Shandong University | Advanced Modern Algebra

Lecture 2 & 3: Group Actions

Mar. 3, 2023

Lecturer: Bin Guan

This lecture refers to §1.7, §2.2 and Chapter 4 in [1]. All the equation numbers without reference labels are from this book.

1 Group actions

Group actions will be a powerful tool which we shall use both for proving theorems for abstract groups and for unravelling the structure of specific examples. Moreover, the concept of an "action" is a theme which will recur throughout the text as a method for studying an algebraic object by seeing how it can act on other structures.

1.1 Definitions

A **(left) group action** of a group G on a set A is a map from $G \times A$ to A (written as $g.a$ or $g(a)$, for all $g \in G$ and $a \in A$) satisfying the following properties:

(1) $g_1.(g_2.a) = (g_1 g_2).a$ for all $g_1, g_2 \in G$, $a \in A$, and

(2) $e.a = a$ for all $a \in A$.

The expression $g.a$ will usually be written simply as ga when there is no danger of confusing this map with, say, the group operation (remember, . is not a binary operation and ga is always a member of A). We denote the (left) group action by $G \curvearrowright A$.

Exercise ([1] §1.7)**.** *Let the group G act on the set A. For each fixed $g \in G$ we get a map $\sigma_g : A \to A$ defined by $\sigma_g(a) \coloneqq ga$. Show that*

(i) for each fixed $g \in G$, σ_g is a permutation of A, and

(ii) the map from G to S_A defined by $g \mapsto \sigma_g$ is a homomorphism.

*Reversely, if $\varphi : G \to S_A$ is any homomorphism from a group G to the symmetric group on a set A, show that the map from $G \times A$ to A defined by $g.a := \varphi(g)(a)$ for all $g \in G$ and all $a \in A$ satisfies the properties of a group action of G on A. The homomorphism from G to S_A given above is called the **permutation representation** associated to the given action.*

If G acts on a set A and distinct elements of G induce distinct permutations of A, the action is said to be **faithful**. A faithful action is therefore one in which the associated permutation representation is injective, i.e. an action is faithful if its kernel is the identity.

The **kernel** of the action of G on A is defined to be $\{g \in G \mid g.a = a \text{ for all } a \in A\}$, namely the elements of G which fix all the elements of A. Note that the kernel of an action is precisely the same as the kernel of the associated permutation representation; in particular, the kernel 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 [the preimage of one element] of the permutation representation φ). In particular an action of G on A may also be viewed as a faithful action of the quotient group $G/\ker\varphi$ on A.

An action is called the **trivial action** and G is said to act **trivially** on A if the kernel of the action is all of G. This action is not faithful when $|G| > 1$. Note that distinct elements of G induce the same permutation on A (in this case the identity permutation). The associated permutation representation $G \to S_A$ is the trivial homomorphism which maps every element of G to the identity.

If G is a group acting on a set A and a is some fixed element of A, the **stabilizer** of a in G is the set

$$G_a = \mathrm{Stab}_G(a) := \{g \in G \mid g.a = a\}.$$

For any $a \in A$, 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 $\ker\varphi = \cap_{a\in A} G_a$.

Exercise ([1] §2.2)**.** *Show that the stabilizer G_a of an element $a \in A$ is a subgroup of G.*

Let G be a group acting on a set A. The relation $\sim$ on A defined by

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

is an equivalence relation. For each $a \in A$ the equivalence class of a under $\sim$ is called the **orbit** of a under the action of G, and is denoted by $\mathcal{O}_a$ or $\mathrm{orb}_G(a)$.

The orbits under the action of G partition the set A. 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 $a = g.b$.

Proposition ([1] §4.1 Proposition 2, the Orbit–Stabilizer Theorem)**.** *Let G be a group acting on the nonempty set A. For any $a \in A$, the map $gG_a \mapsto g.a$ is a bijection from G/G_a, the set of left cosets of G_a in G, to the orbit $\mathcal{O}_a$ of a.*

In particular, if $\mathcal{O}_a$ is a finite set, then its number of elements $|\mathcal{O}_a|$ is equal to $[G : G_a]$, the index of the stabilizer of a.

1.2 Examples

Example. *The axioms for a vector space V over a field F include the two axioms that the multiplicative group $F^\times$ act on the set V. Thus vector spaces are familiar examples of actions of multiplicative groups of fields where there is even more structure (in particular, V must be an*

abelian group) which can be exploited. In the special case when $V = \mathbb{R}^n$ and $F = \mathbb{R}$ the action is specified by

$$\alpha.(r_1, r_2, \ldots, r_n) \coloneqq (\alpha r_1, \alpha r_2, \ldots, \alpha r_n)$$

for all $\alpha \in \mathbb{R}^\times$, $(r_1, r_2, \ldots, r_n) \in \mathbb{R}^n$, where αr_i is just multiplication of two real numbers.

This action is faithful, but not transitive. The orbit of the zero vector does not contain any nonzero vector, and its stabilizer is the whole group $F^\times$.

Given a nonzero vector, what is its orbit and stabilizer?

Example. *If we fix a labelling of the vertices of a regular n-gon ($n \geq 3$), each element α of the dihedral group D_{2n} gives rise to a permutation σ_α of $\{1, 2, \ldots, n\}$ by the way the symmetry α permutes the corresponding vertices. The map of $D_{2n} \times \{1, 2, \ldots, n\}$ onto $\{1, 2, \ldots, n\}$ defined by $(\alpha, i) \mapsto \sigma_\alpha(i)$ (i.e. $\alpha.i \coloneqq \sigma_\alpha(i)$) defines a group action $D_{2n} \curvearrowright \{1, 2, \ldots, n\}$.*

This action is faithful: distinct symmetries of a regular n-gon induce distinct permutations of the vertices.

This action is also transitive: the vertex labelled 1 can move to any vertex a by taking a rotation.

The stabilizer of any vertex a is the subgroup $\{1, \tau\}$ of D_{2n}, where τ is the reflection about the line of symmetry passing through vertex a and the center of the n-gon.

The kernel of this action is the identity subgroup: only the identity symmetry fixes every vertex.

When $n = 3$ the action of D_6 on the three (labelled) vertices of a triangle gives an injective homomorphism from D_6 to S_3. Since these groups have the same order, this map must also be surjective, i.e., is an isomorphism $D_6 \cong S_3$. Geometrically it says that any permutation of the vertices of a triangle is a symmetry.

The analogous statement is not true for any n-gon with $n \geq 4$ (just by order considerations we cannot have D_{2n} isomorphic to S_n for any $n \geq 4$).

Exercise ([1] §1.7 Exercise 11)**.** *Write out the cycle decomposition of the eight permutations in S_4 corresponding to the elements of D_8 given by the action of D_8 on the vertices of a square.*

Exercise. *Find the order of the symmetry group of the cube using the orbit-stabilizer theorem.*

Exercise. *Consider the action of the special linear group*

$$\mathrm{SL}_2(\mathbb{R}) \coloneqq \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(\mathbb{R}) : ad - bc = 1 \right\}$$

on the upper half plane $\mathcal{H} = \{x + iy \mid y > 0\}$ defined by

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} z \coloneqq \frac{az + b}{cz + d}.$$

By taking $a = i$ in the orbit-stabilizer theorem, show that there is a bijection from $\mathrm{SL}_2(\mathbb{R})/\mathrm{SO}_2$ to $\mathcal{H}$, where

$$\mathrm{SO}_2 \coloneqq \left\{ \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} : \theta \in \mathbb{R} \right\}$$

is the special orthogonal group. (Actually this bijection is a homeomorphism of topological spaces.)

2 Applications of group actions

2.1 The left regular action

Let G be any group and let $A = G$. Define a map from $G \times A$ to A by $g.a := ga$ for each $g \in G$ and $a \in A$, where ga on the right hand side is the product of g and a in the group G. This gives a group action of G on itself, where each (fixed) $g \in G$ permutes the elements of G by **left multiplication**:

$$g.a := ga \quad \text{for all } g, a \in G$$

(or, if G is written additively, we get $g.a := g + a$ and call this **left translation**). This action is called the **left regular action** of G on itself. The permutation representation afforded by left multiplication on the elements of G is called the **left regular representation** of G.

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. In this way the elements of G are listed as $g_1, g_2, \ldots g_n$ and for each $g \in G$ the permutation σ_g may be described as a permutation of the indices $1, 2, \ldots, n$ as follows:

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

Example. *Let $G = V_4 = \{e, a, b, c\}$ be the Klein 4-group with multiplication defined by*

$$a^2 = b^2 = e, \ ab = ba = c.$$

Label the group elements e, a, b, c with the integers $1, 2, 3, 4$, respectively. In the permutation representation associated to the action of the Klein 4-group on itself by left multiplication, under this labelling we compute that

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

which explicitly gives the permutation representation $V_4 \to S_4$ associated to this action under this labelling.

Exercise ([1] §1.7 Exercise 13)**.** *Show that the left regular action is transitive and faithful.*

Theorem ([1] §4.2 Corollary 4, 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.*

Proof. Consider the left regular representation $\varphi : G \to S_G$ of G. The above exercise shows that $\ker \varphi$ is trivial. The fundamental homomorphism theorem implies that 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. For example, we exhibited an isomorphism of the Klein 4-group V_4 with the subgroup

$$\{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} = \langle (1\ 2)(3\ 4), (1\ 3)(2\ 4) \rangle$$

of S_4. Subgroups of symmetric groups are called permutation groups, so Cayley's Theorem states that every group is isomorphic to a permutation group.

One might think that we could study all groups more effectively by simply studying subgroups of symmetric groups (and all finite groups by studying subgroups of S_n, for all n). This approach alone is neither computationally nor theoretically practical, since to study groups of order n we would have to work in the much larger group S_n.

We now consider a generalization of the action of a group by left multiplication on the set of its elements. Let H be any subgroup of G and let G/H be the set of all left cosets of H in G. Define an action of G on G/H by

$$g.aH \coloneqq gaH \quad \text{for all } g \in G, aH \in G/H$$

where gaH is the left coset with representative ga. One easily checks that this satisfies the two axioms for a group action, i.e., that G does act on the set of left cosets of H by left multiplication.

In the special case when H is the identity subgroup of G the coset aH is just $\{a\}$, and 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.

Exercise ([1] §4.2 Theorem 3)**.** *Let G be a group, H be a subgroup of G and let G act by left multiplication on the set G/H of left cosets of H in G. Let π_H be the associated permutation representation afforded by this action. Find the stabilizer in G of each point $xH \in G/H$, and find the kernel of the action (i.e., the kernel of π_H).*

2.2 Acting by conjugation

Let G be any group and we first consider G acting on itself (i.e., $A = G$) by conjugation:

$$g.a \coloneqq gag^{-1} \quad \text{for all } g \in G,\ a \in G$$

where gag^{-1} is computed in the group G as usual. This definition satisfies the two axioms for a group action.

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, denoted by $[a]$ or $\mathrm{Conj}(a)$, are called the **conjugacy classes** of G.

Example. *If G is an abelian group then the action of G on itself by conjugation is the trivial action: $g.a = a$, for all $g, a \in G$; and for each $a \in G$ the conjugacy class of a is $\{a\}$.*

Example. *If $|G| > 1$ then, unlike the action by left multiplication, G does not act transitively on itself by conjugation because $\{e\}$ 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:*

$$Z(G) \coloneqq \{g \in G \mid gx = xg \text{ for all } x \in G\}.$$

As in the case of a group acting on itself by left multiplication, the action by conjugation can be generalized. If S is any subset of G, define

$$gSg^{-1} \coloneqq \{gsg^{-1} \mid s \in S\}.$$

A group G acts on the set $\mathcal{P}(G)$ of all subsets of itself by defining $g.S \coloneqq gSg^{-1}$ for any $g \in G$ and $S \in \mathcal{P}(G)$. This defines a group action of G on $\mathcal{P}(G)$.

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).

2.2.1 The class equation

We now apply the Orbit–Stabilizer Theorem to the action of G by conjugation. It proves 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

$$G_S = \{g \in G \mid gSg^{-1} = S\} =: N_G(S)$$

is the **normalizer** of S in G. We summarize this as

Proposition ([1] §4.3 Proposition 6)**.** *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 $s \in G$ is the index of the centralizer of s, $[G : C_G(s)]$.*

Proof. The second assertion of the proposition follows from the observation that $N_G(\{s\}) = C_G(s)$. □

Exercise. *If $H \leq G$, show that $H \trianglelefteq N_G(H) \leq G$.*

Actually, $N_G(H)$ is the largest subgroup of G in which H is normal (cf. [1] §3.1 Exercise 31).

Recall (cf. [1] §2.2) that, if S is a subset of G, the **centralizer** of S in G is defined as

$$C_G(S) \coloneqq \{g \in G \mid gsg^{-1} = s \text{ for all } s \in S\} = \{g \in G \mid gs = sg \text{ for all } s \in S\},$$

i.e., $C_G(S)$ is the set of elements of G which commute with every element of S. In the special case when $S = \{s\}$ we shall write simply $C_G(s)$ instead of $C_G(\{s\})$. In this case $s^n \in C_G(s)$ for all $n \in \mathbb{Z}$. Note that

$$Z(G) = C_G(G) = \bigcap_{s \in G} C_G(s).$$

Example. *Let $G = S_3$ and let S be the subgroup $\{(1), (1\ 2)\}$.*

One can compute directly that $C_{S_3}(S) = S$ (cf. [1] §4.3 Proposition 10). Alternatively, since an element commutes with its powers, $S \leq C_{S_3}(S)$. By Lagrange's Theorem (cf. [1] §3.2 Theorem 8) the order of the subgroup $C_{S_3}(S)$ of S_3 divides $|S_3| = 6$. Also by Lagrange's Theorem applied to the subgroup S of the group $C_{S_3}(S)$ we have that 2 divides $|C_{S_3}(S)|$. The only possibilities are: $|C_{S_3}(S)| = 2$ or 6. If the latter occurs, $C_{S_3}(S) = S_3$, i.e., $S \subseteq Z(S_3)$; this is a contradiction because $(1\ 2)$ does not commute with $(1\ 2\ 3)$. Thus $|C_{S_3}(S)| = 2$ and so $C_{S_3}(S) = S = \{(1), (1\ 2)\}$.

Analogously one can show that $C_{S_3}\big((1\ 2\ 3)\big) = \{(1), (1\ 2\ 3), (1\ 2\ 3)^2 = (1\ 3\ 2)\}$.

Next note that $N_{S_3}(S) = S$ because $\sigma \in N_{S_3}(S)$ if and only if

$$\{\sigma(1)\sigma^{-1},\ \sigma(1\ 2)\sigma^{-1}\} = \{(1), (1\ 2)\}.$$

Since $\sigma(1)\sigma^{-1} = (1)$, this equality of sets occurs if and only if $\sigma(1\ 2)\sigma^{-1} = (1\ 2)$ as well, i.e., if and only if $\sigma \in C_{S_3}(S)$.

The center of S_3 is the identity because $Z(S_3) \subseteq C_{S_3}(S) = S$ and $(1\ 2) \notin Z(S_3)$.

Exercise ([1] §2.2 Exercise 7)**.** *Determine $Z(D_{2n})$ with $n \geq 3$.*

The action of G on itself by conjugation partitions G into the conjugacy classes of G, whose orders can be computed by the above proposition. Since the sum of the orders of these conjugacy classes is the order of G, we obtain the following important relation among these orders.

Theorem ([1] §4.3 Theorem 7, 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*

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

Proof. 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 $Z(G) = \{z_1 = e, z_2, \ldots, z_m\}$, 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 K_i for each i. Then the full set of conjugacy classes of G is given by

$$\{1\},\ \{z_2\},\ \ldots,\ \{z_m\},\ \mathcal{K}_1,\ \mathcal{K}_2,\ \ldots,\ \mathcal{K}_r.$$

Since these partition G we have

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

where $|\mathcal{K}_i|$ is given by the Orbit–Stabilizer Theorem. This proves the class equation. □

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

Example. *Recall that $Z(S_3) = \{(1)\}$, $[S_3 : C_{S_3}\big((1\ 2)\big)] = 6/2 = 3$ and $[S_3 : C_{S_3}\big((1\ 2\ 3)\big)] = 6/3 = 2$. The conjugacy classes of S_3 are*

$$\{1\},\ \{(1\ 2), (2\ 3), (1\ 3)\},\ \{(1\ 2\ 3), (1\ 3\ 2)\}.$$

The class equation for this group is $|S_3| = 1 + 3 + 2$.

Note in particular that all the summands on the right hand side of the class equation are divisors of the group order since they are indices of subgroups of G. This restricts their possible values (cf. [1] §4.3 Exercise 6, for example).

An application of the class equation is to show that groups of prime power order have nontrivial centers, which is the starting point for the study of groups of prime power order.

Theorem ([1] §4.3 Theorem 8)**.** *If p is a prime and P is a group of prime power order p^α for some $\alpha \in \mathbb{Z}_{>0}$, then P has a nontrivial center: $Z(P) \neq \{e\}$.*

Proof. By the class equation

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

where $g_1, \ldots, g_r \notin Z(P)$ are representatives of the distinct non-central conjugacy classes.

By definition, $C_P(g_i) \leq P$ for each i, so $p \mid [P : C_P(g_i)]$ (the index cannot be 1, otherwise $C_P(g_i) = P \Rightarrow g_i \in Z(P)$). Since p also divides $|P|$ it follows that p divides $|Z(P)| \geq 1$ (because $e \in Z(P)$), hence the center must be nontrivial. □

Exercise ([1] §4.3 Corollary 9 & §3.1 Exercise 36)**.** *If $|P| = p^2$ for some prime p, then P is abelian. More precisely, P is isomorphic to either $\mathbb{Z}/p^2\mathbb{Z}$ or $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.*

2.2.2 Conjugacy in S_n

We next consider conjugation in symmetric groups. Readers familiar with linear algebra will recognize 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 ([1] §4.3 Proposition 10)**.** *Let σ, τ be elements of the symmetric group S_n. Then*

$$\tau(a_1\ a_2\ \cdots\ a_k)\tau^{-1} = \big(\tau(a_1)\ \tau(a_2)\ \cdots\ \tau(a_k)\big).$$

In general, suppose σ has cycle decomposition

$$(a_1\ a_2\ \cdots\ a_{k_1})(b_1\ b_2\ \cdots\ b_{k_2})\cdots .$$

Then $\tau\sigma\tau^{-1}$ has cycle decomposition

$$\big(\tau(a_1)\ \tau(a_2)\ \cdots\ \tau(a_{k_1})\big)\big(\tau(b_1)\ \tau(b_2)\ \cdots\ \tau(b_{k_2})\big)\cdots ,$$

that is, $\tau\sigma\tau^{-1}$ is obtained from σ by replacing each entry i in the cycle decomposition for σ by the entry $\tau(i)$.

Proof. Observe that if $\sigma(i) = j$, then

$$\tau\sigma\tau^{-1}\big(\tau(i)\big) = \tau(j).$$

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 $\tau\sigma\tau^{-1}$. This completes the proof. □

Example. *One can compute directly that $C_{S_3}\big((1\ 2\ 3)\big) = \langle(123)\rangle = \{(1), (123), (132)\}$. For example,*

$$(1\ 2)(1\ 2\ 3)(1\ 2)^{-1} = (2\ 1\ 3) \neq (1\ 2\ 3), \quad (1\ 3\ 2)(1\ 2\ 3)(1\ 3\ 2)^{-1} = (3\ 1\ 2) = (1\ 2\ 3).$$

Exercise ([1] §4.3 Exercise 8)**.** *Prove that $Z(S_n) = \{(1)\}$ for all $n \geq 3$.*

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 integers $n_1, n_2, \ldots, n_r$ are called the **cycle type** of σ.

Note that by the results of the preceding section the cycle type of a permutation is unique. For example, the cycle type of an m-cycle in S_n is $1, 1, \ldots, 1, m$, where the m is preceded by $n - m$ ones.

Proposition ([1] §4.3 Proposition 11)**.** *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. (A **partition** of $n \in \mathbb{Z}_{>0}$ is any nondecreasing sequence of positive integers whose sum is n.)*

One can exhibit all normal subgroups of S_n with the help of the above proposition. We first observe that normal subgroups of a group G are the union of conjugacy classes of G, i.e.,

$$\text{if } H \trianglelefteq G, \text{ then for every conjugacy class } \mathcal{K} \text{ of } G, \text{ either } \mathcal{K} \subseteq H \text{ or } \mathcal{K} \cap H = \emptyset.$$

This is because if $x \in \mathcal{K} \cap H$, then $gxg^{-1} \in gHg^{-1}$ for all $g \in G$. Since H is normal, $gHg^{-1} = H$, so that H contains all the conjugates of x, i.e., $\mathcal{K} \subseteq H$.

Other useful properties of normal subgroups, for example, are that

$$\text{if } H \trianglelefteq G, \text{ then } e \in H, \ |H| \text{ divides } |G|, \text{ and } H \text{ is a subgroup of } G.$$

Example. *If $n = 3$, the partitions of 3 and corresponding representatives of the conjugacy classes (with 1-cycles not written) are as given in the following table:*

Partition of 3	**Representative of Conjugacy Class**	**Number of Conjugates**
1, 1, 1	(1)	1
1, 2	$(1\ 2)$	$A_3^2/2 = 3$
3	$(1\ 2\ 3)$	$A_3^3/3 = 2$

The sum of the orders of these conjugacy classes is the order of S_3.

If $H \trianglelefteq S_3$, all the possible choices of conjugacy classes in H can only be given by 1, $1+2$, and $1+3+2$, which correspond to all the normal subgroups of S_3: $\{e\}$, A_3, and S_3.

Example. *If $n = 4$, the partitions of 4 and corresponding representatives of the conjugacy classes (with 1-cycles not written) are as given in the following table:*

Partition of 4	**Representative of Conjugacy Class**	**Order of Conjugacy Class**
1, 1, 1, 1	(1)	1
1, 1, 2	$(1\ 2)$	$A_4^2/2 = 6$
1, 3	$(1\ 2\ 3)$	$A_4^3/3 = 8$
2, 2	$(1\ 2)(3\ 4)$	$(A_4^2/2 \cdot A_2^2/2)/2 = 3$
4	$(1\ 2\ 3\ 4)$	$A_4^4/4 = 6$

The sum of the orders of these conjugacy classes is the order of S_4.

If $H \trianglelefteq S_4$, all the possible choices of conjugacy classes in H can only be given by

$$1, \quad 1+3, \quad 1+8+3, \quad \textit{and} \quad 1+6+8+3+6,$$

which correspond to all the normal subgroups of S_4:

$$\{e\}, \quad \{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}, \quad A_4, \quad \textit{and} \quad S_4.$$

Note that, even though $6+6$ divides $|S_4| = 24$, the union $\mathrm{Conj}\big((1\ 2)\big) \cup \mathrm{Conj}\big((1\ 2\ 3\ 4)\big)$ is not a subgroup of S_4.

Exercise ([1] §1.3 Exercise 16 & §4.3 p.127)**.** *Compute directly the number of m-cycles in S_n by a combinatorial calculation. If $\sigma \in S_n$ is an m-cycle, determine its centralizer and verify the Orbit–Stabilizer Theorem.*

Exercise ([1] §4.3 p.127–128)**.** *Use the partitions of 5 to determine all normal subgroups of S_5.*

Exercise ([1] §4.3 Exercise 20)**.** *Let $\sigma \in A_n$. Show that all elements in the conjugacy class of σ in S_n (i.e., all elements of the same cycle type as σ) are conjugate in A_n if and only if σ commutes with an odd permutation.*

Exercise ([1] §4.3 Exercise 22)**.** *Show that if n is odd then the set of all n-cycles consists of two conjugacy classes of equal size in A_n.*

2.3 The right group action

Exercise ([1] §1.7 Exercises 14 & 15)**.** *Let G be a group and let $A = G$. Show that if G is non-abelian then the maps defined by $g.a := ag$ for all $g, a \in G$ do NOT satisfy the axioms of a (left) group action of G on itself, but the maps defined by $g.a := ag^{-1}$ do.*

In the definition of an action the group elements appear to the left of the set elements and so our notion of an action might more precisely be termed 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 $a.g$ for $a \in A$ and $g \in G$, that satisfies the axioms:

(1) $(a.g_1).g_2 = a.(g_1 g_2)$ for all $g_1, g_2 \in G$, $a \in A$, and

(2) $a.e = a$ for all $a \in A$.

For arbitrary group actions it is an easy exercise to check that if we are given a left group action of G on A then the map $A \times G \to A$ defined by $a.g := g^{-1}.a$ is a right group action. Conversely, given a right group action of G on A we can form a left group action by $g.a := a.g^{-1}$. Call these pairs **corresponding group actions**. Put another way, for corresponding group actions, g acts on the left in the same way that g^{-1} acts on the right.

This is particularly transparent for the action of conjugation because the "left conjugate of a by g", namely gag^{-1}, is the same group element as the "right conjugate of a by g^{-1}" (denoted by $a^{g^{-1}}$). Thus two elements or subsets of a group are "left conjugate" if and only if they are "right conjugate", and so the relation "conjugacy" is the same for the left and right corresponding actions. More generally, it is also an exercise ([1] §4.3 Exercise 1) to see that for any corresponding left and right actions the orbits are the same.

We have consistently used left actions since they are compatible with the notation of applying functions on the left (i.e., with the notation $\varphi(g)$); in this way left multiplication on the left cosets of a subgroup is a left action. Similarly, right multiplication on the right cosets of a subgroup is a right action and the associated permutation representation φ is a homomorphism provided the function $\varphi : G \to S_A$ is written on the right as $(g_1 g_2)\varphi$ (and also provided permutations in S_A are written on the right as functions from A to itself).

There are instances where a set admits two actions by a group G: one naturally on the left and the other on the right, so that it is useful to be comfortable with both types of actions.

3 Sylow's Theorem

3.1 Examples and Proof

In this section, let G be a finite group and let p be a prime. A group of order p^α for some $\alpha \in \mathbb{Z}_{>0}$ is called a **p-group**. Subgroups of G which are p-groups are called **p-subgroups**. If G is a group of order $p^\alpha m$, where $p \nmid m$, then a subgroup of order p^α is called a **Sylow p-subgroup** of G. The set of Sylow p-subgroups of G will be denoted by $\mathrm{Syl}_p(G)$ and 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).

Example.
- *If p does not divide the order of G, the Sylow p-subgroup of G is the trivial group.*
- *If $|G| = p^\alpha$, G is the unique Sylow p-subgroup of G.*

Example. *S_3 has three Sylow 2-subgroups: $\langle(1\ 2)\rangle$, $\langle(2\ 3)\rangle$ and $\langle(1\ 3)\rangle$. It has a unique (normal) Sylow 3-subgroup: $\langle(1\ 2\ 3)\rangle = A_3$.*

The full converse to Lagrange's Theorem is not true: namely, if G is a finite group and n divides $|G|$, then G need not have a subgroup of order n. For example A_4 does not have a subgroup of order 6. There are some partial converses to Lagrange's Theorem.

For finite abelian groups the full converse of Lagrange is true, namely an abelian group has a subgroup of order n for each divisor n of $|G|$ (cf. [1] §3.4 Exercise 4).

The strongest converse to Lagrange's Theorem which applies to arbitrary finite groups is the following:

Theorem ([1] §4.5 Theorem 18, Sylow's Theorem)**.** *Let G be a group of order $p^\alpha m$, 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,

$$n_p = [G : N_G(P)] \mid m.$$

Example. $|A_4| = 12 = 2^2 \cdot 3$. *By* $n_2 \equiv 1 \pmod 2$ *and* $n_2 \mid 3$ *we have* $n_2 = 1$ *or* 3. *By* $n_3 \equiv 1 \pmod 3$ *and* $n_3 \mid 4$ *we have* $n_3 = 1$ *or* 4.

In fact A_4 has a unique (normal) Sylow 2-subgroup: $\langle (1\ 2)(3\ 4), (1\ 3)(2\ 4)\rangle \cong V_4$. *It has four Sylow 3-subgroups:* $\langle (1\ 2\ 3)\rangle$, $\langle (1\ 2\ 4)\rangle$, $\langle (1\ 3\ 4)\rangle$ *and* $\langle (2\ 3\ 4)\rangle$.

Example. $|S_4| = 24 = 2^3 \cdot 3$. *By* $n_2 \equiv 1 \pmod 2$ *and* $n_2 \mid 3$ *we have* $n_2 = 1$ *or* 3. *By* $n_3 \equiv 1 \pmod 3$ *and* $n_3 \mid 8$ *we have* $n_3 = 1$ *or* 4. *In fact S_4 has* $n_2 = 3$ *and* $n_3 = 4$.

Exercise ([1] §4.5 Exercises 6 & 7)**.** *Exhibit all Sylow 2-subgroups and all Sylow 3-subgroups of S_4 and find elements of S_4 which conjugate one of these into each of the others.*

(Note that all elements of order 3 in S_4 are the 3-cycles and there are 8 of them; and S_4 contains a subgroup isomorphic to D_8 given by the action of D_8 on the vertices of a square.)

Recall (cf. [1] §4.4 Corollary 14) that, if H is any subgroup of the group G, then for any fixed $g \in G$, $h \mapsto ghg^{-1}$ defines an isomorphism $H \cong gHg^{-1}$ of groups. Conjugate elements and conjugate subgroups have the same order. In particular, a conjugate of a Sylow p-subgroup is also a Sylow p-subgroup; and any two Sylow p-subgroups of a group (for the same prime p) are isomorphic.

Corollary ([1] §4.5 Corollary 20)**.** *Let P be a Sylow p-subgroup of G. Then TFAE (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, i.e. every automorphism of G maps P to itself;*

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

Example. *A finite abelian group has a unique Sylow p-subgroup for each prime p (note that any subgroup of an abelian group is normal). This subgroup consists of all elements x whose order is a power of p. This is sometimes called the* ***p-primary component*** *of the abelian group.*

Recall that, the classification of finite abelian groups ([1] §5.2 Theorem 5) says, any finite abelian group is the direct sum of all its p-primary component.

Proof of Sylow's Theorem (3). Assume that (1)(2) are true. Let P be a Sylow p-subgroups of G. By (2), G acts by conjugation on $\mathrm{Syl}_p(G)$, i.e., $g.Q \coloneqq gQg^{-1}$ for any $g \in G$, $Q \in \mathrm{Syl}_p(G)$; moreover, the action is transitive, and the stabilizer of $P \in \mathrm{Syl}_p(G)$ is $N_G(P)$. The Orbit–Stabilizer Theorem implies that $n_p = |\mathrm{Syl}_p(G)| = [G : N_G(P)]$ (cf. [1] §4.3 Proposition 6).

Again, consider the action of a fixed Sylow p-subgroup P on $\mathrm{Syl}_p(G)$ by conjugation, i.e., $g.Q \coloneqq gQg^{-1}$ for any $g \in P$, $Q \in \mathrm{Syl}_p(G)$. We now study the **fixed point** of this action, i.e., $Q \in \mathrm{Syl}_p(G)$ such that $g.Q = Q$ for any $g \in P$. Clearly P itself is a fixed point; and by definition, if Q is a fixed point, then $P \leq N_G(Q)$.

Claim that P, Q are also Sylow p-subgroups of $N_G(Q)$. In fact, $|G| = p^\alpha m$ and $|P| = |Q| = p^\alpha$. Recall that $Q \trianglelefteq N_G(Q) \leq G$. By Lagrange's Theorem $|N_G(Q)| = p^\alpha m'$ for some $m' \mid m$, and therefore $p \nmid m'$. So the subgroups P, Q are both Sylow p-subgroups of $N_G(Q)$.

However, $Q \trianglelefteq N_G(Q)$ implies that $N_G(Q)$ has only one Sylow p-subgroup, i.e. $Q = P$. (Note that [1] §4.5 Corollary 20 is a corollary of only [1] §4.5 Theorem 18(2), so this line of reasoning is not circular.) This means, the action of P on $\mathrm{Syl}_p(G)$ by conjugation only has one fixed point P.

Now apply a generalized version of the "Class Equation", i.e.,

$$\begin{aligned} n_p = |\mathrm{Syl}_p(G)| &= \sum_{\text{fixed points}} 1 + \sum_{Q \in \text{non-fixed orbits}} |\mathcal{O}_Q| \\ &= 1 + \sum_{Q \in \text{non-fixed orbits}} [P : \mathrm{Stab}_P(Q)]. \end{aligned}$$

Here for any non-fixed Q, $1 < |\mathcal{O}_Q| = [P : \mathrm{Stab}_P(Q)]$ divides $|P| = p^\alpha$ so each $|\mathcal{O}_Q|$ must be a power of p. This implies $n_p \equiv 1 \pmod p$. □

3.2 Applications of Sylow's Theorem

Most of the examples use Sylow's Theorem to prove that a group of a particular order is not **simple**, i.e., G has a nontrivial normal subgroup. We shall be able to use these results to classify groups of some specific orders n.

Example ([1] §4.5 p.143)**.** *Suppose $|G| = pq$ for primes p and q with $p < q$. Let $P \in \mathrm{Syl}_p(G)$ and let $Q \in \mathrm{Syl}_q(G)$. We show that Q is normal in G.*

Now the three conditions: $n_q = 1 + kq$ for some $k \in \mathbb{Z}_{\geq 0}$, $n_q \mid p$ and $p < q$, together force $k = 0$. Since $n_q = 1$, $Q \trianglelefteq G$.

Since n_p divides the prime q, the only possibilities are $n_p = 1$ or q. In particular, if $p \nmid q - 1$, (that is, if $q \not\equiv 1 \pmod p$), then n_p cannot equal q, so $P \trianglelefteq G$.

Example. *Suppose $|G| = 72 = 2^3 \cdot 3^2$ and we show that G is not simple.*

If $n_3 = 1$ then the only Sylow 3-subgroup of G is normal. Suppose $n_3 \neq 1$. Since $n_3 \mid 8$ and $n_3 \equiv 1 \pmod 3$, it follows that $n_3 = 4$.

Now G acts by conjugation on its four Sylow 3-subgroups, so this action affords a permutation representation $\varphi : G \to S_4$. On one hand, the action is transitive and therefore nontrivial, so $\ker\varphi \neq G$; on the other hand, $|G| = 72 > |S_4| = 24$, therefore φ cannot be injective, i.e. $\ker\varphi \neq \{e\}$. So we construct a nontrivial normal subgroup $\ker\varphi$ of G.

Exercise ([1] §4.5 Exercise 13)**.** *Prove that a group of order 56 has a normal Sylow p-subgroup for some prime p dividing its order and therefore is not simple.*

Example (Classification of groups of order 6)**.** *Suppose $|G| = 6$. Let $Q \in \mathrm{Syl}_2(G)$ and $P \in \mathrm{Syl}_3(G)$. Then P and Q are both cyclic, and we denote $P = \langle a \rangle$, $Q = \langle b \rangle$ with order $\mathrm{ord}(a) = 3$, $\mathrm{ord}(b) = 2$. Since $[G : P] = 2$ and $b \notin \langle a \rangle$, G is a disjoint union of cosets of P:*

$$G = \langle a \rangle \cup \langle a \rangle b.$$

We can also say that G is generated by a and b.

We know $P = \langle a \rangle$ is a normal subgroup of G (by the first example or directly by $[G : P] = 2$), then $bPb^{-1} = P$. In particular

$$bab^{-1} \in P = \{e, a, a^2\}.$$

Assume that $bab^{-1} = a^k$ for some $0 \leq k \leq 2$. Then $b^2 = e$ implies

$$a = b(bab^{-1})b^{-1} = ba^k b^{-1} = (bab^{-1})^k = a^{k^2} \quad \Longrightarrow \quad a^{k^2-1} = e.$$

Recall that $\mathrm{ord}(a) = 3$ and then $3 \mid k^2 - 1$, therefore $k \neq 0$.

- *If $k = 1$ then $bab^{-1} = a$, i.e. $ab = ba$. In this case G is a quotient group of*

  $$\langle a, b \mid a^3 = b^2 = e,\ ab = ba \rangle \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z}.$$

  But G is of order 6, hence $G \cong \mathbb{Z}/6\mathbb{Z}$.

- *If $k = 2$ then $bab^{-1} = a^{-1}$. In this case G is a quotient group of*

  $$\langle a, b \mid a^3 = b^2 = e,\ bab^{-1} = a^{-1} \rangle \cong D_6.$$

  Again by comparing the orders we have $G \cong D_6$.

Other related exercises in [1]

§1.6 25 26
§1.7 17 19
§2.2 6 8 12
§4.1 1 6
§4.2 4 7 13
§4.3 5 6 11 13 25 26 31 32
§4.5 5 9 10 11 17 18 26 39 40

References

[1] D. S. Dummit and R. M. Foote. *Abstract algebra*. John Wiley & Sons, Inc., Hoboken, NJ, third edition, 2004.