8 Group Actions

Actions on Sets

Action: Let G be a multiplicative group and let Ω be a set. An *action of* G *on* Ω is a group homomorphism $G \to Sym(\Omega)$. So, each element $g \in G$ is associated with a permutation of Ω, and for convenience, we let $g(x)$ denote the image of an element $x \in \Omega$ under this permutation. The fact that we have a group homomorphism from G to $Sym(\Omega)$ is equivalent to $g(h(x)) = (gh)(x)$ for $g, h \in G$ and $x \in \Omega$.

Note: above we have defined a *left* action. For a *right* action we would denote the image of x under g by $x \cdot g$ and then $x \cdot (gh) = (x \cdot g) \cdot h$. We will use left actions exclusively.

Examples:

1. The group S_n has a natural action on $[n]$ since each element of S_n is a permutation. More generally $Sym(\Omega)$ acts on Ω.

2. The group $GL(n, \mathbb{F})$ acts on $\mathbb{F}^n$ by matrix multiplication, that is, if $A \in GL(n, \mathbb{F})$ and $\vec{x} \in \mathbb{F}^n$ then $A(\vec{x}) = A\vec{x}$.

3. For any group G, we have that G acts on itself by the rule that $g(x) = gx$ for all $x \in G$ and $g \in G$.

4. For any group G and subgroup $H \leq G$ we define $G/H = \{gH : g \in G\}$, that is, the set of all left H-cosets. Now, G has a natural action on G/H by the rule that $g \in G$ applied to $g'H$ is $gg'H$.

Faithful: We say that the action of G on Ω is *faithful* if the kernel of the homomorphism from G to $Sym(\Omega)$ is trivial. Equivalently, the action is faithful if any two distinct elements $g, h \in G$ give distinct permutations of Ω (otherwise gh^{-1} is in the kernel).

Note: if we have a faithful group action, then we have represented G as a subgroup of $Sym(\Omega)$. If our action is unfaithful, and H is the kernel of our group homomorphism, then $H \triangleleft G$ and G/H has a faithful action on Ω.

Orbit: Let $x \in \Omega$. The *orbit of* x is the set

$$\Omega_x = \{y \in \Omega : g(x) = y \text{ for some } g \in G\}.$$

We let Ω/G denote the set of all orbits.

Stabilizer: The *stabilizer* of $x \in \Omega$ is the set

$$G_x = \{g \in G : g(x) = x\}.$$

Proposition 8.1 *Let $x, y \in \Omega$ let $h \in G$ and assume that $h(x) = y$. Then:*

(i) $\{g \in G : g(x) = y\} = hG_x$

(ii) $G_y = hG_xh^{-1}$

(iii) $|\Omega_x| \cdot |G_x| = |G|$.

Proof: For (i), note that if $g \in G_x$ then $hg(x) = h(x) = y$ (which proves "$\supseteq$") and conversely, if $g(x) = y$ then $h^{-1}g(x) = h^{-1}(y) = x$ so $h^{-1}g \in G_x$ which implies $g \in hG_x$ (thus proving "$\subseteq$"). Similarly for (ii), note that if $g \in G_x$ then $hgh^{-1}(y) = hg(x) = h(x) = y$ (proving "$\supseteq$ ") and conversely if $g \in G_y$ then $h^{-1}gh(x) = h^{-1}g(y) = h^{-1}(y) = x$ which implies $g \in hG_xh^{-1}$ (proving "$\subseteq$"). Part (iii) is an immediate consequence of (i) since each element of Ω which is the image of x under a group element is an image under exactly $|G_x|$ group elements. □

Transitive: The action of G on Ω is *transitive* if there is a single orbit.

Theorem 8.2 *Let G act transitively on Ω. Then there exists $H \leq G$ so that the action of G on Ω is isomorphic to the action of G on G/H.*

Proof: Choose a point $x_0 \in \Omega$ and set $H = G_{x_0}$. Now, apply Proposition 8.1 to choose for every $x_i \in \Omega$ a group element $g_i \in G$ so that g_iH is the subset of G which maps x_0 to x_i. We now show that this correspondence between Ω and G/H yields an isomorphism. For this, we must prove that if $x_i, x_j \in \Omega$ and $h(x_i) = x_j$ then $hg_iH = g_jH$. But this is immediate, if $h(x_i) = x_j$ then $hg_i(x_0) = h(x_i) = x_j$ so $hg_i \in g_jH$ but then $hg_iH = g_jH$. □

Polya Counting

Motivation: How can we count the number of essentially distinct ways of colouring the faces of an Octahedron using $\{red, yellow, blue\}$, where two colourings are considered equivalent if there is a rotational symmetry of the Octahedron which takes one to the other?

Actions on Colourings: Let A, B be finite sets, and let the group G act on A. We regard B as a set of colours, so we think of a function $f : A \to B$ as a colouring of A. Now, the group G inherits an action on the set B^A (the colourings of A) by the rule that $\sigma \in G$ applied to $f \in B^A$ is given by $\sigma(f) = f \circ \sigma^{-1}$. To check this, let $\sigma_1, \sigma_2 \in G$ let $f \in B^A$ and note that

$$(\sigma_2\sigma_1)(f) = f \circ (\sigma_2\sigma_1)^{-1} = f \circ \sigma_1^{-1} \circ \sigma_2^{-1} = \sigma_2(\sigma_1(f))$$

(note here that the $^{-1}$ is necessary to have a group action). In the above problem, A is the set of faces of the Octahedron, G is the rotational symmetry group acting on A, and B is the set of colours $\{red, yellow, blue\}$. Now, two colourings $f, f' \in B^A$ are equivalent if there exists $\sigma \in G$ so that $f' = f \circ \sigma$ or in other words $f' = \sigma^{-1}(f)$. So, the number of essentially different colourings is precisely $|B^A/G|$ (i.e. the number of orbits of the action of G on B^A).

Fixed Points: For every $g \in G$ we let $Fix(g) = \{x \in \Omega : g(x) = x\}$.

Theorem 8.3 (Burnside's Lemma) *If G acts on the finite set Ω then*

$$|\Omega/G| = \frac{1}{|G|} \sum_{g \in G} |Fix(g)|$$

Proof: We have

$$\begin{aligned}\frac{1}{|G|} \sum_{g \in G} |Fix(g)| &= \frac{1}{|G|} \sum_{x \in \Omega} |G_x| \\ &= \sum_{x \in \Omega} \frac{1}{|\Omega_x|} \\ &= |\Omega/G| \qquad \square\end{aligned}$$

Theorem 8.4 (Polya) *Let A, B be finite sets, let G act on A, and let c_k denote the number of group elements $\sigma \in G$ which have exactly k cycles in their action on A. Then*

$$|B^A/G| = \frac{1}{|G|} \sum_{k=1}^{\infty} c_k |B|^k.$$

Proof: Considering the action of G on B^A, we observe that a colouring $f \in B^A$ is a fixed point of $\sigma \in G$ if and only if f is constant on each cycle of σ. It follows that the number of colourings fixed by σ is precisely $|B|^k$ where k is the number of cycles of σ. The theorem follows immediately from this and Burnside's Lemma. □

Problem Solution: The 24 rotational symmetries of the Octahedron consist of:

1. One identity (8 cycles)
2. Six rotations by π about an axis through antipodal edges (4 cycles).
3. Six rotations by $\pm\frac{\pi}{2}$ about an axis through antipodal vertices (2 cycles).
4. Three rotations by π about an axis through antipodal vertices (4 cycles).
5. Eight rotations by $\pm\frac{2\pi}{3}$ about an axis through antipodal faces (4 cycles).

Using the notation from Polya's theorem this gives $c_2 = 6$, $c_4 = 17$ and $c_8 = 1$ so the number of essentially distinct colourings is

$$\frac{1}{24}(6 \cdot 3^2 + 17 \cdot 3^4 + 1 \cdot 3^8) = \frac{1}{24}(54 + 1377 + 6561) = 333$$

The Number Six

Motivating Problem: In what ways can the group S_n act faithfully on a set Ω of size n? There are many obvious actions of this type: just label the points of Ω with $1..n$ and let the permutation $\pi \in S_n$ act accordingly. Could there ever be another such action?

Conjugation: If $g, h \in G$ then we call ghg^{-1} the *conjugate* of h by g. Define a relation on G by declaring two elements to be equivalent if one is a conjugate of the other. It is immediate that this is an equivalence relation and we call the equivalence classes *conjugacy classes.*

Observation 8.5 *A conjugacy class in S_n consists of all permutations with the same cycle structure (i.e. the same number of cycles of each length).*

Proof by Example: Given $\sigma = (123)(4567)(8)(9X)$ and $\tau = (abc)(defg)(h)(ij)$, the function π given by the rule $\pi(1) = a, \pi(2) = b, \ldots, \pi(X) = j$ satisfies $\sigma = \pi^{-1}\tau\pi$. □

Group Automorphism: An *automorphism* of a group G is a group isomorphism $\phi : G \to G$. Let $g \in G$ and let $\phi_g : G \to G$ be given by $\phi_g(x) = gxg^{-1}$. Then $\phi_g(xy) = g(xy)g^{-1} = (gxg^{-1})(gyg^{-1}) = \phi_g(x)\phi_g(y)$ so ϕ_g is an automorphism. We say that any automorphism of this type is *inner* and any other automorphism is *outer*.

Motivating Problem, version 2: We return to the original problem, but now set $\Omega = [n]$. A faithful action of S_n on $[n]$ is, by definition, an injective group homomorphism from S_n to $Sym([n]) = S_n$. So this is precisely a group automorphism of S_n. Now, the "obvious" actions are given by relabeling: if $g \in S_n$ then we may have S_n act on itself by the rule that $x \in S_n$ gives the permutation gxg^{-1}. However, this is precisely an inner automorphism of S_n. So, our motivating problem is equivalent to the question: Does there ever exist an outer automorphism of S_n?

Lemma 8.6 *If ϕ is an automorphism of S_n and ϕ maps the conjugacy class of transpositions to itself, then ϕ is inner.*

Proof: Note that two distinct transpositions commute if and only if they transpose disjoint pairs. Let (a_1a_2) be the image of (12) under ϕ and consider the image of (23) under ϕ. Since (12) and (23) do not commute, we may assume (without loss) that the image of (23) is (a_2a_3). Next, consider the image of (34). This transposition must commute with (ab) but not (bc) so without loss it is (cd). Continuing in this manner we find that $(12), (23), (34), \ldots, (n-1, n)$ map respectively to $(a_1a_2), (a_2a_3), (a_3a_4), \ldots (a_na_{n-1})$. Since the transpositions $(12), (23), \ldots, (n-1n)$ generate S_n (check!) it follows that ϕ is given by the rule $\phi(i) = a_i$. $\square$

Theorem 8.7 *If $n \neq 6$ then there is no outer automorphism of S_n.*

Proof: Consider all conjugacy classes of involutions (elements of order 2). Any group automorphism must map conjugacy classes to conjugacy classes (check!) and must preserve the order of each element (check!) so it follows that every automorphism of S_n sends each conjugacy class of involutions to another conjugacy class of involutions.

Let K_n have vertex set $[n]$. Every involution has the form $(ab)(cd)..(st)(u)(v)..(z)$ so we may identify it with the matching (set of pairwise nonadjecent edges) in K_n consisting of the edges $ab, cd, \ldots, st$. This gives a natural bijection between the conjugacy class of involutions which contain k disjoint transpositions and the set of k edge matchings in K_n. In particular, it is only possible to map the conjugacy class of transpositions to the conjugacy class of involutions with k disjoint transpositions if the number of edges in K_n is equal to the number of k edge matchings in K_n.

To count the number of k edge matchings in K_n, we first choose the $2k$ vertices which are to be covered by the matching edges. This can be done in $\binom{n}{2k}$ ways. Next, we choose a k edge matching on these $2k$ vertices by choosing a pair for the smallest vertex (which can be done in $2k-1$ ways) and then one for the smallest unmatched vertex ($2k-3$ ways), on down. It follows that the total number of k edge matchings in K_n is given by $\binom{n}{2k}(2k-1)(2k-3)\dots(1)$.

It follows from the previous lemma and the above argument that there can only be an outer automorphism of S_n if there exists $k \geq 2$ so that

$$\binom{n}{2} = \binom{n}{2k}(2k-1)(2k-3)\dots(1) \tag{1}$$

If $n - 2k > 2$ then $\binom{n}{2} < \binom{n}{2k}$ and if $n = 2k+2$ then $\binom{n}{2} = \binom{n}{2k}$ but again the right hand side of the equation above is larger than the left. If $n = 2k+1$ then the left hand side is $(2k+1)(k)$ while the right is $(2k+1)(2k-1)(2k-3)\dots(1)$ which is again larger. Thus, the only possibility for equality is when $n = 2k$. In this case the left hand side is $k(2k-1)$ while the right is $(2k-1)(2k-3)\dots(1)$. This implies $(2k-3) \leq k$ so $k \leq 3$. The only possible cases here are $n = 4$ and $k = 2$ (which fails) and $n = 6$ and $k = 3$ which works! □

Theorem 8.8 *There is an outer automorphism of S_6.*

Proof: Again we work with the complete graph K_6 with vertex set $[6]$. We follow Sylvester's notation by calling an edge a *duad*, a 3 edge matching a *syntheme*, and a collection of five pairwise disjoint synthemes (i.e. a 5-edge-colouring) a *pentad*. First observe that every syntheme contains three duad's and every duad is in exactly three synthemes. Since there are $\binom{6}{2} = 15$ duads, there must also be 15 synthemes.

Next consider two disjoint sythemes S, S'. The graph $K_6 \setminus (S \cup S')$ is a 3-prism. Since this graph has just a single 3-edge-colouring, it follows that there is a unique pentad containing S and S'. So, for any syntheme S, we find that S intersects six other synthemes, and of the remaining eight synthemes, they have a natural partition into two sets of size four, each of which form a pentad with S. It follows that each syntheme appears in exactly two pentads.

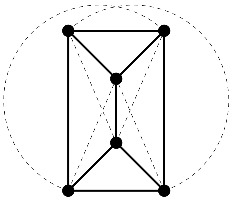

Figure 1: A 3-prism

Since there are exactly 15 synthemes and every pentad contains 5 synthemes, we deduce that the number of pentads is exactly six.

Based on this construction, we now have an action of S_n on the six pentads. If σ is a transposition, then σ does not fix any pentad (check!) and σ^2 is the identity, so σ acts on the pentads by a permutation with cycle structure $(\cdot\cdot)(\cdot\cdot)(\cdot\cdot)$. Labelling the pentads 1..6 yields an outer automorphism of S_6. $\square$

Actions on Structures

Suppose we have a combinatorial structure defined on a ground set Ω. Then we say that a group G acts on this structure if G acts on Ω preserving all properties of the structure.

Examples:

1. If Γ is a graph with vertex set V, we say that a group G acts on Γ if G acts on V preserving adjacency (i.e., if $u, v \in V$ and $g \in G$ then u, v are adjacent if and only if $g(u), g(v)$ are adjacent.)

2. if $P = (X, \leq)$ is a poset we say that G acts on P if G acts on X preserving $\leq$ (i.e., if $x, y \in X$ and $g \in G$ then $x \leq y$ if and only if $g(x) \leq g(y)$.

3. If $I = (V, B, \sim)$ is an incidence structure then we say that G acts on I if there is an action of G on V and an action of G on B which preserves $\sim$ (i.e., if $x \in V$, $\ell \in B$ and $g \in G$ then $x \sim \ell$ if and only if $g(x) \sim g(\ell)$).

Automorphisms: An *automorphism* of a structure on a ground set Ω is a permutation of Ω which preserves all properties of the structure. So, for instance, an automorphism of a graph Γ with vertex set V is a permutation π of V with the property that $u \sim v$ if and only if $\pi(u) \sim \pi(v)$ for every $u, v \in V$. We let $Aut(\Gamma)$ denote the set of automorphisms of G (and we apply similar notation for other structures). Note that $Aut(\Gamma)$ is a group.

PGL: The elements of $PG(n, \mathbb{F})$ are subspaces of $\mathbb{F}^{n+1}$ and there is a natural action of $GL(n+1, \mathbb{F})$ on these subspaces: if V is a subspace of $\mathbb{F}^{n+1}$ and $A \in GL(n+1, \mathbb{F})$ then AV is another subspace of $\mathbb{F}^{n+1}$. It is immediate that this action preserves subspace inclusion, so $GL(n+1, \mathbb{F})$ acts on $PG(n, \mathbb{F})$. Setting $Z = \{sI : s \in \mathbb{F} \setminus \{0\}\}$ we find (check!) that Z is the kernel of this group action (i.e. Z is precisely the set of elements which give the trivial permutation of $PG(n, \mathbb{F})$). We define the *projective general linear group* $PGL(n+1, \mathbb{F}) = GL(n+1, \mathbb{F})/Z$ and note that $PGL(n+1, \mathbb{F})$ acts faithfully on $PG(n, \mathbb{F})$. As with homogeneous coordinates for vectors, we will write elements in $PGL(n+1, \mathbb{F})$ as invertible $(n+1)$-dimensional matrices over $\mathbb{F}$ with the understanding that two such matrices are equivalent if they are scalar multiples.

PSL: The group $SL(n+1, \mathbb{F})$ has a natural action on $PG(n, \mathbb{F})$ (as a subgroup of $GL(n+1, \mathbb{F})$) and setting $Z' = \{sI_{n+1} : s \in \mathbb{F} \setminus \{0\} \text{ and } det(sI_{n+1}) = 1\}$ we find that Z' is the kernel of this action. We define the *projective special linear group* $PSL(n+1, \mathbb{F}) = SL(n+1, \mathbb{F})/Z'$ and note that $PSL(n+1, \mathbb{F})$ acts faithfully on $PG(n, \mathbb{F})$. Note that $|Z'| = |\{s \in \mathbb{F} \setminus \{0\} : s^{n+1} = 1\}|$ which depends on the order of the group (in particular, for $\mathbb{F} = \mathbb{F}_q$ we have $|Z'| = (n+1, q-1)$).

Theorem 8.9 *The group $PSL(n, \mathbb{F}_q)$ is simple whenever $n, q \geq 2$ except for $PSL(2, \mathbb{F}_2) \cong S_3$ and $PSL(2, \mathbb{F}_3) \cong A_4$.*

Projective Line: We call $PG(1, \mathbb{F})$ the *projective line* over $\mathbb{F}$. Using homogeneous coordinates, each point in $PG(1, \mathbb{F})$ may be denoted by a pair $\langle x, y \rangle$ with x, y not both zero. Since these coordinates are invariant under scalar multiples, we may think of $\langle x, y \rangle$ as a slope $\frac{x}{y}$ (indeed this is the familiar notion of slope for graphs of lines in $\mathbb{R}^2$) with the usual convention that $\frac{x}{0} = \infty$. Since slopes form a more convenient labelling of the points, we shall identify $PG(1, \mathbb{F})$ with the set of slopes: $\mathbb{F} \cup \{\infty\}$.

Möbius Transformations: Consider the action of $PGL(2, q)$ on $PG(1, q)$. Using homogeneous coordinates (here as column vectors) we have

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \rightarrow \begin{bmatrix} ax + by \\ cx + dy \end{bmatrix}$$

Interpreting $\langle x, y \rangle$ as a slope $\frac{x}{y}$ we see that this matrix maps $s = \frac{x}{y}$ to $\frac{ax+by}{cx+dy} = \frac{a(x/y)+b}{c(x/y)+d} = \frac{as+b}{cs+d}$ with the interpretations that an output of $\frac{t}{0}$ is ∞ and the input $s = \infty$ goes to $\frac{a}{c}$. These functions are generally called *Möbius Transformations* or *fractional linear transformations.*

Squares: For any field $\mathbb{F}$ we let $\mathbb{F}^{\square} = \{t^2 : t \in \mathbb{F} \setminus \{0\}\}$. It is immediate that $\mathbb{F}^{\square}$ is a multiplicative subgroup of $\mathbb{F} \setminus \{0\}$ which has index 2 if $\mathbb{F} = \mathbb{F}_q$ with q odd.

Special Möbius Transformations: Consider the action of $A \in GL(2, q)$ on $PG(1, \mathbb{F}_q)$. The matrices whose action is equivalent to that of A are precisely $\{tA : t \in \mathbb{F} \setminus \{0\}\}$. If $det(A) = s^2$ then $A' = s^{-1}A \in SL(2, q)$ and has the same action as A. On the other hand, if $det(A) \notin \mathbb{F}^{\square}$ then there is no matrix in $SL(2, q)$ with the same action as A. It follows that we may view the action of $PSL(2, q)$ on $PG(1, \mathbb{F}_q)$ as given by those matrices $A \in GL(2, q)$ with $det(A) \in \mathbb{F}^{\square}$. We call these *special Möbius transformations.*

Note: We now have faithful actions of $PGL(2, q)$ and $PSL(2, q)$ on $q + 1$ points (namely on $PG(1, q) = \mathbb{F}_q \cup \{\infty\}$).

Theorem 8.10 (Galois) *The group $PSL(2, q)$ does not act faithfully on q points except when $q = 5, 7, 11$. Here we have $PSL(2, 5) \cong A_5$ and $PSL(2, 7) \cong GL(3, 2)$.*

High Transitivity

t-homogeneous: We say that a group G acts *t-homogeneously* on Ω if for any two sets X, Y with $|X| = |Y| = t$ there is an element $g \in G$ so that $g(X) = Y$.

t-transitive: We say that a group G acts *t-transitively* on a set Ω if whenever $(x_1, x_2, \ldots, x_t)$ and $(y_1, y_2, \ldots, y_t)$ satisfy $x_i \neq x_j$ and $y_i \neq y_j$ for $i \neq j$, there exists an element $g \in G$ so that $(g(x_1), g(x_2), \ldots, g(x_t)) = (y_1, y_2, \ldots, y_t)$. If there is a unique such element g then we say that G acts *sharply* t-transitively on Ω.

Generalized Stabilizers: If $X \subseteq \Omega$ we let $G_X = \{g \in G : g(X) = X\}$ and if $x_1, \ldots, x_t \in \Omega$ we let $G_{(x_1, x_2, \ldots, x_t)} = \{g \in G : g(x_i) = x_i \text{ for } 1 \leq i \leq k\}$. Note that the proof of (ii) in Propositon 8.1 shows that whenever $h \in G$ satisfies $h(X) = Y$ we have $G_Y = hG_Xh^{-1}$ and whenever $h \in G$ sends x_i to y_i for $1 \leq i \leq t$ we have $G_{(y_1, y_2, \ldots, y_t)} = hG_{(x_1, x_2, \ldots, x_t)}h^{-1}$.

Proposition 8.11 *$PGL(2, \mathbb{F})$ acts sharply 3-transitively on $PG(1, \mathbb{F})$.*

Proof: Let (x, y, z) be a triple of distinct points in $PG(1, \mathbb{F})$. First we shall show that there is a sequence of Möbius transformations which map (x, y, z) to $(\infty, 0, 1)$. If $x \neq \infty$ then the map $s \to \frac{1}{s-x}$ maps x to ∞ and brings our triple to (∞, y', z'). Now, the transform $s \to s - y'$ fixes ∞ and sends y' to 0 bringing our triple to $(\infty, 0, z'')$. Since $z'' \neq 0$ the transform $s \to \frac{1}{z''}s$ now fixes ∞ and 0 and sends z'' to 1 bringing our triple to $(\infty, 0, 1)$ as desired. Composing a function which sends (x, y, z) to $(\infty, 0, 1)$ with the inverse of a function which sends (x', y', z') to $(\infty, 0, 1)$ (in the right order) gives a function which sends (x, y, z) to (x', y', z') thus showing that this action is 3-transitive. To show that this action is sharply 3-transitive, we need only check that $G_{(\infty,0,1)}$ is trivial (why?). However, the transformations which fix ∞ are precisely those of the form $s \to as + b$ (with $a \neq 0$), those that fix $(\infty, 0)$ are precisely those of the form $s \to as$ and thus, only the identity can fix $(\infty, 0, 1)$. □

The Autmorphism Group: For a group G we let $Aut(G)$ denote the set of all group automorphisms of G. Note that if $\phi, \psi \in Aut(G)$ then $\phi \circ \psi \in Aut(G)$, so $Aut(G)$ forms a group under composition.

Examples:

1. Consider the (additive) group $\mathbb{Z}_n$ and let k be relatively prime to n. Then the function $\phi_k : \mathbb{Z}_n \to \mathbb{Z}_n$ given by $\phi_k(a) = ka$ is an automorphism. In this case $Aut(\mathbb{Z}_n) = \mathbb{Z}_n^*$.

2. Consider the (additive) group $G = \mathbb{Z}_2 \times \mathbb{Z}_2$. This group has exactly three nonidentity elements, say α, β, γ, each is its own inverse, and the sum of any two is the third. It follows that any bijection from G to itself which fixes the identity is an automorphism, so $Aut(G) \cong S_3$.

3. If $n \neq 6$ then every automorphism of S_n is of the form $\phi_g(x) = gxg^{-1}$ for some $g \in S_n$. Then $\phi_g \circ \phi_h(x) = g(hxh^{-1})g^{-1} = (gh)x(gh)^{-1} = \phi_{gh}(x)$. It follows that $Aut(S_n) \cong S_n$.

Centralizers & Normalizers: Let G be a group and let $S \subseteq G$. We let

$$Z(S) = \{g \in G : gs = sg \text{ for every } s \in S\}$$
$$N(S) = \{g \in G : gS = Sg\}$$

It is immediate from the definitions that $Z(S) \leq N(S) \leq G$.

Lemma 8.12 *If $H \leq G$ then $Z(H) \lhd N(H)$ and $N(H)/Z(H)$ is isomorphic to a subgroup of $Aut(H)$.*

Proof: Consider the action of $N(H)$ on H by the rule that $g \in N(H)$ applied to $x \in H$ is given by $g(x) = gxg^{-1}$. The Kernel of this action is $Z(H)$, so it follows that $N(H)/Z(H)$ is embedded in $Aut(H)$ (i.e. isomorphic to a subgroup of). □

Lemma 8.13 *If G acts sharply 4-transitively on X then $|X| \leq 11$.*

Proof: We may assume (without loss) that $X = [n]$ and then associate G with its image in S_n and let ι denote the identity permutation. We begin the proof with two easy claims.

Claim 1: If $\delta, \epsilon \in G$ commute then δ fixes the set $\{x \in X : \epsilon(x) = x\}$

This is immediate, if $\epsilon(x) = x$ and $\delta(x) = y$ then we have $y = \delta\epsilon(x) = \epsilon\delta(x) = \epsilon(y)$ so y is also a fixed point of ϵ.

Claim 2: If $\delta, \epsilon \in G$ have order two, they are conjugate.

Now, since only the identity fixes four points, we may assume that δ has cycle structure $(12)(34)\ldots$ and that ϵ has cycle structure $(ab)(cd)\ldots$. Now choose an element $\phi \in G$ so that $\phi(1) = a$, $\phi(2) = b$, $\phi(3) = c$ and $\phi(4) = d$. Now we have that $\delta\phi^{-1}\epsilon\phi$ fixes $1, 2, 3, 4$ so it is the identity. Thus $\delta = \phi^{-1}\epsilon\phi$ and these elements are conjugate as desired.

Now, let α, β, γ be the unique elements of G with $\alpha = (1)(2)(34)\ldots$, $\beta = (12)(3)(4)\ldots$, and $\gamma = (12)(34)\ldots$. Then $\alpha^2, \beta^2, \gamma^2$ all fix the first four elements, so they are the identity. Furthermore $H = \{\iota, \alpha, \beta, \gamma\}$ is a subgroup of G which is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$. If α has a fixed point other than 1,2, then we shall denote it by ∞. Note that since α, β, γ commute it follows from the first claim that if ∞ exists, then it is also fixed by β and γ. Now, γ must fix two other points $5, 6 \neq \infty$ (since it is conjugate to α - and therefore has the same cycle structure). It then follows that $\alpha = (1)(2)(34)(56)\ldots$, $\beta = (12)(3)(4)(56)\ldots$, $\gamma = (12)(34)(5)(6)\ldots$.

Next we shall prove that $Z(H) = H$. To see this, suppose that $\delta \in Z(H)$. Now by the first claim δ must fix the sets $\{1, 2, \infty\}$, $\{3, 4, \infty\}$, $\{5, 6, \infty\}$ so it must be that δ fixes ∞ (if it exists) and either transposes or fixes each of $\{1, 2\}$, $\{3, 4\}$, $\{5, 6\}$. If it fixes two of these sets, then $\delta = \iota$, and otherwise it has the same behavior as one of α, β, γ on 4 elements. Thus

$\delta \in H$ as desired. It now follows from the previous lemma that $N(H)/Z(H) = N(H)/H$ is isomorphic to a subgroup of $Aut(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong S_3$ so in particular, $|N(H)| \leq 24$.

Now, set $W = \{1, 2, 3, 4, 5, 6, \infty\}$ and consider the action of H on X. Since W is a union of orbits which contains all fixed points of α, β, γ it follows that every other orbit has size exactly four, say $Y = \{a, b, c, d\}$ and each of α, β, γ gives a distinct permutation on Y with two cycles of size two. Let $K = G_Y$. Now, by assumption, $K \cong S_4$ and $H \leq K$. But then $H \lhd K$ so it must be that $K = N(H)$. Now, choose an element $\nu \in N(H) \setminus H$ with order 2. It then follows that ν must fix two points in Y an transpose the other two. If $|X| \geq 12$ then the action of H on X must have another orbit $Y' \subseteq X \setminus (W \cup Y)$ of size four, and by the same argument, the element ν must fix two points in Y' and transpose the other two. But then ν has four fixed points, giving us a contradiction. It follows that $|X| \leq 11$ as claimed. □

Theorem 8.14 *If G acts 4-transitively on X and does not give the set of all or all even permutations of X, then one of the following holds (here M_n denotes a* Matthieu *Group):*

(i) $|X| = 11$ *and* $G \cong M_{11}$ *and the action is sharply 4-transitive*

(ii) $|X| = 12$ *and* $G \cong M_{12}$ *and the action is sharply 5-transitive*

(iii) $|X| = 23$ *and* $G \cong M_{23}$

(iv) $|X| = 24$ *and* $G \cong M_{24}$ *and the action is 5-transitive.*