Frobenius’ result on simple groups of order $\frac{p^3-p}{2}$

Paul Monsky

Brandeis University, Waltham MA 02454-9110, USA
monsky@brandeis.edu

Abstract

The complete list of pairs of non-isomorphic finite simple groups having the same order is well-known. In particular for $p > 3$, $PSL_2(\mathbb{Z}/p)$ is the “only” simple group of order $\frac{p^3-p}{2}$. It’s less well-known that Frobenius proved this uniqueness result in 1902. This note presents a version of Frobenius’ argument that might be used in an undergraduate honors algebra course. It also includes a short modern proof, aimed at the same audience, of the much earlier result that $PSL_2(\mathbb{Z}/p)$ is simple for $p > 3$; a result stated by Galois in 1832.

1 Background

Let $p$ be a prime and $SL_2(\mathbb{Z}/p)$ be the group of 2 by 2 determinant 1 matrices with entries in $\mathbb{Z}/p$. The quotient, $PSL_2(\mathbb{Z}/p)$, of $SL_2(\mathbb{Z}/p)$ by \{±I\} is for $p > 2$ a group of order $\frac{p^3-p}{2}$. Galois [2] introduced and studied this group; in his 1832 letter to Auguste Chevalier he says that it is easily shown to be simple for $p > 3$. (There are many proofs of simplicity. I’ll give a short one in section 6.) In 1902 Frobenius [1] classified certain transitive permutation groups on $p + 1$ letters up to permutation isomorphism, and deduced as a corollary that $PSL_2(\mathbb{Z}/p)$ is the “only” simple group of order $\frac{p^3-p}{2}$.

Frobenius’ proof of this very early result in the classification of the finite simple groups, though elementary, isn’t well-known and hasn’t found its way into textbooks. In this note I give a version of it, based on Sylow theory and the cyclicity of $(\mathbb{Z}/p)^*$. This version could perhaps be presented in an undergraduate honors algebra course. I thank Jim Humphreys for his close reading of this note, his encouragement, and his expository suggestions.

Another description of $PSL_2(\mathbb{Z}/p)$ will be useful. Let $V$ be the space of column vectors, (\(x\ y\)), with entries in $\mathbb{Z}/p$. $SL_2(\mathbb{Z}/p)$ acts on the set consisting of the
$p + 1$ one-dimensional subspaces of $V$. We identify this space with $\mathbb{Z}/p \cup \{\infty\}$ as follows. Given a subspace with generator $(x \ y)$, map it to the element $z = \frac{x}{y}$ of $\mathbb{Z}/p \cup \{\infty\}$. Since $(x \ y)$ is mapped to $(x+y \ y)$ by $(\frac{1}{1} \ 1)$ and to $(-y \ y)$ by $(\frac{0}{1} \ -1)$, the images of $(\frac{1}{1} \ 1)$ and $(\frac{1}{0} \ 0)$ are the translation $z \to z + 1$, and the involution $z \to -\frac{1}{z}$. Easy arguments with row and column operations show that $(\frac{1}{1} \ 1)$ and $(\frac{0}{-1})$ generate $SL_2(\mathbb{Z}/p)$. Since the kernel of the action of $SL_2(\mathbb{Z}/p)$ consists of $I$ and $-I$, $PSL_2(\mathbb{Z}/p)$ identifies with the transitive group of permutations of $\mathbb{Z}/p \cup \{\infty\}$ generated by $z \to z + 1$ and $z \to -\frac{1}{z}$.

I’ll prove the following (version of a) result of Frobenius, and its easy corollary:

**Classification Theorem.** Let $p \neq 2$ be prime and $G$ be a transitive group of permutations of $\mathbb{Z}/p \cup \{\infty\}$. Suppose $|G| = p^3 - p^2$, and that $G$ contains the translations. Then one of the following holds:

(a) $z \to -\frac{1}{z}$ is in $G$. (In this case the description of $PSL_2(\mathbb{Z}/p)$ given above and the fact that $|G| = |PSL_2(\mathbb{Z}/p)|$ tell us that $G$ is generated by $z \to z + 1$ and $z \to -\frac{1}{z}$, and is permutation-isomorphic to $PSL_2(\mathbb{Z}/p)$ in its action on the 1-dimensional subspaces of $V$.)

(b) $p = 7$ and $G$ contains the involution $(0\infty)(13)(26)(45)$ or the involution $(0\infty)(15)(23)(46)$. In these cases $G$ is generated by $z \to z + 1$, $z \to 2z$, and the involution, and has a normal subgroup of order 8.

**Corollary.** When $p > 3$, $PSL_2(\mathbb{Z}/p)$ is, up to isomorphism, the only simple group of order $\frac{p^3 - p^2}{2}$.

The theorem is trivial when $p = 3$. For now $|G| = 12$ and $G$ is a permutation group on 4 elements. So $G$ consists of the even permutations, and thus contains $(0\infty)(12)$. In the following sections we prove the theorem for $p > 3$, but now we show how the corollary follows. Suppose $G$ is a simple group of order $\frac{p^3 - p^2}{2}$ with $p > 3$. Then $p$ divides $|G|$ and $G$ has $mp + 1$ $p$-Sylow subgroups; since $G$ is simple $m > 0$. Furthermore $\frac{p^2 - 1}{mp + 1}$ is an integer $\equiv -1 \pmod{p}$ and so is $\geq p - 1$; it follows that $m = 1$. $G$ acts on the set $S$ consisting of the $p + 1$ $p$-Sylows, and by Sylow theory the action is transitive. Since $G$ is simple, the action is faithful. Select an element $\sigma$ of $G$ of order $p$. This element acts by a $p$-cycle on $S$; denote the element it fixes by $\infty$. We may label the remaining elements of $S$ with tags in $\mathbb{Z}/p$ so that $\sigma$ is the translation $(01 \cdots p - 1)$, $z \to z + 1$, of $\mathbb{Z}/p \cup \{\infty\}$. If we view $G$ as a group of permutations of $\mathbb{Z}/p \cup \{\infty\}$, the hypotheses of the classification theorem are satisfied. Since $G$ has no normal subgroup of order 8, we’re in the situation of (a), and we conclude that $G$ is isomorphic to $PSL_2(\mathbb{Z}/p)$.
2 Easy facts about $G$

For the rest of this note $G$ is a group satisfying the hypotheses of the classification theorem. Then the stabilizer, $G_\infty$, of $\infty$ in $G$ contains the translations and so is transitive on $\mathbb{Z}/p$. Consequently:

**Lemma 2.1.** $G$ is doubly transitive on $\mathbb{Z}/p \cup \{\infty\}$.

**Definition 2.2.** $K$ is the subgroup of $G$ consisting of elements fixing 0 and $\infty$. $\bar{K}$ consists of the elements of $G$ interchanging 0 and $\infty$. $H = K \cup \bar{K}$ is the stabilizer of $\{0, \infty\}$ in $G$.

Since $G$ is doubly transitive, $|K| = \frac{|G|}{p(p+1)} = \frac{p-1}{2}$. Double transitivity also shows that $\bar{K}$ is non-empty. So $K$ is of index 2 in $H$, and $|\bar{K}| = |K| = \frac{p-1}{2}$.

**Definition 2.3.** $R$ is the set of squares in $(\mathbb{Z}/p)^*$, $N$ the set of non-squares.

Since $(\mathbb{Z}/p)^*$ is cyclic, so is $R$. Furthermore, $|R| = |N| = \frac{p-1}{2}$.

**Lemma 2.4.**

1. $K$ is cyclic and consists of the maps $z \to az$, $a$ in $R$.
2. No element of $G$ fixes more than 2 letters.

**Proof.** $|G_\infty| = \frac{|G|}{p+1} = p \left(\frac{p-1}{2}\right)$. The Sylow theorems then show that the group of translations is the unique $p$-Sylow subgroup of $G_\infty$, and so is normal in $G_\infty$. So for $\tau$ in $G_\infty$, $\tau \circ (z \to z + 1) = (z \to z + a) \circ \tau$ for some $a$ in $(\mathbb{Z}/p)^*$. If $\tau$ is in $K$, $\tau(0) = 0$. Since $\tau(z + 1) = \tau z + a$, $\tau(z) = az$ for all $z$ in $\mathbb{Z}/p$. Now the maps $z \to az$, $a$ in $(\mathbb{Z}/p)^*$, form a cyclic group of order $p - 1$. Since $K$ is a subgroup of that group of order $\frac{p-1}{2}$, we get (1).

Suppose next that $\tau \neq e$ fixes 3 or more letters. By double transitivity we may assume that 2 of these letters are 0 and $\infty$, so that $\tau$ is in $K$. But the only map $z \to az$ fixing a third letter is $e$. \hfill \square

**Lemma 2.5.** Suppose $\tau \in \bar{K}$.

1. If $p \equiv 1 \pmod{4}$, $-1 \in R$ and $\tau$ stabilizes $R$ and $N$.
2. If $p \equiv 3 \pmod{4}$, $-1 \in N$ and $\tau$ interchanges $R$ and $N$.

**Proof.** By Lemma 2.4 (1), the orbits of $K$ acting on $(\mathbb{Z}/p)^*$ are $R$ and $N$. Since $\tau$ normalizes $K$ it permutes these orbits. Suppose first that $p \equiv 1 \pmod{4}$. Then $|R| = \frac{p-1}{2}$ is even and $R$ contains an element of $(\mathbb{Z}/p)^*$ of order 2, which must be $-1$. Furthermore by Lemma 2.4 (1), $z \to -z$ is in $G$ and has an orbit $(u, v)$ of size 2. By double transitivity some conjugate, $\lambda$, of this element lies
in $K$, and, like $z \to -z$, fixes 2 letters. Such a $\lambda$ cannot possibly interchange $R$ and $N$. So it stabilizes $R$ and $N$, and since $\bar{K}$ is a coset of $K$ in $H$, the same is true of all $\tau$ in $\bar{K}$. Suppose next that $p \equiv 3 \pmod{4}$. Then $|R| = \frac{p-1}{2}$ is odd, so $-1$ cannot be in $R$. If the lemma fails there is a $\tau$ in $\bar{K}$ with $\tau(1)$ in $R$. Since $\bar{K}$ is a coset of $K$ in $H$ there is a $\lambda$ in $\bar{K}$ with $\lambda(1) = 1$. Then $\lambda \circ \lambda$ fixes the letters 0, $\infty$ and 1. By Lemma 2.4 (2), $\lambda$ has order 2 and fixes 1. Since $\lambda$ is a product of disjoint 2-cycles, $\lambda$ must fix a second letter as well. By double transitivity some conjugate of $\lambda$ is an order 2 element of $K$. But $|K| = \frac{p-1}{2}$ is odd.

**Lemma 2.6.** Suppose $\tau \in \bar{K}$. Then there is an $n$ such that whenever $z$ is in $(\mathbb{Z}/p)^*$ and $a$ is in $R$, $\tau(az) = a^n \tau(z)$. Furthermore $\frac{p-1}{2}$ divides $n^2 - 1$.

**Proof.** $\tau$ normalizes $K$. So $\sigma \to \tau \sigma \tau^{-1}$ is an automorphism of $K$ which is of the form $\sigma \to \sigma^n$ since $K$ is cyclic. Then $\tau \circ (z \to az) = (z \to a^n z) \circ \tau$, giving the first result. Since the square of the automorphism is the identity, $\frac{p-1}{2}$ divides $n^2 - 1$.

**Remark.** $n$ is prime to $\frac{p-1}{2}$. So when $p \equiv 1 \pmod{4}$, $n$ is odd. We’re free to modify $n$ by $\frac{p-1}{2}$, and so when $p \equiv 3 \pmod{4}$ we may (and shall) assume that $n$ is odd as well.

### 3 The case $p \equiv 1 \pmod{4}$

In this section $p \equiv 1 \pmod{4}$. Our first goal is to show that the $n$ of Lemma 2.6 can be chosen to be $-1$.

**Definition 3.1.** $X$ is the set of pairs whose first element is a $\tau$ in $G$, and whose second element is a size 2 orbit $\{u, v\}$ of $\tau$.

**Lemma 3.2.** $|X| = \left(\frac{p^2 + p}{2}\right) \left(\frac{p-1}{2}\right)$.

**Proof.** The number of size 2 subsets of $\mathbb{Z}/p \cup \{\infty\}$ is $\frac{p^2 + p}{2}$. We prove the lemma by showing that for each such subset $\{u, v\}$ there are exactly $\frac{p-1}{2}$ elements of $G$ having $\{u, v\}$ as an orbit. By double transitivity we may assume $\{u, v\} = \{0, \infty\}$. But $\tau$ has $\{0, \infty\}$ as an orbit precisely when $\tau$ is in $\bar{K}$.

**Lemma 3.3.** Every element of $\bar{K}$ has order 2.

**Proof.** Since $-1$ is in $R$, $\tau : z \to -z$ is in $K$. The letters fixed by $\tau$ are 0 and $\infty$; it follows that every element of $G$ commuting with $\tau$ stabilizes the set $\{0, \infty\}$ and lies in $H$. So the centralizer of $\tau$ in $G$ has order at most
$|H| = p - 1$, and the number of conjugates of $\tau$ is at least $\frac{|G|}{p - 1} = \frac{p^2 + p}{2}$. Call these conjugates $\tau_i$. Like $\tau$, each $\tau_i$ has $\frac{p-1}{2}$ orbits of size 2. So the number of pairs whose first element is some $\tau_i$ and whose second is an orbit of that $\tau_i$ is at least $\left(\frac{p^2 + p}{2}\right) \cdot \left(\frac{p-1}{2}\right)$. By Lemma 3.2 these pairs exhaust $X$. Suppose now that $\lambda$ is in $\bar{K}$. Then $\lambda$ has a size 2 orbit, $\{0, \infty\}$, and so must be some $\tau_i$, proving the lemma.

**Corollary 3.4.** The $n$ of Lemma 2.6 can be taken to be $-1$.

**Proof.** Take $\tau$ in $\bar{K}$, $\sigma$ in $K$. By Lemma 3.3, $(\tau\sigma)(\tau\sigma) = e$ and $\tau = \tau^{-1}$. So $\tau\sigma\tau^{-1} = \sigma^{-1}$. Examining the proof of Lemma 2.6 we get the result.

**Corollary 3.5.** There is a $\lambda$ in $\bar{K}$ and a $c$ in $(\mathbb{Z}/p)^*$ such that:

1. $\lambda(z) = z^{-1}$ for $z$ in $R$.
2. $\lambda(z) = cz^{-1}$ for $z$ in $N$.

**Proof.** By Lemma 2.5 there is a $\bar{K}$ in $R$ with $\lambda(1) = 1$. The result now follows from Corollary 3.4 and Lemma 2.6.

Suppose we can show that the $c$ of Corollary 3.5 is 1. Then, composing $\lambda$ with the element $z \rightarrow -z$ of $K$ we deduce that $z \rightarrow -\frac{1}{z}$ is in $G$. So to prove the classification theorem for $p \equiv 1 \ (4)$ it’s enough to show that $c = 1$.

**Proposition 3.6.** When $p \equiv 1 \ (4)$, $z \rightarrow -\frac{1}{z}$ is in $G$.

**Proof.** Let $\alpha(z) = 1 - \lambda(z)$ with $\lambda$ as in Corollary 3.5. Since $-1$ is in $R$, $\alpha$ is in $G$. Using the fact that $\lambda \circ \lambda = e$ we see that $\alpha^{-1}(z) = \lambda(1 - z)$. Now $\alpha(0) = \infty$, $\alpha(\infty) = 1$, $\alpha(1) = 1 - 1 = 0$. So $\alpha \circ \alpha \circ \alpha$ fixes the letters 0, $\infty$ and 1. By Lemma 2.4 (2), $\alpha$ has order 3.

Since $p \equiv 1 \ (4)$, $p - 1$ is in $R$. As not all of 1, 2, $\ldots$, $p - 2$ are in $R$ there is an $x$ in $R$ with $x - 1$ in $N$. The paragraph above shows that $\alpha(\alpha(x)) = \alpha^{-1}(x) = \lambda(1 - x)$. We’ll use this to show that $c = 1$. Since $\lambda(x) = -\frac{1}{x}$, $\alpha(x) = \frac{1}{1 - x}$ is in $N$. Consequently, $\lambda(\alpha(x)) = \frac{cx}{x - 1}$. Then $\alpha(\alpha(x)) = \frac{x - 1 - cx}{x - 1} = \frac{x - 1 - cx}{x - 1}$ while $\lambda(1 - x) = -\frac{c}{x - 1}$. So $x - 1 = cx - c$, and $c = 1$.

**4 $p \equiv 3 \ (4)$. The main case**

In this section $p \equiv 3 \ (4)$.
Lemma 4.1. There is a unique $\lambda$ in $K$ with $-\lambda(1)\lambda(-1) = 1$. Furthermore $\lambda$ has order 2.

Proof. Fix $\tau$ in $K$. By Lemma 2.5, $-1$ and $\tau(1)$ are in $N$ while $\tau(-1)$ is in $R$. So $u = -\tau(1)\tau(-1)$ is in $R$. Replacing $\tau$ by $z \mapsto v\tau(z)$ with $v$ in $R$ multiplies $-\tau(1)\tau(-1)$ by $v^2$. Since there is a unique $v$ in $R$ with $v^2 = u^{-1}$ we get the existence and uniqueness of $\lambda$. By Lemma 2.5 there are $a$ and $b$ in $R$ with $\lambda(a) = -1$, $\lambda(-b) = 1$. Taking $n$ as in Lemma 2.6 we find that $a^n\lambda(1) = -1$, $b^n\lambda(-1) = 1$. Multiplying we see that $(ab)^n = 1$, so $ab = 1$. Now $-\lambda^{-1}(-1)\lambda^{-1}(1) = (-a)(-b) = 1$, and the uniqueness of $\lambda$ tells us that $\lambda = \lambda^{-1}$.

Corollary 4.2. Choose $n$ odd as in Lemma 2.6. Then there is a $\lambda$ of order 2 in $K$ and a $c$ in $N$ with

\begin{align*}
(1) \quad & \lambda(z) = cz^n \quad z \text{ in } R \\
(2) \quad & \lambda(z) = c^{-1}z^n \quad z \text{ in } N \\
(3) \quad & c^n = c
\end{align*}

Proof. Take $\lambda$ as in Lemma 4.1 and set $c = \lambda(1)$. By Lemma 2.5, $c$ is in $N$. Since $\lambda(1) = c$, $\lambda(-1) = -\frac{1}{c} = \frac{1}{c} \cdot (-1)^n$. Lemma 2.6 then gives (1) and (2). Since $c$ is in $N$, $\lambda(c) = c^{-1} \cdot c^n$. But as $\lambda$ has order 2, $\lambda(c) = 1$.

Lemma 4.3. Let $\alpha(z) = 1 - c^{-1}\lambda(z)$ with $c$ and $\lambda$ as above. Then $\alpha$ is an element of $G$ of order 3 and $\alpha^{-1}(z) = \lambda(c(1 - z))$.

Proof. Since $c$ is in $N$, $-c^{-1}$ is in $R$, and $\alpha$ is in $G$. Also $\alpha(0) = \infty$, $\alpha(\infty) = 1$ and $\alpha(1) = 1 - c^{-1} \cdot c = 0$. So $\alpha \circ \alpha \circ \alpha$ fixes the letters $0$, $\infty$ and $1$; by Lemma 2.4 (2), $\alpha$ has order 3. Finally if $\mu$ is the map $z \mapsto \lambda(c(1 - z))$, then $\mu(\alpha(z)) = \lambda(\lambda(z)) = z$, and so $\alpha^{-1} = \mu$.

The proof of the classification theorem for $p \equiv 3 \pmod{4}$ now divides into 2 subcases. In this section we treat the “main case” where the $c$ of Corollary 4.2 is $-1$, showing that $n \equiv -1 \pmod{p-1}$ so that $\lambda(z) = -\frac{1}{z}$ for all $z$. The “special case”, $c \neq -1$, which leads to conclusion (b) of the classification theorem will be handled in the next section — it’s a bit more technical.

Lemma 4.4. In the main case the only solutions of $x^n = x$ in $(\mathbb{Z}/p)^*$ are 1 and $-1$.

Proof. Since $c = -1$, $c^{-1} = -1$, and $\lambda(x) = -x^n$ for all $x$ in $(\mathbb{Z}/p)^*$. Thus $\alpha(x) = 1 - x^n$. Suppose now that $x \neq 1$ is in $(\mathbb{Z}/p)^*$ with $x^n = x$. Then $\alpha(x) = 1 - x$ and so $\alpha(\alpha(x)) = 1 - (1 - x)^n$. By Lemma 4.3, $\alpha^{-1}(x) = \lambda(x - 1) = -(x - 1)^n = (1 - x)^n$. Since $\alpha(\alpha(x)) = \alpha^{-1}(x)$, $(1 - x)^n = \frac{1}{2}$. 

6
Raising to the $n$th power we find that $1 - x = 2^{-n}$. So 1 and $1 - 2^{-n}$ are the only possible solutions of $x^n = x$ in $(\mathbb{Z}/p)^*$. Since 1 and $-1$ are solutions we’re done.  

**Proposition 4.5.** Suppose $p \equiv 3 \pmod{4}$. In the main case, $\lambda$ is the map $z \rightarrow -\frac{1}{z}$, and so $z \rightarrow -\frac{1}{z}$ is in $G$.

**Proof.** By Lemma 4.4 the only solution of $x^n = x$ in the cyclic group $R$ of order $\frac{p-1}{2}$ is 1. So $n - 1$ is prime to $\frac{p-1}{2}$. Now $\frac{p-1}{2}$ divides $(n + 1)(n - 1)$ by Lemma 2.6. So it divides $n + 1$, and as $n$ is odd, $n \equiv -1 \pmod{(p - 1)}$. Then for $z$ in $(\mathbb{Z}/p)^*$, $\lambda(z) = -z^n = -\frac{1}{z}$. Furthermore $\lambda(0) = \infty$, $\lambda(\infty) = 0$.  

5 $p \equiv 3 \pmod{4}$. The special case

We continue with the notation of Section 4 but now assume $c \neq -1$

**Lemma 5.1.** Let $x$ be a power of $-c$, and suppose that $1 - x$ is in $N$. Then:

(a) $\alpha(\alpha(x)) = 1 - c^{-2}(1 - x)^n$
(b) $\alpha(\alpha(x^{-1})) = 1 + x^{-1}(1 - x)^n$
(c) $\alpha^{-1}(x) = c^2(1 - x)^n$
(d) $\alpha^{-1}(x^{-1}) = -x^{-1}(1 - x)^n$

**Proof.** Since $c^n = c$ and $n$ is odd, $x^n = x$. Since $c$ is in $N$, $x$ is in $R$. Thus $\alpha(x) = 1 - c^{-1}(cx^n) = 1 - x$, and similarly $\alpha(x^{-1}) = 1 - x^{-1} = \frac{1-x}{-x}$, which is in $R$.

Now $\alpha(\alpha(x)) = \alpha(1 - x) = 1 - c^{-1}c^{-1}(1 - x)^n$ giving (a). And $\alpha(\alpha(x^{-1})) = \alpha\left(\frac{1-x}{-x}\right) = 1 - \left(\frac{1-x}{-x}\right)^n = 1 + x^{-1}(1 - x)^n$ giving (b). Furthermore $\alpha^{-1}(x) = \lambda(c(1 - x))$. Since $c(1 - x)$ is in $R$, this is $c \cdot c(1 - x)^n$. Finally $\alpha^{-1}(x^{-1}) = \lambda\left(\frac{c(1-x)}{-x}\right) = c^{-1}\left(\frac{c}{-x}\right) \cdot (1 - x)^n = -x^{-1}(1 - x)^n$.

**Lemma 5.2.** In the situation of Lemma 5.1, $c^2 + c^{-2} + 2x^{-1} = 0$.

**Proof.** $\alpha(\alpha(x)) = \alpha^{-1}(x)$ by Lemma 4.3. (a) and (c) above tell us that $(c^2 + c^{-2})(1-x)^n = 1$. Similarly, (b) and (d) tell us that $2x^{-1}(1-x)^n = -1$. Adding these identities and noting that $(1-x)^n \neq 0$ we get the result.  

**Lemma 5.3.** $c^3 = -1$, and either $c^4 + 3 = 0$ or $3c^4 + 1 = 0$.

**Proof.** There is an $x$ in $\{c^2, c^{-2}\}$ such that $1 - x$ is in $N$. For neither $1 - c^2$ nor $1 - c^{-2}$ is 0, and if both were in $R$, their quotient, $-c^2$, would be in $R$. 

7
Similarly there is a $y$ in $\{-c, -c^{-1}\}$ such that $1 - y$ is in $N$. By Lemma 5.2, $c^2 + c^{-2} + 2x^{-1}$ and $c^2 + c^{-2} + 2y^{-1}$ are both 0. So $x = y$, and $c^3 = -1$. Also, since $c^2 + c^{-2} + 2x^{-1} = 0$, either $c^2 + 3c^{-2}$ or $3c^2 + c^{-2}$ is 0. \[\square\]

**Proposition 5.4.** $p = 7$. Furthermore either $c = 3$ and $\lambda = (0\infty)(13)(26)(45)$, or $c = 5$ and $\lambda = (0\infty)(15)(23)(46)$

**Proof.** Suppose $c^4 + 3 = 0$. Then, since $c^3 = -1$, $c = 3$. Also $27 = -1$ in $\mathbb{Z}/p$, and so $p = 7$. We know that $c^n = c$ in $(\mathbb{Z}/p)^*$. Since $c = 3$ is a generator of $(\mathbb{Z}/7)^*$, $z^n = z$ for all $z$ in $(\mathbb{Z}/7)^*$. In particular if $z$ is in $R$, $\lambda(z) = cz^n = 3z$, and so $\lambda = (0\infty)(13)(26)(45)$.

Suppose $3c^4 + 1 = 0$. Then since $c^3 = -1$, $3c = 1$. So $27c^3 = 1$, $-27 = 1$ in $\mathbb{Z}/p$, and once again $p = 7$. Since $3c = 1$, $c = 5$. Arguing as in the paragraph above we find that $\lambda = (0\infty)(15)(23)(46)$. \[\square\]

Suppose now that $c = 3$. Then $z \rightarrow z + 1$ is in $G$, and since 2 is in $R$, $z \rightarrow 2z$ is also in $G$. To complete the proof of the classification theorem for $c = 3$ it suffices to show that the group of permutations of $\mathbb{Z}/7 \cup \{\infty\}$ generated by $z \rightarrow z + 1$, $z \rightarrow 2z$ and $\lambda$ is of order 168, and has a normal subgroup of order 8 (since $G$ contains this group, and $|G| = 168$). This can be shown by brute force, but here’s a conceptual argument using some of the theory of finite fields.

Let $F$ be the field of 8 elements, $\zeta$ be a generator of $F^*$, and $U$ be the group of permutations of $F$ generated by $x \rightarrow x + 1$, $x \rightarrow \zeta x$ and $x \rightarrow x^2$. If $r$ is in $F^*$, the conjugate of $x \rightarrow x + 1$ by $x \rightarrow rx$ is $x \rightarrow x + r$. It follows that $x \rightarrow x + 1$ and $x \rightarrow \zeta x$ generate the “affine group” of $F$, a group of order $7 \cdot 8 = 56$. Furthermore $x \rightarrow x^2$ is a permutation of $F$ of order 3 normalizing the affine group. We conclude that $|U| = 56 \cdot 3 = 168$. The translations $x \rightarrow x + a$ evidently form a normal subgroup of $U$ with 8 elements.

Now identify $F$ with $\mathbb{Z}/7 \cup \{\infty\}$ by mapping 0 to $\infty$ and $\zeta^i$ to $i$. Then $U$ may be viewed as a group of permutations of $\mathbb{Z}/7 \cup \{\infty\}$ of order 168. $x \rightarrow \zeta x$ is the permutation $z \rightarrow z + 1$, while $x \rightarrow x^2$ is the permutation $z \rightarrow 2z$. Now $\zeta$ has degree 3 over $\mathbb{Z}/2$, and so $\zeta^3 + \zeta + 1 = 0$ or $\zeta^3 + \zeta^2 + 1 = 0$. Choose $\zeta$ so that $\zeta^3 + \zeta + 1 = 0$. Then, $1 + 1 = 0$, $1 + \zeta = \zeta^4$, $1 + \zeta^2 = \zeta^6$ and $1 + \zeta^4 = \zeta^{12} = \zeta^5$. So $x \rightarrow x + 1$ is the permutation $(0\infty)(13)(26)(45)$ of $\mathbb{Z}/7 \cup \{\infty\}$. Thus the group generated by $z \rightarrow z + 1$, $z \rightarrow 2z$ and $(0\infty)(13)(26)(45)$ identifies with $U$, and has order 168, and a normal subgroup of order 8. The argument is the same when $c = 5$, except that we now take $\zeta$ with $\zeta^3 + \zeta^2 + 1 = 0$.
6 Simplicity results for $\text{PSL}_2(F)$ and final remarks

The simplicity result of Galois has been generalized in various ways. For example if $F$ is any field with more than 3 elements, finite or infinite, then $\text{PSL}_2(F)$ is a simple group. I’ll give one of the many proofs of this result. Let $N$ be a normal subgroup of $\text{SL}_2(F)$ containing some non-scalar matrix. If suffices to show that $N = \text{SL}_2(F)$.

**Lemma 6.1.** There is an $(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix})$ in $N$ with $b \neq 0$.

*Proof.* If not, then since $N$ is normal, every element of $N$ also has $c = 0$, and so is diagonal. But if $(\begin{smallmatrix} a & 0 \\ b & d \end{smallmatrix})$ is a non-scalar element of $N$, the conjugate of $(\begin{smallmatrix} a & 0 \\ b & d \end{smallmatrix})$ by $(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix})$ isn’t diagonal. \[
\]

Now let $P$ and $P'$ be the subgroups $(\begin{smallmatrix} 1 & 0 \\ r & 1 \end{smallmatrix})$ and $(\begin{smallmatrix} 1 & t \\ 0 & 1 \end{smallmatrix})$ of $\text{SL}_2(F)$. $P$ and $P'$ evidently generate $\text{SL}_2(F)$. Since $N$ is normal, $PN = NP$, and is the subgroup of $\text{SL}_2(F)$ generated by $P$ and $N$.

**Remark.** If we can show that $N \supset P$, then since it is normal it also contains $P'$, and so $N = \text{SL}_2(F)$.

**Lemma 6.2.** $PN = NP = \text{SL}_2(F)$.

*Proof.* Take $(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix})$ in $N$ as in Lemma 6.1. Multiplying this matrix on the left by $(\begin{smallmatrix} 1 & 0 \\ r & 1 \end{smallmatrix})$ has the effect of adding $r \cdot \text{(row 1)}$ to row 2. So $PN$ contains a matrix $(\begin{smallmatrix} a & 0 \\ b & d \end{smallmatrix})$. Multiplying this new matrix on the right by $(\begin{smallmatrix} 1 & 0 \\ s & 1 \end{smallmatrix})$ has the effect of adding $s \cdot \text{(column 2)}$ to column 1. So $P'NP = PN$ contains a matrix $(\begin{smallmatrix} a & b \\ s & t \end{smallmatrix})$. This matrix conjugates $P$ into $P'$. So $PN$ contains $P'$ as well as $P$, and is all of $\text{SL}_2(F)$.

**Proposition 6.3.** If $|F| > 3$, $N \supset P$. So by the remark above, $N = \text{SL}_2(F)$. Consequently $\text{SL}_2(F)$ is simple.

*Proof.* Take $a \neq 0, 1$ or $-1$ in $F$ and let $d = a^{-1}$. By Lemma 6.2, $(\begin{smallmatrix} 1 & 0 \\ r & 1 \end{smallmatrix}) \cdot B$ for some $B$ in the normal subgroup $N$. Then $B = (\begin{smallmatrix} 1 & 0 \\ r \cdot 1 \end{smallmatrix}) (\begin{smallmatrix} a & 0 \\ 0 & d \end{smallmatrix}) = (\begin{smallmatrix} a \cdot r & 0 \\ 0 & d \end{smallmatrix})$. A short calculation shows that as $A$ runs over all the elements of $P$, $(ABA^{-1}) \cdot B^{-1}$ also runs over all the elements of $P$. Since each $(ABA^{-1}) \cdot B^{-1}$ is in $N$, we’re done.

In presenting the material of this note to a class one might add the following remarks:
(1) Let $F$ be the field of $q$ elements where $q$ is a prime power. Then $PSL_2(F)$ has order $\frac{q^3-q}{2}$ or $q^3-q$ according as $q$ is odd or even. By Proposition 6.3 these groups are simple for $q > 3$.

(2) If $F$ is the field of $q$ elements it’s true that the “only” simple group having the same order as $PSL_2(F)$ is $PSL_2(F)$ itself. But I think that all proofs of this generalization of Frobenius’ result are very difficult. The case $q = 4$ is trivial — since $4^3 - 4 = \frac{3^3-3}{2} = 60$, uniqueness when $q = 4$ follows from the uniqueness when $q = 5$. The next cases of interest are $q = 9$ when $|G| = \frac{9^3-9}{2} = 360$, and $q = 8$ when $|G| = 8^3-8 = 504$. In 1893, F. N. Cole, [3] (best known to mathematicians for the establishment in his honor of the Cole prize), used intricate arguments to handle these cases. He starts by showing that $G$ is isomorphic to a doubly transitive permutation group on $q+1$ letters. But this is no longer an easy consequence of Sylow theory, as it is in the case of prime $q$.

(3) For $n > 2$, let $SL_n(F)$ be the group of $n$ by $n$ determinant 1 matrices with entries in $F$, and $PSL_n(F)$ be the quotient of $SL_n(F)$ by the group of determinant 1 scalar matrices. It can be shown that for all $F$ and for all $n > 2$ the group $PSL_n(F)$ is simple. But now the generalization of Frobenius’ theorem has an exception. If $F$ is the field of 4 elements then $PSL_3(F)$ and $PSL_4(\mathbb{Z}/2)$ are non-isomorphic simple groups of order 20,160. (The group of even permutations of 8 letters is also simple of order 20,160, but it is isomorphic to $PSL_4(\mathbb{Z}/2)$.)

References

[1] F. G. Frobenius. Über Gruppen des Grades $p$ oder $p + 1$. Gesammelte Abhandlungen v. 3, 223–229.

[2] E. Galois. Oeuvres Mathématiques (deuxième édition, 1951), pages 57–59 and page 28.

[3] F. N. Cole. Simple Groups as far as order 660. Amer. J. of Math., v. 15 no. 4 (1893), 303–315.