4. Le groupe $\mathrm{PGL}_2(k)$ et quelques (iso)morphismes miraculeux

Regardons $\mathrm{PGL}_2(k)$ d'un peu plus près. Considérons pour cela l'ensemble $\mathrm{P}^1(k)$ des droites vectorielles du plan vectoriel k^2 (*droite projective sur* k). Posons

$$\widehat{k} \quad = \quad k \coprod \{\infty\}.$$

(pas de confusion possible avec un dual ici !). On définit $\beta : \widehat{k} \to \mathrm{P}^1(k)$ par

$$\beta(x) \;=\; k\begin{pmatrix} x \\ 1 \end{pmatrix} \;\; \forall\, x \in k, \;\text{ et }\; \beta(\infty) \;=\; k\begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

Comme toute les droites vectorielles de k^2 sont de cette forme de manière unique, on a montré :

Lemme 4.1. *L'application β est une bijection $\widehat{k} \xrightarrow{\sim} \mathrm{P}^1(k)$.*

Comme on l'a déjà dit, le groupe $\mathrm{GL}_2(k)$ agit naturellement, et transitivement, sur $\mathrm{P}^1(k)$. Cette action n'est pas fidèle : par la Proposition 3.8, son noyau est le sous-groupe $k^\times$ des homothéties, de sorte que le groupe $\mathrm{PGL}_2(k)$ agit fidèlement sur $\mathrm{P}^1(k)$. Par transport de structure via β il agit donc sur $\widehat{k}$ (formule : $g.x = \beta^{-1}(g\beta(x))$). Pour cette action, l'élément $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ de $\mathrm{GL}_2(k)$ envoie le point $x \in \widehat{k}$ sur l'élément

$$g.x = \frac{ax+b}{cx+d} \in \widehat{k}$$

avec l'interprétation usuelle de ce quotient quand $cx+d$ est nul ou $x = \infty$. En effet, soit $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ dans $\mathrm{GL}_2(k)$. Pour $x \in k$ et $cx+d \neq 0$, on a

$$g\begin{pmatrix} x \\ 1 \end{pmatrix} \;=\; \begin{pmatrix} ax+b \\ cx+d \end{pmatrix} \;=\; (cx+d)\begin{pmatrix} \frac{ax+b}{cx+d} \\ 1 \end{pmatrix}, \tag{44}$$

ainsi que $g.(-c/d) = \infty$. De même, on a $g\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} a \\ c \end{pmatrix}$, donc $g.\infty = a/c$ pour $c \neq 0$ et $g.\infty = \infty$ pour $c = 0$.

Définition 4.2. *Les bijections de $\widehat{k}$ de la forme $x \mapsto \frac{ax+b}{cx+d}$ avec $ad - bc \neq 0$ sont appelées homographies. Elles forment un sous-groupe de $\mathrm{S}_{\widehat{k}}$ isomorphe à $\mathrm{PGL}_2(k)$.*

Par exemple $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ correspond à l'homographie affine $x \mapsto ax+b$ sur k (fixant ∞), et $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ à *l'inversion* $x \mapsto 1/x$. On a déjà vu au cours précédent que $\mathrm{PGL}_n(k)$ agit 2-transitivement sur $\mathrm{P}(k^n)$ pour $n \geqslant 2$. Pour $n = 3$ il y a mieux : le groupe $\mathrm{PGL}_2(k)$ agit exactement 3 fois transitivement sur l'ensemble $\mathrm{P}^1(k)$.

Proposition 4.3. *Pour tout triplet (α, β, γ) de points distincts dans $\widehat{k}$, il existe une et une seule homographie $g \in \mathrm{PGL}_2(k)$ telle que $(g(\alpha), g(\beta), g(\gamma)) = (0, 1, \infty)$.*

Cette proposition conduit naturellement à la notion de *birapport*, qui sera abordée en TD.

Démonstration — En effet, $\mathrm{PGL}_2(k)$ agit manifestement transitivement sur $\widehat{k}$, donc on peut supposer $\gamma = \infty$. Le stabilisateur de ∞ dans $\mathrm{PGL}_2(k)$ est exactement l'ensemble des homographies affines, de la forme $x \mapsto ax+b$ avec $a \neq 0$. L'unique telle transformation envoyant (α, β) sur $(0, 1)$ est $x \mapsto (x-\alpha)/(\beta-\alpha)$. $\square$

EXEMPLE 4.4. (*Action de* $\mathrm{SL}_2(\mathbb{R})$ *sur le demi-plan de Poincaré*) L'ensemble $\widehat{\mathbb{C}}$ peut aussi être vu comme la *sphère de Riemann*. Le sous-groupe $\mathrm{GL}_2(\mathbb{R}) \subset \mathrm{GL}_2(\mathbb{C})$ agit sur $\widehat{\mathbb{C}}$ par restriction, en préservant $\widehat{\mathbb{R}}$, ainsi donc son complémentaire $\widehat{\mathbb{C}} \smallsetminus \widehat{\mathbb{R}} = \mathbb{C} - \mathbb{R}$. Cet ouvert de $\mathbb{C}$ a deux composantes connexes, l'une d'elles étant l'ouvert $\mathbb{H} = \{\tau \in \mathbb{C} \mid \operatorname{Im}\tau > 0\}$ appelé *demi-plan de Poincaré*. On vérifie facilement [16] que $\mathbb{H}$ est préservé par $\mathrm{SL}_2(\mathbb{R})$. Cette action est particulièrement importante en géométrie hyperbolique et en théorie des nombres.

Pour p premier, l'action fidèle de $\mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$ sur l'ensemble $\mathrm{P}^1(\mathbb{Z}/p\mathbb{Z}) \simeq \widehat{\mathbb{Z}/p\mathbb{Z}}$ à $p+1$ éléments définit donc un morphisme injectif

$$\mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z}) \hookrightarrow \mathrm{S}_{p+1}. \tag{45}$$

Il est particulièrement intéressant pour les petites valeurs de p. En effet, on a l'égalité $(p+1)! = (p+1)p(p-1)(p-2)!$, de sorte que (miracle !) :

COROLLAIRE 4.5. *Pour $p = 2$ et $p = 3$, le morphisme* (45) *induit des isomorphismes* $\mathrm{PGL}_2(\mathbb{Z}/2\mathbb{Z}) \simeq \mathrm{S}_3$ *et* $\mathrm{PGL}_2(\mathbb{Z}/3\mathbb{Z}) \simeq \mathrm{S}_4$.

Noter que les morphismes naturels

$$\mathrm{PSL}_2(\mathbb{Z}/2\mathbb{Z}) \leftarrow \mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \to \mathrm{PGL}_2(\mathbb{Z}/2\mathbb{Z})$$

sont tous des isomorphismes ! Ainsi, tous ces groupes sont isomorphes à S_3. Cela explique pourquoi $\mathrm{PSL}_2(\mathbb{Z}/2\mathbb{Z})$ n'est pas simple. De même, $\mathrm{PSL}_2(\mathbb{Z}/3\mathbb{Z})$ est d'indice 2 dans $\mathrm{PGL}_2(\mathbb{Z}/3\mathbb{Z}) \simeq \mathrm{S}_4$, et donc on a (Exercice 4.2 Chap. 4)

$$\mathrm{PSL}_2(\mathbb{Z}/3\mathbb{Z}) \simeq \mathrm{A}_4,$$

qui est non simple. Cela justifie les exceptions dans l'énoncé du Théorème 3.1. Ce n'est pas tout, le cas $p = 5$ est également intéressant ! En effet, on a $|\mathrm{PGL}_2(\mathbb{Z}/5\mathbb{Z})| = 120 = |\mathrm{S}_6|/6$, de sorte que $\mathrm{PGL}_2(\mathbb{Z}/5\mathbb{Z})$ est isomorphe à un sous-groupe d'indice 6 de S_6. Mais (pour $n \geqslant 2$) on a la :

PROPOSITION 4.6. *Tout sous-groupe d'indice n de S_n est isomorphe à S_{n-1}.*

DÉMONSTRATION — Soit H un sous-groupe d'indice n de S_n. Faisons agit S_n par translations sur l'ensemble $X = \mathrm{S}_n/H$ à n éléments. Identifions X à $\{1, 2, \ldots, n\}$ en faisant correspondre à $H \in X$ l'élément $n \in \{1, \ldots, n\}$. On en déduit un morphisme $f : \mathrm{S}_n \to \mathrm{S}_n$ tel que $f(H)$ est le stabilisateur de l'élément n dans $f(\mathrm{S}_n)$. Mais f est injectif par le Lemme 5.3 Chap. 4, donc un isomorphisme pour des raisons de cardinal. On a donc $f(\mathrm{S}_n) = \mathrm{S}_n$, $f(H) = \mathrm{S}_{n;n} \simeq \mathrm{S}_{n-1}$, et $H \simeq f(H)$. □

COROLLAIRE 4.7. $\mathrm{PGL}_2(\mathbb{Z}/5\mathbb{Z})$ *est isomorphe à* S_5.

L'action transitive de $\mathrm{PGL}_2(\mathbb{Z}/5\mathbb{Z}) \simeq \mathrm{S}_5$ sur l'ensemble à 6 éléments $\mathrm{P}^1(\mathbb{Z}/5\mathbb{Z})$ est alors une autre réalisation de l'action exotique de S_5 ! Nous renvoyons au Complément §10 Chap. 4 pour une justification et une remarque sur cette assertion. Comme le sous-groupe $\mathrm{PSL}_2(\mathbb{Z}/5\mathbb{Z})$ est d'indice 2 dans $\mathrm{PGL}_2(\mathbb{Z}/5\mathbb{Z}) \simeq \mathrm{S}_5$, on en déduit

$$\mathrm{PSL}_2(\mathbb{Z}/5\mathbb{Z}) \simeq \mathrm{A}_5,$$

16. Pour $g \in \mathrm{GL}_2(\mathbb{R})$ et $z \in \mathbb{C} - \mathbb{R}$, on a la formule $\operatorname{Im} g.z = \det g \, \frac{\operatorname{Im} z}{|cz+d|^2}$. Sans calcul, on peut aussi utiliser la connexité de $\mathrm{SL}_2(\mathbb{R})$.

un isomophisme là encore exceptionnel. En effet, cela ne se reproduit plus pour p plus grand :

Proposition 4.8. *Soient $n, p \geqslant 5$ avec p premier. On a $\mathrm{A}_n \simeq \mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$ si, et seulement si, $n = p = 5$.*

Démonstration — Observons que l'élément t_2 est d'ordre p dans $\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$ (car $p \neq 2$). Ainsi, si on a un isomorphisme $\mathrm{A}_n \simeq \mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$ alors A_n possède un élément d'ordre p. Mais un élément d'ordre p dans S_n est un produit d'un certain nombre de p-cycles à supports disjoints. On a donc $n \geqslant p$. Comme pour $p \geqslant 5$ on a $3 \leqslant (p+1)/2 \leqslant p-2$ pour $p \geqslant 5$, on a aussi les inégalités immédiates

$$|\mathrm{A}_n| \;=\; n!/2 \;\geqslant\; p!/2 \;\geqslant\; p(p-1)(p+1)/2 \;=\; |\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})|$$

Ces sont des égalités si, et seulement si, on a $n = p$ (pour la première) et $p = 5$ (pour la seconde !). ☐

Remarque 4.9. (*Autres isomorphismes exceptionnels*) Parmi les groupes simples de la forme A_n et $\mathrm{PSL}_n(\mathbb{Z}/p\mathbb{Z})$, les seuls isomorphismes sont en fait

$$\mathrm{A}_5 \simeq \mathrm{PSL}_2(\mathbb{Z}/5\mathbb{Z}),\;\; \mathrm{PSL}_2(\mathbb{Z}/7\mathbb{Z}) \simeq \mathrm{PSL}_3(\mathbb{Z}/2\mathbb{Z}) \;\text{ et }\; \mathrm{PSL}_4(\mathbb{Z}/2\mathbb{Z}) \simeq \mathrm{A}_8.$$

Si l'on s'autorise des corps finis $\mathbb{F}_q$ plus généraux que $\mathbb{Z}/p\mathbb{Z}$, on a aussi $\mathrm{A}_5 \simeq \mathrm{PSL}_2(\mathbb{F}_4)$, $\mathrm{A}_6 \simeq \mathrm{PSL}_2(\mathbb{F}_9)$, et le fait que $\mathrm{PSL}_3(\mathbb{F}_4)$ a même ordre que A_8 mais ne lui est pas isomorphe.

Les miracles ne s'arrêtent en fait pas là. Les groupes $\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$ avec $p = 7$ et 11 ont également des comportements inhabituels, comme l'avait expliqué Galois dans sa fameuse lettre à son ami Chevalier, écrite le jour avant le duel qui causa sa mort. Le groupe $\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$ agit transitivement sur $\mathrm{P}^1(\mathbb{Z}/p\mathbb{Z})$, qui a $p+1$ éléments. Galois se demande s'il agit aussi transitivement sur un ensemble à $1 < n \leqslant p$ éléments (nécessairement fidèlement pour $p \geqslant 5$). Une condition nécessaire, comme ci-dessus, est $p \,|\, n!$, et donc $p = n$.

Théorème 4.10. (Galois) *Le groupe $\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$ agit transitivement sur un ensemble à p éléments si, et seulement si, on a $p \leqslant 11$. Pour $p = 5, 7, 11$ les stabilisateurs de ces actions exceptionnelles sont respectivement isomorphes aux groupes platoniciens A_4, S_4 et A_5.*

Nous renvoyons à cette note de votre serviteur pour une démonstration élémentaire de cet énoncé. Nous nous contenterons d'observer ici que la question est équivalente à savoir si $\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$ possède un sous-groupe d'indice p, *i.e.* d'ordre $\frac{p^2-1}{2}$, et de constater la coïncidence numérique

$$\frac{p^2-1}{2} = 12,\; 24 \text{ et } 60, \;\text{ pour } p \;=\; 5,\; 7 \text{ et } 11,$$

qui sont les cardinaux respectifs des groupes A_4, S_4 et A_5. Pour $p = 2$ et 3, les actions transitives en question se déduisent de celles de $\mathrm{PSL}_2(\mathbb{Z}/2\mathbb{Z}) \simeq \mathrm{S}_3$ et $\mathrm{PSL}_2(\mathbb{Z}/3\mathbb{Z}) \simeq \mathrm{A}_4$ sur 2 et 3 éléments respectivement (lesquelles ?). Pour $p = 5$, on vu $\mathrm{PSL}_2(\mathbb{Z}/5\mathbb{Z}) \simeq \mathrm{A}_5$, qui agit bien transitivement sur 5 éléments. Ces comportement inhabituels pour $p = 7$ et 11 se sont avérés être aussi la clé de la construction de plusieurs des *groupes sporadiques*, comme les groupes de Mathieu : voir l'article *Three lectures on exceptional groups*, par J. Conway.