Abstract Algebra I

George Voutsadakis[1]

[1]Mathematics and Computer Science
Lake Superior State University

LSSU Math 341

1. Group Actions
   - Group Actions and Permutation Representations
   - Action by Left Multiplication - Cayley's Theorem
   - Action by Conjugation - The Class Equation
   - Automorphisms
   - Sylow's Theorem
   - The Simplicity of A_n

Subsection 1

Group Actions and Permutation Representations

Group Actions and Related Terminology

- Let G be a group acting on a nonempty set A.
- We showed that, for each $g \in G$, the map $\sigma_g : A \to A$, defined by $\sigma_g(a) = g \cdot a$, is a permutation of A.
- We also saw that there is a homomorphism associated to an action of G on A: $\varphi : G \to S_A$, defined by $\varphi(g) = \sigma_g$, called the **permutation representation** associated to the given action.
- Recall some additional terminology associated to group actions:

Definition

(1) The **kernel** of the action is the set of elements of G that act trivially on every element of A: $\{g \in G : g \cdot a = a, \text{ for all } a \in A\}$.

(2) For each $a \in A$, the **stabilizer** of a in G is the set of elements of G that fix the element a: $G_a = \{g \in G : g \cdot a = a\}$.

(3) An action is **faithful** if its kernel is the identity.

Some Remarks on Kernels and Stabilizers

- Since the kernel of an action is the same as the kernel of the associated permutation representation, it is a normal subgroup of G.
- Two group elements induce the same permutation on A if and only if they are in the same coset of the kernel if and only if they are in the same fiber of the permutation representation φ.

  Thus, an action of G on A may also be viewed as a faithful action of the quotient group $G/\ker\varphi$ on A.
- Recall that the stabilizer in G of an element a of A is a subgroup of G. If a is a fixed element of A, then the kernel of the action is contained in the stabilizer G_a since the kernel of the action is the set of elements of G that stabilize every point, namely $\bigcap_{a\in A} G_a$.

Example I

- Let n be a positive integer. The group $G = S_n$ acts on the set $A = \{1, 2, \ldots, n\}$ by

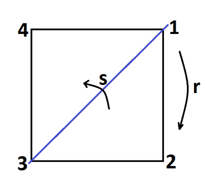
$$\sigma \cdot i = \sigma(i), \quad \text{for all } i \in \{1, 2, \ldots, n\}.$$

  - The permutation representation associated to this action is the identity map $\varphi : S_n \to S_n$.
  - The action is faithful.
  - For each $i \in \{1, \ldots, n\}$, the stabilizer G_i is isomorphic to S_{n-1}.

Example II

- Let $G = D_8$ act on the set A consisting of the four vertices of a square.

  Label these vertices $1, 2, 3, 4$ in a clockwise fashion. Let r be the rotation of the square clockwise by $\frac{\pi}{2}$ radians and let s be the reflection in the line which passes through vertices 1 and 3. Then, the permutations of the vertices given by r and s are $\sigma_r = (1\ 2\ 3\ 4)$ and $\sigma_s = (2\ 4)$.



  Since the permutation representation is a homomorphism, the permutation of the four vertices corresponding to sr is $\sigma_{sr} = \sigma_s \sigma_r = (1\ 4)(2\ 3)$.
  - The action of D_8 on the four vertices of a square is faithful.
  - The stabilizer of any vertex a is the subgroup of D_8 of order 2 generated by the reflection about the line passing through a and the center of the square.

Example III

- Label the four vertices of a square as in the preceding example and let A be the set whose elements consist of unordered pairs of opposite vertices: $A = \{\{1,3\},\{2,4\}\}$.

  Then D_8 also acts on this set A since each symmetry of the square sends a pair of opposite vertices to a pair of opposite vertices. The rotation r interchanges the pairs $\{1,3\}$ and $\{2,4\}$. The reflection s fixes both unordered pairs of opposite vertices. Thus, if we label the pairs $\{1,3\}$ and $\{2,4\}$ as $\mathbf{1}$ and $\mathbf{2}$, respectively, the permutations of A given by r and s are $\sigma_r = (\mathbf{1}\ \mathbf{2})$ and $\sigma_s =$ the identity permutation.
  - This action of D_8 is not faithful: its kernel is $\langle s, r^2 \rangle$.
  - For each $a \in A$, the stabilizer in D_8 of a is the same as the kernel of the action.
- Label the four vertices of a square as before and let A be the following set of unordered pairs of vertices: $\{\{1,2\},\{3,4\}\}$. The group D_8 does not act on this set A because $\{1,2\} \in A$ but $r \cdot \{1,2\} = \{2,3\} \notin A$.

Actions of G on A and Homomorphisms of G into S_A

- The relation between actions and homomorphisms into symmetric groups may be reversed:

  Given any nonempty set A and any homomorphism φ of the group G into S_A, we obtain an action of G on A by defining

  $$g \cdot a = \varphi(g)(a), \text{ for all } g \in G \text{ and all } a \in A.$$

  - The kernel of this action is the same as $\ker\varphi$.
  - The permutation representation associated to this action is precisely the given homomorphism.

Proposition

For any group G and any nonempty set A, there is a bijection between the actions of G on A and the homomorphisms of G into S_A.

Permutation Representations

- The proposition allows rephrasing the definition of a permutation representation:

Definition (Permutation Representation)

If G is a group, a **permutation representation** of G is any homomorphism of G into the symmetric group S_A for some nonempty set A. We say a given action of G on A **affords** or **induces** the associated permutation representation of G.

- We can think of a permutation representation as an analogue of the matrix representation of a linear transformation.
- In the case where A is a finite set of n elements we have $S_A \cong S_n$.

  Fixing a labeling of the elements of A, we may consider our permutations as elements of S_n, in the same way that fixing a basis for a vector space allows us to view a linear transformation as a matrix.

Equivalence Induced by an Action on a Set

Proposition

Let G be a group acting on the nonempty set A. The relation on A defined by

$$a \sim b \quad \text{if and only if} \quad a = g \cdot b, \text{ for some } g \in G,$$

is an equivalence relation. For each $a \in A$, the number of elements in the equivalence class containing a is $|G : G_a|$, the index of the stabilizer of a.

- We first prove $\sim$ is an equivalence relation:
  - Reflexivity: Since $a = 1 \cdot a$, for all $a \in A$, we get $a \sim a$. So, the relation is reflexive.
  - Symmetry: If $a \sim b$, then $a = g \cdot b$, for some $b \in G$. So $g^{-1} \cdot a = g^{-1} \cdot (g \cdot b) = (g^{-1}g) \cdot b = 1 \cdot b = b$. Hence $b \sim a$ and the relation is symmetric.
  - Transitivity: Finally, if $a \sim b$ and $b \sim c$, then $a = g \cdot b$ and $b = h \cdot c$, for some $g, h \in G$. So $a = g \cdot b = g \cdot (h \cdot c) = (gh) \cdot c$. Thus, $a \sim c$, and the relation is transitive.

Equivalence Induced by an Action on a Set (Cont'd)

- Let $C_a = \{g \cdot a : g \in G\}$ the equivalence class containing a fixed $a \in A$.

  To prove that $|C_a|$ is the index $|G : G_a|$ of the stabilizer of a, we exhibit a bijection between the elements of C_a and the left cosets of G_a in G.

  Suppose $b = g \cdot a \in C_a$. Then gG_a is a left coset of G_a in G. The map

  $$b = g \cdot a \mapsto gG_a$$

  is a map from C_a to the set of left cosets of G_a in G.

  - This map is surjective since for any $g \in G$, the element $g \cdot a$ is an element of C_a.
  - Since $g \cdot a = h \cdot a$ if and only if $h^{-1}g \in G_a$ if and only if $gG_a = hG_a$, the map is also injective.

  Hence it is a bijection.

Orbits and Transitivity

- The group G acting on the set A partitions A into disjoint equivalence classes under the action of G.

Definition

Let G be a group acting on the nonempty set A.

(1) The equivalence class $\{g \cdot a : g \in G\}$ is called the **orbit** of G containing a.

(2) The action of G on A is called **transitive** if there is only one orbit, i.e., given any two elements $a, b \in A$, there is some $g \in G$, such that $a = g \cdot b$.

Examples: Let G be a group acting on the set A.

(1) If G acts trivially on A, then $G_a = G$, for all $a \in A$, and the orbits are the elements of A. This action is transitive if and only if $|A| = 1$.

(2) The symmetric group $G = S_n$ acts transitively in its usual action as permutations on $A = \{1, 2, \ldots, n\}$. The stabilizer in G of any point i has index $n = |A|$ in S_n.

More Examples

(3) When group G acts on the set A, any subgroup of G also acts on A. If G is transitive on A, a subgroup of G need not be transitive on A.

E.g., if $G = \langle (1\ 2), (3\ 4) \rangle \leq S_4$, then the orbits of G on $\{1,2,3,4\}$ are $\{1,2\}$ and $\{3,4\}$. There is no element of G that sends 2 to 3.

When $\langle \sigma \rangle$ is any cyclic subgroup of S_n then the orbits of $\langle \sigma \rangle$ consist of the sets of numbers that appear in the individual cycles in the cycle decomposition of σ.

(4) The group D_8 acts transitively on the four vertices of the square. The stabilizer of any vertex is the subgroup of order 2 (and index 4) generated by the reflection about the line of symmetry passing through that point.

(5) The group D_8 also acts transitively on the set of two pairs of opposite vertices. In this action the stabilizer of any point is $\langle s, r^2 \rangle$ (which is of index 2).

Cycle Decomposition: Existence

Claim: Every element of the symmetric group S_n has the unique cycle decomposition.

(**Existence**) Let $A = \{1, 2, \ldots, n\}$, let σ be an element of S_n and let $G = \langle \sigma \rangle$. Then $\langle \sigma \rangle$ acts on A. By a preceding proposition, it partitions $\{1, 2, \ldots, n\}$ into a unique set of (disjoint) orbits. Let $\mathcal{O}$ be one of these orbits and let $x \in \mathcal{O}$. We proved that there is a bijection between the elements of $\mathcal{O}$ and the left cosets of G_x in G, given explicitly by $\sigma^i x \mapsto \sigma^i G_x$. Since G is a cyclic group, $G_x \trianglelefteq G$ and G/G_x is cyclic of order d, where d is the smallest positive integer for which $\sigma^d \in G_x$. Also, $d = |G : G_x| = |\mathcal{O}|$. Thus, the distinct cosets of G_x in G are $1G_x, \sigma G_x, \sigma^2 G_x, \ldots, \sigma^{d-1} G_x$. This shows that the distinct elements of $\mathcal{O}$ are $x, \sigma(x), \sigma^2(x), \ldots, \sigma^{d-1}(x)$. Ordering the elements of $\mathcal{O}$ in this manner shows that σ cycles the elements of $\mathcal{O}$, that is, on an orbit of size d, σ acts as a d-cycle. This proves the existence of a cycle decomposition for each $\sigma \in S_n$.

Cycle Decomposition: Uniqueness

- (**Uniqueness**) The orbits of $\langle\sigma\rangle$ are uniquely determined by σ, the only latitude being the order in which the orbits are listed. Within each orbit $\mathcal{O}$, we may begin with any element as a representative. Choosing $\sigma^i(x)$ instead of x as the initial representative simply produces the elements of $\mathcal{O}$ in the order

$$\sigma^i(x), \sigma^{i+1}(x), \ldots, \sigma^{d-1}(x), x, \sigma(x), \ldots, \sigma^{i-1}(x),$$

  which is a cyclic permutation of the original list. Thus, the cycle decomposition is unique up to a rearrangement of the cycles and up to a cyclic permutation of the integers within each cycle.
- Subgroups of symmetric groups are called **permutation groups**.
  - For any subgroup G of S_n the orbits of G will refer to its orbits on $\{1, 2, \ldots, n\}$.
  - The orbits of an element σ in S_n will mean the orbits of the group $\langle\sigma\rangle$ (i.e., the sets of integers comprising the cycles in its cycle decomposition).

Subsection 2

Action by Left Multiplication - Cayley's Theorem

Action by Left Multiplication

- Let G be a group and consider G **acting on itself** (i.e., $A = G$) **by left multiplication**:

$$g \cdot a = ga, \text{for all } g \in G, a \in G,$$

  where ga is the product of the two group elements g and a in G.
- If G is written additively, the action will be written $g \cdot a = g + a$ and called a **left translation**.
- This action satisfies the two axioms of a group action.
  - $1 \cdot a = 1a = a$;
  - $g_1 \cdot (g_2 \cdot a) = g_1(g_2 a) = (g_1 g_2)a = (g_1 g_2) \cdot a$.

Action by Left Multiplication: Finite Case

- When G is a finite group of order n, it is convenient to label the elements of G with the integers $1, 2, \ldots, n$, in order to describe the permutation representation afforded by this action.

  So the elements of G are listed as $g_1, g_2, \ldots, g_n$.

  For each $g \in G$, σ_g may be described as a permutation of $\{1, 2, \ldots, n\}$ by

$$\sigma_g(i) = j \quad \text{if and only if} \quad gg_i = g_j.$$

- A different labeling of the group elements will give a different description of σ_g as a permutation of $\{1, 2, \ldots, n\}$.

A Representation of the Klein 4-Group

- Let $G = \{1, a, b, c\}$ be the Klein 4-group. Label the group elements $1, a, b, c$ with the integers $1, 2, 3, 4$, respectively. Under this labeling, the permutation σ_a induced by the action of left multiplication by the group element a is:

$$\begin{array}{l} a \cdot 1 = a1 = a \ \Rightarrow \ \sigma_a(1) = 2 \\ a \cdot a = aa = 1 \ \Rightarrow \ \sigma_a(2) = 1 \\ a \cdot b = ab = c \ \Rightarrow \ \sigma_a(3) = 4 \\ a \cdot c = ac = b \ \Rightarrow \ \sigma_a(4) = 3. \end{array}$$

$\cdot$	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

With this labeling of the elements of G, we see that $\sigma_a = (1\ 2)(3\ 4)$. Similarly, we may compute,

$$a \mapsto \sigma_a = (1\ 2)(3\ 4), \quad b \mapsto \sigma_b = (1\ 3)(2\ 4), \quad c \mapsto \sigma_c = (1\ 4)(2\ 3),$$

which explicitly gives the permutation representation $G \to S_4$ associated to this action under the specific labeling.

Properties of the Action by Left Multiplication

Claim: The action of a group on itself by left multiplication is:

(a) transitive;
(b) faithful;
(c) the stabilizer of any point is the identity subgroup.

(a) We must show that, for all $a, b \in G$, there exists $g \in G$, such that $b = g \cdot a$. Taking $g = ba^{-1}$, we get:

$$g \cdot a = (ba^{-1}) \cdot a = (ba^{-1})a = b(a^{-1}a) = b.$$

(b) We must show that the kernel of the action is trivial. Suppose g is in the kernel, i.e., that $g \cdot a = a$, for all $a \in G$. Then, we have $ga = a$. By right cancelation, we get $g = 1$.

(c) Let $a \in G$. We need to show that, if $g \in G_a$, then $g = 1$. Suppose $g \in G_a$. Then $g \cdot a = a$. But $ga = a$ gives, by right cancelation, $g = 1$.

Left Multiplication on Cosets

- Let H be any subgroup of G and let A be the set of all left cosets of H in G. Define an action of G on A by

$$g \cdot aH = gaH, \text{ for all } g \in G, aH \in A,$$

  where gaH is the left coset with representative ga.
- This satisfies the two axioms for a group action:
  - $1 \cdot aH = (1a)H = aH$.
  - $g_1 \cdot (g_2 \cdot aH) = g_1 \cdot (g_2 a)H = (g_1(g_2 a))H = ((g_1 g_2)a)H = (g_1 g_2) \cdot aH$.

  So G does act on the set of left cosets of H by left multiplication.
- If $H = \{1\}$ is the identity subgroup of G, the coset aH is just $\{a\}$.

  If we identify the element a with the set $\{a\}$, this action by left multiplication on left cosets of the identity subgroup is the same as the action of G on itself by left multiplication.

Representations Afforded by Multiplication of Cosets

- When H is of finite index m in G, it is convenient to label the left cosets of H with the integers $1, 2, \ldots, m$ in order to describe the permutation representation afforded by this action.

  So the distinct left cosets of H in G are listed as

  $$a_1 H, a_2 H, \ldots, a_m H.$$

  For each $g \in G$, the permutation σ_g may be described as a permutation of $\{1, 2, \ldots, m\}$ by

  $$\sigma_g(i) = j \quad \text{if and only if} \quad g a_i H = a_j H.$$

- A different labeling of the group elements will give a different description of σ_g as a permutation of $\{1, 2, \ldots, m\}$.

Example: Cosets of $\langle s \rangle$ in D_8

- Let $G = D_8$ and $H = \langle s \rangle$. Label the distinct left cosets $1H, rH, r^2H, r^3H$ with the integers $1, 2, 3, 4$, respectively. Under this labeling, we compute the permutation as induced by the action of left multiplication by the group element s on the left cosets of H:

$$\begin{array}{l} s \cdot 1H = sH = 1H \ \Rightarrow \ \sigma_s(1) = 1 \\ s \cdot rH = srH = r^3H \ \Rightarrow \ \sigma_s(2) = 4 \\ s \cdot r^2H = sr^2H = r^2H \ \Rightarrow \ \sigma_s(3) = 3 \\ s \cdot r^3H = sr^3H = rH \ \Rightarrow \ \sigma_s(4) = 2. \end{array}$$

With this labeling of the left cosets of H we obtain $\sigma_s = (2\ 4)$. Similarly, we can see that $\sigma_r = (1\ 2\ 3\ 4)$.

Since the permutation representation is a homomorphism, once its value has been determined on generators for D_8, its value on any other element can be also determined.

Properties of the Left Multiplication Action on Cosets

Theorem

Let G be a group, H be a subgroup of G and let G act by left multiplication on the set A of left cosets of H in G. Denote by π_H the associated permutation representation afforded by this action. Then:

(1) G acts transitively on A;

(2) The stabilizer in G of the point $1H \in A$ is the subgroup H;

(3) The kernel of the action (i.e., the kernel of π_H) is $\bigcap_{x \in G} xHx^{-1}$, and $\ker \pi_H$ is the largest normal subgroup of G contained in H.

(1) To see that G acts transitively on A, let aH and bH be any two elements of A, and let $g = ba^{-1}$. Then $g \cdot aH = (ba^{-1})aH = bH$. Thus, any two elements aH and bH of A lie in the same orbit.

(2) The stabilizer of the point $1H$ is, by definition, $\{g \in G : g \cdot 1H = 1H\}$, i.e., $\{g \in G : gH = H\} = H$.

Proof of Properties (Cont'd)

(3) By definition of π_H, we have

$$\begin{array}{rcl}\ker\pi_H & = & \{g \in G : gxH = xH, \text{ for all } x \in G\} \\ & = & \{g \in G : (x^{-1}gx)H = H, \text{ for all } x \in G\} \\ & = & \{g \in G : x^{-1}gx \in H, \text{for all } x \in G\} \\ & = & \{g \in G : g \in xHx^{-1}, \text{ for all } x \in G\} \\ & = & \bigcap_{x \in G} xHx^{-1}.\end{array}$$

For the second statement, observe, first, that $\ker\pi_H \trianglelefteq G$ and $\ker\pi_H \leq H$. Suppose, next, that N is any normal subgroup of G contained in H. Then we have $N = xNx^{-1} \leq xHx^{-1}$, for all $x \in G$, whence $N \leq \bigcap_{x \in G} xHx^{-1} = \ker\pi_H$. Therefore, $\ker\pi_H$ is the largest normal subgroup of G contained in H.

Cayley's Theorem

Corollary (Cayley's Theorem)

Every group is isomorphic to a subgroup of some symmetric group. If G is a group of order n, then G is isomorphic to a subgroup of S_n.

- Let $H = 1$ and apply the preceding theorem to obtain a homomorphism of G into S_G. Since the kernel of this homomorphism is contained in $H = 1$, G is isomorphic to its image in S_G.
- Note that G is isomorphic to a subgroup of a symmetric group, not to the full symmetric group itself.

  Example: We exhibited an isomorphism of the Klein 4-group with the subgroup $\langle (1\ 2)(3\ 4), (1\ 3)(2\ 4) \rangle$ of S_4.
- Recall that subgroups of symmetric groups are called **permutation groups**. So Cayley's Theorem states that every group is isomorphic to a permutation group.
- The permutation representation afforded by left multiplication on the elements of G is called the **left regular representation** of G.

Subgroup of Index the Smallest Prime Divisor of the Order

- We generalize our result on the normality of subgroups of index 2.

Corollary

If G is a finite group of order n and p is the smallest prime dividing $|G|$, then any subgroup of index p is normal.

Remark: A group of order n need not have a subgroup of index p (for example, A_4 has no subgroup of index 2).

- Suppose $H \leq G$ and $|G:H| = p$. Let π_H be the permutation representation afforded by multiplication on the set of left cosets of H in G, $K = \ker \pi_H$ and $|H:K| = k$. Then $|G:K| = |G:H||H:K| = pk$. Since H has p left cosets, G/K is isomorphic to a subgroup of S_p, by the First Isomorphism Theorem. By Lagrange's Theorem, $pk = |G/K|$ divides $p!$. Thus, $k \mid \frac{p!}{p} = (p-1)!$. But all prime divisors of $(p-1)!$ are less than p and, by the minimality of p, every prime divisor of k is greater than or equal to p. So $k = 1$, and $H = K \trianglelefteq G$.

Subsection 3

Action by Conjugation - The Class Equation

Action by Conjugation

- Let G be a group and consider G **acting on itself** (i.e., $A = G$) **by conjugation**:
$$g \cdot a = gag^{-1}, \text{ for all } g \in G, a \in G,$$
where gag^{-1} is computed in the group G.
- This definition satisfies the two axioms for a group action, since, for all $g_1, g_2 \in G$ and all $a \in G$,
  - $1 \cdot a = 1a1^{-1} = a$;
  - $g_1 \cdot (g_2 \cdot a) = g_1 \cdot (g_2 a g_2^{-1}) = g_1(g_2 a g_2^{-1})g_1^{-1} = (g_1g_2)a(g_2^{-1}g_1^{-1}) = (g_1g_2)a(g_1g_2)^{-1} = (g_1g_2) \cdot a$.

Definition

Two elements a and b of G are said to be **conjugate** in G if there is some $g \in G$, such that $b = gag^{-1}$, i.e., if and only if they are in the same orbit of G acting on itself by conjugation. The orbits of G acting on itself by conjugation are called the **conjugacy classes** of G.

Examples

(1) If G is an abelian group, then the action of G on itself by conjugation is the trivial action: $g \cdot a = a$, for all $g, a \in G$. Thus, for each $a \in G$, the conjugacy class of a is $\{a\}$.

(2) If $|G| > 1$ then, unlike the action by left multiplication, G does not act transitively on itself by conjugation, because $\{1\}$ is always a conjugacy class, i.e., an orbit for this action.

More generally, the one element subset $\{a\}$ is a conjugacy class if and only if $gag^{-1} = a$, for all $g \in G$, if and only if a is in the center of G.

(3) In S_3 one can compute directly that the conjugacy classes are $\{1\}, \{(1\ 2), (1\ 3), (2\ 3)\}$ and $\{(1\ 2\ 3), (1\ 3\ 2)\}$.

We will develop techniques for computing conjugacy classes more easily, particularly in symmetric groups.

Action on Subsets by Conjugation

- The action by conjugation can be generalized: If S is any subset of G, define
$$gSg^{-1} = \{gsg^{-1} : s \in S\}.$$
- A group G acts on the set $\mathcal{P}(G)$ of all subsets of itself by defining $g \cdot S = gSg^{-1}$, for any $g \in G$ and $S \in \mathcal{P}(G)$.
- This defines a group action of G on $\mathcal{P}(G)$.
- If S is the one element set $\{s\}$ then $g \cdot S$ is the one element set $\{gsg^{-1}\}$, whence this action of G on all subsets of G may be considered as an extension of the action of G on itself by conjugation.

Definition

Two subsets S and T of G are said to be **conjugate** in G if there is some $g \in G$, such that $T = gSg^{-1}$, i.e., if and only if they are in the same orbit of G acting on its subsets by conjugation.

Number of Conjugates of S

- We proved that if S is a subset of G, then the number of conjugates of S equals the index $|G : G_S|$ of the stabilizer G_S of S.
- For action by conjugation $G_S = \{g \in G : gSg^{-1} = S\} = N_G(S)$ is the normalizer of S in G.

Proposition

The number of conjugates of a subset S in a group G is the index of the normalizer of S, $|G : N_G(S)|$. In particular, the number of conjugates of an element s of G is the index of the centralizer of s, $|G : C_G(s)|$.

- The second assertion of the proposition follows from the observation that $N_G(\{s\}) = C_G(s)$.
- The action of G on itself by conjugation partitions G into the conjugacy classes of G, whose orders can be computed by this proposition.

The Class Equation

Theorem (The Class Equation)

Let G be a finite group and let $g_1, g_2, \ldots, g_r$ be representatives of the distinct conjugacy classes of G not contained in the center $Z(G)$ of G. Then

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

- The element $\{x\}$ is a conjugacy class of size 1 if and only if $x \in Z(G)$, since, then, $gxg^{-1} = x$, for all $g \in G$. Let $Z(G) = \{1, z_2, \ldots, z_m\}$, let $\mathcal{K}_1, \mathcal{K}_2, \ldots, \mathcal{K}_r$ be the conjugacy classes of G not contained in the center, and let g_i be a representative of $\mathcal{K}_i$ for each i. Then the full set of conjugacy classes of G is given by $\{1\}, \{z_2\}, \ldots, \{z_m\}, \mathcal{K}_1, \ldots, \mathcal{K}_r$. Since these partition G, we have $|G| = \sum_{i=1}^{m} 1 + \sum_{i=1}^{r} |\mathcal{K}_i| = |Z(G)| + \sum_{i=1}^{r} |G : C_G(g_i)|$.
- All summands on the right hand side of the class equation are divisors of the group order, since they are indices of subgroups of G.

Examples

(1) The class equation gives no information in an abelian group since conjugation is the trivial action and all conjugacy classes have size 1.

(2) In any group G, we have $\langle g \rangle \leq C_G(g)$. This observation helps to minimize computations of conjugacy classes.

Example: In the quaternion group Q_8, $\langle i \rangle \leq C_{Q_8}(i) \leq Q_8$. Since $i \notin Z(Q_8)$ and $|Q_8 : \langle i \rangle| = 2$, we must have $C_{Q_8}(i) = \langle i \rangle$. Thus, i has precisely 2 conjugates in Q_8, namely i and $-i = kik^{-1}$. The other conjugacy classes in Q_8 are $\{1\}, \{-1\}, \{\pm i\}, \{\pm j\}, \{\pm k\}$. The first two classes form $Z(Q_8)$ and the class equation is

$$|Q_8| = 2 + 2 + 2 + 2.$$

Examples (Cont'd)

(3) In D_8, we have

$$Z(D_8) = \{1, r^2\}.$$

Moreover, the three subgroups of index 2

$$\langle r \rangle, \quad \langle s, r^2 \rangle, \quad \langle sr, r^2 \rangle,$$

are abelian. So, if $x \notin Z(D_8)$, then $|C_{D_8}(x)| = 4$.

The conjugacy classes of D_8 are $\{1\}, \{r^2\}, \{r, r^3\}, \{s, sr^2\}, \{sr, sr^3\}$.

The first two classes form $Z(D_8)$ and the class equation for this group is

$$|D_8| = 2 + 2 + 2 + 2.$$

The Center of a Group of Prime Power Order

- Groups of prime power order have nontrivial centers:

Theorem

If p is a prime and P is a group of prime power order p^a, for some $a \geq 1$, then P has a nontrivial center: $Z(P) \neq 1$.

- By the class equation

$$|P| = |Z(P)| + \sum_{i=1}^{r} |P : C_P(g_i)|,$$

where $g_1, \ldots, g_r$ are representatives of the distinct non-central conjugacy classes. By definition, $C_P(g_i) \neq P$, for $i = 1, 2, \ldots, r$. So p divides $|P : C_P(g_i)|$. Since p also divides $|P|$, it follows that p divides $|Z(P)|$. Hence the center must be nontrivial.

$G/Z(G)$ Cyclic Implies G Abelian

Lemma

Let G be a group. If $G/Z(G)$ is cyclic, then G is abelian.

- Suppose $G/Z(G)$ is cyclic. So $G/Z(G) = \langle xZ(G)\rangle$, for some $x \in G$.
  Claim: Every $g \in G$ can be expressed in the form $g = x^a z$, for some $a \in \mathbb{Z}$ and some $z \in Z(G)$.
  Let $g \in G$. Then $gZ(G) \in G/Z(G)$. Thus, there exists $a \in \mathbb{Z}$, such that $gZ(G) = (xZ(G))^a$, i.e., $gZ(G) = x^a Z(G)$. So $(x^a)^{-1} g \in Z(G)$, i.e., there exists $z \in Z(G)$, such that $(x^a)^{-1} g = z$, or, equivalently, $g = x^a z$.
  Now, for all $g_1, g_2 \in G$, we have that $g_1 = x^{a_1} z_1$ and $g_2 = x^{a_2} z_2$, for some $a_1, a_2 \in \mathbb{Z}$, $z_1, z_2 \in Z(G)$. Therefore,
  $$\begin{aligned} g_1 g_2 &= (x^{a_1} z_1)(x^{a_2} z_2) = x^{a_1} x^{a_2} z_1 z_2 = x^{a_1 + a_2} z_2 z_1 \\ &= x^{a_2} x^{a_1} z_2 z_1 = x^{a_2} z_2 x^{a_1} z_1 = g_2 g_1, \end{aligned}$$
  showing that G is abelian.

Groups of Prime Squared Order

Corollary

If $|P| = p^2$, for some prime p, then P is abelian. More precisely, P is isomorphic to either Z_{p^2} or $Z_p \times Z_p$.

- Since $Z(P) \neq 1$, by the preceding theorem, $P/Z(P)$ is cyclic. Thus, by the preceding lemma, P is abelian.
  - If P has an element of order p^2, then P is cyclic.
  - If every nonidentity element of P has order p, let x be such a nonidentity element of P and let $y \in P - \langle x \rangle$. Since $|\langle x, y \rangle| > |\langle x \rangle| = p$, we must have that $P = \langle x, y \rangle$. Both x and y have order p, whence $\langle x \rangle \times \langle y \rangle = Z_p \times Z_p$. It now follows directly that the map $(x^a, y^b) \mapsto x^a y^b$ is an isomorphism from $\langle x \rangle \times \langle y \rangle$ onto P.

Conjugacy in S_n

- From linear algebra we know that, in the matrix group $\mathrm{GL}_n(F)$, conjugation is the same as "change of basis": $A \mapsto PAP^{-1}$.
- The situation in S_n is analogous:

Proposition

Let σ, τ be elements of the symmetric group S_n and suppose σ has cycle decomposition
$$(a_1\ a_2 \ldots a_{k_1})(b_1\ b_2 \ldots b_{k_2}) \cdots .$$
Then $\tau\sigma\tau^{-1}$ has cycle decomposition
$$(\tau(a_1)\ \tau(a_2) \ldots \tau(a_{k_1}))(\tau(b_1)\ \tau(b_2) \ldots \tau(b_{k_2})) \cdots ,$$
i.e., $\tau\sigma\tau^{-1}$ is obtained from σ by replacing each entry i in the cycle decomposition for σ by the entry $\tau(i)$.

- Observe that if $\sigma(i) = j$, then $\tau\sigma\tau^{-1}(\tau(i)) = \tau(j)$. Thus, if the ordered pair i, j appears in the cycle decomposition of σ, then the ordered pair $\tau(i), \tau(j)$ appears in the cycle decomposition of $\tau\sigma\tau^{-1}$.

Cycle Types and Partitions

- Example: Let $\sigma = (1\ 2)(3\ 4\ 5)(6\ 7\ 8\ 9)$ and let $\tau = (1\ 3\ 5\ 7)(2\ 4\ 6\ 8)$. Then
$$\tau\sigma\tau^{-1} = (3\ 4)(5\ 6\ 7)(8\ 1\ 2\ 9).$$

Definition (Cycle Type and Partition)

(1) If $\sigma \in S_n$ is the product of disjoint cycles of lengths $n_1, n_2, \ldots, n_r$, with $n_1 \leq n_2 \leq \cdots \leq n_r$ (including its 1-cycles), then the sequence of integers $n_1, n_2, \ldots, n_r$ is called the **cycle type** of σ.

(2) If $n \in \mathbb{Z}^+$, a **partition** of n is any nondecreasing sequence of positive integers whose sum is n.

- We proved that the cycle type of a permutation is unique.
Example: The cycle type of an m-cycle in S_n is
$$\underbrace{1, 1, \ldots, 1}_{n-m \text{ 1's}}, m.$$

Conjugacy Classes in S_n and Cycle Decomposition

Proposition

Two elements of S_n are conjugate in S_n if and only if they have the same cycle type. The number of conjugacy classes of S_n equals the number of partitions of n.

- By the preceding proposition, conjugate permutations have the same cycle type. Conversely, suppose the permutations σ_1 and σ_2 have the same cycle type. Order the cycles in nondecreasing length, including 1-cycles. Ignoring parentheses, each cycle decomposition is a list in which all the integers from 1 to n appear exactly once. Define τ to be the function which maps the i-th integer in the list for σ_1 to the i-th integer in the list for σ_2. Thus τ is a permutation. Since the parentheses appear at the same positions in each list, $\tau\sigma_1\tau^{-1} = \sigma_2$.
- Since there is a bijection between the conjugacy classes of S_n and the permissible cycle types and each cycle type for a permutation in S_n is a partition of n, the second assertion of the proposition follows.

Examples

(1) Let $\sigma_1 = (1)(3\ 5)(8\ 9)(2\ 4\ 7\ 6)$ and let $\sigma_2 = (3)(4\ 7)(8\ 1)(5\ 2\ 6\ 9)$. Then define τ by $\tau(1) = 3$, $\tau(3) = 4$, $\tau(5) = 7$, $\tau(8) = 8$, etc. Then $\tau = (1\ 3\ 4\ 2\ 5\ 7\ 6\ 9)$ and $\tau\sigma_1\tau^{-1} = \sigma_2$.

(2) Reorder σ_2 as $\sigma_2 = (3)(8\ 1)(4\ 7)(5\ 2\ 6\ 9)$. Then the corresponding τ is defined by $\tau(1) = 3$, $\tau(3) = 8$, $\tau(5) = 1$, $\tau(8) = 4$, etc. This gives the permutation $\tau = (1\ 3\ 8\ 4\ 2\ 5)(6\ 9\ 7)$ again with $\tau\sigma_1\tau^{-1} = \sigma_2$. Hence, there are many elements conjugating σ_1 into σ_2.

(3) If $n = 5$, the partitions of 5 and corresponding representatives of the conjugacy classes (with 1-cycles not written) are:

Partition of 5	Representative of Conjugacy Class
$1,1,1,1,1$	1
$1,1,1,2$	(1 2)
$1,1,3$	(1 2 3)
$1,4$	(1 2 3 4)
5	(1 2 3 4 5)
$1,2,2$	(1 2)(3 4)
$2,3$	(1 2)(3 4 5)

Centralizers of Cycles in S_n

- If σ is an m-cycle in S_n, then the number of conjugates of σ (i.e., the number of m-cycles) is $\frac{n \cdot (n-1) \cdot \cdots \cdot (n-m+1)}{m}$. By a preceding proposition, it equals the index of the centralizer of σ: $\frac{|S_n|}{|C_{S_n}(\sigma)|}$. Since $|S_n| = n!$, we obtain $|C_{S_n}(\sigma)| = m \cdot (n-m)!$.
  - The element σ certainly commutes with $1, \sigma, \sigma^2, \ldots, \sigma^{m-1}$.
  - It also commutes with any permutation in S_n whose cycles are disjoint from σ and there are $(n-m)!$ permutations of this type (the full symmetric group on the numbers not appearing in σ).

  The product of elements of these two types already accounts for $m \cdot (n-m)!$ elements commuting with σ. Thus, this is the full centralizer of a in S_n.

  So, if σ is an m-cycle in S_n, then $C_{S_n}(\sigma) = \{\sigma^i \tau : 0 \leq i \leq m-1, \tau \in S_{n-m}\}$, where S_{n-m} denotes the subgroup of S_n which fixes all integers appearing in the m-cycle σ (and is the identity subgroup if $m = n$ or $m = n-1$).

Normal Subgroups and Conjugacy Classes

- We use this discussion of the conjugacy classes in S_n to give a combinatorial proof of the simplicity of A_5.

Claim

The normal subgroups of a group G are the union of conjugacy classes of G, i.e., if $H \trianglelefteq G$, then for every conjugacy class $\mathcal{K}$ of G, either $\mathcal{K} \subseteq H$ or $\mathcal{K} \cap H = \emptyset$.

- If $\mathcal{K} \cap H = \emptyset$, we are done.
- If $\mathcal{K} \cap H \neq \emptyset$, there exists $x \in \mathcal{K} \cap H$. Then $gxg^{-1} \in gHg^{-1}$, for all $g \in G$. Since H is normal, $gHg^{-1} = H$. Hence H contains all the conjugates of x, i.e., $\mathcal{K} \subseteq H$.

A_n and 3-Cycles

Lemma

If $n \geq 3$, every element of A_n is a 3-cycle or a product of 3-cycles.

- If $\alpha \in A_n$, then α is a product of an even number of transpositions

$$\alpha = \tau_1 \tau_2 \cdots \tau_{2q-1} \tau_{2q}.$$

We may assume that adjacent τ's are distinct. As the transpositions can be grouped in pairs $\tau_{2i-1}\tau_{2i}$ it suffices to consider products $\tau\tau'$, where τ and τ' are transpositions.

  - If τ and τ' are not disjoint, then $\tau = (i\ j)$ and $\tau' = (i\ k)$. Then $\tau\tau' = (i\ k\ j)$.
  - If τ and τ' are disjoint, then $\tau = (i\ j)$ and $\tau' = (k\ \ell)$. Then

$$\tau\tau' = (i\ j)(k\ \ell) = (i\ j)(j\ k)(j\ k)(k\ \ell) = (i\ j\ k)(j\ k\ \ell).$$

Simplicity of A_5

Theorem

A_5 is a simple group.

- We show that if $H \trianglelefteq A_5$ and $H \neq 1$, then $H = A_5$.

  If H contains a 3-cycle, then, by normality, H contains all its conjugates. Thus, H contains all 3-cycles. By the preceding lemma, $H = A_5$. It suffices, therefore, to show that H contains a 3-cycle.

  Since $H \neq 1$, it contains some $\sigma \neq 1$. After a possible renaming, we may assume that it contains $\sigma = (1\ 2\ 3)$ or $\sigma = (1\ 2)(3\ 4)$ or $\sigma = (1\ 2\ 3\ 4\ 5)$.
  - If σ is a 3-cycle, then we are done.
  - If $\sigma = (1\ 2)(3\ 4)$, define $\tau = (1\ 2)(3\ 5)$. By normality, H contains $(\tau\sigma\tau^{-1})\sigma^{-1} = (3\ 5\ 4)$.
  - If $\sigma = (1\ 2\ 3\ 4\ 5)$, define $\rho = (1\ 3\ 2)$. H contains $\rho\sigma\rho^{-1}\sigma^{-1} = (1\ 3\ 4)$.

  Thus, in all cases H contains a 3-cycle.

Right Group Actions

- If in the definition of an action the group elements appear to the left of the set elements, the notion might be termed more precisely a **left group action**.
- One can analogously define the notion of a **right group action** of the group G on the nonempty set A as a map from $A \times G$ to A, denoted by $a \cdot g$, for $a \in A$ and $g \in G$, that satisfies:
  (1) $(a \cdot g_1) \cdot g_2 = a \cdot (g_1 g_2)$, for all $a \in A$, and $g_1, g_2 \in G$;
  (2) $a \cdot 1 = a$, for all $a \in A$.

  Example: Conjugation is often written as a right group action using the notation $a^g = g^{-1}ag$, for all $g, a \in G$.

  Similarly, for subsets S of G one defines $S^g = g^{-1}Sg$.

  In this notation the axioms for a right action are verified as follows, for all $g_1, g_2, a \in G$:
  - $a^1 = 1^{-1}a1 = a$;
  - $(a^{g_1})^{g_2} = (g_1^{-1}ag_1)^{g_2} = g_2^{-1}(g_1^{-1}ag_1)g_2 = (g_1g_2)^{-1}a(g_1g_2) = a^{(g_1g_2)}$.

  The two axioms take the form of the "laws of exponentiation".

Relation Between Left and Right Group Actions

- For arbitrary group actions, if we are given a left group action of G on A, then the map $A \times G \to A$, defined by $a \cdot g = g^{-1} \cdot a$ is a right group action.
- Conversely, given a right group action of G on A, we can form a left group action by $g \cdot a = a \cdot g^{-1}$.
- Call these pairs **corresponding group actions**.
- For any corresponding left and right actions the orbits are the same: In fact, for all $a, b \in A$ and all $g \in G$,

$$a = g \cdot b \quad \text{iff} \quad a = b \cdot g^{-1}.$$

  Thus, a and b are in the same left orbit iff they are in the same right orbit.

Subsection 4

Automorphisms

Automorphisms of a Group

Definition (Automorphism)

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 by $\text{Aut}(G)$.

- Note that composition of automorphisms is defined since the domain and range of each automorphism is the same.
- $\text{Aut}(G)$ is a group under composition of automorphisms, called the **automorphism group** of G.
- Automorphisms of a group G are, in particular, permutations of the set G, whence $\text{Aut}(G)$ is a subgroup of S_G.

Actions by Conjugation on a Normal Subgroup

Proposition

Let H be a normal subgroup of the group G. Then G acts by conjugation on H as automorphisms of H. More specifically, the action of G on H by conjugation is defined, for each $g \in G$, by $h \mapsto ghg^{-1}$, for each $h \in H$. For each $g \in G$, conjugation by g is an automorphism of H. The permutation representation afforded by this action is a homomorphism of G into $\mathrm{Aut}(H)$ with kernel $C_G(H)$. In particular, $G/C_G(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$.

- Let φ_g be conjugation by g. Because g normalizes H, φ_g maps H to itself. Since we have already seen that conjugation defines an action, it follows that:
  - $\varphi_1 = 1$ (the identity map on H);
  - $\varphi_a \circ \varphi_b = \varphi_{ab}$, for all $a, b \in G$.

  Thus, each φ_g gives a bijection from H to itself since it has a 2-sided inverse $\varphi_{g^{-1}}$.

Actions by Conjugation on a Normal Subgroup (Cont'd)

- Each φ_g is a homomorphism from H to H because, for all $h, k \in H$,

$$\begin{aligned} \varphi_g(hk) &= g(hk)g^{-1} = gh(g^{-1}g)kg^{-1} \\ &= (ghg^{-1})(gkg^{-1}) = \varphi_g(h)\varphi_g(k). \end{aligned}$$

This proves that conjugation by any fixed element of G defines an automorphism of H.

By the preceding remark, the permutation representation $\psi : G \to S_H$ defined by $\psi(g) = \varphi_g$ has image contained in the subgroup $\mathrm{Aut}(H)$ of S_H. Finally,

$$\begin{aligned} \ker\psi &= \{g \in G : \varphi_g = \mathrm{id}\} \\ &= \{g \in G : ghg^{-1} = h, \text{ for all } h \in H\} \\ &= C_G(H). \end{aligned}$$

The First Isomorphism Theorem implies the final statement of the proposition.

Consequences of the Proposition

- The action by conjugation on a normal subgroup must send subgroups to subgroups, elements of order n to elements of order n, etc.

Corollary

If K is any subgroup of the group G and $g \in G$, then $K \cong gKg^{-1}$. Conjugate elements and conjugate subgroups have the same order.

- Letting $G = H$ in the proposition shows that conjugation by $g \in G$ is an automorphism of G.

Corollary

For any subgroup H of a group G, the quotient group $N_G(H)/C_G(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$. In particular, $G/Z(G)$ is isomorphic to a subgroup of $\mathrm{Aut}(G)$.

- Since H is a normal subgroup of the group $N_G(H)$, the proposition applied with $N_G(H)$ playing the role of G, implies the first assertion. When $H = G$, $N_G(G) = G$ and $C_G(G) = Z(G)$.

Inner Automorphisms

Definition

Let G be a group and let $g \in G$. Conjugation by g is called an **inner automorphism** of G. The subgroup of $\text{Aut}(G)$ consisting of all inner automorphisms is denoted by $\text{Inn}(G)$.

- The collection of inner automorphisms of G is a subgroup of $\text{Aut}(G)$. By the preceding corollary, $\text{Inn}(G) \cong G/Z(G)$.
- If H is a normal subgroup of G, conjugation by an element of G when restricted to H is an automorphism of H but need not be an inner automorphism of H (see next slide).

Examples of Inner Automorphisms

(1) A group G is abelian if and only if every inner automorphism is trivial. If H is an abelian normal subgroup of G and H is not contained in $Z(G)$, then there is some $g \in G$, such that conjugation by g restricted to H is not an inner automorphism of H.

Example: Consider

$$\begin{array}{rcl} G & = & A_4 = \{1, (1\ 2\ 3), (1\ 3\ 2), (1\ 2\ 4), (1\ 4\ 2), (1\ 3\ 4), (1\ 4\ 3), \\ & & (2\ 3\ 4), (2\ 4\ 3), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}; \\ H & = & \{1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}; \\ g & = & \text{any 3-cycle.} \end{array}$$

(2) Since $Z(Q_8) = \langle -1 \rangle$, we have $\mathrm{Inn}(Q_8) \cong V_4$.

(3) Since $Z(D_8) = \langle r^2 \rangle$, we have $\mathrm{Inn}(D_8) \cong V_4$.

(4) Since for all $n \geq 3$, $Z(S_n) = 1$, we have $\mathrm{Inn}(S_n) \cong S_n$.

Information from Automorphism Groups of Subgroups

- Information about the automorphism group of a subgroup H of a group G translates into information about $N_G(H)/C_G(H)$.

  Example: If $H \cong Z_2$, then H has unique elements of orders 1 and 2. Thus, by the corollary, $\text{Aut}(H) = 1$. Thus, if $H \cong Z_2$, $N_G(H) = C_G(H)$.

  If, in addition, H is a normal subgroup of G, then $H \leq Z(G)$.

- The example illustrates that the action of G by conjugation on a normal subgroup H can be restricted by knowledge of the automorphism group of H.

  This in turn can be used to investigate the structure of G and obtain certain classification theorems.

Characteristic Subgroups

Definition (Characteristic Subgroup)

A subgroup H of a group G is called **characteristic in** G, denoted H char G, if every automorphism of G maps H to itself, i.e., $\sigma(H) = H$, for all $\sigma \in \mathrm{Aut}(G)$.

- Some results concerning characteristic subgroups:
  (1) Characteristic subgroups are normal.
  (2) If H is the unique subgroup of G of a given order, then H is characteristic in G.
  (3) If K char H and $H \trianglelefteq G$, then $K \trianglelefteq G$ (so, although "normality" is not a transitive property (i.e., a normal subgroup of a normal subgroup need not be normal), a characteristic subgroup of a normal subgroup is normal).
- The properties show that, in a certain sense, characteristic subgroups may be thought of as "strongly normal" subgroups.

Automorphism Group of Z_n

Proposition

The automorphism group of the cyclic group of order n is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$, an abelian group of order $\varphi(n)$, where φ is Euler's function.

- Let x be a generator of the cyclic group Z_n. If $\psi \in \mathrm{Aut}(Z_n)$, then $\psi(x) = x^a$, for some $a \in \mathbb{Z}$, and the integer a uniquely determines ψ. Denote this automorphism by ψ_a. As usual, since $|x| = n$, the integer a is only defined mod n. Since ψ_a is an automorphism, x and x^a must have the same order. Hence $(a, n) = 1$. Furthermore, for every a relatively prime to n, the map $x \mapsto x^a$ is an automorphism of Z_n. Hence, we have a surjective map $\Psi : \mathrm{Aut}(Z_n) \to (\mathbb{Z}/n\mathbb{Z})^\times$; $\psi_a \mapsto a \pmod{n}$. The map Ψ is a homomorphism: For all $\psi_a, \psi_b \in \mathrm{Aut}(Z_n)$, $\psi_a \circ \psi_b(x) = \psi_a(x^b) = (x^b)^a = x^{ab} = \psi_{ab}(x)$. So $\Psi(\psi_a \circ \psi_b) = \Psi(\psi_{ab}) = ab \pmod{n} = \Psi(\psi_a)\Psi(\psi_b)$. Finally, Ψ is clearly injective. Hence Ψ is an isomorphism.

Groups of Order pq

Claim: Let G be a group of order pq, where p and q are primes (not necessarily distinct) with $p \leq q$. If $p \nmid q-1$, then G is abelian.

If $Z(G) \neq 1$, Lagrange's Theorem forces $G/Z(G)$ to be cyclic. Hence G is abelian. Hence we may assume $Z(G) = 1$.

- Suppose every nonidentity element of G has order p. Then the centralizer of every nonidentity element has index q. Thus, the class equation for G reads $pq = 1 + kq$. This is impossible.
- Thus G contains an element x of order q. Let $H = \langle x \rangle$. Since H has index p and p is the smallest prime dividing $|G|$, the subgroup H is normal in G by a preceding corollary. Since $Z(G) = 1$, we must have $C_G(H) = H$. Thus $G/H = N_G(H)/C_G(H)$ is a group of order p isomorphic to a subgroup of $\mathrm{Aut}(H)$, by a preceding corollary. By a preceding proposition, $\mathrm{Aut}(H)$ has order $\varphi(q) = q - 1$. By Lagrange's Theorem, $p \mid q - 1$, contrary to assumption.

This shows that G must be abelian.

Groups of Order pq (Cont'd)

Claim: Let G be an abelian group of order pq, with p, q two different primes. Then G is cyclic.

Since $|G| = pq$, with p, q prime, there exist, by Cauchy's Theorem, elements $x, y \in G$, such that $|x| = p$ and $|y| = q$. We have

$$(xy)^{pq} = x^{pq}y^{pq} = (x^p)^q(y^q)^p = 1^q1^p = 1.$$

Therefore, we get that $|xy| \mid pq$. We show that $|xy| \neq 1, p, q$. Then $|xy| = pq$ and $G = \langle xy \rangle$.

- If $|xy| = 1$, then $xy = 1$. Then $y = x^{-1}$ whence $|y| = |x| = p$, a contradiction.
- If $|xy| = p$, then $y^p = x^py^p = (xy)^p = 1$. But then $q \mid p$, a contradiction.
- The case $|xy| = q$ is similar to the preceding one.

Subsection 5

Sylow's Theorem

p-Groups and Sylow's p-Subgroups

- Sylow's Theorem provides a partial converse to Lagrange's Theorem.

Definition (p-Groups and Sylow's p-Subgroups)

Let G be a group and let p be a prime.

(1) A group of order p^a, for some $a \geq 1$, is called a p-**group**. Subgroups of G which are p-groups are called p-**subgroups**.

(2) If G is a group of order $p^a m$, where $p \nmid m$, then a subgroup of order p^a is called a **Sylow** p-**subgroup** of G.

(3) The set of Sylow p-subgroups of G will be denoted by $\mathrm{Syl}_p(G)$.

The number of Sylow p-subgroups of G will be denoted by $n_p(G)$ (or just n_p, when G is clear from the context).

A Preliminary Lemma

Lemma

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

- Let $H = N_G(P) \cap Q$. Since $P \leq N_G(P)$, it is clear that $P \cap Q \leq H$. So, it suffices to prove the reverse inclusion. Since, by definition, $H \leq Q$, this is equivalent to showing $H \leq P$. We do this by demonstrating that PH is a p-subgroup of G containing both P and H. Since, P is a p-subgroup of G of largest possible order, we must have $PH = P$, i.e., $H \leq P$.

  Since $H \leq N_G(P)$, by a preceding corollary, PH is a subgroup. We know that $|PH| = \frac{|P||H|}{|P \cap H|}$. All the numbers in the above quotient are powers of p, so PH is a p-group. Moreover, P is a subgroup of PH so the order of PH is divisible by p^a, the largest power of p which divides $|G|$. These two facts force $|PH| = p^a = |P|$. This, in turn, implies $P = PH$ and $H \leq P$.

Sylow's Theorem

Theorem (Sylow's Theorem)

Let G be a group of order $p^a m$, where p is a prime not dividing m.

(1) Sylow p-subgroups of G exist, i.e., $\mathrm{Syl}_p(G) \neq \emptyset$.

(2) If P is a Sylow p-subgroup of G and Q is any p-subgroup of G, then there exists $g \in G$, such that $Q \leq gPg^{-1}$, i.e., Q is contained in some conjugate of P.
In particular, any two Sylow p-subgroups of G are conjugate in G.

(3) The number of Sylow p-subgroups of G is of the form $1 + kp$, i.e., $n_p \equiv 1 \pmod{p}$.
Further, n_p is the index in G of the normalizer $N_G(P)$ for any Sylow p-subgroup P, whence n_p divides m.

Proof of Sylow's Theorem Part (1)

- $\mathrm{Syl}_p(G) \neq \emptyset$: By induction on $|G|$.
  - If $|G| = 1$, there is nothing to prove.
  - Assume inductively the existence of Sylow p-subgroups for all groups of order less than $|G|$.
    - If p divides $|Z(G)|$, then by Cauchy's Theorem for abelian groups, $Z(G)$ has a subgroup N of order p. Let $\overline{G} = G/N$, so that $|\overline{G}| = p^{a-1}m$. By induction, $\overline{G}$ has a subgroup $\overline{P}$ of order p^{a-1}. If we let P be the subgroup of G containing N such that $P/N = \overline{P}$, then $|P| = |P/N||N| = p^a$. Thus, P is a Sylow p-subgroup of G.
    - Suppose p does not divide $|Z(G)|$. Let $g_1, g_2, \ldots, g_r$ be representatives of the distinct non-central conjugacy classes of G. The class equation for G is $|G| = |Z(G)| + \sum_{i=1}^r |G : C_G(g_i)|$. If $p \mid |G : C_G(g_i)|$, for all i, then since $p \mid |G|$, we would also have $p \mid |Z(G)|$, a contradiction. Thus, for some i, p does not divide $|G : C_G(g_i)|$. For this i, let $H = C_G(g_i)$. Then $|H| = p^a k$, where $p \nmid k$. Since $g_i \notin Z(G)$, $|H| < |G|$. By induction, H has a Sylow p-subgroup P, which of course is also a subgroup of G. Since $|P| = p^a$, P is a Sylow p-subgroup of G, which completes the induction.

Preparation for Sylow's Theorem Parts (2) and (3)

- By Part (1), there exists a Sylow p-subgroup P of G. Let $\{P_1, P_2, \ldots, P_r\} = \mathcal{S}$ include all conjugates of P, i.e., $\mathcal{S} = \{gPg^{-1} : g \in G\}$ and let Q be any p-subgroup of G. By definition of $\mathcal{S}$, G and, hence, also Q, acts by conjugation on $\mathcal{S}$. Write $\mathcal{S}$ as a disjoint union of orbits under this action by Q: $\mathcal{S} = \mathcal{O}_1 \cup \mathcal{O}_2 \cup \cdots \cup \mathcal{O}_s$, where $r = |\mathcal{O}_1| + \cdots + |\mathcal{O}_s|$ (r does not depend on Q, but the number of Q-orbits s does). By definition, G has only one orbit on $\mathcal{S}$, but a subgroup Q of G may have more than one orbit. Renumber the elements of $\mathcal{S}$ so that $P_i \in \mathcal{O}_i$, $1 \leq i \leq s$. Now $|\mathcal{O}_i| = |Q : N_Q(P_i)|$. By definition, $N_Q(P_i) = N_G(P_i) \cap Q$. By the lemma, $N_G(P_i) \cap Q = P_i \cap Q$. Thus, $|\mathcal{O}_i| = |Q : P_i \cap Q|$, $1 \leq i \leq s$.
- We show $r \equiv 1 \pmod{p}$: Take $Q = P_1$. Then, $|\mathcal{O}_1| = 1$. For all $i > 1$, $P_1 \neq P_i$. So $P_1 \cap P_i < P_1$. It follows $|\mathcal{O}_i| = |P_1 : P_1 \cap P_i| > 1$, $2 \leq i \leq s$. Since P_1 is a p-group, $|P_1 : P_1 \cap P_i|$ must be a power of p. Hence, $p \mid |\mathcal{O}_i|$, $2 \leq i \leq s$. So $r = |\mathcal{O}_1| + \sum_{i=2}^{s} |\mathcal{O}_i| \equiv 1 \pmod{p}$.

Proof of Sylow's Theorem Parts (2) and (3)

(2) If P is a Sylow p-subgroup of G and Q is any p-subgroup of G, then there exists $g \in G$, such that $Q \leq gPg^{-1}$, i.e., Q is contained in some conjugate of P:

Let Q be any p-subgroup of G. Suppose Q is not contained in P_i, for any $i \in \{1, 2, \ldots, r\}$, i.e., $Q \not\leq gPg^{-1}$, for any $g \in G$. Then $Q \cap P_i < Q$, for all i. By preceding slide, $|\mathcal{O}_i| = |Q : Q \cap P_i| > 1$. Thus, $p \mid |\mathcal{O}_i|$, for all i, whence p divides $|\mathcal{O}_1| + \cdots + |\mathcal{O}_s| = r$, contradictng $r \equiv 1 \pmod{p}$.

If Q is any Sylow p-subgroup of G, $Q \leq gPg^{-1}$, for some $g \in G$. Since $|gPg^{-1}| = |Q| = p^a$, we must have $gPg^{-1} = Q$.

(3) The number of Sylow p-subgroups of G is of the form $1 + kp$ and $n_p = |G : N_G(P)|$, for any Sylow p-subgroup P, whence $n_p \mid m$:

By Part (2), $\mathcal{S} = \mathrm{Syl}_p(G)$, since every Sylow p-subgroup of G is conjugate to P. So $n_p = r \equiv 1 \pmod{p}$. Since all Sylow p-subgroups are conjugate, $n_p = |G : N_G(P)|$, for any $P \in \mathrm{Syl}_p(G)$.

Normality of a Sylow p-Subgroup

- Note that the conjugacy part of Sylow's Theorem shows that any two Sylow p-subgroups of a group are isomorphic.

Corollary

Let P be a Sylow p-subgroup of G. Then the following are equivalent:

(1) P is the unique Sylow p-subgroup of G, i.e., $n_p = 1$.

(2) P is normal in G.

(3) P is characteristic in G.

(4) All subgroups generated by elements of p-power order are p-groups, i.e., if X is any subset of G, such that $|x|$ is a power of p, for all $x \in X$, then $\langle X \rangle$ is a p-group.

(1)$\Leftrightarrow$(2): If (1) holds, then $gPg^{-1} = P$, for all $g \in G$, since $gPg^{-1} \in \text{Syl}_p(G)$. Hence P is normal in G.
Conversely, if $P \trianglelefteq G$ and $Q \in \text{Syl}_p(G)$, then, by Sylow's Theorem, exists $g \in G$, such that $Q = gPg^{-1} = P$. Thus, $\text{Syl}_p(G) = \{P\}$.

Normality of a Sylow p-Subgroup (Cont'd)

(2)$\Leftrightarrow$(3): Since characteristic subgroups are normal, (3) implies (2).

Conversely, if $P \trianglelefteq G$, we just proved P is the unique subgroup of G of order p^a, whence P char G.

(1)$\Leftrightarrow$(4): Finally, assume (1) holds and suppose X is a subset of G, such that $|x|$ is a power of p, for all $x \in X$. By the conjugacy part of Sylow's Theorem, for each $x \in X$, there is some $g \in G$, such that $x \in gPg^{-1} = P$. Thus, $X \subseteq P$, whence $\langle X \rangle \leq P$, and $\langle X \rangle$ is a p-group.

Conversely, if (4) holds, let X be the union of all Sylow p-subgroups of G. If P is any Sylow p-subgroup, P is a subgroup of the p-group $\langle X \rangle$. Since P is a p-subgroup of G of maximal order, we must have $P = \langle X \rangle$.

Examples

- Let G be a finite group and let p be a prime.
  (1) If $p \nmid |G|$, the Sylow p-subgroup of G is the trivial group (and all parts of Sylow's Theorem hold trivially).
  If $|G| = p^a$, G is the unique Sylow p-subgroup of G.
  (2) A finite abelian group has a unique Sylow p-subgroup for each prime p. This subgroup consists of all elements x whose order is a power of p. It is sometimes called the p-**primary component** of the group.
  (3) S_3 has three Sylow 2-subgroups: $\{(1\ 2)\}, \{(2\ 3)\}$ and $\{(1\ 3)\}$. It has a unique (hence normal) Sylow 3-subgroup: $\{(1\ 2\ 3)\} = A_3$. Note that $3 \equiv 1 \pmod 2$.
  (4) A_4 has a unique Sylow 2-subgroup: $\{(1\ 2)(3\ 4), (1\ 3)(2\ 4)\} \cong V_4$. It has four Sylow 3-subgroups:
  $$\{(1\ 2\ 3)\},\ \{(1\ 2\ 4)\},\ \{(1\ 3\ 4)\} \text{ and } \{(2\ 3\ 4)\}.$$
  Note that $4 \equiv 1 \pmod 3$.
  (5) S_4 has $n_2 = 3$ and $n_3 = 4$. Since S_4 contains a subgroup isomorphic to D_8, every Sylow 2-subgroup of S_4 is isomorphic to D_8.

Tips for Applying Sylow's Theorem

- Most of the examples use Sylow's Theorem to prove that a group of a particular order is not simple.
- For groups of small order, the congruence condition of Sylow's Theorem alone is often sufficient to force the existence of a normal subgroup.
- The first step in any numerical application of Sylow's Theorem is to factor the group order into prime powers.
- The largest prime divisors of the group order tend to give the fewest possible values for n_p, which limits the structure of the group G.
- In some situations where Sylow's Theorem alone does not force the existence of a normal subgroup, but some additional argument (often involving studying the elements of order p for a number of different primes p) proves the existence of a normal Sylow subgroup.

Groups of Order pq, p and q Primes With $p < q$

Claim: Suppose $|G| = pq$, for primes p and q, with $p < q$. Let $P \in \mathrm{Syl}_p(G)$ and let $Q \in \mathrm{Syl}_q(G)$. Then Q is normal in G and, if P is also normal in G, then G is cyclic.

The three conditions: $n_q = 1 + kq$, for some $k \geq 0$, n_q divides p and $p < q$, together force $k = 0$. Since $n_q = 1$, $Q \trianglelefteq G$.
Since n_p divides the prime q, we must have $n_p = 1$ or q.

Suppose $P \trianglelefteq G$. Let $P = \langle x \rangle$ and $Q = \langle y \rangle$. Since $P \trianglelefteq G$, $G/C_G(P)$ is isomorphic to a subgroup of $\mathrm{Aut}(Z_p)$. The latter group has order $p - 1$. Lagrange's Theorem together with the observation that neither p nor q can divide $p - 1$ imply that $G = C_G(P)$. In this case $x \in P \leq Z(G)$. So x and y commute. This means $|xy| = pq$. Hence, in this case G is cyclic: $G \cong Z_{pq}$.

Groups of Order 30

Claim Let G be a group of order 30. Then G has a normal subgroup isomorphic to Z_{15}.

Note that any subgroup of order 15 is necessarily normal (index 2) and cyclic (preceding result). So it is only necessary to show there exists a subgroup of order 15. We give an argument which illustrates how Sylow's Theorem can be used in conjunction with a counting of elements of prime order to produce a normal subgroup:

Let $P \in \mathrm{Syl}_5(G)$ and let $Q \in \mathrm{Syl}_3(G)$. If either P or Q is normal in G, then PQ is a group of order 15.

- Note, also, that, if either P or Q is normal, then both P and Q are characteristic subgroups of PQ.
- Moreover, since $PQ \trianglelefteq G$, both P and Q are normal in G.

We assume, therefore, that neither Sylow subgroup is normal.

Groups of Order 30 (Cont'd)

- We assume that neither Sylow subgroup $P \in \mathrm{Syl}_5(G)$ or $Q \in \mathrm{Syl}_3(G)$ is normal. The only possibilities by Part (3) of Sylow's Theorem are $n_5 = 6$ and $n_3 = 10$.
  - Each element of order 5 lies in a Sylow 5-subgroup;
  - Each Sylow 5-subgroup contains 4 nonidentity elements;
  - By Lagrange's Theorem, distinct Sylow 5-subgroups intersect in the identity.

  Thus, the number of elements of order 5 in G is the number of nonidentity elements in one Sylow 5-subgroup times the number of Sylow 5-subgroups. This would be $4 \cdot 6 = 24$ elements of order 5.

  By similar reasoning, the number of elements of order 3 would be $2 \cdot 10 = 20$.

  This is absurd since a group of order 30 cannot contain $24 + 20 = 44$ distinct elements. One of P or Q (hence, both) must be normal in G.

Groups of Order 12

Claim: Let G be a group of order 12. Then either G has a normal Sylow 3-subgroup or $G \cong A_4$ (in the latter case G has a normal Sylow 2-subgroup).

Suppose $n_3 \neq 1$ and let $P \in \mathrm{Syl}_3(G)$. Since $n_3 \mid 4$ and $n_3 \equiv 1 \pmod{3}$, it follows that $n_3 = 4$. Since distinct Sylow 3-subgroups intersect in the identity and each contains two elements of order 3, G contains $2 \cdot 4 = 8$ elements of order 3. Since $|G : N_G(P)| = n_3 = 4$, $N_G(P) = P$. Now G acts by conjugation on its four Sylow 3-subgroups. So this action affords a permutation representation. Its kernel K is the subgroup of G which normalizes all Sylow 3-subgroups of G. In particular, $K \leq N_G(P) = P$. Since P is not normal in G, by assumption, $K = 1$, i.e., φ is injective and $G \cong \varphi(G) \leq S_4$. Since G contains 8 elements of order 3 and there are precisely 8 elements of order 3 in S_4, all contained in A_4, it follows that $\varphi(G)$ intersects A_4 in a subgroup of order at least 8. Since both groups have order 12 it follows that $\varphi(G) = A_4$, so that $G \cong A_4$.

Groups of Order p^2q, p and q Distinct Primes

Claim: Let G be a group of order p^2q. Then G has a normal Sylow subgroup (for either p or q).

Let $P \in \mathrm{Syl}_p(G)$ and let $Q \in \mathrm{Syl}_q(G)$.

- Suppose, first, $p > q$. Since $n_p \mid q$ and $n_p = 1 + kp$, we must have $n_p = 1$. Thus, $P \trianglelefteq G$.
- Consider now the case $p < q$.
  - If $n_q = 1$, Q is normal in G.
  - Assume $n_q > 1$, i.e., $n_q = 1 + tq$, for some $t > 0$. Now n_q divides p^2. So $n_q = p$ or p^2. Since $q > p$, we cannot have $n_q = p$, Hence, $n_q = p^2$. Thus, $tq = p^2 - 1 = (p-1)(p+1)$. Since q is prime, either $q \mid p - 1$ or $q \mid p + 1$. The former is impossible since $q > p$ so the latter holds. Since $q > p$, but $q \mid p + 1$, we must have $q = p + 1$. This forces $p = 2$, $q = 3$ and $|G| = 12$.

    The result now follows from the preceding example.

Groups of Order 60

- We use the technique of changing from one prime to another and induction in order to study groups of order 60.

Proposition

If $|G| = 60$ and G has more than one Sylow 5-subgroup, then G is simple.

- Suppose by way of contradiction that $|G| = 60$ and $n_5 > 1$, but that there exists H a normal subgroup of G with $H \neq 1$ or G. By Sylow's Theorem, the only possibility for n_5 is 6. Let $P \in \mathrm{Syl}_5(G)$, so that $|N_G(P)| = 10$, since its index is n_5.
  - If $5 \mid |H|$, then H contains a Sylow 5-subgroup of G. Since H is normal, it contains all 6 conjugates of this subgroup. In particular, $|H| \geq 1 + 6 \cdot 4 = 25$. The only possibility is $|H| = 30$. This leads to a contradiction since a previous example proved that any group of order 30 has a normal (hence unique) Sylow 5-subgroup. This argument shows 5 does not divide $|H|$, for any proper normal subgroup H of G.

Groups of Order 60 (Cont'd)

- We have assumed $|G| = 60$ and $n_5 > 1$, but that there exists H a normal subgroup of G with $H \neq 1$ or G. We reasoned that $n_5 = 6$, we let $P \in \mathrm{Syl}_5(G)$ (thus, $|N_G(P)| = 10$), and showed that $5 \nmid |H|$.
  - If $|H| = 6$ or 12, H has a normal, hence characteristic, Sylow subgroup, which is therefore also normal in G. Replacing H by this subgroup, if necessary, we may assume $|H| = 2$, 3 or 4. Let $\overline{G} = G/H$, so $|\overline{G}| = 30$, 20 or 15. In each case, $\overline{G}$ has a normal subgroup $\overline{P}$ of order 5 by previous results. If we let H_1 be the complete preimage of $\overline{P}$ in G, then $H_1 \trianglelefteq G$, $H_1 \neq G$ and $5 \mid |H_1|$. This contradicts the preceding paragraph and completes the proof.

Corollary

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, so the result follows immediately from the proposition.

Simple Group of Order 60

Proposition

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

- Let G be a simple group of order 60, so $n_2 = 3$, 5 or 15. Let $P \in \mathrm{Syl}_2(G)$ and let $N = N_G(P)$, so $|G : N| = n_2$.
  Observe that G has no proper subgroup H of index less that 5:
  If H were a subgroup of G of index 4, 3 or 2, then, by a preceding theorem, G would have a normal subgroup K contained in H, with G/K isomorphic to a subgroup of S_4, S_3 or S_2. Since $K \neq G$, simplicity forces $K = 1$. This is impossible since 60 $(= |G|)$ does not divide 4!. This argument shows, in particular, that $n_2 \neq 3$.
- If $n_2 = 5$, then N has index 5 in G. So the action of G by left multiplication on the set of left cosets of N gives a permutation representation of G into S_5. Since the kernel of this representation is a proper normal subgroup and G is simple, the kernel is 1 and G is isomorphic to a subgroup of S_5.

Simple Group of Order 60 (Cont'd)

- We continue with the case $n_2 = 5$: We discovered that G is isomorphic to a subgroup of S_5. Identifying G with this isomorphic copy so that we may assume $G \leq S_5$. If G is not contained in A_5, then $S_5 = GA_5$. By the Second Isomorphism Theorem, $A_5 \cap G$ is of index 2 in G. Since G has no (normal) subgroup of index 2, this is a contradiction. This argument proves $G \leq A_5$.

  Since $|G| = |A_5|$, the isomorphic copy of G in S_5 coincides with A_5.

Simple Group of Order 60 (The Case $n_2 = 15$)

- Finally, assume $n_2 = 15$.

  If, for all distinct Sylow 2-subgroups P and Q of G, $P \cap Q = 1$, then the number of nonidentity elements in Sylow 2-subgroups of G would be $(4-1) \cdot 15 = 45$. But $n_5 = 6$, whence the number of elements of order 5 in G is $(5-1) \cdot 6 = 24$, accounting for 69 elements. This contradiction proves that there exist distinct Sylow 2-subgroups P and Q, with $|P \cap Q| = 2$.

  Let $M = N_G(P \cap Q)$. Since P and Q are abelian (being groups of order 4), P and Q are subgroups of M. Since G is simple, $M \neq G$. Thus 4 divides $|M|$ and $|M| > 4$ (otherwise, $P = M = Q$). The only possibility is $|M| = 12$, i.e., M has index 5 in G (recall M cannot have index 3 or 1). But now the argument of the preceding paragraph, applied to M in place of N, gives $G \cong A_5$. This leads to a contradiction in this case because $n_2(A_5) = 5$.

Subsection 6

The Simplicity of A_n

Simplicity of A_n

- There are a number of proofs of the simplicity of A_n, $n \geq 5$.
  - The most elementary involves showing A_n is generated by 3-cycles and that a normal subgroup must contain one 3-cycle, hence must contain all the 3-cycles so cannot be a proper subgroup.
  - We use, next, a less computational approach.
- Note that A_3 is an abelian simple group and that A_4 is not simple ($n_2(A_4) = 1$).

Theorem

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

- By induction on n.
  - The result has already been established for $n = 5$.
  - So assume $n \geq 6$ and let $G = A_n$. Assume there exists $H \trianglelefteq G$, with $H \neq 1$ or G. For each $i \in \{1, 2, \ldots, n\}$, let G_i be the stabilizer of i in the natural action of G on $i \in \{1, 2, \ldots, n\}$. Thus, $G_i \leq G$ and $G_i \cong A_{n-1}$. By induction, G_i is simple for $1 \leq i \leq n$.

Simplicity of A_n: If $\tau \neq 1$, then, for all i, $\tau(i) \neq i$

- We continue with the Induction Step:
  - Suppose first that there is some $\tau \in H$, with $\tau \neq 1$, but $\tau(i) = i$, for some $i \in \{1, 2, \ldots, n\}$. Since $\tau \in H \cap G_i$ and $H \cap G_i \trianglelefteq G_i$, by the simplicity of G_i, we must have $H \cap G_i = G_i$, i.e., $G_i \leq H$. Since, for all σ, $\sigma G_i \sigma^{-1} = G_{\sigma(i)}$, we get, for all i, $\sigma G_i \sigma^{-1} \leq \sigma H \sigma^{-1} = H$. Thus, $G_j \leq H$, for all $j \in \{1, 2, \ldots, n\}$. Any $\lambda \in A_n$ may be written as a product of an even number $2t$ of transpositions, so $\lambda = \lambda_1 \lambda_2 \cdots \lambda_t$, where λ_k is a product of two transpositions. Since $n > 4$, each $\lambda_k \in G_j$, for some j. Hence, $G = \langle G_1, G_2, \ldots, G_n \rangle \leq H$, which is a contradiction.

  We conclude that:

  If $\tau \neq 1$ is an element of H, then $\tau(i) \neq i$, for all $i \in \{1, 2, \ldots, n\}$, i.e., no nonidentity element of H fixes any element of $\{1, 2, \ldots, n\}$.

Simplicity of A_n: Conclusion

It follows that:

If τ_1, τ_2 are elements of H, with $\tau_1(i) = \tau_2(i)$, for some i, then $\tau_1 = \tau_2$, since then $\tau_2^{-1}\tau_1(i) = i$.

- Now, we conclude the Induction Step:
  - Suppose there exists a $\tau \in H$, such that the cycle decomposition of τ contains a cycle of length ≥ 3, say $\tau = (a_1\ a_2\ a_3 \ldots)(b_1\ b_2 \ldots)\cdots$. Let $\sigma \in G$ be an element with $\sigma(a_1) = a_1$, $\sigma(a_2) = a_2$, but $\sigma(a_3) \neq a_3$ (such a σ exists in A_n, since $n \geq 5$). Then, $\tau_1 = \sigma\tau\sigma^{-1} = (a_1\ a_2\ \sigma(a_3)\ldots)(\sigma(b_1)\ \sigma(b_2)\ldots)\cdots$. So τ and τ_1 are distinct elements of H with $\tau(a_1) = \tau_1(a_1) = a_2$, contrary to the preceding conclusion. This proves that only 2-cycles can appear in the cycle decomposition of nonidentity elements of H.
  - Let $\tau \in H$, with $\tau \neq 1$, so that $\tau = (a_1\ a_2)(a_3\ a_4)(a_5\ a_6)\cdots$ ($n \geq 6$ is used here). Let $\sigma = (a_1\ a_2)(a_3\ a_5) \in G$. Then $\tau_1 = \sigma\tau\sigma^{-1} = (a_1\ a_2)(a_5\ a_4)(a_3\ a_6)\cdots$. Hence τ and τ_1 are distinct elements of H with $\tau(a_1) = \tau_1(a_1) = a_2$, again contrary to the previous conclusion.