Iwasawa's Criterion and Simplicity of $\mathrm{PSL}_n(F)$

Ryan Catullo

1 Introduction

The special linear group $\mathrm{SL}_n(F)$ where F is a field is the group of $n \times n$ matrices with entries in F that have determinant 1. We define the *projective special linear group* $\mathrm{PSL}_n(F)$ to be the quotient of the special linear group with its center, that is $\mathrm{SL}_n(F)/Z(\mathrm{SL}_n(F))$. It turns out that, as Galois claimed without proof in 1831, $\mathrm{PSL}_n(F_p)$ is simple for all $n \geq 2$ and primes p, except $n = 2$ and $p = 2$ or 3, in which case $\mathrm{PSL}_2(F_2) \cong S_3$ and $\mathrm{PSL}_2(F_3) \cong A_4$, both of which are solvable. In this paper, we will prove the simplicity of $\mathrm{PSL}_2(F)$ for fields F with $|F| > 3$ (not necessarily of prime order). In fact, this holds in general: $\mathrm{PSL}_n(F)$ is simple for $n \geq 2$ unless $n = 2$ and $F = F_2$ or F_3.

2 Commutator Subgroups

Let G be a group. We define the *commutator* of $g, h \in G$ to be $g^{-1}h^{-1}gh$, and denote it $[g, h]$. The commutator arises as a natural way to determine how far from being abelian a group G is. For example, if G is abelian then $g^{-1}h^{-1}gh = e$ so the only commutator in G is e. We then define the *commutator subgroup* of G to be the subgroup generated by all the commutators of G, and we denote it $[G, G]$. In fact, this subgroup is normal in G.

Proposition $[G, G]$ is a normal subgroup of G.

Proof: Let $[g, h] = g^{-1}h^{-1}gh \in [G, G]$, and let $k \in G$. Then $k[g, h]k^{-1} = kg^{-1}h^{-1}ghk^{-1}$. We can add kk^{-1} and $k^{-1}k$ between terms to get $(kg^{-1}k^{-1})(kh^{-1}k^{-1})(kgk^{-1})(khk^{-1}) = (kgk^{-1})^{-1}(khk^{-1})^{-1}(kgk^{-1})(khk^{-1})$. Note that this is $[kgk^{-1}, khk^{-1}] \in [G, G]$, and therefore $[G, G]$ is normal in G. □

We can then use $G/[G, G]$ as a measure of how "abelian" a group G is. If G is abelian, then $[G, G] = \{e\}$ as noted above, so $G/\{e\} \cong G$ is abelian. We note that the converse is also true: if the commutator of any $g, h \in G$ is the identity, then G is abelian. This is immediate since if $[g, h] = e$ then $g^{-1}h^{-1}gh = e$, which implies $gh = hg$ for all $g, h \in G$. We also have the nice property that $G/[G, G]$ is always abelian.

Proposition $G/[G, G]$ is abelian.

Proof: Let $g[G, G], h[G, G] \in G/[G, G]$ be elements of this group. Then $(g[G, G])^{-1}(h[G, G])^{-1}(g[G, G])(h[G, G]) = (g^{-1}h^{-1}gh)[G, G] = [G, G]$ since $g^{-1}h^{-1}gh = [g, h] \in [G, G]$. Thus, the commutator of any $g[G, G], h[G, G] \in G/[G, G]$ is $[G, G] = e_{G/[G,G]}$. By the above note, $G/[G, G]$ is abelian. □

We can now formalize how $G/[G, G]$ is a measure of how "abelian" a group is.

Theorem Let N be a normal subgroup of G. Then G/N is abelian if and only if $[G, G] \leq N$.

Proof: Assume G/N is abelian, that is for $gN, hN \in G/N$ we have $(gN)(hN) = (hN)(gN)$ or $(gh)N = (hg)N$. Then $(g^{-1}h^{-1}gh)N = N$, which implies $g^{-1}h^{-1}gh = [g, h] \in N$ for all $g, h \in G$. Thus, $[G, G] \leq N$. For the converse, assume $[G, G] \leq N$. Then for all $g, h \in G$, we have $(g^{-1}h^{-1}gh) \in N$, which implies $(g^{-1}h^{-1}gh)N = N$. Then $(gh)N = (hg)N$, which implies $(gN)(hN) = (hN)(gN)$ or that G/N is abelian. □

Intuitively, $[G, G]$ creates the smallest abelian quotient group G/N by modding out non-abelian elements. If $[G, G] = G$, then $G/G \cong \{e\}$ is the "smallest" abelian quotient group. That is, if N is normal in G then G/N is non-abelian unless $N = G$. If $[G, G] = G$, we say G is *perfect*. Intuitively speaking, perfect groups are "anti-abelian".

3 Doubly-Transitive Actions

Recall that we call a group action of G on a set X transitive if for every $x \in X$, there is some $g \in G$ such that $g \cdot x = x$. We call a group action *doubly-transitive* if for every two ordered pairs $(x_1, x_2), (y_1, y_2) \in X \times X$ with $x_1 \neq x_2$ and $y_1 \neq y_2$, there is some $g \in G$ such that $g \cdot x_1 = y_1$ and $g \cdot x_2 = y_2$. That is, doubly-transitive actions have group elements that take any distinct pair of points in $X \times X$ to any other distinct pair of points in $X \times X$. As an example, consider the action of A_4 on $\{1, 2, 3, 4\}$. Pick $a, b \in \{1, 2, 3, 4\}$ with $a \neq b$ and $c, d \in \{1, 2, 3, 4\}$ with $c \neq d$. If $a = c$ and $b = d$, then the identity permutation $e \in A_4$ sends $e \cdot a = a = c$ and $e \cdot b = b = d$. If without loss of generality $a = c$ and $b \neq d$, then let $\sigma = (b\ d)(d\ e)$ where e is whatever element is left in $\{1, 2, 3, 4\}$ that is not a, b, or d. Then $\sigma \in A_4$ since it is the product of two odd permutations, and $\sigma \cdot a = a = c$ and $\sigma \cdot b = d$. If $a \neq c$ and $b \neq d$, then let $\sigma = (a\ c)(b\ d)$ such that $\sigma \in A_4$ and $\sigma \cdot a = c$ and $\sigma \cdot b = d$. Thus, the action of A_4 on $\{1, 2, 3, 4\}$ is doubly-transitive. We also have the following theorem on doubly-transitive actions.

Theorem Let G act doubly-transitively on a set X, and let $x \in X$. Then $\mathrm{Stab}_G(x)$ is a maximal subgroup of G.

Proof: Recall that a maximal subgroup of G is a proper subgroup such that no other proper subgroup of G contains it. Let $H_x = \mathrm{Stab}_G(x)$. We will first show that for each $g \notin H_x$, we must have $G = H_x \cup H_x g H_x$. Let $g' \in G$ such that $g' \notin H_x$. We will show $g' \in H_x g H_x$. Since $g, g' \notin H_x = \mathrm{Stab}_G(x)$, we have $g \cdot x$ and $g' \cdot x$ are not x. Therefore, $g^{-1} \cdot x$ and $g'^{-1} \cdot x$ are not x, so by double-transitivity with $(x, g^{-1} \cdot x)$ and $(x, g'^{-1} \cdot x)$ there exists some $h \in G$ such that $h \cdot x = x$ and $h \cdot (g^{-1} \cdot x) = g'^{-1} \cdot x$. Since $h \cdot x = x$, we have $h \in H_x$. Thus, since $(hg^{-1}) \cdot x = g'^{-1} \cdot x$, we also have that $(g'hg^{-1}) \cdot x = x$, or $g'hg^{-1} \in H_x$. Therefore, $g' \in H_x gh \subset H_x g H_x$, so $G = H_x \cup H_x g H_x$ and we are done.

Now we know that $H_x \neq G$ since $|X| \geq 2$ implies there exists $y \in X$ with $x \neq y$ such that $g \cdot x = y \implies g \notin H_x$. Let $H_x \subsetneq K \subset G$, and choose $g \in K - H_x$. Then $g \notin H_x$, so $G = H_x \cup H_x g H_x$. Since $H_x \subset K$ and $g \in K$, by closure we have $H_x g H_x \subset K$, so $H_x \cup H_x g H_x = G \subset K$. Therefore, $K = G$ or H_x is maximal. □

Theorem Suppose G acts on a set X doubly-transitively. Then any normal subgroup $N \triangleleft G$ acts on X either trivially or transitively.

Proof: Suppose N does not act on X trivially. Then for $x \in X$, there is some $n \in N$ such that $n \cdot x \neq x$. Now let $y, y' \in X$ with $y \neq y'$. Then by double-transitivity, there is some $g \in G$ such that $g \cdot x = y$ and $g \cdot (n \cdot x) = y'$. Using the first equation, $x = g^{-1} \cdot y$, so $g \cdot (n \cdot x) = g \cdot (n \cdot (g^{-1} \cdot y)) = (gng^{-1}) \cdot y = y'$. Since $N \triangleleft G$, $gng^{-1} \in N$ so for any $y, y' \in X$ we have that there is some $n \in N$ such that $n \cdot y = y'$. Thus, N acts transitively on X. □

We now have the necessary tools to discuss simplicity of groups in an abstract sense, without explicitly having to look at group orders and use Sylow Theorems and various tricks to deduce simplicity. Namely, we prove a powerful criterion for simplicity due to Iwasawa.

4 Iwasawa's Criterion

This is the main result used in the proof of the simplicity of $\mathrm{PSL}_2(F)$.

Theorem (Iwasawa) Let G act doubly-transitively on a set X, and let K be the kernel of this group action. Assume the following two conditions:

1. For some $x \in X$, $\mathrm{Stab}_G(x)$ has an abelian normal subgroup whose conjugates generate G.
2. $[G, G] = G$

Then G/K is simple.

Proof: Recall that the kernel K of G acting on X is the set of $g \in G$ such that $g \cdot x = x$ for all $x \in X$, i.e. the set of g that act trivially on X. To show G/K is simple, by the fourth isomorphism theorem it suffices to show that the only normal subgroup of G containing K is G. Suppose $K \subset N \subset G$ with $N \triangleleft G$, and let $x \in X$ be the element such that $\mathrm{Stab}_G(x)$ has an abelian normal subgroup whose conjugates generate G. Let $H = \mathrm{Stab}_G(x)$ such that H is a maximal subgroup of G. Since N is normal, NH is a subgroup of G by the second isomorphism theorem. Since $H \subset NH$ and H is maximal, either $NH = H$ or $NH = G$.

If $NH = H$, then $N \subset H$ so N fixes x. Since $N \triangleleft G$, it acts trivially or transitively. But N fixes x, so N acts trivially on X. Therefore, $N \subset K$, and since $K \subset N$ by hypothesis this implies $N = K$.

Suppose instead that $NH = G$, and let U be the abelian normal subgroup of H whose conjugates generate G. Since $U \triangleleft H$, we have $NU \triangleleft NH = G$. Then for every $g \in G$, $gUg^{-1} \subset g(NU)g^{-1} = NU$ since $NU \triangleleft G$ as we just showed. Thus, since the conjugates of U generate G and NU contains all conjugates of U, $NU = G$. Then by the second isomorphism theorem, $G/N = (NU)/N \cong U/N \cap U$. Since U is abelian, $U/N \cap U$ is abelian. By the isomorphism, this implies G/N is abelian, so $[G, G] \leq N$. By our second assumption, $[G, G] = G$, so $N = G$. Therefore, any normal subgroup containing K is either K or G, so by the fourth isomorphism theorem the only normal subgroups of G/K are $K/K = \{e_{G/K}\}$ and G/K. By definition, G/K is simple. □

As an example application, we can use this theorem to demonstrate the simplicity of A_5. Consider the action of A_5 on $\{1, 2, 3, 4, 5\}$. Using the same construction as for A_4 acting on $\{1, 2, 3, 4\}$, this action is doubly-transitive. Note that the kernel of this action is the set of $\sigma \in A_5$ such that $\sigma(n) = n$ for $n = 1, \ldots, 5$. By definition, $\sigma = e$, so the kernel of this action $K = \{e\}$ is trivial. Let $x = 5$ such that $\mathrm{Stab}_{A_5}(x) \cong A_4$, which has the abelian normal subgroup

$$U = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

U abelian is immediate from the fact that $|U| = 4$. Also note that U is a Sylow 2-subgroup of A_4, so since $n_4 \mid 3$ and $n_4 \equiv 1 \pmod 4$, $n_4 = 1$ so $U \lhd A_4$. To see that the conjugates of U generate A_5, note that the conjugates of U are exactly $[(1\ 2)(3\ 4)]$ in A_5, that is all $(2, 2)$-cycles of the form $(1\ 2)(3\ 4)$. Then $(1\ 2)(3\ 4)(2\ 3)(4\ 5) = (1\ 2\ 4\ 5\ 3)$ is a 5-cycle in the group generated by the g-conjugates of U, and $(1\ 2)(3\ 4)(1\ 2)(4\ 5) = (3\ 4\ 5)$ is a 3-cycle in this group. Thus, the order of the group is at least $\mathrm{lcm}(2, 3, 5) = 2 * 3 * 5 = 30$. Since U is in this group, 4 divides its order. Thus, the order of the group generated by the g-conjugates of U has order 60, and therefore the g-conjugates of U generate A_5.

Further, let $(a\ b)(c\ d)$ be a $(2, 2)$-cycle in A_5 with $a \neq b \neq c \neq d$. Then

$$(a\ b)(c\ d) = (a\ b\ c)(a\ b\ d)(a\ c\ b)(a\ d\ b) = (a\ b\ c)(a\ b\ d)(a\ b\ c)^{-1}(a\ b\ d)^{-1} \in [A_5, A_5]$$

Thus, every $(2, 2)$-cycle is in $[A_5, A_5]$, and since these $(2, 2)$-cycles generate A_5 as we have just shown, this implies $[A_5, A_5] = A_5$. By Iwasawa's Criterion, $A_5/\{e\} \cong A_5$ is simple.

5 The Simplicity of $\mathrm{PSL}_2(F)$

Consider F^2 as a vector space over F. Recall that a *linear subspace* of F^2 is a subspace of F^2 as a vector space. Since F^2 has dimension 2, a linear subspace has dimension 0, 1, or 2. If it has dimension 2, then the linear subspace is the whole space F^2. If it has dimension zero then it is just the zero vector $(0, 0)$. Otherwise, if it has dimension one, then it has a basis $\{v\}$ where $v \in F^2$. Then the subspace is $\{sv \mid s \in F\}$, which we will denote Fv; intuitively, Fv is all scalar multiples of v.

Further recall that all linear transformations of a finite dimensional vector space arise as matrices, so linear transformations of F^2 are 2×2 matrices over F. In a specific case, we will consider the action of $\mathrm{SL}_2(F)$ on 1-dimensional linear subspaces of F^2 by linear transformation. From now on, we will just call these linear subspaces, assuming the fact that they are 1-dimensional. Then if $A \in \mathrm{SL}_2(F)$ and Fv is a linear subspace, $A \cdot Fv = F(Av)$ (this just takes the basis $\{v\}$ for the linear subspace Fv to $\{Av\}$, and $F(Av)$ is the linear subspace spanned by this basis).

Theorem The action of $\mathrm{SL}_2(F)$ on the linear subspaces of F^2 is doubly-transitive.

Proof: We will show that for any $v, w \in F^2$ with $v \neq w$, there is an $A \in \mathrm{SL}_2(F)$ such that $A \cdot F\binom{1}{0} = Fv$ and $A \cdot F\binom{0}{1} = Fw$. This suffices since if $v', w' \in F^2$ with $v' \neq w'$, then there is some $B \in \mathrm{SL}_2(F)$ such that $B \cdot F\binom{1}{0} = Fv'$ and $B \cdot F\binom{0}{1} = Fw'$. This implies $B^{-1} \cdot Fv' = F\binom{1}{0}$ and $B^{-1} \cdot Fw' = F\binom{0}{1}$, so $(AB^{-1}) \cdot Fv' = Fv$ and $(AB^{-1}) \cdot Fw' = Fw$. Let $v = \binom{v_1}{v_2}$ and $w = \binom{w_1}{w_2}$. Since $Fv \neq Fw$, v and w are linearly independent. Thus, $D = v_1w_2 - v_2w_1$ is nonzero, since if it was 0 then $v_1w_2 - v_2w_1 = v_1w_2 + v_1w_1 - v_1w_1 - v_2w_1 = v_1(w_1 + w_2) - w_1(v_1 + v_2) = 0$ implies $w_1 + w_2 = 0$ and $v_1 + v_2 = 0$ or $F\binom{w_1}{w_2} = F\binom{w_1}{-w_1} = F\binom{v_1}{-v_1} = F\binom{v_1}{v_2}$, a contradiction. Let

$$A = \begin{pmatrix} v_1 & w_1/D \\ v_2 & w_2/D \end{pmatrix}$$

Such that $\det(A) = (v_1w_2 - v_2w_1)/D = D/D = 1$ and $A \in \mathrm{SL}_2(F)$. Then $A\binom{1}{0} = \binom{v_1}{v_2} = v$ and $A\binom{0}{1} = \binom{w_1/D}{w_2/D} = (1/D)w$. Thus, $A \cdot F\binom{1}{0} = Fv$ and $A \cdot F\binom{0}{1} = F(1/D)w = Fw$. This concludes the proof that this action is doubly transitive. □

Theorem The kernel of this action is $Z(\mathrm{SL}_2(F))$.

Proof: Let

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(F)$$

be in the kernel of this action. Then $A \cdot F\binom{1}{0} = F\binom{1}{0}$, so $A\binom{1}{0} = \binom{a}{c} = \binom{\lambda}{0}$ for $\lambda \in F$. Thus, $c = 0$. Similarly, $A \cdot F\binom{0}{1} = F\binom{0}{1}$, so $A\binom{0}{1} = \binom{b}{d} = \binom{0}{\lambda}$ for $\lambda \in F$, implying $b = 0$. Thus,

$$A = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$$

Since $\det(A) = ad = 1$, we have $d = 1/a$. Moreover, since $A \cdot F\binom{1}{1} = F\binom{1}{1}$, we have $A\binom{1}{1} = \binom{a}{1/a} = \binom{\lambda}{\lambda}$ so $a = 1/a = \lambda \implies a^2 = 1 \implies a = \pm 1$. Thus, the kernel is the matrices $\pm\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ which both fix all linear subspaces.
We will check that this is in fact the center of $\mathrm{SL}_2(F)$. Let $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in Z(\mathrm{SL}_2(F))$. Then $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ implies that $\left(\begin{smallmatrix} a+c & b+d \\ c & d \end{smallmatrix}\right) = \left(\begin{smallmatrix} a & a+b \\ c & c+d \end{smallmatrix}\right)$. Since $a+c = a$, $c = 0$, and since $a+b = b+d$ we have $a = d$. We also have that $\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$ implies $\left(\begin{smallmatrix} a & b \\ a+c & b+d \end{smallmatrix}\right) = \left(\begin{smallmatrix} a+b & b \\ c+d & d \end{smallmatrix}\right)$, so $a = a+b$ implies $b = 0$ as well. Thus, $A = \left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)$, and since $A \in \mathrm{SL}_2(F)$ we have $a^2 = 1$ or $a = \pm 1$. Therefore, $Z(\mathrm{SL}_2(F)) = \pm\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, and the kernel of this action is the center of $\mathrm{SL}_2(F)$. □
Let $x = F\binom{1}{0}$ and consider $\mathrm{Stab}_{\mathrm{SL}_2(F)}(F\binom{1}{0})$. Then $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{Stab}_{\mathrm{SL}_2(F)}(F\binom{1}{0})$ if $A\binom{1}{0} = \binom{\lambda}{0}$ for $\lambda \in F$. This implies $c = 0$, and $\det(A) = ad - bc = 1$ implies then that $d = 1/a$. Thus,

$$\mathrm{Stab}_{\mathrm{SL}_2(F)}\left(F\begin{pmatrix} 1 \\ 0 \end{pmatrix}\right) = \left\{ \begin{pmatrix} a & b \\ 0 & 1/a \end{pmatrix} \in \mathrm{SL}_2(F) \right\}$$

Consider the subgroup

$$U = \left\{ \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \;\middle|\; \lambda \in F \right\}$$

This subgroup is normal in $\mathrm{Stab}_{\mathrm{SL}_2(F)}(F\binom{1}{0})$ since $\left(\begin{smallmatrix} a & b \\ 0 & 1/a \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & \lambda \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1/a & -b \\ 0 & a \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & \lambda a^2 \\ 0 & 1 \end{smallmatrix}\right) \in U$ and is abelian since $\left(\begin{smallmatrix} 1 & \lambda \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & \mu \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & \lambda+\mu \\ 0 & 1 \end{smallmatrix}\right)$
Theorem The conjugates of U generate $\mathrm{SL}_2(F)$.
Proof: Consider $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \in \mathrm{SL}_2(F)$ and $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & \lambda \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 0 \\ -\lambda & 1 \end{smallmatrix}\right)$, so lower triangular matrices are in the group generated by conjugates of U. Consider the matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(F)$. If $b \neq 0$, then

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ (d-1)/b & 1 \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ (a-1)/b & 1 \end{pmatrix}$$

If $c \neq 0$ then

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & (a-1)/c \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix} \begin{pmatrix} 1 & (d-1)/c \\ 0 & 1 \end{pmatrix}$$

If $b = c = 0$ then this matrix is $\left(\begin{smallmatrix} a & 0 \\ 0 & 1/a \end{smallmatrix}\right)$, and

$$\begin{pmatrix} a & 0 \\ 0 & 1/a \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ (1-a)/a & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ a-1 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1/a \\ 0 & 1 \end{pmatrix}$$

So all matrices in $\mathrm{SL}_2(F)$ are in the group generated by conjugates of U. □
Theorem If $|F| \geq 4$ then $[\mathrm{SL}_2(F), \mathrm{SL}_2(F)] = \mathrm{SL}_2(F)$.
Proof: Consider the following commutator in $[\mathrm{SL}_2(F), \mathrm{SL}_2(F)]$.

$$\begin{pmatrix} a & 0 \\ 0 & 1/a \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & 1/a \end{pmatrix}^{-1} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} a & 0 \\ 0 & 1/a \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1/a & 0 \\ 0 & a \end{pmatrix} \begin{pmatrix} 1 & -b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b(a^2-1) \\ 0 & 1 \end{pmatrix}$$

Since $|F| \geq 4$, there is an $a \neq 0, 1, -1$ such that $\left(\begin{smallmatrix} a & 0 \\ 0 & 1/a \end{smallmatrix}\right)$ exists and $a^2 - 1 \neq 0$. Note that this is true because $a = \pm 1$ are the only solutions to $a^2 - 1 = 0$ in a field, as $a^2 - 1 = (a-1)(a+1) = 0$ and since every nonzero element is a unit, F has no zero divisors, which implies either $a - 1 = 0$ or $a + 1 = 0$. Letting b run over F, we have that $U \in [\mathrm{SL}_2(F), \mathrm{SL}_2(F)]$. Since $[\mathrm{SL}_2(F), \mathrm{SL}_2(F)]$ is normal in $\mathrm{SL}_2(F)$, all the conjugates of U are in $[\mathrm{SL}_2(F), \mathrm{SL}_2(F)]$. But these conjugates generate the whole group, so $[\mathrm{SL}_2(F), \mathrm{SL}_2(F)] = \mathrm{SL}_2(F)$. □
Theorem For $|F| \geq 4$, the group $\mathrm{PSL}_2(F)$ is simple.
Proof: We have that $\mathrm{SL}_2(F)$ acts doubly-transitively on the set of linear subspaces of F^2. The kernel of this action is $Z(\mathrm{SL}_2(F))$. Further, there is a linear subspace Fv such that $\mathrm{Stab}_{\mathrm{SL}_2(F)}(Fv)$ contains an abelian normal subgroup whose conjugates generate $\mathrm{SL}_2(F)$, and $[\mathrm{SL}_2(F), \mathrm{SL}_2(F)] = \mathrm{SL}_2(F)$. By Iwasawa's Criterion, $\mathrm{SL}_2(F)/Z(\mathrm{SL}_2(F)) = \mathrm{PSL}_2(F)$ is simple. □