SUR LES ACTIONS DE $\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$ SUR p ÉLÉMENTS DANS LA LETTRE DE GALOIS À CHEVALIER

GAËTAN CHENEVIER

RÉSUMÉ. Dans cette note d'exposition, nous revenons sur la classification des actions exceptionnelles de $\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$ sur un ensemble à p éléments, annoncée par Galois dans sa dernière lettre à Chevalier.

1. INTRODUCTION

Soit p un nombre premier. On considère le groupe

$$\mathrm{L}_2(p) := \mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})/\{\pm 1\}.$$

On sait bien qu'il agit fidèlement et 2-transitivement sur la droite projective

$$\mathrm{P}^1(\mathbb{Z}/p\mathbb{Z}) = \mathbb{Z}/p\mathbb{Z} \coprod \{\infty\},$$

qui a $p+1$ éléments. Dans sa fameuse lettre à Chevalier [G] en 1832, Galois pose la question de savoir si $\mathrm{L}_2(p)$ peut agir non trivialement sur un ensemble à $\leq p$ éléments. Comme $\mathrm{L}_2(p)$ est engendré par ses transvections, qui sont d'ordre p, la seule possibilité est celle d'une action *transitive* sur p éléments. Il est équivalent de demander si $\mathrm{L}_2(p)$ possède un sous-groupe d'indice p, *i.e.* d'ordre $\frac{p^2-1}{2}$ pour $p > 2$. La découverte de Galois, annoncée dans sa lettre, est alors la suivante :

Théorème 1. (Galois) *Le groupe* $\mathrm{L}_2(p)$ *possède une action transitive sur un ensemble à* p *éléments si, et seulement si, on a* $p \leq 11$.

Ajoutons que pour $p \leq 5$, il existe en fait une *unique* action de $\mathrm{L}_2(p)$ sur p éléments à équivalence près, alors que pour $p = 7$ et 11, il en existe exactement deux, conjuguées extérieures l'une de l'autre sous l'action naturelle de $\mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$ par automorphismes de $\mathrm{L}_2(p)$. Ces actions exceptionnelles de $\mathrm{L}_2(p)$ pour $p \leq 11$ ont fasciné de nombreux mathématiciens : voir par exemple Conway [C] et Kostant [K]. Pour $p = 5, 7$ et 11, leurs stabilisateurs, qui sont d'ordre $\frac{p^2-1}{2} = 12, 24$ et 60, sont respectivement isomorphes aux groupes A_4, S_4 et A_5 des rotations des solides platoniciens. Nous verrons qu'une manière simple de démontrer l'existence de ces actions, et cette propriété de leurs stabilisateurs, consiste à contempler les polyèdres réguliers suivants étiquetés par $\mathrm{P}^1(\mathbb{Z}/p\mathbb{Z})$, et à constater que leurs isométries

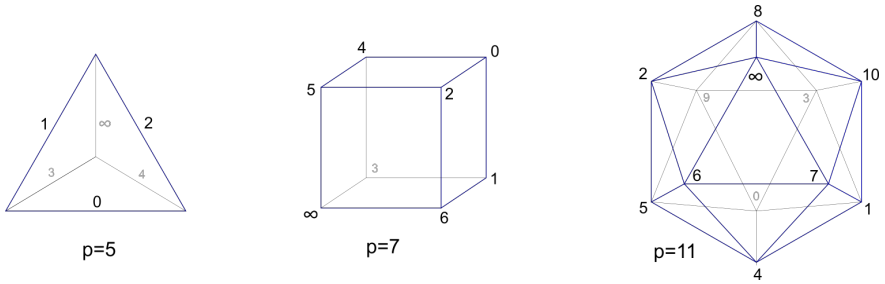


FIGURE 1.

directes sont induites par des homographies de $\mathrm{P}^1(\mathbb{Z}/p\mathbb{Z})$ appartenant à $\mathrm{L}_2(p)$. Ce

L'auteur est financé par le CNRS et soutenu par le projet ANR-19-CE40-0015-02. Il remercie le rapporteur pour ses remarques utiles.

dernier fait se vérifie aisément sur des rotations génératrices bien choisies, et nous reviendrons en détail sur cette vérification plus loin (Proposition 1).

Le but de cette modeste note est de donner une démonstration élémentaire du Théorème 1 qui semble dans l'esprit des méthodes de Galois, et qui soit accessible aux étudiants d'un premier cours de théorie des groupes. Notre approche figure peut-être déjà quelque part dans la littérature, mais nous n'avons pas été capable de la localiser. Galois lui-même ne donne que peu d'indications dans [G]. Plusieurs références, dont Conway et Kostant, renvoient à Huppert [H] p. 214 pour une preuve du Théorème ci-dessus. L'approche de Huppert, bien que naturelle, est assez indirecte : elle utilise des éléments de la classification de Dickson des sous-groupes d'ordre premier à p de $\mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$ (en fait, un tel sous-groupe se plonge dans $\mathrm{SO}(3)$, et donc est cyclique, diédral, ou isomorphe à A_4, S_4 ou A_5).

Mentionnons pour finir que les actions exceptionnelles ci-dessus pour $p \leq 7$ peuvent aussi s'expliquer à l'aide des isomorphismes exceptionnels classiques :

$$\mathrm{L}_2(2) \simeq \mathrm{S}_3,\ \mathrm{L}_2(3) \simeq \mathrm{A}_4,\ \mathrm{L}_2(5) \simeq \mathrm{A}_5 \text{ et } \mathrm{L}_2(7) \simeq \mathrm{GL}_3(\mathbb{Z}/2\mathbb{Z}).$$

Par exemple pour $p = 7$, le groupe $\mathrm{GL}_3(\mathbb{Z}/2\mathbb{Z}) \simeq \mathrm{L}_2(7)$ agit transitivement sur l'ensemble $(\mathbb{Z}/2\mathbb{Z})^3 - \{0\}$ à 7 éléments, ou encore sur l'ensemble des formes linéaires non nulles sur $(\mathbb{Z}/2\mathbb{Z})^3$, aussi à 7 éléments. Ces deux actions sont non isomorphes : les stabilisateurs sont des "paraboliques" non conjugués, et tous deux isomorphes à $\mathrm{S}_4 \simeq (\mathbb{Z}/2\mathbb{Z})^2 \rtimes \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$. Le cas $p = 11$ est plus subtil, et profondément relié à l'existence du groupe de Mathieu M_{12} : voir [C]. Nous renvoyons aux articles susmentionnés de Conway et Kostant pour de nombreux autres développements et points de vue sur ces constructions. Mentionnons que l'on peut montrer plus généralement, par exemple par *réduction modulo p*, que pour $p > 2$, le groupe A_4 se plonge dans $\mathrm{L}_2(p)$, et le groupe S_4 (resp. A_5) se plonge dans $\mathrm{L}_2(p)$ si, et seulement si, 2 (resp. 5) est un carré modulo p.

2. Démonstration du Théorème 1

Commençons par quelques rappels préliminaires sur $\mathrm{L}_2(p)$. Soit p un nombre premier. On identifiera de manière usuelle la droite projective $\mathrm{P}^1(\mathbb{Z}/p\mathbb{Z})$ sur le corps $\mathbb{Z}/p\mathbb{Z}$ avec l'ensemble $\mathbb{Z}/p\mathbb{Z} \coprod \{\infty\}$. Le groupe

$$\mathrm{L}_2(p)^+ := \mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z}) = \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})/(\mathbb{Z}/p\mathbb{Z})^\times$$

agit donc naturellement sur $\mathrm{P}^1(\mathbb{Z}/p\mathbb{Z})$ par homographies, une action que l'on notera $(g, z) \mapsto g.z$ et qui vérifie $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right).z = \frac{az+b}{cz+d}$ avec les conventions usuelles relatives au symbole ∞. Pour des raisons générales, cette action est fidèle et exactement 3-transitive. En particulier, de $|\mathrm{P}^1(\mathbb{Z}/p\mathbb{Z})| = p + 1$ on déduit

$$|\mathrm{L}_2(p)^+| \ = \ (p+1)p(p-1) = p^3 - p. \tag{1}$$

On note C_p le sous-groupe des carrés de $(\mathbb{Z}/p\mathbb{Z})^\times$ et N_p l'ensemble des non carrés de $\mathbb{Z}/p\mathbb{Z}$, de sorte qu'on a la partition $\mathbb{Z}/p\mathbb{Z} = \{0\} \coprod \mathrm{C}_p \coprod \mathrm{N}_p$. L'inclusion $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ et le déterminant $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}) \to (\mathbb{Z}/p\mathbb{Z})^\times$ induisent une suite exacte courte

$$1 \longrightarrow \mathrm{L}_2(p) \longrightarrow \mathrm{L}_2(p)^+ \longrightarrow (\mathbb{Z}/p\mathbb{Z})^\times/\mathrm{C}_p \to 1. \tag{2}$$

Nous identifierons ainsi $\mathrm{L}_2(p)$ au sous-groupe de $\mathrm{L}_2(p)^+$ constitué des classes des matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ de déterminant $ad-bc$ dans C_p, et on écrira simplement $\mathrm{L}_2(p) \subset \mathrm{L}_2(p)^+$. Traitons à part le cas $p = 2$.

Exemple 1. (Cas $p = 2$). *On a trivialement* $\mathrm{L}_2(2) = \mathrm{L}_2(2)^+$. *Le groupe* $\mathrm{L}_2(2)^+$ *a* 6 *éléments, et son action fidèle sur l'ensemble* $\mathrm{P}^1(\mathbb{Z}/2\mathbb{Z})$, *a trois éléments, fournit donc un isomorphisme* $\mathrm{L}_2(2) \simeq \mathrm{S}_3$. *Le groupe* S_3 *possède un unique sous-groupe d'ordre* 3, *et donc une unique action transitive sur l'ensemble* $\{1, 2\}$, *obtenue en composant la signature* $\mathrm{S}_3 \to \{\pm 1\}$ *et l'isomorphisme* $\{\pm 1\} \simeq \mathrm{S}_2$.

On suppose donc désormais $p > 2$. Dans ce cas, on sait depuis Euler que C_p est d'indice 2 dans $(\mathbb{Z}/p\mathbb{Z})^\times$, de sorte que l'on a $|\mathrm{C}_p| = |\mathrm{N}_p| = \frac{p-1}{2}$, puis $|\mathrm{L}_2(p)| = \frac{p^3-p}{2}$ par (1) et (2). Les éléments familiers suivants de $\mathrm{L}_2(p)$ joueront un rôle important

$$\alpha := \pm\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},\ \mathrm{t}_\lambda := \pm\begin{pmatrix} \mu & 0 \\ 0 & \mu^{-1} \end{pmatrix} \text{ et } \gamma := \pm\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

où λ désigne un élément de C_p quelconque, et μ est l'élément de $(\mathbb{Z}/p\mathbb{Z})^\times$, unique au signe près, vérifiant $\mu^2 = \lambda$. Pour $z \in \mathrm{P}^1(\mathbb{Z}/p\mathbb{Z})$, on a donc $\alpha.z = z + 1$, $\mathrm{t}_\lambda.z = \lambda z$ et $\gamma.z = -1/z$. L'élément α est d'ordre p et γ est d'ordre 2. La seule chose que l'on utilisera [1] sur $\mathrm{L}_2(p)$ est le fait très classique qu'il est engendré par ses deux *transvections standards* α et $\gamma\alpha\gamma^{-1}$, et en particulier que l'on a :

Lemme 1. *Le groupe* $\mathrm{L}_2(p)$ *est engendré par* α *et* γ.

On notera $T \subset \mathrm{L}_2(p)$ le sous-groupe diagonal, constitué des t_λ avec $\lambda \in \mathrm{C}_p$. Le cas $p = 3$ est un peu particulier, car on a $\mathrm{C}_3 = \{1\}$ et donc $T = 1$, c'est pourquoi nous le traitons aussi à part en exemple.

Exemple 2. (Cas $p = 3$). *On a* $|\mathrm{L}_2(3)^+| = 3^3 - 3 = 24 = |\mathrm{S}_4|$ *et* $|\mathrm{P}^1(\mathbb{Z}/3\mathbb{Z})| = 4$. *L'action par homographies donne alors l'isomorphisme exceptionnel classique* $\mathrm{L}_2(3)^+ \simeq \mathrm{S}_4$. *Mais il est bien connu que* S_n *a un unique sous-groupe d'indice* 2 *pour tout* $n \geq 2$, *à savoir* A_n, *de sorte que l'on a aussi* $\mathrm{L}_2(3) \simeq \mathrm{A}_4$. *Le groupe* A_4 *possède un unique sous-groupe d'ordre* 4, *à savoir celui* $\simeq (\mathbb{Z}/2\mathbb{Z})^2$ *constitué de l'identité et de ses trois doubles-transpositions. Il y a donc bien une action transitive de* $\mathrm{L}_2(3)$ *sur* 3 *éléments, et elle est unique à équivalence près.*

Notre point de départ dans la démonstration du Théorème 1 est le lemme suivant.

Lemme 2. *Soit* $\centerdot$ *une action non triviale de* $\mathrm{L}_2(p)$ *sur un ensemble à* p *éléments avec* $p > 3$. *Alors l'action* $\centerdot$ *est transitive, et il existe* $a, b \in (\mathbb{Z}/p\mathbb{Z})^\times$ *tels que* $\centerdot$ *est équivalente à une action* $\star$ *de* $\mathrm{L}_2(p)$ *sur* $\mathbb{Z}/p\mathbb{Z}$ *vérifiant :*

(i) $\alpha \star x = x + 1$ *pour tout* $x \in \mathbb{Z}/p\mathbb{Z}$,

(ii) $\mathrm{t}_\lambda \star x = \lambda x$ *pour tout* $\lambda \in \mathrm{C}_p$ *et* $x \in \mathbb{Z}/p\mathbb{Z}$,

(iii) $\gamma \star 0 = 0$, $\gamma \star x = a/x$ *pour* $x \in \mathrm{C}_p$, *et* $\gamma \star x = b/x$ *pour* $x \in \mathrm{N}_p$.

Preuve — Supposons donnée une action non triviale $\centerdot$ de $\mathrm{L}_2(p)$ sur un ensemble X à p éléments. Quitte à la remplacer par une action équivalente, on peut supposer $X = \mathbb{Z}/p\mathbb{Z}$. Si l'élément α de $\mathrm{L}_2(p)$ agit trivialement sur X, il en va de même de son conjugué $\gamma\alpha\gamma^{-1}$, puis de tout $\mathrm{L}_2(p)$ par le Lemme 1, contredisant la non trivialité de $\centerdot$. Ainsi, l'élément α, qui est d'ordre p dans $\mathrm{L}_2(p)$, agit comme un p-cycle sur X. Quitte à conjuguer l'action $\centerdot$ par un élément de S_X, on peut donc supposer $\alpha \centerdot x = x + 1$ pour tout $x \in X$, ce qui montre le (i).

Fixons $\lambda \in \mathrm{C}_p$. La relation immédiate $\mathrm{t}_\lambda\, \alpha = \alpha^\lambda\, \mathrm{t}_\lambda$ dans $\mathrm{L}_2(p)$ entraîne

$$\mathrm{t}_\lambda \centerdot (x + 1) = \mathrm{t}_\lambda \centerdot x + \lambda \text{ pour tout } x \in X.$$

1. En particulier, nous n'utiliserons pas la simplicité de $\mathrm{L}_2(p)$ pour $p > 3$.

On en déduit $\mathrm{t}_\lambda \centerdot x = \lambda\, x + \mathrm{t}_\lambda \centerdot 0$ pour tout $x \in X$. En particulier, pour $\lambda \neq 1$ l'élément t_λ a un unique point fixe dans X, à savoir $\frac{\mathrm{t}_\lambda \centerdot 0}{1-\lambda}$. Comme T est commutatif, les t_λ avec $\lambda \in \mathrm{C}_p \smallsetminus \{1\}$ ont tous même point fixe dans $\mathbb{Z}/p\mathbb{Z}$, notons-le k. Quitte à conjuguer l'action $\centerdot$ par la bijection α^k de X, ce qui ne change pas l'action de l'élément α, on peut finalement supposer $k = 0$, et donc $t \centerdot 0 = 0$ pour tout $t \in T$. On a montré que $\centerdot$ satisfait (i) et (ii).

Enfin, la relation $\gamma\, \mathrm{t}_\lambda = \mathrm{t}_{\lambda^{-1}}\, \gamma$ dans $\mathrm{L}_2(p)$ pour $\lambda \in \mathrm{C}_p$ implique

$$\gamma \centerdot (\lambda x) = \frac{\gamma \centerdot x}{\lambda} \text{ pour tout } x \in \mathbb{Z}/p\mathbb{Z} \text{ et tout } \lambda \in \mathrm{C}_p. \tag{3}$$

Cette identité entraîne $\gamma \centerdot 0 = 0$ en prenant $x = 0$ et $\lambda \neq 1$ (un tel λ existe pour $p > 3$). On en déduit $\gamma \centerdot (\mathbb{Z}/p\mathbb{Z})^\times = (\mathbb{Z}/p\mathbb{Z})^\times$, puis l'identité (3) conclut en posant $a := \gamma \centerdot 1$ et $b := n\,(\gamma \centerdot n)$ pour $n \in \mathrm{N}_p$ quelconque. □

Dans toute la suite, on suppose définitivement $p > 3$. D'après le Lemme 1, étant donnés $a, b \in (\mathbb{Z}/p\mathbb{Z})^\times$ il existe au plus une action de $\mathrm{L}_2(p)$ sur $\mathbb{Z}/p\mathbb{Z}$ vérifiant les points (i) et (iii) du Lemme 2.

Définition 1. *Pour $a, b \in (\mathbb{Z}/p\mathbb{Z})^\star$, on note $\star_{a,b}$ l'unique action de $\mathrm{L}_2(p)$ sur $\mathbb{Z}/p\mathbb{Z}$ vérifiant les assertions (i), (ii) et (iii) du Lemme 2, si elle existe.*

Lemme 3. *Soient $a, a', b, b' \in (\mathbb{Z}/p\mathbb{Z})^\times$ tels que $\star_{a,b}$ et $\star_{a',b'}$ existent. On a*

$$\star_{a,b} \simeq \star_{a',b'} \iff a = a' \text{ et } b = b'.$$

Preuve — Supposons qu'il existe une bijection $\sigma : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ vérifiant

$$\sigma(\, g \star_{a,b} x\,) = g \star_{a',b'} \sigma(x) \text{ pour tout } x \in \mathbb{Z}/p\mathbb{Z} \text{ et tout } g \in \mathrm{L}_2(p). \tag{4}$$

Pour $g = \alpha$ on en déduit $\sigma(x+1) = \sigma(x) + 1$ pour tout $x \in \mathbb{Z}/p\mathbb{Z}$, et donc $\sigma(x) = x + \sigma(0)$. En prenant $g = \mathrm{t}_\lambda$ on a aussi $\sigma(\lambda x) = \lambda\sigma(x)$ pour tout $x \in \mathbb{Z}/p\mathbb{Z}$ et $\lambda \in \mathrm{C}_p$. En considérant $\lambda \neq 1$, ce qui est loisible car on a $p > 3$, on a donc $\sigma(0) = 0$, puis $\sigma = \mathrm{id}$, et enfin $(a, b) = (a', b')$ en prenant $g = \gamma$ dans (4). □

Lemme 4. *Soient $a, b \in (\mathbb{Z}/p\mathbb{Z})^\times$ tels que $\star_{a,b}$ existe. Alors, la conjuguée de $\star_{a,b}$ par un élément de $\mathrm{L}_2(p)^+ \smallsetminus \mathrm{L}_2(p)$ est isomorphe à $\star_{b,a}$. En particulier, $\star_{b,a}$ existe.*

Preuve — Fixons $n \in \mathrm{N}_p$ et notons $\theta \in \mathrm{L}_2(p)^+$ la classe de l'élément diagonal $\left(\begin{smallmatrix} n & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Alors θ engendre $\mathrm{L}_2(p)^+/\mathrm{L}_2(p) \simeq \mathbb{Z}/2\mathbb{Z}$ et pour tout $z \in \mathrm{P}^1(\mathbb{Z}/p\mathbb{Z})$ on a $\theta.z = nz$. Notons $\centerdot$ la conjuguée extérieure de l'action $\star_{a,b}$ par θ. On a

$$g \centerdot x = (\theta\, g\, \theta^{-1}) \star_{a,b} x \text{ pour tout } x \in \mathbb{Z}/p\mathbb{Z} \text{ et tout } g \in \mathrm{L}_2(p)$$

par définition. La relation $\theta\, \alpha\, \theta^{-1} = \alpha^n$ dans $\mathrm{L}_2(p)$ entraîne $\alpha \centerdot x = x + n$. Soit $\sigma : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ la bijection $x \mapsto nx$, et considérons l'action $*$ de $\mathrm{L}_2(p)$ sur $\mathbb{Z}/p\mathbb{Z}$ définie par $g * x = \sigma^{-1}(g \centerdot \sigma(x)) = n^{-1}(g \centerdot nx)$. Alors $*$ est équivalente à $\centerdot$ par définition, et satisfait $\alpha * x = x + 1$. La relation évidente $\theta\, \mathrm{t}_\lambda\, \theta^{-1} = \mathrm{t}_\lambda$ dans $\mathrm{L}_2(p)^+$ montre de plus $\mathrm{t}_\lambda * x = \lambda x$. Enfin, la bijection σ fixe 0 et échange C_p et N_p, et on a la relation $\theta\, \gamma\, \theta^{-1} = \mathrm{t}_{n^2}\, \gamma$ dans $\mathrm{L}_2(p)^+$. On en déduit $\gamma * 0 = 0$,

$$\gamma * x = n^{-1}(\, n^2\, b/(nx)\,) = b/x \text{ pour } x \in \mathrm{C}_p,$$

et de même $\gamma * x = a/x$ pour $x \in \mathrm{N}_p$. On a montré $* = \star_{b,a}$. □

Dans tout ce qui suit, on fixe $a, b \in (\mathbb{Z}/p\mathbb{Z})^\times$ et on suppose que $\star_{a,b}$ existe. On rappelle en outre $p > 3$. Pour ne pas trop alourdir les notations on posera

$$g(x) := g \star_{a,b} x \text{ pour } g \in \mathrm{L}_2(p) \text{ et } x \in \mathbb{Z}/p\mathbb{Z}.$$

Il ne faudra donc pas confondre $g(x)$ et $g.x$ (action par homographie). L'idée de la démonstration est de considérer l'élément

$$\delta := \alpha\gamma \in \mathrm{L}_2(p).$$

Cet élément agit par $\delta.z = 1 - 1/z$ sur $\mathrm{P}^1(\mathbb{Z}/p\mathbb{Z})$, et donc par le 3-cycle $(1\,0\,\infty)$ sur $\{0, 1, \infty\} \subset \mathrm{P}^1(\mathbb{Z}/p\mathbb{Z})$. En particulier, on a la relation bien connue $\delta^3 = 1$ dans $\mathrm{L}_2(p)$. Concernant l'action $\star_{a,b}$, on a $\delta(0) = 1$, $\delta(x) = 1 + a/x$ pour $x \in \mathrm{C}_p$ et $\delta(x) = 1 + b/x$ pour $x \in \mathrm{N}_p$.

Lemme 5. *La décomposition en cycles de l'élément δ agissant sur $\mathbb{Z}/p\mathbb{Z}$ via $\star_{a,b}$ contient le 3-cycle $(0\ 1\ a+1)$. En particulier, nous avons $a \notin \{0, -1\}$.*

Preuve — La relation $\delta^3 = 1$ dans $\mathrm{L}_2(p)$ montre que δ agit sur $\mathbb{Z}/p\mathbb{Z}$ via $\star_{a,b}$ par un élément d'ordre divisant 3. On conclut car il envoie 0 sur 1 et 1 sur $1 + a$. □

Lemme 6. *On a l'égalité $a + b = -1$. De plus, si -1 est dans C_p on a en outre $a = b = -1/2$.*

Preuve — On a $\delta^{-1}(0) = \gamma\alpha^{-1}(0) = \gamma(-1)$. Par le Lemme 5, on a aussi $\delta^{-1}(0) = a + 1$, et donc $\gamma(-1) = a + 1$. Si -1 est un carré, on a donc $-a = 1 + a$, puis $a = -1/2$, et aussi $b = -1/2$ en considérant l'action $\star_{b,a}$ (Lemme 4). Sinon, on a $-b = 1 + a$. Dans tous les cas, on constate $a + b = -1$. □

Lemme 7. *Supposons $a = b$. Alors on a $p = 5$ et $a = b = -1/2$.*

Preuve — L'égalité $a + b = -1$ montre $a = b = -1/2$, puis $\delta(x) = 1 - \frac{1}{2x}$ pour tout $x \in (\mathbb{Z}/p\mathbb{Z})^\times$. Un calcul montre $\delta(-1) = 3/2$, $\delta^2(-1) = 2/3$ et $\delta^3(-1) = 1/4$. On a donc $-1 = 1/4$, puis $5 = 0$. □

Lemme 8. *Supposons $a \neq b$. Alors a et b sont dans C_p et on a $-1 \in \mathrm{N}_p$.*

Preuve — On a $-1 \in \mathrm{N}_p$ par le Lemme 6. Par définition, l'involution γ de $\mathrm{L}_2(p)$ agit sur $(\mathbb{Z}/p\mathbb{Z})^\times$ via $\star_{a,b}$ en préservant $\{\mathrm{C}_p, \mathrm{N}_p\}$. Si elle échange C_p et N_p, on a $a = \gamma(1) \in \mathrm{N}_p$ et donc $1 = \gamma^2(1) = b/a$, puis $b = a$: absurde. On a donc $\gamma(\mathrm{C}_p) = \mathrm{C}_p$ et $\gamma(\mathrm{N}_p) = \mathrm{N}_p$, *i.e.* a et b sont des carrés. □

On étudie d'abord le cas particulier $\{a, b\} \subset \{-3, -2, 1, 2\}$ avec $a \neq b$. Comme les ensembles $\{-3, -2, 1, 2\}$ et $\{a, b\}$ sont stables par $x \mapsto -1 - x$, il n'y a que deux cas, à savoir $\{a, b\} = \{1, -2\}$, et $\{a, b\} = \{2, -3\}$ pour $p \neq 5$.

Lemme 9. *Supposons $\{a, b\} = \{1, -2\}$. Alors on a $p = 11$.*

Preuve — On peut supposer $a = 1$ et $b = -2$ par le Lemme 4. On a $a \neq b$ car p est > 3, et donc $-1 \in \mathrm{N}_p$ par le Lemme 8, puis $\delta(-1) = 3$ (non nul). Si 3 est dans C_p, on a $\delta(3) = 4/3 \in \mathrm{C}_p$ puis $\delta(4/3) = 7/4$. On a donc $-1 = 7/4$, puis $11 = 4 + 7 = 0$ et $p = 11$. Si 3 est dans N_p, on constate $\delta(3) = 1/3 \in \mathrm{N}_p$, puis $\delta(1/3) = -5$, et donc $-1 = -5$ et $4 = 0$: une contradiction. □

Lemme 10. *Supposons $\{a,b\}=\{2,-3\}$ et $p\neq 5$. Alors on a $p=7$.*

Preuve — On peut supposer $a=2$ et $b=-3$. On a $2\in \mathrm{C}_p$ et $-1\in \mathrm{N}_p$ par le Lemme 8, puis $-2\in \mathrm{N}_p$. On a donc $\delta(-2)=5/2$ (non nul). Si 5 est dans N_p, on a $5/2\in \mathrm{N}_p$ puis $\delta(5/2)=-1/5\in \mathrm{C}_p$ et $\delta(-1/5)=-9$. On a donc $-2=-9$ puis $7=0$. Si 5 est dans C_p, on a $5/2\in \mathrm{C}_p$ puis $\delta(5/2)=9/5\in \mathrm{C}_p$ et $\delta(9/5)=19/9$. On a donc $-2=19/9$ puis $37=0$, une contradiction car -1 est dans C_{37}. □

D'après ces deux derniers lemmes, pour conclure la condition nécéssaire $p\leq 11$ de l'énoncé du Théorème 1, il ne reste qu'à démontrer le :

Lemme 11. *On a l'inclusion $\{a,b\}\subset\{-3,-2,1,2\}$ dans $\mathbb{Z}/p\mathbb{Z}$.*

Preuve — On a $\{a,b\}\cap\{0,-1\}=\emptyset$ par le Lemme 5. Le lemme est donc évident pour $p=5$, et on peut supposer $p>5$. Les ensembles $\{-3,-2,1,2\}$ et $\{a,b\}$ étant stables par $x\mapsto -1-x$, il suffit de montrer que a ou b est dans $\{-3,-2,1,2\}$. D'après les Lemmes 6, 7 et 8, on a $a\neq b$ ainsi que $a,b\in \mathrm{C}_p$ et $-1\in \mathrm{N}_p$. Comme b est dans C_p, on a $\delta(b)=1+a/b=(a+b)/b=-1/b\in \mathrm{N}_p$, puis

$$\delta(-1/b)=1-b^2=(1-b)(1+b)=a(b-1).$$

Dans le cas $b=1$, on a terminé. Si $b-1$ est dans C_p, alors $a(b-1)\in \mathrm{C}_p$ puis

$$b=\delta^3(b)=\delta(a(b-1))=1+1/(b-1)=b/(b-1).$$

Cela montre $b=b/(b-1)$ puis $b=2$, ce qui conclut encore. Supposons enfin $b-1\in \mathrm{N}_p$. Nous allons voir que ce cas est impossible. On a en effet

$$b=\delta^3(b)=\delta(1-b^2)=1+b/(1-b^2).$$

On en déduit que b est racine du polynôme

$$P=T^3-T^2+1.$$

Par symétrie, *i.e.* en appliquant le raisonnement ci-dessus à l'action $\star_{b,a}$ qui existe par le Lemme 4, on en déduit que a est aussi racine de P. Mais on a $a\neq b$, de sorte que si c désigne la 3-ème racine de P, on a $a+b+c=1$, puis $c=2$ car $a+b=-1$, et donc $5=2^3-2^2+1=0$, ce qui contredit $p>5$. □

Remarque 1. *Donnons un autre argument montrant $p\leq 19$ à partir du Lemme 8. Observons d'abord qu'il existe $\frac{p+1}{4}$ eléments $x\in \mathrm{C}_p$ tels que $x+a\in \mathrm{N}_p$. En effet, la conique $u^2+v^2=-a$ possède exactement $p+1$ solutions $(u,v)\in(\mathbb{Z}/p\mathbb{Z})^2$, car elle n'a pas de solutions à l'infini (-1 non carré). De plus, $-a$ n'est pas un carré, donc pour tout (u,v) solution on a $u\neq 0$ et $v\neq 0$, d'où l'observation. Considérons maintenant $x\in \mathrm{C}_p$ tel que $x+a\in \mathrm{N}_p$. On a $\delta(x)=(x+a)/x\in \mathrm{N}_p$, donc*

$$\delta^2(x)=1+bx/(x+a)=(x+a+bx)/(x+a)=a(1-x)/(x+a)=\delta^{-1}(x)$$

Écartons $x=1$, qui vérifie bien $\delta^3(1)=1$. On a alors

$$\delta^{-1}(x)=\gamma\tau^{-1}(x)=\gamma(x-1)=a/(x-1)\text{ ou }b/(x-1).$$

Ainsi, que l'on ait $x-1\in \mathrm{N}_p$ ou $x-1\in \mathrm{C}_p$, l'équation $\delta^3(x)=x$ est quadratique en x et a donc au plus 2 solutions. Par l'observation précédente, on a $\frac{p+1}{4}\leq 1+2+2=5$.

Au final, nous avons montré que si $\star_{a,b}$ existe, il y a au plus 5 possibilités pour le triplet (p,a,b), résumées dans la table ci-dessous. Les colonnes 3 et 4 donnent $\gamma(x)$ pour $x\neq 0$, les colonnes 5 et 6 les décompositions en cycles de γ et de $\delta=\alpha\gamma$ agissant sur $\mathbb{Z}/p\mathbb{Z}$ via $\star_{a,b}$, et la colonne 7 donne les points fixes $f\in\mathbb{Z}/p\mathbb{Z}$ de δ.

p	(a,b)	$x \in \mathrm{C}_p$	$x \in \mathrm{N}_p$	γ	$\alpha\gamma$	f
5	$(-1/2,-1/2)$	$2/x$	$2/x$	$(1\,2)\,(3\,4)$	$(0\,1\,3)$	$2,4$
7	$(2,-3)$	$2/x$	$4/x$	$(1\,2)\,(3\,6)$	$(0\,1\,3)\,(4\,5\,6)$	2
7	$(-3,2)$	$4/x$	$2/x$	$(1\,4)\,(5\,6)$	$(0\,1\,5)\,(2\,3\,4)$	6
11	$(1,-2)$	$1/x$	$9/x$	$(2\ 10)\,(3\,4)\,(5\,9)\,(6\,7)$	$(0\,1\,2)\,(3\,5\,10)\,(6\,8\,9)$	$4,7$
11	$(-2,1)$	$9/x$	$1/x$	$(1\,9)\,(2\,6)\,(4\,5)\,(7\,8)$	$(0\,1\,10)\,(2\,7\,9)\,(3\,4\,6)$	$5,8$

TABLE 1. Les actions de γ et $\alpha\gamma$ sur $\mathbb{Z}/p\mathbb{Z}$ via $\star_{a,b}$.

Remarque 2. *Les décompositions en cycles ci-dessus pour γ sont exactement celles données par Conway dans* [C] *p. 266 (notre γ est noté δ par Conway).*

Pour terminer la démonstration du Théorème 1, il ne reste qu'à montrer que les cinq cas ci-dessus se produisent vraiment. Il suffit de montrer que pour $p = 5, 7, 11$ le groupe $\mathrm{L}_2(p)$ possède un sous-groupe d'indice p, *i.e.* d'ordre $\frac{p^2-1}{2}$. En effet, l'action par translations sur les classes à gauche d'un tel sous-groupe est transitive, donc équivalente à l'une des actions $\star_{a,b}$ avec (p,a,b) de la Table 1, par ce que nous avons démontré. L'existence et l'inéquivalence des deux actions données pour $p = 7$ et 11 résultera alors des Lemmes 4 et 3. Au final, nous sommes conduits à poursuivre l'analyse précédente et à examiner ce que doit être le stabilisateur dans $\mathrm{L}_2(p)$ du point 0 de $\mathbb{Z}/p\mathbb{Z}$ pour l'action $\star_{a,b}$, si elle existe. Il contient trivialement γ et T, ainsi que, pour tout point fixe f de δ dans $\mathbb{Z}/p\mathbb{Z}$, l'élément

$$\alpha^{-f}\delta\alpha^{f} = \alpha^{1-f}\gamma\alpha^{f},$$

qui agit sur $\mathrm{P}^1(\mathbb{Z}/p\mathbb{Z})$ par $z \mapsto 1 - f - \frac{1}{z+f}$.

Proposition 1. *Soient $p \in \{5, 7, 11\}$ et S le sous-groupe de $\mathrm{L}_2(p)$ engendré par γ, T, et par un élément de la forme $\alpha^{-f}\delta\alpha^{f}$ avec f comme dans la Table 1. Alors on a $|S| = \frac{p^2-1}{2}$ et S s'identifie naturellement au groupe des rotations du polyèdre régulier de la Figure 1 étiqueté par $\mathrm{P}^1(\mathbb{Z}/p\mathbb{Z})$.*

Preuve — Nous allons démontrer cette proposition au cas par cas en contemplant simplement les polyèdres réguliers de la Figure 1, reproduits ci-dessous. Dans chacun des cas $p = 5, 7$ et 11, les sommets ou les arêtes du polyèdre correspondant P ont été soigneusement indexés par $\mathrm{P}^1(\mathbb{Z}/p\mathbb{Z})$. Il est bien connu [2] que le groupe G des rotations de P permute fidèlement l'ensemble de ses sommets (resp. de ses arêtes), de sorte que la numérotation choisie nous permet de voir G comme un sous-groupe de bijections de $\mathrm{P}^1(\mathbb{Z}/p\mathbb{Z})$. Comme $\mathrm{L}_2(p)$ agit aussi fidèlement sur $\mathrm{P}^1(\mathbb{Z}/p\mathbb{Z})$ par homographie, il y aura donc un sens à comparer S et G à l'intérieur du groupe des bijections de $\mathrm{P}^1(\mathbb{Z}/p\mathbb{Z})$. Nous choisirons enfin dans chaque cas un générateur β du groupe cyclique $T \simeq \mathrm{C}_p$ et une valeur arbitraire du point fixe f (l'autre choix de f, quand il existe, se traiterait de la même manière).

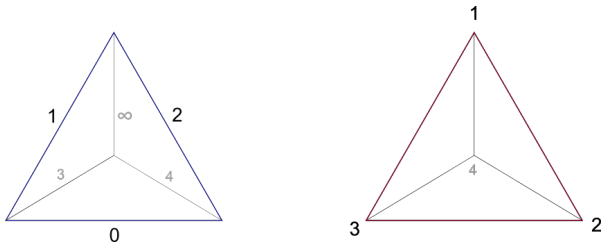
CAS $p = 5$.

On choisit $\beta.z = 4z$ et $f = 2$. En terme de l'action sur $\mathrm{P}^1(\mathbb{Z}/5\mathbb{Z})$, on constate

$$\beta = (1\,4)(2\,3), \quad \gamma = (0\,\infty)(1\,4) \quad \text{et} \quad \alpha^{-2}\delta\alpha^{2} = (3\,\infty\,4)(0\,1\,2).$$

2. Nous renvoyons par exemple à [B, §12.5] pour une discussion détaillée des solides de Platon et de leurs groupes d'isométries.

(Noter $\alpha\gamma = (0\,\infty\,1)(2\,3\,4)$.) Ces trois générateurs de S agissent manifestement sur $\mathrm{P}^1(\mathbb{Z}/5\mathbb{Z})$ comme des rotations d'ordre $2, 2$ et 3 du tétraèdre régulier en bleu ci-dessous (voir la Remarque 3 pour l'explication du tétraèdre rouge). Ainsi, S est



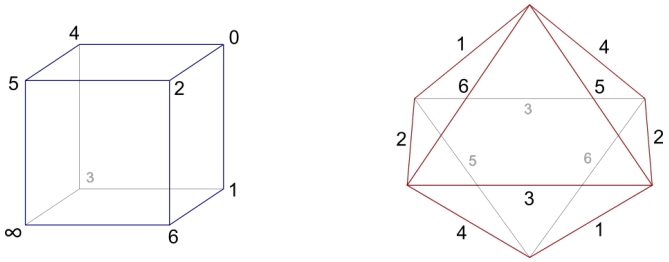
inclus dans le groupe G des rotations de ce tétraèdre. Comme ces trois rotations engendrent trivialement G, on en déduit $S = G$. On conclut car on a $G \simeq \mathrm{A}_4$ et donc $|S| = 12 = \frac{5^2-1}{2}$.

Cas $p = 7$ et $(a, b) = (-3, 2)$.

On a $f = -1$ et disons $\beta.z = 2z$. En terme de l'action sur $\mathrm{P}^1(\mathbb{Z}/7\mathbb{Z})$, on constate

$$\beta = (1\,2\,4)(3\,6\,5), \quad \gamma = (0\,\infty)(1\,6)(2\,3)(4\,5) \quad \text{et} \quad \alpha\delta\alpha^{-1} = (1\,\infty\,2)(3\,5\,0).$$

(Noter $\alpha\gamma = (0\,\infty\,1)(2\,4\,6)$.) Ces trois générateurs de S agissent manifestement sur $\mathrm{P}^1(\mathbb{Z}/7\mathbb{Z})$ comme des rotations d'ordre $3, 2$ et 3 du cube bleu ci-dessous. Ainsi,



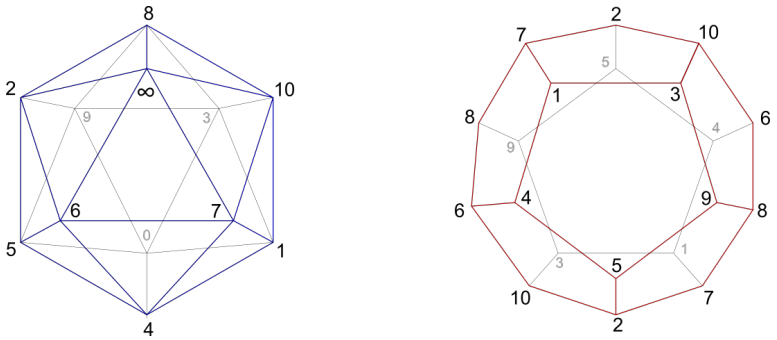
S est inclus dans le groupe G des rotations de ce cube. Comme ces trois rotations engendrent trivialement G, on a $S = G$. On conclut car on a $G \simeq \mathrm{S}_4$ et donc $|S| = 24 = \frac{7^2-1}{2}$.

Cas $p = 11$ et $(a, b) = (-2, 1)$.

Disons $f = 5$ et $\beta.z = 3z$. En terme de l'action sur $\mathrm{P}^1(\mathbb{Z}/11\mathbb{Z})$, on constate

$$\beta = (1\,3\,9\,5\,4)(2\,6\,7\,10\,8), \quad \gamma = (0\,\infty)(1\,10)(2\,5)(3\,7)(4\,8)(6\,9) \quad \text{et} \quad \alpha^{-5}\delta\alpha^{5} = (6\,\infty\,7)(8\,1\,5)(9\,3\,0)(2\,10\,4).$$

(Noter $\alpha\gamma = (0\,\infty\,1)(2\,6\,10)(3\,8\,5)(7\,4\,9)$.) Ces trois générateurs de S agissent manifestement sur $\mathrm{P}^1(\mathbb{Z}/11\mathbb{Z})$ comme des rotations d'ordre $5, 2$ et 3 de l'icosaèdre régulier en bleu ci-dessous. Ainsi, S est inclus dans le groupe G des rotations de cet ico-



saèdre. Comme ces trois rotations engendrent trivialement G, on a $S = G$. On conclut car on a $G \simeq \mathrm{A}_5$ et donc $|S| = 60 = \frac{11^2-1}{2}$. □

Cela termine la démonstration du Théorème 1. La remarque suivante explique les polyèdres en rouge donnés ci-dessus.

Remarque 3. *Dans chacun des trois cas étudiés ci-dessus, considérons l'action associée* $\star_{a,b}$ *de* $\mathrm{L}_2(p)$ *sur* $\mathbb{Z}/p\mathbb{Z}$*. Le stabilisateur de* 0 *est d'ordre* $\frac{p^2-1}{2}$ *et contient le groupe* S *de la Proposition 1 par construction : ce stabilisateur coincide donc avec* S *(c'était fait pour !). Mais il agit aussi naturellement sur* $(\mathbb{Z}/p\mathbb{Z})^\times$*, qui a* $p-1$ *éléments. En considérant dans chacun des cas le polyèdre régulier donné ci-dessus en rouge, étiqueté par* $(\mathbb{Z}/p\mathbb{Z})^\times$*, et les permutations données par la Table 1, on retrouve d'une autre manière que ce stabilisateur s'identifie au groupe d'isométries du polyèdre en question. Par exemple, dans les* 3 *cas considérés, l'élément* $\alpha^{-f}\delta\alpha^f$ *agit sur* $(\mathbb{Z}/p\mathbb{Z})^\times$ *respectivement par* $(3\,4\,1)$,$(1\,2\,6)(3\,4\,5)$ *et* $(6\,7\,5)(8\,2\,4)(9\ 10\ 1)$.

Enfin, on termine par une dernière assertion concernant les actions transitives du groupe $\mathrm{L}_2(p)^+ = \mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$ tout entier sur p éléments.

Corollaire 1. *Le groupe* $\mathrm{L}_2(p)^+$ *possède une action transitive sur un ensemble à* p *éléments si, et seulement si, on a* $p \leq 5$.

Preuve — Supposons d'abord $p > 3$. Soit $\star$ la restriction à $\mathrm{L}_2(p)$ d'une action transitive de $\mathrm{L}_2(p)^+$ sur un ensemble à p éléments. Cette action $\star$ est non triviale car on a $p > 2$, puis de la forme $\star_{a,b}$ par le Lemme 2. Mais $\star$ est isomorphe à sa conjuguée extérieure sous $\mathrm{L}_2(p)^+ \smallsetminus \mathrm{L}_2(p)$ par définition. On a donc $a = b$ par les Lemmes 3 et 4, puis $p = 5$ par le Lemme 7.

Il reste à voir que pour $p \leq 5$ il existe une action transitive de $\mathrm{L}_2(p)^+$ sur p éléments (on pourrait même voir qu'elle est unique à équivalence près). Pour $p = 2$, nous l'avons déjà expliqué dans l'Exemple 1, à l'aide d'un isomorphisme $\mathrm{L}_2(2)^+ \simeq \mathrm{S}_3$. Pour $p = 3$, nous avons rappelé $\mathrm{L}_2(3)^+ \simeq \mathrm{S}_4$ dans l'Exemple 2, et il existe une action transitive fameuse de S_4 sur 3 éléments (par exemple, considérer les 3 couples d'arêtes opposées d'un tétraèdre régulier). Enfin, pour $p = 5$ on a même un isomorphisme $\mathrm{L}_2(5)^+ \simeq \mathrm{S}_5$. En effet, l'action par homographies réalise $\mathrm{L}_2(5)^+$ comme un sous-groupe d'indice 6 dans S_6, et on sait que pour $n \geq 2$ un sous-groupe d'indice n de S_n est toujours isomorphe à S_{n-1}. □

Références

[B] M. Berger, *Géométrie*, tome 2, Nathan (1990).

[C] J .H. Conway, *Three lectures on exceptional groups*, Chapitre 10 de *Sphere packings, lattices and groups*, Grundlehren der Math. Wissenschaften 290, Springer-Verlag, New York (1999).

[G] E. Galois, lettre à Chevalier, 29 Mai 1832. Retranscrite à l'adresse http://www.galois.ihp.fr/ressources/vie-et-oeuvre-de-galois/lettres/lettre-testament/.

[H] B. Huppert, *Endliche Gruppen I*, Springer-Verlag (1967).

[K] B. Kostant, *The Graph of the Truncated Icosahedron and the Last Letter of Galois*, notices of the A.M.S. vol 42 no 9, 959–968 (1995).

École Normale Supérieure, DMA, 45 rue d'Ulm, 75005 Paris, France.