_6$ dont le noyau est trivial (car on connaît les sous-groupes distingués de $\mathfrak{S}_5$). On note alors $H := \mu(\mathfrak{S}_5) \subset \mathfrak{S}_6$.

f) Le groupe $H' = \mathrm{PGL}_2(\mathbb{F}_5)$, vu comme sous-groupe de $\mathfrak{S}_6$ par action sur $\mathbb{P}^1(\mathbb{F}_5)$ (voir exercice 1), n'est pas conjugué à $\mathfrak{S}_5 = \mathrm{Stab}(6) \subset \mathfrak{S}_6$ puisqu'il ne fixe aucun point.

g) Les questions d) et e) (ou f)) assurent que le groupe $\mathfrak{S}_6$ possède au moins un automorphisme extérieur.

**Exercice 6 :** $\star\star$

Soit $K$ un corps.

a) Montrer que l'action de $\mathrm{PGL}_2(K)$ sur $\mathbb{P}^1(K)$ est 3-transitive. Est-elle 4-transitive ?

b) Pour $n = 1, 2, 3$, décrire le quotient $\mathbb{P}^1(K)^{[n]}/\mathrm{PGL}_2(K)$ (i.e. l'ensemble des orbites) où $\mathbb{P}^1(K)^{[n]}$ désigne l'ensemble des $n$-uplets de points deux-à-deux distincts de $\mathbb{P}^1(K)$.

c) Montrer que l'on a une bijection naturelle $(\mathbb{P}^1(K)^{[3]} \times \mathbb{P}^1(K))/\mathrm{PGL}_2(K) \to \mathbb{P}^1(K)$. Cette bijection est notée $(a, b, c, d) \mapsto [a, b, c, d]$ et $[a, b, c, d]$ est appelé le birapport des points $a, b, c, d$.

d) Expliciter la bijection précédente via l'identification $\mathbb{P}^1(K) \cong K \cup \{\infty\}$.

*Solution de l'exercice* 6.

a) Soient $(x_1, x_2, x_3) \in \mathbb{P}^1(K)^3$ et $(y_1, y_2, y_3) \in \mathbb{P}^1(K)^3$ deux triplets de points de $\mathbb{P}^1(K)$ deux-à-deux distincts. Par définition, il existe des vecteurs non nuls $u_i \in K^2$ et $v_i \in K^2$, définis à un scalaire près, tels que $x_i$ est la classe de $u_i$ et $y_i$ celle de $v_i$ dans $\mathbb{P}^1(K)$. Les points initiaux étant deux-à-deux distincts, cela assure que les vecteurs $u_i$ (resp. $v_i$) sont deux-à-deux non proportionnels. En particulier, il existe des scalaires $\lambda_i$ et $\mu_i$ non nuls tels que $u_3 = \lambda_1 u_1 + \lambda_2 u_2$ et $v_3 = \mu_1 v_1 + \mu_2 v_2$. Quitte à remplacer $u_i$ par $\lambda_i u_i$ et $v_i$ par $\mu_i v_i$, on peut supposer que $\lambda_i = \mu_i = 1$. Comme $(u_1, u_2)$ et $(v_1, v_2)$ sont des bases de $K^2$, il existe $g \in \mathrm{GL}(K^2)$ telle que $g(u_i) = v_i$ pour $i = 1$ et 2. Alors par linéarité, on a $g(u_3) = v_3$. Si on note $h$ l'image de $g$ dans $\mathrm{PGL}_2(K)$, on a $h(x_i) = y_i$ pour $i = 1, 2, 3$. Cela assure que l'action de $\mathrm{PGL}_2(K)$ sur $\mathbb{P}^1(K)$ est 3-transitive.

En revanche, elle n'est pas 4-transitive si $K \neq \mathbb{F}_2, \mathbb{F}_3$ : on voit facilement qu'un élément de $\mathrm{PGL}_2(K)$ est complétement déterminé par les images de trois points distincts de $\mathbb{P}^1(K)$ : une application linéaire de $K^2$ qui a trois droites propres distinctes est une homothétie.

b) La question a) assure que $\mathbb{P}^1(K)^{[n]}/\mathrm{PGL}_2(K)$ est réduit à un point si $n = 1, 2, 3$, i.e. l'action de $\mathrm{PGL}_2(K)$ sur $\mathbb{P}^1(K)^{[n]}$ a une seule orbite.

c) On définit une application $\varphi : \mathbb{P}^1(K)^{[3]} \times \mathbb{P}^1(K) \to \mathbb{P}^1(K)$ par $\varphi(x_1, x_2, x_3, x_4) := h(x_4)$, où $h \in \mathrm{PGL}_2(K)$ est l'unique homographie de $\mathbb{P}^1(K)$ telle que $h(x_1) = \infty$, $h(x_2) = 0$ et $h(x_3) = 1$. Cette application est bien définie (voir solution de la question a)). Elle est surjective car $\varphi(\infty, 0, 1, x) = x$ pour tout $x \in \mathbb{P}^1(K)$.

Soient $(x_i) \in \mathbb{P}^1(K)^{[3]} \times \mathbb{P}^1(K)$ et $g \in \mathrm{PGL}_2(K)$. Si $h \in \mathrm{PGL}_2(K)$ est définie par $h(x_1) = \infty$, $h(x_2) = 0$ et $h(x_3) = 1$, alors $\varphi(x_i) = h(x_4)$, et on voit que $h \circ g^{-1}$ envoie le triplet $(g(x_1), g(x_2), g(x_3))$ sur le triplet $(\infty, 0, 1)$, ce qui assure que $\varphi(g(x_i)) = h \circ g^{-1}(g(x_4)) = h(x_4) = \varphi(x_i)$. Donc $\varphi$ passe au quotient par $\mathrm{PGL}_2(K)$ et induit une application surjective $\overline{\varphi} : (\mathbb{P}^1(K)^{[3]} \times \mathbb{P}^1(K))/\mathrm{PGL}_2(K) \to \mathbb{P}^1(K)$.

Soient $(x_i)$ et $(y_i)$ dans $\mathbb{P}^1(K)^{[3]} \times \mathbb{P}^1(K)$. On a $\varphi(x_1, x_2, x_3, x_4) = \varphi(y_1, y_2, y_3, y_4)$ si et seulement $h(x_4) = g(y_4)$ où $h$ (resp. $g$) est l'unique élément de $\mathrm{PGL}_2(K)$ tel que $h(x_1) = \infty$, $h(x_2) = 0$ et $h(x_3) = 1$ (resp. $g(y_1) = \infty$, $g(y_2) = 0$ et $g(y_3) = 1$). Alors l'homographie $g^{-1} \circ h$ envoie $x_i$ sur $y_i$ pour $i = 1, 2, 3, 4$. Cela assure que l'application $\overline{\varphi}$ est une bijection.

d) On identifie $\mathbb{P}^1(K)$ avec $K \cup \infty$. Soient $x_i \in K \cup \{\infty\}$ tels que $x_1, x_2, x_3$ sont deux-à-deux distincts. Si $x_1, x_2, x_3 \neq \infty$, on vérifie que l'application $h : K \cup \infty \to K \cup \infty$ définie par $x \mapsto \frac{x_3 - x_1}{x_2 - x_1} \frac{x - x_2}{x - x_1}$ (avec les conventions usuelles) envoie le triplet $(x_1, x_2, x_3)$ sur le triplet $(\infty, 0, 1)$, et

que $h$ coïncide avec l'homographie $h' \in \mathrm{PGL}_2(K)$ définie par la matrice $\begin{pmatrix} x_3-x_1 & -x_2(x_3-x_1) \\ x_2-x_1 & -x_1(x_2-x_1) \end{pmatrix} \in \mathrm{GL}_2(K)$, ce qui assure que $\varphi(x_i) = h(x_4)$, i.e.

$$\varphi(x_i) = \frac{x_3-x_1}{x_2-x_1}\frac{x_4-x_2}{x_4-x_1}\,.$$

Si $x_1 = \infty$, on considère $h : x \mapsto \frac{x-x_2}{x_3-x_2}$ et on vérifie que c'est une homographie envoyant $(x_i)$ sur $(\infty, 0, 1)$, ce qui redonne la même formule pour $\varphi(x_i)$ avec les convientions usuelles. De même, si $x_2 = \infty$, on considère $h : x \mapsto \frac{x_3-x_1}{x-x_1}$, qui redonne la même formule, et si $x_3 = \infty$, on considère $h : x \mapsto \frac{x-x_2}{x-x_1}$, qui redonne encore une fois la même formule.
Finalement, dans tous les cas, on a bien

$$\varphi(x_i) = \frac{x_3-x_1}{x_2-x_1}\frac{x_4-x_2}{x_4-x_1}\,.$$

**Exercice 7 :**

a) Montrer que le groupe $\mathrm{PSL}_2(\mathbb{Z})$ agit naturellement sur le demi-plan de Poincaré $\mathcal{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$.

b) Montrer que cette action est fidèle. Identifier le stabilisateur de $i \in \mathcal{H}$.

c) Soit $G$ un groupe agissant sur un espace topologique $X$. Une partie $F$ de $X$ est appelée *domaine fondamental* pour l'action de $G$ sur $X$ si elle vérifie :

$$\text{(i) } \overline{F^\circ} = F, \quad \text{(ii) } X = \bigcup_{h\in G} hF, \quad \text{(iii) } \forall g \in G\setminus\{1\},\ F^\circ \cap (gF)^\circ = \emptyset.$$

Soit $D = \{z \in \mathcal{H} \ : \ |\mathrm{Re}(z)| \le \frac{1}{2}, |z| \ge 1\}$.

i) En maximisant la partie imaginaire des éléments d'une orbite $\mathrm{PSL}_2(\mathbb{Z})\cdot z$, montrer que $D$ vérifie la propriété (ii).

ii) Montrer que $D$ est un domaine fondamental pour l'action de $\mathrm{PSL}_2(\mathbb{Z})$ sur $\mathcal{H}$.

iii) En déduire que les matrices $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ engendrent $\mathrm{SL}_2(\mathbb{Z})$.

*Solution de l'exercice* 7.

a) On considère l'action usuelle de $\mathrm{PGL}_2(\mathbb{C})$ sur $\mathbb{C}\cup\{\infty\} = \mathbb{P}^1(\mathbb{C})$ par homographie, via la formule

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z := \frac{az+b}{cz+d}\,.$$

On vérifie facilement que pour tout $z \in \mathcal{H}$, et tout $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PSL}_2(\mathbb{Z})$, on a $A\cdot z \in \mathbb{C}$ et

$$\mathrm{Im}\,(A\cdot z) = \frac{\mathrm{Im}\,(z)}{|cz+d|^2}\,,$$

ce qui assure que $A\cdot z \in \mathcal{H}$. D'où l'action recherchée.

b) Soit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PSL}_2(\mathbb{Z})$. On a

$$A\cdot i = i \Leftrightarrow a = d \text{ et } b = -c \Leftrightarrow A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ ou } A = I_2\,.$$

On note $S := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Alors $\mathrm{Stab}(i) = \{I_2, S\} \cong \mathbb{Z}/2\mathbb{Z}$.

En outre, comme pour tout $z \in \mathcal{H}$, on a $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\cdot z = \frac{-1}{z}$, on voit que la matrice $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ ne fixe pas le point $z = 1+i \in \mathcal{H}$, ce qui assure que l'action de $\mathrm{PSL}_2(\mathbb{Z})$ sur $\mathcal{H}$ est fidèle.

c) i) Soit $z \in \mathcal{H}$. On considère l'orbite $\mathrm{PSL}_2(\mathbb{Z}) \cdot z$ de $z$, et on note $X := \{z' \in \mathrm{PSL}_2(\mathbb{Z}) \cdot z : \mathrm{Im}\,(z') \geq \mathrm{Im}\,(z)\}$. On a vu que pour tout $A \in \mathrm{PSL}_2(\mathbb{Z})$, on a $\mathrm{Im}\,(A \cdot z) = \frac{\mathrm{Im}\,(z)}{|cz+d|^2}$, donc pour tout $z' = A \cdot z \in X$, on a $|cz + d|^2 \leq 1$, ce qui n'arrive que pour un nombre fini d'entiers $c$ et $d$. Par conséquent, il existe $z' \in X$ tel que $\mathrm{Im}\,(z')$ soit maximal.
Comme la matrice $T := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ est dans $\mathrm{PSL}_2(\mathbb{Z})$, et que pour tout $n \in \mathbb{Z}$, $T^n \cdot z' = z' + n$, on peut supposer que $|\mathrm{Re}\,(z)| \leq \frac{1}{2}$. Or $S \cdot z' = \frac{-1}{z'}$ et $\mathrm{Im}\,(\frac{-1}{z'}) = \frac{\mathrm{Im}\,(z')}{|z'|^2} \leq \mathrm{Im}\,(z')$ par maximalité de $z'$, donc $|z'| \geq 1$. Donc $z' \in D$ et $D$ vérifie la propriété (ii).

ii) La propriété (i) est clairement vérifiée par $D$. Vérifions la propriété (iii) : soit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PSL}_2(\mathbb{Z})$. Soit $z \in D^\circ$ tel que $A \cdot z \in D$. Par symétrie, on peut supposer quer $\mathrm{Im}\,(A \cdot z) \geq \mathrm{Im}\,(z)$. Alors on a vu que $|cz + d|^2 \leq 1$, donc $|c| \leq \frac{2}{\sqrt{3}}$, donc $c = -1$, 0 ou 1.
— si $c = 0$, alors $a = d = 1$ et $A$ est une translation de vecteur $(b, 0)$ ($b \in \mathbb{Z}$) dans $\mathcal{H}$, donc $b = 0$ (sinon $A \cdot z \notin D^\circ$).
— si $c = \pm 1$, alors on vérifie que $a = d = 0$ et $b = -1$, ce qui est impossible.
Donc $A = I_2$.
Donc $D$ est bien un domaine fondamental pour cette action.

iii) Soient $A \in PSL_2(\mathbb{Z})$ et $z \in D^\circ$, on a $A \cdot z \in \mathcal{H}$, donc en adaptant la preuve de la question c)i) en remplaçant le groupe $\mathrm{PSL}_2(\mathbb{Z})$ par son sous-groupe $\langle S, T\rangle$, on voit qu'il existe $B \in \langle S, T\rangle$ tel que $B \cdot (A \cdot z) \in D$. Alors $z \in D^\circ$ et $(BA) \cdot z \in D$. On a vu à la question c)i) qu'alors $BA = \pm I_2$, ce qui assure que $A = B^{-1}$ dans $\mathrm{PSL}_2(\mathbb{Z})$, donc $A \in \langle S, T\rangle$, donc $\mathrm{PSL}_2(\mathbb{Z}) = \langle S, T\rangle$, et comme $S^2 = -I_2$, on a $\mathrm{SL}_2(\mathbb{Z}) = \langle S, T\rangle$.

**Exercice 8 :**
Soit $K$ un corps.
Montrer que les homographies sont exactement les $K$-automorphismes du corps $K(T)$ (les automorphismes de $K(T)$ dont la restriction à $K$ est l'identité), i.e. que $\mathrm{Aut}_K(K(T)) \cong \mathrm{PGL}_2(K)$.

*Solution de l'exercice* 8. On dispose d'un morphisme de groupes évident $\varphi : \mathrm{PGL}_2(K) \to \mathrm{Aut}_K(K(T))$ défini de la façon suivante : si $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ représente un élément de $\mathrm{PGL}_2(K)$, on note $\varphi(A)$ le $K$-automorphisme de $K(T)$ défini par $\varphi(A) : T \mapsto \frac{aT+b}{cT+d}$. Il est clair que $\varphi$ est un morphisme de groupes. Montrons que $\varphi$ est injectif : si $\varphi(A) = \mathrm{id}$, cela signifie que $\frac{aT+b}{cT+d} = T$, ce qui implique $aT+b = cT^2+dT$, donc $b = c = 0$ et $a = d$, donc $A$ est une homothétie. Donc $\varphi$ est injectif. Montrons que $\varphi$ est surjectif : soit $\sigma \in \mathrm{Aut}_K(K(T))$. La fraction rationnelle $\sigma(T)$ s'écrit $\frac{P}{Q}$, avec $P, Q \in K[T]$ premiers entre eux. Comme $\sigma$ est une bijection de $K(T)$, on peut écrire $T$ comme une fraction rationnelle en $\frac{P}{Q}$, donc il existe des polynômes $R$ et $S$, premiers entre eux, tels que $T = \frac{R(\sigma(T))}{S(\sigma(T))}$.
En écrivant $r_0$ et $s_0$ les coefficients constants de $R$ et $S$, et $n := \max(\deg R, \deg S)$, on déduit de cette égalité que $(s_0T - r_0)Q^n = PU$, pour un certain polynôme $U \in K[T]$. Comme $P$ et $Q$ sont premiers entre eux, on en déduit que $P$ divise $s_0T - r_0$. Or $r_0$ ou $s_0$ est non nul, donc cela implique que $\deg P \leq 1$. Symétriquement, on montre que $\deg Q \leq 1$ en utilisant les coefficients $s_n$ et $r_n$. Donc finalement $\sigma(T)$ est de la forme $\frac{aT+b}{cT+d}$. Enfin, pour que $\sigma$ soit bijective, on constate que l'on doit avoir $ad - bc \neq 0$, ce qui assure que $\sigma$ est bien une homographie, i.e. que $\varphi$ est surjectif.

**Exercice 9 :** $\star\star\star$
Soit $G$ un groupe simple d'ordre 360.

a) Montrer que $G$ admet dix 3-Sylow.

b) Montrer que $G$ est isomorphe à un sous-groupe de $\mathfrak{A}_{10}$. On supposera désormais que $G$ est un sous-groupe de $\mathfrak{A}_{10}$.

c) Soit $S$ un 3-Sylow de $G$. Montrer que $S$ n'est pas cyclique, et que l'on peut supposer que $N_G(S)$ est le stabilisateur de 10 dans $G \subset \mathfrak{A}_{10}$.

d) Montrer que tout élément non trivial de $S$ ne fixe aucun point de $\{1, 2, \ldots, 9\}$.

e) Montrer que l'on peut supposer que $S$ est engendré par les éléments $x = (1\,2\,3)(4\,5\,6)(7\,8\,9)$ et $y = (1\,4\,7)(2\,5\,8)(3\,6\,9)$.

f) Montrer que le stabilisateur $P$ de 1 dans $N_G(S)$ est cyclique d'ordre 4 et est un 2-Sylow de $N_G(S)$. On note $z$ un générateur de $P$.

g) Montrer qu'on peut supposer que $z = (2\,4\,3\,7)(5\,6\,9\,8)$.

h) Soit $T$ un 2-Sylow de $G$ contenant $z$. Montrer que $T = \langle z, t\rangle$, avec $t$ d'ordre 2.

i) Montrer que l'on peut supposer que $t = (1\,10)(2\,3)(5\,6)(8\,9)$.

j) Montrer que $G = \langle x, y, z, t\rangle$.

k) Que peut-on en conclure pour les groupes simples d'ordre 360 ?

l) Montrer que $\mathrm{PSL}_2(\mathbb{F}_9) \cong \mathfrak{A}_6$.

*Solution de l'exercice* 9.

a) On note $n_3$ le nombre de 3-Sylow. Les théorèmes de Sylow assurent que $n_3 \in \{1, 4, 10, 40\}$. Alors la simplicité de $G$ assure que $n_3 = 10$ ou 40. Montrons que $n_3 = 40$ est impossible.

Première solution : supposons $n_3 = 40$. Alors pour tout 3-Sylow $S$, le normalisateur $N_G(S) \subset G$ est d'indice 40, donc $N_G(S)$ est de cardinal 9. Donc $N_G(S) = S$. Et $|S| = 9$ assure que $S$ est abélien. Par conséquent, $S = Z(N_G(S))$. Alors le théorème de transfert de Burnside (voir TD5, exercice 16) assure que $G$ n'est pas simple, ce qui est contradictoire.

Seconde solution : on voit qu'il existe deux 3-Sylow $S$ et $T$ tels que $I := S \cap T$ est non trivial, i.e. est d'ordre 3. Alors $N_G(I)$ contient $S$ et $T$, donc $|N_G(I)|$ est multiple de 9, divise 360 et est distinct de 9. Or $|N_G(I)| \neq 18, 45$ car un groupe d'ordre 18 (resp. 45) a un unique 3-Sylow. Si $|N_G(I)| \geq 72$, alors $N_G(I)$ est un sous-groupe strict de $G$ d'indice $\leq 5$, donc $G$ se plonge dans un groupe symétrique $\mathfrak{S}_d$ avec $d \leq 5$, ce qui est contradictoire car 360 ne divise pas 5!. Donc $|N_G(I)| = 36$. Donc $N_G(I)$ a un unique 2-Sylow $P$, qui est donc distingué dans $N_G(I)$. Alors $N_G(P)$ contient $N_G(I)$, et $P$ est contenu comme sous-groupe d'indice 2 dans un 2-Sylow $Q$ de $G$, donc $Q \subset N_G(P)$, donc $|N_G(P)|$ est multiple de 8, donc $|N_G(P)|$ est multiple de 72, et distinct de 360, donc $|N_G(P)| = 72$, donc $G$ admet un sous-groupe d'indice 5, ce qui est contradictoire à nouveau.

b) Puisque $n_3 = 10$, l'action de $G$ sur l'ensemble $X$ des 3-Sylow de $G$ fournit un morphisme de groupes, injectif par simplicité de $G$, $\varphi : G \to \mathfrak{S}(X) \cong \mathfrak{S}_{10}$. Alors $\varphi(G) \cap \mathfrak{A}_{10}$ est distingué non trivial dans $\varphi(G)$, donc par simplicité, $\varphi(G) \subset \mathfrak{A}_{10}$, d'où le résultat.

c) Comme $N_G(S)$ fixe $S \in X$, le groupe $N_G(S)$ s'identifie bien au stabilisateur du point $S \in X$ dans $G$.

Supposons $S$ cyclique. Alors un générateur de $S$ est un élément d'ordre 9 dans $\mathfrak{A}_{10}$, donc un 9-cycle. Donc $N_G(S)$ est formé d'éléments de $\mathfrak{A}_9$ (on a vu que $N_G(S)$ fixe un point) normalisant un 9-cycle. Or le centralisateur d'u 9-cycle dans $\mathfrak{A}_9$ est exactement le sous-groupe engendré par ce cycle, donc cela assure que le morphisme naturel $N_G(S)/S \to \mathrm{Aut}(S)$ est injectif. Or $|N_G(S)/S|4$ et $|\mathrm{Aut}(S)| = 6$, ce qui est contradictoire.

Donc $S$ n'est pas cyclique.

d) Supposons qu'il existe $s \in S \setminus \{\mathrm{id}\}$ fixant un point $i \in \{1, \ldots, 9\}$. Alors $s$ est d'ordre 3, et $s \in S \cap T$, où $T$ est le 3-Sylow de $G$ correspondant au point $i \in \{1, \ldots, 9\}$. Alors on est exactement dans la situation de la seconde solution de la question a), et on arrive donc à la même contradiction. D'où le résultat.

e) Les questions c) et d) assurent que $S$ est engendré par deux éléments $x$ et $y$ de $\mathfrak{A}_9$ d'ordre 3, qui commutent et qui ne fixent aucun point de $\{1, \ldots, 9\}$. Cela implique que chacun de ces deux générateurs est un produit de trois 3-cycles à supports disjoints. Notons $x = (a\,b\,c)(d\,e\,f)(g\,h\,i)$, avec $\{a, b, c, d, e, f, g, h, i\} = \{1, \ldots, 9\}$. Comme $y$ commute avec $x$, $y$ permute les supports des trois 3-cycles de $x$ en respectant l'ordre cyclique sur ces supports. En outre, un 3-cycle de $y$ ne peut avoir le même support qu'un 3-cycle de $x$, sinon un élément non trivial de $S$

fixe les trois points de ce support. Donc quitte à permuter $(d\,e\,f)$ et $(g\,h\,i)$, on peut supposer que $y = (a\,d\,g)(b\,e\,h)(c\,f\,i)$. Quitte à renuméroter les éléments de $\{1,\dots,9\}$, on a le résultat souhaité.

f) La question précédente assure que $S$ agit (librement et) transitivement sur $\{1,\dots,9\}$. Donc $|P| = 4$. Donc $P$ est un 2-Sylow de $N_G(S)$ (qui est de cardinal 36) et $N_G(S) = S.P$. Donc $P$ est isomorphe à $N_G(S)/S$ et on vérifie que le centralisateur de $S$ dans $\mathfrak{A}_9$ est un 3-groupe, donc $Z_G(S) = S$, donc $P \cong N_G(S)/G$ s'injecte dans $\mathrm{Aut}(S) \cong \mathrm{GL}_2(\mathbb{F}_3)$. Et comme $N_G(S)$ est un sous-groupe de $\mathfrak{A}_9$, on vérifie que son action par conjugaison sur $S$ se factorise en un morphisme $N_G(S) \to \mathrm{SL}_2(\mathbb{F}_3)$. Donc $P$ s'injecte dans $\mathrm{SL}_2(\mathbb{F}_3)$. Or l'exercice 10, question b) du TD2 assure que l'unique 2-Sylow de $\mathrm{SL}_2(\mathbb{F}_3)$ est isomorphe au groupe des quaternions d'ordre 8, et tout sous-groupe d'ordre 4 du groupe des quaternions est cyclique. Donc $P$ est cyclique.

g) L'élément $z \in P$ fixe 1 et 10, donc $z \in \mathfrak{A}(\{2,3,\dots,9\})$. Et $z$ est d'ordre 4, donc $z$ est un produit de deux 4-cycles à supports disjoints. Notons $a \in \{3,\dots,9\}$ l'image de 2 par $z$. Puisque $z$ normalise $S$ et est d'ordre 4, on voit que $a \in \{4,7\}$. Et si $a = 4$, nécessairement $z = (2\,4\,3\,7)(5\,6\,9\,8)$, et si $a = 7$, alors $z = (2\,7\,3\,4)(5\,8\,9\,6)$. Comme ces deux éléments sont inverses l'un de l'autre, ils engendrent le même groupe $P$, donc quitte à remplacer $z$ par $z^{-1}$, on peut supposer que $z = (2\,4\,3\,7)(5\,6\,9\,8)$.

Remarquons que cette question implique qu'un élément non trivial de $G$ fixe au plus deux points de $\{1,\dots,10\}$.

h) Comme $\langle z\rangle \subset T$ est d'indice 2, il existe bien $t \in T$ tel que $T = \langle z, t\rangle$. Comme $G$ est simple, $T$ ne peut pas être un groupe cyclique, donc $t$ est d'ordre 2 ou 4. Or $t \notin N_G(S)$, donc $t(10) \neq 10$. Comme $z$ fixe 1 et 10, on voit que nécessairement $t(1) = 10$ et $t(10) = 1$.

Supposons maintenant $t$ d'ordre 4. Comme $t$ est paire et contient le cycle $(1\,10)$ dans sa décomposition, la restriction de $t$ à $\{1,\dots,9\}$ est soit un 4-cycle, soit le produit d'un 4-cycle par une bitransposition de supports disjoints. Dans les deux cas, $t^2$ est une bitransposition, or $t^2 = c^2$ et $c^2$ est un produit de quatre transpositions à supports disjoints. D'où une contradiction.

Donc $t$ est d'ordre 2.

i) La question précédente assure que $T \cong D_4$. Comme $t$ est paire, d'ordre 2 et fixe au plus deux points (voir question g)), on voit que $t$ est produit de quatre transpositions (dont $(1\,10)$). Comme $t$ normalise $P = \langle z\rangle$, une étude au cas par cas assure que, quitte à multiplier $t$ par une puissance de $z$ (ce qui est acceptable), $t$ est bien de la forme souhaitée.

j) Par construction, $\langle x, y, z, t\rangle \subset G$ est un sous-groupe de cardinal $\geq 72$. Or $G$ n'admet pas de sous-groupe strict d'indice $\leq 5$, donc $G = \langle x, y, z, t\rangle$.

k) Les questions précédentes assurent que tout groupe simple d'ordre 360 est isomorphe au sous-groupe $G_0$ de $\mathfrak{A}_{10}$ engendré par les éléments explicites $x, y, z, t$ de $\mathfrak{A}_{10}$ (ces éléments ne dépendent pas de $G$). En particulier, cela implique que tous les groupes simples d'ordre 360 sont isomorphes.

l) Ces deux groupes sont simples d'ordre 360, donc la question précédente assure le résultat.