Math 155: Designs and groups
Handout #3:

Simplicity of $\text{PSL}_2(F)$ ($|F| \geq 4$) and $\text{PSL}_n(F)$ ($n \geq 3$) — Outline

0. Let $F$ be a finite field of $q$ elements. $\text{PSL}_n(F)$ is a normal subgroup [indeed the commutator subgroup, but we won’t need this] of $\text{PGL}_n(F)$ with index $\gcd(n, q - 1)$, and is generated by “transvections” because $\text{SL}_n(F)$ is; indeed even coordinate transvections suffice. (A coordinate transvection is a matrix with 1’s on the diagonal and a single nonzero off-diagonal entry. A linear transformation $T: F^n \rightarrow F^n$ that is of that form for some choice of basis is a transvection; an equivalent coordinate-free criterion is: $T - I$ has rank 1 and square zero.) When $n = 2$ the transvections in $\text{PSL}_2(F)$ are precisely the fractional linear transformations of $\mathbb{P}^1(F)$ with exactly one fixed point; if that point is $\infty$, the transformation is $x \mapsto x + c$ for some $c \in F^*$. 

1. Let $G = \text{PSL}_2(F)$ and assume $H$ is a normal subgroup of $G$. If $H$ contains a transvection then it contains all of them, and thus coincides with $G$. (The $G$-conjugates of $x \mapsto x + c$ include $x \mapsto x + c'$ where $c'/c$ is a square in $F$, and these $c'$ additively generate $F$. This works even if $F$ is infinite as long as it is not of characteristic 2, or of characteristic 2 and perfect.)

2. Assume then that $H$ contains no transvections. Let $G_1 \subset G$ be the stabilizer of $\infty$, which is the group of affine linear transformations $x \mapsto ax + b$ with $a \in F^{*2}$. Then $H_1 := H \cap G_1$ is normal in $G_1$. Since the commutator of $x \mapsto ax + b$ with $x \mapsto x + 1$ is a transvection unless $a = 1$, it follows that $H_1 = \{\text{id}\}$.

3. Now assume $H \neq \{\text{id}\}$ and let $h \in H$ be any non-identity element. Let $u = h(\infty)$, and note that $u \neq \infty$ because $h \neq H_1$. Translating the coordinate on $\mathbb{P}^1(F)$ by $u$ (or equivalently replacing $h$ by its conjugate by the transvection $x \mapsto x + u$, a conjugate also contained in $H - \{\text{id}\}$), we may assume $u = 0$. For $a \in F^*$ let $g_a \in G$ be the transformation $x \mapsto ax + b$. Then the commutator $g_a^{-1}h^{-1}g_ah \in H$ fixes $\infty$, so by the previous paragraph must be the identity element. Thus each $g_a$ commutes with $h$. Thus if $h$ is $x \mapsto 1/(cx + d)$ then $a^2/(cx + d) = 1/(ca^2x + d)$ for all $a \in F^*$. But then $a^4 = 1$, whence $q \leq 3$ or $q = 5$, and we already know that $\text{PSL}_2(F_5)$ is isomorphic to the simple group $A_5$, QED.

[NB $G$ does have a nontrivial normal subgroup for $q = 2, 3$.]
The case \( n \geq 3 \) is similar to \( \text{PSL}_2(F) \), but actually easier:

- All transvections are conjugate in \( \text{SL}_n \), not only in \( \text{GL}_n \), because any transvection \( t \) commutes with linear transformations \( g \) of arbitrary determinant. (It suffices to prove this for coordinate transvections, for which \( g \) can be taken to be a diagonal matrix.)

- A normal subgroup \( H \neq \{ \text{id} \} \) of \( \text{PSL}_n(F) \) necessarily contains a non-identity element \( h \) with a stable hyperplane. Indeed for any transvection \( t \) and any \( g \in \text{PSL}_n(F) \) the commutator \( h = gtg^{-1}t^{-1} \) is the product of two transvections \( gtg^{-1} \) and \( t^{-1} \) and so has a fixed subspace of dimension at least \( n - 2 > 0 \). (This is enough because a transvection of \( V \) is also a transvection of the dual space \( V^* \), and a nonzero fixed vector in \( V^* \) yields a stable hyperplane in \( V \).) If \( g \in H \) then \( h \in H \) too, and if \( g \neq \text{id} \) then \( h \neq \text{id} \) for some choice of \( t \), else all transvections \( t \) commute with \( g \) and thus (since these generate \( \text{PSL}_n(F) \)) \( g \) is in the center of \( \text{PSL}_n(F) \) — but that center is trivial.

- The complement of a hyperplane in \( \mathbb{P}^{n-1}(F) \) is an affine \((n-1)\)-space over \( F \); so \( h \) is an affine linear transformation \( v \mapsto Av + b \) for some \( A \in \text{GL}_{n-1}(F) \) and \( b \in F^{n-1} \). The translations \( v \mapsto v + c \) of this affine space correspond to transvections in \( \text{PSL}_n(F) \). If \( A = I \) then \( b \neq 0 \) (since \( h \neq \text{id} \)) and so \( h \) is a transvection. Else let \( c \in F^{n-1} \) be a vector not fixed by \( A \); then the commutator of \( h \) with the \( v \mapsto v + c \) is a nonzero translation and thus yields the desired transvection in \( H \).