Galois's theorems on $\mathrm{PSL}(2, p)$

Péter P. Pálfy
Alfréd Rényi Institute of Mathematics
Budapest

AAA108
Wien, February 6, 2026

Évariste Galois

Bourg-la-Reine, October 25, 1811 – Paris, May 31, 1832

$\mathrm{PSL}(2, p)$

Galois studied the so-called modular equations from the theory of elliptic functions. (One concrete equation for each prime number p.) The Galois group of this equation is $\mathrm{PGL}(2, p)$. Analyzing this group he arrived at $\mathrm{PSL}(2, p)$ as a permutation group of degree $p + 1$ acting on the set $\{0, 1, 2, \ldots, p - 1, \infty\}$ by linear fractional transformations, i.e.,

$$x \mapsto \frac{ax + b}{cx + d},$$

where $ad - bc = 1$ (or equivalenty: a quadratic residue) modulo p.

(if $c \neq 0$, then $\infty \mapsto \frac{a}{c}$, $-\frac{d}{c} \mapsto \infty$; if $c = 0$, then $\infty \mapsto \infty$)

After Galois's death

Liouville published his manuscripts 14 years after his death:

Œuvres mathématiques d'Évariste Galois, Journal de Mathématiques Pures et Appliqués 11 (1846), 381–444.

Later the manuscripts became into the possession of the French Academy. Now they can be seen in digitalized form:

www.bibliotheque-institutdefrance.fr/numerisation/

The latest edition is by Πter Neumann

P. M. Neumann: The mathematical writings of Évariste Galois, EMS, 2011

The goal of this talk

Galois made two important statements on $\mathrm{PSL}(2, p)$ — conceived as a permutation group on $\{0, 1, 2, \ldots, p-1, \infty\}$ — in his famous "testamentary letter" written the day before his fatal duel.

He did not write down the proofs of these results. He probably planned to include them in his Second Mémoire (*Des équations primitives qui sont solubles par radicaux*), but this work had not been finished.

Our goal is to try to give a proof that uses ideas known to Galois.

The testamentary letter (1)

(in Пter Neumann's translation)

Letter to Auguste Chevallier

Paris, 29 May 1832

My dear friend,

I have done several new things in analysis. [i.e., mathematics]

Some concern the theory of equations, others integral functions.

...

The last application of the theory of equations relates to the modular equations of elliptic functions.

It is known that the group of the equation which has for its roots the sines of the amplitudes of the $p^2 - 1$ divisions of a period is this:

$$x_{k,l} \qquad x_{ak+bl,ck+dl}.$$

The testamentary letter (2)

Consequently the corresponding modular equation will have for group

$$x_{\frac{k}{l}} \qquad x_{\frac{ak+bl}{ck+dl}},$$

in which $\frac{k}{l}$ can take the $p+1$ values $\infty, 0, 1, 2, \ldots, p-1$. Thus, with the convention that k may be infinite one can simply write

$$x_k \qquad x_{\frac{ak+b}{ck+d}}.$$

Giving to a, b, c, d all the values one obtains $(p+1)p(p-1)$ permutations.

Now this group may be *properly* decomposed into two groups [i.e., into a normal subgroup and a coset], whose substitutions are

$$x_k \qquad x_{\frac{ak+b}{ck+d}},$$

$ad - bc$ being a quadratic residue of p.

The testamentary letter (3)

Thus simplified the group has $(p+1)p^{\frac{p-1}{2}}$ permutations. **But it is easy to see [!] that it is not further decomposable properly unless** $p = 2$ **or** $p = 3$. Thus in whatever way one transforms the equation its group will always have the same number of permutations.

But it is interesting to know if the degree can be reduced.

And to begin with, it cannot be reduced below p, because an equation of degree smaller than p cannot have p as a factor in the number of permutations of its group.

Let us see then whether the equation of degree $p+1$ whose roots x_k are indicated by giving to k all its values, including infinity, and of which the group has for substitutions

$$x_k \qquad x_{\frac{ak+b}{ck+d}},$$

$ad - bc$ being a square, may be reduced to degree p.

The testamentary letter (4)

Well, for that it is necessary that the group may be decomposed (improperly of course) into p groups [meaning 'cosets'] each of $(p+1)\frac{p-1}{2}$ permutations.

Let 0 and ∞ be **two letters that are linked** [*lettres conjointes* in the original] in one of these groups. The substitutions which do not make 0 and ∞ change their places will be of the form

$$x_k \qquad x_{m^2 k}.$$

Therefore if M is the letter linked with 1 the letter linked with m^2 will be $m^2 M$. When M is a square one will therefore have $M^2 = 1$. **But this simplification cannot take place except for** $p = 5$.

The testamentary letter (5)

For $p = 7$ one finds a group of $(p+1)\frac{p-1}{2}$ permutations, in which $\infty, 1, 2, 4$ have respectively $0, 3, 6, 5$ for linked letters. This group has its substitutions of the form

$$x_k \qquad x_{a\frac{k-b}{k-c}}$$

b being the letter linked with c, and a a letter [coefficient] which is residue or non-residue at the same time as c [corrected form: $b - c$].

For $p = 11$ the same substitutions will occur with the same notation,
$\infty, 1, 3, 4, 5,\ 9$ having respectively for their linked letters
$0,\ 2, 6, 8, 10, 7.$

Thus for the cases $p = 5,\ 7,\ 11$ the modular equation is reducible to degree p.

The testamentary letter (6)

In all rigour this reduction is not possible in the higher cases.

. . .

Often in my life I have risked advancing propositions of which I was not certain. But all that I have written here has been in my head for almost a year and it is not in my interest to make a mistake so that one could suspect me of having announced theorems of which I did not have the complete proof.

You will publicly ask Jacobi or Gauss to give their opinion not on the truth but on the importance of the theorems.

After that there will, I hope, be people who will find profit in deciphering all this mess.

I embrace your warmly,

E Galois

29 May 1832.

The two results of Galois about $\mathrm{PSL}(2, p)$

Let $p \geq 5$ be a prime number.

$|\mathrm{PSL}(2, p)| = \frac{1}{2}(p+1)p(p-1)$

Theorem 1. $\mathrm{PSL}(2, p)$ is a simple group.

Theorem 2. There exists a subgroup of index p in $\mathrm{PSL}(2, p)$ only in the cases $p = 5$, 7, 11.

Note that these are the most common nonabelian finite simple groups. If we list the simple groups in increasing order, then the proportion of $\mathrm{PSL}(2, p)$'s in this list tends to 1.

Galois did not prove that the alternating groups are simple.

"In all rigour"

One of Galois's papers, published in 1830, contains a remark:

It is worthy of note that the general modular equation of degree 6, corresponding to the number 5, can be reduced to one of the 5^{th} degree of which it is the reduced equation. By contrast, for higher degrees the modular equations cannot be reduced.

Linked letters

What did Galois mean by "linked letters"?

Recall

for $p = 5$ they are $0 \sim \infty$, $1 \sim 4$, $2 \sim 3$

for $p = 7$ they are $0 \sim \infty$, $1 \sim 3$, $2 \sim 6$, $4 \sim 5$

for $p = 11$ they are $0 \sim \infty$, $1 \sim 2$, $3 \sim 6$, $4 \sim 8$, $5 \sim 10$, $9 \sim 7$

Imprimitive permutation groups

Dossier 15 (title: Fragments on the theory of permutations and equations), folio 84 in the library of the Institut de France:

"An irreducible non-primitive group is one where one has n places and n letters such that one of the letters cannot occupy one of these places, without the n letters occupying the n places.

"One sees that the letters can be partitioned into classes of n letters such that the n places in question cannot be occupied at the same time except by one of these" [classes].

The linked letters referred to in Galois's letter form 2-element classes, i.e., blocks of imprimitivity in modern terms. So the subgroups of index p will be imprimitive with $\frac{p+1}{2}$ 2-element blocks.

Proof (1)

Theorem 2. There exists a subgroup of index p in $\mathrm{PSL}(2,p)$ ($p \geq 5$) only in the cases $p = 5$, 7, 11.

Proof. $G = \mathrm{PSL}(2,p)$, $|G : H| = p$. We will show $p \leq 11$.

$|G| = \frac{1}{2}(p+1)p(p-1)$

$G_\infty = \{x \mapsto ax + b \mid a \in (\mathbb{F}_p^\times)^2\}$

$|H_\infty|$ divides both $|H|$ and $|G_\infty|$, hence $|H_\infty| = \frac{1}{2}(p-1)$.

Every subgroup of this order in G_∞ is the stabilizer of another element, hence $H_\infty = G_{\infty,k}$ for some $k \in \mathbb{F}_p$.

Since G is doubly transitive, replacing H by a suitable conjugate, we may assume $H_\infty = G_{\infty,0} = \{x \mapsto ax \mid a \in (\mathbb{F}_p^\times)^2\}$.
Then H_∞ has exactly two fixed points: ∞ and 0, so $H_\infty = H_0$.

"Let 0 and ∞ be two letters that are linked in one of these groups."

Proof (2)

$|H : H_\infty| = p + 1$, so H is transitive.

If $h \in H$ and $H_y = H_x$, then $H_{yh} = h^{-1} H_y h = h^{-1} H_x h = H_{xh}$. If we denote by $x \sim y$ that $H_x = H_y$, then we obtain an H-invariant equivalence relation. So H is imprimitive with 2-element blocks. This is what Galois calls linked letters.

In particular, if $a \in (\mathbb{F}_p^\times)^2$ and $x \sim y$ $(x, y \in \{1, 2, \ldots, p-1\})$, then $ax \sim ay$.

Keeping the notation of Galois, let M be the letter linked to 1.

If M is a square, then $1 \sim M \Rightarrow M \cdot 1 \sim M \cdot M$, so $M^2 = 1$, $M = -1$ (this can happen only if $p \equiv 1 \pmod 4$), and every square x is linked to $-x$ which is also a square. Then any non-square is linked to a non-square. If for a non-square x we have $x \sim M'x$, then M' is a square, $M'x \sim M'^2 x$, so $M'^2 = 1$, $M' = -1$.

Proof (3): M is a square

Thus every $x \in \{1, 2, \ldots, p-1\}$ is linked to $-x$.

As H is transitive, there must be an $h \in H$ mapping 1 to ∞.

Since h preserves $\sim$, it maps -1 to 0, hence

$$h(x) = a\frac{x+1}{x-1},$$

with a suitable a ($-2a$ must be a square).

Now for every $x \in \{2, 3, \ldots, p-2\}$ the pair of linked elements x, $-x$ is mapped to some pair of linked elements, so $h(-x) = -h(x)$, that is

$$a\frac{(-x)+1}{(-x)-1} = -a\frac{x+1}{x-1},$$

or, equivalently, $x^2 + 1 = 0$. Thus $|\{2, 3, \ldots, p-2\}| \leq 2$, $p \leq 5$.

"But this simplification cannot take place except for $p = 5$."

Proof (4): M is a non-square

If M is non-square, then $\forall x \in (\mathbb{F}_p^\times)^2 : x \sim Mx$.

Let $h \in H$ such that $h(1) = \infty$. Then $h(M) = 0$, so $h(x) = a(x - M)/(x - 1)$.

If $x \neq 0, 1$ is a square, then the linked pair x, Mx is mapped to a linked pair y, My for some square $y \neq 0$. So we must have for every square $x \neq 0, 1$ that

$$\{x, Mx\} \mapsto \left\{ a\frac{x - M}{x - 1}, a\frac{Mx - M}{Mx - 1} \right\} = \{y, My\},$$

that is

$$Ma\frac{x - M}{x - 1} = a\frac{Mx - M}{Mx - 1} \quad \text{or} \quad Ma\frac{Mx - M}{Mx - 1} = a\frac{x - M}{x - 1}.$$

Then we obtain the equations $x^2 - (M + 1)x + 1 = 0$, and $x^2 - (\frac{1}{M} + 1)x + 1 = 0$, respectively. There can be at most two squares satisfying each of these equations, so the number of nonzero squares in $\mathbb{F}_p$ is at most $1 + 2 + 2 = 5$, hence $p \leq 11$. $\square$

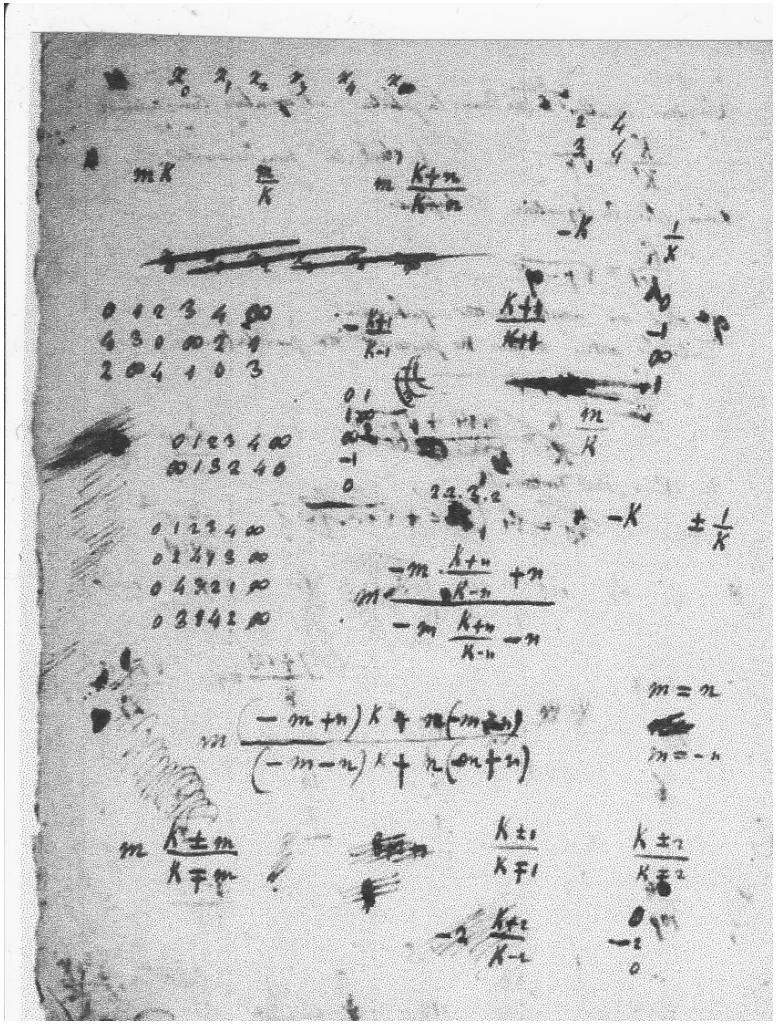
Later proofs

Enrico Betti, Sopra l'abbassamento delle equazioni modulari delle funzioni ellittiche, Annali di scienze matematiche e fisiche 4 (1853), 81–100.

Camille Jordan, Traité des substitutions et des équations algébriques, 1870. (Sections 481–484)

Joseph Gierster, Die Untergruppen der Galois'schen Gruppe der Modulargleichungen für den Fall eines primzahligen Transformationsgrades, Mathematische Annalen 18 (1881), 319–365.

Some calculations by Galois



Thank you for your attention.
Enjoy algebra.