MATH5353

Harley Caham Combest

Fa2025 Ch4 Group Actions

Ch 4: Historical Context

Overview. These are designed to test your memory on a few selected historical points on the basics of group actions as presented in Ch4 of Dummit and Foote.

Development 1. From permutations to actions (early–mid 19th century)

- **Who.** Augustin-Louis Cauchy (1815–1840s), Évariste Galois (1830s), Arthur Cayley (1854), Camille Jordan (1870s).
- **What.** Groups first appeared concretely as *permutation* groups acting on roots of equations; later abstracted into axiomatic groups acting on arbitrary sets.
- **When/Where.** France (Galois, Cauchy, Jordan) and Britain (Cayley), 1830–1875.
- **Why.** Studying how symmetries *move* objects reveals structure not visible from elements alone.
- **How.** Shift from "a group *is* permutations" to "a group *acts* by permutations on a set," setting up orbits, stabilizers, and kernels.

Development 2. Cayley's Theorem and permutation representations (1854)

- **Who.** Arthur Cayley.
- **What.** Every group embeds into a symmetric group via left translation; actions correspond to homomorphisms into S_A.
- **Why.** Connects abstract groups to concrete permutations, giving a universal model for actions.
- **How.** Map $g \mapsto$ permutation of G given by $x \mapsto gx$; generalize to actions on cosets G/H to produce permutation representations.

Development 3. Orbits, stabilizers, and the counting paradigm (late 19th century)

- **Who.** Jordan; later popularized across texts by Burnside et al.
- **What.** The orbit–stabilizer principle: $|G \cdot a| = |G : G_a|$; partition of a set into orbits under a group's action.
- **Why.** Converts algebra to arithmetic: sizes of orbits and stabilizers control structure and counting.
- **How.** Equivalence relation "$a \sim b$ iff $a = g \cdot b$" partitions the set; bijection with cosets gives the index formula.

Development 4. Conjugation, centralizers, and the class equation (late 19th century)

- **Who.** Jordan; later systematized in early group theory texts.
- **What.** Action of G on itself by conjugation; conjugacy classes; centralizers $C_G(g)$ and normalizers $N_G(H)$.
- **Why.** Decomposes G into conjugacy classes; *class equation* relates $|G|$ to $|Z(G)|$ and orbit sizes.
- **How.** Apply orbit–stabilizer to conjugation: $|\mathrm{Cl}(g)| = |G : C_G(g)|$; sum over classes to get the class equation.

Development 5. Sylow's Theorems via actions (1872)

- **Who.** Ludwig Sylow (1872).
- **What.** Existence, conjugacy, and number of Sylow p-subgroups; $n_p \equiv 1 \pmod{p}$ and $n_p \mid m$ for $|G| = p^a m$.
- **Why.** Keystone for classifying finite groups and forcing normal subgroups in many orders.
- **How.** Let G act by conjugation on its p-subgroups and on coset spaces G/H; orbit–stabilizer and counting give the congruences.

Development 6. Beyond sets: actions on algebraic structures and representation theory (1890s–20th century)

- **Who.** Ferdinand Frobenius (1896–1899) and successors; later Noether, Artin, and many others.
- **What.** From set actions to linear actions (representations) on vector spaces; automorphism groups acting on subgroups; characteristic and normal subgroups via action.
- **Why.** Linearizing actions unlocks powerful tools (characters, modules) and connects groups to geometry and number theory.
- **How.** Homomorphisms $G \to \mathrm{GL}(V)$; restriction to substructures yields $N_G(H)/C_G(H) \hookrightarrow \mathrm{Aut}(H)$; simplicity tests via conjugation actions (e.g., A_n).

Ch 4: Lingua Franca

Overview. These are designed to test your memory on the tools of the trade: the words, the axioms, the theorems, etc of the basics of Group Actions as presented in Ch4 of Dummit and Foote.

4pt1.

Definition.: Kernel of an action; stabilizer of a point; faithful action

(1) The kernel of the action is the set of elements of G that act trivially on every element of A: $\{g \in G \mid g \cdot a = a \text{ for all } a \in A\}$.
(2) For each $a \in A$ the stabilizer of a in G is the set of elements of G that fix a: $\{g \in G \mid g \cdot a = a\}$ and is denoted by G_a.
(3) An action is faithful if its kernel is the identity.

Proposition.: Bijection between G-actions on A and homomorphisms $G \to S_A$

Giving an action of G on A is equivalent to giving a homomorphism $\varphi : G \to S_A$, where $\varphi(g)$ is the permutation $a \mapsto g \cdot a$. The kernel of the action equals $\ker \varphi = \{g \in G : \varphi(g) = \mathrm{id}_A\} = \bigcap_{a \in A} G_a$.

. . . . . .

Intuition. The action axioms translate exactly to homomorphism laws: e acts as id_A and (gh) acts as the composition of g and h, so "an action is a homomorphism into permutations."

. . . . . .

Proof.

Step 1 (Action $\Rightarrow$ homomorphism). Define $\varphi(g)(a) = g \cdot a$. Then $\varphi(e) = \mathrm{id}_A$ and $\varphi(gh) = \varphi(g)\varphi(h)$ by the action axioms.

Step 2 (Homomorphism $\Rightarrow$ action). Given $\varphi : G \to S_A$, set $g \cdot a := \varphi(g)(a)$. Then $e \cdot a = a$ and $(gh) \cdot a = \varphi(g)(\varphi(h)(a)) = g \cdot (h \cdot a)$.

Step 3 (Kernel identification). g fixes every a iff $\varphi(g) = \mathrm{id}_A$, hence $\ker(\text{action}) = \ker \varphi = \bigcap_{a \in A} G_a$.

Definition.: Permutation representation of a group

A *permutation representation* of G on a nonempty set A is any homomorphism $\varphi : G \to S_A$. An action of G on A affords such a representation via $g \mapsto (a \mapsto g \cdot a)$.

Proposition.: The orbit relation is an equivalence; $|G \cdot a| = [G : G_a]$ (finite G gives $|G \cdot a|\,|G_a| = |G|$)

Define $a \sim b$ iff $b = g \cdot a$ for some $g \in G$. Then $\sim$ is an equivalence relation, and the equivalence class of a is the orbit $G \cdot a$. Moreover the map $\theta : G/G_a \to G \cdot a$, $\theta(gG_a) = g \cdot a$, is a well-defined bijection; hence $|G \cdot a| = [G : G_a]$ and (if G is finite) $|G \cdot a|\,|G_a| = |G|$.

. . . . . .

Intuition. "Reachability under the action" behaves like sameness (equivalence). Distinct cosets of G_a encode distinct ways to move a, so orbit size equals index.

. . . . . .

Proof.

Step 1 (Equivalence). Reflexive: $a = e \cdot a$. Symmetric: if $b = g \cdot a$ then $a = g^{-1} \cdot b$. Transitive: if $c = h \cdot b$ and $b = g \cdot a$, then $c = (hg) \cdot a$.

Step 2 (Well-defined map). If $gG_a = hG_a$, then $h^{-1}g \in G_a$, hence $(h^{-1}g) \cdot a = a$ and $g \cdot a = h \cdot a$, so θ is well-defined.

Step 3 (Bijectivity). Surjective: for $b \in G \cdot a$, pick g with $g \cdot a = b$; then $\theta(gG_a) = b$. Injective: if $\theta(gG_a) = \theta(hG_a)$, then $g \cdot a = h \cdot a$, so $h^{-1}g \in G_a$ and $gG_a = hG_a$.

Step 4 (Cardinality). Bijectivity gives $|G \cdot a| = [G : G_a]$ and, for finite G, $|G \cdot a|\,|G_a| = |G|$.

Definition.: Orbit and transitive action

For $a \in A$, the *orbit* is $G \cdot a = \{g \cdot a \mid g \in G\}$. The action is *transitive* if there is only one orbit, i.e., for all $a, b \in A$ there exists $g \in G$ with $g \cdot a = b$.

4pt2.

GROUPS ACTING ON THEMSELVES BY LEFT MULTIPLICATION - CAYLEY'S THEOREM

Definition.: Left regular action of G on itself

Let G act on itself by left multiplication: for $g, a \in G$, set $g \cdot a := ga$. If G is written additively, this reads $g \cdot a = g + a$ and is called *left translation*.

Example.: Klein 4–group $V_4 = \{1, a, b, c\}$ under left regular action

Label $1, a, b, c$ by $1, 2, 3, 4$ respectively. Compute the permutation for a:

$a{\cdot}1 = a \Rightarrow a_a(1) = 2, \quad a{\cdot}a = 1 \Rightarrow a_a(2) = 1, \quad a{\cdot}b = c \Rightarrow a_a(3) = 4, \quad a{\cdot}c = b \Rightarrow a_a(4) = 3,$

so $a \mapsto (1\ 2)(3\ 4)$. Similarly,

$$a \mapsto (1\ 2)(3\ 4), \qquad b \mapsto (1\ 3)(2\ 4), \qquad c \mapsto (1\ 4)(2\ 3).$$

Thus the associated permutation representation embeds V_4 into S_4 as $\langle (1\ 2)(3\ 4), (1\ 3)(2\ 4) \rangle$.

Definition.: Coset action $G \curvearrowright G/H$ by left multiplication

For $H \leq G$, let A be the set of left cosets of H in G. Define $g \cdot aH := (ga)H$. This satisfies the axioms of a group action. When $H = \{1\}$ this reduces to the left regular action on G.

Example.: $D_8 = \langle r, s \mid r^4 = s^2 = 1,\ srs = r^{-1} \rangle$ acting on the cosets of $\langle s \rangle$

Let $H = \langle s \rangle$. Label the distinct left cosets $1H, rH, r^2H, r^3H$ by $1, 2, 3, 4$. Then

$$s \cdot 1H = sH = 1H \Rightarrow a_s(1) = 1, \quad s \cdot rH = srH = r^3H \Rightarrow a_s(2) = 4,$$

$$s \cdot r^2H = sr^2H = r^2H \Rightarrow a_s(3) = 3, \quad s \cdot r^3H = sr^3H = rH \Rightarrow a_s(4) = 2,$$

so $s \mapsto (2\ 4)$ and $r \mapsto (1\ 2\ 3\ 4)$. Since the representation is a homomorphism, this determines the image of all elements.

Theorem.: For $G \curvearrowright G/H$ by left multiplication: (1) the action is transitive; (2) $\mathrm{Stab}_G(1H) = H$; (3) $\ker(\text{action}) = \bigcap_{x \in G} xHx^{-1}$ (the core of H in G)

Let G act on $A = G/H$ by $g \cdot aH = (ga)H$. Then:

1. G acts transitively on A;
2. $\mathrm{Stab}_G(1H) = H$;
3. $\ker(G \curvearrowright A) = \bigcap_{x \in G} xHx^{-1}$, the largest normal subgroup of G contained in H.

. . . . . .

Intuition. Multiply aH by ba^{-1} to land on bH (transitivity). Fixing $1H$ means $gH = H$, i.e., $g \in H$ (stabilizer). Acting trivially on every coset forces $x^{-1}gx \in H$ for all x—precisely membership in the core.

. . . . . .

Proof.

Step 1 (Transitivity). For any $aH, bH \in A$, take $g = ba^{-1}$; then $g \cdot aH = (ba^{-1})aH = bH$.

Step 2 (Stabilizer of $1H$). By definition, $\mathrm{Stab}(1H) = \{g \in G : g \cdot 1H = 1H\} = \{g : gH = H\} = H$.

Step 3 (Kernel $\subseteq$ core). If g is in the kernel, then $g \cdot xH = xH$ for all x, i.e., $(gx)H = xH$. Thus $x^{-1}gx \in H$ for all x, so $g \in \bigcap_{x \in G} xHx^{-1}$.

Step 4 (Core $\subseteq$ kernel). If $g \in \bigcap_{x \in G} xHx^{-1}$, then $x^{-1}gx \in H$ for all x, hence $(gx)H = xH$ for all x, so g fixes every coset; thus g lies in the kernel.

Step 5 (Largest normal in H). If $N \trianglelefteq G$ with $N \leq H$, then $xNx^{-1} \leq xHx^{-1}$ for all x, so $N \leq \bigcap_{x \in G} xHx^{-1}$; hence the core is the largest normal subgroup of G contained in H.

Corollary.: (Cayley's Theorem) Every group G is isomorphic to a subgroup of a symmetric group; if $|G| = n$, then $G \hookrightarrow S_n$

Apply the theorem with $H = \{1\}$ to obtain the left regular representation $\pi : G \to S_G$. Since $\ker \pi \subseteq H = \{1\}$, the kernel is trivial and π is injective. If $|G| = n$, identify G with $\{1, \ldots, n\}$ to view $\pi(G) \leq S_n$.

. . . . . .

Intuition. "Let G act on itself by left translation." Distinct elements translate differently, so the action yields an embedding into permutations.

. . . . . .

Proof.

Step 1 (Define the map). $\lambda : G \to S_G$, $\lambda(g)(x) = gx$, is a homomorphism since $\lambda(gh)(x) = ghx = \lambda(g)(\lambda(h)(x))$.

Step 2 (Injective). If $\lambda(g) = \mathrm{id}$, then $gx = x$ for all x; taking $x = e$ gives $g = e$. Hence $\ker \lambda = \{e\}$ and $G \cong \lambda(G) \leq S_G$.

Step 3 (S_n model). If $|G| = n$, fix a bijection $G \leftrightarrow \{1, \ldots, n\}$ to regard $\lambda(G) \leq S_n$.

Corollary.: If G is finite and p is the smallest prime dividing $|G|$, then every subgroup of index p is normal

Let $H \leq G$ with $[G : H] = p$. Let $\pi_H : G \to S_{G/H} \cong S_p$ be the coset action. Put $K = \ker \pi_H$ and set $[H : K] = k$. Then $[G : K] = [G : H][H : K] = pk$. Since $\pi_H(G) \leq S_p$, by Lagrange $pk = |G/K| \mid p!$, so $k \mid (p-1)!$. All prime divisors of k are $\geq p$ by minimality of p, forcing $k = 1$ and thus $H = K \trianglelefteq G$.

. . . . . .

Intuition. The coset action lands in S_p; divisibility bounds squeeze the index of the kernel down to 1, so H equals the kernel and is normal.

. . . . . .

Proof.

Step 1 (Coset action). Let $\pi_H : G \to S_{G/H}$ be the action; its kernel K satisfies $[G : K] = |\pi_H(G)|$.

Step 2 (Index factorization). Since $[G : H] = p$ and $[H : K] = k$, we have $[G : K] = [G : H]\,[H : K] = pk$.

Step 3 (Image in S_p). $\pi_H(G) \leq S_p$ so $pk = [G : K] = |\pi_H(G)| \mid p!$, hence $k \mid (p-1)!$.

Step 4 (Minimal prime squeeze). Any prime dividing k is $\geq p$ (by minimality of p), but all primes dividing $(p-1)!$ are $< p$; thus $k = 1$.

Step 5 (Normality). $k = 1$ gives $H = K = \ker \pi_H \trianglelefteq G$, so H is normal.

4pt3.

GROUPS ACTING ON THEMSELVES BY CONJUGATION-THE CLASS EQUATION

Definition.: Conjugation action; conjugate elements; conjugacy class

Let G act on itself by *conjugation*: $g \cdot a := gag^{-1}$ for $g, a \in G$. Two elements $a, b \in G$ are *conjugate* if $b = gag^{-1}$ for some $g \in G$. The orbits of this action are the *conjugacy classes*. [§4.3]

Proposition.: Number of conjugates equals index of the normalizer; for an element, index of the centralizer

For any subset $S \subseteq G$, the number of distinct conjugates gSg^{-1} equals $[G : N_G(S)]$, where $N_G(S) = \{g \in G : gSg^{-1} = S\}$ is the normalizer. In particular, for $s \in G$, the number of conjugates of s equals $[G : C_G(s)]$, where $C_G(s) = \{g \in G : gs = sg\}$ is the centralizer. [§4.3, Prop. 6]

. . . . . .

Intuition. Conjugating S by g depends only on the coset $gN_G(S)$; different cosets yield different conjugates. For a single element s, "staying the same under conjugation" is exactly commuting with s—the centralizer.

. . . . . .

Proof.

Step 1 (Orbit–stabilizer for subsets). Consider the action $G \curvearrowright \mathcal{P}(G)$ by $g \cdot S = gSg^{-1}$. The stabilizer of S is $N_G(S)$ by definition.

Step 2 (Count conjugates). The orbit of S has size $[G : N_G(S)]$ by orbit–stabilizer, giving the first claim.

Step 3 (Element case). For $S = \{s\}$, the stabilizer is $N_G(\{s\}) = C_G(s)$ since $g\{s\}g^{-1} = \{s\}$ iff $gsg^{-1} = s$. Thus the number of conjugates of s is $[G : C_G(s)]$.

Theorem.: The Class Equation

Let G be finite. Let $g_1, \ldots, g_r$ represent the distinct noncentral conjugacy classes. Then

$$|G| = |Z(G)| + \sum_{i=1}^{r} [\, G : C_G(g_i) \,].$$

[§4.3, Thm. 7]

. . . . . .

Intuition. Partition G into its conjugacy classes. Central elements contribute $|Z(G)|$ many 1-element classes; each noncentral class size is an index of a centralizer by the previous proposition.

. . . . . .

Proof.

Step 1 (Partition). The conjugation action partitions G into disjoint conjugacy classes; sum of their sizes equals $|G|$.

Step 2 (Central classes). If $x \in Z(G)$, its class is $\{x\}$; all central elements contribute $|Z(G)|$.

Step 3 (Noncentral classes). For a representative $g_i \notin Z(G)$, its class size is $[G : C_G(g_i)]$ by the proposition.

Step 4 (Sum). Summing over all classes gives the displayed equation.

Theorem.: If $|P| = p^a$ with p prime and $a \geq 1$, then $Z(P) \neq 1$

For a finite p-group P, the center is nontrivial. [§4.3, Thm. 8]

. . . . . .

Intuition. In the class equation, each noncentral class size divides p; modulo p the sum of noncentral class sizes vanishes, forcing $p \mid |Z(P)|$.

. . . . . .

Proof.

Step 1 (Class equation mod p). Write $|P| = |Z(P)| + \sum[P : C_P(x_i)]$ over noncentral representatives x_i.

Step 2 (Divisibility). Each index $[P : C_P(x_i)]$ is divisible by p since $C_P(x_i) \neq P$ in a p-group.

Step 3 (Conclusion). Reducing mod p gives $|Z(P)| \equiv |P| \equiv 0 \pmod{p}$, hence $|Z(P)| \geq p$, so $Z(P) \neq 1$.

Corollary.: If $|P| = p^2$ then P is abelian; hence $P \cong \mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \times \mathbb{Z}_p$

Every group of order p^2 is abelian; consequently it is cyclic of order p^2 or the elementary abelian group of order p^2. [§4.3, Cor. 9]

. . . . . .

Intuition. The center has order p or p^2. If $|Z(P)| = p^2$ we are done; if $|Z(P)| = p$, then the quotient $P/Z(P)$ is cyclic of order p, forcing P abelian.

. . . . . .

Proof.

Step 1 (Center size). By the theorem, $|Z(P)| \in \{p, p^2\}$.

Step 2 (Quotient cyclic). If $|Z(P)| = p$, then $|P/Z(P)| = p$, hence $P/Z(P)$ is cyclic.

Step 3 (Cyclic-quotient test). If $P/Z(P)$ is cyclic, then P is abelian.

Step 4 (Classification). An abelian group of order p^2 is either $\mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \times \mathbb{Z}_p$.

Proposition.: Conjugation in S_n acts by relabelling symbols in the cycle decomposition

If $\sigma, \tau \in S_n$ and the cycle decomposition of σ is written out, then $\tau\sigma\tau^{-1}$ is obtained by applying τ to each symbol appearing in those cycles, preserving cycle structure. [§4.3, Prop. 10]

. . . . . .

Intuition. Conjugation transports the action: if $\sigma(i) = j$, then $(\tau\sigma\tau^{-1})(\tau(i)) = \tau(j)$—same arrows, relabelled.

. . . . . .

Proof.

Step 1 (Arrow transport). From $\sigma(i) = j$ compute $(\tau\sigma\tau^{-1})(\tau(i)) = \tau(\sigma(i)) = \tau(j)$.

Step 2 (Cycle preservation). Thus each successor relation in the cycle notation is relabelled by τ, giving the stated description.

Proposition.: Two permutations in S_n are conjugate iff they have the same cycle type; the number of conjugacy classes equals the number of partitions of n

Permutations of the same cycle type are conjugate in S_n, and conversely. Hence conjugacy classes in S_n correspond bijectively to partitions of n. [§4.3, Prop. 11]

. . . . . .

Intuition. Conjugation permutes labels without changing cycle lengths; conversely, align equal-length cycles (including 1-cycles) to build a permutation that conjugates one decomposition to the other.

. . . . . .

Proof.

Step 1 (Only-if). By the previous proposition, conjugates have identical cycle lengths, so cycle type is preserved.

Step 2 (If). Order the cycles of each permutation by nondecreasing length (including 1-cycles). Define τ mapping the ith symbol in the first list to the ith in the second.

Step 3 (Conjugation works). By Step 2 and Prop. 10, $\tau\sigma_1\tau^{-1} = \sigma_2$. Thus they are conjugate.

Step 4 (Counting classes). Each partition of n yields a unique cycle type; hence the number of conjugacy classes equals the number of partitions of n.

Theorem.: A_5 is a simple group

A_5 has no proper, nontrivial normal subgroups. [§4.3, Thm. 12]

. . . . . .

Intuition. List the conjugacy classes inside A_5 using the conjugation-action facts from §4.3. The possible normal subgroups are unions of whole A_5-classes (plus $\{1\}$). The class sizes in A_5 are 20 (all 3-cycles), 12 and 12 (the two 5-cycle classes), and 15 (all double transpositions). No nonempty proper union of these sizes sums to a divisor of 60, so no proper nontrivial normal subgroup can exist.

. . . . . .

Proof.

Step 1 (Conjugacy classes in A_5). In S_5, a 3-cycle has centralizer of order $3(5-3)! = 6$, so its class has $120/6 = 20$ elements; all 3-cycles are even, hence lie in A_5. They remain a single A_5-class (Exercise/Prop. on S_n-conjugacy relabelling).

Step 2 (Five-cycles split). A 5-cycle in S_5 has centralizer of order 5, so its class in S_5 has $120/5 = 24$ elements; all 5-cycles are even. In A_5 this class splits into two classes of size 12 (a 5-cycle is not A_5-conjugate to its square).

Step 3 (Double transpositions). The S_5-elements of type $(ab)(cd)$ are even; there are 15 of them and they form a single A_5-class (centralizer/normalizer count from §4.3).

Step 4 (Class equation in A_5). Thus the A_5-classes are:

$$\{1\}, \quad \text{one class of 20 (3-cycles)}, \quad \text{two classes of 12 (5-cycles)}, \quad \text{one class of 15 } ((ab)(cd)).$$

Indeed $1 + 20 + 12 + 12 + 15 = 60 = |A_5|$.

Step 5 (Normal-subgroup test). Let $1 \neq N \trianglelefteq A_5$. Then N is a union of whole conjugacy classes together with $\{1\}$. The possible nonempty sums from $\{20, 12, 12, 15\}$ are

$$20,\ 12,\ 15,\ 32,\ 27,\ 24,\ 44,\ 35,\ 39,\ 59,$$

none of which divides 60. Hence no such proper N exists.

Step 6 (Conclusion). The only normal subgroups of A_5 are $\{1\}$ and A_5; therefore A_5 is simple.

Definition.: Right group action; conjugation as a right action

A *right action* of G on A is a map $A \times G \to A$, $(a, g) \mapsto a \cdot g$, with $(a \cdot g_1) \cdot g_2 = a \cdot (g_1 g_2)$ and $a \cdot 1 = a$. Conjugation is often written as a right action via $a \cdot g := g^{-1} a g$; the left and right conjugation actions have the same orbits. [§4.3, Right Group Actions]

4pt4.

AUTOMORPHISMS

Definition.: Automorphism; the group $\mathrm{Aut}(G)$

Let G be a group. An isomorphism from G onto itself is called an *automorphism* of G. The set of all automorphisms of G is denoted $\mathrm{Aut}(G)$. It is a group under composition, and since automorphisms are permutations of the set G, we have $\mathrm{Aut}(G) \leq S_G$. [§4.4]

Proposition.: If $H \trianglelefteq G$, then G acts by conjugation on H as automorphisms; the induced homomorphism $G \to \mathrm{Aut}(H)$ has kernel $C_G(H)$

Let $H \trianglelefteq G$. For each $g \in G$, conjugation $\varphi_g : H \to H$, $\varphi_g(h) = ghg^{-1}$, is an automorphism of H. The action $G \curvearrowright H$ by conjugation affords a homomorphism $\psi : G \to \mathrm{Aut}(H)$, $g \mapsto \varphi_g$, with kernel $C_G(H) = \{g \in G : gh = hg \ \forall h \in H\}$. Hence $G/C_G(H) \cong \psi(G) \leq \mathrm{Aut}(H)$. [§4.4, Prop. 13]

. . . . . .

Intuition. Normality makes conjugation by any g land back in H. Conjugation respects multiplication, so each φ_g is an automorphism. Fixing every $h \in H$ is exactly commuting with H, i.e., lying in $C_G(H)$.

. . . . . .

Proof.

Step 1 (Well-defined action). Since $H \trianglelefteq G$, $ghg^{-1} \in H$ for all $h \in H$, so $g \cdot h := ghg^{-1}$ defines $G \curvearrowright H$.

Step 2 (Automorphism). For fixed g, φ_g has inverse $\varphi_{g^{-1}}$ and $\varphi_g(hk) = ghkg^{-1} = (ghg^{-1})(gkg^{-1})$, so $\varphi_g \in \mathrm{Aut}(H)$.

Step 3 (Homomorphism). $\psi(gh) = \varphi_{gh} = \varphi_g \circ \varphi_h$, hence $\psi : G \to \mathrm{Aut}(H)$ is a homomorphism.

Step 4 (Kernel). $\ker \psi = \{g : \varphi_g = \mathrm{id}_H\} = \{g : ghg^{-1} = h \ \forall h \in H\} = C_G(H)$.

Step 5 (Image). By the First Isomorphism Theorem, $G/C_G(H) \cong \psi(G) \leq \mathrm{Aut}(H)$.

Corollary.: For any subgroup $K \leq G$ and any $g \in G$, $K \cong gKg^{-1}$; conjugate elements and conjugate subgroups have the same order

Conjugation by $g \in G$ is an automorphism of G, hence restricts to an isomorphism $K \to gKg^{-1}$; in particular, orders are preserved under conjugacy. [§4.4, Cor. 14]

. . . . . .

Intuition. Conjugation is a relabelling that preserves the multiplication table.

. . . . . .

Proof.

Step 1 (Restriction). The map $x \mapsto gxg^{-1}$ sends K bijectively onto gKg^{-1}.

Step 2 (Homomorphism). $(gxg^{-1})(gyg^{-1}) = g(xy)g^{-1}$, so it's an isomorphism. Orders are preserved under isomorphism.

Corollary.: $N_G(H)/C_G(H) \cong$ a subgroup of $\mathrm{Aut}(H)$; in particular $G/Z(G) \leq \mathrm{Aut}(G)$

Since $H \trianglelefteq N_G(H)$, Proposition 13 applied in $N_G(H)$ gives a homomorphism $N_G(H) \to \mathrm{Aut}(H)$ with kernel $C_G(H)$, so $N_G(H)/C_G(H) \leq \mathrm{Aut}(H)$. Taking $H = G$ yields $G/Z(G) \leq \mathrm{Aut}(G)$. [§4.4, Cor. 15]

. . . . . .

Intuition. Only elements that normalize H induce permutations of H by conjugation; those that centralize H act trivially.

. . . . . .

Proof.

Step 1 (Apply Prop. 13). Use $N_G(H) \curvearrowright H$ by conjugation; kernel $= C_G(H)$.

Step 2 (Quotient). First Isomorphism Theorem gives $N_G(H)/C_G(H) \leq \mathrm{Aut}(H)$. For $H = G$, $N_G(G) = G$ and $C_G(G) = Z(G)$.

Definition.: Inner automorphism; the subgroup $\mathrm{Inn}(G)$

For $g \in G$, conjugation by g is called an *inner automorphism*. The subgroup of $\mathrm{Aut}(G)$ consisting of all inner automorphisms is denoted $\mathrm{Inn}(G)$. By Corollary 15, $\mathrm{Inn}(G) \cong G/Z(G)$. [§4.4]

Example.: Inner automorphisms and centers in common groups

- G is abelian $\iff$ every inner automorphism is trivial. If $H \trianglelefteq G$ is abelian but $H \not\subseteq Z(G)$, then the restriction of conjugation by some $g \in G$ to H is not inner in H (e.g., $G = A_4$, $H = V_4$, g any 3-cycle). [§4.4]
- $Z(Q_8) = \{\pm 1\}$, hence $\mathrm{Inn}(Q_8) \cong Q_8/Z(Q_8) \cong V_4$. [§4.4]
- $Z(D_8) = \langle r^2 \rangle$, hence $\mathrm{Inn}(D_8) \cong D_8/\langle r^2 \rangle \cong V_4$. [§4.4]
- For $n \geq 3$, $Z(S_n) = 1$, hence $\mathrm{Inn}(S_n) \cong S_n$. [§4.4]

Definition.: Characteristic subgroup ($H \triangleleft G$)

A subgroup H of G is *characteristic* in G if $u(H) = H$ for every $u \in \mathrm{Aut}(G)$. Facts: (1) characteristic $\Rightarrow$ normal; (2) if H is the unique subgroup of G of a given order, then H is characteristic; (3) if $K \triangleleft H$ and $H \trianglelefteq G$, then $K \trianglelefteq G$. [§4.4]

Proposition.: $\mathrm{Aut}(\mathbb{Z}_n) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ (of order $\varphi(n)$)

Let x generate the cyclic group $\mathbb{Z}_n = \langle x \rangle$. Any $\psi \in \mathrm{Aut}(\mathbb{Z}_n)$ is determined by $\psi(x) = x^a$ with $\gcd(a, n) = 1$, and every such a gives an automorphism. The map $\Phi : \mathrm{Aut}(\mathbb{Z}_n) \to (\mathbb{Z}/n\mathbb{Z})^\times$, $\psi_a \mapsto a \pmod{n}$, is an isomorphism. [§4.4, Prop. 16]

. . . . . .

Intuition. Automorphisms of a cyclic group are "choose a new generator." Exponents a mod n with $\gcd(a, n) = 1$ are exactly the generators of $\mathbb{Z}_n$.

. . . . . .

Proof.

Step 1 (Parametrization). $\psi(x) = x^a$ determines ψ, and ψ is bijective $\iff$ $\mathrm{ord}(x^a) = n \iff \gcd(a, n) = 1$.

Step 2 (Surjectivity). For each $a \in (\mathbb{Z}/n\mathbb{Z})^\times$, define $\psi_a(x^k) = x^{ak}$; this is an automorphism.

Step 3 (Homomorphism). $\psi_a \circ \psi_b(x) = \psi_a(x^b) = x^{ab}$, so $\Phi(\psi_a \circ \psi_b) = ab = \Phi(\psi_a)\Phi(\psi_b)$.

Step 4 (Injectivity). If $\Phi(\psi_a) = \Phi(\psi_b)$ then $a \equiv b \pmod{n}$, hence $\psi_a = \psi_b$. Thus Φ is an isomorphism.

Example (Theorem-style).: If $|G| = pq$ with primes $p \leq q$ and $p \nmid (q-1)$, then G is abelian

Assume $Z(G) = 1$. Then G has an element x of order q. Let $H = \langle x \rangle$. Since $[G : H] = p$ and p is the smallest prime dividing $|G|$, $H \trianglelefteq G$. Also $C_G(H) = H$ (as $Z(G) = 1$). By Cor. 15, $G/H \cong N_G(H)/C_G(H) \leq \mathrm{Aut}(H)$, so $p \mid |\mathrm{Aut}(H)| = \varphi(q) = q - 1$, a contradiction. Hence $Z(G) \neq 1$ and then $G/Z(G)$ is cyclic, so G is abelian. [§4.4, Example after Prop. 16]

Proposition.: Selected automorphism groups (summary)

1. If p is odd prime and $n \in \mathbb{Z}_{>0}$, then $\mathrm{Aut}(\mathbb{Z}_{p^n}) \cong C_{p^{n-1}(p-1)}$ (cyclic). For $n = 1$, $\mathrm{Aut}(\mathbb{Z}_p) \cong C_{p-1}$.

2. For $n \geq 3$, $\mathrm{Aut}(\mathbb{Z}_{2^n}) \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{n-2}}$ (hence not cyclic but with a cyclic subgroup of index 2).

3. If V is elementary abelian of order p^m (p prime), then $\mathrm{Aut}(V) \cong \mathrm{GL}_m(\mathbb{F}_p)$.

4. For $n \neq 6$, $\mathrm{Aut}(S_n) = \mathrm{Inn}(S_n) \cong S_n$; for $n = 6$, $|\mathrm{Aut}(S_6) : \mathrm{Inn}(S_6)| = 2$.

5. $\mathrm{Aut}(D_8) \cong D_8$ and $\mathrm{Aut}(Q_8) \cong S_4$.

[§4.4, Prop. 17 (summary; proofs deferred in text)]

. . . . . .

Intuition. Cyclic groups: "choose a generator" $\Rightarrow$ units mod n. Elementary abelian groups: automorphisms are nonsingular linear maps. Symmetric groups: conjugacy-class constraints force inner automorphisms (except S_6).

. . . . . .

Proof.

Step 1 (Cyclic cases). Use number-theoretic structure of $(\mathbb{Z}/n\mathbb{Z})^\times$ as in Prop. 16 and later results cited in §9.5.

Step 2 (Elementary abelian). Identify $V \cong \mathbb{F}_p^m$; automorphisms are invertible linear maps: $\mathrm{GL}_m(\mathbb{F}_p)$.

Step 3 (Symmetric groups). Conjugacy-class sizes pin down images of transpositions; exercises show all automorphisms are inner for $n \neq 6$, and index 2 extension for S_6.

Step 4 (Dihedral/quaternion). Exercise-based computations (centralizers/normalizers) yield the stated isomorphisms.

4pt5.

SYLOW'S THEOREM

Definition.: p-groups; Sylow p-subgroups; $\mathrm{Syl}_p(G)$ and $n_p(G)$

Let G be a finite group and let p be a prime. (1) A group of order p^a with $a \geq 1$ is called a *p-group*. Subgroups of G which are p-groups are *p-subgroups*. (2) If $|G| = p^a m$ with $p \nmid m$, a subgroup of order p^a is a *Sylow p-subgroup* of G. (3) The set of Sylow p-subgroups of G is denoted $\mathrm{Syl}_p(G)$ and the number of Sylow p-subgroups is $n_p(G)$ (or simply n_p when G is clear).

Lemma.: If $P \in \mathrm{Syl}_p(G)$ and Q is any p-subgroup of G, then $Q \cap N_G(P) = Q \cap P$

Let $P \in \mathrm{Syl}_p(G)$ and $Q \leq G$ be a p-subgroup. Put $H = N_G(P) \cap Q$. Then $P \cap Q \leq H$. Moreover PH is a subgroup and a p-group containing P, hence $PH = P$ and therefore $H \leq P$. Consequently $Q \cap N_G(P) = Q \cap P$.

. . . . . .

Intuition. Inside the normalizer, P behaves like a normal subgroup; multiplying P by H can't enlarge P because P already has maximal p-power order.

. . . . . .

Proof.

Step 1 (Form H and PH). Let $H = N_G(P) \cap Q$. Since $H \leq N_G(P)$, Cor. 3.2.15 gives $PH \leq G$.

Step 2 (PH is a p-group). By the product formula $|PH| = \dfrac{|P||H|}{|P \cap H|}$—a power of p; hence PH is a p-group.

Step 3 (Maximality of P). $P \leq PH$ and P has maximal p-power order in G, so $PH = P$. Thus $H \leq P$.

Step 4 (Conclusion). Since $H = N_G(P) \cap Q \leq P$, we have $Q \cap N_G(P) = Q \cap P$.

Theorem.: Sylow's Theorem

Let G be a finite group with $|G| = p^a m$ and $p \nmid m$. Then: (1) $\mathrm{Syl}_p(G) \neq \emptyset$ (existence). (2) If $P \in \mathrm{Syl}_p(G)$ and Q is any p-subgroup of G, then $Q \leq gPg^{-1}$ for some $g \in G$; in particular, any two Sylow p-subgroups are conjugate. (3) $n_p \equiv 1 \pmod{p}$ and $n_p = [G : N_G(P)]$ for $P \in \mathrm{Syl}_p(G)$, hence $n_p \mid m$.

. . . . . .

Intuition. For (1) lift a p-subgroup from a central quotient or find one inside a proper centralizer via the class equation. For (2)–(3) let a p-subgroup act by conjugation on the set of conjugates of a fixed Sylow subgroup and count orbits; p divides every orbit size except the fixed-point orbit, forcing the $1 \pmod{p}$ congruence and conjugacy containment.

. . . . . .

Proof.

Step 1 (Existence by induction). Induct on $|G|$. If $p \mid |Z(G)|$, take $N \leq Z(G)$ of order p and lift a Sylow subgroup from G/N to G.

Step 2 (Class equation case). If $p \nmid |Z(G)|$, write $|G| = |Z(G)| + \sum |G : C_G(g_i)|$. Some i has $p \nmid |G : C_G(g_i)|$, so $|C_G(g_i)| = p^a k$ with $p \nmid k < |G|$. By induction $C_G(g_i)$ has a Sylow p-subgroup, which is also Sylow in G.

Step 3 (Set of conjugates). Fix $P \in \mathrm{Syl}_p(G)$ and let $S = \{gPg^{-1} \mid g \in G\}$ with $|S| = n_p = [G : N_G(P)]$.

Step 4 (Q-action and orbit sizes). For any p-subgroup $Q \leq G$, let Q act on S by conjugation. Then $|\mathcal{O}| = [Q : Q \cap N_G(P_i)]$ for each orbit representative P_i. By the lemma, $Q \cap N_G(P_i) = Q \cap P_i$, so each nonfixed orbit has size a power of p.

Step 5 ($n_p \equiv 1 \pmod{p}$). Taking $Q = P$, the orbit containing P has size 1 and all others have size divisible by p; hence $n_p \equiv 1 \pmod{p}$.

Step 6 (Containment/conjugacy). If a p-subgroup Q fixes some P_i, then $Q \leq N_G(P_i)$ and thus $Q \leq P_i$. If Q fixed none, every orbit would have size divisible by p, contradicting Step 5. Therefore $Q \leq gPg^{-1}$ for some g, and Sylow p-subgroups are conjugate.

Step 7 (Normalizer index). By definition of S, $n_p = [G : N_G(P)] \mid m$.

Corollary.: For $P \in \mathrm{Syl}_p(G)$ the following are equivalent: (1) $n_p = 1$; (2) $P \trianglelefteq G$; (3) $P \triangleleft G$; (4) every subgroup generated by p-power order elements is a p-group

If $n_p = 1$ then $gPg^{-1} = P$ for all $g \in G$, so $P \trianglelefteq G$. Conversely, if $P \trianglelefteq G$ then $gPg^{-1} = P$ for every g, whence $n_p = 1$. Since characteristic subgroups are normal, (3)⇒(2); if $P \trianglelefteq G$, then P is the unique subgroup of order p^a and hence characteristic. Finally, (1)⇒(4): every p-element lies in some $gPg^{-1} = P$, so the subgroup generated by any set of p-elements is a p-group. Conversely, with X the union of all Sylow p-subgroups, (4) forces $\langle X \rangle$ to be a p-group containing a Sylow subgroup, hence equal to it, so $n_p = 1$.

. . . . . .

Intuition. "Unique ⇔ fixed by conjugation" gives normality; "unique of its order" gives characteristic. Gathering all p-elements can't produce non-p structure when there's only one Sylow.

. . . . . .

Proof.

Step 1 ((1) ⇒ (2)). If $n_p = 1$, conjugates of P equal P, hence $P \trianglelefteq G$.

Step 2 ((2) ⇒ (1)). If $P \trianglelefteq G$, any Sylow p-subgroup is G-conjugate to P, hence equals P.

Step 3 (Characteristic). If $P \trianglelefteq G$ and is the unique subgroup of order p^a, every automorphism of G fixes P, so $P \triangleleft G$.

Step 4 ((1) ⇒ (4)). Each p-element lies in P; a subgroup generated by p-elements lies in P, hence is a p-group.

Step 5 ((4) ⇒ (1)). Let X be the union of Sylow p-subgroups. Then $\langle X \rangle$ is a p-group containing a Sylow subgroup, so equals it and is unique.

Example.: Sample computations and quick consequences of Sylow's Theorem

- S_3: $n_2 = 3$, $n_3 = 1$; the unique Sylow 3-subgroup A_3 is normal.

- A_4: $n_2 = 1$ (normal V_4), $n_3 = 4$.

- Order pq $(p < q)$: $n_q = 1$; if $p \nmid (q-1)$ then $n_p = 1$, hence the group is cyclic.

- Order 30: at least one of the Sylow 5- or 3-subgroups is normal (counting contradiction if both are nonnormal).

- Order 12: either a normal Sylow 3-subgroup or $G \cong A_4$ (then the Sylow 2-subgroup is normal).

- Order p^2q $(p \neq q)$: some Sylow subgroup is normal; if $p > q$, the Sylow p-subgroup is normal; if $p < q$ and $n_q > 1$ then $p = 2$, $q = 3$, so $|G| = 12$ and use the previous item.

- Order 60: if $n_5 > 1$ then G is simple; consequently A_5 is simple and any simple group of order 60 is isomorphic to A_5.

Example.: If $|G| = pq$ with primes $p < q$, then $n_q = 1$ (so $Q \in \mathrm{Syl}_q(G)$ is normal); moreover, if $p \nmid (q-1)$ then G is cyclic

Suppose $|G| = pq$ with $p < q$. Then the number n_q of Sylow q-subgroups satisfies $n_q \equiv 1 \pmod{q}$ and $n_q \mid p$, hence $n_q = 1$ and $Q \trianglelefteq G$. If also $p \nmid (q-1)$, then $n_p \equiv 1 \pmod{p}$ and $n_p \mid q$, so $n_p = 1$ and $P \trianglelefteq G$. With $P = \langle x \rangle$, $Q = \langle y \rangle$ and $P, Q \trianglelefteq G$, one has $[x, y] = 1$, so $|xy| = pq$ and $G \cong \mathbb{Z}_{pq}$ is cyclic. [§4.5 Applications]

. . . . . .

Intuition. The congruence $n_q \equiv 1 \pmod{q}$ and divisibility $n_q \mid p$ force $n_q = 1$. When also $p \nmid (q-1)$, the same squeeze argument forces $n_p = 1$. Two commuting generators of orders p and q then yield a cyclic group of order pq.

. . . . . .

Proof.

Step 1 (q-Sylow). $n_q \equiv 1 \pmod{q}$ and $n_q \mid p \Rightarrow n_q = 1$; hence $Q \trianglelefteq G$.

Step 2 (p-Sylow under $p \nmid (q-1)$). $n_p \equiv 1 \pmod{p}$ and $n_p \mid q \Rightarrow n_p \in \{1, q\}$. If $p \nmid (q-1)$ then $n_p \neq q$, so $n_p = 1$ and $P \trianglelefteq G$.

Step 3 (Abelian, hence cyclic). With $P, Q \trianglelefteq G$, conjugation by Q induces a map $Q \to \mathrm{Aut}(P) \cong (\mathbb{Z}/p)^\times$ whose image order divides q and $p-1$; by $p \nmid (q-1)$ this image is trivial, so $[P, Q] = 1$. Then $|xy| = pq$ and $\langle xy \rangle = G$.

Example.: If $|G| = 30$, at least one of the Sylow 5- or Sylow 3-subgroups is normal

Write $|G| = 2 \cdot 3 \cdot 5$. If neither $P \in \mathrm{Syl}_5(G)$ nor $Q \in \mathrm{Syl}_3(G)$ is normal, then by Sylow's Theorem $n_5 \in \{1, 6\}$ and $n_3 \in \{1, 10\}$ force $n_5 = 6$, $n_3 = 10$. Distinct Sylow 5-subgroups intersect trivially, so G has $6 \cdot (5-1) = 24$ elements of order 5. Likewise it has $10 \cdot (3-1) = 20$ elements of order 3. This is impossible in a group of order 30. Hence at least one of P or Q is normal. [§4.5 Applications]

. . . . . .

Intuition. Count nonidentity elements in each prime-power order and use disjointness of distinct Sylow-p's when $|P| = p$ to force a contradiction.

. . . . . .

Proof.

Step 1 (Possibilities). $n_5 \equiv 1 \pmod 5$, $n_5 \mid 6 \Rightarrow n_5 \in \{1, 6\}$; $n_3 \equiv 1 \pmod 3$, $n_3 \mid 10 \Rightarrow n_3 \in \{1, 10\}$.

Step 2 (Assume both nonnormal). Then $(n_5, n_3) = (6, 10)$.

Step 3 (Counting). Elements of order 5: $6 \cdot 4 = 24$. Elements of order 3: $10 \cdot 2 = 20$. Total > 30. Contradiction.

Step 4 (Conclusion). At least one of P or Q is normal.

Example.: If $|G| = 12$, then either G has a normal Sylow 3-subgroup or $G \cong A_4$ (in which case the Sylow 2-subgroup is normal)

Assume $n_3 \neq 1$ and let $P \in \mathrm{Syl}_3(G)$. Then $n_3 \mid 4$ and $n_3 \equiv 1 \pmod 3$, so $n_3 = 4$. Distinct 3-Sylows intersect trivially, giving eight elements of order 3. Since $[G : N_G(P)] = n_3 = 4$, we have $N_G(P) = P$. Let G act by conjugation on its four Sylow 3-subgroups to obtain an injective homomorphism $\varphi : G \hookrightarrow S_4$ with transitive image of order 12; hence $\varphi(G) \cong A_4$ and $G \cong A_4$. In A_4 the Sylow 2-subgroup V_4 is normal. [§4.5 Applications]

. . . . . .

Intuition. Force $n_3 = 4$, then use the conjugation action on the four Sylow 3-subgroups: kernel collapses to 1, so G embeds as a transitive subgroup of S_4 of order 12, necessarily A_4.

. . . . . .

Proof.

Step 1 ($n_3 = 4$). $n_3 \mid 4$, $n_3 \equiv 1 \pmod 3 \Rightarrow n_3 = 4$; thus G has eight elements of order 3.

Step 2 (Normalizer). $[G : N_G(P)] = n_3 = 4 \Rightarrow N_G(P) = P$.

Step 3 (Conjugation action). Conjugation on the set $\mathcal{P}$ of four 3-Sylows yields $\varphi : G \to S_4$. Kernel K normalizes every $P' \in \mathcal{P}$, so $K \subseteq N_G(P) = P$; but P is not normal, hence $K = 1$ and φ is injective.

Step 4 (Image). $\varphi(G)$ is a transitive subgroup of S_4 of order 12; the unique such subgroup is A_4. Hence $G \cong A_4$, whose Sylow 2-subgroup V_4 is normal.

Step 5 (Dichotomy). Therefore either $n_3 = 1$ and $P \trianglelefteq G$, or $G \cong A_4$ (so a Sylow 2-subgroup is normal).

Corollary 22.: A_5 is simple

The subgroups $\langle(1\,2\,3\,4\,5)\rangle$ and $\langle(1\,3\,2\,4\,5)\rangle$ are distinct Sylow 5-subgroups of A_5, and the simplicity conclusion follows immediately from the preceding proposition.

. . . . . .

Intuition. If a nontrivial normal subgroup contained a Sylow 5-subgroup, it would contain all its conjugates—hence all six Sylow 5-subgroups—forcing the whole group. Distinct Sylow 5-subgroups exist in A_5, so no proper, nontrivial normal subgroup can exist.

. . . . . .

Proof.

Step 1 (Distinct Sylow-5's). $(1\,2\,3\,4\,5)$ and $(1\,3\,2\,4\,5)$ generate different order-5 subgroups of A_5.

Step 2 (Normality would force all). Any normal subgroup containing one Sylow 5-subgroup contains all its conjugates.

Step 3 (Conclusion). The union of all Sylow 5-subgroups generates A_5, so no proper, nontrivial normal subgroup exists; A_5 is simple.

Proposition 23.: If G is a simple group of order 60, then $G \cong A_5$

Let G be simple with $|G| = 60 = 2^2 \cdot 3 \cdot 5$. Let $P \in \mathrm{Syl}_3(G)$ and put $N = N_G(P)$, so $|G : N| = n_3$.

. . . . . .

Intuition. First rule out small indices: a simple group of order 60 cannot act faithfully on fewer than five cosets. Then force the Sylow counts $n_5 = 6$ and $n_3 = 10$. Finally, show there are exactly five Sylow 2-subgroups and use the permutation action on these five subgroups to embed G in S_5. Elements of orders 3 and 5 act as even permutations, so the image lands in A_5. Since $|G| = |A_5|$, the embedding is an isomorphism.

. . . . . .

Proof.

Step 1 (No index < 5). Suppose $H < G$ has index 3 or 4. The left–coset action gives a homomorphism $G \to S_3$ or S_4 with kernel normal. As G is simple, the kernel is trivial, so $|G|$ divides $|S_3|$ or $|S_4|$, impossible. Hence G has no subgroup of index 3 or 4.

Step 2 (Count 5-Sylows). By Sylow, $n_5 \equiv 1 \pmod 5$ and $n_5 \mid 12$, so $n_5 \in \{1, 6\}$. If $n_5 = 1$, the Sylow 5-subgroup is normal, contradicting simplicity; thus $n_5 = 6$.

Step 3 (Count 3-Sylows). By Sylow, $n_3 \equiv 1 \pmod 3$ and $n_3 \mid 20$, so $n_3 \in \{1, 4, 10, 20\}$. The case $n_3 = 1$ is impossible (normal). If $n_3 = 4$, then G acts on G/N with $|G : N| = 4$, contradicting Step 1. If $n_3 = 20$, G has 20 subgroups of order 3, giving 40 elements of order 3; the remaining 20 elements cannot be accommodated by the 6 Sylow 5-subgroups and the Sylow 2-structure (a counting contradiction). Hence $n_3 = 10$.

Step 4 (Count 2-Sylows). By Sylow, $n_2 \equiv 1 \pmod 2$ and $n_2 \mid 15$, so $n_2 \in \{1, 3, 5, 15\}$. The cases 1 and 3 would give subgroups of index 1 or 3 (ruled out). If $n_2 = 15$, then even with maximal overlap the number of involutions exceeds $|G|$; hence $n_2 = 5$.

Step 5 (Embed in S_5). Let Ω be the set of the five Sylow 2-subgroups. Conjugation yields a faithful action $G \hookrightarrow S(\Omega) \cong S_5$: the kernel normalizes every Sylow 2-subgroup and so is normal in G, hence trivial.

Step 6 (Image lies in A_5). An element of order 3 permutes Ω in disjoint 3-cycles (even), and an element of order 5 acts as a 5-cycle (even). Since G is generated by elements of orders 2, 3, and 5, the image consists of even permutations; thus $G \leq A_5$.

Step 7 (Conclude). $|G| = 60 = |A_5|$ and $G \leq A_5$ inside S_5, so $G \cong A_5$.

4pt6.

THE SIMPLICITY OF A_n

Remark.: Base cases for simplicity

A_3 is abelian and simple. A_4 is not simple (it contains the normal Klein group V_4).

Theorem.: A_n is simple for all $n \geq 5$

For each integer $n \geq 5$, the alternating group A_n has no proper nontrivial normal subgroups.

. . . . . .

Intuition. Work by induction. If a nontrivial normal subgroup $H \lhd A_n$ contains an element fixing some point, then by simplicity of the point stabilizer (isomorphic to A_{n-1}) we are forced to have all point stabilizers inside H, hence $H = A_n$—contradiction. Thus every nonidentity element of H moves every point. That forces a rigidity: two elements of H that agree on one point must be equal. Conjugation then produces contradictions unless every nonidentity element is a product of disjoint 2-cycles, and a final conjugation trick rules even that out. Hence $H = 1$.

. . . . . .

Proof.

Step 1 (Induction setup). The result holds for $n = 5$. Assume $n \geq 6$ and let $G = A_n$. Suppose $1 \neq H \lhd G$ with $H \neq G$.

Step 2 (Point stabilizers). For $i \in \{1, \ldots, n\}$ let $G_i = \mathrm{Stab}_G(i) \cong A_{n-1}$ (via the natural action). By induction, each G_i is simple.

Step 3 (If some $h \in H$ fixes a point, then $H = G$). Suppose $\exists\, h \in H \setminus \{1\}$ and i with $h(i) = i$. Then $1 \neq h \in H \cap G_i \lhd G_i$, so $H \cap G_i = G_i$ by simplicity of G_i, hence $G_i \leq H$. Conjugating, $G_j \leq H$ for all j, so $\langle G_1, \ldots, G_n \rangle = G \leq H$, contradicting $H \neq G$. Thus every $1 \neq h \in H$ moves every point.

Step 4 (Rigidity: agreement at one point forces equality). If $r_1, r_2 \in H$ with $r_1(i) = r_2(i)$ for some i, then $r_2^{-1} r_1(i) = i$. By Step 3 this forces $r_2^{-1} r_1 = 1$, so $r_1 = r_2$.

Step 5 (No cycles of length ≥ 3 in H). Suppose $1 \neq r \in H$ has a cycle of length ≥ 3, say $(a_1\, a_2\, a_3\, \ldots)$. Choose $a \in G$ with $a(a_1) = a_1$, $a(a_2) = a_2$, but $a(a_3) \neq a_3$ (possible since $n \geq 5$). Then $r' := ara^{-1} \in H$ satisfies $r(a_1) = r'(a_1) = a_2$, so by Step 4 we must have $r = r'$, contradicting $a(a_3) \neq a_3$. Hence every nonidentity $r \in H$ is a product of disjoint 2-cycles.

Step 6 (Rule out products of 2-cycles). Take $1 \neq r \in H$; write $r = (a_1\, a_2)(a_3\, a_4) \cdots$. With $n \geq 6$, pick $a = (a_1\, a_2)(a_3\, a_5) \in G$. Then $r' := ara^{-1} \in H$ satisfies $r(a_1) = r'(a_1) = a_2$, but $r \neq r'$ (the second transposition changes), contradicting Step 4.

Step 7 (Conclusion). Steps 5–6 force $H = 1$. Thus A_n is simple for all $n \geq 5$.