1. Introduction

Any finite group of rotations of the round 2-sphere describes a regular polygon or polytope: look at the action of the group on a point of the sphere. In the 1870s, Klein showed that the symmetry groups of regular polygons and polytopes are the only way to obtain finite groups of rotations of the sphere [7, Ch.V.2]. Klein’s approach was to use stereographic projection to identify the 2-sphere in \( \mathbb{R}^3 \) with the Riemann sphere \( \mathbb{C} \cup \{ \infty \} \), and then to classify the finite subgroups of Möbius transformations \( z \mapsto \frac{az + b}{cz + d} \). In modern parlance, we could say that Klein classified the finite subgroups of \( \text{PGL}_2(\mathbb{C}) \), the group of invertible \( 2 \times 2 \) complex matrices modulo scalar matrices.

One can also look at Möbius transformations with coefficients in a finite field, as Galois did in the early 1830s while studying symmetries of equations [5, pp.28-30]. Later, Klein’s technique was extended by his student, Gierster, to give a complete description of the subgroups of \( \text{PGL}_2(\mathbb{F}_q) \) when \( q \) is an odd prime [6]. A decade after that, E.H. Moore further extended this method to classify the subgroups of \( \text{PGL}_2(\mathbb{F}_q) \) when \( q \) is an arbitrary prime power [8]. The definitive version of this method appears in the writing of Moore’s student, L.E. Dickson [3, §239-261]. (To be precise, all of the authors in this paragraph considered subgroups of \( \text{PSL}_2(\mathbb{F}_q) \), the subgroup of \( \text{PGL}_2(\mathbb{F}_q) \) consisting of classes of matrices with square determinant. As \( \text{PSL}_2(\mathbb{F}_q) \) is of index at most 2 inside \( \text{PGL}_2(\mathbb{F}_q) \), little is lost in discussing \( \text{PGL}_2(\mathbb{F}_q) \) instead.)

More recently, Beauville gave a beautiful exposition of the classification of finite subgroups of \( \text{PGL}_2(k) \) of order prime to \( \text{char}(k) \) — for an arbitrary field \( k \) — using Galois cohomology [1]. His proof takes advantage of the accidental isomorphism \( \text{PGL}_2(k) \cong \text{SO}(k, q) \), where the latter is the special orthogonal group for the quadratic form \( q(x, y, z) = x^2 + yz \). (This isomorphism exists because \( \text{PGL}_2(k) \) is the automorphism group of the projective line, which may be embedded in \( \mathbb{P}^2 \) as the conic \( x^2 + yz = 0 \).) Serre also gives an excellent discussion of existence results for certain subgroups of \( \text{PGL}_2(k) \) in [10, §2].

In the present work, we extend these classifications to arbitrary finite subgroups \( G \subset \text{PGL}_2(k) \). The case of new interest is then an infinite field of characteristic \( p > 0 \) and a subgroup \( G \) whose order is divisible by \( p \) — a \( p \)-irregular subgroup. We learn that a finite \( p \)-irregular subgroup of \( \text{PGL}_2(k) \) is isomorphic to \( \text{PSL}_2(\mathbb{F}_q) \) or \( \text{PGL}_2(\mathbb{F}_q) \) for \( q \) a power of the characteristic of \( k \), to a \( p \)-semi-elementary group, to a dihedral group, or to the alternating group on 5 letters. Theorems A and B in the next section are our novel contributions in this article: Theorem A gives precise conditions for the existence of \( p \)-irregular subgroups, and Theorem B gives the classification of such subgroups up to conjugacy inside \( \text{PGL}_2(k) \).
The subgroups of $\text{PGL}_2$ came to the author’s attention as automorphism groups of rational functions, viewed as discrete dynamical systems on the projective line. Given a rational function $\phi \in \mathbb{Q}(z)$, the automorphism group is $\text{Aut}_D(\mathbb{Q}) = \{f \in \text{PGL}_2(\mathbb{Q}) : f \circ \phi \circ f^{-1} = \phi \}$. The author, Manes, and Viray designed an algorithm for computing $\text{Aut}_D(\mathbb{Q})$ by piecing it together from $\text{Aut}_D(F_p) \subset \text{PGL}_2(F_p)$ for several primes $p$ of good reduction for $\phi$ [4]; evidently the classification of subgroups of $\text{PGL}_2(F_p)$ up to conjugation is invaluable for such a pursuit. Such a classification does not seem to appear explicitly in the literature in a form that can be readily cited, and so we deduce it as a special case of the main results of the present work. See Theorem D in the next section.

This article consists of two main parts, which are somewhat disparate in nature. The first part — Sections 3 through 6 — is devoted to generalizing the arguments of Klein, Gierster, and Moore, following Dickson’s exposition [3, §239–261], in order to give a complete classification of finite subgroups of $\text{PGL}_2(k)$ when $k$ is algebraically closed.1 The argument is elementary — it uses only some basics of group actions, the Sylow theorems, and a little knowledge of the action of $\text{PGL}_2(k)$ on $\mathbb{P}^1(k)$. We have endeavored to keep this part of the article completely self-contained; it could serve as the basis for a reading project by an undergraduate with a background in abstract algebra. As a natural byproduct of this approach, we were able to recover the classical description of finite $p$-regular subgroups of $\text{PGL}_2(k)$ for an algebraically closed field $k$ (cf. Theorem C). We stress that nothing in this part of the article is new; however, the next part depends heavily on these statements.

The second part of this paper — Sections 7 and 10 — completes the classification of finite subgroups of $\text{PGL}_2(k)$ by first passing to separably closed fields, and then by applying Galois descent. This part is less elementary and draws heavily from Beauville’s paper [1]. The main idea is to use a cohomological parameterization of the set of conjugacy classes of subgroups in $\text{PGL}_2(k)$ that coincide over a separable closure of $k$. For $p$-irregular subgroups, the relevant cohomology set turns out to be trivial, and so we reduce to the case of separably closed fields. In this sense, the classification of $p$-irregular subgroups is easier than its $p$-regular counterpart.

We close this section with a more precise description of the contents of the article. Section 2 contains our notational conventions and the statements of the main theorems. Section 3 collects a number of invaluable trace/determinant equations that characterize when an element of $\text{PGL}_2(k)$ has a certain small order. In Section 4, we study several seemingly special subgroups of $\text{PGL}_2(k)$; we then show that these special cases exhaust all possible finite subgroups in Sections 5 ($p$-regular subgroups) and 6 ($p$-irregular subgroups). We will restrict to the case in which $k$ is algebraically closed in Sections 3 through 6. Ignoring the question of when certain equations actually have solutions in $k$ clarifies the presentation dramatically. In the remainder of the paper, we will want to lean on the results of Serre and Beauville on existence and classification of $p$-regular subgroups of $\text{PGL}_2(k)$; we recall these in the form we require in Section 7. In Section 8 we pass to separably closed fields $k$; this requires extra work only in characteristic 2. Section 9 contains the Galois cohomology computation necessary to pass from separably closed fields to the general case. We finish in Section 10 with proofs of the main theorems.

2. The Classification

Let $k$ be a field. Define $\text{GL}_2(k)$ to be the group of invertible $2 \times 2$ matrices with entries in $k$; it contains an isomorphic copy of $k^\times$ given by multiples of the identity matrix. We write $\text{PGL}_2(k) = \text{GL}_2(k)/k^\times$, and elements of $\text{PGL}_2(k)$ will be represented by equivalence classes of matrices $\left( \begin{array}{cc} \alpha & \beta \\ \gamma & \delta \end{array} \right)$ with $\alpha \delta - \beta \gamma \neq 0$. Here $\left( \begin{array}{cc} \alpha & \beta \\ \gamma & \delta \end{array} \right) = \left( \begin{array}{cc} \lambda \alpha & \lambda \beta \\ \lambda \gamma & \lambda \delta \end{array} \right)$ for any $\lambda \neq 0$. We write $I$ for the identity of $\text{PGL}_2(k)$. An element $s \in \text{PGL}_2(k)$ acts on $\mathbb{P}^1(k) = k \cup \{\infty\}$ by the formula $s.z = \frac{\alpha z + \beta}{\gamma z + \delta}$, with the usual conventions that $s.\infty = \alpha/\gamma$ and $\alpha/0 = \infty$.

The determinant map $\det : \text{GL}_2(k) \to k^\times$ descends to a homomorphism $\overline{\det} : \text{PGL}_2(k) \to k^\times/(k^\times)^2$. Write $\text{PSL}_2(k)$ for the kernel of $\overline{\det}$.

---

1A list of isomorphism types of subgroups of $\text{PSL}_2(k)$ for $k$ algebraically closed appears in Suzuki’s book [11, p.404], but no description of conjugacy classes is given. In addition, Suzuki incorrectly attributes the classification of subgroups of $\text{PSL}_2(F_q)$ to Dickson [11, p.392].
The letter $q$ will always denote a power of $p$. We say that an element of a finite group $G$ is $p$-regular if its order is prime to $p$, and we say that $G$ is $p$-regular if all of its elements are $p$-regular. Otherwise, an element or a group is $p$-irregular.

For the following statements, we will use the notation $O_n$, $S_n$, and $A_n$ for the dihedral group with $2n$ elements, the symmetric group on $n$ letters, and the alternating group on $n$ letters, respectively. Write $\mu_n(k)$ for the group of $n$-th roots of unity in $k$.

An abstract finite group $G$ will be called $p$-semi-elementary if it has a unique Sylow $p$-subgroup $P$ of exponent $p$ with $G/P$ cyclic. If $G/P$ is trivial, we say that $G$ is $p$-elementary. Write $k_3$ for an algebraic closure of $k$. A $p$-semi-elementary subgroup $G \subset \text{PGL}_2(k)$ acts on $\mathbb{P}^1(k_3)$ with a unique fixed point ($\S$4.2). If the fixed point is $k$-rational, we say that $G$ is split; otherwise, $G$ is non-split.

As we will see in Theorem B, any finite $p$-irregular subgroup of $\text{PGL}_2(k)$ is isomorphic to $\text{PSL}_2(\mathbb{F}_q)$ or $\text{PGL}_2(\mathbb{F}_q)$ for some $q$, to a $p$-semi-elementary group, to a dihedral group, or to $A_5$. The following theorem describes the precise conditions under which these types of subgroups exist in $\text{PGL}_2(k)$.

**Theorem A** (Existence of Finite $p$-Irregular Subgroups). Let $k$ be a field of characteristic $p > 0$.

1. Let $q$ be a power of $p$. Then $\text{PGL}_2(k)$ contains subgroups isomorphic to $\text{PGL}_2(\mathbb{F}_q)$ and $\text{PSL}_2(\mathbb{F}_q)$ if and only if $\mathbb{F}_q \subset k$.
2. Let $m \geq 1$ and $n \geq 1$ be integers with $n$ coprime to $p$. Let $e$ be the order of $p$ in $\langle \mathbb{Z}/n\mathbb{Z} \rangle^\times$. Then $\text{PGL}_2(k)$ contains a $p$-semi-elementary subgroup of order $p^m n$ if and only if $\mathbb{F}_{p^e} \subset k$, $e \mid m$, and $m \leq \dim_{\mathbb{F}_p}(k)^2$.
3. If $p = 2$ and $m \geq 1$ is an integer, then $\text{PGL}_2(k)$ contains a non-split 2-elementary subgroup of order $2^m$ if and only if $k$ contains a non-square element.
4. If $p = 2$ and $n > 1$ is odd, then $\text{PGL}_2(k)$ contains a dihedral subgroup $O_n$ if and only if $\zeta + \zeta^{-1} \in k$ for some primitive $n$-th root of unity $\zeta$.
5. If $p = 3$, then $\text{PGL}_2(k)$ contains a subgroup isomorphic to $A_5$ if and only if $\mathbb{F}_9 \subset k$.

**Theorem B** (Classification of Finite $p$-Irregular Subgroups). Let $k$ be a field of characteristic $p > 0$.

1. Fix $q > 2$ a power of $p$ such that $\mathbb{F}_q \subset k$. There is exactly one conjugacy class of subgroups isomorphic to each of $\text{PSL}_2(\mathbb{F}_q)$ and $\text{PGL}_2(\mathbb{F}_q)$.
2. Let $m, n \geq 1$ be integers with $n$ coprime to $p$, and suppose that $k$ contains a primitive $n$-th root of unity. The conjugacy classes of split $p$-semi-elementary subgroups of order $p^{{\lambda}n}$ are in bijection with the set of homothety classes of rank-$m$ subgroups $\Gamma \subset k$ that are stable under multiplication by elements of $\mu_n(k)$. The correspondence is

$$\Gamma \mapsto \left( \mu_n(k) \Gamma \right).$$

3. Suppose that $p = 2$, and let $m \geq 1$ be an integer. The conjugacy classes of non-split 2-elementary subgroups of order $2^m$ are parameterized by pairs $(k(\tau), G)$, where $k(\tau)$ is a quadratic inseparable extension of $k$ and $G$ is a subgroup of order $2^m$ of the abelian group

$$\{1\} \cup \left\{ \left( \begin{array}{cc} \alpha & \tau^2 \\ 1 & \alpha \end{array} \right) : \alpha \in k \setminus \{\tau\} \right\}.$$

4. Suppose that $p = 2$ and $n > 1$ is an odd integer such that $\lambda := \zeta + \zeta^{-1} \in k$ for some primitive $n$-th root of unity $\zeta$. Let $\text{Dih}_n(k)$ denote the set of conjugacy classes of dihedral subgroups of $\text{PGL}_2(k)$.

---

2The condition $\mathbb{F}_{p^e} \subset k$ is equivalent to the assertion that there is a primitive $n$-th root of unity in $k$.

3Two subgroups $\Gamma, \Gamma' \subset k$ are homothetic if $\Gamma' = \alpha \Gamma$ for some $\alpha \in k^\times$. 

---

3
of order 2n. The map $\mathfrak{Di}_{n}(k) \to k^\times/(k^\times)^2$ defined by $G \mapsto \det(t)$ for any involution $t \in G$ is well defined and injective. It is surjective if $k$ contains a primitive $n$-th root of unity.

(5) If $\mathbb{F}_9 \subset k$, then there is exactly one conjugacy class of subgroups isomorphic to $\mathfrak{A}_5$.

Any $p$-irregular subgroup of $\text{PGL}_2(k)$ is among the five types listed here.

**Remark 2.1.** Over an algebraically closed field $k$, dihedral and $p$-semi-elementary subgroups may be characterized geometrically as follows. A subgroup of $\text{PGL}_2(k)$ ($p$-regular or otherwise) is dihedral if and only if it stabilizes a pair of distinct points of $\mathbb{P}^1(k)$, but does not fix them. A subgroup is $p$-semi-elementary if it fixes a unique point of $\mathbb{P}^1(k)$.

**Remark 2.2.** The map $\mathfrak{Di}_{n}(k) \to k^\times/(k^\times)^2$ from Theorem B(4) is not surjective in general. For example, taking $k = \mathbb{F}_2(T)$ and $n = 3$, one can show that the class of $T$ does not lie in the image.

The methods used to prove Theorem B allow us, with essentially no extra work, to give an elementary classification of the finite $p$-regular subgroups of $\text{PGL}_2(k)$ up to conjugation when $k$ is separably closed. By elementary, we mean that it avoids the use of representation theory; see [1] for the representation theory approach and for analogues of Theorems A and B for $p$-regular finite subgroups.

**Theorem C** (Finite $p$-regular subgroups). Let $k$ be a separably closed field, and let $G$ be a finite subgroup of $\text{PGL}_2(k)$ such that $p \nmid |G|$. Then up to conjugation, $G$ is one of the following subgroups:

1. $G = \langle (\zeta^i 1) \rangle$ for some $\zeta \in k^\times$; here $G$ is cyclic.
2. $G = \langle (\zeta^i 1) \rangle \times \langle (1 \pm 1) \rangle$ for some $\zeta \in k^\times$; here $G$ is dihedral.
3. $G = N \rtimes C \cong \mathfrak{A}_4$, where $N = \{ (\pm 1, 1) \}, \{ (1, \pm 1) \}$ and $C = \{ I, (1 1\pm 1) \}$, where $i$ is any primitive fourth root of unity.
4. $G = \langle T, (1 1) \rangle \cong \mathfrak{S}_4$, where $T = N \rtimes C \cong \mathfrak{A}_4$ is the group in (3).
5. $G = \langle s, t \rangle \cong \mathfrak{A}_5$, where $s = (\lambda^{-1}, 1), t = \left( \frac{1}{\lambda} - 1, -1 \right)$, and $\lambda$ is any primitive fifth root of unity. These generators satisfy $s^5 = t^2 = (st)^3 = I$.

In particular, if $G, G' \subset \text{PGL}_2(k)$ are (abstractly) isomorphic finite groups, then they are conjugate.

**Remark 2.3.** The symmetric and alternating subgroups that occur in the classification of $p$-regular subgroups (Theorem C) also appear in Theorems A and B, albeit in disguise. When $p = 2$, the subgroups isomorphic to $\mathfrak{A}_4$ are all conjugate to the $p$-semi-elementary subgroup $B(\mathfrak{F}_4) = \left( \mathfrak{F}_4^\times \mathfrak{F}_4^1 \right)$; a subgroup isomorphic to $\mathfrak{A}_5$ is necessarily conjugate to $\text{PGL}_2(\mathfrak{F}_4)$; and there is no finite subgroup of $\text{PGL}_2(k)$ isomorphic to $\mathfrak{S}_4$. When $p = 3$, any subgroup isomorphic to $\mathfrak{A}_4$ (resp. $\mathfrak{S}_4$) is conjugate to $\text{PSL}_2(\mathfrak{F}_3)$ (resp. $\text{PGL}_2(\mathfrak{F}_3)$). When $p = 5$, any subgroup isomorphic to $\mathfrak{A}_5$ is conjugate to $\text{PSL}_2(\mathfrak{F}_5)$.

**Remark 2.4.** For the classification of $p$-regular subgroups up to conjugation over an arbitrary field, see [1]. We summarize these results in §7.

Finally, as a concrete application of these results we characterize all subgroups of the projective linear group over a finite field. A $p$-regular cyclic subgroup of $\text{PGL}_2(\mathbb{F}_q)$ is said to be **split** if it fixes two $\mathbb{F}_q$-rational points of $\mathbb{P}^1(\mathbb{F}_q)$. It is called **non-split** if it fixes a pair of quadratic conjugate points of $\mathbb{P}^1(\mathbb{F}_q^2)$. A $p$-regular dihedral subgroup of $\text{PGL}_2(\mathbb{F}_q)$ will be called split or non-split depending on whether its normal cyclic subgroup is split or non-split.

**Theorem D.** Let $\mathbb{F}_q$ be a finite field with $q = p^r$, and write $G = \text{PGL}_2(\mathbb{F}_q)$. Each conjugacy class of nontrivial subgroups of $G$ is described by one of the following ten cases:
(1) (Split cyclic) If \( n \geq 2 \) satisfies \( q \equiv 1 \pmod{n} \), then \( G \) contains a unique conjugacy class of split cyclic subgroups of order \( n \).

(2) (Non-split cyclic) If \( n \geq 2 \) satisfies \( q \equiv -1 \pmod{n} \), then \( G \) contains a unique conjugacy class of non-split cyclic subgroups of order \( n \).

(3) (Split dihedral) Suppose \( n \geq 3 \) satisfies \( q \equiv 1 \pmod{n} \). If \( q \equiv 1 \pmod{2n} \), then \( G \) contains two conjugacy classes of split dihedral subgroups of order \( 2n \); otherwise, it contains one such conjugacy class.

(4) (Non-split dihedral) Suppose \( n \geq 3 \) satisfies \( q \equiv -1 \pmod{n} \). If \( q \equiv -1 \pmod{2n} \), then \( G \) contains two conjugacy classes of non-split dihedral subgroups of order \( 2n \); otherwise, it contains one such conjugacy class.

(5) (4-groups) If \( q \) is odd, then \( G \) contains exactly two conjugacy classes of subgroups isomorphic to \((\mathbb{Z}/2\mathbb{Z})^2\).

(6) If \( p \) is odd, or if \( p = 2 \) and \( r \) is even, then \( G \) contains a unique conjugacy class of subgroups isomorphic to \( \mathfrak{A}_4 \).

(7) If \( p \neq 2 \), then \( G \) contains a unique conjugacy class of subgroups isomorphic to \( \mathfrak{S}_4 \).

(8) If \( q \equiv 0, \pm 1 \pmod{5} \), then \( G \) contains a unique conjugacy class of subgroups isomorphic to \( \mathfrak{A}_5 \).

(9) If \( s \mid r \), then \( G \) contains a unique conjugacy class of subgroups isomorphic to \( \text{PGL}_2(\mathbb{F}_{p^r}) \) and \( \text{PSL}_2(\mathbb{F}_{p^r}) \).

(10) If \( m, n \) are positive integers with \( m \leq r \) and \( n \) coprime to \( p \), and if \( e \mid \gcd(r, m) \), where \( e \) is the order of \( p \) in \((\mathbb{Z}/n\mathbb{Z})^\times \), then \( G \) contains \( p \)-semi-elementary subgroups of order \( p^mn \). The conjugacy classes of such subgroups are in bijection with the set of homothety classes of \( \mathbb{F}_{p^r} \)-vector subspaces of \( \mathbb{F}_q \) of dimension \( m/e \).

3. Fixed points

**Convention.** Throughout this section, \( k \) is an algebraically closed field of characteristic \( p \geq 0 \).

The fixed points of an element \( s \in \text{PGL}_2(k) \) will be of paramount interest in our study, and it will often be convenient to relocate them by a suitable conjugation. More precisely, if \( s \) fixes the point \( x \in \mathbb{P}^1(k) \), and if \( t \in \text{PGL}_2(k) \) satisfies \( t.x = y \), then \( tst^{-1} \) fixes \( y \). We say that we have “conjugated the fixed point \( x \) to \( y \)”.

If \( s = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \text{PGL}_2(k) \) is nontrivial, then \( s \) has either one or two distinct fixed points in \( \mathbb{P}^1(k) \). Indeed, the fixed point equation \( s.z = z \) is equivalent to

\[
\gamma z^2 + (\delta - \alpha)z - \beta = 0. 
\]  

(3.1)

If \( \gamma = 0 \), then \( z = \infty \) is fixed, and the fixed point equation has at most one solution. Otherwise, the fixed point equation has at most two solutions. An immediate consequence of these observations is the following well known fact about \( \text{PGL}_2(k) \):

**Proposition 3.1.** Let \( s \in \text{PGL}_2(k) \). If \( s \) fixes three distinct points of \( \mathbb{P}^1(k) \), then \( s \) is the identity.

Assume now that \( s \) has finite order. If \( s \) has a unique fixed point, we may conjugate it to \( \infty \) and see that \( s.z = z + \beta \), or in matrix form: \( s = \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix} \). Since \( s^m = \begin{pmatrix} 1 & m\beta \\ 0 & 1 \end{pmatrix} \), we find \( s \) has order \( p > 0 \).

Conversely, if \( s \in \text{PGL}_2(k) \) has order \( p > 0 \), then we claim that \( s \) has a unique fixed point. For suppose \( s \) has two distinct fixed points, and let us conjugate them to 0 and \( \infty \). Then \( s.z = \alpha z \), so that \( \alpha^p = 1 \); hence, \( \alpha = 1 \). This contradiction shows that \( s \) must have a unique fixed point.
Lemma 3.2. Let $s = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \text{PGL}_2(k)$ be nontrivial and of finite order. Write $\text{tr}(s)$ for the trace of $s$ (which is well defined up to a scalar multiple). The following are equivalent:

1. $s$ has a unique fixed point in $\mathbb{P}^1(k)$;
2. $s$ has order $p > 0$; and
3. $\text{tr}(s)^2 = 4 \det(s)$.

Proof. The equivalence of the first two statements was proved above. We now prove the equivalence of the first and third statements. The final statement is homogeneous and quadratic in the entries of the matrix $s$, so it is well defined on $\text{PGL}_2(k)$. Moreover, the first and third statements are invariant under conjugation in $\text{PGL}_2(k)$, so we may assume that $s$ fixes $\infty$. Thus $\gamma = 0$. Now $\infty$ is the unique fixed point of $s$ precisely when $\delta - \alpha = 0$ by (3.1), or equivalently, when

$$\text{tr}(s)^2 - 4 \det(s) = (\alpha + \delta)^2 - 4\alpha\delta = (\delta - \alpha)^2 = 0.$$

We say that $s$ is unipotent if it satisfies the three equivalent conditions in the lemma. Note that a unipotent element can be conjugated to $\begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix}$.

Lemma 3.3. Let $s = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \text{PGL}_2(k)$ be nontrivial.

- $s$ has order 2 if and only if $\text{tr}(s) = 0$.
- $s$ has order 3 if and only if $\text{tr}(s)^2 = \det(s)$.
- $s$ has order 5 if and only if $\text{tr}(s)^4 - 3\text{tr}(s)^2 \det(s) + \det(s)^2 = 0$.

Remark 3.4. Note that these trace/determinant equations are homogeneous in the entries of $s$ of degree 1, 2, and 4, respectively, so that their solutions are well defined elements of $\text{PGL}_2(k)$.

Remark 3.5. Using Chebychev polynomials, one can formulate trace/determinant equations like this to characterize the elements of any order.

Proof. In all cases, the conditions are invariant under conjugation, so we may assume that $s$ fixes $\infty$. If $\infty$ is the only fixed point, then the previous lemma shows that $s = \begin{pmatrix} 1 & \gamma \\ 0 & 1 \end{pmatrix}$ for some nonzero $\gamma \in k$ and $s$ has order $p$. For $p = 2, 3$, the third statement of the previous lemma reduces immediately to the desired equations for the trace and determinant of $s$. For $p = 5$, we see that

$$\text{tr}(s)^4 - 3\text{tr}(s)^2 \det(s) + \det(s)^2 = [\text{tr}(s)^2 - 4 \det(s)]^2,$$

so that the desired criterion for order 5 reduces to the one in the previous lemma.

Suppose now that $s$ has two distinct fixed points. Then we may suppose after conjugation that it fixes 0 and $\infty$. Hence $s = \begin{pmatrix} \lambda & 0 \\ 0 & 1 \end{pmatrix}$, and $s$ has order $n$ precisely when $\lambda$ is a primitive $n$-th root of unity. For $n = 2$, this means $\lambda = -1$, so that $\text{tr}(s) = 0$. For $n = 3$, this means $\lambda^2 + \lambda + 1 = 0$, so that

$$\text{tr}(s)^2 - \det(s) = (\lambda + 1)^2 - \lambda = 0.$$

For $n = 5$, it means $\lambda^4 + \lambda^3 + \lambda^2 + \lambda + 1 = 0$, so that

$$\text{tr}(s)^2 - 3\text{tr}(s)^2 \det(s) + \det(s)^2 = (\lambda + 1)^4 - 3\lambda(\lambda + 1)^2 + \lambda^2 = 0.$$

\[\square\]

4. Special subgroups

Convention. Throughout this section, $k$ is an algebraically closed field unless otherwise specified.
4.1. Cyclic subgroups. If $s \in \text{PGL}_2(k)$ is nontrivial, then it fixes at least one point of $\mathbb{P}^1(k)$, which we may assume is $\infty$ after a suitable conjugation. If $\infty$ is the only fixed point of $s$, then $s = \left( \begin{smallmatrix} 1 & \beta \\ 1 & 1 \end{smallmatrix} \right)$, and it generates a cyclic group of order $p$ (Lemma 3.2), where $\text{char}(k) = p$. Moreover, we see that $\left( \begin{smallmatrix} \beta^{-1} \\ 1 \end{smallmatrix} \right) s \left( \begin{smallmatrix} \beta \\ 1 \end{smallmatrix} \right) = \left( \begin{smallmatrix} 1 \\ 1 \end{smallmatrix} \right)$, and hence every cyclic subgroup of order $p$ is conjugate to the subgroup $\langle \left( \begin{smallmatrix} 1 \\ 1 \end{smallmatrix} \right) \rangle$ inside $\text{PGL}_2(k)$.

Now suppose that $s$ fixes two distinct points of $\mathbb{P}^1(k)$. After a suitable conjugation, we may assume that $s$ fixes 0 and $\infty$. Hence $s = \left( \begin{smallmatrix} \alpha \\ 1 \end{smallmatrix} \right)$. If $\alpha^m \neq 1$ for any $m \neq 0$, then $s$ has infinite order and generates a subgroup isomorphic to $\mathbb{Z}$. If $\alpha^m = 1$ for some $m > 1$, then $\alpha$ is a root of unity in $k$. The roots of unity in $k$ have order prime to the characteristic. Hence $s$ generates a $p$-regular cyclic subgroup of $\text{PGL}_2(k)$.

Proposition 4.1. Let $G$ be a nontrivial finite cyclic subgroup of $\text{PGL}_2(k)$. Then exactly one of the following is true:

1. $|G| = p$, it fixes a unique point of $\mathbb{P}^1(k)$, and $G$ is conjugate to $\left( \begin{smallmatrix} 1 & \infty \\ 1 & 1 \end{smallmatrix} \right)$; or

2. $G$ is $p$-regular, it fixes exactly two points of $\mathbb{P}^1(k)$, and $G$ is conjugate to $\langle \lambda \rangle$ for some (cyclic) subgroup $\Lambda$ of the roots of unity of $k$.

In particular, the order of a finite cyclic group uniquely determines its conjugacy class in $\text{PGL}_2(k)$.

Proof. We have already proved everything but the final statement about conjugacy classes. If $|G| = p$, then it is conjugate to $\left( \begin{smallmatrix} 1 & \infty \\ 1 & 1 \end{smallmatrix} \right)$, so that any cyclic group of order $p$ lies in the same conjugacy class. If $p \nmid |G|$, then it is conjugate to $\langle \lambda \rangle$ for some finite cyclic group $\Lambda \subset k^\times$. The group of roots of unity in $k^\times$ contains a unique cyclic subgroup of every order prime to the characteristic. That is, the order of $G$ uniquely determines $\Lambda$, and hence also the conjugacy class of $G$.

Another normal form for $p$-regular cyclic subgroups will be useful when we pass to non-algebraically closed fields.

Corollary 4.2. Let $G$ be a finite $p$-regular cyclic subgroup of $\text{PGL}_2(k)$ of order $n \geq 3$, and let $\zeta$ be a primitive $n$-th root of unity. Then $G$ is conjugate to the subgroup generated by $\langle \lambda + 1, -1 \rangle$, where $\lambda = \zeta + \zeta^{-1}$.

Proof. The elements $\langle \lambda + 1, -1 \rangle$ and $\langle \zeta \rangle$ are conjugate:

$$\left( \begin{smallmatrix} 1 & -\zeta^{-1} \\ 1 & -\zeta \end{smallmatrix} \right) \left( \begin{smallmatrix} \lambda + 1 \\ 1 \end{smallmatrix} \right) \left( \begin{smallmatrix} 1 & -\zeta^{-1} \\ 1 & -\zeta \end{smallmatrix} \right)^{-1} = \left( \begin{smallmatrix} \lambda + 1 \\ 1 \end{smallmatrix} \right).$$

4.2. $p$-subgroups. In this section, we will assume $\text{char}(k) = p > 0$. Suppose $G \subset \text{PGL}_2(k)$ is a nontrivial $p$-group, and let $s \in G$ be any nontrivial element. We saw in Lemma 3.2 that $s$ must fix a unique point of $\mathbb{P}^1(k)$, so after conjugating $G$ if necessary, we may assume that $s$ fixes $\infty$. We claim that every element of $G$ fixes $\infty$. Suppose not, and select $s' \in G \setminus \{1, s\}$ that fixes a (unique) point $x \neq \infty$. After conjugating $G$ by $\left( \begin{smallmatrix} 1 \\ 1 \end{smallmatrix} \right)$, we may assume that $s'$ fixes 0 and $s$ still fixes $\infty$. So $s = \left( \begin{smallmatrix} 1 & \beta \\ 1 & 1 \end{smallmatrix} \right)$ and $s' = \left( \begin{smallmatrix} 1 & \beta' \\ 1 & 1 \end{smallmatrix} \right)$ for some $\beta, \beta' \in k^\times$. Since $G$ is a $p$-group, it follows that $ss'$ must fix a unique point as well. Lemma 3.2 shows that

$$\text{tr}(ss')^2 - 4 \det(ss') = \beta \beta' (4 + \beta \beta') = 0.$$

When $p = 2$, this contradicts $\beta \beta' \neq 0$. When $p > 2$, we find that $s^{-1}s' \in G$ as well, so that

$$\text{tr}(s^{-1}s') - 4 \det(s^{-1}s') = -\beta \beta' (4 - \beta \beta') = 0.$$

Adding these last two equations gives a contradiction. Hence every element of $G$ fixes $\infty$. We have proved the following lemma.

Lemma 4.3. If $G \subset \text{PGL}_2(k)$ is a nontrivial $p$-group, then $G$ is conjugate to $\langle \lambda \rangle$, where $\Gamma$ is an additive subgroup of $k$, and hence an $\mathbb{F}_p$-vector space. In particular, $G$ is abelian and fixes a unique point of $\mathbb{P}^1(k)$. 

Now suppose that $G$ and $G'$ are two finite $p$-groups in $\text{PGL}_2(k)$. To determine necessary and sufficient conditions for these two subgroups to be conjugate, it suffices to assume that $G = (\begin{smallmatrix} 1 & 1 \\ \tau & 1 \end{smallmatrix})$ and $G' = (\begin{smallmatrix} 1 & 1 \\ \tau' & 1 \end{smallmatrix})$ for some additive subgroups $\Gamma$ and $\Gamma'$ inside $k$. If there exists $u \in \text{PGL}_2(k)$ so that $uGu^{-1} = G'$, then $u$ must fix $\infty$, so that $u = (\begin{smallmatrix} \alpha & \beta \\ 1 & 1 \end{smallmatrix})$. Hence

$$uGu^{-1} = \left(\begin{array}{cc} \alpha & \beta \\ 1 & 1 \end{array}\right) \left(\begin{array}{cc} 1 & \Gamma \\ \tau & 1 \end{array}\right) \left(\begin{array}{cc} \alpha^{-1} & -\alpha^{-1}\beta \\ 1 & 1 \end{array}\right) = \left(\begin{array}{cc} 1 & \alpha\Gamma \\ \tau & 1 \end{array}\right),$$

which implies that $\Gamma' = \alpha\Gamma$. This calculation also shows that it is sufficient that $\alpha\Gamma = \Gamma'$ for some $\alpha \in k^\times$ in order to have $G$ and $G'$ be conjugate.

**Proposition 4.4.** The conjugacy classes of finite $p$-subgroups of $\text{PGL}_2(k)$ are in bijective correspondence with the finite additive subgroups of $k$ modulo homotheties.

To close this section, we define the stabilizer$^4$ of a finite additive subgroup $\Gamma \subset k$ to be

$$\mathbb{F}_\Gamma = \{ \alpha \in k : \alpha\Gamma \subset \Gamma\}.$$ 

Then one verifies immediately that $\mathbb{F}_\Gamma$ is a subfield of $k$. Moreover, each nonzero element of $\mathbb{F}_\Gamma$ induces an $\mathbb{F}_p$-linear automorphism of $\Gamma$, and since $\Gamma$ is finite, there are only finitely many possibilities in total for such an automorphism. Hence $\mathbb{F}_\Gamma$ is a finite subfield of $k$. Observe further that for any $\alpha \in k^\times$, we have $\mathbb{F}_\alpha\Gamma = \mathbb{F}_\Gamma$, so that the stabilizer is a homothety class invariant.

4.3. **Subgroups stabilizing a pair of points.** Let $G$ be a finite subgroup of $\text{PGL}_2(k)$ that stabilizes a pair of points, but does not fix them. After conjugation, we may assume that $G$ stabilizes $\{0, \infty\}$. Define

$$H = \{ s \in G : s.\infty = \infty \text{ and } s.0 = 0 \}.$$ 

We saw in §4.1 that $H$ is cyclic and generated by an element $\left(\begin{smallmatrix} \lambda & 1 \\ 1 & 1 \end{smallmatrix}\right)$. We observe that $H$ is normal in $G$. Indeed, it is invariant under conjugation by any element fixing both $0$ and $\infty$ as these are precisely the elements of $H$. Any element of $G$ that stabilizes the set $\{0, \infty\}$ without fixing it pointwise must be of the form $t = (\begin{smallmatrix} \tau \\ 1 \end{smallmatrix})$ for some $\tau \in k^\times$. We find that

$$t \left(\begin{array}{cc} \lambda \\ 1 \end{array}\right) t^{-1} = \left(\begin{array}{cc} \lambda \\ 1 \end{array}\right) \left(\begin{array}{cc} \tau \\ 1 \end{array}\right) = \left(\begin{array}{cc} \lambda^{-1} \\ 1 \end{array}\right).$$

Hence $H$ is normal. In fact, this computation also shows that the subgroup of $G$ generated by $H$ and $t$ is dihedral.

We now prove that $G$ is generated by $H$ and $t$. We may conjugate $G$ by $\left(\begin{smallmatrix} \sqrt{\tau} & 1 \\ 1 & 1 \end{smallmatrix}\right)$ in order to assume that $t = (\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix})$; note that this operation does not affect $H$. We have already shown that $G \setminus H$ consists of elements of the form $(\lambda \begin{smallmatrix} 1 \\ 1 \end{smallmatrix})$. Suppose we have such an element. Then $\left(\begin{smallmatrix} 1 & \tau \\ 1 & 1 \end{smallmatrix}\right) = (\begin{smallmatrix} \tau' \\ 1 \end{smallmatrix}) \in H$. If $\lambda$ has order $n = |H|$, then $\tau^n = 1$, which means there are at most $n$ such elements in $G$. On the other hand, we can generate $n$ elements of this shape via

$$\left(\begin{array}{cc} \lambda^j \\ 1 \end{array}\right) \left(\begin{array}{cc} 1 \\ 1 \end{array}\right) = \left(\begin{array}{cc} \lambda^j \\ 1 \end{array}\right), \quad j = 1, \ldots, n.$$ 

Hence $G$ is generated by $H$ and $t$ as desired.

**Proposition 4.5.** Let $G \subset \text{PGL}_2(k)$ be a finite subgroup that stabilizes a pair of points of $\mathbb{P}^1(k)$. Then up to $\text{PGL}_2(k)$-conjugacy, $G$ satisfies one of the following:

1. $G = (\begin{smallmatrix} \lambda & 1 \\ 1 & 1 \end{smallmatrix})$ for some cyclic subgroup $\Lambda \subset k^\times$; in this case, $G$ fixes a pair of points of $\mathbb{P}^1(k)$.

2. $G = (\begin{smallmatrix} \lambda & 1 \\ 1 & 1 \end{smallmatrix}) \times ((\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}))$ for some cyclic subgroup $\Lambda \subset k^\times$; in this case, $G$ stabilizes a pair of points, but does not fix them.

$^4$The multiplicative group $k^\times$ acts on the set of all finite additive subgroups of $k$, and the stabilizer (in the usual sense of a group action) of a particular such subgroup $\Gamma$ is precisely $\mathbb{F}_\Gamma^\times$. Dickson prefers to call $\mathbb{F}_\Gamma$ the multiplier [3, §70].
In either case, we observe that $G$ is uniquely determined up to $\text{PGL}_2(k)$-conjugacy by its order and whether it fixes a pair of points.

Now let us suppose that $G$ is a finite subgroup of $\text{PGL}_2(k)$, and let $H$ be a nontrivial maximal $p$-regular cyclic subgroup. We showed in Proposition 4.1 that $H$ fixes a pair of points $\{x, y\} \subset \mathbb{P}^1(k)$. If $s \in G$ lies in the normalizer of $H$, then for each nontrivial $h \in H$, there is $h' \in H$ such that $shs^{-1} = h'$. Observe that

$$h's.x = sh.x = s.x \quad h's.y = sh.y = s.y,$$

so that $s.x$ and $s.y$ are fixed points of $h'$. This means $s$ stabilizes the pair $\{x, y\}$. If $s$ fixes both of these points, then $s \in H$ by maximality; otherwise, $s$ swaps $x$ and $y$. It follows that the normalizer $N_G(H)$ consists of the elements of $G$ that stabilize the pair of points $\{x, y\}$, so that our above work proves $N_G(H) = H$ or $N_G(H)$ is dihedral with maximal cyclic subgroup $H$ (of index 2).

**Proposition 4.6.** Let $G$ be a finite subgroup of $\text{PGL}_2(k)$, and let $H$ be a nontrivial maximal $p$-regular cyclic subgroup. Then the normalizer of $H$ satisfies $[N_G(H) : H] = 1$ or 2. In the latter case, $N_G(H)$ is dihedral.

### 4.4. Subgroups fixing a unique point

The goal of this section is to prove the following result:

**Proposition 4.7.** Suppose $G$ is a finite subgroup of $\text{PGL}_2(k)$ that fixes a unique point of $\mathbb{P}^1(k)$. Then $k$ has positive characteristic $p$, and up to conjugation in $\text{PGL}_2(k)$, there exist a nontrivial additive subgroup $\Gamma \subset k$ and a positive integer $n$ coprime to $p$ satisfying $\mu_n(k) \subset \mathbb{F}_p^\times$ and

$$G = \left( \begin{array}{cc} \mu_n(k) & \Gamma \\ 1 & 1 \end{array} \right) = \left( \begin{array}{cc} 1 & \Gamma \\ 1 & 1 \end{array} \right) \rtimes \left( \begin{array}{cc} \mu_n(k) \\ 1 \end{array} \right).$$

The group $G$ is determined up to $\text{PGL}_2(k)$-conjugation by $n$ and the homothety class $\{\alpha \Gamma : \alpha \in k^\times\}$.

**Remark 4.8.** With the notation of the proposition, let $e$ be the order of $p$ in $(\mathbb{Z}/n\mathbb{Z})^\times$. Then $\mathbb{F}_{p^e}$ is the smallest extension of $\mathbb{F}_p$ containing $\mu_n(k)$, and hence $\mathbb{F}_{p^e} \subset \mathbb{F}_\Gamma$.

**Corollary 4.9.** If $G$ is a finite subgroup of $\text{PGL}_2(k)$, then $G$ fixes a unique point of $\mathbb{P}^1(k)$ if and only if $G$ is $p$-semi-elementary with nontrivial Sylow $p$-subgroup, where $p = \text{char}(k) > 0$.

**Proof.** One implication follows immediately from the preceding proposition. For the other, $G$ is $p$-semi-elementary if and only if it fits into an exact sequence $1 \to P \to G \to G/P \to 1$ with $P$ a $p$-group and $G/P$ cyclic of order prime to $p$. We saw in §4.2 that $P$ must fix a unique point of $\mathbb{P}^1(k)$, and so must any group that normalizes it. \hfill $\square$

Before proving the proposition, we discuss Borel and unipotent subgroups. Write $B(k)$ for the **standard Borel subgroup** of $\text{PGL}_2(k)$:

$$B(k) = \{ s \in \text{PGL}_2(k) : s.\infty = \infty \} = \left\{ \left[ \begin{array}{cc} \alpha & \beta \\ 0 & 1 \end{array} \right] : \alpha, \beta \in k^\times \right\}.$$

Write $U(k)$ for the unipotent subgroup of $B(k)$ — i.e., those elements with $\alpha = 1$. Note that $U(k)$ is an abelian group, and it can be written concretely as $U(k) = \{ (1, 0) \}$. Moreover, an immediate calculation shows that $U(k)$ is a normal subgroup of $B(k)$.

More generally, any subgroup conjugate to $B(k)$ will be called a Borel subgroup. Equivalently, a Borel subgroup may be characterized as the set of all elements of $\text{PGL}_2(k)$ fixing a particular point of $\mathbb{P}^1(k)$.

There is an exact sequence of homomorphisms

$$1 \to U(k) \to B(k) \xrightarrow{\pi} k^\times \to 1,$$

where $\pi$ maps an element $s = \left[ \begin{array}{cc} \alpha & \beta \\ 0 & 1 \end{array} \right]$ to the derivative of $s.z = \alpha z + \beta$. (Note that this is well defined independent of the matrix representation of $s$.) For any subgroup $G \subset \text{PGL}_2(k)$, we write $B_G = B(k) \cap G$.
and \( U_G = U(k) \cap G = (\begin{smallmatrix} 1 & \Gamma \\ 1 & 1 \end{smallmatrix}) \) for some additive subgroup \( \Gamma \subset k \). Then the above exact sequence descends to an exact sequence
\[
1 \rightarrow U_G \rightarrow B_G \xrightarrow{\pi} \pi(B_G) \rightarrow 1.
\]
If \( \pi(B_G) \) is cyclic, generated by \( \lambda \in k^\times \), then there exists \( s = \begin{pmatrix} \lambda & \eta \\ 1 & 1 \end{pmatrix} \in B_G \) for some \( \eta \in k \). The subgroup generated by \( s \) is isomorphic to \( \pi(B_G) \), so we may represent \( B_G \) as a semidirect product:
\[
B_G = \begin{pmatrix} 1 & \Gamma \\ 1 & 1 \end{pmatrix} \rtimes \langle s \rangle.
\]
This is the case, for example, if \( G \) is a finite group, so that \( \pi(B_G) \subset \mu_n(k) \) for some \( n \geq 1 \). Note that if \( s \) is nontrivial, then \( \lambda \neq 1 \).

**Proof of Proposition 4.7.** Suppose now that \( G \) is a finite subgroup of \( \text{PGL}_2(k) \) that fixes a unique point of \( \mathbb{P}^1(k) \). As usual, we may assume that \( G \) fixes \( \infty \) after a suitable conjugation, so that \( G \subset B(k) \). Moreover, let us write \( U_G = \left( \begin{smallmatrix} 1 & \Gamma \\ 1 & 1 \end{smallmatrix} \right) \) and choose an element \( s \) as above so that \( G = \left( \begin{smallmatrix} 1 & \Gamma \\ 1 & 1 \end{smallmatrix} \right) \rtimes \langle s \rangle \). Now \( s \) fixes \( \infty \) and at least one other point of \( \mathbb{P}^1(k) \). Note that \( \Gamma \neq 0 \), else \( G \) fixes at least two points. In particular, the characteristic of \( k \) is positive. After conjugating \( G \) by an element of \( U(k) \), we may assume that \( s \) fixes 0, so that it is of the form \( s = \begin{pmatrix} \lambda & 1 \\ 1 & 1 \end{pmatrix} \). That is, \( \langle \lambda \rangle = \mu_n(k) \) for some \( n \) coprime to \( p \), and \( G = \left( \begin{smallmatrix} 1 & \Gamma \\ 1 & 1 \end{smallmatrix} \right) \rtimes \langle \mu_n(k) \rangle = \langle \mu_n(k) \Gamma \rangle \).

Now observe that, with \( \lambda \) as above and \( \gamma \in \Gamma \), we have
\[
\left( \begin{array}{cc} \lambda & 1 \\ 1 & 1 \end{array} \right) \left( \begin{array}{cc} 1 & \gamma \\ 1 & 1 \end{array} \right) \left( \begin{array}{cc} \lambda^{-1} & 1 \\ 1 & 1 \end{array} \right) = \left( \begin{array}{cc} 1 & \lambda \gamma \\ 1 & 1 \end{array} \right) \in G,
\]
so that \( \lambda \Gamma \subset \Gamma \). That is, \( \mu_n(k) \subset \mathbb{F}_\Gamma^\times \).

Finally we must deal with the question of conjugacy of these subgroups. Let \( G, G' \subset \text{PGL}_2(k) \) be finite subgroups of the following form:
\[
G = \left( \begin{smallmatrix} 1 & \Gamma \\ 1 & 1 \end{smallmatrix} \right) \rtimes \langle \mu_n(k) \rangle, \quad G' = \left( \begin{smallmatrix} 1 & \Gamma' \\ 1 & 1 \end{smallmatrix} \right) \rtimes \langle \mu_n'(k) \rangle,
\]
where \( n, n' \in \mathbb{N} \setminus p\mathbb{N} \) and \( \Gamma, \Gamma' \subset k \) are finite nontrivial additive subgroups. Suppose first that there is \( s \in \text{PGL}_2(k) \) such that \( sGs^{-1} = G' \). Then \( s \) must fix \( \infty \), so that \( s = \left( \begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix} \right) \). Since \( sU_Gs^{-1} = U_{G'} \), our work in §4.2 shows that \( \Gamma' = \alpha \Gamma \). Comparing the orders of \( G \) and \( G' \) shows \( n = n' \).

Conversely, suppose that \( G \) and \( G' \) are as above, that \( \Gamma' = \alpha \Gamma \), and \( n = n' \). For \( \gamma \in \Gamma \) and \( \lambda \in \mu_n(k) \), we have
\[
\left( \begin{array}{cc} \alpha & 1 \\ 1 & 1 \end{array} \right) \left( \begin{array}{cc} \lambda & \gamma \\ 1 & 1 \end{array} \right) \left( \begin{array}{cc} \alpha^{-1} & 1 \\ 1 & 1 \end{array} \right) = \left( \begin{array}{cc} \lambda & \alpha \gamma \\ 1 & 1 \end{array} \right) \in G'.
\]
As \( G \) and \( G' \) have the same order, it follows that \( G \) and \( G' \) are conjugate. \( \square \)

When we deal with non-algebraically closed fields later, it will be useful to have a description of 2-elementary subgroups that fix a point other than infinity.

**Proposition 4.10.** Suppose that \( k \) has characteristic 2. Let \( \tau \in \mathbb{P}^1(k) \setminus \infty \). The subgroup of \( \text{PGL}_2(k) \) given by
\[
\Omega(\tau) := \{ I \} \cup \left\{ \left( \begin{array}{cc} \alpha & \beta \\ 1 & \alpha \end{array} \right)^2 : \alpha \in k \setminus \{ \tau \} \right\}
\]
fixes \( \tau \), and any element of \( \text{PGL}_2(k) \) with unique fixed point \( \tau \) lies in \( \Omega(\tau) \).

**Proof.** It is immediate that \( \Omega(\tau) \) fixes \( \tau \). If \( s = \left( \begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix} \right) \) is a nontrivial element of \( \text{PGL}_2(k) \) with unique fixed point \( \tau \), then \( s \) has order 2 and trace zero (Lemma 3.2). It follows that \( \delta = \alpha \). As \( s \) does not fix \( \infty \), we must have \( \gamma \neq 0 \). Without loss, set \( \gamma = 1 \). The fixed point of \( s = \left( \begin{smallmatrix} \alpha & \beta \\ 1 & \alpha \end{smallmatrix} \right) \) is \( \sqrt{\beta} = \tau \). Hence, \( \beta = \tau^2 \), as desired. \( \square \)
4.5. Tetrahedral subgroups. Recall that the group of orientation-preserving symmetries of a regular tetrahedron is isomorphic to $\mathfrak{A}_4$. (Look at the action of the symmetry group on the four vertices of the tetrahedron.) Any group isomorphic to $\mathfrak{A}_4$ will therefore be called tetrahedral.

Lemma 4.11. Let $G$ be a non-abelian group of order 12 possessing a normal Klein 4-subgroup. Then $G$ is tetrahedral.

Proof. Let $N = \{e, n_1, n_2, n_3\}$ be the given normal subgroup, let $h \in G$ be an element of order 3, and let $H = \langle h \rangle$. Then $N \cap H = \{e\}$ and $NH = G$. We observe that $hn_1h^{-1} = n_j$ for some $j$. If conjugation by $h$ fixes all $n_i$, then we would find that $G$ is abelian. If conjugation by $h$ fixes any one $n_i$ and permuted the other 2, then $h$ would have order 2. So $h$ permutes the $n_i$ cyclically. Hence $G = N \rtimes H$, and the action $H \to \text{Aut}(N)$ is given by cyclic permutation on the three nontrivial elements of $N$. One now checks that $\mathfrak{A}_4$ may also be written as a semidirect product of the normal subgroup $\{e, (12)(34), (13)(24), (14)(23)\}$ (containing all elements of order 2) and the subgroup generated by $(123)$; hence, it is isomorphic to $G$. \hfill $\square$

Proposition 4.12. If $p = 2$ and $G$ is a tetrahedral subgroup of $\text{PGL}_2(k)$, then $G$ is conjugate to the standard Borel subgroup $B(F_4) = \left(\begin{smallmatrix} F_4^+ \\ 1 \end{smallmatrix}\right) \rtimes \left(\begin{smallmatrix} F_4^\times \\ 1 \end{smallmatrix}\right)$.

Proof. We know $G$ contains a normal 4-group $N$, each nontrivial element of which must be unipotent since $p = 2$. After conjugating $G$ if needed, we may assume that $N = \left(\begin{smallmatrix} 1 \Gamma \\ 1 \end{smallmatrix}\right)$ for some $\Gamma \subseteq k$ of rank 2 (Lemma 4.3). By normality, if $s \in G$ and $u \in N$, then there is $u' \in N$ such that $su = u's$. Since $s \infty$ is the unique fixed point of each nontrivial element of $N$, we have

\[ s \cdot \infty = s(u, \infty) = u'(s, \infty) \Rightarrow s \cdot \infty = \infty. \]

That is, $G$ fixes $\infty$, or equivalently $G \subset B(k)$.

By Proposition 4.7, we may assume $G = \left(\begin{smallmatrix} 1 \Gamma \\ 1 \end{smallmatrix}\right) \rtimes \left(\begin{smallmatrix} \mu_3(k) \\ 1 \end{smallmatrix}\right)$, where $\Gamma$ is an additive subgroup of $k$ of order 4 that is stable under multiplication by $\mu_3(k) = F_4^\times$. For $\gamma \in \Gamma \setminus \{0\}$, observe that

\[ \left(\begin{smallmatrix} \gamma^{-1} \\ 1 \end{smallmatrix}\right) \left(\begin{smallmatrix} 1 \Gamma \\ 1 \end{smallmatrix}\right) \left(\begin{smallmatrix} \gamma \\ 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 \gamma^{-1}\Gamma \\ 1 \end{smallmatrix}\right). \]

So after an appropriate conjugation, we may assume that $1 \in \Gamma$. Since $\Gamma$ is stable under multiplication by elements of $F_4^\times$, we conclude that $\Gamma = F_4$. \hfill $\square$

Proposition 4.13. Suppose $p \neq 2$ and let $G$ be a tetrahedral subgroup of $\text{PGL}_2(k)$. Then $G$ is conjugate to the semidirect product $N \rtimes \Gamma$, where $N = \langle \left(\begin{smallmatrix} \pm 1 \\ 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 \pm 1 \\ 1 \end{smallmatrix}\right) \rangle$, and $\Gamma$ is the cyclic group of order 3 generated by $\left(\begin{smallmatrix} 1 & i \\ 1 & -i \end{smallmatrix}\right)$, where $i$ is any choice of primitive fourth root of unity. In particular, any two tetrahedral subgroups of $\text{PGL}_2(k)$ are conjugate when $\text{char}(k)$ is different from 2.

Proof. A tetrahedral group contains a normal 4-group $N$. Let $s_1$ be a nontrivial element of $N$, and let us conjugate $G$ so that $s_1$ fixes 0 and $\infty$. (Here we have used the hypothesis $p \neq 2$.) If $s_2 \in N$ is another element of order 2, then it must commute with $s_1$, so that

\[ s_1s_2,0 = s_2s_1,0 = s_2,0 \quad s_1s_2,\infty = s_2s_1,\infty = s_2,\infty. \]

Hence $s_2$ stabilizes the set $\{0, \infty\}$, and it cannot fix these elements since $s_1$ is the only element of order 2 with this property. Repeating this argument for the third nontrivial element of $N$ shows that there exist $\tau \neq \tau' \in k^\times$ such that

\[ N = \left\{I, \left(\begin{smallmatrix} -1 \\ 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} \tau \\ 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} \tau' \\ 1 \end{smallmatrix}\right)\right\}. \]

After conjugating by $\left(\begin{smallmatrix} \sqrt{-1} \\ 1 \end{smallmatrix}\right)$, we may assume that $\tau = 1$. Since $N$ is abelian, we have

\[ \left(\begin{smallmatrix} 1 \\ \tau' \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 \\ \tau' \end{smallmatrix}\right) \left(\begin{smallmatrix} 1 \\ \tau' \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 \\ \tau' \end{smallmatrix}\right) \left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} \tau' \\ 1 \end{smallmatrix}\right). \]
Hence $(\tau')^2 = 1$, or $\tau' = -1$, and $N$ is of the form claimed in the statement of the proposition.

The group $G$ has normal subgroup $N$ and four conjugate subgroups of order 3. In particular, every element of $G \setminus N$ has order 3. We now compute the set of all elements of $\text{PGL}_2(k)$ of order 3 that normalize $N$. Suppose $s = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ is such an element. Then

$$
\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix} = \begin{pmatrix} -\alpha \delta + \beta \gamma & 2 \alpha \beta \\ -2 \gamma \delta & \alpha \delta + \beta \gamma \end{pmatrix}.
$$

For $s$ to be a normalizing element, we must have either

$$
\alpha \beta = \gamma \delta = 0, \quad \text{or} \quad \alpha \delta = -\beta \gamma \quad \text{and} \quad \alpha \beta \gamma \delta \neq 0. \tag{4.1}
$$

Let us suppose first that (4.1) holds. Then either $\alpha = \delta = 0$ or $\beta = \gamma = 0$. In the former case, $s$ has order 3 if and only if $\text{tr}(s)^2 - \det(s) = -\det(s) = 0$, so that this cannot occur (Lemma 3.3). In the latter case, we may assume $\delta = 1$, so that $s$ has order 3 precisely when $\alpha^3 = 1$ and $\alpha \neq 1$. But observe that

$$
\begin{pmatrix} \alpha & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} \alpha^{-1} & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \alpha^2 & 0 \\ 0 & 1 \end{pmatrix} \not\in N,
$$

so that the full subgroup $N$ is not stable under conjugation by $s$. Hence (4.1) may discarded.

Let us now suppose that (4.2) holds, so that $\beta \gamma = -\alpha \delta$. By Lemma 3.3, if $s$ has order 3, then

$$
0 = \text{tr}(s)^2 - \det(s) = (\alpha + \delta)^2 - \alpha \delta + \beta \gamma = \alpha^2 + \beta^2.
$$

Hence $\delta = \pm i \alpha$. Squaring both sides of the second equation in (4.2) and dividing by $\alpha^2 = -\beta^2$, we see that $\beta^2 = -\gamma^2$. Without loss of generality, we may suppose that $\gamma = 1$, so that $\beta = \pm i$. Squaring both sides of the first equation in (4.2) and replacing $\beta^2$ with $-\alpha^2$ and $\gamma^2$ with $-\beta^2 = 1$, we find that $\alpha^4 = 1$. We conclude that $s = \begin{pmatrix} \varepsilon & 0 \\ 0 & \varepsilon \end{pmatrix}$, where $\varepsilon_j = 1$ for $j = 1, 2, 3$ and $\beta = \pm i$. In order for the first equation of (4.2) to be satisfied, we must have $\beta = -\varepsilon_1 \varepsilon_2$, so that exactly one of $\varepsilon_1$ and $\varepsilon_2$ is a primitive fourth root of unity, while the other is $\pm 1$. Hence the elements of order 3 that normalize $N$ lie in the following set:

$$
\left\{ \begin{pmatrix} \varepsilon & -\varepsilon \varepsilon' \\ 0 & \varepsilon \varepsilon' \end{pmatrix} : \varepsilon^2 = (\varepsilon')^2 = 1 \right\} \cup \left\{ \begin{pmatrix} \varepsilon i & -\varepsilon \varepsilon' i \\ 0 & \varepsilon' \varepsilon \end{pmatrix} : \varepsilon^2 = (\varepsilon')^2 = 1 \right\}.
$$

As there are 8 elements in this set, and since a tetrahedral group has 8 elements of order 3, we have found all of them.

Let $s \in G$ be any element of order 3. Evidently $N \union Ns \union Ns^2 = G$, so that $G = N \rtimes \langle s \rangle$. Now choose $\varepsilon = 1$ and $\varepsilon' = -1$ in the first of the above sets of elements of order 3 to arrive at the desired generator $G$. \hfill $\square$

**Corollary 4.14.** If $p = 3$ and $G \subset \text{PGL}_2(k)$ is tetrahedral, then $G$ is conjugate to $\text{PSL}_2(\mathbb{F}_3)$.

**Proof.** The group $\text{PSL}_2(\mathbb{F}_3)$ acts faithfully on the set $\mathbb{P}^1(\mathbb{F}_3)$, which has four points. This gives an injective homomorphism $\text{PSL}_2(\mathbb{F}_3) \rightarrow \mathfrak{S}_4$. By comparing orders, we see that the image in $\mathfrak{S}_4$ has index 2, which means $\text{PSL}_2(\mathbb{F}_3) \cong \mathfrak{A}_4$. Thus $\text{PSL}_2(\mathbb{F}_3)$ is tetrahedral, and the preceding proposition shows $G$ and $\text{PSL}_2(\mathbb{F}_3)$ must be conjugate. \hfill $\square$

### 4.6 Octahedral subgroups.

Recall that the group of orientation-preserving symmetries of a regular octahedron is isomorphic to $\mathfrak{S}_4$. (Look at the action of the symmetry group on the set of pairs of opposite faces, of which there are four.) Any group isomorphic to $\mathfrak{S}_4$ will therefore be called octahedral.

**Lemma 4.15.** Let $G$ be a group of order 24 such that (a) $G$ has no central element of order 2, and (b) $G$ has exactly 4 conjugate cyclic subgroups of order 3, each of which has normalizer equal to a dihedral subgroup of order 6. Then $G$ is octahedral.
Proof. Let \( C_1, \ldots, C_4 \) be the four conjugate cyclic subgroups of order 3, and let \( D_1, \ldots, D_4 \) be the associated dihedral normalizers. Note that the \( D_i \) must also be conjugate. We claim that \( D_1 \cap \cdots \cap D_4 = \{ e \} \). If it contains an element \( g \) of order 3, then \( g \) belongs to each of the \( C_i \), and hence the \( C_i \) are not distinct, a contradiction. If the intersection contains a pair of distinct elements of order 2, then it contains their product, which has order 3, another contradiction. If the intersection contains a unique element of order 2, say \( g \), then \( sgs^{-1} \) lies in the intersection as well for every \( s \in G \). Hence \( sgs^{-1} = g \), or \( g \) lies in the center of \( G \), a final contradiction. Thus \( D_1 \cap \cdots \cap D_4 \) is trivial.

Consider the action of \( G \) on the set \( \{ C_1, \ldots, C_4 \} \) given by conjugation; it induces a homomorphism \( \phi : G \to S_4 \). Suppose that \( g \) lies in the kernel of \( \phi \). Then \( gC_ig^{-1} = C_i \) for each \( i \), so that \( g \) belongs to each normalizer \( D_i \). We showed above that the intersection of the normalizers is trivial, so \( g = e \). We deduce that \( \phi \) is injective, and that \( G \cong S_4 \). \( \square \)

Proposition 4.16. Suppose \( p \neq 2 \) and \( G \subset \operatorname{PGL}_2(k) \) is an octahedral subgroup. Then up to conjugation, \( G \) is generated by the tetrahedral subgroup \( T = N \times C \) given by Proposition 4.13 and the element \( (i, 1) \), where \( i \) is any primitive fourth root of unity. In particular, any two octahedral subgroups of \( \operatorname{PGL}_2(k) \) are conjugate when \( \text{char}(k) \) is different from 2.

Remark 4.17. When \( p = 2 \), we know that every element of finite order in \( \operatorname{PGL}_2(k) \) has order 2 or odd order (Proposition 4.1). It follows that \( \operatorname{PGL}_2(k) \) does not contain an octahedral subgroup since such groups have elements of order 4.

Proof. Evidently \( G \) contains a tetrahedral subgroup \( T \), so after conjugation, we may assume \( T = N \times C \) as in Proposition 4.13. Since \( [G : T] = 2 \), we know \( G \) is generated by \( T \) and any element \( s \in G \) of order 4. Then \( s^2 \) has order 2 and corresponds to an even permutation in \( S_4 \), so that it lies in \( N \). The three nontrivial elements of \( N \) are conjugate via elements of \( C \), so we may assume that \( s^2 = (1^{−1}) \). Now \( s \) fixes two points of \( \mathbb{P}^1(k) \), and its square fixes the same two points. Hence \( s = (i \ 1) \) for some \( \varepsilon \in k^× \). Since \( s \) has order 4, we must have \( \varepsilon = ±i \). Replacing \( s \) with \( s^{-1} \) if necessary, we find that \( \varepsilon = i \). \( \square \)

Corollary 4.18. If \( p = 3 \) and \( G \subset \operatorname{PGL}_2(k) \) is octahedral, then \( G \) is conjugate to \( \operatorname{PGL}_2(F_3) \).

Proof. The group \( \operatorname{PGL}_2(F_3) \) acts faithfully on the set \( \mathbb{P}^1(F_3) \), which has four points. This gives an injective homomorphism \( \operatorname{PGL}_2(F_3) \to S_4 \). As these groups have the same order, they must be isomorphic. Thus \( \operatorname{PGL}_2(F_3) \) is octahedral, and the preceding proposition shows \( G \) and \( \operatorname{PGL}_2(F_3) \) must be conjugate. \( \square \)

4.7. Icosahedral subgroups. Recall that the group of orientation-preserving symmetries of a regular icosahedron is isomorphic to \( \mathfrak{A}_5 \). (See [2, §3.6–3.7].) Any group isomorphic to \( \mathfrak{A}_5 \) will therefore be called icosahedral.

Lemma 4.19. Let \( G \) be a group of order 60 with exactly ten conjugate 3-subgroups and exactly fifteen elements of order 2 lying in five conjugate Klein 4-groups. Then \( G \) is icosahedral.

Proof. Let \( K_1, \ldots, K_5 \) be the conjugate Klein 4-subgroups. We let \( G \) act on the set \( \{ K_1, \ldots, K_5 \} \) by conjugation, so that we have a homomorphism \( \phi : G \to \mathfrak{A}_5 \). If we can show that \( G \) is injective, then it is isomorphic to an index 2 subgroup of \( \mathfrak{A}_5 \), which must be \( \mathfrak{A}_5 \).

First note that if \( N_i \) is the normalizer of \( K_i \) in \( G \), then \( |N_i| = 12 \) by the orbit-stabilizer theorem. Each \( N_i \) is tetrahedral by Lemma 4.11. Indeed, it suffices to show that \( N_i \) is non-abelian. But if it were abelian, then it would contain a normal subgroup \( C_i \) of order 3, which would be one of at most five conjugate Sylow 3-subgroups of \( G \). But \( G \) has ten conjugate 3-subgroups, a contradiction.

To show that \( \phi \) is injective, we must prove that \( N_1 \cap \cdots \cap N_5 = \{ e \} \). Write \( N \) for this intersection. Then \( N \) is a normal subgroup of \( G \), and hence of each \( N_i \). Now \( N_i \) is tetrahedral, so its only normal subgroups are its trivial subgroups and \( K_i \). No two of the \( N_i \) are equal since they contain conjugate subgroups \( K_i \); hence
$N \neq N_i$ for any $i$. The $K_i$ have only the identity in common as they contain all fifteen of the elements of $G$ of order 2. We conclude that $N \neq K_i$ for any $i$. So $N = \{e\}$. \hfill \Box

**Lemma 4.20.** An icosahedral group $G$ can be generated by two elements $g, h$ subject to the relations $g^5 = h^2 = (gh)^3 = 1$.

**Proof.** We may assume $G = \mathfrak{A}_5$. Let $g = (12345)$ and $h = (12)(34)$. Then $gh = (135)$ has order 3. Let $H = \langle g, h \rangle \subset G$. Evidently $g$ and $h$ have the correct relations, so it suffices to prove that $|H| = |G|$. By Cauchy, $H$ contains subgroups of order 3 and 5. We now show that $H$ has a subgroup of order 4, so that $|H|$ is divisible by $4 \cdot 3 \cdot 5 = 60$. We have the following relations:

$$g^{-1}hg = (15)(23) \quad \text{(15)(23)}$$
$$ghg^{-1}h = (13)(25) \quad \text{(13)(25)}$$

These two products of 2-cycles generate a Klein 4-subgroup of $H$, which completes the proof. \hfill \Box

**Proposition 4.21.** Suppose $p \neq 5$ and $G \subset \text{PGL}_2(k)$ is icosahedral. For any primitive fifth root of unity $\zeta$, the group $G$ is conjugate to the group $\langle s, t \rangle$, where $s = (\zeta 1)$ and $t = \left(1, 1-\zeta^{-1}\zeta^{-3}\right)$. These generators satisfy $s^5 = t^2 = (st)^3 = 1$. In particular, any two icosahedral subgroups of $\text{PGL}_2(k)$ are conjugate when $\text{char}(k) \neq 5$.

**Proof.** We begin by showing that $G$ is conjugate to a subgroup of the sort given in the proposition for some primitive fifth root of unity $\zeta$; afterward, we will show that we may specify $\zeta$. Let $s, t \in G$ be generators as in Lemma 4.20; i.e., $s$ has order 5, $t$ has order 2, and $(st)^3 = 1$. Since $p \neq 5$, $s$ must fix two elements of $\mathbb{P}^1(k)$. After conjugation, we may assume that $s = (\zeta 1)$ with $\zeta$ some primitive fifth root of unity.

Since $t$ has order 2, it may be written as $t = \left(\frac{\alpha}{\gamma}, \frac{\beta}{-\alpha}\right)$ (Lemma 3.3). Now

$$st = \left(\begin{array}{c}
\zeta \\
1
\end{array}\right) \left(\begin{array}{c}
\alpha \\
\gamma
\end{array}\right) = \left(\begin{array}{c}
\zeta\alpha \\
\gamma
\end{array}\right).$$

The condition for $st$ to have order 3 is

$$0 = \text{tr}(st)^2 - \text{det}(st) = \zeta^2\alpha^2 + \zeta(\gamma\beta - \alpha^2) + \alpha^2.$$

If $\alpha = 0$, then this implies $\text{det}(t) = 0$. So we may assume that $\alpha = 1$. Now the previous equation becomes

$$\beta\gamma = -\frac{1}{\zeta}(\zeta^2 - \zeta + 1) = -\frac{\zeta^3 + 1}{\zeta(\zeta + 1)}. \quad (4.3)$$

As $\zeta$ is a primitive fifth root of unity, we find $\beta\gamma \neq 0$. If we conjugate $G$ by $(\gamma 1)$, then the subgroup generated by $(\zeta 1)$ is unaffected, while

$$\left(\begin{array}{c}
\gamma \\
1
\end{array}\right) \left(\begin{array}{c}
1 \\
\gamma -1
\end{array}\right) \left(\begin{array}{c}
\gamma^{-1} \\
1
\end{array}\right) = \left(\begin{array}{c}
1 \\
1 - \frac{\gamma}{\zeta - \zeta^{-1}}
\end{array}\right).$$

So without loss of generality, we may assume that $\gamma = 1$. From (4.3), we find that

$$t = \left(\begin{array}{c}
1 \\
1 - (\zeta^2 - \zeta + 1)/\zeta
\end{array}\right) = \left(\begin{array}{c}
1 \\
1 - \zeta - \zeta^{-1}
\end{array}\right).$$

By construction, $s^5 = t^2 = (st)^3 = 1$.

It remains to show that different fifth roots of unity give rise to conjugate subgroups of $\text{PGL}_2(k)$. For each $i = 1, 2, 3, 4$, let

$$s_i = \left(\begin{array}{c}
\zeta^i \\
1
\end{array}\right), \quad t_i = \left(\begin{array}{c}
1 \\
1 - \zeta - \zeta^{-i}
\end{array}\right), \quad G_i = \langle s_i, t_i \rangle.$$
Evidently the symmetry \( i \mapsto -i \) in \( t_1 \) shows \( G_1 = G_4 \) and \( G_2 = G_3 \); in general, there are no further equalities among the \( G_i \). If we let \( \lambda = \zeta^3 - \zeta^2 + \zeta \), then a direct calculation shows that
\[
\begin{pmatrix} \lambda & 1 \\ 1 & 1 \end{pmatrix} s_2 \begin{pmatrix} \lambda & 1 \\ 1 & 1 \end{pmatrix} s_1^2 \in G_1 \quad \text{and} \quad \begin{pmatrix} \lambda & 1 \\ 1 & 1 \end{pmatrix} t_2 \begin{pmatrix} \lambda & 1 \\ 1 & 1 \end{pmatrix} = t_1 s_1 t_1 s_1 t_1 \in G_1.
\]
It follows that \( \begin{pmatrix} \lambda & 1 \\ 1 & 1 \end{pmatrix} G_2 \begin{pmatrix} \lambda & 1 \\ 1 & 1 \end{pmatrix} \subset G_1 \), and since \( G_1 \) and \( G_2 \) have the same order, we have proved they are conjugate.

**Proposition 4.22.** Suppose \( p = 5 \) and \( G \subset \text{PGL}_2(k) \) is icosahedral. Then \( G \) is conjugate to \( \text{PSL}_2(\mathbb{F}_5) \). Moreover, we can take \( s = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \) and \( t = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \) as generators such that \( s^5 = t^2 = (st)^3 = 1 \).

**Proof.** The strategy is essentially the same as in the previous proposition. First we choose elements \( s, t \) with \( s^5 = t^2 = (st)^3 = 1 \) (Lemma 4.20). Since \( p = 5 \), \( s \) is unipotent, so we may conjugate to get \( s = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \). Write \( t = \begin{pmatrix} \alpha & \beta \\ \gamma & -\alpha \end{pmatrix} \). Then
\[
st = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & -\alpha \end{pmatrix} = \begin{pmatrix} \alpha + \gamma & \beta - \alpha \\ \gamma & -\alpha \end{pmatrix}.
\]
The condition for \( st \) to have order 3 is
\[
\text{tr}(st)^2 - \text{det}(st) = \alpha^2 + \beta \gamma + \gamma^2 = 0.
\]
If \( \gamma = 0 \), then this implies \( \alpha = 0 \), so that \( \text{det}(t) = 0 \). Hence \( \gamma \neq 0 \), and we may as well assume that \( \gamma = 1 \). The previous equation then implies \( \beta = -\alpha^2 - 1 \). That is, \( t = \begin{pmatrix} \alpha & \alpha^2 - 1 \\ 1 & -\alpha \end{pmatrix} \). Finally, we conjugate \( G \) by \( \begin{pmatrix} 1 & -\alpha \\ 1 & 1 \end{pmatrix} \). This does not affect the subgroup generated by \( s \), but it does give
\[
\begin{pmatrix} 1 & -\alpha \\ 1 & 1 \end{pmatrix} \begin{pmatrix} \alpha & -\alpha^2 - 1 \\ 1 & -\alpha \end{pmatrix} \begin{pmatrix} 1 & \alpha \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}.
\]
Hence we may assume without loss of generality that \( t = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \).

We have shown that, up to \( \text{PGL}_2(k) \)-conjugacy, we have \( G = \langle \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \rangle \subset \text{PSL}_2(\mathbb{F}_5) \). But these two groups have the same order, so that \( G = \text{PSL}_2(\mathbb{F}_5) \).

5. **The \( p \)-regular case**

**Convention.** Throughout this section, we will assume \( k \) is an algebraically closed field.

Our goal for this section is to prove Theorem C when \( k \) is an algebraically closed field.

Let \( G \subset \text{PGL}_2(k) \) be a finite \( p \)-regular subgroup. Any nontrivial element \( s \in G \) fixes a unique pair of points \( \{x_s, y_s\} \), and so there is a maximal cyclic subgroup \( G(s) \subset G \) containing \( s \), namely the set of all elements of \( G \) fixing \( x_s \) and \( y_s \). Let \( N(s) \) be its normalizer in \( G \); then \( [N(s) : G(s)] = 1 \) or 2 by Proposition 4.6. By letting \( G \) act by conjugation on its maximal cyclic subgroups, we find that \( G(s) \) lies in a system of \( [G]/|N(s)| \) conjugate subgroups. Let \( G_1, \ldots, G_r \) be a complete set of representatives of the conjugacy classes of maximal cyclic subgroups of \( G \). Let \( d_i = |G_i| \geq 2 \) and \( f_i = |N_G(G_i) : G_i| \). As \( G \) is \( p \)-regular, each of its nontrivial elements lies in a unique maximal cyclic subgroup. This yields
\[
|G| = 1 + \sum_{i=1}^{r} (d_i - 1) \frac{|G|}{d_i f_i}.
\]
Dividing by \( |G| \) and rearranging, we have
\[
\frac{1}{|G|} = 1 - \sum_{i=1}^{r} \frac{1}{d_i f_i} \left( 1 - \frac{1}{d_i} \right), \quad \text{and} \quad d_i f_i \leq |G| \quad (i = 1, \ldots, r). \tag{5.1}
\]
The summands on the right side of (5.1) have size at least \( \frac{1}{2} \left(1 - \frac{1}{d_i} \right) = \frac{1}{d_i} \); as the left side is positive, we find that \( r \leq 3 \). In the remainder of the proof, we treat the various cases that can occur for \( r, f_i, d_i \).
Case $r = 1$. If $f = 2$, then (5.1) implies $|G| = 2d/(d + 1)$, which is not an integer. Hence $f = 1$, and (5.1) gives $|G| = d$. That is, $G$ is cyclic.

Case $r = 2$. In this case, (5.1) becomes
\[
1 - \frac{1}{|G|} = \frac{1}{f_1} \left(1 - \frac{1}{d_1}\right) + \frac{1}{f_2} \left(1 - \frac{1}{d_2}\right)
\]
If $f_1 = f_2 = 1$, then the left side is smaller than 1 while the right side is $\geq 1$. If $f_1 = f_2 = 2$, then (5.1) and (5.2) become
\[
\frac{2}{|G|} = \frac{1}{d_1} + \frac{1}{d_2}, \quad \frac{2}{|G|} \leq \frac{1}{d_1}
\]
Evidently this is impossible, so we may assume without loss of generality that $f_1 = 1$ and $f_2 = 2$.

Now we find that
\[
\frac{1}{|G|} = \frac{1}{d_1} + \frac{1}{d_2} - \frac{1}{2} \leq \frac{1}{d_1} - \frac{1}{4},
\]
so that $d_1 = 2$ or 3. If $d_1 = 2$, then $|G| = 2d_2$, so that $G$ is dihedral. If $d_1 = 3$, then $1/|G| = 1/(2d_2) - 1/6$, so that $d_2 = 2$. Thus $|G| = 12$. We claim $G$ is tetrahedral. The normalizer of a Sylow 3-subgroup is not all of $G$ since $f_1 = 2$; in particular, $G$ is non-abelian. The subgroups of order 2, of which there are $|G|/2f_2 = 3$, form a single conjugacy class, so that they generate a normal subgroup of order 4. Hence $G$ is tetrahedral by Lemma 4.11.

Case $r = 3$. Here we must have $f_1 = f_2 = f_3 = 2$. Indeed, if $f_1 = 1$, then (5.1) becomes
\[
1 - \frac{1}{|G|} = \frac{1}{d_1} - \frac{d_2 - 1}{f_2 d_2} - \frac{d_3 - 1}{f_3 d_3} \leq \frac{1}{d_1} - \frac{1}{4} - \frac{1}{4} \leq 0,
\]
an evident contradiction. So letting $f_i = 2$ for all $i$, (5.1) is equivalent to
\[
1 + \frac{2}{|G|} = \frac{1}{d_1} + \frac{1}{d_2} + \frac{1}{d_3}
\]
If every $d_i \geq 3$, then the right side is at most 1 while the left is strictly larger than 1. So without loss of generality, we have $d_3 = 2$:
\[
\frac{1}{2} + \frac{2}{|G|} = \frac{1}{d_1} + \frac{1}{d_2}
\]
If $d_1$ or $d_2$ is 2, we may take $d_2 = 2$, so that $|G| = 2d_1$ and $G$ is dihedral. Otherwise, we have $d_1 > 2$ and $d_2 > 2$. The above equation implies that both $d_1$ and $d_2$ cannot be larger than 3. So let us suppose $d_2 = 3$. Thus
\[
\frac{1}{6} + \frac{2}{|G|} = \frac{1}{d_1}
\]
Hence $d_1 < 6$. For $d_1 = 3, 4, 5$, we find $|G| = 12, 24, 60$, respectively. We treat these cases separately now.

If $d_1 = 3, d_2 = 3, d_3 = 2$, we find that $G$ has two non-conjugate subgroups of order 3. But $G$ has order $12 = 3 \cdot 4$, so we have contradicted the Sylow theorems.

If $d_1 = 4, d_2 = 3, d_3 = 2$, then $|G| = 24$, and $G$ is octahedral by Lemma 4.15. Indeed, to check that $G$ has no central element of order 2, observe that if $s$ were such an element, then it would fix exactly two points $x$ and $y$. By commutativity, the subgroups of order 3 would act on these two points, hence fixing them, and hence $s$ lies in a maximal cyclic subgroup containing an element of order 3, a contradiction.

If $d_1 = 5, d_2 = 3, d_3 = 2$, then we argue that $G$ is of icosahedral type. Let $n_i$ be the number of elements of $G$ of order $i$. By hypothesis on the $d_i$’s, we see that $n_i = 0$ if $i \neq 1, 2, 3, 5$. Thus, $n_1 = 1$ and
\[
60 = 1 + n_2 + n_3 + n_5.
\]
The Sylow 3- and 5-subgroups are not normal in $G$ because $f_1 = f_2 = 2$. By the Sylow theorems, there are 6 Sylow 5-subgroups, either 4 or 10 Sylow 3-subgroups, and 1, 3, 5, or 15 Sylow 2-subgroups. Note that each Sylow 2-subgroup is dihedral of order 4 — i.e., a Klein 4-group. Thus, $n_5 = 24$, $n_3 = 8$ or 20, and

\[
(5.3)\]
$n_2 = 3, 9, 15,$ or 45. To satisfy (5.3), we must have $n_3 = 20$ and $n_2 = 15$. That is, there are 10 conjugate 3-subgroups and 15 elements of order 2 lying in 5 conjugate Klein 4-groups. Apply Lemma 4.19 to see that $G$ is icosahedral.

We have now shown that the groups presented in Theorem C constitute all possible isomorphism classes of finite $p$-regular subgroups of $\text{PGL}_2(k)$. In the previous section we constructed all of these groups and showed that they are unique up to $\text{PGL}_2(k)$-conjugation.

Remark 5.1. For the reader with a background in algebraic geometry, Klein originally deduced equation (5.1) from the Riemann-Hurwitz formula for the quotient map $\mathbb{P}^1 \to \mathbb{P}^1/G$; see [7, Ch.V.2].

6. Subgroups with elements of order $p$

Convention. Throughout this section we will assume $k$ is an algebraically closed field.

This entire section is devoted to a proof of Theorem B in the case where $k$ is an algebraically closed field. More precisely, the statement reduces to the following:

Theorem 6.1. Let $k$ be an algebraically closed field of characteristic $p > 0$.

1. Let $q$ be a power of $p$. There is exactly one conjugacy class of subgroups of $\text{PGL}_2(k)$ isomorphic to each of $\text{PSL}_2(\mathbb{F}_q)$ and $\text{PGL}_2(\mathbb{F}_q)$.

2. Let $n \in \mathbb{N} \setminus p\mathbb{N}$ and $m \in \mathbb{N}$ with $m \geq 1$. The conjugacy classes of $p$-semi-elementary subgroups of $\text{PGL}_2(k)$ of order $p^m n$ are parameterized by the set of homothety classes of rank-$m$ subgroups $\Gamma \subset k$ that are stable under multiplication by elements of $\mu_n(k)$. The correspondence is

$$\Gamma \mapsto \begin{pmatrix} \mu_n(k) & \Gamma \\ 1 & 1 \end{pmatrix}.$$

3. Suppose that $p = 2$ and $n > 1$ is an odd integer. Then there is a unique conjugacy class of dihedral subgroups of $\text{PGL}_2(k)$ of order $2n$.

4. If $p = 3$, then there is exactly one conjugacy class of subgroups of $\text{PGL}_2(k)$ isomorphic to $\mathfrak{A}_5$.

Any $p$-irregular subgroup of $\text{PGL}_2(k)$ is among the four types listed here.

Remark 6.2. Evidently the above result gives Theorem B when $k$ is algebraically closed except perhaps when $p = 2$ and $G$ is dihedral. But in this latter case, we observe that $(k^\times)^2 = k^\times$, and so the two statements agree.

Let us begin the proof of Theorem 6.1. Suppose that $G \subset \text{PGL}_2(k)$ is a finite subgroup containing an element of order $p$. Write $|G| = p^m n$ with $p \mid n$ and $m \geq 1$, and fix a Sylow $p$-subgroup $P \subset G$. Without loss of generality, we may conjugate $G$ so that $P = (1, \Gamma)$ for some additive subgroup $\Gamma \subset k$ of rank $m$ (§4.2). Let $N = N_G(P)$ be the normalizer of $P$ in $G$. Every element of $N$ fixes $\infty \in \mathbb{P}^1(k)$. Indeed, every element of $P$ fixes $\infty$, and

$$s \in N \implies sus^{-1} \in P \quad (u \in P)$$

$$\implies sus^{-1, \infty} = \infty \quad (u \in P)$$

$$\implies u.(s^{-1, \infty}) = s^{-1, \infty} \quad (u \in P)$$

$$\implies s^{-1, \infty} = \infty.$$

After a suitable conjugation of $G$ we may suppose that $N \subset P \rtimes \left( \mu_d(k) \right)$ for some integer $d$ coprime to $p$ with $\mu_d(k) \subset \mathbb{F}_p^\times$ (Proposition 4.7). But $P$ is normal is this semi-direct product, so $N = P \rtimes \left( \mu_d(k) \right) \rtimes \Gamma$. Let us write $\mathbb{F}_\Gamma = \mathbb{F}_{\mu^\prime}$. As $\Gamma$ is an $\mathbb{F}_\Gamma$-vector space, we find $\ell \mid m$. 

\[ \text{17} \]
If $P$ is normal in $G$, then $N = G$ is a subset of the standard Borel subgroup; we have already dealt with this case in §4.4. Now suppose that $P$ is not normal in $G$, and let us count the elements of $G$ of order $p$ in two different ways.

First, let $P$ act on $G$ by conjugation. If $Q$ is another Sylow $p$-subgroup, then $Q$ fixes a unique point $x \in \mathbb{P}^1(k) \setminus \{\infty\}$. As $s$ varies over $P$, we find $s.x$ varies over a set of $|P| = p^m$ distinct elements. For $s \in P$, we also have $sQs^{-1}(s.x) = s.x$, so that $sQs^{-1}$ fixes $s.x$. Thus, the orbit of $Q$ under the conjugation action of $P$ has cardinality $p^m$. Writing $f > 0$ for the number of orbits of Sylow $p$-subgroups distinct from $P$, it follows that

$$|\{s \in G : s^p = I, s \neq I\}| = (|P| - 1) + f p^m (|P| - 1) = (1 + f p^m)(p^m - 1),$$

(6.1)

and the elements of order $p$ lie in $1 + f p^m$ Sylow $p$-subgroups of $G$. Note further that $G$ acts transitively on the set of Sylow $p$-subgroups by conjugation, and the stabilizer of $P$ under this action is precisely $N$. Hence

$$|G| = |N| \cdot |1 + f p^m| = (1 + f p^m)p^m.$$

Second, we estimate the number of elements of order $p$ in $G$ as follows. Let $\{s_i : i = 1, \ldots, f p^m\}$ be representatives of the nontrivial cosets of $G/N$, and write $s_i = \left( \begin{smallmatrix} \alpha_i & \beta_i \\ \gamma_i & \delta_i \end{smallmatrix} \right)$. Note that $\gamma_i \neq 0$, else $s_i \in N$. If $t_{\lambda, \mu} = \left( \begin{smallmatrix} \lambda & 1 \\ \mu & 1 \end{smallmatrix} \right) \in N$, then we have

$$s_i t_{\lambda, \mu} = \left( \begin{smallmatrix} \alpha_i \lambda + \alpha_i \mu + \beta_i \\ \gamma_i \lambda + \gamma_i \mu + \delta_i \end{smallmatrix} \right).$$

By Lemma 3.2, $s_i t_{\lambda, \mu}$ has order $p$ if and only if

$$(\alpha_i \lambda + \gamma_i \mu + \delta_i)^2 = 4 \lambda \det(s_i).$$

(6.2)

Define $\varepsilon_2 = 1$ and $\varepsilon_p = 2$ for $p \geq 3$ prime. For fixed $s_i$ and $\lambda$, there are precisely $\varepsilon_p$ values of $\mu \in k$ such that (6.2) is satisfied. So for a given $s_i$, there are at most $\varepsilon_p d$ elements $t_{\lambda, \mu} \in N$ such that (6.2) is satisfied. Combining this argument with (6.1), we find that

$$(1 + f p^m)(p^m - 1) = |\{s \in G : s^p = I, s \neq I\}| \leq (p^m - 1) + \varepsilon_p d f p^m.$$

Subtracting $p^m - 1$ from both sides yields

$$f p^m (p^m - 1) \leq \varepsilon_p d f p^m \Rightarrow p^m - 1 \leq \varepsilon_p d p^\ell - 1 \quad (p^\ell = |\mathbb{F}_\Gamma|)$$

(6.3)

If $\ell < m$, then this gives $p^{m-\ell} < 2$, which is impossible. Since $\ell \mid m$, we must have $\ell = m$.

For simplicity in what follows, let us write $q = p^m$. Now $\mathbb{F}_\Gamma = \mathbb{F}_q$, $|\Gamma| = q$, and $\mu_d(k) \subset \mathbb{F}_q^\times = \mathbb{F}_q^\times$. After conjugating by $\left( \begin{smallmatrix} \gamma & 0 \\ 0 & 1 \end{smallmatrix} \right)$ for some $\gamma \in \Gamma \setminus \{0\}$, we may assume that $1 \in \Gamma$. Since $\Gamma$ is stable under multiplication by $\mathbb{F}_\Gamma$, it follows that $\Gamma = \mathbb{F}_q^\times$.

The first line of (6.3) gives

$$d \geq \frac{q - 1}{\varepsilon_p}.$$ 

So if $p = 2$, then $\mu_d(k) = \mathbb{F}_q^\times$, and if $p > 2$, then $\mu_d(k) = \mathbb{F}_q^\times$ or $(\mathbb{F}_q^\times)^2$. We summarize what has been achieved thus far.

**Lemma 6.3.** If $G$ is a finite subgroup of $\text{PGL}_2(k)$ containing an element of order $p$, then up to conjugation, exactly one of the following is true:

- $G \subset B(k)$ (in which case $G$ is $p$-semi-elementary), or
- $G$ contains the Sylow $p$-subgroup $\left( \begin{smallmatrix} 1 & F_q \\ 0 & 1 \end{smallmatrix} \right)$ with normalizer $N = \left( \begin{smallmatrix} 1 & F_q \\ 0 & 1 \end{smallmatrix} \right) \rtimes \left( \begin{smallmatrix} \Lambda & 0 \\ 0 & 1 \end{smallmatrix} \right)$, where $\Lambda = \mathbb{F}_q^\times$ or $\Lambda = (\mathbb{F}_q^\times)^2$. There exists an integer $f > 0$ such that

$$|G| = |\Lambda|(1 + fq)q.$$
We assume in what follows that we are in the second case of Lemma 6.3. It will also be convenient to have the following result at our disposal.

**Lemma 6.4.** Write \( G = N \sqcup s_1N \sqcup \cdots \sqcup s_{fq}N \) as above. Then \( s_i,\infty \neq s_j,\infty \) whenever \( i \neq j \).

**Proof.** If \( s_i,\infty = s_j,\infty \), then \( s_i^{-1}s_j,\infty = \infty \). By the characterization of \( N \) as the largest subgroup of \( G \) that fixes \( \infty \), we must have \( s_i^{-1}s_j \in N \), or equivalently \( s_j \in s_iN \).

### 6.1. The case \( \Lambda = (F_q^\times)^2 \)

Note that this includes the case \( q \) even, where \( (F_q^\times)^2 = F_q^\times \). For \( q > 3 \), we will show that, perhaps after a further conjugation, we have \( G \subset \text{PSL}_2(F_q) \).

Then
\[
q(fq + 1)(q - 1) \varepsilon_p = |G| \leq |\text{PSL}_2(F_q)| = \frac{q(q^2 - 1)}{\varepsilon_p},
\]
so that \( f = 1 \) and \( G = \text{PSL}_2(F_q) \). For \( q = 2 \), we will show that \( G \cong D_{1+2f} \), a dihedral group. For \( q = 3 \), we will show that \( G \) is tetrahedral, and hence conjugate to \( \text{PSL}_2(F_3) \) by Corollary 4.14.

We begin by arranging for the nontrivial coset representatives \( s_1, \ldots, s_{f} \) to have order \( p \). Since \( \Lambda = (F_q^\times)^2 \), the first inequality of (6.3) is actually an equality, which implies that for each fixed coset representative \( s_i \), and each \( \lambda \in \Lambda \), there are exactly \( \varepsilon_p > 0 \) elements \( \mu \in F_q \) satisfying (6.2). In particular, each coset contains an element of order \( p \), so after choosing new coset representatives, we may assume that each \( s_i \) has order \( p \).

We divide the remainder of the proof into four cases: \( q = 2^m \) for \( m > 1 \), \( q > 3 \) odd, \( q = 2 \), and \( q = 3 \).

#### 6.1.1. The Case \( q = 2^m \) with \( m > 1 \).

Write our coset representative as \( s_i = \left( \begin{smallmatrix} \alpha_i & \beta_i \\ \gamma_i & \delta_i \end{smallmatrix} \right) \) for \( i = 1, \ldots, qf \). Replace \( s_i \) with \( \gamma_i^{-1}s_i \) in order to assume that \( \gamma_i = 1 \). (Recall that \( \gamma_i = 0 \) would imply \( s_i \in N \), contradicting our setup.) If we can show that \( \alpha_i, \beta_i, \delta_i \in F_q \), then we will be able to conclude that \( G \subset \text{PGL}_2(F_q) = \text{PSL}_2(F_q) \).

As \( s_i \) has order 2, we see that \( \delta_i = \alpha_i \) (Lemma 3.3). We saw above that for each coset representative \( s_i \), and each \( \lambda \in \Lambda = F_q^\times \), there is a choice of \( \mu \in F_q \) such that \( s_it_{\lambda,\mu} \) has order 2. Take \( \lambda \neq 1 \) so that \( s_it_{\lambda,\mu} \neq s_i \).

Looking at (6.2), we find that
\[
(\alpha_i \lambda + \gamma_i \mu + \delta_i)^2 = 0.
\]
Since \( \delta_i = \alpha_i \) and \( \gamma_i = 1 \), we conclude that \( \alpha_i = \mu/(\lambda + 1) \in F_q \).

It remains to show that \( \beta_i \in F_q \). If \( s_is_j \in N \), then \( s_j \in s_iN \), so that \( i = j \). So for \( i \neq j \) there exist \( \ell \) and \( t_{\lambda,\mu} = \left( \begin{smallmatrix} \lambda & \mu \\ 1 & 1 \end{smallmatrix} \right) \in N \) such that \( s_is_j = s_it_{\lambda,\mu} \). It follows that
\[
\alpha_i = s_{i,\infty} = s_it_{\lambda,\mu,\infty} = s_is_j,\infty = s_is_j,\alpha_j = \frac{\alpha_i \alpha_j + \beta_i}{\alpha_j - \alpha_i} = \frac{\alpha_i \alpha_j + \beta_i}{\alpha_j - \alpha_i} + \beta_i = \frac{1}{\alpha_j - \alpha_i}.
\]

Note that \( \alpha_j - \alpha_i \neq 0 \), else \( \alpha_i = \alpha_j \), from which we deduce that \( s_i,\infty = s_j,\infty \), in contradiction to Lemma 6.4. The above computation shows that \( \beta_i \in F_q \), as desired.

#### 6.1.2. The Case \( q > 3 \) Odd

Recall that each of our coset representatives \( s_i \) has order \( p \). After a suitable scaling, we may further assume that \( \det(s_i) = 1 \). By Lemma 3.2, to say that \( s_i \) has order \( p \) means that
\[
(\alpha_i + \delta_i)^2 = 4 \det(s_i) = 4.
\]

Hence \( \alpha_i + \delta_i = \pm 2 \). Replacing \( s_i \) with \( -s_i \), we may assume that \( \text{tr}(s_i) = \alpha_i + \delta_i = 2 \). We will now argue that \( \alpha_i, \beta_i, \gamma_i, \delta_i \in F_q \).

Write \( \Lambda = \{ \eta^2 : \eta \in F_q^\times \} \). Then (6.2) becomes
\[
(\alpha_i \eta^2 - \gamma_i \mu + 2 - \alpha_i) = 4\eta^2 \iff \alpha_i(\eta^2 - 1) + \gamma_i \mu = -2 + 2\eta.
\]

The right side lies in \( F_q \), and we know that for each choice of \( i \) and \( \eta \in F_q^\times \), there is an element \( \mu = \mu_{i,\eta} \in F_q \) satisfying the above equation.

Setting \( \eta = -1 \) in (6.4) shows \( \gamma_i = -4/\mu_{i,-1} \in F_q \setminus \{0\} \).
As $q > 3$, we may choose $\eta \neq \pm 1$. Then $\alpha_i = (-2 + 2q - \gamma_i \mu_{i; \eta})(\eta^2 - 1)^{-1} \in \mathbb{F}_q$, and $\delta_i = 2 - \alpha_i \in \mathbb{F}_q$. Since $\det(s_i) = 1$, it follows that $\beta_i \in \mathbb{F}_q$ as well. Thus $G \supset \text{PGL}_2(\mathbb{F}_q)$. But $\det(s_i) = 1$ for each $i$ and $\det(t)$ is a square for each $t \in N$. Hence $G \supset \text{PSL}_2(\mathbb{F}_q)$ as desired.

6.1.3. The Case $q = 2$. Setting $s_0 = \{1 \} \}$ and observing that $N = \{I, s_0\}$, our setup allows us to write $G = \sqcup_{i=0}^{2f} N_i$, where each $s_i$ has order 2. As $|G| = 2(1 + 2f)$, each Sylow subgroup has order 2. There are at least $1 + 2f$ such subgroups. As $s_0, \ldots, s_{2f}$ are distinct elements of order 2, they must be all of the elements of order 2. Define

$$t_i = s_is_0 \quad (i = 0, \ldots, 2f).$$

Then $G = \{t_0, \ldots, t_{2f}, s_0, \ldots, s_{2f}\}$, and each $t_i$ has odd order.

Define the set $H = \{t_i : i = 0, \ldots, 2f\}$. We claim that $H$ is an abelian subgroup of $G$. First observe that $t_it_j \neq H$ for any $a, b$. Indeed, since the $s_i$ are all conjugate, there exists $u \in G$ such that $s_0 = usbu^{-1}$. Set $t_c = ut_cu^{-1}$. Then

$$(ut_cu^{-1})(usbu^{-1}) = tcs_0 = t_c \Rightarrow t_a s_b = u^{-1}s_cu \in G \setminus \{H\}.$$  

Now define $s_{b'} = t_as_b$. Then

$$t_a t_b s_0 = t_a s_b = t_{b'} s_0 \Rightarrow t_a t_b = t_{b'} \in H,$$

and hence $H$ is closed under multiplication. Next note that

$$s_0 t_a s_0^{-1} = s_0 t_a s_0 = s_0 s_a = (s_a s_0)^{-1} = t_a^{-1}.$$  

(6.5)

Thus $t_a^{-1}$ is a conjugate of $t_a$ cannot have order 2, and hence $H$ is closed under inversion. Finally, for $t_a, t_b \in H$, we have shown that $t_d := t_b^{-1} t_a^{-1} \in H$. It follows that

$$t_a t_b = (t_b^{-1} t_a^{-1})^{-1} = t_d^{-1} = s_0 t_d s_0^{-1} \quad \text{by (6.5)}$$

$$= (s_0 t_b^{-1})(t_a^{-1} s_0^{-1})$$

$$= (t_b s_0)(s_0 t_a) \quad \text{by (6.5)}$$

$$= t_b t_a,$$

so that $H$ is abelian.

Since $H$ is abelian of odd order, we may apply Theorem C (which we have already proved in the algebraically closed setting) to conclude that $H$ is cyclic. If $t$ is a generator, then $G = \langle t, s_0 \rangle$. Now (6.5) gives $s_0 t_s = t^{-1}$, which is precisely the relation that defines a dihedral group. So $G \cong \mathfrak{D}_{1+2f}$, and there is a unique conjugacy class of such groups by Proposition 4.5.

6.1.4. The Case $q = 3$. As $q = 3$, every Sylow 3-subgroup of $G$ is cyclic. Moreover, every element whose order is divisible by 3 has order exactly 3 (Proposition 4.1), and hence lies in a Sylow 3-subgroup. We may therefore apply the argument at the beginning of §5. Let $G_i, \ldots, G_r$ be a complete set of representatives for conjugacy classes of maximal cyclic subgroups; without loss, we assume that $|G_1| = 3$. Since $\Lambda = (\mathbb{F}_q^*)^2 = \{1\}$ in our setting, we see that $d_1 = 3$ and $f_1 = 1$. Thus, (5.1) and (5.2) become

$$\frac{1}{|G|} = \frac{1}{3} - \sum_{i=2}^r \frac{1}{f_i} \left(1 - \frac{1}{d_i}\right) \quad \text{and} \quad d_if_i \leq |G| \quad (i = 2, \ldots, r).$$

(6.6)

Moreover, since $G_2, \ldots, G_r$ are $p$-regular, we find that $f_i = 1$ or 2 for $i \geq 2$. As in §5, each summand above is at least $\frac{2}{3}$, so that $r = 1$ or 2. If $r = 1$, then $|G| = 3$, and $G$ is contained inside a Borel subgroup of $\text{PGL}_2(k)$. Recall that we are assuming that $G$ does not lie in a Borel subgroup, so $r = 2$. If $d_2 > 2$, then the right side of (6.6) is nonpositive. Thus, $d_2 = 2$ and $f_2 = 2$, and $|G| = 12$.

Evidently $G$ is nonabelian since the normalizer of its Sylow 3-subgroup is not equal to $G$. The Sylow theorems show that $G$ has 4 Sylow 3-subgroups, and hence 8 elements of order 3. Since $d_2 = f_2 = 2$, $G$ contains a dihedral subgroup $K$ of order 4 — i.e., a Klein 4-group. As $|G| = 12$, we conclude there are only 3 elements of order 2. Thus, $K$ is normal, and Lemma 4.11 shows that $G$ is tetrahedral.
6.2. The Case $\Lambda = \mathbb{F}_q^\times$, odd. Suppose now that $\Lambda = \mathbb{F}_q^\times$. Then $|G| = q(q-1)(1+fq)$ with $f > 0$. Observe that $(\Lambda, 1)$ is the maximal subgroup of $G$ fixing 0 and $\infty$. For if $(\alpha, 1) \in G$, then this element normalizes $P = (1, 1)$, and so $\alpha \in \Lambda$.

Let $t_0 = (-1, 1) \in G$. We claim that the centralizer of $t_0$ in $G$ is either $H = \mathbb{F}_q^\times \langle \delta \rangle$ or the dihedral group $D = H \rtimes \langle (1, \tau) \rangle$ for some $\tau \in k^\times$. Indeed, any element that commutes with $t_0$ must stabilize 0 and $\infty$. The maximal subgroup of $G$ that fixes both of these points is $H$. If the centralizer is larger than $H$, then the remaining elements must swap 0 and $\infty$; any such element has the form $(1, \tau)$. If $(1, \tau)$ and $(1, \tau')$ are two such elements, then their product is $(\tau/\tau')_1 \in H$. Hence, the centralizer is either $H$ or $D$, as desired.

We now argue that the centralizer of $t_0$ in $G$ cannot be $H$. We are going to count elements in $G \setminus N$ of order 2 in two different ways to obtain a contradiction. Letting $H$ act on itself by conjugation, the orbit-stabilizer theorem shows that there are $|G|/|H| = q(1+fq)$ elements conjugate to $t_0$, all of which have order 2. We note that the elements conjugate to $t_0$ in $N = (1, 1) \mathbb{F}_q^\times \times (\mathbb{F}_q^\times)_1$ must fix $\infty$ and one other $\mathbb{F}_q$-rational point, so that there are $q$ of them in $N$. Hence

\[ |\{ s \in G \setminus N : s^2 = I \}| \geq q(1+fq) - q =fq^2. \]

An element of $s_i N$ is of the form

\[ s_i t_{\lambda, \mu} = \begin{pmatrix} \alpha_i \lambda & \alpha_i \mu + \beta_i \\ \gamma_i \lambda & \gamma_i \mu + \delta_i \end{pmatrix}, \]

and it has order 2 if and only if $\alpha_i \lambda + \gamma_i \mu + \delta_i = 0$. Note $\gamma_i \neq 0$ else $s_i N$. So given $s_i$ and $\lambda$, there is exactly one $\mu \in \mathbb{F}_q$ such that $s_i t_{\lambda, \mu}$ has order 2. Combining with the above lower bound for the number of elements of order 2, we have that

\[ fq^2 \leq |\{ s \in G \setminus N : s^2 = I \}| = f(q-1), \]

which is absurd. We conclude that $t_0$ is centralized by a dihedral group $D = \mathbb{F}_q^\times \times \langle (1, \tau) \rangle$.

Applying the argument in the last paragraph to $D$ instead of $H$, we find that the number of elements in $G \setminus N$ conjugate to $t_0$ is precisely $\frac{1}{2}q(1+fq) - q = \frac{1}{2}q(fq-1)$. Since this is an integer, we conclude $f$ must be odd. Moreover, it gives the lower bound

\[ \frac{1}{2}q(fq-1). \]

We are going to count the number of elements of order 2 in $G \setminus N$ in yet another way in order to bound $f$.

Since $\gamma_i \neq 0$ for any $i = 1, \ldots, fq$, we may assume that $\gamma_i = 1$ in what follows. Let $n$ be the number of cosets $s_i N$ containing at least two elements of order 2. For each of these cosets, we may assume that $s_i$ has order 2, so that $\delta_i = - \alpha_i$. Moreover, for each such $i$, there exists $(\lambda, \mu) \in \mathbb{F}_q^\times \times \mathbb{F}_q^\times \setminus \{(1,0)\}$ such that $s_i t_{\lambda, \mu}$ has order 2 — i.e.,

\[ \text{tr}(s_i t_{\lambda, \mu}) = \alpha_i(\lambda - 1) + \mu = 0. \]

Hence $\alpha_i = \mu/(1-\lambda) \in \mathbb{F}_q$. For different choices of $i$, we get different values of $\alpha_i = s_i, \infty$ (Lemma 6.4), so that $n \leq |\mathbb{F}_q^\times| = q$. Since $\alpha_i \in \mathbb{F}_q^\times$, for fixed $i$ and $\lambda \in \mathbb{F}_q^\times$ there exists a unique solution $\mu \in \mathbb{F}_q$ to the above trace equation. Thus, a coset $s_i N$ contains precisely $q-1$ elements of order 2 or one element of order 2.

Let $m$ be the number of cosets $s_i N$ containing exactly one element of order 2. Note that $m + n \leqfq$, the total number of nontrivial cosets. The lower bound (6.7) for the number of elements of order 2 combined with the arguments in the last paragraph gives

\[ \frac{1}{2}q(fq-1) \leq m + n(q-1) = m + n + n(q-2) \leq f + q(q-2) \]

\[ \implies f \leq \frac{2q - 3}{q - 2} = 2 + \frac{1}{q - 2}. \]

Since $f$ is odd, we find $f = 1$, or $f = 3$ and $q = 3$. 21
6.2.1. The case \( f = 1 \). Here we have \(|G| = |\Lambda|(1 +fq)q = q(q^2 - 1) = |\text{PGL}_2(\mathbb{F}_q)|\). We now prove that \( G \subset \text{PGL}_2(\mathbb{F}_q) \), so that this containment must actually be equality.

We showed above that \( G \) contains an element of the form \((\begin{smallmatrix} 1 & \tau \\ 1 & -\tau \end{smallmatrix})\) with \( \tau \in k^\times \). For each \( \mu \in \mathbb{F}_q \), we have
\[
v_\mu := \begin{pmatrix} 1 & \mu \\ 1 & -\mu \end{pmatrix} = \begin{pmatrix} \mu & 1 \\ 1 & -\mu \end{pmatrix}.
\]
As \( \mu \) varies over the elements of \( \mathbb{F}_q \), we get \( q \) distinct elements \( v_\mu \) of order 2 satisfying \( v_\mu, \infty = \mu \). Since none of them lies in \( N \), each \( v_\mu \) must lie in a distinct nontrivial coset \( s_iN \) (Lemma 6.4). There are only \(fq = q\) such cosets, so we conclude that every coset contains an element of order 2.

We have now shown that \( N \subset \text{PGL}_2(\mathbb{F}_q) \), and that each nontrivial coset representative may be chosen to have the form \( s_i = \begin{pmatrix} \alpha_i & -\beta_i \\ 1 & \alpha_i \end{pmatrix} \) with \( \alpha_i \in \mathbb{F}_q \). The final paragraph of §6.1.1 applies verbatim to show that \( \beta_i \in \mathbb{F}_q \) as well, which proves that \( G \subset \text{PGL}_2(\mathbb{F}_q) \) as desired.

6.2.2. The case \( f = 3, q = 3 \). Here we find that \(|G| = |\Lambda|(1 +fq)q = 60\). Note that all of the inequalities in (6.8) becomes equalities in this case, so that \( n = 3 \) and \( m = 6 \), and \( G \) contains \( 12 + 3 = 15 \) elements of order 2. We showed at the beginning of this subsection that \( t_0 \) is centralized by a dihedral group \( D \) of order 4. Each such dihedral group \( D \) contains three of the elements of order 2, so that \( G \) contains five conjugate Klein 4-groups. Moreover, at the beginning of §6 we showed that the number of Sylow 3-subgroups is \( 1 +fq = 10 \). It follows that \( G \) is icosahedral (Lemma 4.19). This conjugacy class is unique by Proposition 4.21.

7. Results of Serre and Beauville

We now recall an arithmetic criterion for the existence of certain types of subgroup in \( \text{PGL}_2(k) \). Serre proves the analogous statements for \( \text{GL}_2(k) \) [10, §2], which we adapt for our purposes.

**Theorem 7.1.** Let \( k \) be a field of characteristic \( p \geq 0 \).

(1) If \( n \) is coprime to \( p \), then \( \text{PGL}_2(k) \) contains a cyclic subgroup of order \( n \) if and only if \( \zeta + \zeta^{-1} \in k \) for some primitive \( n \)-th root of unity \( \zeta \).

(2) \( \text{PGL}_2(k) \) contains a tetrahedral subgroup if and only if

- \( p = 2 \) and \( \mathbb{F}_4 \subset k \); or
- \( p \neq 2 \) and \(-1\) is the sum of two squares in \( k \).

(3) \( \text{PGL}_2(k) \) contains an octahedral subgroup if and only if \( p \neq 2 \) and \(-1\) is a sum of two squares in \( k \).

(4) \( \text{PGL}_2(k) \) contains an icosahedral subgroup if and only if \(-1\) is a sum of two squares in \( k \) and either

- \( p = 2 \) and \( \mathbb{F}_4 \subset k \);
- \( p = 5 \); or
- \( p \neq 2, 5 \) and \( \sqrt{5} \in k \).

**Remark 7.2.** If \( p = 2 \), then \( \text{PGL}_2(k) \) does not contain an element of order 4 (Proposition 4.1). In particular, it cannot contain an octahedral subgroup.

**Proof of Theorem 7.1.** We begin with the statement about cyclic groups. Given a primitive \( n \)-th root of unity \( \zeta \) for some \( n \), let us set \( \lambda = \zeta + \zeta^{-1} \). If \( \lambda \in k \), then the element \( \left( \begin{smallmatrix} \lambda^2 + 1 & -1 \\ 1 & \lambda \end{smallmatrix}\right) \) is in \( \text{PGL}_2(k) \) has order \( n \). Indeed, it is conjugate over \( k(\zeta) \) to \( \left( \begin{smallmatrix} \zeta & 1 \\ 1 & \zeta \end{smallmatrix}\right) \) (Corollary 4.2). Conversely, suppose \( s \in \text{PGL}_2(k) \) has order \( n \), and \( p \nmid n \). If \( s \) fixes two points of \( \mathbb{P}^1(k) \), then we may conjugate those points to 0 and \( \infty \) using an element of \( \text{PGL}_2(k) \). In this way, we may assume without loss of generality that \( s = \left( \begin{smallmatrix} \zeta & 1 \\ 1 & \zeta \end{smallmatrix}\right) \) for some primitive \( n \)-th root of unity \( \zeta \in k \). If instead the two fixed points of \( s \) are quadratic over \( k \), then after passing to a quadratic extension \( k'/k \) we are in the previous case and \( \zeta \in k' \). The minimal polynomial for \( \zeta \) over \( k \) is \( z^2 - \lambda z + 1 \), so we must have \( \lambda \notin k \).
To prove the remaining statements, we observe that Serre gives precisely the same criteria for existence of tetrahedral, octahedral, and icosahedral subgroups of GL$_2(k)$ [10, §2.5]. The kernel of the natural homomorphism $\pi$: GL$_2(k) \to$ PGL$_2(k)$ is $k^\times I$, which is the center of GL$_2(k)$. In particular, since $A_4$, $S_4$, and $A_5$ have trivial center, $\pi$ induces an isomorphism on any subgroup isomorphic to one of these. Thus, such a subgroup exists in GL$_2(k)$ if and only if it exists in PGL$_2(k)$.

Next, we give Beauville’s description of the conjugacy classes of $p$-regular subgroups of PGL$_2(k)$:

**Theorem 7.3 ([1, Thm. 4.2]).** Let $k$ be a field of characteristic $p \geq 0$.

1. PGL$_2(k)$ contains at most one conjugacy class of $p$-regular subgroups isomorphic to each of $\mathbb{Z}/n\mathbb{Z}$ ($n > 2$), $A_4$, $S_4$, and $A_5$.

2. If $p \neq 2$, the conjugacy classes of subgroups of order 2 of PGL$_2(k)$ are parameterized by $k^\times/(k^\times)^2$. The correspondence is given by $\tau \mapsto (1^\tau)$.

3. If $p \neq 2$, the homomorphism $\text{det}: \text{PGL}_2(k) \to k^\times/(k^\times)^2$ induces a bijection between
   - Conjugacy classes of subgroups of PGL$_2(k)$ isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$,
   - Subgroups $G = \{1, \alpha, \beta, \alpha\beta\} \subset k^\times/(k^\times)^2$ of order at most 4 such that the conic $x^2 + ay^2 + \beta z^2 = 0$ has a point in $\mathbb{P}^2(k)$. Here we take $\beta = 1$ if $|G| \leq 2$ and $\alpha = 1$ if $|G| = 1$.

The reverse correspondence is given by

$$G \mapsto \left\{ \begin{pmatrix} \lambda & \alpha \mu \\ \mu & -\lambda \end{pmatrix}, \begin{pmatrix} 1 & -\alpha \\ \alpha & 1 \end{pmatrix} \right\},$$

where $(\lambda, \mu, 1)$ is a point on the conic.$^5$

4. Let $n > 2$, and assume that $k$ contains a primitive $n$-th root of unity, say $\zeta$. Let $\text{Dih}_n(k)$ denote the set of conjugacy classes of $p$-regular dihedral subgroups of PGL$_2(k)$ of order $2n$. Then $\text{Dih}_n(k)$ is parameterized by $k^\times/\mu_n(k)(k^\times)^2$, and the correspondence is

$$\alpha \mapsto \left\{ \begin{pmatrix} \zeta & \alpha \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & \alpha \\ \alpha & 1 \end{pmatrix} \right\}.$$ 

**Remark 7.4.** In the version of Theorem 7.3(3) that appears in [1], Beauville incorrectly insists that the conic $x^2 + ay^2 + bz^2 = 0$ have a point for every $a, b \in G$. For a counterexample, we take $k = \mathbb{R}$. Then $\mathbb{R}^\times/(\mathbb{R}^\times)^2 = \{\pm 1\}$. The subgroup

$$\Gamma = \left\{ \begin{pmatrix} \pm 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & \pm 1 \\ \pm 1 & 1 \end{pmatrix} \right\}$$

satisfies $\text{det}(\Gamma) = \{\pm 1\}$. But the conic $x^2 + y^2 + z^2 = 0$ does not have a real point. One can show directly that every subgroup of PGL$_2(\mathbb{R})$ isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$ is conjugate to $\Gamma$. But since $\mathbb{R}^\times/(\mathbb{R}^\times)^2$ has only two subgroups, and one of them doesn’t satisfy the conic property we require, this fact follows immediately from the corrected version of Theorem 7.3(3).

8. Separably Closed Fields

**Convention.** Throughout this section we assume that $k$ is a separably closed field with algebraic closure $k_a$.

The goal of this section is to prove Theorem C and Theorem B in the case where $k$ is a separably closed field. In this setting, Theorem B becomes:

**Theorem 8.1.** Let $k$ be a separably closed field of characteristic $p > 0$. 

$^5$A smooth conic in $\mathbb{P}^2$ either has no rational point or is isomorphic to a line. In the latter case, it must have a point with nonzero $z$-coordinate.
(1) Fix $q > 2,$ a power of $p$. There is exactly one conjugacy class of subgroups isomorphic to each of $\text{PSL}_2(\mathbb{F}_q)$ and $\text{PGL}_2(\mathbb{F}_q)$.

(2) Let $m,n$ be positive integers with $n$ coprime to $p$. The conjugacy classes of split $p$-semi-elementary subgroups of order $p^m n$ are parameterized by the set of homothety classes of rank-$m$ subgroups $\Gamma \subset k$ that are stable under multiplication by elements of $\mu_n(k)$. The correspondence is
\[ \Lambda \mapsto \left( \mu_n(k) \right)^\Gamma. \]

(3) Suppose that $p = 2$, and let $m \geq 1$ be an integer. The conjugacy classes of non-split 2-elementary subgroups of order $2^m$ are parameterized by pairs $(k(\tau), G)$, where $k(\tau)$ is a quadratic inseparable extension of $k$ and $G$ is a subgroup of order $2^m$ of the abelian group
\[ \Omega(\tau) := \{ I \} \cup \left\{ \left( \begin{array}{cc} \alpha & \tau \\ \alpha & \tau \end{array} \right) : \alpha \in k \right\}. \]

(4) Suppose that $p = 2$ and $n > 1$ is an odd integer. Let $\text{Dih}_n(k)$ denote the set of conjugacy classes of dihedral subgroups of $\text{PGL}_2(k)$ of order $2n$. The map $\text{Dih}_n(k) \to k^\times/(k^\times)^2$ defined by $G \mapsto \text{det}(t)$ for any involution $t \in G$ is well defined and bijective.

(5) If $p = 3$, then there is exactly one conjugacy class of subgroups isomorphic to $\mathfrak{A}_5$.

Any $p$-irregular subgroup of $\text{PGL}_2(k)$ is among the five types listed here.

Tracing through the proofs in Sections 3–6, we find that there are a few ways in which the algebraically closed nature of $k$ was used:

- To conjugate a stable pair of points to 0 and $\infty$ (§4.1, §4.3). If a subgroup $G$ stabilizes a pair of distinct points $\{x,y\}$, then any nontrivial $s \in G$ has this property. It follows that either $s$ or $s^2$ fixes $x$ and $y$. If $s$ does not have order 2, then $x,y$ are distinct roots of a quadratic equation over $k$, and they are separable.

- To replace $s$ with $\text{det}(s)^{-1/2} s$ in order to assume $\text{det}(s) = 1$. This was only used in §6.1.2 where $p$ is assumed to be odd. In that case, square roots are separable.

- To assert the existence of a primitive fourth root of unity (§4.5, §4.6) and a primitive fifth root of unity (§4.7). Roots of unity are always separable.

- To find a $k$-rational fixed point of $s = \left( \begin{array}{cc} \alpha & \beta \\ \gamma & \delta \end{array} \right)$, which was then conjugated to $\infty$. If $\gamma = 0$, then $\infty$ is a fixed point of $s$. So we may suppose $\gamma = 1$. Then the equation defining the fixed points of $s$ is $z^2 + (\delta - \alpha)z - \beta = 0$. This polynomial is separable — in which case it will have a root in $k$ — if and only if $p > 2$ or $p = 2$ and $\delta \neq \alpha$. So $s$ fails to have a $k$-rational fixed point if and only if $p = 2$, $\delta = \alpha$, and $\beta$ is not a square in $k$. In particular, $s$ must have order 2.

- To assert the existence of $\sqrt{\tau}$, the fixed point of the element $s = (1 \tau)$ in §4.3. This square root is separable when $p > 2$, but it may fail to be when $p = 2$. Note that $s$ has order 2.

This discussion shows that Theorem C holds for an arbitrary separably closed field, and Theorem 8.1 holds provided the characteristic of $k$ is at least 3.

Convention. In the remainder of this section, we assume that $k$ is a separably closed field of characteristic 2.

Let us summarize what we have learned.

**Lemma 8.2.** Let $s \in \text{PGL}_2(k)$ be an element with no $k$-rational fixed point. Then $s = \left( \begin{array}{cc} \alpha & \beta \\ 1 & \alpha \end{array} \right)$ for some $\alpha, \beta \in k$ with $\beta$ a non-square. In particular, $s$ has order 2.
Theorem 6.1 applied to $\text{PGL}_2(k_a)$ shows that a finite $p$-irregular subgroup of $\text{PGL}_2(k)$ is either dihedral, isomorphic to $\text{PGL}_2(\mathbb{F}_q)$ for some $q$, or $p$-semi-elementary. We treat each of these cases in turn.

**Lemma 8.3.** Let $n > 1$ be an odd integer. Let $\mathfrak{Dih}_n(k)$ denote the set of $k$-conjugacy classes of dihedral subgroups of $\text{PGL}_2(k)$ of order $2n$. Write $D: \mathfrak{Dih}_n(k) \to k^\times/(k^\times)^2$ for the map that sends $G$ to $\det(t)$ for any involution $t \in G$. Then $D$ is well defined.

**Proof.** Let $G$ be dihedral of order $2n$, and let $t$ be an involution in $G$. Replacing $G$ with one of its conjugates has the effect of replacing $t$ with an element of the same determinant. So it suffices to show that every involution in $G$ has the same determinant, up to squares. Write $G = C \rtimes \langle t \rangle$ for a cyclic group $C \subset \text{PGL}_2(k)$. Any involution in $G$ is of the form $st$ for some $s \in C$. Any two cyclic groups of odd order are conjugate in $\text{PGL}_2(k)$ (Theorem 7.3), and so $usu^{-1} = (\lambda^{s^{-1}1})$ for some $\lambda \in k$ and $u \in \text{PGL}_2(k)$ (Corollary 4.2). Here $\lambda = \zeta + \zeta^{-1}$ for some root of unity $\zeta$ with the same order as $s$. Then $\det(s) = \lambda$. Since $\lambda$ lies in the algebraic closure of $\mathbb{F}_2$, it is a square. \hfill $\Box$

**Remark 8.4.** We can simplify the above proof by conjugating $C$ to $(\mu_n(k)^{-1})$ since we are working over a separably closed field. However, our approach applies over an arbitrary field, and will thus be more useful in the final section of these notes.

**Proposition 8.5.** Fix an odd integer $n > 1$. Let $\mathfrak{Dih}_n(k)$ denote the set of $k$-conjugacy classes of dihedral subgroups of $\text{PGL}_2(k)$ of order $2n$. Write $D: \mathfrak{Dih}_n(k) \to k^\times/(k^\times)^2$ for the map that sends $G$ to $\det(t)$ for any involution $t \in G$. Then $D$ is a bijection.

**Proof.** We showed in Lemma 8.3 that the map $D: \mathfrak{Dih}_n(k) \to k^\times/(k^\times)^2$ given by $D(G) = \det(t)$ for any involution $t$ in $G$ is well defined. To see that it is surjective, fix $\tau \in k^\times$ and define $G_\tau := \left(\mu_n(k)^{-1}\right) \times \langle \left(\begin{array}{c} 1 \\ \tau \end{array}\right) \rangle$.

Evidently $G_\tau$ is dihedral of order $2n$, and $D(G_\tau) = \tau$. It remains to prove injectivity.

Let $G$ be a dihedral subgroup of $\text{PGL}_2(k)$ of order $2n$, and let $\zeta \in k$ be a primitive $n$-th root of unity. We begin by showing that there is $\tau \in k^\times$ such that $G$ is conjugate to $G_\tau$. Write $G = C \rtimes \langle t \rangle$ with $C$ the index 2 cyclic normal subgroup of $G$ and $t$ an element of order 2. Since $C$ has odd order, the quadratic polynomial defining its fixed points must have distinct — and hence $k$-rational — roots. Let us conjugate them to 0 and $\infty$ to get a new group $G' = (\mu_n(k)^{-1}) \times \langle t' \rangle$. Then $t'$ acts on the fixed points of $(\mu_n(k)^{-1})$, but it cannot fix both of them. Hence $t' = \left(\begin{array}{c} 1 \\ \tau \end{array}\right)$ for some $\tau \in k^\times$.

Next we show that $G_\tau$ and $G_{\tau'}$ lie in the same conjugacy class if and only if $\tau' = \mu^2\tau$ for some $\mu \in k^\times$.

One direction is easy: $(\mu_1^1)G_\tau(\mu_1^{-1}) = G_{\mu^2\tau}$. For the other direction, suppose that $s^{-1}G_\tau s = G_{t'}$ for some $s \in \text{PGL}_2(k)$. Note that $s$ conjugates the index 2 normal subgroup of $G_{t'}$ to that of $G_\tau$, which is to say that $s$ lies in the normalizer of $(\mu_n(k)^{-1})$. Hence $s = (\mu_1^1)$ or $(\mu_1^-\mu)$ for some $\mu \in k^\times$. In these two cases, we have

$$s^{-1}\left(\begin{array}{c} \tau \\ 1 \end{array}\right)s = \left(\begin{array}{c} \mu^{-1} - \tau \\ 1 \end{array}\right) \quad \text{or} \quad \left(\begin{array}{c} \mu^2\tau^{-1} \\ 1 \end{array}\right).$$

Since these elements have order 2 in $G_{t'}$, there must be $\zeta \in \mu_n(k)$ such that

$$\left(\begin{array}{c} \tau' \\ 1 \end{array}\right) = \left(\begin{array}{c} \zeta \\ 1 \end{array}\right) \left(\begin{array}{c} \mu^{-2}\tau \\ 1 \end{array}\right) \quad \text{or} \quad \left(\begin{array}{c} \zeta \quad \mu^{-2}\tau^{-1} \\ 1 \end{array}\right).$$

As the squaring map on $\mu_n(k)$ is surjective, it follows that $\zeta$ is a square in $k$, and hence $\tau'$ is equal to a square times $\tau$, as desired. \hfill $\Box$

**Lemma 8.6.** Let $G$ be a finite subgroup of $\text{PGL}_2(k)$ of even order. Define $k(G)/k$ to be the field extension generated by the fixed points of all Sylow 2-subgroups of $G$. (We define $k(\infty) = k$.) Then $k(G)/k$ has degree at most 2. If $[k(G):k] = 2$, then every Sylow 2-subgroup of $G$ is its own normalizer.
Proof. Let \( P \) be a Sylow 2-subgroup of \( G \). Recall that \( P \) is abelian and has a single fixed point in \( \mathbb{P}^1(k) \), say \( \tau \) (Lemma 4.3). Since all Sylow 2-subgroups are conjugate, we have \( k(G) = k(\tau) \). If \( \tau \in \mathbb{P}^1(k) \), then \( k(G) = k \). Otherwise, \( P \) does not have a \( k \)-rational fixed point. Let \( s = \begin{pmatrix} \alpha & \beta \\ 1 & \alpha \end{pmatrix} \) be a nontrivial element of \( P \) (Lemma 8.2). Then the fixed point of \( s \) is given by the equation \( z^2 = \beta \not\in (k^\times)^2 \), so that \( \tau = \sqrt{\beta} \). Therefore \( k(G)/k \) has degree 2.

Suppose now that \( u \) is a nontrivial element of the normalizer of \( P \), so that \( u^{-1}Pu = P \). It follows that \( \tau \) is a fixed point of \( u \). Since the fixed points of \( u \) are defined by an equation with \( k \)-coefficients, and since \( \tau \) is quadratic inseparable, it follows that \( \tau \) is the unique fixed point of \( u \). Thus \( u \) has order 2 by Lemma 8.2, and \( u \in P \). \( \square \)

Next, we treat subgroups isomorphic to \( \text{PGL}_2(\mathbb{F}_q) = \text{PSL}_2(\mathbb{F}_q) \). Note that when \( q = 2 \), this group is dihedral and hence has already been dealt with.

**Proposition 8.7.** Let \( q = 2^r \) for some \( r > 1 \). If \( G \subset \text{PGL}_2(k) \) is isomorphic to \( \text{PGL}_2(\mathbb{F}_q) \), then it is \( k \)-conjugate to \( \text{PGL}_2(\mathbb{F}_q) \).

**Proof.** Let \( P \) be a Sylow 2-subgroup of \( G \). As \( |\text{PGL}_2(\mathbb{F}_q)| = q(q^2-1) \), the order of \( P \) is \( q \). If the unique fixed point \( \tau \) of \( P \) is \( k \)-rational, then the argument in §6.1 shows that \( G \) is \( k \)-conjugate to \( \text{PGL}_2(\mathbb{F}_q) \), as desired. Otherwise, \( |k(\tau) : k| = 2 \), and \( P \) is its own normalizer (Lemma 8.6). But this is absurd: the normalizer of a Sylow \( p \)-subgroup of \( \text{PGL}_2(\mathbb{F}_q) \) is the Borel group containing \( P \). \( \square \)

Finally, we attend to the finite 2-semi-elementary subgroups of \( \text{PGL}_2(k) \). If \( G \) is such a subgroup, then it fixes a unique point \( \tau \in \mathbb{P}^1(k) \). If \( \tau \) is \( k \)-rational, then \( G \) is split and we may conjugate \( \tau \) to infinity. The discussion in Section 4.4 applies and we obtain the description in Theorem 8.1. If \( \tau \) is not rational, then it must be quadratic inseparable. In particular, \( \tau^2 \in k \).

**Lemma 8.8.** Let \( \tau \in k \) be such that \( \tau^2 \in k \) but \( \tau \not\in k \). Suppose that \( s \in \text{PGL}_2(k) \) fixes \( \tau \). Then

\[
\begin{align*}
ds & \in \Omega(\tau) = \{I\} \cup \left\{ \begin{pmatrix} \alpha & \tau^2 \\ 1 & \alpha \end{pmatrix} : \alpha \in k \setminus \{\tau\} \right\}.
\end{align*}
\]

**Proof.** We may suppose that \( s \) is nontrivial. Since \( \tau \) is inseparable and \( s \) is defined over \( k \), the fixed point polynomial for \( s \) vanishes only at \( \tau \). Apply Proposition 4.10. \( \square \)

If \( G \) is a non-split 2-semi-elementary subgroup with fixed point \( \tau \), then the lemma shows \( G \subset \Omega(\tau) \). If \( \tau' \in k(\tau) \setminus k \), then \( \Omega(\tau) \) is conjugate to \( \Omega(\tau') \). Indeed, since \( \tau \) is quadratic, we may write \( \tau' = u + v\tau \) for some \( u, v \in k \) and \( u \neq 0 \). Looking at fixed points, we see immediately that

\[
\Omega(\tau) = \begin{pmatrix} v & u \\ u & 1 \end{pmatrix} \begin{pmatrix} \tau^2 \\ 1 \end{pmatrix} \Omega(\tau') \begin{pmatrix} v & u \\ u & 1 \end{pmatrix}^{-1}.
\]

In particular, any finite subgroup of \( \Omega(\tau) \) is conjugate to one inside \( \Omega(\tau') \).

It remains to show that if \( G, G' \subset \Omega(\tau) \) are subgroups that are conjugate inside \( \text{PGL}_2(k) \), then in fact they are equal. Suppose that \( s^{-1}Gs = G \) for some \( s \in \text{PGL}_2(k) \). Then \( s \) must fix \( \tau \). The above lemma shows that \( s \in \Omega(\tau) \). As \( \Omega(\tau) \) is abelian, we conclude that \( G = G' \).

9. **Galois Descent**

**Convention.** For this section, \( k \) denotes an arbitrary field of positive characteristic \( p \), \( k_a \) denotes a separable closure of \( k \), \( k_s \) denotes an algebraic closure of \( k_a \), and \( g = \text{Gal}(k_s/k) \).

We use the technique of Galois descent to pass from the classification of finite subgroups of \( \text{PGL}_2 \) over separably closed fields to the case of arbitrary fields. It begins with a result of Beauville:
Theorem 9.1 ([1, §2]). Let $G$ be an algebraic group defined over a field $k$, let $H$ be a subgroup of $G(k)$, let $N = N_{G(k)}(H)$ be its normalizer in $G(k)$, and let $Z$ be the centralizer of $H$ in $G(k)$. Write $\text{Conj}(H, G(k))$ for the set of subgroups of $G(k)$ that are conjugate to $H$ in $G(k)$ modulo conjugacy in $G(k)$. Then there is a canonical isomorphism of pointed sets
\[
\ker \left[ H^1(g, Z) \to H^1(g, G(k)) \right] / N \simeq \text{Conj}(H, G(k)).
\]

We are able to give a complete description of the kernel in Beauville’s result when $H$ is a $p$-irregular subgroup.

Theorem 9.2. Let $H \subset \text{PGL}_2(k)$ be a finite $p$-irregular subgroup, and let $Z$ be the centralizer of $H$ in $\text{PGL}_2(k_g)$.

1. If $p > 2$, then $H^1(g, Z) = 1$.
2. If $p = 2$ and $H$ is not a 2-group, then $H^1(g, Z) = 1$.
3. If $p = 2$ and $H$ is a split 2-group, then $H^1(g, Z) = 1$.
4. If $p = 2$ and $H$ is a non-split 2-group with inseparable fixed point $\tau$, then there is an isomorphism of abelian groups
\[
k/\langle k \times k \rangle \simeq H^1(g, Z),
\]
where $f(x, y) = x^2 + y + \tau^2 y^2$.

In all cases, the canonical homomorphism $H^1(g, Z) \to H^1(g, \text{PGL}_2)$ has trivial kernel.

Applying Theorem 9.1, we find that $\text{Conj}(H, \text{PGL}_2(k))$ contains a unique element for any finite $p$-irregular subgroup $H$. We state this formally:

Corollary 9.3. Let $H$ be a finite $p$-irregular subgroup of $\text{PGL}_2(k)$. If $H' \subset \text{PGL}_2(k)$ is another subgroup that is conjugate to $H$ inside $\text{PGL}_2(k_g)$, then it is already conjugate inside $\text{PGL}_2(k)$.

Proof of Theorem 9.2. Any element $s \in Z$ must stabilize the unique fixed point of any Sylow $p$-subgroup of $H$. If $H$ has at least 3 Sylow $p$-subgroups, then $s$ fixes at least 3 points of $\mathbb{P}^1(k)$, so $s \in Z$. Thus $H^1(g, Z) = 1$ for trivial reasons. Looking at the possible isomorphism types of $p$-irregular subgroups in Theorem 6.1, we see that this argument covers everything but the case where $H$ is a $p$-semi-elementary subgroup.

Now suppose that $H$ is a $p$-semi-elementary subgroup of $\text{PGL}_2(k)$ with Sylow $p$-subgroup $P$. Write $\tau \in \mathbb{P}^1(k)$ for the unique fixed point of $H$. We have two cases to consider depending on whether $\tau$ is $k$-rational.

Case $\tau$ is $k$-rational. We may conjugate $\tau$ to $\infty$, so that $P \subset \left\{ \left( \begin{smallmatrix} 1 & k \\ 0 & 1 \end{smallmatrix} \right) \right\}$. The centralizer of $P$ in $\text{PGL}_2(k_g)$ is $U(k_g) = \left\{ \left( \begin{smallmatrix} 1 & k_g \\ 0 & 1 \end{smallmatrix} \right) \right\}$, and hence $Z \subset U(k_g)$. If $P = H$, then $Z = U(k_g) \cong G_2(k_g)$ as $g$-modules. It is well known that $H^1(g, G_2) = 1$ [9, Ch. X.1]. If instead $P \subsetneq H$, then $H$ contains an element $u$ of order prime to $p$. The fixed points of $u$ are $\infty$ and a second $k$-rational point $\tau'$. Any $s \in Z$ must also fix $\tau'$, which means $Z = 1$, and $H^1(g, Z) = 1$.

Note that the case where $\tau$ is $k$-rational covers the case where $p > 2$. Indeed, the defining equation for the fixed points of a nontrivial element of $P$ is quadratic with a unique solution; if $p > 2$, then $\tau$ is automatically $k$-rational.

Case $\tau$ is not $k$-rational. We must have $p = 2$ and $H$ is a 2-group. Then $\tau$ is purely inseparable over $k$, so $\tau^2 \in k$. The centralizer of $H$ is the group of elements that fix $\tau$:
\[
Z = \left\{ \left( \begin{array}{cc} \alpha & \tau^2 \beta \\ \beta & \alpha \end{array} \right) : \alpha, \beta \in k, \alpha^2 + \tau^2 \beta^2 \neq 0 \right\}.
\]
Consider the short exact sequence of $\mathfrak{g}$-module homomorphisms
\[
1 \rightarrow Z \xrightarrow{\phi} G_\alpha \times G_\alpha \xrightarrow{f} G_\alpha \rightarrow 0,
\]
where
\[
\phi \left( \begin{array}{c} \alpha \\ \beta \\ \tau^2 \beta \end{array} \right) = \left( \begin{array}{c} \alpha \beta \\ \alpha^2 + \tau^2 \beta^2 \\ \alpha^2 + \tau^2 \beta^2 \end{array} \right) \quad \text{and} \quad f(x, y) = x^2 + y + \tau^2 y^2.
\]
(To see that $\ker(\phi) \subset \text{im}(\phi)$, take $\alpha = x/y$ and $\beta = 1$ when $y \neq 0$. To see that $f$ is onto, take $z \in k$, and note that $\tau^2 y^2 + y + z$ is separable as a polynomial in $y$. So $f(0, y) = z$.) Passing to the long exact sequence on cohomology and using the fact that $H^1(\mathfrak{g}, G_\alpha \times G_\alpha) \cong H^1(\mathfrak{g}, G_\alpha) \times H^1(\mathfrak{g}, G_\alpha) = 1$, we see that
\[
H^0(\mathfrak{g}, G_\alpha \times G_\alpha) \xrightarrow{f} H^0(\mathfrak{g}, G_\alpha) \xrightarrow{k} H^1(\mathfrak{g}, Z) \rightarrow 1.
\]
The coboundary map $\delta$ induces the desired isomorphism $k/f(k \times k) \cong H^1(\mathfrak{g}, Z).

Finally, we must show that the kernel of the homomorphism $H^1(\mathfrak{g}, Z) \rightarrow H^1(\mathfrak{g}, \text{PGL}_2)$ is trivial. It is obvious when $H^1(\mathfrak{g}, Z) = 1$, so let us assume that $p = 2$, $H$ is a 2-group, and its fixed point $\tau$ satisfies $\sqrt{\tau} \notin k$. Let $z_s : \mathfrak{g} \rightarrow Z$ be a 1-cocycle that becomes a coboundary when its target is extended to $\text{PGL}_2$. Then there exists $u \in \text{PGL}_2(k)$ such that $z_s = u^{-1}(s)u$ for every $s \in \mathfrak{g}$. Since every element of $Z$ fixes $\sqrt{\tau}$, we see that
\[
\sqrt{\tau} = z_s \cdot \sqrt{\tau} = u^{-1}(s)u \cdot \sqrt{\tau} \Rightarrow u \cdot \sqrt{\tau} = (s)u \cdot \sqrt{\tau} = s(u \cdot \sqrt{\tau}).
\]
The final equality follows from the fact that $\sqrt{\tau}$ lies in a purely inseparable extension of $k$, so that $\mathfrak{g}$ acts trivially on it. Thus $u \cdot \sqrt{\tau}$ is defined over $k(\sqrt{\tau})$. Note that $u \cdot \sqrt{\tau} \notin \mathbb{F}_2(k)$ since that would imply $\sqrt{\tau} = u^{-1} \cdot (u \cdot \sqrt{\tau}) \in \mathbb{F}_1(k)$. Choose $v \in \text{PGL}_2(k)$ such that $v(u \cdot \sqrt{\tau}) = \sqrt{\tau}$. Then $vu \in Z$, and $z_s = (vu)^{-1} \cdot s(vu)$. That is, $z_s$ is already a coboundary, and hence trivial in $H^1(\mathfrak{g}, Z)$.
\[\square\]

10. PROOFS OF THE MAIN THEOREMS

Convention. Throughout this section, $k$ is an arbitrary field of characteristic $p \geq 0$.

Theorem C has already been proved in §5 and §8. We are now ready to prove Theorems A and B from the introduction.

**Proof of Theorem A.** As $\text{PGL}_2(k) \subset \text{PGL}_2(k_0)$, the isomorphism type of a finite $p$-irregular subgroup of $\text{PGL}_2(k)$ must be among those in Theorem 8.1.

We begin with subgroups isomorphic to $\text{PGL}_2(\mathbb{F}_q)$ for some $q$. If $\mathbb{F}_q \subset k$, then evidently $\text{PGL}_2(\mathbb{F}_q) \subset \text{PGL}_2(k)$. Conversely, suppose that $G \subset \text{PGL}_2(k)$ is isomorphic to $\text{PGL}_2(\mathbb{F}_q)$. We must show $\mathbb{F}_q \subset k$; as this is obvious when $q = 2$, we may assume $q > 2$. Theorem 8.1 shows that $G$ is conjugate inside $\text{PGL}_2(k_0)$ to $\text{PGL}_2(\mathbb{F}_q)$, and Corollary 9.3 shows that this conjugacy takes place in $\text{PGL}_2(k)$. It follows that $\mathbb{F}_q \subset k$.

An identical argument applies to subgroups isomorphic to $\text{PSL}_2(\mathbb{F}_q)$.

Next we treat the $p$-semi-elementary subgroups of order $p^m n$ with $m \geq 1$ and $n \geq 1$ coprime to $p$. Let $e$ be the minimum positive integer such that $p^e \equiv 1 \pmod{n}$, and suppose that $e \mid m$ and $m \leq \dim_{\mathbb{F}_p}(k)$. Let $\Gamma \subset k$ be an $\mathbb{F}_{p^e}$-vector space of dimension $m/e$. Then $|\Gamma| = p^m$, and $(\mu_n(k)^{-1})$ is a $p$-semi-elementary subgroup of order $p^m n$. Conversely, suppose that $G \subset \text{PGL}_2(k)$ is a split $p$-semi-elementary group of order $p^m n$. Writing $e$ for the order of $p$ in $(\mathbb{Z}/n\mathbb{Z})^\times$, we must show that $e \mid m$ and $m \leq \dim_{\mathbb{F}_p}(k)$. Since $G$ is split, its unique fixed point is $k$-rational. We can conjugate its fixed point to infinity and write $G = (\mu_n(k)^{-1})$ as in §4.4. Then $\mathbb{F}_{p^e} \subset \mathbb{F}_\Gamma$, since $\mathbb{F}_\Gamma$ contains the $n$-th roots of unity. It follows that $\Gamma$ is an $\mathbb{F}_{p^e}$-vector space, from which we conclude that $e \mid m$. As $\Gamma \subset k$, it is clear that $m = \dim_{\mathbb{F}_p}(\Gamma) \leq \dim_{\mathbb{F}_p}(k)$.

Now we suppose that $p = 2$ and treat the non-split 2-elementary subgroups of order $2^m$, $m \geq 1$. Suppose there is $\tau \in k_0$ such that $\tau^2 \notin k$ but $\tau \notin k$. Evidently $k$ is not finite, and so the group $\Omega(\tau) \subset \text{PGL}_2(k)$ of Proposition 4.10 is a 2-elementary group of infinite rank. Choose any subgroup of rank $m$. Conversely, suppose there exists a non-split 2-elementary subgroup $G \subset \text{PGL}_2(k)$ of order $2^m$. By definition, the unique
fixed point $\tau$ of $G$ is not $k$-rational. Let $s \in G$ be non-trivial. By Proposition 4.10, we see $s = (\zeta_\alpha^2)$ for some $\alpha \in k$. It follows that $\tau^2 \in k$, but $\tau \notin k$. That is, $k$ contains a non-square.

Next we assume $p = 2$ and deal with the existence of dihedral subgroups of order $2n$ with $n > 1$ odd. If $\zeta$ is a primitive $n$-th root of unity such that $\lambda = \zeta + \zeta^{-1} \in k$, then we set $s = (\zeta_{\lambda + 1}^1)$ and $t = (1^1)$. Corollary 4.2 shows that $s$ has order $n$, and direct calculation shows that $tst = s^{-1}$. That is, $(s, t) \subset \text{PGL}_2(k)$ is dihedral of the desired order. Conversely, suppose that $H \subset \text{PGL}_2(k)$ is dihedral of order $2n$. In particular, $H$ contains a 2-regular cyclic subgroup of order $n$, which shows that $\zeta + \zeta^{-1} \in k$ for some primitive $n$-th root of unity $\zeta$ (Theorem 7.1).

Finally, we suppose that $p = 3$ and consider the existence of icosahedral subgroups of $\text{PGL}_2(k)$. If we assume that $F_9 \subset k$, then $k$ contains a solution $\lambda$ to $X^2 + X + 2 = 0$. Define
\[
s = \begin{pmatrix} \lambda + 1 & -1 \\ 1 & 1 \end{pmatrix}, \quad t = \begin{pmatrix} -1 \\ 1 \end{pmatrix}.
\]

Lemma 3.3 shows that $s$ has order 5, that $t$ has order 2, and that $st$ has order 3. It follows that the subgroup $(s, t) \subset \text{PGL}_2(F_9)$ is isomorphic to $A_5$ (Lemma 4.20). Conversely, suppose that $G \subset \text{PGL}_2(k)$ is an icosahedral subgroup. Then it contains a subgroup of order 5. By Theorem 7.1, we see that $\lambda := \zeta + \zeta^{-1} \in k$ for some primitive fifth root of unity $\zeta$. But $\lambda$ is quadratic over $F_3$, with minimal polynomial $X^2 + X + 2$, and hence it generates $F_9$.

**Proof of Theorem B.** Over the separable closure $k_s$ of $k$, there are five kinds of subgroups to consider (Theorem 8.1). We will determine the conjugacy classes over $k$ in each case.

We begin with subgroups isomorphic to $\text{PGL}_2(F_q)$ or $\text{PSL}_2(F_q)$ with $q > 2$. Theorem 8.1 shows there is a unique $\text{PGL}_2(k_s)$-conjugacy class of subgroups isomorphic to either of these, and Corollary 9.3 shows there is at most one conjugacy class in $\text{PGL}_2(k)$.

The case of split $p$-semi-elementary subgroups of order $p^m n$ is handled just as in §4.4.

The case of non-split 2-elementary subgroups of order $2^m$ is immediate from the discussion at the end of §8; indeed, the hypothesis that $k$ was separably closed was never used there.

Next we assume $p = 2$ and deal with existence of dihedral subgroups of order $2n$ $(n > 1$ odd). Lemma 8.3 shows that the map $D: \text{Dih}_2(k) \to k^\times/(k^\times)^2$ associating $G$ to the determinant of one of its involutions is well defined. Suppose that $G, G'$ are dihedral of order $2n$ satisfying $D(G) = D(G')$. Then $G$ and $G'$ are conjugate over $k_s$ by Theorem 8.1. Corollary 9.3 shows that $G$ and $G'$ are conjugate over $k$. It follows that $D$ is injective. To complete the proof in this case, we must show that $D$ is surjective when $k$ contains a primitive $n$-th root of unity, say $\zeta$. But this is clear: given any $\tau \in k^\times$, the group $G_\tau := \langle (\zeta_1^1), (1^\tau) \rangle$ is dihedral of order $2n$ and satisfies $D(G_\tau) = \tau$.

Finally, suppose that $p = 3$, and $F_9 \subset k$. Theorem A shows that $\text{PGL}_2(k)$ contains an icosahedral subgroup. As above, Theorem 8.1 and Corollary 9.3 show that there is at most one conjugacy class of such subgroups in $\text{PGL}_2(k)$.

**Proof of Theorem D.** Let $F_q$ be a finite field with $q = p^r$ elements. Theorems A and C give the list of possible isomorphism types of subgroups for us to consider: cyclic, dihedral, tetrahedral, octahedral, icosahedral, split $p$-semi-elementary, and $\text{PSL}/\text{PGL}$. We look at each in turn, though there will be overlap among the cases.

Suppose first that $C = (s)$ is a cyclic subgroup of $\text{PGL}_2(F_q)$ of order $n > 2$ and coprime to $p$. Theorem 7.1 asserts that $\lambda := \zeta + \zeta^{-1} \in F_q$ for some primitive $n$-th root of unity $\zeta$. If $\zeta \in F_q$, then $n \mid (q - 1)$. Otherwise, $\zeta$ is quadratic over $F_q$ and $n \mid (q + 1)$. That is, $q \equiv \pm 1 \pmod n$. Conversely, if $\lambda := \zeta + \zeta^{-1} \in F_q$ for some primitive $n$-th root of unity $\zeta$, then $(\lambda_{\pm 1}^1) \in \text{PGL}_2(k)$ has order $n$ (Corollary 4.2). Theorem 7.3 shows that if a cyclic subgroup of order $n$ exists, then it is unique up to conjugation.

Next we look at cyclic subgroups of order 2 when $p \neq 2$. The element $(1^1)$ has order 2, so such subgroups always exist. Since $F_q^\times/(F_q^\times)^2$ has order 2, Theorem 7.3(3) shows that there are two distinct conjugacy classes.
They may be represented by \{I, (1 \ 1)\} and \{I, (1 \ \zeta)\} for \zeta a primitive (q - 1)-st root of unity. The former is split and the latter is not.

Now we turn to the dihedral groups, beginning with those of order 2n where \(n \geq 3\) and \(p\) is coprime to \(2n\). Suppose first that \(q \equiv 1 \pmod{n}\), so that \(F_q\) contains a primitive \(n\)-th root of unity \(\zeta\). Theorem 7.3(5) asserts that conjugacy classes of dihedral subgroups of order 2n are in bijection with elements of the group \(\mathbb{F}_q^\times/\mu_n(F_q)(\mathbb{F}_q^\times)^2\). If \(q \equiv 1 \pmod{2n}\), then every \(n\)-th root of unity is a square and this group has order 2; otherwise, it has order 1.

Next we consider dihedral groups of order 2n where \(q \equiv -1 \pmod{n}\) and \(n \geq 3\). First note that such subgroups always exist: if \(\zeta \in \mathbb{F}_q^\times\) is a primitive \(n\)-th root of unity, then \(\lambda := \zeta + \zeta^{-1} \in \mathbb{F}_q\) and \(\langle(\lambda^{n+1} - 1)/2, (1, \lambda)\rangle\) is dihedral of the desired order (cf. Corollary 4.2). Suppose now that \(H \subset \text{PGL}_2(\mathbb{F}_q)\) is any dihedral subgroup of order 2n. Let \(s\) be a generator of the cyclic subgroup of index 2. Since cyclic \(p\)-regular subgroups are unique up to conjugation, we may assume that \(s = (1, \lambda)\). Let \(t\) be an involution in \(H\), so that \(H = \langle s, t \rangle\). Set \(u = \left(\begin{smallmatrix} 1 & -\zeta^{-1} \\ \zeta & 1 \end{smallmatrix}\right) \in \text{PGL}_2(\mathbb{F}_q^\times)\); conjugating by \(u\) has the effect of moving the fixed points of \(s\) to \(\infty\) and 0:

\[
usu^{-1} = \left(\begin{array}{c} \zeta \\ 1 \end{array}\right).
\]

Since \(s\) fixes \(\zeta\) and \(\zeta^{-1}\), \(t\) must swap these points. It follows that there is \(\tau \in \mathbb{F}_q^\times\) such that

\[
uttu^{-1} = \left(\begin{array}{c} \tau \\ 1 \end{array}\right).
\]

We can recover \(t\) from \(\tau\):

\[
u^{-1} \left(\begin{array}{c} 1 \\ \tau \end{array}\right) u = \left(\begin{array}{cc} \zeta^{-1} - \tau \zeta & -\zeta^{-2} + \tau \zeta^2 \\ 1 - \tau & -\zeta^{-1} + \tau \zeta \end{array}\right).
\]

If \(\tau = 1\), then \(u^{-1} \left(\begin{array}{c} 1 \\ \tau \end{array}\right) u = \left(\begin{array}{c} 1 \\ 1 \end{array}\right) \in \text{PGL}_2(\mathbb{F}_q)\). Otherwise, we find that

\[
u^{-1} \left(\begin{array}{c} 1 \\ \tau \end{array}\right) u = \left(\begin{array}{cc} \zeta^{-1} - \tau \zeta & -\zeta^{-2} + \tau \zeta^2 \\ 1 - \tau & -\zeta^{-1} + \tau \zeta \end{array}\right)
\]

\((\tau \neq 1)\).

Since this must lie in \(\text{PGL}_2(\mathbb{F}_q)\), the top left entry must lie in \(\mathbb{F}_q\). That is, it is Frobenius invariant, and we have

\[
\frac{\zeta - \tau \zeta^{-1}}{1 - \tau^q} = \frac{\zeta^{-1} - \tau \zeta}{1 - \tau}.
\]

Clearing denominators and massaging shows that \(\tau^{q+1} = 1\). Thus \(\tau \in (\mathbb{F}_q^\times)^{q-1}\).

We wish to determine how \(\tau\) depends on the conjugacy class of \(H\). The normalizer of \(uHu^{-1}\) in \(\text{PGL}_2(\mathbb{F}_q^\times)\) consists of elements of the form \((\alpha \ 1)\) and \((1 \ \beta)\), with \(\alpha, \beta \in \mathbb{F}_q^\times\). We restrict attention to elements \(v\) of this form with \(u^{-1}vu \in \text{PGL}_2(\mathbb{F}_q)\). A computation as in the previous paragraph shows that \(\alpha^{q+1} = \beta^{q+1} = 1\). Conjugating \(uHu^{-1}\) by \((\alpha \ 1)\) has the effect of replacing \(\tau\) with \(\alpha^2 \tau\). Conjugating by \((1 \ \beta)\) replaces \(\tau\) with \(\beta^2 \tau^{-1} = (\beta/\tau)^2 \tau\). Note that \(uH_u^{-1}\) also contains the involutions \(\zeta^i \tau\) for any \(i\). It follows that for any \(\tau' \in \mu_n(\mathbb{F}_q^\times)(\mathbb{F}_q^\times)^{2(q-1)}\), the group \(H\) is conjugate in \(\text{PGL}_2(\mathbb{F}_q)\) to the group \(H'\), where \(uH' u^{-1} = \langle(\zeta^i, 1), (1, \tau')\rangle\). Thus, the conjugacy classes of dihedral subgroups of \(\text{PGL}_2(\mathbb{F}_q)\) of order 2n are in bijection with elements of the group \((\mathbb{F}_q^\times)^{2(q-1)}/\mu_n(\mathbb{F}_q^\times)(\mathbb{F}_q^\times)^{2(q-1)}\). (Compare Theorem 7.3(5).) If \(q \equiv -1 \pmod{2n}\), then every element of \(\mu_n(\mathbb{F}_q^\times)\) is a square in \(\mu_{q+1}(\mathbb{F}_q^\times)\) and \((\mathbb{F}_q^\times)^{q-1}/\mu_n(\mathbb{F}_q^\times)(\mathbb{F}_q^\times)^{2(q-1)}\) has order 2. Otherwise, it has order 1.

Now we look at 4-groups with \(p \neq 2\). Since every conic over \(\mathbb{F}_q\) has a point, and since \(\mathbb{F}_q^\times/(\mathbb{F}_q^\times)^2\) has order 2, Theorem 7.3(4) shows that there are exactly two conjugacy classes of subgroups of order 4.

Next we consider dihedral subgroups of order 2n when \(p = 2\) and \(n > 1\) is odd. We may suppose that \(q \equiv \pm 1 \pmod{n}\), so that cyclic subgroups of order \(n\) exist. Since \(\mathbb{F}_q^\times = (\mathbb{F}_q^\times)^2\), Theorem B(4) shows that there is a unique conjugacy class of dihedral subgroups of order 2n.

30
Next we consider subgroups isomorphic to $\mathfrak{A}_4$. If $p \neq 2$, then Theorem 7.1 shows that such a subgroup exists if and only if $-1$ is the sum of two squares in $F_q$, which always holds by a counting argument. If $p = 2$, then Theorem 7.1 shows that such a subgroup exists if and only if $F_4 \subset F_q = F_{2^r}$, which is to say $r$ is even. Theorem 7.3 shows that such a subgroup is unique up to conjugation when $p \neq 2, 3$. When $p = 3$, we find that $\mathfrak{A}_4 \cong \operatorname{PSL}_2(F_3)$ (Corollary 4.14). Theorem B(1) shows that such a subgroup is unique up to conjugation. When $p = 2$, a tetrahedral subgroup is 2-semi-elementary; the argument used to prove Proposition 4.12 shows that it is conjugate to the standard Borel subgroup in $\operatorname{PGL}_2(F_4)$.

The case of octahedral subgroups is identical to that of tetrahedral subgroups, except that they cannot occur when $p = 2$. Indeed, $\mathfrak{S}_4$ contains an element of order 4, while $\operatorname{PGL}_2(F_{2^m})$ does not. Use Corollary 4.18 to handle the case $p = 3$.

Next we look at subgroups isomorphic to $\mathfrak{A}_5$. If $p \neq 2, 5$, then Theorem 7.1 shows that such a subgroup exists if and only if $-1$ is the sum of two squares in $F_q$ (always true) and $\sqrt{5} \in F_q$. By quadratic reciprocity, the latter condition holds if and only if $q \equiv \pm 1 \pmod{5}$. The case $p = 5$ is taken care of by the fact that $\operatorname{PGL}_2(F_5) \cong \mathfrak{A}_5$ (Proposition 4.22). If $p = 2$, then Theorem 7.1 shows that such a subgroup exists if and only if $-1$ is the sum of two squares in $F_q$ (always true) and $F_4 \subset F_q = F_{2^r}$, which is to say $r$ is even. Note that $r$ is even if and only if $q \equiv \pm 1 \pmod{5}$. Theorem 7.3 shows that there is at most one conjugacy class of isocahedral subgroups when $p \neq 2, 3, 5$. Theorem B(1,5) yield the same conclusion for $p = 3, 5$. When $p = 2$, we note that $\operatorname{PGL}_2(F_4) \cong \mathfrak{A}_5$ (Theorem 7.1(4)); Theorem B(1) shows that the conjugacy class of isocahedral subgroups is unique in this case.

Next, let us look at the subgroups isomorphic to $\operatorname{PSL}_2(F_{p^r})$ and $\operatorname{PGL}_2(F_{p^r})$. Evidently, such subgroups exist if $s \mid r$, since then $F_{p^r} \subset F_q$. Theorem A(1) shows this is a sufficient condition as well, and Theorem B(1) shows that there is a unique conjugacy class of such subgroups.

Finally, we treat the $p$-semi-elementary subgroups of $\operatorname{PGL}_2(F_q)$. Every such subgroup has a unique fixed point, which must be $F_q$-rational since this field is perfect. Let $G$ be such a subgroup, and suppose that its order is $p^mn$ with $n$ coprime to $p$. Theorem B(2) shows that $G$ is conjugate to $(\mu_{p^n}(F_q) \Gamma)$ for some rank-$m$ subgroup $\Gamma \subset F_q$ that is stable under multiplication by elements of $\mu_n(F_q)$. In particular, note that $m \leq r$. Let $e$ be the order of $p$ in $(\mathbb{Z}/n\mathbb{Z})^\times$. Then $n \mid (p^e - 1)$, which implies $F_{p^e} \subset F_q$. That is, $e \mid r$. Since $\Gamma$ is stable under the multiplicative action of $F_{p^r}$, it follows that it is an $F_{p^e}$-vector space. Thus, $e \mid m$. Conversely, let us suppose that $e$ is the order of $p$ in $(\mathbb{Z}/n\mathbb{Z})^\times$, that $e \mid \gcd(r, m)$, and that $m \leq r$. Then $F_q$ contains a primitive $n$-th root of unity, and $(\mu_{p^n}(F_q) F_{p^m})$ is a $p$-semi-elementary subgroup of the desired order. Theorem B(2) shows that the conjugacy classes of such subgroups are given by homothety classes $F_{p^e}$-vector subspaces of $F_q$.

\[ \square \]

References

[1] Arnaud Beauville. Finite subgroups of $\operatorname{PGL}_2(K)$. In Vector bundles and complex geometry, volume 522 of Contemp. Math., pages 23–29. Amer. Math. Soc., Providence, RI, 2010.

[2] H. S. M. Coxeter. Regular polytopes. Dover Publications Inc., New York, third edition, 1973.

[3] Leonard Eugene Dickson. Linear groups: With an exposition of the Galois field theory. With an introduction by W. Magnus. Dover Publications Inc., New York, 1958.

[4] Xander Faber, Michelle Manes, and Bianca Viray. Computing conjugating sets and automorphism groups of rational functions. J. Algebra, 423:1161–1190, 2015.

[5] Évariste Galois. Œuvres mathématiques. Éditions Jacques Gabay, Sceaux, 1989. Publiées en 1846 dans le Journal de Liouville, suivies d’une étude par Sophus Lie, “Influence de Galois sur le développement des mathématiques” (1895). [Published in 1846 in the Journal de Liouville, followed by a study by Sophus Lie, “Influence de Galois sur le développement des mathématiques” (1895)], With a foreword by J. Liouville.

[6] J. Gierster. Die Untergruppen der Galois’schen Gruppe der Modulargleichungen für den Fall eines primzahlalen Transformationsgrades. Math. Ann., 18(2):319–365, 1881.

[7] Felix Klein. Lectures on the icosahedron and the solution of equations of the fifth degree. Dover Publications Inc., New York, N.Y., revised edition, 1956. Translated into English by George Gavin Morrice.

[8] E. Hastings Moore. A doubly-infinite system of simple groups. Bull. Amer. Math. Soc., 3(3):73–78, 1893.

[9] Jean-Pierre Serre. Corps locaux. Hermann, Paris, 1968. Deuxième édition, Publications de l’Université de Nancago, No. VIII.
[10] Jean-Pierre Serre. Propriétés galoisiennes des points d’ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.

[11] Michio Suzuki. *Group theory. I*, volume 247 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1982. Translated from the Japanese by the author.

IDA CENTER FOR COMPUTING SCIENCES, BOWIE, MD

*Email address: aufaber@super.org*