Sur un énoncé de la lettre de Galois à Chevalier

Gaëtan Chenevier

SUR UN ÉNONCÉ DE 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 possibilié est celle d'une action *transititive* sur p éléments. Pour $p \neq 2$, il est équivalent de demander si $\mathrm{L}_2(p)$ possède un sous-groupe d'indice p, *i.e.* d'ordre $\frac{p^2-1}{2}$. La découverte de Galois, annoncée dans sa lettre, est alors la suivante :

Théorème 1. (Galois) *Le groupe* $\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$ *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. En fait, une manière simple de démontrer l'existence de ces actions consiste à contempler les polyèdres réguliers suivants étiquetés par $\mathrm{P}^1(\mathbb{Z}/p\mathbb{Z})$

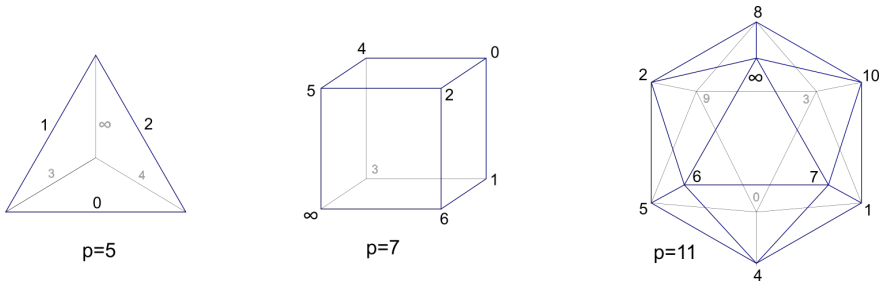


Figure 1.

et constater que leurs isométries directes sont induites par des homographies de $\mathrm{P}^1(\mathbb{Z}/p\mathbb{Z})$ dans $\mathrm{L}_2(p)$. Comme nous le verrons, cela se vérifie aisément sur des générateurs bien choisis, et nous reviendrons sur cette vérification plus loin (Lemme 8).

Le 15 février 2022, École Normale Supérieure, DMA, 45 rue d'Ulm, 75005 Paris, France.
L'auteur est financé par le CNRS et soutenu par l'ANR-19-CE40-0015-02.

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 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, dihédral, 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

On suppose désormais $p \neq 2$. On note C_p le sous-groupe des carrés de $(\mathbb{Z}/p\mathbb{Z})^\times$. On sait depuis Gauss que C_p est cyclique d'ordre $(p-1)/2$. On note N_p l'ensemble des non carrés de $\mathbb{Z}/p\mathbb{Z}$. On a donc

$$\mathbb{Z}/p\mathbb{Z} = \{0\} \coprod \mathrm{C}_p \coprod \mathrm{N}_p.$$

On note $\alpha \in \mathrm{L}_2(p)$ l'homographie $z \mapsto z + 1$ et T le sous-groupe des éléments diagonaux de $\mathrm{L}_2(p)$, ou ce qui revient au même des homographies de la forme $\mathrm{t}_\lambda(z) = \lambda z$ avec $\lambda \in \mathrm{C}_p$. On note enfin $\gamma \in \mathrm{L}_2(p)$ l'homographie $z \mapsto -1/z$. Bien entendu, ces formules concernent l'action de $\mathrm{L}_2(p)$ sur $\mathrm{P}^1(\mathbb{Z}/p\mathbb{Z})$.

Lemme 1. *Soit $\star$ une action transitive de $\mathrm{L}_2(p)$ sur un ensemble à p éléments. Il existe $a, b \in (\mathbb{Z}/p\mathbb{Z})^\times$ tels que $\star$ est équivalente à une action de $\mathrm{L}_2(p)$ sur $X = \mathbb{Z}/p\mathbb{Z}$ vérifiant :*

(i) $\alpha(x) = x + 1$ pour tout $x \in X$,

(ii) $\mathrm{t}_\lambda(x) = \lambda x$ pour tout $\lambda \in \mathrm{C}_p$ et $x \in X$,

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

Preuve — Supposons que $\mathrm{L}_2(p)$ agit transitivement sur $X = \mathbb{Z}/p\mathbb{Z}$. L'élément α de $\mathrm{L}_2(p)$ ne peut agir trivialement sur X, car $\mathrm{L}_2(p)$ est engendré par α et $\gamma\alpha\gamma^{-1}$, donc l'élément α d'ordre p agit comme un p-cycle sur X. Quitte à conjuguer l'action $\star$ par un élément de S_X, on peut donc supposer $\alpha(x) = x + 1$ pour tout

$x \in X$. On sait que T normalise $\langle\alpha\rangle$ dans $\mathrm{L}_2(p)$ et que le normalisateur du sous-groupe engendré par $x \mapsto x+1$ dans S_X est constitué des transformations affines

$$x \mapsto ax + b \text{ avec } a \in (\mathbb{Z}/p\mathbb{Z})^\times \text{ et } b \in \mathbb{Z}/p\mathbb{Z}.$$

Une telle transformation a toujours au moins un point fixe dans $\mathbb{Z}/p\mathbb{Z}$, sauf pour $a = 1$ et $b \neq 0$, auquel cas elle est d'ordre p. Tout générateur de T, étant d'ordre premier à p, admet donc au moins un point fixe $k \in \mathbb{Z}/p\mathbb{Z}$. Quitte à conjuguer $\star$ par α^{-k}, ce qui ne change pas l'action de α, on peut donc supposer $t(0) = 0$ pour tout $t \in T$. Soit $\lambda \in \mathrm{C}_p$. On a montré qu'il existe $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ avec $\mathrm{t}_\lambda(x) = ax$ pour tout $x \in X$. La relation $\mathrm{t}_\lambda\,\alpha = \alpha^\lambda\,\mathrm{t}_\lambda$ dans $\mathrm{L}_2(p)$ s'écrit, pour tout $x \in X$,

$$\lambda x + \lambda = ax + \lambda,$$

puis $a = \lambda$ pour $x = 1$. Comme γ normalise T dans $\mathrm{L}_2(p)$, et que 0 est unique point fixe de T dans X car $p \neq 2$, on a aussi $\gamma(0) = 0$. Mieux, la relation $\gamma t = t^{-1}\gamma$ pour tout t dans T s'écrit aussi

$$\gamma(\lambda x) = \lambda^{-1}\gamma(x) \text{ pour } x \in \mathbb{Z}/p\mathbb{Z} \text{ et } \lambda \in \mathrm{C}_p.$$

On conclut en posant $a = \gamma(1)$, et $b = \gamma(n)n$ pour $n \in \mathrm{N}_p$ quelconque. □

Comme $\mathrm{L}_2(p)$ est engendré par α et γ, les éléments $a, b \in (\mathbb{Z}/p\mathbb{Z})^\times$ étant donnés 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 précédent. Notons-là $\star_{a,b}$ si elle existe. Nous allons voir que $\star_{b,a}$ existe alors aussi. On rappelle que $\mathrm{L}_2(p)$ est distingué d'indice 2 dans le groupe

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

Lemme 2. *(i) On a $\star_{a,b} \simeq \star_{a',b'}$ si, et seulement si, $(a', b') = (a, b)$.*

(ii) La conjuguée de $\star_{a,b}$ par un élément de $\mathrm{L}_2(p)^+ \smallsetminus \mathrm{L}_2(p)$ est isomorphe à $\star_{b,a}$.

Preuve — Notons $f_{a,b} : \mathrm{L}_2(p) \to \mathrm{S}_{\mathbb{Z}/p\mathbb{Z}}$ le morphisme associé à l'action $\star_{a,b}$. Montrons d'abord le (i). Soit $\sigma \in \mathrm{S}_{\mathbb{Z}/p\mathbb{Z}}$ tel que $\sigma f_{a,b}(g)\sigma^{-1} = f_{a',b'}(g)$ pour tout $g \in \mathrm{L}_2(p)$. En prenant $g = \alpha$, on en déduit que σ commute à $x \mapsto x+1$. C'est donc $x \mapsto x + k$ pour un certain $k \in \mathbb{Z}/p\mathbb{Z}$. En prenant $g \in T$ on voit aussi $\sigma(0) = 0$, et donc $k = 0$, puis $\sigma = 1$, $f_{a,b} = f_{a',b'}$, et $(a, b) = (a', b')$ en prenant $g = \gamma$.

Montrons le (ii). Soit $g \in \mathrm{L}_2(p)^+$ diagonal agissant sur $\mathrm{P}^1(\mathbb{Z}/p\mathbb{Z})$ par $g(z) = nz$ avec $n \in \mathrm{N}_p$. Alors g engendre $\mathrm{L}_2(p)^+/\mathrm{L}_2(p)$. Dans $\mathrm{L}_2(p)$ on a les relations

$$g\alpha g^{-1} = \alpha^n, \quad g\mathrm{t}_\lambda g^{-1} = \mathrm{t}_\lambda \ (\lambda \in \mathrm{C}_p) \quad \text{et} \quad g\gamma g^{-1} = \mathrm{t}_{n^2}\gamma.$$

Cela suggère de considérer l'élément $\sigma \in \mathrm{S}_{\mathbb{Z}/p\mathbb{Z}}$ défini par $\sigma(x) = nx$, et de poser $f'_{a,b} : \mathrm{L}_2(p) \to \mathrm{S}_{\mathbb{Z}/p\mathbb{Z}}$, $\quad h \mapsto \sigma^{-1} f_{a,b}(ghg^{-1})\sigma$. On a clairement $f'_{a,b}(h) = f_{a,b}(h)$ pour $h = \alpha$ ou $h \in T$. Regardons l'élément $f'_{a,b}(\gamma) = \sigma^{-1} f_{a,b}(t_{n^2}) f_{a,b}(\gamma)\sigma^{-1}$. Pour $x \in \mathrm{C}_p$ on a $nx \in \mathrm{N}_p$ et donc

$$f'_{a,b}(\gamma)(x) = \sigma^{-1} f_{a,b}(t_{n^2}) f_{a,b}(\gamma)(nx) = n^{-1} \cdot n^2 \frac{b}{nx} = \frac{b}{x}.$$

On a de même $f'_{a,b}(\gamma)(x) = a/x$ pour $x \in \mathrm{N}_p$, $f'_{a,b}(\gamma)(0) = 0$, puis $f'_{a,b} = f_{b,a}$. □

On suppose désormais que $\star_{a,b}$ existe. L'idée est de considérer l'élément

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

Cet élément agit par $z \mapsto 1-1/z$ sur $\mathrm{P}^1(\mathbb{Z}/p\mathbb{Z})$, et donc par le 3-cycle $(1\,0\,\infty)$ sur $\{0,1,\infty\}$. En particulier, on a la relation bien connue $\delta^3 = 1$ dans $\mathrm{L}_2(p)$. L'élément δ doit donc aussi agir sur $\mathbb{Z}/p\mathbb{Z}$, via $\star_{a,b}$, par un élément d'ordre divisant 3. On a $\delta(0) = 1$, $\delta(x) = 1 + a/x$ pour $x \in \mathrm{C}_p$ et $\delta(x) = 1 + b/x$ pour $x \in \mathrm{N}_p$. On en déduit déjà que δ contient le 3-cycle $(0\ 1\ a+1)$, puis

$$a \notin \{0, -1\}.$$

Lemme 3. *On a l'égalité $a + b = -1$, et si $-1 \in \mathrm{C}_p$ alors $a = b = -1/2$.*

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

Si $p = 3$, on a $a, b \in \{\pm 1\}$, donc la seule possibilité est $a = b = 1$. On suppose donc désormais $p > 3$.

Lemme 4. *Supposons $a = b$. Alors $a = b = -1/2$ et $p = 5$.*

Preuve — L'égalité $a+b = -1$ montre $a = b = -1/2$. Utilisant $p > 3$ on constate $(\delta(-1),\, \delta^2(-1),\, \delta^3(-1)) = (3/2,\, 2/3,\, 1/4)$. On a donc $-1 = 1/4$, puis $5 = 0$. □

Lemme 5. *Supposons $a \neq b$. Alors a et b sont des carrés et $-1 \in \mathrm{N}_p$.*

Preuve — On a déjà vu $-1 \in \mathrm{N}_p$ (Lemme 3). Le Lemme 1 (iii) montre que l'involution γ de $(\mathbb{Z}/p\mathbb{Z})^\times$ permute C_p et 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 suppose donc définitivement $a, b \neq -1/2$, $p > 5$, $a, b \in \mathrm{C}_p$ et $-1 \in \mathrm{N}_p$.

Lemme 6. *Supposons $(a, b) = (1, -2)$ ou $(-2, 1)$. Alors $p = 11$.*

Preuve — On peut supposer $a = 1$ et $b = -2$ par le Lemme 2 (ii). On a $p \neq 3$ et $-1 \in \mathrm{N}_p$, donc $\delta(-1) = 3$ non nul. Si $3 \in \mathrm{C}_p$, 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 $3 \in \mathrm{N}_p$, on constate $\delta(3) = 1/3 \in \mathrm{N}_p$, puis $\delta(1/3) = -5$, et donc $-1 = -5$ et $4 = 0$: absurde. □

Lemme 7. *Supposons $(a, b) = (2, -3)$ ou $(-3, 2)$. Alors $p = 7$.*

Preuve — On peut supposer $a = 2$ et $b = -3$. On a $-1, -2 \in \mathrm{N}_p$ par le Lemme 5. On a donc $\delta(-2) = 5/2$, non nul car $p > 5$. Si $5 \in \mathrm{N}_p$, 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 $5 \in \mathrm{C}_p$, 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 $-1 \notin \mathrm{N}_{37}$. □

Supposons enfin que a et b ne sont pas dans $\{-3,-2,1,2\}$ (stable par $x \mapsto -1-x$). Nous allons montrer que $\star_{a,b}$ n'existe pas. Comme $b \in \mathrm{C}_p$, on a $\delta(b) = 1+a/b = (a+b)/b = -1/b \in \mathrm{N}_p$, puis

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

qui est non nul car $b \neq 1$. Supposons d'abord $b-1 \in \mathrm{C}_p$. On a alors $a(b-1) \in \mathrm{C}_p$ et donc $\delta(a(b-1)) = 1+1/(b-1) = b/(b-1)$. On a donc $b = b/(b-1)$ puis $b = 2$: absurde. On a donc $b-1 \in \mathrm{N}_p$, puis l'égalité

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

On en déduit que b est racine du polynôme

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

Par symétrie (*i.e.* en considérant de même $\star_{b,a}$ par le Lemme 2 (ii)), 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 $c = 2$, et donc $5 = 2^3 - 2^2 + 1 = 0$: c'est la contradiction cherchée !

Remarque 1. *Donnons un autre argument montrant $p \leq 19$ à partir du Lemme 5. 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 6 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 $\mathbb{Z}/p\mathbb{Z}$, 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
3	$(1,1)$	$1/x$	$1/x$	1	$(0\,1\,2)$	
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.

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).*

Il ne reste qu'à montrer que les 6 cas ci-dessus se produisent vraiment. D'après les Lemmes 1 et 2 (ii), il suffit de montrer que pour $p \leq 11$ le groupe $\mathrm{L}_2(p)$ possède un sous-groupe d'indice p, *i.e.* d'ordre $\frac{p^2-1}{2}$. L'inéquivalence des deux actions données pour $p = 7$ et 11 résultera alors du Lemme 2 (i). Cela pousse à examiner le stabilisateur de 0 dans $\mathbb{Z}/p\mathbb{Z}$ 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 $z \mapsto 1 - f - \frac{1}{z+f}$. Le cas $p = 3$ est trivial : l'élément γ commute avec $T \simeq \mathbb{Z}/2\mathbb{Z}$, et on a $\langle \gamma, T\rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, d'ordre $4 = \frac{3^2-1}{2}$.

Lemme 8. *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 $\mathrm{P}^1(\mathbb{Z}/p\mathbb{Z})$.*

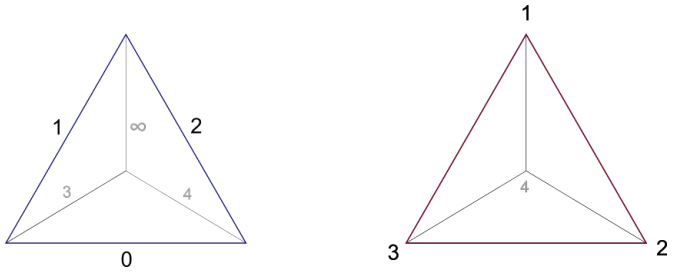
Nous allons démontrer ce lemme au cas par cas en contemplant simplement les polyèdres de la Figure 1. On rappelle que le groupe des rotations d'un solide de Platon agit fidèlement et transitivement sur ses sommets, sur ses arêtes, et que le stabilisateur d'un sommet permute simplement transitivement les faces auxquelles ce sommet appartient. Il sera commode d'introduire un générateur β de T.

Cas $p = 5$.

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

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

(Noter $\alpha\gamma = (0\,\infty\,1)(2\,3\,4)$.) Ces trois éléments sont manifestement induits par des rotations d'ordre $2, 2$ et 3 du tétraèdre de la Figure 1, reproduit à gauche ci-dessous (voir la Remarque 3 pour l'explication des polyèdres en rouge),



dont les 6 arêtes sont les éléments de $\mathrm{P}^1(\mathbb{Z}/5\mathbb{Z})$. Ces trois rotations engendrent trivialement le groupe G des isométries de ce tétraèdre, de sorte que le morphisme naturel $S \to G$ est un isomorphisme. On a donc $S \simeq G \simeq \mathrm{A}_4$, puis $|S| = 12 = \frac{5^2-1}{2}$.

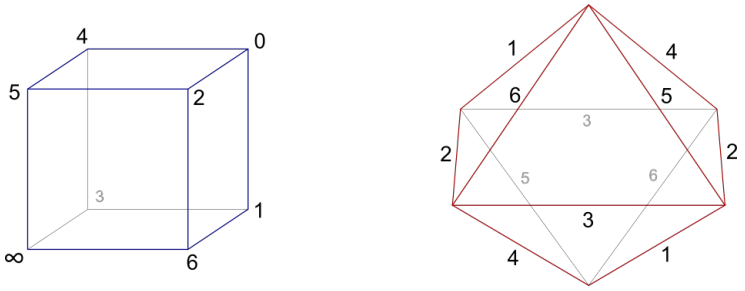
Cas $p = 7$ et $(a, b) = (-3, 2)$.

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 éléments sont manifestement induits par des rotations d'ordre $3, 2$ et 3 du cube de la Figure 1, reproduit à gauche ci-dessous,

dont les 8 sommets sont les éléments de $\mathrm{P}^1(\mathbb{Z}/7\mathbb{Z})$. Ces trois rotations engendrent trivialement le groupe G des isométries de ce cube, de sorte que le morphisme naturel $S \to G$ est un isomorphisme. On a donc $S \simeq G \simeq \mathrm{S}_4$, puis $|S| = 24 = \frac{7^2-1}{2}$.

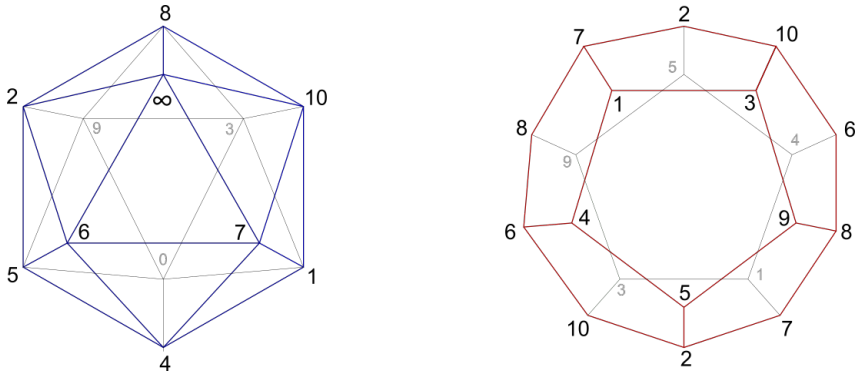


CAS $p = 11$ ET $(a, b) = (-2, 1)$.

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

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

(Noter $\alpha\gamma = (0\,\infty\,1)(2\,6\,10)(3\,8\,5)(7\,4\,9)$.) Ces trois éléments agissent par des rotations d'ordre $5, 2$ et 3 de l'icosaèdre de la Figure 1, reproduit à gauche ci-dessous,



dont les 12 sommets sont les éléments de $\mathrm{P}^1(\mathbb{Z}/11\mathbb{Z})$. Ces trois rotations engendrent manifestement le groupe G des isométries de cet icosaèdre, de sorte que le morphisme naturel $S \to G$ est un isomorphisme. On a donc $S \simeq G \simeq \mathrm{A}_5$, puis $|S| = 60 = \frac{11^2-1}{2}$. Cela termine la démonstration du théorème. □

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 du Lemme 8 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 bien que ce stabilisateur s'identifie au groupe d'isométrie du polyèdre en question. Par exemple, dans les 3 cas considérés, l'élément $\alpha^{-f}\delta\alpha^f$ agit sur $\mathbb{Z}/p\mathbb{Z}$ respectivement par $(3\,4\,1)$,$(1\,2\,6)(3\,4\,5)$ et $(6\,7\,5)(8\,2\,4)(9\,10\,1)$.*

RÉFÉRENCES

[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.

[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. (1995).