TRANSITIVE GROUP ACTIONS

KEITH CONRAD

1. Introduction

Every action of a group on a set decomposes the set into orbits. The group acts on each of the orbits and an orbit does not have sub-orbits (unequal orbits are disjoint), so the decomposition of a set into orbits could be considered as a "factorization" of the set into "irreducible" pieces for the group action. Our focus here is on these irreducible parts, namely group actions with a single orbit.

Definition 1.1. A action of a group on a set is called *transitive* when the set is nonempty and there is exactly one orbit.

Example 1.2. For $n \geq 1$, the usual action of S_n on $\{1, 2, \ldots, n\}$ is transitive since there is a permutation sending 1 to any number.

Example 1.3. For $n \geq 3$, the usual action of A_n on $\{1, 2, \ldots, n\}$ is transitive since the 3-cycles $(12n), (13n), \ldots, (1\ n-1\ n), (1n2)$ send 1 to every other number. Notice A_2 does not act transitively on $\{1, 2\}$, since A_2 is trivial.

Example 1.4. For $n \geq 3$, the usual action of D_n on the vertices of a regular n-gon is transitive since any vertex of the n-gon can be carried to all the other vertices by rotations in D_n.

In Section 2 we give some further examples (and non-examples) of transitive actions. Section 3 gives a few general properties of transitive actions. Doubly transitive actions are the subject of Section 4 and they are applied in Section 5 to prove simplicity of most of the groups $\mathrm{PSL}_2(F)$. Highly transitive actions are used in Section 6 to prove most alternating groups are simple. In Section 7 we look at equivalence relations preserved by a group action, which leads to a concept lying between transitivity and double transitivity, called primitivity. For further reading, see [1] and [3].

2. More examples

Example 2.1. Let the group $\mathbf{R}^n$ act on itself by translations: for $\mathbf{v} \in \mathbf{R}^n$, $T_{\mathbf{v}} \colon \mathbf{R}^n \to \mathbf{R}^n$ by $T_{\mathbf{v}}(\mathbf{w}) = \mathbf{w} + \mathbf{v}$. Since $\mathbf{v} = T_{\mathbf{v}}(\mathbf{0})$, every vector is in the orbit of $\mathbf{0}$, so this action is transitive. Concretely, this just means you can move to any point in $\mathbf{R}^n$ from $\mathbf{0}$ by a suitable translation.

Example 2.2. The usual action of $\mathrm{GL}_2(\mathbf{R})$ on $\mathbf{R}^2$ is not transitive, since $\mathbf{0}$ is in its own orbit. However, the action of $\mathrm{GL}_2(\mathbf{R})$ on $\mathbf{R}^2 - \{\mathbf{0}\}$ is transitive. To see why, pick a non-zero vector $\mathbf{v} = \binom{a}{b}$. We will find an $A \in \mathrm{GL}_2(\mathbf{R})$ such that $A\binom{1}{0} = \mathbf{v}$, which means every $\mathbf{v} \neq \mathbf{0}$ is in the $\mathrm{GL}_2(\mathbf{R})$-orbit of $\binom{1}{0}$. If $a \neq 0$, let $A = \left(\begin{smallmatrix} a & 0 \\ b & 1 \end{smallmatrix}\right)$. If $b \neq 0$, let $A = \left(\begin{smallmatrix} a & 1 \\ b & 0 \end{smallmatrix}\right)$. These matrices are invertible in each case, and they send $\binom{1}{0}$ to $\binom{a}{b} = \mathbf{v}$.

Example 2.3. The action of $\mathrm{SL}_2(\mathbf{R})$ on $\mathbf{R}^2 - \{\mathbf{0}\}$ is also transitive. Indeed, in the previous example replace the choice of $\left(\begin{smallmatrix} a & 0 \\ b & 1 \end{smallmatrix}\right)$ with $\left(\begin{smallmatrix} a & 0 \\ b & 1/a \end{smallmatrix}\right)$ when $a \neq 0$ and $\left(\begin{smallmatrix} a & 1 \\ b & 0 \end{smallmatrix}\right)$ with $\left(\begin{smallmatrix} a & -1/b \\ b & 0 \end{smallmatrix}\right)$ when $b \neq 0$. We've found a matrix with determinant 1 that sends $\binom{1}{0}$ to $\binom{a}{b}$ when $\binom{a}{b} \neq \mathbf{0}$.

Example 2.4. The action of the orthogonal group $\mathrm{O}_2(\mathbf{R})$ on $\mathbf{R}^2 - \{\mathbf{0}\}$ is not transitive. Its orbits are the circles centered at the origin. If we let $\mathrm{O}_2(\mathbf{R})$ act on a particular circle centered at the origin, such as the unit circle, then we get a transitive action of $\mathrm{O}_2(\mathbf{R})$ on that circle.

Now we turn to examples (and non-examples) of transitive actions using abstract groups.

Example 2.5. Let a group G act on itself by left multiplication. Since $g = g \cdot e$, every element is in the orbit of e, so there is one orbit. When $G = \mathbf{R}^n$, this is exactly Example 2.1.

Example 2.6. Let G be a group with a subgroup H. The action of G by left multiplication on the coset space G/H has one orbit, since $gH = g \cdot H$: the orbit of $H \in G/H$ is the whole coset space. Example 2.5 is the special case where H is the trivial subgroup.

Example 2.7. The action of G on itself by conjugation is not transitive if $|G| > 1$. Indeed, the orbits of the conjugation action are the conjugacy classes of G and $\{e\}$ is its own conjugacy class. What about the conjugation action of G on $G - \{e\}$? This is not transitive if G is finite and $|G| > 2$ since finite groups with at least three elements have at least three conjugacy classes. (There are infinite groups where the non-identity elements form a single conjugacy class.)

Example 2.8. The conjugation action of G on its subgroups of a fixed size may or may not be transitive. If the size is a maximal prime power dividing $|G|$ then the action is transitive (conjugacy of p-Sylow subgroups), but otherwise it need not be. For instance, there could be a normal subgroup of some size and other subgroups of the same size.

3. Properties of transitive actions

Our first theorem about transitive actions is an equivalence between the definition and another description.

Theorem 3.1. *For $X \neq \emptyset$, an action of G on X is transitive if and only if, given any x and y in X, there is some $g \in G$ such that $y = gx$.*

Proof. Suppose the action is transitive, so there is one orbit. Given any x in X, its orbit must fill up X, so every element of X has the form gx for some $g \in G$.

Conversely, suppose that given any x and y in X we can write $y = gx$ for some g. Fix $x \in X$. Since every $y \in X$ has the form gx for some g, every y is in the orbit of x. Thus X has only one orbit. □

Theorem 3.2. *If a finite group G acts transitively on X then $|X| \mid |G|$.*

Proof. Pick $x \in X$. Since the G-orbit of x is X, the set X is finite and the orbit-stabilizer formula tells us $|X| = [G : \mathrm{Stab}_x]$, so $|X| \mid |G|$. □

Example 3.3. Let p be prime. If G is a subgroup of S_p and its natural action on $\{1, 2, \ldots, p\}$ is transitive then $p \mid |G|$ by Theorem 3.2, so G contains an element of order p by Cauchy's theorem. The only elements of order p in S_p are p-cycles, so every subgroup of S_p whose natural action on $\{1, 2, \ldots, p\}$ is transitive contains a p-cycle.

Theorem 3.4. *Suppose G acts on two finite sets X and Y and there is a function $f\colon X \to Y$ that respects the G-actions: $f(gx) = gf(x)$ for all $g \in G$ and $x \in X$. If the action is transitive on Y then $|Y| \mid |X|$.*

Proof. The set X can be decomposed into disjoint subsets according to the f-values of the elements. That is,

$$X = \bigcup_{y \in Y} f^{-1}(y),$$

and the sets $f^{-1}(y)$ are disjoint. We will show $|f^{-1}(y)| = |f^{-1}(y')|$ for y and y' in Y, and therefore $|X|$ equals $|Y|$ times the common size of the inverse images.

For y and y' in Y, write $y' = g_0 y$. Then we get maps $f^{-1}(y) \mapsto f^{-1}(y')$ and $f^{-1}(y') \mapsto f^{-1}(y)$ by $x \mapsto g_0 x$ and $x' \mapsto g_0^{-1}x'$. These maps are inverses of each other, so $|f^{-1}(y)| = |f^{-1}(y')|$. □

As an exercise, show Theorem 3.2 is a special case of Theorem 3.4.

Here is a cute application of Theorem 3.4 to counting Sylow subgroups. For a group G, $n_p(G)$ denotes the size of $\mathrm{Syl}_p(G)$. If $H \subset G$ and $N \lhd G$, then $n_p(H) \leq n_p(G)$ and $n_p(G/N) \leq n_p(G)$. Might these inequalities really be divisibilities? Not always. There are several copies of A_4 in A_5, and $n_3(A_4) = 4$ while $n_3(A_5) = 10$. However, if we stick to normal subgroups only, then we do get a divisibility relation on the Sylow counts.

Corollary 3.5. *When G is a finite group and $N \lhd G$, $n_p(N) \mid n_p(G)$ and $n_p(G/N) \mid n_p(G)$.*

Proof. Let $X = \mathrm{Syl}_p(G)$ and $Y = \mathrm{Syl}_p(N)$. The group G acts on both X and Y by conjugation. By the Sylow theorems, the action of N on Y is transitive, so the action of G on Y is transitive. (Also the action of G on X is transitive, but we won't need this.) There is a natural map $f\colon X \to Y$ given by $f(P) = P \cap N$. (That $P \cap N$ is a p-Sylow subgroup of N is the first part of Theorem A.1.) Since $g(P \cap N)g^{-1} = gPg^{-1} \cap gNg^{-1} = gPg^{-1} \cap N$, f respects the conjugation action of G on X and Y. Now use Theorem 3.4 to see $|Y| \mid |X|$, so $n_p(N) \mid n_p(G)$.

To show $n_p(G/N) \mid n_p(G)$, use $X = \mathrm{Syl}_p(G)$ again but now let $Y = \mathrm{Syl}_p(G/N)$. Once again G acts on both X and Y by conjugation, and the action on Y (and on X) is transitive. Let $f\colon X \to Y$ by $f(P) = PN/N$ (that this is p-Sylow subgroup of G/N is the second part of Theorem A.1) and check f respects the action of G on the two sets. □

Our next theorem about transitive actions is fundamental. It says that Example 2.6 is actually the most general example: every transitive action can be viewed as a left multiplication action on cosets of a subgroup, even though it may not appear that way at first.

Theorem 3.6. *Any transitive action of a group G is equivalent to the action of G by left multiplication on a coset space G/H.*

Proof. Let G act transitively on X. We want to show this action is the same as the left multiplication action of G on some coset space G/H.

Pick $x_0 \in X$. Every element of X has the form gx_0 for some $g \in G$. Consider the map $G \to X$ by $g \mapsto gx_0$. This is onto by transitivity. Let $H = \mathrm{Stab}_{x_0}$. For g and g' in G,

$$gx_0 = g'x_0 \iff g^{-1}g' \in H \iff gH = g'H.$$

This shows there is a bijection $G/H \to X$ by $gH \mapsto gx_0$. (Concretely, since $(gh)x_0 = gx_0$ for any $h \in H$, it makes sense to associate the whole coset gH with the point gx_0.) This

bijection between G/H and X respects the G-actions on both sides. To see this, pick $x \in X$ and $g \in G$, and set $y = gx$. What coset in G/H corresponds to x? Writing $x = g_0x_0$, the coset corresponding to x is g_0H. Similarly, since $y = g(g_0x_0) = (gg_0)x_0$, the coset corresponding to y is $(gg_0)H = gg_0H$. Thus, when $x \leftrightarrow g_0H$, we see that $gx \leftrightarrow gg_0H$, so the G-actions on X and G/H correspond to each other by the bijection between them. □

To summarize the above proof, when G acts transitively on X fix an $x_0 \in X$ and let $H = \mathrm{Stab}_{x_0}$. Then G/H is in bijection with X by letting gH correspond to gx_0, and this bijection identifies left multiplication on G/H with the action of G on X.

Example 3.7. Let's look at a transitive action that does not appear to be a coset action at first, and understand why it really is. We consider the action of $\mathrm{GL}_2(\mathbf{R})$ on $\mathbf{R}^2 - \{\mathbf{0}\}$ by matrix-vector multiplication. We saw in Example 2.2 that the orbit of $\binom{1}{0}$ takes us through the whole space.

Following the idea in the proof of Theorem 3.6, we are going to show this action of $\mathrm{GL}_2(\mathbf{R})$ on $\mathbf{R}^2 - \{\mathbf{0}\}$ is the same as the action of $\mathrm{GL}_2(\mathbf{R})$ on a certain left coset space $\mathrm{GL}_2(\mathbf{R})/H$.

Define $H = \mathrm{Stab}_{\binom{1}{0}} = \{A \in \mathrm{GL}_2(\mathbf{R}) : A\binom{1}{0} = \binom{1}{0}\}$. Carrying out the matrix-vector multiplication explicitly, the stabilizing condition $A\binom{1}{0} = \binom{1}{0}$ means the first column of A is $\binom{1}{0}$, so

$$H = \left\{ \begin{pmatrix} 1 & x \\ 0 & y \end{pmatrix} : y \neq 0 \right\}.$$

(Note $H \cong \mathrm{Aff}(\mathbf{R})$ by $\left(\begin{smallmatrix} 1 & x \\ 0 & y \end{smallmatrix}\right) \mapsto \left(\begin{smallmatrix} y & x \\ 0 & 1 \end{smallmatrix}\right)^{-1}$.)

Theorem 3.6 tells us the coset space $\mathrm{GL}_2(\mathbf{R})/H$ looks like $\mathbf{R}^2 - \{\mathbf{0}\}$. Let's try to understand how this works. For a typical matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ in $\mathrm{GL}_2(\mathbf{R})$, which matrices belong to the left coset $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)H$? For any $\left(\begin{smallmatrix} 1 & x \\ 0 & y \end{smallmatrix}\right)$ in H (x and y vary, except $y \neq 0$),

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & x \\ 0 & y \end{pmatrix} = \begin{pmatrix} a & ax + by \\ c & cx + dy \end{pmatrix}.$$

The second column in the matrix on the right is the vector $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\binom{x}{y}$. As $\binom{x}{y}$ runs through all vectors with $y \neq 0$, $\binom{ax+by}{cx+dy}$ runs through all vectors except the scalar multiples of $\binom{a}{c}$, so symbolically

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} H = \begin{pmatrix} a & * \\ c & * \end{pmatrix},$$

where the $*$ means "put anything here, keeping the matrix invertible." (A matrix $\left(\begin{smallmatrix} a & * \\ c & * \end{smallmatrix}\right)$ is invertible if and only if the second column is not a scalar multiple of $\binom{a}{c}$.) Thus, the essential data in a left coset of H is just the *common first column* of all the matrices of the coset. We can see now how cosets in $\mathrm{GL}_2(\mathbf{R})/H$ naturally correspond to non-zero vectors of $\mathbf{R}^2$: associate to a left coset the common first column of the matrices in that coset.

Now we check that the $\mathrm{GL}_2(\mathbf{R})$-action on non-zero vectors in $\mathbf{R}^2$ matches the left multiplication action of $\mathrm{GL}_2(\mathbf{R})$ on $\mathrm{GL}_2(\mathbf{R})/H$ under our "first column" correspondence $\mathrm{GL}_2(\mathbf{R})/H \to \mathbf{R}^2 - \{\mathbf{0}\}$.

Pick a left coset $\{\left(\begin{smallmatrix} \alpha & * \\ \beta & * \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbf{R})\}$ of H, where α and β are fixed. Let $\mathbf{v} = \binom{\alpha}{\beta}$. For any $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ in $\mathrm{GL}_2(\mathbf{R})$, we have $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\mathbf{v} = \binom{a\alpha+b\beta}{c\alpha+d\beta}$. On the coset side, write a typical $\left(\begin{smallmatrix} \alpha & * \\ \beta & * \end{smallmatrix}\right)$ in

explicit form, say as $\left(\begin{smallmatrix}\alpha & \gamma\\ \beta & \delta\end{smallmatrix}\right)$. Then

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} = \begin{pmatrix} a\alpha + b\beta & a\gamma + b\delta \\ c\alpha + d\beta & c\gamma + d\delta \end{pmatrix}.$$

Passing back to the cosets by ignoring the second columns, we have

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} \alpha & * \\ \beta & * \end{pmatrix} = \begin{pmatrix} a\alpha + b\beta & * \\ c\alpha + d\beta & * \end{pmatrix}.$$

This matches the way $\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right)$ multiplies the vector $\binom{\alpha}{\beta}$, so the actions of $\mathrm{GL}_2(\mathbf{R})$ on $\mathbf{R}^2 - \{\mathbf{0}\}$ by matrix-vector multiplication and on $\mathrm{GL}_2(\mathbf{R})/H$ by left multiplication agree.

It is left to the reader to examine how $\mathbf{R}^2 - \{\mathbf{0}\}$ can be viewed as a left coset space of $\mathrm{SL}_2(\mathbf{R})$ using Example 2.3.

Example 3.8. Consider the usual action of S_n on $\{1, 2, \ldots, n\}$, which is transitive. We will interpret this as a left coset action in the spirit of Theorem 3.6. The stabilizer of the last number n is naturally identified with $S_{n-1} \subset S_n$. The elements in any left coset σS_{n-1} in S_n have a common value at n since S_{n-1} fixes n. That is, for all $\pi \in S_{n-1}$ we have $(\sigma\pi)(n) = \sigma(n)$. Conversely, if $\sigma_1(n) = \sigma_2(n)$ then $\sigma_1^{-1}\sigma_2(n) = n$, so $\sigma_1^{-1}\sigma_2 \in S_{n-1}$. Thus $\sigma_1 S_{n-1} = \sigma_2 S_{n-1}$. Associating each left coset of S_{n-1} in S_n to the common value of its members at n (a number in $\{1, 2, \ldots, n\}$) converts the multiplication action of S_n on the left coset space S_n/S_{n-1} into the usual action of S_n on $\{1, 2, \ldots, n\}$.

Theorem 3.9. *Let G act transitively on X. If $N \lhd G$ then all orbits of N on X have the same cardinality.*

Proof. Pick two points x and y in X. By transitivity of G, we can write $y = gx$ for some $g \in G$. A bijection between the orbits Nx and $Ny = Ngx = gNx$ is $t \mapsto gt$. (This bijection depends on the choice of g such that $y = gx$.) □

Example 3.10. Let $G = D_4$ act on the four vertices of a square in the natural way and let $N = Z(G) = \{1, r^2\}$. The N-orbits on the four vertices are two orbits of length 2, namely pairs of opposite vertices. On the other hand, the subgroup $\{1, s\}$ is not normal, where s is reflection across a diagonal of the square, and the orbits of the vertices under this subgroup do not all have equal size: there are two orbits of length 1 and one orbit of length 2.

Example 3.11. Let p be prime. If G is a subgroup of S_p and its natural action on $\{1, 2, \ldots, p\}$ is transitive then the action of any nontrivial normal subgroup $N \lhd G$ on $\{1, 2, \ldots, p\}$ is also transitive! Indeed, the N-orbits on $\{1, 2, \ldots, p\}$ all have the same size by Theorem 3.9, say m, so $m > 1$ since *some* N-orbit is not a point (because N is nontrivial in S_p). Then counting $\{1, 2, \ldots, p\}$ by counting the orders of different N-orbits, we get $p = m \cdot |\{N\text{-orbits}\}|$ with $m > 1$, so $m = p$, which means there is only one N-orbit.

By Example 3.3, N contains a p-cycle.

Theorem 3.12 (Frattini)**.** *If G acts on X and H is a subgroup of G, then the following are equivalent:*

(1) *H acts transitively on X,*
(2) *G acts transitively on X and $G = H\,\mathrm{Stab}_x$ for some $x \in X$.*

When this occurs, $G = H\,\mathrm{Stab}_x$ for every $x \in X$.

Proof. Suppose H acts transitively on X. Then obviously G acts transitively on X. Fix an $x \in X$. For $g \in G$, $gx = hx$ for some $h \in H$, so $h^{-1}g \in \mathrm{Stab}_x$. Thus $g \in H\,\mathrm{Stab}_x$, so

$G = H\,\mathrm{Stab}_x$. Conversely, if G acts transitively on X and $G = H\,\mathrm{Stab}_x$ for some $x \in X$ then $X = Gx = H\,\mathrm{Stab}_x\, x = Hx$, so H acts transitively on X. □

Example 3.13. Let G be a finite group and $N \lhd G$. Since G acts by conjugation on N, it acts on $\mathrm{Syl}_p(N)$ (for each prime p). The conjugation action of N on $\mathrm{Syl}_p(N)$ is transitive by the Sylow theorems, so for any $P \in \mathrm{Syl}_p(N)$ we have $G = N\,\mathrm{Stab}_P = N\,\mathrm{N}_G(P)$.

Corollary 3.14. *Let G act on X. If H is a subgroup of G such that H acts transitively on X and $\mathrm{Stab}_x \subset H$ for some $x \in X$ then $H = G$.*

Proof. In Theorem 3.12, use for x the point such that $\mathrm{Stab}_x \subset H$. Then Theorem 3.12 becomes $G = H\,\mathrm{Stab}_x = H$. □

For a group G, consider the natural action of the group $\mathrm{Aut}(G)$ on G: an automorphism φ sends $g \in G$ to $\varphi(g) \in G$. The identity element in G is a fixed point: $\varphi(e) = e$ for any $\varphi \in \mathrm{Aut}(G)$. Could the action of $\mathrm{Aut}(G)$ on $G - \{e\}$ be transitive? That is, could any two non-identity elements of a group be linked by an automorphism of the group? One case where this happens is $G = (\mathbf{Z}/(p))^n$: $\mathrm{Aut}(G)$ equals $\mathrm{GL}_n(\mathbf{Z}/(p))$ and the transitivity of $\mathrm{GL}_n(\mathbf{Z}/(p))$ on $(\mathbf{Z}/(p))^n$ follows from the fact that any nonzero vector can be extended to a basis. We now show this is the only situation where $\mathrm{Aut}(G)$ acts transitively on $G - \{e\}$ and G is finite.

Theorem 3.15. *Let G be finite with $|G| > 1$. If $\mathrm{Aut}(G)$ acts transitively on $G - \{e\}$ then $G \cong (\mathbf{Z}/(p))^n$ for some prime p.*

Proof. Elements that are linked by an automorphism have the same order, so the hypothesis in the theorem implies all non-identity elements of G have the same order. Let p be a prime factor of $|G|$. Cauchy's theorem gives us an element with order p, so all non-identity elements have order p. Thus $|G|$ is a power of p. Since G is a non-trivial p-group, it has a non-trivial center. Elements that are linked by an automorphism are both in or both not in the center, so by the hypothesis of the theorem every non-identity element of G is in the center. Thus G is abelian. Since each non-zero element has order p, we can view G as a vector space over $\mathbf{Z}/(p)$, necessarily finite-dimensional since G is finite. Picking a basis shows $G \cong (\mathbf{Z}/(p))^n$ for some n. □

4. Doubly transitive group actions

Some group actions don't just take any element to any other element, but can do so in pairs. Of course, we have to assume our set has at least two elements.

Definition 4.1. An action of a group G on a set X, with $|X| \geq 2$, is called *doubly transitive* when, for any two ordered pairs of distinct elements (x, x') and (y, y') in X, there is a $g \in G$ such that $y = gx$ and $y' = gx'$.

The distinctness of elements means $x \neq x'$ and $y \neq y'$. We say g *takes the pair* (x, x') *to the pair* (y, y').

Example 4.2. When $|X| = 2$, any non-trivial action of G on X is doubly transitive. Writing $X = \{x_1, x_2\}$, the only ordered pairs of distinct elements are (x_1, x_2) and (x_2, x_1). The identity in G sends each pair to itself, and an element of G that acts non-trivially on X must send the pair (x_1, x_2) to (x_2, x_1) and *vice versa*.

Example 4.3. Let F be a field and let $\mathrm{Aff}(F)$ act on F by $\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) \cdot x = ax+b$. (Such an action on F by matrices is exactly the effect of linear polynomials on F under composition.) This is doubly transitive: for ordered pairs (x, x') and (y, y') of distinct elements in F, finding $a \in F^\times$ and $b \in F$ such that $ax + b = y$ and $ax' + b = y'$ amounts to solving for a and b in the equation $\left(\begin{smallmatrix} x & 1 \\ x' & 1 \end{smallmatrix}\right)\binom{a}{b} = \binom{y}{y'}$, which can be done since the matrix is invertible. We have $a \neq 0$ since $y \neq y'$.

Remark 4.4. The possibility $x = y$ (or y') or $x' = y'$ (or y) in Definition 4.1 is allowed. For instance, if $|X| \geq 3$ and x, y, and z are different elements of X then (x, y) and (x, z) are ordered pairs of distinct elements in X, so a doubly transitive action admits a $g \in G$ such that $gx = x$ and $gy = z$. In particular, any doubly transitive action is transitive (this is obvious when $|X| = 2$).

Example 4.5. For $n \geq 2$, S_n acts doubly transitively on $\{1, 2, \ldots, n\}$. When $n = 2$ this follows from Example 4.2. When $n \geq 3$ it is easy to see that the action of S_n can take the ordered pair $(1, 2)$ to any other ordered pair of distinct numbers from 1 to n.

Example 4.6. For $n \geq 4$, A_n acts doubly transitively on $\{1, 2, \ldots, n\}$. Indeed, if two ordered pairs of distinct numbers have no elements in common then we might as well write the ordered pairs as $(1, 2)$ and $(3, 4)$. Then the even permutation $(13)(24)$ takes the first pair to the second: 1 goes to 3 and 2 goes to 4. (Don't confuse the notation for ordered pairs with the notation for transpositions!) If the ordered pairs have one element in common then they might as well be $(1, 2)$ and $(1, 3)$. Then the 3-cycle (234) sends the first pair to the second. However, A_3 does not act doubly transitively on $\{1, 2, 3\}$: there is no $\sigma \in A_3$ taking the pair $(1, 2)$ to the pair $(2, 1)$. Similarly, A_2 does not act doubly transitively on $\{1, 2\}$ since A_2 is trivial.

Example 4.7. The action of D_n on the n vertices of a regular n-gon is *not* doubly transitive for $n \geq 4$ (it is for $n = 3$). For instance, an element of D_n that fixes one vertex does not have the freedom to exchange any other two vertices.

Example 4.8. Although $\mathrm{GL}_2(\mathbf{R})$ acts transitively on $\mathbf{R}^2 - \{\mathbf{0}\}$ (Example 2.2), it does *not* act doubly transitively. The reason has to do with linear dependence. For $A \in \mathrm{GL}_2(\mathbf{R})$ and $\mathbf{v} \in \mathbf{R}^2 - \{\mathbf{0}\}$, A takes the pair $(\mathbf{v}, -\mathbf{v})$ to the pair $(A\mathbf{v}, -A\mathbf{v})$, which are negatives of each other. In particular, given linearly independent vectors $\mathbf{v}_1$ and $\mathbf{v}_2$, it is impossible for any matrix in $\mathrm{GL}_2(\mathbf{R})$ to take a pair $(\mathbf{v}, -\mathbf{v})$ to the pair $(\mathbf{v}_1, \mathbf{v}_2)$.

Theorem 3.9 tells us the orbits of a normal subgroup of a group acting transitively share the same cardinality. We can say more about orbits of a normal subgroup when the action of the original group is doubly transitive.

Theorem 4.9. *Suppose G acts doubly transitively on a set X. Any normal subgroup $N \lhd G$ acts on X either trivially or transitively.*

Proof. Suppose N does not act trivially: $nx \neq x$ for some $x \in X$ and $n \neq 1$ in N. Pick any y and y' in X with $y \neq y'$. There is $g \in G$ such that $y = gx$ and $y' = g(nx)$. Then $y' = (gng^{-1})(gx) = (gng^{-1})(y)$ and $gng^{-1} \in N$, so N acts transitively on X. □

Example 4.10. The action of A_4 on $\{1, 2, 3, 4\}$ is doubly transitive and the normal subgroup $\{(1), (12)(34), (13)(24), (14)(23)\} \lhd A_4$ acts transitively on $\{1, 2, 3, 4\}$.

Example 4.11. Let $\mathrm{Aff}(F)$ act on F by $\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)x = ax + b$. This is doubly transitive and the normal subgroup $N = \{\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) : b \in F\}$ acts transitively (by translations) on F.

Example 4.12. We noted in Example 4.7 that the action of D_4 on the 4 vertices of a square is not doubly transitive. Consistent with Theorem 4.9, recall from Example 3.10 that the normal subgroup $\{1, r^2\}$ of D_4 acts on the vertices neither trivially nor transitively.

In Remark 4.4, we observed that a doubly transitive action on a set X with $|X| \geq 3$ has to be able to fix any one element x while sending any element $\neq x$ to any other element $\neq x$. This reflects a transitivity of the action of the stabilizer subgroup of x on the set $X - \{x\}$. (For each $g \in \mathrm{Stab}_x$ and $y \in X - \{x\}$, $y \neq x \Longrightarrow gy \neq gx = x$, so Stab_x acts on $X - \{x\}$.) In fact, this transitivity of Stab_x on $X - \{x\}$ is equivalent to double transitivity of G on X:

Theorem 4.13. *Let G act on X with $|X| \geq 3$. The action is doubly transitive if and only if, for each $x \in X$, the group Stab_x acts transitively on $X - \{x\}$.*

The if direction is false if $|X| = 2$ and G acts trivially on X: the action is not doubly transitive but Stab_x is transitive on the one element set $X - \{x\}$.

Proof. If G acts doubly transitively on X and $x \in X$ then Stab_x acts transitively on $X - \{x\}$ by Remark 4.4.

To prove the converse, assume for each $x \in X$ that the action of Stab_x on $X - \{x\}$ is transitive. We consider two ordered pairs (x_1, x_2) and (y_1, y_2) in $X \times X$, with $x_1 \neq x_2$ and $y_1 \neq y_2$. Our goal is to find an element of G taking the first pair to the second.

Usually we can do this in two steps. Use elements of Stab_{x_1} and Stab_{y_2} with the successive effects

$$(x_1, x_2) \mapsto (x_1, y_2) \mapsto (y_1, y_2).$$

The only time this recipe doesn't work is when $x_1 = y_2$ (why?).

If $x_1 = y_2$, choose some $z \neq x_1, y_1$ in X. (There is such a z since $|X| \geq 3$.) Now use elements of Stab_{x_1}, Stab_z, and Stab_{y_1} to obtain

$$(x_1, x_2) \mapsto (x_1, z) \mapsto (y_1, z) \mapsto (y_1, y_2).$$

□

Example 4.14. We can use Theorem 4.13 to give alternate explanations of Examples 4.5 and 4.6. Taking $G = S_n$ for $n \geq 2$, the stabilizer of any point in $\{1, 2, \ldots, n\}$ acts on the complement of that point just like S_{n-1} in its natural action. Since we already know the natural action of S_{n-1} is transitive, Theorem 4.13 tells us S_n acts doubly transitively for $n \geq 3$ (and it is obvious for $n = 2$). A similar argument shows A_n acts doubly transitively for $n \geq 4$. (We need $n - 1 \geq 3$ in order for A_{n-1} to act transitively on $\{1, 2, \ldots, n-1\}$, by Example 1.3.) Note A_3 acts transitively but not doubly transitively on $\{1, 2, 3\}$.

Corollary 4.15. *If a finite group acts doubly transitively on a set then the group has even size.*

Proof. Let G act doubly transitively on X, with $|X| = n \geq 2$. Pick $x_1 \in X$ and $x_2 \in X - \{x_1\}$. Set $H = \mathrm{Stab}_{x_1}$, so $[G : H] = n$ (Theorem 3.2). Since $n \mid |G|$, we may assume $n \geq 3$. Then H acts transitively on $X - \{x_1\}$ by Theorem 4.13. Set $K = H \cap \mathrm{Stab}_{x_2}$, so $[H : K] = |X - \{x_1\}| = n - 1$. Thus

$$|G| = [G : H][H : K]|K| = n(n-1)|K|.$$

Either n or $n - 1$ is even, so $2 \mid |G|$. □

Note it is the group in Corollary 4.15 that has to have even size, not the set. For instance, $\mathrm{Aff}(F)$ acts doubly transitively on F for any field F and finite F can have odd size. But $|\mathrm{Aff}(F)| = |F|(|F|-1)$ always has even size when F is finite.

Theorem 4.13 leads to two other characterizations of double transitivity.

Corollary 4.16. *Let G act on X with $|X| \geq 2$. Fix $x_0 \in X$. The action is doubly transitive if and only if it is transitive and Stab_{x_0} acts transitively on $X - \{x_0\}$.*

Proof. The result is clear when $|X| = 2$ (Example 4.2), so take $|X| \geq 3$.

The "only if" direction follows from Theorem 4.13. Conversely, assume the "if" hypothesis holds. We will show for any $y \in X$ that Stab_y acts transitively on $X - \{y\}$. Then G acts doubly transitively by Theorem 4.13.

Write $y = gx_0$. Then $\mathrm{Stab}_y = g\,\mathrm{Stab}_{x_0}\,g^{-1}$. For $z_1, z_2 \neq y$ we have $g^{-1}z_1$ and $g^{-1}z_2$ not equal to $g^{-1}y = x_0$. Then by hypothesis, some $h \in \mathrm{Stab}_{x_0}$ satisfies $hg^{-1}z_1 = g^{-1}z_2$, so $ghg^{-1}z_1 = z_2$. Since $ghg^{-1} \in \mathrm{Stab}_{gx_0} = \mathrm{Stab}_y$, the group Stab_y acts transitively on $X - \{y\}$. □

Corollary 4.17. *Let G act on X with $|X| \geq 2$ and let H be the stabilizer subgroup of a point in X. Then the action of G on X is doubly transitive if and only if it is transitive and*

$$G = H \cup HgH$$

for some $g \notin H$, in which case this is true for any $g \notin H$.

Proof. If $|X| = 2$ then G acts doubly transitively if and only if G acts transitively. When the action is transitive H has index 2. Subgroups of index 2 are normal, so the decomposition in the theorem holds because $HgH = gH$; we get the decomposition of G into two (left) H-cosets.

Now let $|X| \geq 3$. Let x be a point having H as its stabilizer. Pick $g \notin H$, so $gx \neq x$. If the action is doubly transitive then it is transitive and by Theorem 4.13 $X - \{x\} = Hgx$. For any $g' \in G$, if $g' \notin H$ then $g'x = hgx$ for some $h \in H$, so $g' = hg\widetilde{h}$ for some $\widetilde{h} \in H$. Thus $G = H \cup HgH$. This union is disjoint since H fixes x and no element of HgH fixes x.

Conversely, if G acts transitively and we have a decomposition $G = H \cup HgH$ for some $g \notin H$ then the union is disjoint and H sends gx to all of $X - \{x\}$ (because $X = Gx$). Therefore G acts doubly transitively by Corollary 4.16. □

Remark 4.18. There is another way (besides Theorem 4.13 and Corollaries 4.16 and 4.17) to characterize double transitivity. When G acts on X it also acts on $X \times X$ in a natural way, by $g \cdot (x, y) = (gx, gy)$. This is easily checked to be a group action. Since $gx = gy$ if and only if $x = y$, G acts separately on the diagonal $\Delta = \{(x, x) : x \in X\}$ and on its complement $X \times X - \Delta = \{(x, y) : x \neq y\}$. The action of G on X is doubly transitive if and only if G acts transitively on $X \times X - \Delta$.

Note Theorem 4.13, Corollaries 4.16 and 4.17, and Remark 4.18 give characterizations of doubly transitive actions. The following theorem gives only a necessary (not a sufficient) condition for double transitivity.

Theorem 4.19. *If G acts doubly transitively on X then the stabilizer subgroup of any point is a maximal subgroup of G.*

A maximal subgroup is a proper subgroup contained in no other proper subgroup.

Proof. Pick $x_0 \in X$ and let $H = \mathrm{Stab}_{x_0}$. Assume K is a subgroup strictly containing H. By Corollary 4.17, $G = H \cup HgH$ for any $g \notin H$. Pick $g \in K - H$. Then $G = H \cup HgH \subset K$, so $K = G$. □

Example 4.20. According to Example 4.5 and Theorem 4.19, S_{n-1} is a maximal subgroup of S_n (with index n) for $n \geq 2$.

The converse of Theorem 4.19 is false: by Corollary 4.15 a finite group of odd size has no doubly transitive actions, but it does have actions where all the stabilizer subgroups are maximal subgroups (consider left multiplication of G on G/H with H a maximal subgroup of G).

Let F be a field. The action of $\mathrm{GL}_2(F)$ on $F^2 - \{\binom{0}{0}\}$ is not doubly transitive since linearly dependent vectors can't be sent to linearly independent vectors by a matrix. Since linearly dependent vectors in F^2 lie along the same line through the origin, consider the action of $\mathrm{GL}_2(F)$ on the one-dimensional subspaces of F^2: $A \in \mathrm{GL}_2(F)$ sends the line $L = Fv$ to the line $A(L) = F(Av)$. (Equivalently, we are letting $\mathrm{GL}_2(F)$ act on $\mathbf{P}^1(F)$, the projective line over F.) Not only does this action of $\mathrm{GL}_2(F)$ turn out to be doubly transitive, but the restriction of this action to $\mathrm{SL}_2(F)$ is doubly transitive.

Theorem 4.21. *For any field F, the action of $\mathrm{SL}_2(F)$ on the one-dimensional subspaces of F^2 is doubly transitive. In particular, the action of $\mathrm{GL}_2(F)$ is also doubly transitive.*

Proof. The action of $\mathrm{SL}_2(F)$ on $F^2 - \{\binom{0}{0}\}$ is transitive (Example 2.3 for $F = \mathbf{R}$), so its action on the one-dimensional subspaces of F^2 is also transitive. Thus, to show the action of $\mathrm{SL}_2(F)$ on the one-dimensional subspaces of F^2 is doubly transitive we will follow Corollary 4.16 and show the stabilizer subgroup of the one-dimensional subspace $F\binom{1}{0}$ acts transitively on the other one-dimensional subspaces.

The stabilizer subgroup of $F\binom{1}{0}$ in $\mathrm{SL}_2(F)$ is

$$\begin{aligned} \mathrm{Stab}_{F\binom{1}{0}} &= \left\{ A \in \mathrm{SL}_2(F) : A\begin{pmatrix} 1 \\ 0 \end{pmatrix} \in F\begin{pmatrix} 1 \\ 0 \end{pmatrix} \right\} \\ &= \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \mathrm{SL}_2(F) \right\} \\ &= \left\{ \begin{pmatrix} a & b \\ 0 & 1/a \end{pmatrix} : a \in F^\times, b \in F \right\}. \end{aligned} \tag{4.1}$$

Pick one-dimensional subspaces Fv and Fw with neither equal to $F\binom{1}{0}$. That means the lines Fv and Fw each contain a vector with a non-zero second coordinate, so each of these lines contains a vector with second coordinate 1, say $Fv = F\binom{x}{1}$ and $Fw = F\binom{y}{1}$. Since $\left(\begin{smallmatrix} 1 & y-x \\ 0 & 1 \end{smallmatrix}\right)\binom{x}{1} = \binom{y}{1}$, $\left(\begin{smallmatrix} 1 & y-x \\ 0 & 1 \end{smallmatrix}\right)$ sends Fv to Fw. Thus $\mathrm{SL}_2(F)$ acts doubly transitively. □

One can formulate the idea of a triply-transitive action, and more generally a k-fold transitive action for any integer $k \geq 1$: given any two ordered k-tuples $(x_1, \ldots, x_k)$ and $(y_1, \ldots, y_k)$ of distinct elements in the set, some element of the group sends x_i to y_i for all i. For instance, S_n is n-fold transitive on $\{1, 2, \ldots, n\}$ for any n and A_n is $(n-2)$-fold transitive on $\{1, 2, \ldots, n\}$ for $n \geq 3$. An action that is k-fold transitive is ℓ-fold transitive for $\ell < k$, so any triply transitive action is doubly transitive and transitive.

Example 4.22. Let F be a field. The action of $\mathrm{GL}_2(F)$ on the one-dimensional subspaces of F^2 is triply transitive.

It is enough to show the particular one-dimensional subspaces $F\binom{1}{0}$, $F\binom{0}{1}$, and $F\binom{1}{1}$ can be sent by some matrix in $\mathrm{GL}_2(F)$ to any other triple of distinct one-dimensional subspaces Fu, Fv, Fw (in this order). We need to find an $A \in \mathrm{GL}_2(F)$ such that $A\binom{1}{0} \in Fu$, $A\binom{0}{1} \in Fv$, and $A\binom{1}{1} \in Fw$. Since $Fu \neq Fv$, u and v are linearly independent and thus are a basis of F^2. Write $w = \alpha u + \beta v$ with $\alpha, \beta \in F$. We have $\alpha, \beta \neq 0$ since Fw is not Fu or Fv. Let A be the 2×2 matrix $(\alpha u \ \beta v)$, which is invertible since the columns are linearly independent. Then $A\binom{1}{0} = \alpha u$, $A\binom{0}{1} = \beta v$, and $A\binom{1}{1} = w$.

Example 4.23. Let F be a field. The action of $\mathrm{SL}_2(F)$ on the one-dimensional subspaces of F^2 is triply transitive if and only if $F^\times = F^{\times 2}$.

Generalizing Corollary 4.16, a group G acting transitively on a set X acts triply transitively if and only if $\mathrm{Stab}_x \cap \mathrm{Stab}_y$ acts transitively on $X - \{x, y\}$ for some distinct pair x and y in X. Taking $G = \mathrm{SL}_2(F)$ acting on the one-dimensional subspaces of F^2,

$$\mathrm{Stab}_{F\binom{1}{0}} \cap \mathrm{Stab}_{F\binom{0}{1}} = \left\{ \begin{pmatrix} a & 0 \\ 0 & 1/a \end{pmatrix} : a \in F^\times \right\}.$$

For any $t \neq 0$ or 1 in F, there is an a such that $\left(\begin{smallmatrix} a & 0 \\ 0 & 1/a \end{smallmatrix}\right)\binom{1}{1} \in F\binom{t}{1}$ if and only if $\binom{a}{1/a} \in F\binom{t}{1}$, *i.e.*, $t = a^2$.

The condition $F^\times = (F^\times)^2$ holds when F is algebraically closed (*e.g.*, $F = \mathbf{C}$). When F is finite, $F^\times = (F^\times)^2$ if and only if F has characteristic 2.

Example 4.24. Let F be a field. The action of $\mathrm{Aff}(F)$ on F is doubly transitive (Example 4.3) but it is not triply transitive when $|F| \geq 3$: for any choice of $t \neq 0, 1$ in F there is no $\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)$ in $\mathrm{Aff}(F)$ that sends 0 to 0, 1 to 1, and t to $t+1$ since the first two conditions force the matrix to be $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, which sends t to t. More generally, for any $x \neq y$ in F the two-point stabilizer $\mathrm{Stab}_{x,y} := \mathrm{Stab}_x \cap \mathrm{Stab}_y$ in $\mathrm{Aff}(F)$ is trivial. This action is also faithful; for instance, a matrix in $\mathrm{Aff}(F)$ is determined by where it sends 0 and 1.

Conversely, every faithful doubly transitive action on a finite set with trivial two-point stabilizers is equivalent to the natural action of the affine group of a finite *near field* [3, §7.6]. The set of all finite faithful doubly transitive actions (with no assumptions on the two-point stabilizers) is described in [3, §7.7].

Remark 4.25. Examples of faithful k-fold transitive actions with $k \geq 4$ other than the natural actions of $S_n (n \geq 4)$ and $A_n (n \geq 6)$ are rare: the only others are related to four of the five Mathieu groups (which we do not define here, but will meet again in Appendix 6). Two are 4-fold transitive and two are 5-fold transitive.

Here is the doubly transitive refinement of Theorem 3.15.

Theorem 4.26. *Let G be finite with $|G| > 1$. If $\mathrm{Aut}(G)$ acts doubly transitively on $G - \{e\}$ then $G \cong (\mathbf{Z}/(2))^n$ or $G \cong \mathbf{Z}/(3)$.*

Proof. By Theorem 3.15, $G \cong (\mathbf{Z}/(p))^n$. If $n \geq 2$, pick linearly independent v and w in G. If $p > 2$ then $v, -v$, and w are distinct elements of G and there is no $A \in \mathrm{Aut}(G) \cong \mathrm{GL}_n(\mathbf{Z}/(p))$ such that $Av = v$ while $A(-v) = w$. So if $\mathrm{Aut}(G)$ acts doubly transitively on G then $p = 2$ or $n = 1$. If $n = 1$ then an automorphism of $G \cong \mathbf{Z}/(p)$ that fixes a non-zero element fixes all elements, so by double transitivity there can be at most 2 non-zero elements. Thus if $n = 1$ we have $p - 1 \leq 2$, so $p \leq 3$. □

The converse is true. To see that $\mathrm{GL}_n(\mathbf{Z}/(2))$ acts doubly transitively on $(\mathbf{Z}/(2))^n - \{\mathbf{0}\}$, pick $x \neq x'$ and $y \neq y'$ in $(\mathbf{Z}/(2))^n - \{\mathbf{0}\}$. Then, letting $F = \mathbf{Z}/(2)$,

$$G \cong F^n = Fx + Fx' + U = Fy + Fy' + V$$

for suitable subspaces U and V. Let $A : F^n \to F^n$ be a linear map such that $Ax = y$, $Ax' = y'$, and A identifies a basis of U with a basis of V. Then $A \in \mathrm{GL}_n(\mathbf{Z}/(2))$, so the action of $\mathrm{Aut}(G)$ on $G - \{e\}$ is doubly transitive. The group $\mathrm{Aut}(\mathbf{Z}/(3)) = (\mathbf{Z}/(3))^\times$ acts doubly transitively on $\mathbf{Z}/(3) - \{0\}$ since it is a non-trivial action on a set of size 2.

Corollary 4.27. *Let G be finite with $|G| > 1$. If $\mathrm{Aut}(G)$ acts triply transitively on $G - \{e\}$ then $G \cong (\mathbf{Z}/(2))^2$.*

Proof. Since $|G - \{e\}| \geq 3$, by Theorem 4.26 we have $G \cong (\mathbf{Z}/(2))^n$ for some $n \geq 2$.

Let v and w be linearly independent in $(\mathbf{Z}/(2))^n$. Then by triple transitivity $\mathrm{Stab}_v \cap \mathrm{Stab}_w$ acts transitively on the remaining non-zero vectors. Since a linear map fixing v and w also fixes $v + w$, the whole group is just $\{0, v, w, v + w\}$. Therefore $n = 2$. □

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

The goal of this section is to use the doubly transitive action of $\mathrm{SL}_2(F)$ on the one-dimensional subspaces of F^2 to prove the simplicity of most groups $\mathrm{PSL}_2(F)$ from the following criterion of Iwasawa.

Theorem 5.1 (Iwasawa)**.** *Let G be a group that acts doubly transitively on a set X. Suppose for some $x \in X$ that Stab_x has an abelian normal subgroup whose conjugate subgroups generate G. If $[G, G] = G$ then G/K is a simple group, where K is the kernel of the action of G on X.*

The kernel of an action is the kernel of the homomorphism $G \to \mathrm{Sym}(X)$; it's those g that act like the identity permutation on X. An action is faithful if and only if it has a trivial kernel.

Proof. To show G/K is simple we will show the only normal subgroups of G lying between K and G are K and G. Let $K \subset N \subset G$ with $N \lhd G$. Let $H = \mathrm{Stab}_x$, so H is a maximal subgroup of G (Theorem 4.19). Since NH is a subgroup of G containing H, either $NH = H$ or $NH = G$. By Theorem 4.9, N acts trivially or transitively on X, so $N \subset K$ or $NH = G$ (check!). If $N \subset K$ then $N = K$ by hypothesis.

Now suppose $NH = G$. Let U be the abelian normal subgroup of H in the hypothesis: its conjugate subgroups generate G. Since $U \lhd H$, $NU \lhd NH = G$. Then for $g \in G$, $gUg^{-1} \subset g(NU)g^{-1} = NU$, which shows NU contains all the conjugate subgroups of U. By hypothesis it follows that $NU = G$.

Thus $G/N = (NU)/N \cong U/(N \cap U)$ is abelian, so $[G, G] \subset N$. Since $G = [G, G]$ by hypothesis, we have $N = G$. □

Example 5.2. We can use Theorem 5.1 to show A_5 is a simple group. Its natural action on $\{1, 2, 3, 4, 5\}$ is doubly transitive and faithful. Let $x = 5$, so $\mathrm{Stab}_x \cong A_4$, which has the abelian normal subgroup

$$\{(1), (12)(34), (13)(24), (14)(23)\}.$$

The A_5-conjugates of this subgroup generate A_5 since the (2,2)-cycles in A_5 are all conjugate and generate A_5. It remains to show $[A_5, A_5] = A_5$. The commutator subgroup $[A_5, A_5]$

contains every (2,2)-cycle:

$$(abc)(abd)(abc)^{-1}(abd)^{-1} = (ab)(cd).$$

Therefore $[A_5, A_5] = A_5$, so A_5 is simple.

We will apply Theorem 5.1 to $G = \mathrm{SL}_2(F)$ acting doubly transitively on the set of one-dimensional subspaces of F^2. What is the kernel K of this action? That is, which matrices $A \in \mathrm{SL}_2(F)$ carry each one-dimensional subspace of F^2 back to itself? If $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ preserves the lines $F\binom{1}{0}$ and $F\binom{0}{1}$ then $c = 0$ and $b = 0$, so $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \left(\begin{smallmatrix} a & 0 \\ 0 & d \end{smallmatrix}\right)$. The determinant is 1, so $d = 1/a$. If $\left(\begin{smallmatrix} a & 0 \\ 0 & 1/a \end{smallmatrix}\right)$ preserves the line $F\binom{1}{1}$ then $a = 1/a$, so $a = \pm 1$. This means the matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ equals $\pm\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, which is the center of $\mathrm{SL}_2(F)$. Thus $G/K = \mathrm{PSL}_2(F)$.

Let $x = F\binom{1}{0}$. Its stabilizer subgroup in $\mathrm{SL}_2(F)$ is given in (4.1). This subgroup has an abelian normal subgroup

$$U = \left\{ \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \right\} = \left\{ \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} : \lambda \in F \right\}.$$

Note $U \cong F$ by $\left(\begin{smallmatrix} 1 & \lambda \\ 0 & 1 \end{smallmatrix}\right) \mapsto \lambda$. For example, $\left(\begin{smallmatrix} 1 & \lambda \\ 0 & 1 \end{smallmatrix}\right)^{-1} = \left(\begin{smallmatrix} 1 & -\lambda \\ 0 & 1 \end{smallmatrix}\right)$.

Theorem 5.3. *The subgroup U and its conjugates generate $\mathrm{SL}_2(F)$. More precisely, every element of $\mathrm{SL}_2(F)$ is the product of at most 3 elements from U and its conjugates.*

We will arrive at a proof of Theorem 5.3 after a definition and a lemma.

Definition 5.4. Any matrix in $\mathrm{SL}_2(F)$ that is conjugate to a matrix in U is called a *transvection*.

If $F = \mathbf{R}$, then U consists of *horizontal shears*: each vector is moved to another vector on the same horizontal line and the x-axis is fixed pointwise. Intuitively, a transvection is a shear transformation in some (not necessarily horizontal) direction.

Example 5.5. Since $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & \lambda \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)^{-1} = \left(\begin{smallmatrix} 1 & 0 \\ -\lambda & 1 \end{smallmatrix}\right)$, the matrices $\left(\begin{smallmatrix} 1 & 0 \\ * & 1 \end{smallmatrix}\right)$ are all transvections. A general transvection looks like

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

where $\alpha\delta - \beta\gamma = 1$. Notice there is no dependence on β or δ on the right side.

Lemma 5.6. *For any nonzero vector v in F^2, there is a transvection or a product of two transvections taking $\binom{1}{0}$ to v.*

Proof. The basic idea is this: if v is not on the line $F\binom{1}{0}$ then a shear in some direction will take $\binom{1}{0}$ to v. If v is on the line $F\binom{1}{0}$, then we can move $\binom{1}{0}$ off that line by some shear and then move it back onto that line to land on v by another shear. This is where the one or two transvections in the lemma come from.

Write $v = \binom{x}{y}$. We look for $\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$ in $\mathrm{SL}_2(F)$ and $\lambda \in F$ such that

$$\begin{pmatrix} 1-\alpha\gamma\lambda & \alpha^2\lambda \\ -\gamma^2\lambda & 1+\alpha\gamma\lambda \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1-\alpha\gamma\lambda \\ -\gamma^2\lambda \end{pmatrix} \stackrel{?}{=} \begin{pmatrix} x \\ y \end{pmatrix}.$$

We want $1 - \alpha\gamma\lambda = x$, $-\gamma^2\lambda = y$, and $\alpha\delta - \beta\gamma = 1$. Use $\lambda = -y$, $\gamma = 1$ and $\alpha = (x-1)/y$; we need $y \neq 0$. In this case, we can get $\alpha\delta - \beta\gamma = 1$ with $\beta = -1$ and $\delta = 0$. The transvection $\left(\begin{smallmatrix} (x-1)/y & -1 \\ 1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & -y \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} (x-1)/y & -1 \\ 1 & 0 \end{smallmatrix}\right)^{-1} = \left(\begin{smallmatrix} x & -(x-1)^2/y \\ y & 2-x \end{smallmatrix}\right)$ sends $\binom{1}{0}$ to $\binom{x}{y} = v$.

What if $y = 0$? Then $x \neq 0$. The transvection $t_1 = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$ sends $v = \binom{x}{0}$ to $\binom{x}{x}$, whose second coordinate is non-zero. Therefore, by the previous paragraph there is a transvection t_2 sending $\binom{1}{0}$ to $\binom{x}{x}$, so $t_1^{-1}t_2$ sends $\binom{1}{0}$ to $\binom{x}{0} = v$. □

Now we prove Theorem 5.3.

Proof. Pick any $M \in \mathrm{SL}_2(F)$. Set $v = M\binom{1}{0}$. By Lemma 5.6 there is a product h of 1 or 2 transvections such that $h\binom{1}{0} = v$. Then $(h^{-1}M)\binom{1}{0} = \binom{1}{0}$, so $h^{-1}M = \left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right)$. Since the determinant of $h^{-1}M$ is 1, $h^{-1}M = \left(\begin{smallmatrix} 1 & \mu \\ 0 & 1 \end{smallmatrix}\right)$ for some μ. This last matrix is a transvection, so $M = h\left(\begin{smallmatrix} 1 & \mu \\ 0 & 1 \end{smallmatrix}\right)$ is a product of at most 3 transvections. □

Remark 5.7. Here is a second proof of Theorem 5.3. Given a matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ in $\mathrm{SL}_2(F)$ we can write it as a product of three matrices of type $\left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} 1 & 0 \\ * & 1 \end{smallmatrix}\right)$ when b or c is non-zero. 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 $b = 0$ and $c = 0$ then the matrix is $\left(\begin{smallmatrix} a & 0 \\ 0 & 1/a \end{smallmatrix}\right)$. We can conjugate this to a matrix with non-zero upper-right entry as $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} a & 0 \\ 0 & 1/a \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)^{-1} = \left(\begin{smallmatrix} a & a-1/a \\ 0 & 1/a \end{smallmatrix}\right)$, provided $a^2 \neq 1$. Then the explicit calculations above express $\left(\begin{smallmatrix} a & a-1/a \\ 0 & 1/a \end{smallmatrix}\right)$ as a product of three matrices of type $\left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} 1 & 0 \\ * & 1 \end{smallmatrix}\right)$ so we can conjugate back to express $\left(\begin{smallmatrix} a & 0 \\ 0 & 1/a \end{smallmatrix}\right)$ as a product of three transvections. The remaining cases are $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. The identity matrix is $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & -1 \\ 0 & 1 \end{smallmatrix}\right)$ and its negative is $\left(\begin{smallmatrix} 1 & 0 \\ -1 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} -1 & 4 \\ -1 & 3 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 4 \\ 0 & 1 \end{smallmatrix}\right)$, where $\left(\begin{smallmatrix} -1 & 4 \\ -1 & 3 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 2 & -1 \\ 1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 2 & -1 \\ 1 & 0 \end{smallmatrix}\right)^{-1}$ is a transvection.

Allowing four transvections, we can write all the diagonal matrices in $\mathrm{SL}_2(F)$ explicitly in terms of matrices of type $\left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 0 \\ * & 1 \end{smallmatrix}\right)$:

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

So far F can be any field. Now we reach a result where we need $|F| \geq 4$.

Theorem 5.8. *If $|F| \geq 4$ then $[\mathrm{SL}_2(F), \mathrm{SL}_2(F)] = \mathrm{SL}_2(F)$.*

Proof. We compute an explicit commutator:

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

Since $|F| \geq 4$, there is an $a \neq 0, 1$, or -1 in F, so $a^2 \neq 1$. Using this value of a and letting b run over F shows $[\mathrm{SL}_2(F), \mathrm{SL}_2(F)]$ contains U. Since the commutator subgroup is normal, it contains every subgroup conjugate to U, so $[\mathrm{SL}_2(F), \mathrm{SL}_2(F)] = \mathrm{SL}_2(F)$ by Theorem 5.3. □

Theorem 5.8 is false when $|F| = 2$ or 3: $\mathrm{SL}_2(\mathbf{Z}/(2)) = \mathrm{GL}_2(\mathbf{Z}/(2))$ is isomorphic to S_3 and $[S_3, S_3] = A_3$. In $\mathrm{SL}_2(\mathbf{Z}/(3))$ the 2-Sylow subgroup is normal with index 3, so the quotient by it is abelian. Therefore the commutator subgroup of $\mathrm{SL}_2(\mathbf{Z}/(3))$ lies inside the 2-Sylow subgroup (in fact, the commutator subgroup is the 2-Sylow subgroup).

Corollary 5.9. *If $|F| \geq 4$ then the group $\mathrm{PSL}_2(F)$ is simple.*

Proof. The action of $\mathrm{SL}_2(F)$ on the one-dimensional subspaces of F^2 satisfies the hypotheses of Iwasawa's theorem with K equal to the center of $\mathrm{SL}_2(F)$. □

Since $\mathrm{PSL}_2(\mathbf{Z}/(2)) \cong S_3$ and $\mathrm{PSL}_2(\mathbf{Z}/(3)) \cong A_4$ are not simple, the constraint on $|F|$ in Corollary 5.9 is necessary.

By similar arguments, if $n \geq 3$ then $\mathrm{PSL}_n(F)$ is a simple group for every field F. This is proved by studying the action of $\mathrm{SL}_n(F)$ on the one-dimensional subspaces of F^n (*i.e.*, on the projective space $\mathbf{P}^{n-1}(F)$). The restriction $|F| \geq 4$ from the $n = 2$ case does not arise when $n \geq 3$ since $[\mathrm{SL}_n(F), \mathrm{SL}_n(F)] = \mathrm{SL}_n(F)$ for every F. Once $n \geq 3$ there is enough room to move around even when $|F| < 4$.

By comparison to $\mathrm{PSL}_2(F)$, the groups $\mathrm{PGL}_2(F)$ are never simple, although it is instructive to run through the above proof with $\mathrm{GL}_2(F)$ in place of $\mathrm{SL}_2(F)$ to see where things go wrong with the application of Iwasawa's theorem. They start off well, since the action of $\mathrm{GL}_2(F)$ on the one-dimensional subspaces of F^2 is doubly transitive (even triply transitive). But we run into a problem with the GL_2-analogue of Theorem 5.8: the commutator subgroup of $\mathrm{GL}_2(F)$ is not $\mathrm{GL}_2(F)$ but is $\mathrm{SL}_2(F)$ for $|F| \geq 4$. (Any commutator in $\mathrm{GL}_2(F)$ has determinant 1; now use Theorem 5.8.) The commutator subgroup of $\mathrm{GL}_2(F)$ is a proper subgroup of $\mathrm{GL}_2(F)$ even when $|F| < 4$.

6. Simplicity of A_n

Exploiting the highly transitive action of A_{n-1} on $\{1, 2, \ldots, n-1\}$, we will prove A_n is simple for $n \geq 5$.

Lemma 6.1. *If a group G admits a faithful doubly transitive action on a set X and Stab_x is a simple group for some $x \in X$ then any non-trivial proper normal subgroup of G acts regularly on X.*

Recall a group action is called regular when the action is equivalent to the left multiplication action of the group on itself.

Proof. Set $H_x = \mathrm{Stab}_x$ for each $x \in X$. Then all the H_x's are conjugate (so isomorphic) to each other and therefore are simple groups by hypothesis. Since G acts doubly transitively, H_x is a maximal subgroup of G (Theorem 4.19).

Assume there is a normal subgroup N not equal to $\{e\}$ or G. Since N is non-trivial and the action of G on X is faithful, N does not act trivially on X. Therefore N acts transitively on X (Theorem 4.9). Pick $x \in X$. Since $N \lhd G$, we have $N \cap H_x \lhd H_x$. Since H_x is a simple group, $N \cap H_x = \{e\}$ or $N \cap H_x = H_x$. Let's eliminate the second possibility. If $N \cap H_x = H_x$ for some x then $H_x \subset N$, so $N = H_x$ or $N = G$ because H_x is a maximal subgroup of G. As $N \neq G$ we get $N = H_x$, but then N does not act transitively. This is a contradiction, so $N \cap H_x = \{e\}$ for each x. Hence N acts transitively on X with trivial stabilizers, so N acts regularly on X. □

Theorem 6.2. *Let G be a group with a faithful triply transitive action on a finite set X and assume Stab_x is a simple group for some $x \in X$. Then G is simple or $|X|$ is a power of 2 or is 3. If the action is 4-fold transitive then G is simple.*

Before proving Theorem 6.2 we note the primary consequence.

Corollary 6.3. *For $n \geq 5$, A_n is a simple group.*

Proof. We argue by induction on n. The case $n = 5$ was handled in Example 5.2 using Iwasawa's simplicity criterion (Theorem 5.1).

Now we take $n \geq 6$ and assume A_{n-1} is simple. In Theorem 6.2 let $G = A_n$ in its natural action on $X = \{1, 2, \ldots, n\}$. The action is faithful and is $(n-2)$-fold transitive, so 4-fold transitive since $n \geq 6$. Thus A_n is a simple group. □

Theorem 6.2 is also applicable to four of the five Mathieu groups. The five Mathieu groups are denoted $M_{11}, M_{12}, M_{22}, M_{23}$, and M_{24}. We will not define these groups, but each M_n has a highly (*i.e.*, at least triply) transitive faithful action on a set of size n. The groups M_{11} and M_{23} act 4-fold transitively, M_{12} and M_{24} act 5-fold transitively, and M_{22} acts triply transitively. The simplicity of M_{11} is proved in [2]. The action of M_{22} has point stabilizer isomorphic to $\mathrm{PSL}_3(\mathbf{F}_4)$, which is simple, so M_{22} is simple by Theorem 6.2. For $n = 12$, 23, and 24, the point stabilizer of M_n is M_{n-1}. None of these n's is a power of 2 or is 3, so Theorem 6.2 implies simplicity of M_{12}, M_{23}, and M_{24} from simplicity of M_{11} and M_{22}.

Remark 6.4. The only finite simple groups admitting a 4-fold transitive action are the Mathieu groups except M_{22} and the alternating groups A_n for $n \geq 6$. Therefore Theorem 6.2 has no applications to proving groups are simple beyond the ones we have already made.

Now we prove Theorem 6.2.

Proof. Let $n = |X| \geq 3$. Assume G is not simple and let N be a non-trivial proper normal subgroup. From Lemma 6.1, N acts regularly on X, so $|N| = n$. We are going to show $N \cong (\mathbf{Z}/(2))^m$ for some m or $N \cong \mathbf{Z}/(3)$, so $n = 2^m$ or $n = 3$. Then we we will get a contradiction if G acts 4-fold transitively, so G is simple in that case.

Fix a point $x_0 \in X$. Let

$$H = \mathrm{Stab}_{x_0} \subset G.$$

Then $|G| = |H| \cdot n = |H||N|$. The subgroup H acts on $X - \{x_0\}$. We can also make H act on N by conjugation. Conjugations on N fix the identity, so we will think about the conjugation action of H on the set $N - \{e\}$. These two actions of H, on $X - \{x_0\}$ in the natural way and on $N - \{e\}$ by conjugation, are equivalent to each other. Let's see why.

First, we can set up a bijection between $X - \{x_0\}$ and $N - \{e\}$. Since N acts regularly on X, for each $x \in X$ (even $x = x_0$) there is a unique $g \in N$ such that $gx_0 = x$. Set $\varphi(x) = g$. Then $\varphi(x_0) = e$, so $\varphi\colon X - \{x_0\} \to N - \{e\}$ is a bijection. For $h \in H$, how are the effects of h on $x \in X - \{x_0\}$ and on $\varphi(x) \in N - \{e\}$ related? Its effect on $\varphi(x)$ is by conjugation:

$$h \cdot \varphi(x) = h\varphi(x)h^{-1}.$$

This element of $N - \{e\}$ sends x_0 to

$$(h\varphi(x)h^{-1})(x_0) = h(\varphi(x)(h^{-1}(x_0))) = h(\varphi(x)(x_0)) = h(x),$$

so $\varphi(h(x)) = h \cdot \varphi(x)$ by the definition of φ (check!). Thus φ respects the H-actions on $X - \{x_0\}$ and on $N - \{e\}$. It shows how the actions of H on these two sets are equivalent.

Since G acts on X triply transitively, H acts on $X - \{x_0\}$ doubly transitively and therefore its action on $N - \{e\}$ is doubly transitive. The (conjugation) action of H on N is a homomorphism $H \to \mathrm{Aut}(N)$, so $\mathrm{Aut}(N)$ acts doubly transitively on $N - \{e\}$. By Theorem 4.26, $N \cong (\mathbf{Z}/(2))^m$ or $N \cong \mathbf{Z}/(3)$. Thus $|X| = |N| = 2^m$ or 3.

Assume G acts 4-fold transitively on X. Then the action of H on $X - \{x_0\}$ is 3-fold transitive, so the conjugation action of H on $N - \{e\}$ is triply transitive. Therefore $\mathrm{Aut}(N)$ acts triply transitively on $N - \{e\}$, so $N \cong (\mathbf{Z}/(2))^2$ by Corollary 4.27. Since H is simple

and acts non-trivially on N, the homomorphism $H \to \mathrm{Aut}(N) \cong \mathrm{GL}_2(\mathbf{Z}/(2)) \cong S_3$ is injective. Therefore $H \cong \mathbf{Z}/(2)$ or $H \cong \mathbf{Z}/(3)$, so $|G| = |H| \cdot 4 = 8$ or 12. Since H is a maximal subgroup of G, the possibility $|H| = 2$ (and $|G| = 8$) can't occur. Thus $|H| = 3$ and $|G| = 12$. There are 5 groups of size 12, up to isomorphism. In all of them except A_4 the subgroup of size 3 is a normal subgroup. A normal subgroup of size 3 and an element of order 2 generate a subgroup of size 6. Therefore, since H is maximal in G, we must have $G \cong A_4$. But a calculation of the subgroups of size 3 in A_4 shows the action of G on G/H is equivalent to the natural action of A_4, which is not 4-fold transitive, so we have a contradiction. □

7. G-equivalence relations and primitivity

Some useful properties of doubly transitive actions, such as Theorem 4.9, are true for a broader class of group actions that are called primitive actions. The relation looks like this:

$$\text{doubly transitive actions} \subset \text{primitive actions} \subset \text{transitive actions}.$$

We will approach the definition of primitivity (Definition 7.12) as an outgrowth of the consideration of equivalence relations preserved by a group action.

Let G act transitively on X. For any (nonempty) subset $Y \subset X$ the subsets gY (as g runs over G) share the same cardinality and cover X:

$$X = \bigcup_{g \in G} gY.$$

For instance, if Y is a one-point set then the fact that this union is X is exactly the condition of transitivity of the action. When $|Y| > 1$ the different gY's may or may not partially overlap. (When we speak of "different" gY's we mean different subsets, not simply different g's.)

Example 7.1. Let $\mathrm{GL}_2(\mathbf{R})$ act on $\mathbf{R}^2 - \{\mathbf{0}\}$ by matrix-vector multiplication. If Y is a one-dimensional subspace without the origin then gY is also a one-dimensional subspace without the origin and the different gY's do not overlap.

Example 7.2. Let D_n act on the vertices of a regular n-gon and label the vertices $1, 2, \ldots, n$ in counterclockwise order (so 1 and 2 are adjacent vertices, for instance). If we take $Y = \{1, 2\}$ then $rY = \{2, 3\}$, so $Y \cap rY = \{2\}$. The different sets gY cover the vertex set as g runs over D_n, but there are some proper nonempty overlaps between them.

There may be subsets Y of the vertex set of the regular n-gon such that the different gY's don't partially overlap. For instance, if n is *composite* and d is a proper factor of n greater than 1, then the vertex sets of regular d-gons inside the regular n-gon (that is, sets of vertices of the n-gon that are n/d units apart from each other) can be transformed into each other by the elements of D_n and these subsets are disjoint. As a particular example, with $n = 4$ and $d = 2$, the pairs of opposite vertices $\{1, 3\}$ and $\{2, 4\}$ are non-overlapping and are carried into each other by D_4.

If $n = p$ is an odd prime then the only proper subsets Y of the vertex set such that the gY's don't overlap are individual vertices: if the gY's don't overlap then the size of the vertex set is $|Y|$ times the number of different gY's, so $|Y| \mid p$. Therefore $|Y| = 1$.

To say, back in the general setting of a transitive action, that different gY's do not overlap is the same as saying they form a partition of X. A partition of a set is the same as equivalence classes for an equivalence relation on the set, so when the gY's form a

partition of X they provide us with an equivalence relation on X that is preserved by G: $x \sim x' \Longrightarrow gx \sim gx'$ for all $g \in G$, so in fact $x \sim x' \Longleftrightarrow gx \sim gx'$ for all $g \in G$. Conversely, any equivalence relation on X that is preserved by G will have equivalence classes that partition X and if Y is one of the equivalence classes then the rest are gY as g varies since G acts transitively on X. For example, vertices of regular d-gons in the vertices of a regular n-gon for a fixed divisor d of n form a basic example of a partition of the vertices that is preserved by the action of D_n.

Definition 7.3. When G acts on X, a *G-equivalence relation* on X is an equivalence relation satisfying $x \sim x' \Rightarrow gx \sim gx'$ for all $g \in G$ and $x, x' \in X$.

There are always two G-equivalence relations on X: the equivalence relation whose equivalence classes are individual points of X and the equivalence relation having all of X as a single equivalence class. Can there be others?

Lemma 7.4. *Let G act transitively on X and $Y \subset X$ be a non-empty subset. The following conditions are equivalent:*

(1) *for any g_1 and g_2 in G, the subsets g_1Y and g_2Y are either equal or are disjoint,*
(2) *for each $g \in G$, the subset gY either equals Y or is disjoint from Y.*

Proof. The second condition is clearly a special case of the first. Since $g_1Y \cap g_2Y = g_2(g_2^{-1}g_1Y \cap Y)$, the first condition follows from the second. □

Theorem 7.5. *Let G act transitively on X and let H be the stabilizer subgroup of a point in X. The G-equivalence relations on X are in bijection with the intermediate subgroups $H \subset K \subset G$. Moreover, in the equivalence relation corresponding to K each equivalence class has size $[K : H]$.*

Proof. Say $H = \mathrm{Stab}_y$, for some $y \in X$. Suppose there is a G-equivalence relation on X. Let $Y \subset X$ be the equivalence class containing y. Every equivalence class has the form gY for some $g \in G$, so all equivalence classes have the same size. What is it?

Set

$$K = \mathrm{Stab}_Y = \{g \in G : gY = Y\}.$$

Since the gY's partition X, we can also say

$$K = \{g \in G : gY \cap Y \neq \emptyset\}. \tag{7.1}$$

(That is, as soon as gY and Y overlap they coincide because equivalence classes partition X.) So $gy \in Y$ if and only if $g \in K$. In particular, $H \subset K$: if $h \in H$ then $hy = y \in Y$, so $h \in K$. Since every element of X has the form gy for some $g \in G$, $Y = Ky$. Thus $|Y| = |Ky| = [K : H]$.

Given a G-equivalence relation on X, (7.1) gives us a subgroup between H and G. Conversely, suppose K is a subgroup between H and G. Define $Y = Ky$. The sets gY ($g \in G$) partition X. To see this, it suffices by Lemma 7.4 to check that $gY \cap Y \neq \emptyset \Longrightarrow gY = Y$. Suppose $g(ky) = k'y$, so $k'^{-1}gky = y$. Then $k'^{-1}gk \in H$, so $g \in k'Hk^{-1} \subset K$, so $gY = gKy = Ky = Y$. We have produced a partition $\{gY : g \in G\}$ of X where Y is the equivalence class of y and $K = \{g : gy \in Y\}$.

This work provides a bijection between the subgroups between H and G and the G-equivalence relations on X, where the equivalence relation $\sim$ leads to the intermediate subgroup $\{g \in G : gy \sim y\}$ and the intermediate subgroup K leads to the equivalence relation $gy \sim g'y \Longleftrightarrow gK = g'K$. □

Letting $X = G/H$, G-equivalence relations on X are the same as fibers of the natural maps $G/H \to G/K$ where $H \subset K \subset G$.

Example 7.6. If $G = D_n$ acts in the usual way on the vertices of a regular n-gon, $H = \{1, s\}$ for a reflection s across a line through a vertex, and $d \mid n$ then the equivalence relation of vertices lying on a regular d-gon inside the n-gon corresponds to the subgroup $K = D_d$ containing H. Note $[K : H] = 2d/2 = d$ is the size of each equivalence class.

If we apply Theorem 7.5 to the action of G on itself by left multiplication, whose stabilizer subgroups are trivial, then it tells us that the G-equivalence relations on G that are preserved by the left multiplication action are precisely the left coset decompositions of G by different subgroups of G. Each left coset decomposition comes from a particular subgroup, and that is how the subgroups of G match up with the G-equivalence relations on G.

Corollary 7.7. *When a finite cyclic group G acts transitively on a set X, for each divisor d of $|X|$ there is one G-equivalence relation on X whose equivalence classes have size d.*

Proof. Let H be the stabilizer of a point of X, so $|X| = [G : H]$ and $d \mid [G : H]$. Since G is cyclic, there is exactly one subgroup K between H and G such that $[K : H] = d$. □

Remark 7.8. In the literature, the equivalence classes in a G-equivalence relation on X are called *blocks* and the totality of equivalence classes for a given equivalence relation is called a *block system*. If we view X as G/H, a block system is simply the left cosets of a subgroup K lying between H and G; a block is one of those cosets.

As a nice application of G-equivalence relations to group theory, we will prove an extension of part of Sylow's third theorem due to Weisner [4]. Our argument is based on some notes of H. Lenstra (which in turn are based on an argument of H. Wielandt.)

Theorem 7.9 (Weisner)**.** *Let G be a finite group and p be a prime dividing $|G|$. For any p-subgroup $H \subset G$, the number of intermediate p-subgroups $H \subset K \subset G$ with a fixed size is $\equiv 1 \bmod p$.*

The case of Theorem 7.9 where H is trivial and the subgroups have maximal p-power size is part of Sylow's third theorem. The case when H is trivial and the fixed size is any p-power dividing $|G|$ is due to Frobenius (1895).

We will derive Theorem 7.9 from the following result about group actions.

Theorem 7.10. *Let G be a finite group acting transitively on a set X. Assume the stabilizer subgroup of a point of X is a p-subgroup of G, where p is a prime. If $p^m \mid |X|$ then the number of G-equivalence relations on X whose equivalence classes each have size p^m is $\equiv 1 \bmod p$.*

To deduce Theorem 7.9 from Theorem 7.10, apply Theorem 7.5 to the usual action of G on G/H: it shows the G-equivalence relations on G/H are in bijection with the subgroups between H and G, with the size of an equivalence class in an equivalence relation being equal to the index of H in the subgroup corresponding to that equivalence relation. Since H is a p-subgroup of G, an intermediate subgroup $H \subset K \subset G$ is a p-subgroup if and only if $[K : H]$ is a p-power.

Theorems 7.9 and 7.10 are equivalent to each other. They are saying the same thing in different languages.

Now we prove Theorem 7.10.

Proof. Write $|X| = rp^m$. Fix a point $x \in X$. Set $T = \{Y \subset X : |Y| = p^m\}$, on which G acts from the left. Note $|T| = \binom{rp^m}{p^m}$.

For $Y \in T$, the sets gY as g varies cover X (G acts transitively on X) and each has size p^m, so

$$|X| \leq |\{gY : g \in G\}| \cdot |Y|$$

with equality precisely when $\{gY : g \in G\}$ is a partition of X. Writing out the sizes of X and Y explicitly, this becomes

$$r \leq |\{gY : g \in G\}| \tag{7.2}$$

with equality if and only if $\{gY : g \in G\}$ is a partition of X.

Set

$$K_Y = \{g \in G : gY = Y\}.$$

This is the stabilizer subgroup of Y for the action of G on T.

Choose $y \in Y$ and let $H_y = \mathrm{Stab}_y = \{g : gy = y\}$. By hypothesis this is a p-subgroup of G. Write

$$\widetilde{Y} = \{g \in G : gy \in Y\}.$$

This is a subset of G. (There is no reason to expect it is closed under inversion, so it need not be a subgroup of G.) Easily $H_y \subset \widetilde{Y}$ and $K_Y \subset \widetilde{Y}$. For g and g' in $\widetilde{Y}$, $gy = g'y$ if and only if $gH_y = g'H_y$. Since $H_y \subset \widetilde{Y}$, $\widetilde{Y}$ is a union of as many left H_y-cosets as there are elements of Y, so

$$|\widetilde{Y}| = |Y||H_y|, \tag{7.3}$$

which is a power of p.

If $k \in K_Y$ and $g \in \widetilde{Y}$ then $kgy \in kY = Y$, so $kg \in \widetilde{Y}$. Thus K_Y acts by left multiplication on $\widetilde{Y}$. Since $\widetilde{Y}$ is a subset of G, its K_Y-orbits are right K_Y-cosets, so $|K_Y| \mid |\widetilde{Y}|$. Therefore by (7.3) K_Y is a p-subgroup of G.

Since $\{gY : g \in G\}$ is a G-orbit in T and the stabilizer of Y is K_Y,

$$|\{gY : g \in G\}| = [G : K_Y] = \frac{|G|}{|K_Y|} = \frac{[G : H_y]|H_y|}{|K_Y|} = \frac{rp^m|H_y|}{|K_Y|} = rp^{i(Y)}$$

for some integer $i(Y)$. By (7.2) $p^{i(Y)} \geq 1$, so $i(Y) \geq 0$. (If p does not divide r then we could say $i(Y) \geq 0$ because $rp^{i(Y)} \in \mathbf{Z}$.)

Now we apply the orbit-stabilizer formula to the G-action on T. Fix an element $y \in X$. Each G-orbit in T is a collection of sets $\{gY : g \in G\}$; it covers X so we can choose Y to contain y. (At least one of the sets gY contains y and we can relabel one of those as Y by the transitivity of G on X.) Let $Y_1, \ldots, Y_d$ be representatives for the different G-orbits in T. Then

$$|T| = \sum_{j=1}^{d} |\{gY_j : g \in G\}|,$$

so

$$\binom{rp^m}{p^m} = \sum_{j=1}^{d} rp^{i(Y_j)}.$$

Since $\binom{rp^m}{p^m} = r\binom{rp^m-1}{p^m-1}$,

$$\binom{rp^m-1}{p^m-1} = \sum_{j=1}^{d} p^{i(Y_j)} \equiv |\{j : i(Y_j) = 0\}| \bmod p. \tag{7.4}$$

When does a $Y \in T$ have $i(Y) = 0$? From the definition of $i(Y)$, its vanishing is equivalent to $|\{gY : g \in G\}| = r$, which is equivalent to the sets $\{gY : g \in G\}$ forming a partition of X. (See (7.2) and the surrounding text.) This partition contains equivalence classes for a G-equivalence relation on X where the classes have size p^m. Therefore

$$|\{j : i(Y_j) = 0\}| = |\{G\text{-equiv. relns. with classes of size } p^m\}|. \tag{7.5}$$

Notice the binomial coefficient on the left side of (7.4) is determined entirely by r and p^m, not by the finer group structure of G. So far, G has been any group admitting a transitive action on some set with size rp^m and having p-subgroups as its point-stabilizers. A particular example of this is the group $G = \mathbf{Z}/(p^m r)$ acting on itself from the left (trivial stabilizers). With this choice, Corollary 7.7 implies (7.5) equals 1, so the left side of (7.4) is 1 modulo p. Therefore by (7.4), (7.5) is 1 mod p for any G fitting the hypotheses of the theorem. □

Remark 7.11. The trick at the end of the proof with the switch to the cyclic group can be avoided. The left side of (7.4) can be calculated directly modulo p using a result of Lucas: if $a = a_0 + a_1 p + \cdots + a_n p^n$ and $b = b_0 + b_1 p + \cdots + b_n p^n$ where $0 \leq a_i, b_i \leq p-1$ for $i < n$ and $a_n, b_n \geq 0$, then $\binom{a}{b} \equiv \binom{a_0}{b_0}\binom{a_1}{b_1}\cdots\binom{a_n}{b_n} \bmod p$. In particular, since

$$\begin{aligned} rp^m - 1 &= (p-1) + (p-1)p + \cdots + (p-1)p^{m-1} + (r-1)p^m, \\ p^m - 1 &= (p-1) + (p-1)p + \cdots + (p-1)p^{m-1}, \end{aligned}$$

the congruence of Lucas shows $\binom{rp^m-1}{p^m-1} \equiv \prod_{i=0}^{m-1}\binom{p-1}{p-1} \cdot \binom{r-1}{0} \equiv 1 \bmod p$.

Definition 7.12. Let G act transitively on X with $|X| > 1$. The action is called *primitive* if there are no G-equivalence relations on X other than the two equivalence relations of individual points and the whole set.

If the group action is not transitive then it has a G-equivalence relation on X other than the two trivial relations: its orbits! (Well, the orbits are a trivial equivalence relation when the action is trivial, but in that case any partition of X is a G-equivalence relation). Therefore it is natural to include transitivity in the definition of a primitive action: only transitive actions could have no non-trivial G-equivalence relations. Let's look at some examples and nonexamples.

Example 7.13. For $n \geq 2$, the action of $\mathrm{GL}_n(\mathbf{R})$ on $\mathbf{R}^n - \{\mathbf{0}\}$ is transitive but *not* primitive: the one-dimensional subspaces (excluding the origin from them) form a non-trivial $\mathrm{GL}_n(\mathbf{R})$-equivalence relation of $\mathbf{R}^n - \{\mathbf{0}\}$, where $v \sim v'$ when $v' = cv$ for some $c \in \mathbf{R}^\times$.

Example 7.14. When $n \geq 3$ is a composite number, the action of D_n on the vertices of a regular n-gon is transitive but *not* primitive: if $d \mid n$ and $1 < d < n$ then the vertices of the regular d-gons inside the n-gon are the equivalence classes for a non-trivial D_n-equivalence relation on the vertex set.

Example 7.15. If $|X|$ is prime then any transitive action of G on X *is* primitive because a subset $Y \subset X$ such that the gY's partition X has size dividing a prime, so $|Y|$ is 1 or $|X|$. In particular, when p is an odd prime the natural action of D_p is primitive.

To show a transitive action on a set of non-prime size is primitive it is useful to reformulate the condition. Then more examples of primitive actions will easily follow.

Theorem 7.16. *Let G act transitively on X. The following conditions are equivalent:*

(1) *the action is primitive,*
(2) *for some $x \in X$, Stab_x is a maximal subgroup of G,*
(3) *for every $x \in X$, Stab_x is a maximal subgroup of G.*

Proof. Since G acts transitively, stabilizer subgroups of different points in X are conjugate, so (2) and (3) are equivalent to each other. Properties (1) and (2) are equivalent by Theorem 7.5. □

Concretely, a primitive G-action is equivalent to the left multiplication action of G on G/H where H is a maximal subgroup of G.

Example 7.17. We already saw that the natural action of D_n is not primitive when n is composite (Example 7.14). In terms of maximal subgroups, the stabilizer subgroup of the vertex 1 is $\mathrm{Stab}_1 = \{1, s\} = \langle s \rangle$, and if n is composite this subgroup is not maximal: letting $d \mid n$ and $1 < d < n$ we have $\langle s \rangle \subset \langle r^{n/d}, s \rangle \subset \langle r, s \rangle$. When $n = p$ is an odd prime, the natural action of D_p is primitive since the vertex set has prime size (or the subgroup $\langle s \rangle$ has index p in D_p so it is maximal).

Corollary 7.18. *A doubly transitive group action is primitive.*

Proof. Use Theorems 4.19 and 7.16. □

Example 7.19. The natural actions of S_n ($n \geq 3$) and A_n ($n \geq 4$) on $\{1, 2, \ldots, n\}$ are primitive, as is the action of $\mathrm{Aff}(F)$ on F and the actions of $\mathrm{GL}_2(F)$ and $\mathrm{SL}_2(F)$ on the one-dimensional subspaces of F^2.

By Corollary 7.18, doubly transitive actions are special cases of primitive actions. Any primitive action is transitive, so primitivity lies between transitivity and double transitivity. The inclusions are strict, *e.g.*, the natural action of D_n on a regular n-gon ($n \geq 3$) is transitive but not primitive for composite n and is primitive but not doubly transitive for prime n. The natural action of A_3 is primitive (Example 7.15) but not doubly transitive. Table 1 summarizes the situation.

Type	Space
transitive	G/H
primitive	G/H, H maximal
doubly transitive	G/H, $G = H \cup HgH$

TABLE 1. Levels of Transitivity

In a sense, transitive and primitive G-actions are almost "dual" concepts. If G acts on the sets S and T, let a *G-map* from S to T be a function $f\colon S \to T$ that respects the actions: $f(gs) = gf(s)$ for all $g \in G$ and $s \in S$. Then the action of G on a set X is transitive if and only if any G-map *to* X is surjective, while the action on X is primitive if and only if the action is non-trivial and any (nonconstant) G-map *out of* X is injective. (We met G-maps in a concrete setting in Corollary 3.5.)

Theorem 4.9 and Theorem 5.1 (Iwasawa's theorem) generalize from doubly transitive actions to primitive actions, as follows.

Theorem 7.20. *Suppose G acts primitively on a set X. Any normal subgroup $N \lhd G$ acts on X either trivially or transitively.*

Proof. Let $H = \mathrm{Stab}_x$ be the stabilizer of a point in X. Then $H \subset NH \subset G$. Since H is maximal, $NH = H$ or $NH = G$. If $NH = H$ then $N \subset H$, so $N \subset gHg^{-1}$ for all g. Since the stabilizer subgroup of each point in X is conjugate to H, we conclude that N acts trivially on X. Now suppose $NH = G$. Then

$$X = Gx = NHx = Nx,$$

so N acts transitively on X. □

Remark 7.21. Using Theorem 7.20 in place of Theorem 4.9, Lemma 6.1 remains true if the doubly transitive hypothesis is replaced with primitivity, as the reader can check.

Theorem 7.22 (Iwasawa)**.** *Suppose G acts primitively on a set X and, for some $x \in X$, Stab_x has an abelian normal subgroup whose conjugate subgroups generate G. If $[G, G] = G$ then G/K is a simple group, where K is the kernel of the action of G on X.*

Proof. The proof is just like the proof of Theorem 5.1; replace the reference to Theorem 4.9 with Theorem 7.20. □

There are groups whose simplicity is proved using a primitive action that is not doubly transitive, *e.g.*, simplicity of most projective symplectic groups.

Appendix A. Sylow subgroups under intersection and quotient

We prove here a theorem about Sylow subgroups needed in the proof of Corollary 3.5.

Theorem A.1. *Let G be a finite group and N be a normal subgroup.*

1. *If P is a p-Sylow subgroup of G then $P \cap N$ is a p-Sylow subgroup of N.*
2. *PN/N is a p-Sylow subgroup of G/N.*

Proof. (1): The group $P \cap N$ is a p-group since it is contained in P. To show it is a p-Sylow subgroup of N we will show the index $[N : P \cap N]$ is not divisible by p. The set PN is a subgroup of G since $N \lhd G$ and $|PN| = |P||N|/|P \cap N|$, so $[N : P \cap N] = |N|/|P \cap N| = |PN|/|P| = [PN : P]$, which is a factor of $[G : P]$ and thus is not divisible by p. (Here is an alternate proof. By the Sylow theorems $P \cap N$ is contained in a p-Sylow subgroup of N, say K. Then K, being a p-subgroup of G, is contained in a conjugate of P: $K \subset gPg^{-1}$. Thus $g^{-1}Kg \subset P$. Also $g^{-1}Kg \subset g^{-1}Ng = N$, so $g^{-1}Kg \subset P \cap N \subset K$. Since $|K| = |g^{-1}Kg|$, we get $|P \cap N| = |K|$, so $P \cap N = K$ is a p-Sylow subgroup of N.)

(2): First observe that PN/N is a p-group (either because every element has p-power order or because $PN/N \cong P/(P \cap N)$). Using the inclusions

$$G \supset PN \supset N, \quad G \supset PN \supset P,$$

the first one shows $[G/N : PN/N] = [G : PN]$ and the second one shows $[G : PN] \not\equiv 0 \bmod p$. Therefore PN/N is a p-subgroup of G/N whose index is not divisible by p, so PN/N is a p-Sylow subgroup of G/N. □

References

[1] N. Biggs and A. T. White, "Permutation Groups and Combinatorial Structures," Cambridge Univ. Press, Cambridge, 1979.
[2] R. Chapman, An Elementary Proof of the Simplicity of the Mathieu Groups M_{11} and M_{23}, *Amer. Math. Monthly* **102** (1995), 544–545.
[3] J. Dixon and B. Mortimer, "Permutation Groups," Springer-Verlag, New York, 1996.
[4] L. Weisner, Some properties of prime-power groups, *Trans. Amer. Math. Soc.* **38** (1935), 485–492.