INTRO TO ABSTRACT ALGEBRA

JOHN COBB
DEPARTMENT OF MATHEMATICS, AUBURN UNIVERSITY, AUBURN, AL
Email address: jdcobb3@gmail.com

Last updated: July 7, 2026

ABSTRACT. These are my class notes developed for my intro to algebra class at Auburn. These are synthesized from and at times wholly lifted from some of my favorite sources: Dummit and Foote [DF03], Eloisa Grifo, an infinite napkin, mathematics and its history.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION TO GROUPS

All of this course will be focused on concepts related to groups, one of the most important unifying ideas in mathematics. The group concept was implicit in mathematics for a long time – arguably from the introduction of negative numbers. It was a French teenager, Evariste Galois (1831), who first defined a group and gave it a name, writing up the sum total of his ideas in a long letter the night before he died in a duel to defend the honor of a sex worker. As you'll soon see, the definition of a group is fairly simple. I think of groups as sitting fairly low down within the structure of mathematics. This means they are foundational – knowing more about groups tells you about all the objects that build upon them.

Group theory today is often described as the theory of symmetry. Some of the largest discoveries in science have been due to framing symmetries in nature in terms of groups. Noether's theorem says that, in a precise sense, all conservation laws within a physical theory come from symmetries of that theory. For example, one way to phrase the development of special relativity is that physicists identified the correct symmetry group of spacetime – the Lorentz group. Group theory predicted the existence of many elementary particles before they were found experimentally. Several of the most important problems in physics and computer science can be phrased similarly.

The point of this first chapter is not to master every example. The point is to see the shape of the subject early: examples, calculations, subgroups, generators, homomorphisms, isomorphisms, and actions. Later chapters return to all of these ideas in much more detail.

1.1 DEFINITIONS AND FIRST EXAMPLES

A group consists of two pieces of data: a set G, and an associative binary operation $*$ with some properties. Before the formal definition, let's give two examples:

Example 1.1.1. The pair $(\mathbb{Z}, +)$ is a group. $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ is a set and the associative operation is addition. Note that there is a special element $0 \in \mathbb{Z}$ that has a special property:

$$a + 0 = 0 + a = a \quad \text{for all } a \in \mathbb{Z}.$$

This is called the identity element. Every element $a \in \mathbb{Z}$ has an additive inverse:

$$a + (-a) = (-a) + a = 0. \qquad \diamond$$

Example 1.1.2. Let $\mathbb{Q} - \{0\}$ be the set of nonzero rational numbers. The pair $(\mathbb{Q} - \{0\}, \cdot)$ is a group: the set is $\mathbb{Q} - \{0\}$ and the associative operation is multiplication. Again we see the same two nice properties: There is a special element $1 \in \mathbb{Q} - \{0\}$ such that

$$a \cdot 1 = 1 \cdot a = a.$$

This is the identity element. For any rational number $x \in \mathbb{Q} - \{0\}$, there is an inverse $1/x$ such that

$$x \cdot x^{-1} = x^{-1} \cdot x = 1. \qquad \diamond$$

Definition 1.1.3. A *group* is a pair $(G, *)$ consisting of a set of elements G, and a binary operation $*$ on G, such that:

- G has an *identity element* e with the property that $e * g = g * e = g$ for all $g \in G$.
- The operation $*$ is *associative*, meaning that $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$.
- Every element $g \in G$ has an *inverse* g^{-1}, meaning that $g * g^{-1} = g^{-1} * g = e$.

We'll denote the size of the group by $|G|$, sometimes called the *order* of the group. If $|G|$ is finite, we say G is a *finite group*.

Note that we'll often refer to the group only by the underlying set G itself, leaving you to infer the operation $*$ from context.

Remark 1.1.4 (Unimportant pedantic point). Some authors like to add a "closure axiom", i.e. to explicitly say that $g * h \in G$. This is implied already by the fact that $*$ is a binary operation on G.

Example 1.1.5. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are all groups under addition with $e = 0$ and $a^{-1} = -a$, for all a. $\diamond$

Example 1.1.6. $\mathbb{Q} - \{0\}$, $\mathbb{R} - \{0\}$, $\mathbb{C} - \{0\}$, $\mathbb{Q}^+$ and $\mathbb{R}^+$ are all groups under multiplication with $e = 1$ and $a^{-1} = 1/a$, for all a. $\diamond$

Example 1.1.7 (Invertible matrices)**.** Consider the set of all invertible $n \times n$ matrices with real entries, denoted by $GL_n(\mathbb{R})$. This set forms a group under matrix multiplication, known as the general linear group. The identity element is the identity matrix, and the inverse of a matrix A is its inverse A^{-1}, which also has real entries. The group operation is associative because matrix multiplication is associative. But wait, is it closed under multiplication? Yes! The product of two invertible matrices is also invertible, and the inverse of the product is given by $(AB)^{-1} = B^{-1}A^{-1}$, which is also an invertible matrix. Therefore, $GL_n(\mathbb{R})$ satisfies all the group axioms and is indeed a group. $\diamond$

Example 1.1.8 (Non-examples of groups).

- $\mathbb{Z} - \{0\}$ is not a group under multiplication, since elements like 2 do not have multiplicative inverses in $\mathbb{Z} - \{0\}$.
- The pair $(\mathbb{Q}, \cdot)$ is not a group. While there is an identity element, the element $0 \in \mathbb{Q}$ does not have an inverse.
- The natural numbers $\mathbb{N}$ are not a group under addition. There is an identity element, but 3 has no additive inverse inside $\mathbb{N}$.
- Let $\mathrm{Mat}_{2\times 2}(\mathbb{R})$ be the set of 2×2 real matrices. Even though we have an identity matrix
$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$
not every matrix has a multiplicative inverse. For example, the zero matrix does not have a multiplicative inverse. Even if you delete the zero matrix from the set, it is still not a group – any matrix with determinant zero cannot have an inverse.

◇

1.2 BASIC ALGEBRA IN A GROUP

In a group we can calculate without knowing what the elements actually are. The symbols a, b, c might be integers, matrices, functions, symmetries, or something stranger, but the same algebraic rules still hold.

Proposition 1.2.1. *If* G *is a group under the operation* $*$*, then*

- *The identity of* G *is unique.*
- *For each* $a \in G$, a^{-1} *is uniquely determined.*

Proof. Suppose f and g were both identities. Then $f * g = f$ since g is an identity, and $f * g = g$ since f is an identity. Thus $f = g$.

Suppose b and c were both inverses of a. Then $a * b = e$ and $a * c = e$. Thus

$$b = b * e = b * (a * c) = (b * a) * c = e * c = c. \qquad \blacksquare$$

Therefore we can refer to *the* identity of G and *the* inverse of g without ambiguity.

From now on, when the operation is clear, we usually omit the symbol $*$ and write ab instead of $a * b$. This is called *multiplicative notation*. When the group operation is addition, we use additive notation: the identity is written 0, the inverse of a is written $-a$, and the product a^n is written na.

Proposition 1.2.2. *Let* G *be a group and let* $x, y, a \in G$*. Show that the following properties hold:*

1. *If* $ax = ay$*, then* $x = y$*.*

2. *If* $xa = ya$, *then* $x = y$.
3. $(x^{-1})^{-1} = x$.
4. $(x * y)^{-1} = (y^{-1}) * (x^{-1})$.

Proof. Let e be the identity element of G.

1. If $ax = ay$, then multiplying on the left by a^{-1} gives $a^{-1}ax = a^{-1}ay$, so $ex = ey$, hence $x = y$.
2. If $xa = ya$, then multiplying on the right by a^{-1} gives $xaa^{-1} = yaa^{-1}$, so $xe = ye$, hence $x = y$.
3. Since $x^{-1}x = e$ and $xx^{-1} = e$, the element x is the inverse of x^{-1}. Thus $(x^{-1})^{-1} = x$.
4. We have
$$(x * y) * (y^{-1} * x^{-1}) = x * (y * y^{-1}) * x^{-1} = x * e * x^{-1} = e$$
and similarly
$$(y^{-1} * x^{-1}) * (x * y) = y^{-1} * (x^{-1} * x) * y = y^{-1} * e * y = e.$$
Hence $y^{-1} * x^{-1}$ is the inverse of $x * y$, so $(x * y)^{-1} = y^{-1} * x^{-1}$. ■

Some notation: if $x \in G$ and $n > 0$, we write x^n to denote the element obtained by multiplying x with itself n times:
$$x^n = \underbrace{x * x * \cdots * x}_{n \text{ times}}.$$
We also set $x^0 = e$ and $x^{-n} = (x^{-1})^n$ for $n > 0$.

Exercise (1.2.1). Let G be a group and let $x, y \in G$. Show that the following properties hold:

1. $(x^{-1})^n = (x^n)^{-1}$.
2. $(x^{-1}yx)^n = x^{-1}y^nx$ for any integer $n \geq 1$.

Exercise (1.2.2). Suppose G is a finite group. For $a \in G$, prove that the functions
$$L_a : G \to G, \qquad L_a(x) = ax$$
and
$$R_a : G \to G, \qquad R_a(x) = xa$$
are bijections.

Deduce that each row and each column of the multiplication table of G contains every element of G exactly once.

Exercise (1.2.3). We have seen that a group element has a unique inverse. However, group elements need not have a unique square root. By a square root of an element g in a group G, we mean an element h such that $h^2 = g$.

1. Give an example of an element g in a group G that has no square roots.
2. Give an example of an element g in a group G which has more than one square root.
3. Give an example of an element g in a group G which has infinitely many square roots.
4. Give an example of an element g in a group G which has a unique square root.

Most of the examples so far have had the special property that $a * b = b * a$ for all $a, b \in G$. This is called commutativity, and it is not a requirement for a group. Groups that do have this property are called abelian groups, after the Norwegian mathematician Niels Henrik Abel.

Definition 1.2.3. A group G is *abelian* if $*$ is commutative, i.e. for all $a, b \in G$ we have $a * b = b * a$.

Example 1.2.4. The groups $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ under addition are abelian. The groups $\mathbb{Q}^\times$, $\mathbb{R}^\times$, $\mathbb{C}^\times$, $\mathbb{Q}^+$, and $\mathbb{R}^+$ under multiplication are also abelian. ◇

Example 1.2.5. So far, the only example we've given of a nonabelian group is $GL_n(\mathbb{R})$. For instance, in $GL_2(\mathbb{R})$,

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix},$$

while

$$\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}.$$

These products are different, so matrix multiplication is not commutative. ◇

Exercise (1.2.4). Prove that if $x^2 = 1$ for all $x \in G$ then G is abelian.

1.3 A FIRST GALLERY OF EXAMPLES

The next examples will come up a lot. The goal here is exposure: you should know these groups exist and have a rough sense of how they behave. We will return to most of them later.

Example 1.3.1 (Addition mod n)**.** Here is an example from number theory: Let $n > 1$ be an integer, and consider the residues (remainders) modulo n. That is, we partition

the integers into n equivalence classes:

$$\begin{aligned}
\overline{0} &= \{a \in \mathbb{Z} \mid a \equiv 0 \mod n\} = \{0, n, -n, 2n, -2n, \dots\} \\
\overline{1} &= \{a \in \mathbb{Z} \mid a \equiv 1 \mod n\} = \{1, n+1, -n+1, 2n+1, -2n+1, \dots\} \\
&\vdots \\
\overline{n-1} &= \{a \in \mathbb{Z} \mid a \equiv n-1 \mod n\} = \{n-1, 2n-1, -1, 3n-1, -2n-1, \dots\}.
\end{aligned}$$

These form a group under addition. We call this the *cyclic group of order* n, and denote it as $\mathbb{Z}/n\mathbb{Z}$ with elements $\overline{0}, \overline{1}, \dots, \overline{n-1}$. The identity is $\overline{0}$. ◇

Example 1.3.2 (Multiplication mod n)**.** For $n \in \mathbb{N}$, the set $(\mathbb{Z}/n\mathbb{Z})^\times$ of equivalence classes $\overline{a}$ which have multiplicative inverses mod n is a group under multiplication of classes. The identity element is the element $\overline{1}$ and by definition, each element has a multiplicative inverse. In general, we will use the notation $G^\times$ to mean the group of invertible elements of a set. ◇

Sometimes we organize the information of a group into a *group table*. For example, consider $(\mathbb{Z}/5\mathbb{Z} - \{\overline{0}\}, \cdot) = (\mathbb{Z}/5\mathbb{Z})^\times$. The group table is as follows:

$\cdot$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

You can check this is a group: the identity is $\overline{1}$, every element has an inverse (for example, $\overline{2}^{-1} = \overline{3}$), and the operation is associative because multiplication of integers is associative. This, in a sense, contains all information about the group. However, it won't be a very useful way to organize the information for large groups.

Just for fun, let's start reasoning through all groups of small order.

1. The only group of order 1 is the trivial group $\{e\}$, where e is the identity element. That is, up to renaming the group elements, there is only one group of order 1.

2. The only group of order 2 is

$\cdot$	e	a
e	e	a
a	a	e

   where a is the non-identity element. The assignments are forced upon you. So up to renaming your group elements, there is only one group of order 2. Since we already know that $\mathbb{Z}/2\mathbb{Z}$ is a group of order 2, we can conclude that $\mathbb{Z}/2\mathbb{Z}$ is the only group of order 2.

3. The only group of order 3 is

$\cdot$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

   where a and b are the non-identity elements. The assignments are forced upon you. So up to renaming your group elements, there is only one group of order 3. Since we already know that $\mathbb{Z}/3\mathbb{Z}$ is a group of order 3, we can conclude that $\mathbb{Z}/3\mathbb{Z}$ is the only group of order 3.

4. There are two options for the group of order 4. The first is the cyclic group $\mathbb{Z}/4\mathbb{Z}$:

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

   The second is the Klein four group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$:

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

   So there are two groups of order 4 up to renaming the group elements: $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

5. The only group of order 5 is $\mathbb{Z}/5\mathbb{Z}$.

6. There are two groups of order 6 up to renaming the group elements: $\mathbb{Z}/6\mathbb{Z}$ and S_3, the symmetric group of order 6. The first is abelian, while the second is not. This is the first non-abelian group.

We will define what it means for groups to be "the same up to renaming" soon, but much of early group theory is about classifying all groups in this way.

Example 1.3.3 (Product groups)**.** Let $(G, *)$ and $(H, \cdot)$ be groups. The *product group* $G \times H$ is the set of pairs (g, h) with $g \in G$ and $h \in H$, with the operation defined by

$$(g_1, h_1)(g_2, h_2) = (g_1 * g_2, h_1 \cdot h_2).$$

The identity element is (e_G, e_H), where e_G and e_H are the identity elements of G and H, respectively. The inverse of an element (g, h) is given by (g^{-1}, h^{-1}). The operation is associative because both $*$ and $\cdot$ are associative. Therefore, $G \times H$ satisfies all the group axioms and is indeed a group. $\diamond$

Example 1.3.4. Let S^1 be the set of complex numbers z with absolute value one; that is

$$S^1 := \{z \in \mathbb{C} \mid |z| = 1\}.$$

Then $(S^1, \times)$ is a group because

- The complex number $1 \in S^1$ serves as the identity, and
- Each complex number $z \in S^1$ has an inverse $1/z$ which is also in S^1, since $|z^{-1}| = |z|^{-1} = 1$.
- You should also check that $z_1 \times z_2$ actually still lives in S^1. This follows from the fact that $|z_1 z_2| = |z_1||z_2| = 1$.

$\diamond$

Example 1.3.5. Let $SL_n(\mathbb{R})$ denote the set of $n \times n$ matrices whose determinant is 1. This is a subgroup (more on this soon) of $GL_n(\mathbb{R})$, and is called the special linear group. The identity element is the identity matrix, and the inverse of a matrix A in $SL_n(\mathbb{R})$ is its inverse A^{-1}, which also has determinant 1. The group operation is associative because matrix multiplication is associative. Therefore, $SL_n(\mathbb{R})$ satisfies all the group axioms and is indeed a group. $\diamond$

Example 1.3.6 (Dihedral group)**.** Consider a regular n-sided polygon. The symmetries of this polygon form a group under composition, known as the dihedral group D_n. What does the word symmetric mean here? We apply the label "symmetric" to anything that is invariant under some transformations. In this case, the elements of D_n include rotations and reflections that preserve the shape of the polygon. The identity element is the rotation by 0 degrees, and each symmetry has an inverse that undoes its effect. The group operation is associative because composition of functions is associative. Therefore, D_n satisfies all the group axioms and is indeed a group.

If r denotes rotation by $2\pi/n$ and s denotes a reflection, then every element of D_n can be written as either r^i or $r^i s$ for some $0 \leq i < n$. The relations

$$r^n = e, \qquad s^2 = e, \qquad srs = r^{-1}$$

explain most computations in this group. We will study these groups carefully later. $\diamond$

The next example is actually the original motivation for the definition of a group. That is, when Galois defined a group, he was thinking about the following example.

Example 1.3.7 (Symmetric group)**.** The symmetric group S_n is the group of all permutations of $\{1, \ldots, n\}$. By viewing these permutations as functions from $\{1, \ldots, n\}$ to itself, we can consider compositions $\circ$ of permutations. The pair $(S_n, \circ)$ is a group. There is an identity element: the permutation that leaves all elements fixed. Each permutation has an inverse, which is the permutation that undoes its effect. ◇

A huge theorem of Cayley, which we will later show, says that every group is isomorphic to a subgroup of some symmetric group. This means that, in a sense, the symmetric groups are the most general groups. So maybe Galois was right to focus on them!

Example 1.3.8 (Quaternions)**.** The *quaternion group* Q_8 is the group with elements

$$\{1, -1, i, -i, j, -j, k, -k\}$$

and multiplication defined by the following rules:

$$\begin{aligned} i^2 = j^2 = k^2 &= -1, \\ ij = k, \quad ji &= -k, \\ jk = i, \quad kj &= -i, \\ ki = j, \quad ik &= -j. \end{aligned}$$

This group is not abelian, since $ij = k$ but $ji = -k$. ◇

Exercise (1.3.1). Let $G = \{a + b\sqrt{2} \in \mathbb{R} \mid a, b \in \mathbb{Q}\}$. Prove that G is a group under addition, and prove that the nonzero elements of G are a group under multiplication.

Exercise (1.3.2). This exercise gives a first glimpse of a Lie algebra. Let $M_2(\mathbb{C})$ be the vector space of all 2×2 complex matrices. For $A, B \in M_2(\mathbb{C})$, define

$$[A, B] = AB - BA.$$

This operation is called the *commutator bracket*. In Lie theory, this is the basic example of a *Lie bracket*.

1. Compute $[A, B]$ for
$$A = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \qquad B = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}.$$
2. Prove that $[A, B] = -[B, A]$ for all $A, B \in M_2(\mathbb{C})$. In particular, $[A, A] = 0$.
3. Prove that $[A, B] = 0$ if and only if A and B commute.
4. Let
$$\mathfrak{sl}_2(\mathbb{C}) = \{A \in M_2(\mathbb{C}) \mid \mathrm{Tr}(A) = 0\}.$$
Prove that if $A, B \in \mathfrak{sl}_2(\mathbb{C})$, then $[A, B] \in \mathfrak{sl}_2(\mathbb{C})$.

1.4 SUBGROUPS: FIRST PASS

Every time we define an algebraic object, we should ask which subsets inherit the same structure. For groups, these inherited objects are called subgroups. Often the best way to understand a group is to find smaller groups inside it.

Definition 1.4.1. A *subgroup* of a group $(G, *)$ is a group $(H, *)$ such that $H \subseteq G$ and the operation on H is the operation on G restricted to H. We write $H \leq G$ to mean that H is a subgroup of G.

The words "under the operation of G" are important. We are not allowed to put a new operation on H and then call it a subgroup. A subgroup has to use the same multiplication law as the ambient group.

Example 1.4.2. Every group G has two trivial subgroups: the group itself, and the subgroup $\{e\}$ consisting of just the identity element. For the groups $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$, these are the only subgroups. ◇

Example 1.4.3. Under addition, we have the chain of subgroups $\mathbf{Z} \leq \mathbf{Q} \leq \mathbf{R} \leq \mathbf{C}$. ◇

Example 1.4.4. For any integer n, the set

$$n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$$

is a subgroup of $\mathbb{Z}$ under addition. For instance, $3\mathbb{Z} \subset \mathbb{Z}$ is the subgroup of all multiples of 3. ◇

In practice, we usually do not want to check every group axiom from scratch.

Proposition 1.4.5 (Subgroup test)**.** *Let G be a group and let H be a nonempty subset of G. Then H is a subgroup of G if and only if*

$$ab^{-1} \in H$$

for all $a, b \in H$. Equivalently, H is a subgroup if and only if H is nonempty and closed under the group operation and taking inverses.

Proof. If H is a subgroup, then $b^{-1} \in H$, so $ab^{-1} \in H$.

Conversely, suppose H is nonempty and $ab^{-1} \in H$ for all $a, b \in H$. Choose some $h \in H$. Taking $a = b = h$ gives $e = hh^{-1} \in H$. Taking $a = e$ and $b = h$ gives $h^{-1} \in H$. Finally, if $a, b \in H$, then $b^{-1} \in H$, so taking a and b^{-1} in the test gives $a(b^{-1})^{-1} = ab \in H$. Thus H has the identity, inverses, and is closed under the group operation. Associativity comes from G, so H is a subgroup. ■

Example 1.4.6. $SL_n(\mathbb{R}) \leq GL_n(\mathbb{R})$. Indeed, if $A, B \in SL_n(\mathbb{R})$, then

$$\det(AB^{-1}) = \det(A)\det(B)^{-1} = 1 \cdot 1^{-1} = 1,$$

so $AB^{-1} \in SL_n(\mathbb{R})$. ◇

Example 1.4.7. If $g \in G$, then

$$\langle g \rangle = \{\dots, g^{-2}, g^{-1}, e, g, g^2, \dots\}$$

is a subgroup of G, called the cyclic subgroup generated by g. ◇

Definition 1.4.8. The *order* $|g|$ of an element $g \in G$ is the size of the cyclic subgroup $\langle g \rangle$ generated by g. That is, it is the least positive integer n such that $g^n = e$, or ∞ if no such n exists.

Exercise (1.4.1). If x and g are elements of the group G, prove that $|x| = |g^{-1}xg|$. Deduce that $|xy| = |yx|$ for all $x, y \in G$.

Example 1.4.9. In S_n, the set of permutations fixing 1 is a subgroup:

$$\{\sigma \in S_n \mid \sigma(1) = 1\} \leq S_n.$$

This is called the stabilizer of 1 in S_n.

In D_n, the rotations form a subgroup

$$\{e, r, r^2, \dots, r^{n-1}\} \leq D_n.$$

Also, for any reflection s, the two-element set $\{e, s\}$ is a subgroup of D_n. ◇

Exercise (1.4.2). In a nonabelian group, two elements need not commute. On the other hand, they might commute. If $h \in G$, the *centralizer* of h in G is

$$C_G(h) = \{g \in G \mid gh = hg\}.$$

1. Prove that $C_G(h)$ is a subgroup of G.
2. Let G be the symmetric group on 4 letters and let h be the permutation $(1\,2)(3\,4)$. What is the centralizer $C_G(h)$?

Exercise (1.4.3). Let G be a group. The *center* of G is

$$Z(G) = \{z \in G \mid zg = gz \text{ for all } g \in G\}.$$

1. Prove that $Z(G)$ is a subgroup of G.
2. Prove that
$$Z(G) = \bigcap_{h \in G} C_G(h).$$
3. Compute $Z(S_3)$ and $Z(D_4)$.

Exercise (1.4.4). Let G be a finite group. The *commuting graph* of G is the graph whose vertices are the elements of G, with an edge between distinct vertices x and y exactly when $xy = yx$.

1. Draw the commuting graph of S_3.
2. Explain how the degree of the vertex x is related to the size of the centralizer $C_G(x)$.

1.5 SYMMETRIC GROUPS

Permutation groups or *symmetric groups* are among the most important examples of groups. They are concrete enough that you can compute with them by hand, but also flexible enough that many abstract questions about groups can be reduced to questions about permutations. Furthermore, this was how Galois thought of groups and were what people meant for a long time when they said "group".

Definition 1.5.1. A *permutation* of a set X is a bijection $\sigma\colon X \to X$. When $X = \{1, 2, \ldots, n\}$, the set of all permutations of X is denoted S_n and is called the *symmetric group* on n letters.

The group operation on S_n is composition of functions. Thus if $\sigma, \tau \in S_n$, then $\sigma\tau$ means "first do τ, then do σ." This convention is annoying for approximately one week and then becomes second nature.

Proposition 1.5.2. *The set S_n forms a group under composition, and $|S_n| = n!$.*

Proof. The composition of two bijections is again a bijection, composition of functions is associative, the identity map is the identity element, and every bijection has an inverse bijection. Hence S_n is a group.

To count its elements, note that there are n choices for $\sigma(1)$, then $n-1$ choices for $\sigma(2)$, and so on. Therefore

$$|S_n| = n(n-1)\cdots 2 \cdot 1 = n!.$$

■

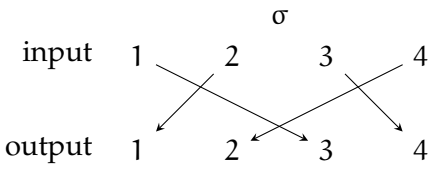
Example 1.5.3. The group S_3 has six elements. One of them is the identity permutation, and the other five are the nontrivial rearrangements of $\{1, 2, 3\}$. Since $|S_3| = 6$, this is the smallest symmetric group that is not abelian. ◇

There are several ways to write permutations. The most literal is *two-line notation*:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$$

means that $\sigma(1) = 3$, $\sigma(2) = 1$, $\sigma(3) = 4$, and $\sigma(4) = 2$.

The same permutation can be pictured by drawing arrows from each input to its output:



Two-line notation is fine for small examples, but it quickly becomes clunky. A better notation records how a permutation cycles elements around.

Definition 1.5.4. A *cycle* is a permutation of the form

$$(a_1\ a_2\ \ldots\ a_k),$$

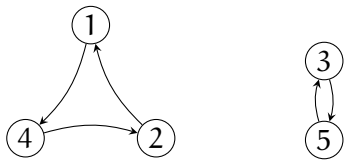
which sends a_1 to a_2, a_2 to a_3, ..., a_{k-1} to a_k, a_k to a_1, and fixes every other element.

A cycle of length 2 is called a *transposition*.

Example 1.5.5. In S_5, the cycle $(1\,4\,2)$ sends $1 \mapsto 4$, $4 \mapsto 2$, $2 \mapsto 1$, and fixes 3 and 5. The permutation

$$(1\,4\,2)(3\,5)$$

sends $1 \mapsto 4$, $4 \mapsto 2$, $2 \mapsto 1$, $3 \mapsto 5$, and $5 \mapsto 3$. The two disjoint cycles show up as two separate directed components:



$(1\,4\,2)$ $(3\,5)$

◇

Definition 1.5.6. Two cycles are called *disjoint* if they move disjoint sets of elements.

Proposition 1.5.7. *Disjoint cycles commute.*

Proof. Suppose σ and τ are disjoint cycles. If x is moved by σ, then $\tau(x) = x$, so

$$(\sigma\tau)(x) = \sigma(x) = (\tau\sigma)(x).$$

The same argument works if x is moved by τ, and if x is moved by neither cycle then both compositions fix x. Therefore $\sigma\tau = \tau\sigma$. ■

Theorem 1.5.8. *Every permutation in S_n can be written as a product of disjoint cycles. Aside from the order in which the disjoint cycles are written, this decomposition is unique if we ignore 1-cycles.*

Proof. Let $\sigma \in S_n$. Pick some element $a \in \{1, \ldots, n\}$. Repeatedly apply σ:

$$a,\ \sigma(a),\ \sigma^2(a),\ \sigma^3(a),\ \ldots$$

Since there are only finitely many elements, eventually this sequence repeats. Because σ is invertible, the first repeated element must be a, so these elements form a cycle

$$(a\ \sigma(a)\ \sigma^2(a)\ \ldots\ \sigma^{k-1}(a)).$$

If this cycle does not already involve every element of $\{1, \dots, n\}$, pick an element not yet used and repeat the process. Continuing in this way produces disjoint cycles whose product is exactly σ.

For uniqueness, observe that the cycle containing a given element a is completely determined by the orbit

$$a,\ \sigma(a),\ \sigma^2(a), \dots$$

so there is no freedom except to reorder the disjoint cycles and omit fixed points. ■

Example 1.5.9. Consider the permutation $\sigma \in S_7$ given by

$$\sigma(1) = 3,\ \sigma(3) = 5,\ \sigma(5) = 1, \qquad \sigma(2) = 4,\ \sigma(4) = 2, \qquad \sigma(6) = 6,\ \sigma(7) = 7.$$

Then

$$\sigma = (1\,3\,5)(2\,4).$$

We usually suppress the fixed points 6 and 7 rather than writing $(6)(7)$. ◇

Exercise (1.5.1). Show that

$$(a_1\, a_2 \cdots a_n) = (a_1\, a_n)(a_1\, a_{n-1}) \cdots (a_1\, a_3)(a_1\, a_2)$$

for any $n > 1$.

Cycle notation makes inverses very easy to compute:

$$(a_1\, a_2 \,\dots\, a_k)^{-1} = (a_k\, a_{k-1} \,\dots\, a_2\, a_1).$$

It also makes the order of a permutation easier to see. For example, $(1\,2\,3)$ has order 3, while $(1\,2)(3\,4)$ has order 2.

Proposition 1.5.10. *Every permutation is a product of transpositions.*

Proof. It is enough to show that every cycle is a product of transpositions. But

$$(a_1\, a_2 \,\dots\, a_k) = (a_1\, a_k)(a_1\, a_{k-1}) \cdots (a_1\, a_2).$$

Since every permutation is a product of cycles, it follows that every permutation is a product of transpositions. ■

Corollary 1.5.11. *The symmetric group S_n is generated by the transpositions.*

In fact, one can say more: S_n is generated by the *adjacent transpositions*

$$(1\,2),\ (2\,3),\ \dots,\ (n-1\,n).$$

This fact lies behind the idea that any rearrangement can be built by repeatedly swapping neighboring entries.

Exercise (1.5.2). Prove that the order of an element in S_n is the least common multiple of the lengths of the cycles in its cycle decomposition.

We will see later that *Cayley's theorem* says that every group is isomorphic to a subgroup of some symmetric group. Thus, in a sense, the symmetric groups are the most fundamental groups.

Exercise (1.5.3). A reduced word for a permutation is a way to write the permutation as a product of the smallest possible number of adjacent transpositions. Look up the Rothe diagram or pipe dream of a permutation and compute one for $(1\,4\,2\,3) \in S_4$.

Exercise (1.5.4). Find all numbers n such that S_5 contains an element of order n.

1.6 Dihedral Groups

Fix an integer $n \geq 3$, and let P_n be a regular n-gon centered at the origin in the plane. Label its vertices

$$V_0, V_1, \ldots, V_{n-1}$$

in counterclockwise order. Throughout this subsection, vertex subscripts are read modulo n.

Definition 1.6.1. An *isometry* of the plane is a function $f : \mathbb{R}^2 \to \mathbb{R}^2$ preserving Euclidean distance:

$$d(f(A), f(B)) = d(A, B)$$

for all points $A, B \in \mathbb{R}^2$.

A *symmetry* of P_n is an isometry $f : \mathbb{R}^2 \to \mathbb{R}^2$ such that $f(P_n) = P_n$ as a set. This does not mean that f fixes every point of P_n; it means that f moves the polygon onto itself.

Definition 1.6.2. The *dihedral group* D_n is the set of symmetries of the regular n-gon P_n, with group operation given by composition.

Remark 1.6.3. There are two common conventions for the notation. In these notes, D_n means the symmetry group of the regular n-gon, so $|D_n| = 2n$. Some authors call this group D_{2n} instead, emphasizing its order rather than the polygon.

Proposition 1.6.4. *The set D_n is a group under composition.*

Proof. The composition of two isometries is again an isometry. If $f(P_n) = P_n$ and $g(P_n) = P_n$, then

$$(f \circ g)(P_n) = f(g(P_n)) = f(P_n) = P_n,$$

so $f \circ g \in D_n$. Composition of functions is associative. The identity map is a symmetry of P_n, and the inverse of a symmetry is again a symmetry. Therefore D_n is a group. ∎

There are two basic kinds of symmetries.

Definition 1.6.5. Let $r \in D_n$ be counterclockwise rotation by $2\pi/n$. Thus

$$r(V_i) = V_{i+1}.$$

The rotations in D_n are

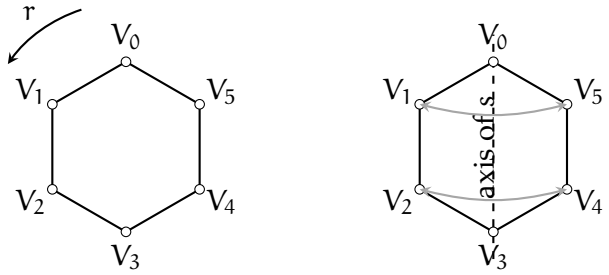
$$e, r, r^2, \ldots, r^{n-1}.$$

Definition 1.6.6. A *reflection* in D_n is reflection across a line of symmetry of P_n. If n is odd, each reflection line passes through one vertex and the midpoint of the opposite side. If n is even, there are two kinds of reflection lines: those passing through two opposite vertices, and those passing through the midpoints of two opposite sides.

There are n rotations and n reflections. To name the reflections efficiently, fix the reflection s across the line through the origin and V_0. With our labeling,

$$s(V_i) = V_{-i}.$$

For example, when $n = 6$, the chosen generators look like this:



Theorem 1.6.7. *The dihedral group* D_n *has* $2n$ *elements.*

Proof. First we show that there are at most $2n$ symmetries. Any symmetry sends vertices to vertices and sends adjacent vertices to adjacent vertices. The image of V_0 can be any one of the n vertices. Once $f(V_0)$ is chosen, the image of V_1 must be one of the two vertices adjacent to $f(V_0)$.

Every symmetry fixes the center of P_n, and a plane isometry is determined by the images of three non-collinear points. Thus the images of the center, V_0, and V_1 determine the whole symmetry. Therefore $|D_n| \leq 2n$.

Now we exhibit $2n$ distinct symmetries:

$$e, r, r^2, \ldots, r^{n-1}, \qquad s, rs, r^2s, \ldots, r^{n-1}s.$$

The rotations r^i are distinct because $r^i(V_0) = V_i$. The elements r^is are distinct for the same reason, since $r^is(V_0) = V_i$. Finally, r^i and r^is are different because

$$r^i(V_1) = V_{i+1} \qquad \text{but} \qquad r^is(V_1) = r^i(V_{-1}) = V_{i-1},$$

and $V_{i+1} \neq V_{i-1}$ since $n \geq 3$.

Hence D_n has at least $2n$ elements and at most $2n$ elements, so $|D_n| = 2n$. ∎

Remark 1.6.8. The rotations preserve the counterclockwise order of the vertices. The reflections reverse that order. This is often the quickest way to tell the two types of symmetries apart.

The two symmetries r and s generate the whole group. Their most important relations are

$$r^n = e, \qquad s^2 = e, \qquad srs^{-1} = r^{-1}.$$

Since $s^2 = e$, the last relation is often written as $sr = r^{-1}s$.

Lemma 1.6.9. *In* D_n, *we have* $srs^{-1} = r^{-1}$.

Proof. Since $s^{-1} = s$, it is enough to compare srs and r^{-1} on the vertices. For every i,

$$srs(V_i) = sr(V_{-i}) = s(V_{1-i}) = V_{i-1}.$$

But $r^{-1}(V_i) = V_{i-1}$ as well. A symmetry of P_n is determined by what it does to the vertices, so $srs = r^{-1}$. ■

Corollary 1.6.10. *For every integer* i, *we have*

$$sr^i s^{-1} = r^{-i}.$$

Proof. This follows by applying Lemma 1.6.9 repeatedly. Equivalently, conjugating by s turns the basic rotation r into its inverse, so it turns r^i into r^{-i}. ■

Theorem 1.6.11 (Normal form in D_n)**.** *Every element of* D_n *can be written uniquely in one of the forms*

$$r^i \qquad \textit{or} \qquad r^i s,$$

where $0 \le i < n$.

Proof. The previous counting argument already exhibited the $2n$ distinct elements

$$e, r, r^2, \ldots, r^{n-1}, \qquad s, rs, r^2 s, \ldots, r^{n-1}s.$$

Since D_n has exactly $2n$ elements, this list contains every element of D_n, and no element occurs twice. ■

Example 1.6.12. The group D_4, the symmetry group of the square, has 8 elements:

$$e,\ r,\ r^2,\ r^3,\ s,\ rs,\ r^2 s,\ r^3 s.$$

Here r is rotation by $90°$, r^2 is rotation by $180°$, and r^3 is rotation by $270°$. The other four elements are reflections. ◇

Exercise (1.6.1). The groups D_4 and Q_8 both have 8 elements, and both are nonabelian. Prove that they are not isomorphic.

Hint: compare the numbers of elements satisfying $x^2 = e$ in the two groups.

Example 1.6.13. The group D_n is not abelian for $n \geq 3$. Indeed, the relation $srs^{-1} = r^{-1}$ gives

$$sr = r^{-1}s.$$

If $sr = rs$, then $r^{-1}s = rs$, so $r^{-1} = r$ by cancellation. This would imply $r^2 = e$, contradicting the fact that r has order $n \geq 3$. ◇

Informally, we summarize everything above by writing the presentation

$$D_n = \langle r, s \mid r^n = e,\ s^2 = e,\ srs^{-1} = r^{-1} \rangle.$$

The symbols r and s generate the group, and the listed relations are enough to reduce any word in r and s to the normal form r^i or $r^i s$.

For example, since $sr^j = r^{-j}s$, multiplication in normal form is governed by

$$r^i r^j = r^{i+j}, \qquad r^i(r^j s) = r^{i+j}s,$$
$$(r^i s)r^j = r^{i-j}s, \qquad (r^i s)(r^j s) = r^{i-j},$$

where the exponents are read modulo n.

Exercise (1.6.2). In D_5, simplify each expression to the form r^i or $r^i s$ with $0 \leq i < 5$:

$$sr^2s, \qquad r^3sr^4, \qquad sr^3sr.$$

1.7 HOMOMORPHISMS AND ISOMORPHISMS: FIRST PASS

In this section we make precise the notion of when two groups "look the same".

Definition 1.7.1. Let G_1, G_2 be groups. A *homomorphism* from G_1 to G_2 is a function $\varphi : G_1 \to G_2$ such that

$$\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$$

for all $g_1, g_2 \in G_1$. An *isomorphism* is a homomorphism which is also a bijection. In this case, we'll write $G \cong H$.

It's the same as a map on sets, but it needs to respect the group structure of the domain and codomain. Two groups G and H are isomorphic if we can obtain H from G by just renaming elements. Very often we care about groups only up to isomorphism. For instance, the group $\mathbb{Z}^\times = \{1, -1\}$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$ by $f(1) = \overline{0}$ and $f(-1) = \overline{1}$. We could loosely say that $\mathbb{Z}^\times$ and $\mathbb{Z}/2\mathbb{Z}$ are the same group, even though they are written differently.

Example 1.7.2. The determinant gives a homomorphism

$$\det : GL_n(\mathbb{R}) \to \mathbb{R}^\times,$$

since $\det(AB) = \det(A)\det(B)$ for all $A, B \in GL_n(\mathbb{R})$. However, det is not an isomorphism, since it is not injective. It is surjective though, since the determinant of a diagonal matrix can be any nonzero real number. ◇

Example 1.7.3. The exponential map $\exp : \mathbb{R} \to \mathbb{R}^+$ defined by $\exp(x) = e^x$ is an isomorphism from $(\mathbb{R}, +)$ to $(\mathbb{R}^+, \cdot)$, since $\exp(x+y) = \exp(x)\exp(y)$ for all $x, y \in \mathbb{R}$, and exp is a bijection (it has inverse ln). ◇

Example 1.7.4. The inclusion $\iota : \mathrm{GL}_n(\mathbb{Z}) \hookrightarrow \mathrm{GL}_n(\mathbb{R})$ is a homomorphism: when you multiply two integral matrices you get the same answer whether you think of the integers as integers or as real numbers! Note that this homomorphism is *injective*. That is, $\mathrm{GL}_n(\mathbb{Z})$ is a subgroup of $\mathrm{GL}_n(\mathbb{R})$. ◇

Example 1.7.5. We have $S_n \cong S_m$ if and only if $n = m$ since $|S_n| = n!$ and $|S_m| = m!$, and the order of a group is preserved by isomorphism. ◇

Example 1.7.6. Since $\mathbb{Z}/6\mathbb{Z}$ is abelian and S_3 is not abelian, we conclude that $\mathbb{Z}/6\mathbb{Z} \ncong S_3$. ◇

Exercise (1.7.1). Prove that the multiplicative groups $\mathbb{R} \setminus \{0\}$ and $\mathbb{C} \setminus \{0\}$ are not isomorphic.

Example 1.7.7. The reduction map

$$\pi_n : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \qquad \pi_n(a) = \overline{a},$$

is a homomorphism from $(\mathbb{Z}, +)$ to $(\mathbb{Z}/n\mathbb{Z}, +)$, because

$$\pi_n(a+b) = \overline{a+b} = \overline{a} + \overline{b} = \pi_n(a) + \pi_n(b). \qquad ◇$$

Example 1.7.8. Homomorphisms out of cyclic groups are completely determined by one element. If $G = \langle g \rangle$ and $f : G \to H$ is a homomorphism, then

$$f(g^m) = f(g)^m.$$

Thus once you know $f(g)$, you know f on every element of G. In particular, a homomorphism $\mathbb{Z} \to H$ is determined by the image of 1. ◇

Group homomorphisms preserve the group structure. In particular, group homomorphisms preserve the identity element and all inverses:

Lemma 1.7.9. *Let $f : G \to H$ be a group homomorphism. Then $f(e_G) = e_H$. Moreover, for every $g \in G$, we have $f(g^{-1}) = f(g)^{-1}$.*

Proof. We have

$$f(e_G) = f(e_G e_G) = f(e_G)f(e_G),$$

so $f(e_G)$ is an idempotent element of H. The only idempotent element of a group is the identity, so $f(e_G) = e_H$.

For the second part, we have

$$e_H = f(e_G) = f(gg^{-1}) = f(g)f(g^{-1}),$$

so $f(g^{-1})$ is a right inverse of $f(g)$. Similarly, we can show that $f(g^{-1})$ is a left inverse of $f(g)$, and thus $f(g^{-1}) = f(g)^{-1}$. ■

Remark 1.7.10. Given a group G generated by a set S, any homomorphism $G \to H$ is completely determined by the images of the generators in S. In particular, if we want to construct a homomorphism from G to H, it suffices to specify the images of the generators in S and check that the relations in G are satisfied in H.

Definition 1.7.11. The *image* of a homomorphism $f : G \to H$ is the set $\{f(g) \mid g \in G\}$. The *kernel* of f is the set $\{g \in G \mid f(g) = e_H\}$.

Exercise (1.7.2). Prove that the image of a homomorphism is a subgroup of H and the kernel of a homomorphism is a subgroup of G.

Remark 1.7.12. Given any group homomorphism $f : G \to H$, we must have $e_G \in \ker f$ since $f(e_G) = e_H$.

When the kernel is as small as possible, meaning $\ker(f) = \{e\}$, then we say that the kernel is trivial. A homomorphism is injective if and only if its kernel is trivial, and a homomorphism is surjective if and only if its image is all of H.

Lemma 1.7.13. *A group homomorphism $f : G \to H$ is injective if and only if* $\ker f = \{e_G\}$.

Proof. If f is injective, then the only element of G that maps to e_H is e_G, so $\ker f = \{e_G\}$. Conversely, if $\ker f = \{e_G\}$ and $f(g_1) = f(g_2)$, then

$$e_H = f(g_1)f(g_2)^{-1} = f(g_1 g_2^{-1}),$$

so $g_1 g_2^{-1} \in \ker f$. Since $\ker f = \{e_G\}$, we have $g_1 g_2^{-1} = e_G$, so $g_1 = g_2$. Therefore, f is injective. ■

The easiest way to show that two groups are not isomorphic is to find a property that one group has but the other does not. For example, S_3 is not isomorphic to $\mathbb{Z}/6\mathbb{Z}$ because S_3 is not abelian while $\mathbb{Z}/6\mathbb{Z}$ is abelian.

Exercise (1.7.3). An isomorphism $G \to G$ is called an *automorphism* of G. Prove that the set of automorphisms of a group G forms a group under composition, called the *automorphism group* of G and denoted $\mathrm{Aut}(G)$.

Exercise (1.7.4). Let G be any group. Prove that the map from G to itself defined by $g \mapsto g^{-1}$ is an automorphism if and only if G is abelian.

1.8 GROUP ACTIONS: FIRST PASS

Group actions provide the perspective under which groups describe "symmetries". The confusing thing about the word "symmetries" is that it is being used in a technical sense. You can think of a group action as a way for a group to act on a set, moving its elements around in a way that respects the group structure.

Definition 1.8.1. Let G be a group and let X be a set. A *left action* of G on X is a rule that assigns to each $g \in G$ and each $x \in X$ an element $g \cdot x \in X$ (so a map $G \times X \to X$) such that

- $e \cdot x = x$ for every $x \in X$.
- $(gh) \cdot x = g \cdot (h \cdot x)$ for every $g, h \in G$ and every $x \in X$.

Example 1.8.2. The dihedral group D_n acts on the set of vertices of a regular n-gon. A rotation or reflection sends each vertex to another vertex, and composing symmetries agrees with the group operation in D_n. ◇

Example 1.8.3. The symmetric group S_n acts on $\{1, \ldots, n\}$ by $\sigma \cdot i = \sigma(i)$. This is the most basic example of a permutation group acting on a set. ◇

Note that we've already been thinking about D_n and S_n using group actions. Rather than thinking about them as being made up of abstract elements, we've been thinking of them as *symmetries of some set*. Symmetry here means: a bijection from the set to itself.

For each fixed $g \in G$, we get a map $\sigma_g : X \to X$ defined by $\sigma_g(x) = g \cdot x$.

Proposition 1.8.4. *Let G act on a set X. For each $g \in G$, the map $\sigma_g : X \to X$ is a bijection. Moreover, the assignment*

$$\rho : G \to \mathrm{Sym}(X), \qquad \rho(g) = \sigma_g$$

is a group homomorphism.

Proof. The map $\sigma_{g^{-1}}$ provides the inverse of σ_g:

$$(\sigma_{g^{-1}} \circ \sigma_g)(x) = g^{-1} \cdot (g \cdot x) = (g^{-1}g) \cdot x = e \cdot x = x,$$

and similarly $(\sigma_g \circ \sigma_{g^{-1}})(x) = x$. Thus σ_g is a bijection.

To check that ρ is a homomorphism, let $g, h \in G$. For every $x \in X$,

$$\rho(gh)(x) = (gh) \cdot x = g \cdot (h \cdot x) = (\rho(g) \circ \rho(h))(x).$$

Hence $\rho(gh) = \rho(g) \circ \rho(h)$. ■

The homomorphism $\rho : G \to \mathrm{Sym}(X)$ is called the *permutation representation* associated to the action. Conversely, any homomorphism $\rho : G \to \mathrm{Sym}(X)$ gives an action of G on X by the rule

$$g \cdot x = \rho(g)(x).$$

Thus a group action is the same thing as a way to represent elements of G as permutations of a set.

Example 1.8.5. The action of D_n on the vertices of a regular n-gon gives a permutation representation

$$\rho : D_n \to \mathrm{Sym}(\{V_0, \ldots, V_{n-1}\}) \cong S_n.$$

If r is the rotation with $r(V_i) = V_{i+1}$, then $\rho(r)$ is the cycle

$$(V_0\ V_1\ \cdots\ V_{n-1}).$$

If s is the reflection with $s(V_i) = V_{-i}$, then $\rho(s)$ is the permutation of the vertices determined by $V_i \mapsto V_{-i}$. So the abstract relation $srs = r^{-1}$ can be seen directly as a relation among permutations of the vertices. ◇

Example 1.8.6. Every group G acts on itself by left multiplication:

$$g \cdot x = gx.$$

The associated permutation representation is

$$\lambda : G \to \mathrm{Sym}(G), \qquad \lambda(g)(x) = gx.$$

This homomorphism is injective: if $\lambda(g)$ is the identity permutation of G, then it fixes e, so

$$g = ge = \lambda(g)(e) = e.$$

Thus G is isomorphic to the subgroup $\lambda(G) \leq \mathrm{Sym}(G)$. ◇

Theorem 1.8.7 (Cayley's theorem)**.** *Every finite group is isomorphic to a subgroup of* S_n.

Proof. Let G be a finite group with $|G| = n$. By the previous example, G is isomorphic to a subgroup of $\mathrm{Sym}(G)$. Since G has n elements, choosing a labeling of the elements of G identifies $\mathrm{Sym}(G)$ with S_n. ■

From a practical perspective, this is a nearly useless theorem. It is, however, a beautiful fact.

Exercise (1.8.1). Matrix groups also act naturally on vector spaces. For example, let

$$C_4 = \langle r \mid r^4 = e \rangle$$

be the cyclic group of order 4, and let

$$R = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

Show that there is a group action C_4 on $\mathrm{GL}_2(\mathbb{R})$ given by $r^k \cdot v = R^k v$ for $v \in \mathbb{R}^2$. This is a small example of a *representation*: instead of representing group elements as permutations of a set, we represent them as invertible matrices acting on a vector space.

Example 1.8.8. Every group G also acts on itself by conjugation:

$$g \cdot x = gxg^{-1}.$$

This action measures how far a group is from being abelian. If G is abelian, conjugation does nothing, since $gxg^{-1} = x$ for all $g, x \in G$. ◇

Later we will attach two important pieces of information to an action: the *orbit* of a point, which records where the point can move, and the *stabilizer* of a point, which records which group elements fix it.

CHAPTER 2

SUBGROUPS

2.1 DEFINITIONS AND EXAMPLES

As a reminder:

Definition 2.1.1. A *subgroup* of a group $(G, *)$ is a group $(H, *)$ such that $H \subseteq G$ and the operation on H is the operation on G restricted to H. We write $H \leq G$ to mean that H is a subgroup of G.

Proposition 2.1.2 (Standard sources of subgroups)**.** *Let* G *be a group.*

1. *If* $K \leq H$ *and* $H \leq G$*, then* $K \leq G$*.*
2. *If* $\{H_\alpha\}_{\alpha \in A}$ *is any collection of subgroups of* G*, then*

$$\bigcap_{\alpha \in A} H_\alpha$$

   is a subgroup of G*.*

3. *If* $f : G \to K$ *is a group homomorphism and* $H \leq G$*, then*

$$f(H) = \{f(h) \mid h \in H\}$$

   is a subgroup of K*.*

4. *If* $f : G \to K$ *is a group homomorphism, then* $\ker(f) \leq G$*.*
5. *The center*

$$Z(G) = \{z \in G \mid zg = gz \text{ for all } g \in G\}$$

   is a subgroup of G*.*

Proof. We prove the less immediate items with the one-step test.

For intersections, if the collection is empty, then the intersection is all of G. Otherwise, every subgroup H_α contains e_G, so the intersection is nonempty. If $x, y \in \bigcap_{\alpha \in A} H_\alpha$, then $x, y \in H_\alpha$ for every α, so $xy^{-1} \in H_\alpha$ for every α. Hence xy^{-1} is in the intersection.

For images, note that $\mathrm{im}(f)$ is nonempty since it contains $f(e_G) = e_K$. If $x, y \in \mathrm{im}(f)$, then $x = f(a)$ and $y = f(b)$ for some $a, b \in G$, and

$$xy^{-1} = f(a)f(b)^{-1} = f(ab^{-1}) \in \mathrm{im}(f).$$

This proves $\mathrm{im}(f) \leq K$. The same argument applied to the restriction of f to H proves that $f(H) \leq K$.

For kernels, if $x, y \in \ker(f)$, then

$$f(xy^{-1}) = f(x)f(y)^{-1} = e_K e_K^{-1} = e_K,$$

so $xy^{-1} \in \ker(f)$.

Finally, suppose $x, y \in Z(G)$. Since y commutes with every element of G, so does y^{-1}. For any $g \in G$, we have

$$(xy^{-1})g = x(y^{-1}g) = x(gy^{-1}) = (xg)y^{-1} = (gx)y^{-1} = gxy^{-1}.$$

Thus $xy^{-1} \in Z(G)$, so $Z(G) \leq G$.

The first item follows directly from the definition. ■

Exercise (2.1.1). Let H and K be subgroups of G. Prove that $H \cup K$ is a subgroup of G if and only if $H \subseteq K$ or $K \subseteq H$.

Definition 2.1.3. Let $f : G \to K$ be a group homomorphism and let $L \leq K$. The *preimage* of L under f is

$$f^{-1}(L) = \{g \in G \mid f(g) \in L\}.$$

Exercise (2.1.2). Prove that if $f : G \to K$ is a group homomorphism and $L \leq K$, then $f^{-1}(L) \leq G$.

Definition 2.1.4. Let X be a subset of a group G. The *subgroup generated by* X, denoted $\langle X \rangle$, is the intersection of all subgroups of G which contain X:

$$\langle X \rangle = \bigcap_{\substack{H \leq G \\ X \subseteq H}} H.$$

If $X = \{x\}$ has one element, we write $\langle x \rangle$ instead of $\langle \{x\} \rangle$ and call it the *cyclic subgroup generated by* x.

The subgroup $\langle X \rangle$ really is a subgroup by Proposition 2.1.2. By construction, it is the smallest subgroup of G containing X: every subgroup containing X also contains $\langle X \rangle$.

Proposition 2.1.5. *Let X be a subset of a group G. Then*

$$\langle X \rangle = \{x_1^{n_1} \cdots x_m^{n_m} \mid m \geq 0,\ x_i \in X,\ n_i \in \mathbb{Z}\}.$$

Here the product with $m = 0$ is defined to be the identity element.

Proof. Let

$$S = \{x_1^{n_1} \cdots x_m^{n_m} \mid m \geq 0,\ x_i \in X,\ n_i \in \mathbb{Z}\}.$$

Since $\langle X \rangle$ is a subgroup containing X, it must contain all finite products of elements of X and their inverses. Thus $S \subseteq \langle X \rangle$.

Conversely, S contains e_G by allowing the empty product. If $a, b \in S$, say

$$a = x_1^{n_1} \cdots x_m^{n_m} \qquad \text{and} \qquad b = y_1^{r_1} \cdots y_\ell^{r_\ell},$$

then

$$ab^{-1} = x_1^{n_1} \cdots x_m^{n_m} y_\ell^{-r_\ell} \cdots y_1^{-r_1} \in S.$$

Hence $S \leq G$ by the one-step test, and $X \subseteq S$. Since $\langle X \rangle$ is the smallest subgroup containing X, we have $\langle X \rangle \subseteq S$. ■

If $\langle S \rangle = G$, we say that S *generates* G, or that S is a *set of generators* for G.

Exercise (2.1.3). Let $f : G \to H$ be a group homomorphism and let $A \subseteq G$. Prove that

$$f(\langle A \rangle) = \langle f(a) \mid a \in A \rangle.$$

Deduce that if A generates G, then $f(A)$ generates $\mathrm{im}(f)$.

Exercise (2.1.4). Prove that the set of rotations in D_n is a subgroup of D_n. Prove that this subgroup is isomorphic to $\mathbb{Z}/n\mathbb{Z}$.

Exercise (2.1.5). Let

$$D_n = \langle r, s \mid r^n = e,\ s^2 = e,\ srs = r^{-1} \rangle.$$

For an integer k, prove that

$$\langle s, r^k s \rangle = \langle s, r^k \rangle.$$

Determine the order of this subgroup in terms of $\gcd(n, k)$.

Exercise (2.1.6). Prove that S_n is generated by the adjacent transpositions

$$(1\,2),\ (2\,3),\ \ldots,\ (n-1\,n).$$

2.2 Generators and Relations

Now that generated subgroups are defined, we can use them to talk about groups with chosen generating sets.

Definition 2.2.1. A group G is called *cyclic* if it can be generated by a single element. A group G is *finitely generated* if it can be generated by a finite set of elements.

Example 2.2.2. The group $\mathbb{Z}$ has one generator, the element 1, since every integer is a sum of copies of 1 and -1. Thus $\mathbb{Z} = \langle 1 \rangle$. ◇

Example 2.2.3. The group $\mathbb{Z}/n\mathbb{Z}$ is cyclic: $\mathbb{Z}/n\mathbb{Z} = \langle\overline{1}\rangle$. This means every residue class is obtained by adding $\overline{1}$ to itself some number of times. ◇

Definition 2.2.4. For an element x in a group G, define the *order* of x to be the smallest positive integer n such that $x^n = e$. We denote this integer $|x|$. If no such positive integer exists, we say that x has infinite order.

Example 2.2.5. The order of -1 in $\mathbb{Q}^\times$ is 2, since $(-1)^2 = 1$ and there is no smaller positive integer n such that $(-1)^n = 1$. The order of 1 in $\mathbb{Z}$ is infinite. ◇

Note that any element of a finite group has finite order. The proof is: consider an infinite sequence $1, g, g^2, \ldots$. Since the group is finite, there must be some repetition in this sequence. That is, there exist integers $m > n \geq 0$ such that $g^m = g^n$. Thus $g^{m-n} = e$, and so g has finite order.

Exercise (2.2.1). Prove that every cyclic group is abelian.

Exercise (2.2.2). Prove that $(\mathbb{Q}, +)$ and $\mathrm{GL}_2(\mathbb{Z}_2)$ are not cyclic groups.

Exercise (2.2.3). We can define an equivalence relation on rational numbers by declaring two rational numbers to be equal whenever they differ by an integer. We denote the set of equivalence classes by $\mathbb{Q}/\mathbb{Z}$.

1. For each n, prove that $\mathbb{Q}/\mathbb{Z}$ has a subgroup of order n.
2. Prove that $\mathbb{Q}/\mathbb{Z}$ is a divisible group: that is, if x is an element of $\mathbb{Q}/\mathbb{Z}$ and n is an integer, there exists an element y of $\mathbb{Q}/\mathbb{Z}$ such that $ny = x$.
3. Prove that $\mathbb{Q}/\mathbb{Z}$ is not finitely generated. (Hint: prove that if $x_1, \ldots, x_d$ is a finite subset of $\mathbb{Q}/\mathbb{Z}$, the subgroup generated by $x_1, \ldots, x_d$ is finite.)
4. Conclude that $\mathbb{Q}$ is not finitely generated.

Exercise (2.2.4). Let G be a group and let $S \subseteq G$. The *directed Cayley graph* $\mathrm{Cay}(G, S)$ has vertex set G, with a directed edge

$$g \longrightarrow gs$$

for every $g \in G$ and every $s \in S$. In additive notation, the edges are $g \to g + s$.

Draw the directed Cayley graphs of $\mathbb{Z}/6\mathbb{Z}$ with respect to each of the following subsets:

$$\{\overline{1}\}, \qquad \{\overline{2}\}, \qquad \{\overline{2}, \overline{3}\}, \qquad \{\overline{2}, \overline{5}\}.$$

Which of these subsets generate $\mathbb{Z}/6\mathbb{Z}$? What feature of the graph detects whether the subset generates the group?

Another way to organize the information of a group is by giving a presentation. For now this is only a preview; presentations become much more natural after quotient groups.

Definition 2.2.6. A *presentation* for a group is a way to specify a group in the following format:

$$G = \langle \text{set of generators} \,|\, \text{set of relations} \rangle.$$

A *relation* is an identity that holds between the generators. We usually record just enough relations so that every other valid equality between the generators can be deduced from these relations.

Example 2.2.7. The group $\mathbb{Z}$ has one generator, the element 1, which satisfies no relations. So we can write $\mathbb{Z} = \langle 1 \rangle$. ◇

Example 2.2.8. The following is a presentation for the group $\mathbb{Z}/n\mathbb{Z}$:

$$\mathbb{Z}/n\mathbb{Z} = \langle a \,|\, a^n = e \rangle.$$ ◇

In general, given a presentation, it is very difficult to prove that certain expressions are not actually equal to each other. In fact, there is no algorithm that, given a group presentation as input, can decide whether the group is actually the trivial group with one element.

More strikingly, there exists a finite presentation whose triviality is independent of the usual axioms of set theory.

2.3 Cyclic Groups in Detail

Recall that a group G is cyclic if $G = \langle x \rangle$ for some element $x \in G$. In this case we call x a *generator* of G. In this section, we do our first classification task of groups: we classify all cyclic groups up to isomorphism.

Theorem 2.3.1. *Let $G = \langle x \rangle$ be a cyclic group.*

1. *If x has infinite order, then G is infinite and the elements*

$$\ldots, x^{-2}, x^{-1}, e, x, x^2, \ldots$$

are all distinct. In particular, $G \cong \mathbb{Z}$.

2. *If x has finite order n, then*

$$G = \{e, x, x^2, \ldots, x^{n-1}\}$$

and $|G| = |x| = n$. In particular, $G \cong \mathbb{Z}/n\mathbb{Z}$.

Proof. First suppose x has infinite order. Since $G = \langle x \rangle$, every element of G has the form x^m for some $m \in \mathbb{Z}$. If $x^a = x^b$ with $a > b$, then $x^{a-b} = e$, contradicting the assumption that x has infinite order. Thus all powers of x are distinct. The map

$$\mathbb{Z} \to G, \qquad m \mapsto x^m$$

is therefore a bijective homomorphism from $(\mathbb{Z}, +)$ to G.

Now suppose $|x| = n$. The elements

$$e = x^0, x, x^2, \ldots, x^{n-1}$$

are distinct: if $x^i = x^j$ with $0 \leq i < j < n$, then $x^{j-i} = e$ with $0 < j - i < n$, contradicting the minimality of n.

Finally, every integer m can be written as $m = qn + r$ with $0 \leq r < n$, and then

$$x^m = x^{qn+r} = (x^n)^q x^r = x^r.$$

Thus the displayed list contains every element of G.

It remains to prove the isomorphism statement. Define

$$\phi : \mathbb{Z}/n\mathbb{Z} \to G, \qquad \phi(\overline{m}) = x^m.$$

Its easy to check this is well-defined and a homomorphism. It is surjective because every element of G is a power of x. It is injective because if $\phi(\overline{m}) = e$, then $x^m = e$, so n divides m by the minimality of $n = |x|$. Hence $\overline{m} = \overline{0}$. Thus ϕ is an isomorphism, so $G \cong \mathbb{Z}/n\mathbb{Z}$. ■

So up to isomorphism, the only cyclic groups are $\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$ for $n \geq 1$. More than this: every subgroup of these are also cyclic.

Exercise (2.3.1). Let G be a group and let $g \in G$. Define

$$\varphi_g : \mathbb{Z} \to G, \qquad \varphi_g(n) = g^n.$$

1. Prove that φ_g is a group homomorphism.
2. Prove that $\mathrm{im}(\varphi_g) = \langle g \rangle$.
3. Determine $\ker(\varphi_g)$ when g has finite order m.
4. Determine $\ker(\varphi_g)$ when g has infinite order.

Proposition 2.3.2. *Every subgroup of a cyclic group is cyclic.*

Proof. Let $G = \langle x \rangle$ be a cyclic group, and let $H \leq G$. If $H = \{e\}$, then H is cyclic. Otherwise, let n be the smallest positive integer such that $x^n \in H$. We claim that $H = \langle x^n \rangle$.

Since $x^n \in H$, we have $\langle x^n \rangle \leq H$. Conversely, take any element $x^m \in H$. Write $m = qn + r$ with $0 \leq r < n$. Then

$$x^r = x^{m-qn} = x^m (x^n)^{-q} \in H.$$

By the minimality of n, we must have $r = 0$, so $x^m \in \langle x^n \rangle$. Thus $H = \langle x^n \rangle$. ■

But which subgroups of a cyclic group are there? The answer is that they correspond to the divisors of the order of the group.

Lemma 2.3.3. *Let G be a group and let $x \in G$ have finite order n. If $x^m = e$ for some integer m, then n divides m.*

Proof. By the division algorithm, write

$$m = qn + r$$

with $0 \leq r < n$. Since $x^n = e$ and $x^m = e$, we have

$$e = x^m = x^{qn+r} = (x^n)^q x^r = x^r.$$

By the minimality of $n = |x|$, this forces $r = 0$. Hence n divides m. ■

Theorem 2.3.4. *Let $G = \langle x \rangle$ be a cyclic group of order n. For any integer k,*

$$|x^k| = \frac{n}{\gcd(n, k)}.$$

In particular,

$$\langle x^k \rangle = G \quad \textit{if and only if} \quad \gcd(n, k) = 1.$$

Proof. Set $d = \gcd(n, k)$, and write $n = da$ and $k = db$ with $\gcd(a, b) = 1$. Let $y = x^k$. Then

$$y^a = x^{ka} = x^{dba} = x^{nb} = e,$$

so $|y|$ divides a by Lemma 2.3.3.

On the other hand, $y^{|y|} = e$, so $x^{k|y|} = e$. Again by Lemma 2.3.3, n divides $k|y|$. Substituting $n = da$ and $k = db$, we get $da \mid db|y|$, and hence $a \mid b|y|$. Since $\gcd(a, b) = 1$, it follows that $a \mid |y|$.

Thus $|y|$ divides a and a divides $|y|$, so

$$|x^k| = |y| = a = \frac{n}{\gcd(n, k)}.$$

The final statement follows because x^k generates G exactly when $|x^k| = |G| = n$. ■

Example 2.3.5. In $\mathbb{Z}/n\mathbb{Z}$, the element $\overline{k}$ generates the whole group if and only if $\gcd(n,k) = 1$. For example, the generators of $\mathbb{Z}/12\mathbb{Z}$ are $\overline{1}, \overline{5}, \overline{7}$, or $\overline{11}$. ◇

Exercise (2.3.2). Let $x, y \in G$ commute, and suppose $|x| = m$, $|y| = n$, and $\gcd(m,n) = 1$. Prove that $|xy| = mn$. Give an example showing the coprime hypothesis cannot simply be omitted.

Proposition 2.3.6. *Let $G = \langle x \rangle$ be a finite cyclic group. The subgroups of G are in bijection with the positive divisors of $|G|$:*

$$d \longmapsto \langle x^{|G|/d} \rangle.$$

Proof. Let $n = |G|$. If d is a positive divisor of n, then by Theorem 2.3.4,

$$|x^{n/d}| = \frac{n}{\gcd(n, n/d)} = \frac{n}{n/d} = d.$$

Therefore $\langle x^{n/d} \rangle$ is a subgroup of G of order d. Since different divisors give subgroups of different orders, the assignment is injective.

It remains to show that every subgroup appears this way. Let $H \leq G$. By Proposition 2.3.2, H is cyclic, so $H = \langle x^k \rangle$ for some integer k. Set $d = |H|$. Again by Theorem 2.3.4,

$$d = |x^k| = \frac{n}{\gcd(n,k)}.$$

Set $s = \gcd(n,k) = n/d$. Then $k = sb$ and $n = sd$ for some integer b with $\gcd(b,d) = 1$. Inside the cyclic group $\langle x^s \rangle$ of order d, the element

$$x^k = (x^s)^b$$

is a generator. Hence

$$H = \langle x^k \rangle = \langle x^s \rangle = \langle x^{n/d} \rangle.$$

Thus every subgroup is in the image, so the assignment is a bijection. ■

Exercise (2.3.3). List all subgroups of $\mathbb{Z}/18\mathbb{Z}$.

Exercise (2.3.4). Show that if a finite group G has a unique subgroup of order d for each positive divisor d of $|G|$, then G is cyclic.

Exercise (2.3.5). Prove that the following groups are *not* cyclic: $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$, and $\mathbb{Z} \times \mathbb{Z}$.

Exercise (2.3.6). Prove that $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ is cyclic if and only if $\gcd(m,n) = 1$. When it is cyclic, exhibit a generator.

This completes a classification of cyclic groups and their subgroups. For a general finite group, the divisors of $|G|$ do not control subgroups so cleanly. The main Sylow theorem is the strongest general substitute: if

$$|G| = p^r m \qquad \text{with} \qquad p \nmid m,$$

then G has a subgroup of order p^r; all such subgroups are conjugate; and the number of such subgroups divides m and is congruent to 1 modulo p. We will not prove this theorem here, but it is one of the main tools for understanding finite groups beyond the cyclic case.

Exercise (2.3.7). Let p be a prime and let n be a positive integer. Show that if x is an element of the group G such that $x^{p^n} = e$, then $|x| = p^m$ for some integer $m \leq n$.

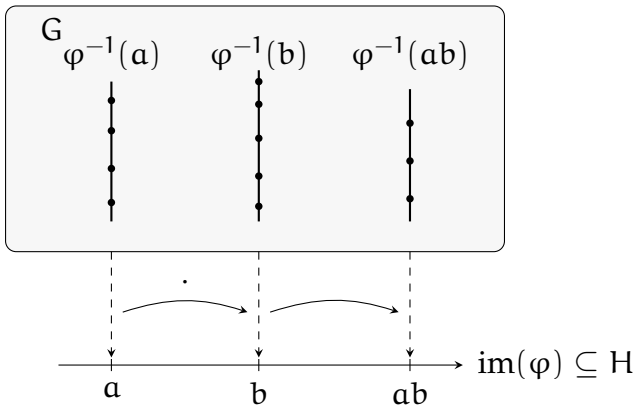
Exercise (2.3.8). Show that $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is not cyclic for $n \geq 3$.

CHAPTER 3

QUOTIENT GROUPS

Recall the construction of $\mathbb{Z}/n\mathbb{Z}$: we put an equivalence relation on $\mathbb{Z}$, take equivalence classes, and then add classes by choosing representatives. This was our first quotient group. We now seek to generalize and understand this construction for arbitrary groups G. This will be another way to obtain a "smaller" group from G, and it can also be used to study the structure of G, like subgroups did.

Here is a perspective that helped me a lot: The study of quotient groups of G is essentially equivalent to the study of homomorphisms of G to another group. Let $\varphi : G \to H$ be a homomorphism and recall that the fibers of φ are the sets of elements of G projecting to single elements of H. You can picture this as in the following figure.



The group operation in H provides a way to multiply two elements a and b in the image of φ. This gives a natural multiplication of the *fibers* lying above those two points. This then makes the *set of fibers into a group*. This is a quotient group – G has been partitioned into pieces and these pieces have the structure of a group.

Since the multiplication of fibers is defined from multiplication in H, it is easy to see an important fact: this quotient group is isomorphic to $\mathrm{im}\,\varphi$. We now need to make all of this precise: how do we form a quotient group from a group G without having a homomorphism to another group? The answer is that we need to find a way to partition G into pieces that "behave like fibers", and we will see that the answer is normal subgroups.

3.1 Cosets and Lagrange's Theorem

Definition 3.1.1. Let $\sim$ be an equivalence relation on a group G. We say that $\sim$ is *compatible with multiplication* if, whenever $x \sim y$, we also have

$$xz \sim yz \qquad \text{and} \qquad zx \sim zy$$

for every $z \in G$.

Lemma 3.1.2. *Let G be a group and let $\sim$ be an equivalence relation on G. The rule*

$$[x] \cdot [y] = [xy]$$

is well-defined on the set of equivalence classes $G/\sim$ if and only if $\sim$ is compatible with multiplication. In that case, $G/\sim$ is a group under this operation.

Proof. Suppose first that $\sim$ is compatible with multiplication. If $[x] = [x']$ and $[y] = [y']$, then $x \sim x'$ and $y \sim y'$. Compatibility gives

$$xy \sim x'y \qquad \text{and} \qquad x'y \sim x'y',$$

so by transitivity $xy \sim x'y'$. Hence $[xy] = [x'y']$, and the product of classes is well-defined.

Conversely, suppose $[x] \cdot [y] = [xy]$ is well-defined. If $x \sim x'$, then $[x] = [x']$, so for any $z \in G$,

$$[xz] = [x][z] = [x'][z] = [x'z].$$

Thus $xz \sim x'z$. Similarly,

$$[zx] = [z][x] = [z][x'] = [zx'],$$

so $zx \sim zx'$. Therefore $\sim$ is compatible with multiplication.

Finally, if the operation is well-defined, the group axioms are inherited from G:

$$[x]([y][z]) = [x][yz] = [x(yz)] = [(xy)z] = [xy][z] = ([x][y])[z],$$

the identity is $[e_G]$, and the inverse of $[x]$ is $[x^{-1}]$. ∎

Definition 3.1.3. If $\sim$ is an equivalence relation on a group G compatible with multiplication, then the group $G/\sim$ of equivalence classes is called the *quotient group* of G by $\sim$.

Example 3.1.4. Let $G = \mathbb{Z}$ and fix an integer $n \geq 1$. Let $\sim_n$ be congruence modulo n. This equivalence relation is compatible with addition, and

$$\mathbb{Z}/\sim_n = \mathbb{Z}/n\mathbb{Z}.$$ ◇

Now we need a systematic way to produce equivalence relations on groups. Subgroups give the most important examples.

Definition 3.1.5. Let $H \leq G$ be a subgroup. A *left coset* of H in G is a subset of G of the form

$$gH = \{gh \mid h \in H\}$$

for some $g \in G$. A *right coset* of H in G is a subset of G of the form

$$Hg = \{hg \mid h \in H\}$$

for some $g \in G$.

Example 3.1.6. Let $G = \mathbb{Z}$ and let $H = n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$. Since $\mathbb{Z}$ is abelian, the left and right cosets are the same:

$$a + n\mathbb{Z} = \{a + nk \mid k \in \mathbb{Z}\}.$$

These are exactly the congruence classes modulo n. ◇

Lemma 3.1.7 (Coset criterion)**.** *Let* $H \leq G$ *and let* $x, y \in G$*. Then*

$$xH = yH \quad \iff \quad y^{-1}x \in H \quad \iff \quad x^{-1}y \in H.$$

Equivalently, x *and* y *lie in the same left coset of* H *exactly when* $y^{-1}x \in H$*. The same statement holds for right cosets.*

Proof. If $xH = yH$, then $x \in yH$, so $x = yh$ for some $h \in H$ and hence $y^{-1}x = h \in H$. Conversely, if $y^{-1}x = h \in H$, then $x = yh$, and

$$xH = yhH = yH.$$

Since H is closed under inverses, $y^{-1}x \in H$ if and only if $x^{-1}y = (y^{-1}x)^{-1} \in H$. The right coset statement is exactly the same. ■

Proposition 3.1.8. *Let* $H \leq G$*. The left cosets of* H *in* G *partition* G*, and the right cosets of* H *in* G *also partition* G*.*

Proof. We prove the statement for left cosets. Every element $g \in G$ belongs to at least one left coset, namely gH, since $g = ge_G$ and $e_G \in H$.

Now suppose two left cosets xH and yH intersect. Choose $z \in xH \cap yH$. Then z lies in the same left coset as x and also in the same left coset as y. By Lemma 3.1.7, $xH = zH$ and $zH = yH$, so $xH = yH$. Thus any two left cosets are either equal or disjoint. ■

Proposition 3.1.9. *Let* $H \leq G$*. Every left coset and every right coset of* H *has the same cardinality as* H*. More precisely, for every* $g \in G$*,*

$$|gH| = |H| = |Hg|.$$

Proof. The map

$$H \to gH, \qquad h \mapsto gh$$

is surjective by definition of gH. It is injective because $gh_1 = gh_2$ implies $h_1 = h_2$ after multiplying on the left by g^{-1}. Thus $|gH| = |H|$.

Similarly, the map

$$H \to Hg, \qquad h \mapsto hg$$

is a bijection, so $|Hg| = |H|$. ■

Definition 3.1.10. The *index* of a subgroup H in a group G, denoted $[G : H]$, is the number of left cosets of H in G. Equivalently, it is the number of right cosets of H in G.

Now, we prove a statement older than the modern definition of a group. Lagrange's theorem says that the order of a subgroup must divide the order of the group.

Theorem 3.1.11 (Lagrange's theorem)**.** *Let* G *be a finite group and let* $H \leq G$*. Then*

$$|G| = |H|[G : H].$$

In particular, $|H|$ *divides* $|G|$*.*

Proof. The left cosets of H partition G, and each left coset has $|H|$ elements. If there are $[G : H]$ left cosets, then

$$|G| = |H|[G : H].$$

■

One reason Lagrange's theorem is important is that it turns counting information about a group into arithmetic information about its elements.

Example 3.1.12 (Fermat's little theorem)**.** Let p be prime. The nonzero congruence classes modulo p form a group under multiplication:

$$(\mathbb{Z}/p\mathbb{Z})^\times = \{\overline{1}, \overline{2}, \ldots, \overline{p-1}\}.$$

This group has $p - 1$ elements. If a is an integer not divisible by p, then $\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^\times$. By Lagrange's theorem, the order of the subgroup $\langle \overline{a} \rangle$ divides $p - 1$. Therefore

$$\overline{a}^{p-1} = \overline{1},$$

or equivalently

$$a^{p-1} \equiv 1 \pmod{p}.$$

This is Fermat's little theorem. If $p \nmid a$, multiplying both sides by a gives

$$a^p \equiv a \pmod{p}$$

and if $p \mid a$, the same congruence is immediate. ◇

The converse of Lagrange's theorem is false: if d divides $|G|$, there need not be a subgroup of G of order d. The strongest general converse is given by the Sylow theorem, which we will not prove.

Theorem 3.1.13 (Sylow)**.** *If* p *is prime and* p^a *divides* $|G|$*, then* G *has a subgroup of order* p^a*.*

At this point, these cosets are looking a lot like the equivalence classes we need to form a quotient group, or the fibers of a homomorphism we introduced in the beginning. That is, what we'd like to do is use $x \sim y$ if x and y are in the same coset. But there is a critical problem: the left and right cosets need not be the same. This is exactly the obstruction to $\sim$ being compatible with multiplication.

Example 3.1.14. Let $G = D_n$ and let $H = \langle s \rangle = \{e, s\}$, where s is a reflection. The left cosets of H are

$$\{e, s\}, \{r, rs\}, \{r^2, r^2 s\}, \ldots, \{r^{n-1}, r^{n-1} s\}.$$

The right cosets are

$$\{e, s\}, \{r, r^{-1} s\}, \{r^2, r^{-2} s\}, \ldots, \{r^{n-1}, r^{-(n-1)} s\}.$$

These lists need not be the same. For example, r lies in the left coset $\{r, rs\}$, while its right coset is $\{r, r^{-1} s\}$. Since $|D_n| = 2n$ and $|H| = 2$, we have $[D_n : H] = n$. ◇

If we choose certain subgroups it works out:

Example 3.1.15. Again let $G = D_n$, but now let $K = \langle r \rangle$ be the subgroup of rotations. The left cosets are

$$K \qquad \text{and} \qquad sK = \{s, sr, \ldots, sr^{n-1}\},$$

while the right cosets are

$$K \qquad \text{and} \qquad Ks = \{s, rs, \ldots, r^{n-1} s\}.$$

In this case $sK = Ks$, so the left and right cosets agree. Since $|K| = n$, we have $[D_n : K] = 2$. ◇

This is because K is a *normal subgroup* of D_n, which we will explore in the next section.

Exercise (3.1.1). In S_3, let $H = \langle (1\,2) \rangle$. List the left cosets of H. Then show directly that the rule

$$(xH)(yH) = xyH$$

is not well-defined.

3.2 NORMAL SUBGROUPS

The examples at the end of the previous section show that left and right cosets do not always agree. This is exactly the obstruction to multiplying cosets in a sensible way. The subgroups for which this obstruction disappears are called normal subgroups.

Definition 3.2.1. We say that $N \leq G$ is a *normal subgroup* of G, written $N \trianglelefteq G$, if

$$gNg^{-1} = N$$

for every $g \in G$.

The element gng^{-1} is called the *conjugate* of n by g. Thus a subgroup is normal if it is closed under conjugation by every element of the ambient group.

Remark 3.2.2. Just to be clear, you dont ask if a group is normal. Normality is a property of a subgroup inside a group, and it has very little to do with the actual structure of the subgroup.

Here are many examples of normal subgroups.

Example 3.2.3. Every group G has two trivial normal subgroups:

$$\{e_G\} \trianglelefteq G \qquad \text{and} \qquad G \trianglelefteq G. \qquad \diamond$$

Example 3.2.4. Every subgroup of an abelian group is normal. Indeed, if G is abelian and $H \leq G$, then

$$ghg^{-1} = gg^{-1}h = h$$

for all $g \in G$ and $h \in H$. Hence $gHg^{-1} = H$ for every $g \in G$. $\diamond$

Example 3.2.5. More generally, for any group G, the center

$$Z(G) = \{z \in G \mid zg = gz \text{ for all } g \in G\}$$

is normal in G. $\diamond$

Exercise (3.2.1). Prove that the kernel of a group homomorphism is a normal subgroup.

The following proposition gives some useful criteria for checking normality.

Proposition 3.2.6. *Let* $N \leq G$. *The following conditions are equivalent:*

1. $N \trianglelefteq G$.
2. $gNg^{-1} \subseteq N$ *for every* $g \in G$.
3. $gN = Ng$ *for every* $g \in G$.

Proof. Clearly (1) implies (2). Conversely, if $gNg^{-1} \subseteq N$ for every $g \in G$, then applying this to g^{-1} gives $g^{-1}Ng \subseteq N$. Conjugating by g gives $N \subseteq gNg^{-1}$, so $gNg^{-1} = N$. Thus (1) and (2) are equivalent.

Also, $gNg^{-1} = N$ if and only if $gN = Ng$, by multiplying on the right by g. Thus (1) and (3) are equivalent. ■

Exercise (3.2.2). Prove that every subgroup of index 2 is normal.

Exercise (3.2.3). Let $f : G \to H$ be a group homomorphism and let $K \trianglelefteq H$. Prove that

$$f^{-1}(K) \trianglelefteq G.$$

So how do we find normal subgroups? We've already show that kernels of homomorphism are normal, but in fact, these are the only examples.

Proposition 3.2.7. *A subgroup $N \leq G$ is normal if and only if it is the kernel of some homomorphism $f : G \to H$.*

Proof. Deferred till later. ■

Remark 3.2.8. The relation "is a normal subgroup of" is not transitive. Let

$$V = \{e, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\} \leq S_4.$$

One can show that $V \trianglelefteq S_4$. Since V is abelian, the subgroup

$$A = \{e, (1\,2)(3\,4)\}$$

is normal in V. But A is not normal in S_4, because

$$(1\,3)(1\,2)(3\,4)(1\,3)^{-1} = (1\,4)(2\,3) \notin A.$$

We will end with an example which is part of the motivation for Galois to create group theory.

Definition 3.2.9. A permutation in S_n is *even* if it can be written as a product of an even number of transpositions. The *alternating group* A_n is the set of all even permutations in S_n.

Remark 3.2.10. In Chapter 1 we proved that every permutation is a product of transpositions. What is not obvious is that the parity of the number of transpositions is well-defined: a permutation cannot be written both as a product of an even number of transpositions and as a product of an odd number of transpositions. Equivalently, there is a well-defined homomorphism

$$\operatorname{sgn} : S_n \to \{1, -1\},$$

which sends even permutations to 1 and odd permutations to -1.

Proposition 3.2.11. *For $n \geq 2$, the alternating group A_n is normal in S_n.*

Proof. By the previous remark, $A_n = \ker(\text{sgn})$. Since kernels of homomorphisms are normal, $A_n \trianglelefteq S_n$. ■

Remark 3.2.12. At the time, formulas for solving polynomial equations were being sought (like the quadratic formula). Such formulas were known for polynomials of degree 2, 3, and 4, but not for degree 5 or higher. He wanted to show that a general quintic polynomial is not solvable by radicals. We will return to this story later and sketch how he proved this.

3.3 QUOTIENT GROUPS

We now arrive at the point of normal subgroups: they are exactly the subgroups for which we can multiply cosets in a well-defined way.

Theorem 3.3.1. *Let $N \leq G$. The operation*

$$xN \cdot yN = xyN$$

makes the set of left cosets of N in G into a group if and only if $N \trianglelefteq G$.

Proof. Suppose $N \trianglelefteq G$. We first check that the operation is well-defined. If $xN = x'N$ and $yN = y'N$, then $x' = xn_1$ and $y' = yn_2$ for some $n_1, n_2 \in N$. Since N is normal, $y^{-1}n_1y \in N$, and hence

$$x'y' = xn_1yn_2 = xy(y^{-1}n_1y)n_2 \in xyN.$$

Therefore $x'y'N = xyN$. The identity is N, the inverse of gN is $g^{-1}N$, and associativity follows from associativity in G.

Conversely, suppose the formula gives a well-defined group operation on the set of left cosets. If $n \in N$ and $g \in G$, then $gN = gnN$, so well-definedness gives

$$N = (gN)(g^{-1}N) = (gnN)(g^{-1}N) = gng^{-1}N.$$

Hence $gng^{-1} \in N$. By Proposition 3.2.6, $N \trianglelefteq G$. ■

Definition 3.3.2. Let $N \trianglelefteq G$. The *quotient group* G/N is the group whose elements are the left cosets of N in G, with multiplication

$$(xN)(yN) = (xy)N.$$

The identity element is $e_GN = N$ and the inverse of gN is $(gN)^{-1} = g^{-1}N$.

This is the same quotient group as $G/\sim_N$, where $\sim_N$ is the equivalence relation defined by $x \sim_N y$ if and only if $x^{-1}y \in N$. The equivalence classes of $\sim_N$ are exactly the left cosets of N in G.

Remark 3.3.3. Since N is normal, the left and right cosets of N agree. Thus we can also view G/N as the set of right cosets of N in G, with multiplication

$$(Nx)(Ny) = N(xy).$$

Remark 3.3.4. The order of the quotient group is the index of N in G:

$$|G/N| = [G : N].$$

If G is finite, then Lagrange's theorem gives

$$|G/N| = \frac{|G|}{|N|}.$$

Example 3.3.5. Since $A_n = \ker(\mathrm{sgn})$, the quotient S_n/A_n has two elements. The non-trivial coset is the set of odd permutations, and

$$S_n/A_n \cong \mathbb{Z}/2\mathbb{Z}.$$

◇

Exercise (3.3.1). Let $N \trianglelefteq G$ and let $g \in G$. Prove that the order of $gN \in G/N$ is the smallest positive integer m such that $g^m \in N$, if such an m exists. Use this to compute the orders of all elements of

$$(\mathbb{Z}/12\mathbb{Z})/\langle\overline{4}\rangle.$$

Remember the motivation from the beginning of this chapter: we should think of the quotient group G/N as the set of fibers of a homomorphism from G to another group. The next lemma makes this precise.

Definition 3.3.6. Let $N \trianglelefteq G$. The map

$$\pi : G \to G/N, \qquad \pi(g) = gN,$$

is called the *canonical quotient map*, the *canonical surjection*, or the *canonical projection* from G to G/N.

Lemma 3.3.7. *Let* $N \trianglelefteq G$. *The canonical quotient map*

$$\pi : G \to G/N$$

is a surjective group homomorphism with kernel N.

Proof. Surjectivity is immediate: every element of G/N has the form gN for some $g \in G$. The map π is a homomorphism since

$$\pi(g_1g_2) = g_1g_2N = (g_1N)(g_2N) = \pi(g_1)\pi(g_2).$$

Using Lemma 3.1.7, its kernel is

$$\begin{aligned}\ker(\pi) &= \{g \in G \mid \pi(g) = N\}\\ &= \{g \in G \mid gN = N\}\\ &= \{g \in G \mid g \in N\} = N.\end{aligned}$$

■

Corollary 3.3.8 (Proposition 3.2.7)**.** *A subgroup* $N \leq G$ *is normal if and only if it is the kernel of some homomorphism* $f : G \to H$*.*

Proof. If N is the kernel of a homomorphism, then the earlier exercise shows that N is normal. Lemma 3.3.7 gives the converse. ■

Example 3.3.9. The *infinite dihedral group* D_∞ is the set

$$D_\infty = \{r^i, r^i s \mid i \in \mathbb{Z}\},$$

with multiplication determined by

$$\begin{aligned} r^i r^j &= r^{i+j}, & r^i(r^j s) &= r^{i+j}s, \\ (r^i s)r^j &= r^{i-j}s, & (r^i s)(r^j s) &= r^{i-j}. \end{aligned}$$

Informally, this is the group with presentation

$$D_\infty = \langle r, s \mid s^2 = e,\ srs^{-1} = r^{-1}\rangle.$$

For $n \geq 3$, the subgroup $\langle r^n\rangle$ is normal in D_∞, and

$$D_\infty / \langle r^n\rangle \cong D_n.$$

The isomorphism is induced by sending

$$r\langle r^n\rangle \longmapsto r \qquad \text{and} \qquad s\langle r^n\rangle \longmapsto s. \qquad \diamond$$

Exercise (3.3.2). Let $m \mid n$ with $m \geq 3$. In $D_n = \langle r, s\rangle$, prove that $\langle r^m\rangle \trianglelefteq D_n$, and prove that

$$D_n / \langle r^m\rangle \cong D_m.$$

Remark 3.3.10. In the previous example, both D_∞ and $\langle r^n\rangle$ are infinite, but the quotient is finite. Thus a quotient of an infinite group by an infinite subgroup can be finite.

A quotient of an infinite group by an infinite subgroup can also be infinite. For example, in the additive group $\mathbb{Z} \times \mathbb{Z}$, the subgroup $\mathbb{Z} \times \{0\}$ is normal, and the quotient has one coset for each possible second coordinate. In contrast, every quotient of a finite group is finite.

Definition 3.3.11. Let G be a group. For $x, y \in G$, the *commutator* of x and y is the element

$$[x, y] = xyx^{-1}y^{-1}.$$

The *commutator subgroup*, or *derived subgroup*, of G is the subgroup generated by all commutators:

$$[G, G] = \langle [x, y] \mid x, y \in G\rangle.$$

We have $[x, y] = e_G$ if and only if $xy = yx$. More generally, $[G, G] = \{e_G\}$ if and only if G is abelian. Thus the commutator subgroup measures how far G is from being abelian.

Exercise (3.3.3). Show that $[G, G]$ is a normal subgroup of G. Hint: first show that

$$g[x, y]g^{-1} = [gxg^{-1}, gyg^{-1}].$$

Exercise (3.3.4). Let G be a group. Define the *abelianization* of G as $G_{ab} = G/[G, G]$. Prove that the abelianization is the largest abelian quotient of G, in the following sense: if $N \trianglelefteq G$ and G/N is abelian, then $[G, G] \leq N$.

Exercise (3.3.5). Compute the commutator subgroups $[S_3, S_3]$ and $[D_4, D_4]$. Then determine S_3^{ab} and D_4^{ab}.

It is now time to prove the isomorphism theorems, which explain how homomorphisms and quotient groups fit together.

3.4 ISOMORPHISM THEOREMS

Take any homomorphism $\varphi : G \to H$. As we showed, the kernel $\ker \varphi$ is a normal subgroup of G (and in fact all normal subgroups arise as kernels of homomorphisms), so we may take the quotient group $G/\ker \varphi$. Now, think back to the picture we have of quotient groups as fibers of a homomorphism. This picture makes it clear that the quotient group $G/\ker \varphi$ is isomorphic to the image of φ in H. This is the first fundamental isomorphism theorem, which we now state and prove.

Theorem 3.4.1 (First Isomorphism Theorem)**.** *If* $\varphi : G \to H$ *is a homomorphism of groups, then* $\ker \varphi \trianglelefteq G$ *and* $G/\ker \varphi \cong \operatorname{im} \varphi$*.*

Proof. We have already shown that $\ker \varphi \trianglelefteq G$. Define a map

$$\psi : G/\ker \varphi \to \operatorname{im} \varphi, \qquad \psi(g \ker \varphi) = \varphi(g).$$

This is well-defined: if $g \ker \varphi = g' \ker \varphi$, then $g^{-1}g' \in \ker \varphi$, so $\varphi(g^{-1}g') = e_H$ and hence $\varphi(g) = \varphi(g')$. The map ψ is surjective by definition of the image, and it is injective because if $\psi(g \ker \varphi) = e_H$, then $g \in \ker \varphi$ and hence $g \ker \varphi = \ker \varphi$. ■

Example 3.4.2. Suppose $\varphi : V \to W$ is a linear transformation of finite-dimensional vector spaces. Then the first isomorphism theorem implies that $|V : \ker(\varphi)| = |\operatorname{im} \varphi|$. This is the the rank-nullity theorem, which says that

$$\dim V = \dim \ker(\varphi) + \dim \operatorname{im}(\varphi).$$ ◇

Example 3.4.3. The First Isomorphism Theorem gives a second proof of the classification of cyclic groups. Let $G = \langle x \rangle$ and define

$$\phi : \mathbb{Z} \to G, \qquad \phi(m) = x^m.$$

This is a surjective homomorphism. If x has infinite order, then $\ker \phi = \{0\}$, so $\mathbb{Z} \cong G$. If x has finite order n, then $\ker \phi = n\mathbb{Z}$, so the First Isomorphism Theorem gives

$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\ker \phi \cong G. \qquad \diamond$$

Example 3.4.4. Let F be a field and let $n \geq 1$. The determinant map

$$\det : GL_n(F) \to F^\times$$

is a surjective group homomorphism. Its kernel is

$$SL_n(F) = \{A \in GL_n(F) \mid \det(A) = 1\}.$$

Therefore $SL_n(F) \trianglelefteq GL_n(F)$, and the First Isomorphism Theorem gives

$$GL_n(F)/SL_n(F) \cong F^\times. \qquad \diamond$$

Example 3.4.5. Let $G = \mathbb{R}^\times$ and let $N = \{1, -1\}$. Since G is abelian, $N \trianglelefteq G$. The absolute value map

$$|\cdot| : \mathbb{R}^\times \to \mathbb{R}^\times_{>0}$$

is a surjective homomorphism with kernel N. Hence

$$\mathbb{R}^\times/\{1, -1\} \cong \mathbb{R}^\times_{>0}. \qquad \diamond$$

To state the Second Isomorphism Theorem, we first need a small piece of notation.

Definition 3.4.6. Let H and K be subgroups of a group G. Define

$$HK = \{hk \mid h \in H,\ k \in K\}.$$

In general, HK is only a subset of G, not necessarily a subgroup.

Remark 3.4.7. The subsets H and K are both contained in HK: for example, $h = he_G \in HK$ for every $h \in H$, and $k = e_G k \in HK$ for every $k \in K$.

Exercise (3.4.1). Let H and K be subgroups of G.

1. Prove that HK is a subgroup of G if and only if $HK = KH$.
2. Prove that if at least one of H or K is normal in G, then

$$HK \leq G \qquad \text{and} \qquad HK = KH = \langle H \cup K \rangle.$$

Remark 3.4.8. The equality $HK = KH$ does not mean that every element of H commutes with every element of K. It is an equality of subsets.

Theorem 3.4.9 (Second Isomorphism Theorem)**.** *Let* G *be a group, let* $H \leq G$*, and let* $N \trianglelefteq G$*. Then*

$$HN \leq G, \qquad H \cap N \trianglelefteq H, \qquad N \trianglelefteq HN,$$

and there is an isomorphism $H/(H \cap N) \cong HN/N$*.*

Proof. Since N is normal in G, Exercise (3.4.1) gives $HN \leq G$. Also, $H \cap N \trianglelefteq H$ because $N \trianglelefteq G$, and $N \trianglelefteq HN$ because $HN \leq G$.

Let

$$\varphi : H \to HN/N, \qquad \varphi(h) = hN.$$

This is the composition of the inclusion $H \hookrightarrow HN$ with the canonical projection $HN \twoheadrightarrow HN/N$, so it is a homomorphism. The map φ is surjective because every element of HN/N has the form $hnN = hN$, with $h \in H$ and $n \in N$.Finally,

$$\ker \varphi = \{h \in H \mid hN = N\} = H \cap N.$$

The result follows from the First Isomorphism Theorem. ■

Corollary 3.4.10. *If* H *and* N *are finite subgroups of* G *and* $N \trianglelefteq G$*, then*

$$|HN| = \frac{|H||N|}{|H \cap N|}.$$

Theorem 3.4.11 (Lattice Isomorphism Theorem)**.** *Let* G *be a group, let* $N \trianglelefteq G$*, and let* $\pi : G \twoheadrightarrow G/N$ *be the canonical projection. There is an order-preserving bijection*

$$\left\{ \begin{array}{c} \textit{subgroups } H \leq G \\ \textit{such that } N \leq H \end{array} \right\} \longleftrightarrow \left\{ \textit{ subgroups of } G/N \right\}$$

given by

$$H \longmapsto H/N \qquad \textit{and} \qquad A \longmapsto \pi^{-1}(A).$$

This correspondence has the following properties:

1. $H \leq K$ *if and only if* $H/N \leq K/N$*.*
2. $H \trianglelefteq G$ *if and only if* $H/N \trianglelefteq G/N$*.*
3. $[G : H] = [G/N : H/N]$*.*
4. *If* $N \leq H, K \leq G$*, then*

$$(H/N) \cap (K/N) = (H \cap K)/N$$

and

$$\langle H/N \cup K/N \rangle = \langle H \cup K \rangle /N.$$

Exercise (3.4.2). Prove the Lattice Isomorphism theorem.

Example 3.4.12. Let $G = \mathbb{Z}$ and let $N = 12\mathbb{Z}$. Since $\mathbb{Z}$ is abelian, $12\mathbb{Z} \trianglelefteq \mathbb{Z}$. The Lattice Isomorphism Theorem says that the subgroups of $\mathbb{Z}$ containing $12\mathbb{Z}$ correspond exactly to the subgroups of $\mathbb{Z}/12\mathbb{Z}$.

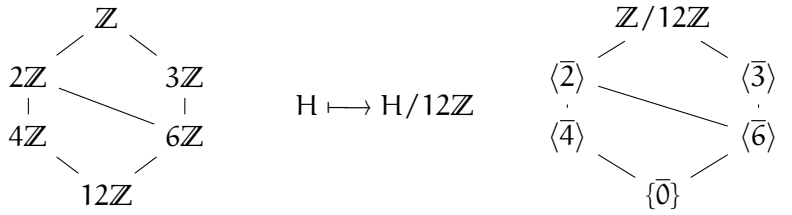
The subgroups of $\mathbb{Z}$ containing $12\mathbb{Z}$ are

$$\mathbb{Z}, \quad 2\mathbb{Z}, \quad 3\mathbb{Z}, \quad 4\mathbb{Z}, \quad 6\mathbb{Z}, \quad 12\mathbb{Z}.$$

Under the correspondence $H \mapsto H/12\mathbb{Z}$, these become the subgroups of $\mathbb{Z}/12\mathbb{Z}$:

$$\mathbb{Z}/12\mathbb{Z}, \quad \langle\overline{2}\rangle, \quad \langle\overline{3}\rangle, \quad \langle\overline{4}\rangle, \quad \langle\overline{6}\rangle, \quad \{\overline{0}\}.$$

The two lattices have exactly the same shape:



subgroups between $12\mathbb{Z}$ and $\mathbb{Z}$ subgroups of $\mathbb{Z}/12\mathbb{Z}$

For example, on the left

$$2\mathbb{Z} \cap 3\mathbb{Z} = 6\mathbb{Z}.$$

On the right, the corresponding statement is

$$\langle\overline{2}\rangle \cap \langle\overline{3}\rangle = \langle\overline{6}\rangle.$$

The theorem says that every inclusion, intersection, and generated subgroup visible in the left lattice is preserved in the quotient lattice.

Of course, the actual subgroup structure of $\mathbb{Z}$ is much much larger than the one shown here – you should think that G/N describes the structure of G "above" the normal subgroup N. ◇

The canonical projection $\pi : G \twoheadrightarrow G/N$ is the basic map out of G that kills every element of N. The next theorem says that any homomorphism out of G that kills N must come from a unique homomorphism out of G/N.

Theorem 3.4.13 (Universal mapping property of quotient groups)**.** *Let G be a group and let $N \trianglelefteq G$. Let $f : G \to H$ be a group homomorphism such that $N \leq \ker f$. Then there exists a unique group homomorphism*

$$\overline{f} : G/N \to H$$

such that the diagram

$$\begin{array}{ccc} G & \xrightarrow{\pi} & G/N \\ & \searrow^{f} & \downarrow{\scriptstyle \overline{f}} \\ & & H \end{array}$$

commutes. Equivalently, $\overline{f}(gN) = f(g)$ *for every* $g \in G$.

Moreover,

$$\operatorname{im}(\overline{f}) = \operatorname{im}(f) \quad \textit{and} \quad \ker(\overline{f}) = \ker(f)/N.$$

Proof. If such a map exists, then it must satisfy

$$\overline{f}(gN) = \overline{f}(\pi(g)) = f(g),$$

so uniqueness is forced.

To prove existence, define

$$\overline{f}(gN) = f(g).$$

We must check that this is well-defined. Suppose $xN = yN$. Then $y^{-1}x \in N \leq \ker f$, so

$$f(y)^{-1}f(x) = f(y^{-1}x) = e_H.$$

Hence $f(x) = f(y)$, so the value of $\overline{f}$ does not depend on the chosen representative.

The map $\overline{f}$ is a homomorphism because

$$\overline{f}((xN)(yN)) = \overline{f}((xy)N) = f(xy) = f(x)f(y) = \overline{f}(xN)\overline{f}(yN).$$

By construction, $\overline{f} \circ \pi = f$.

The image statement follows from the formula $\overline{f}(gN) = f(g)$. Finally,

$$\begin{aligned} gN \in \ker(\overline{f}) &\iff \overline{f}(gN) = e_H \\ &\iff f(g) = e_H \\ &\iff g \in \ker f. \end{aligned}$$

Therefore $\ker(\overline{f}) = \ker(f)/N$. ∎

In short, to define a homomorphism out of G/N, it is enough to define a homomorphism out of G whose kernel contains N.

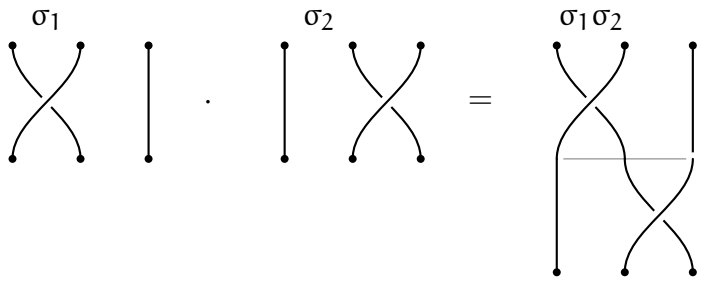
Exercise (3.4.3). The *braid group* B_n is generated by symbols $\sigma_1, \ldots, \sigma_{n-1}$ subject to the relations

$$\sigma_i\sigma_j = \sigma_j\sigma_i \qquad \text{if } |i-j| \geq 2$$

and

$$\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}.$$

The generator σ_i represents the braid where strand i crosses over strand $i+1$. Products of braids are formed by stacking one braid on top of another:



The second displayed relation is a three-strand braid move. It is not the relation $\sigma_i^2 = e$: doing the same crossing twice is usually not the identity braid.

Show that forgetting the crossing information and recording only the final order of the endpoints defines a surjective homomorphism

$$B_n \to S_n \qquad \text{with} \qquad \sigma_i \longmapsto (i\ i+1).$$

Describe the kernel geometrically; it is called the *pure braid group* P_n. Then prove that imposing the additional relations $\sigma_i^2 = e$ on B_n gives the symmetric group S_n.

Exercise (3.4.4). The braid group B_3 can be pictured as the *mapping class group* of a disk with three marked points: its elements record ways to move the marked points around each other, where two motions are considered the same if one can be continuously deformed into the other while keeping the boundary of the disk fixed. The standard generators σ_1 and σ_2 are the positive half-twists interchanging the first two and last two marked points:

$$B_3 = \langle \sigma_1, \sigma_2 \mid \sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2 \rangle.$$

Define

$$\Delta = \sigma_1\sigma_2\sigma_1.$$

Geometrically, Δ is the *half twist* that turns the three marked points halfway around each other; Δ^2 is the *full twist*, where every pair of strands winds once around each other.

1. Show algebraically that $\Delta\sigma_1 = \sigma_2\Delta$ and $\Delta\sigma_2 = \sigma_1\Delta$.

2. Deduce that Δ^2 is central in B_3, and show that

$$\Delta^2 = (\sigma_1\sigma_2)^3.$$

3. Since Δ^2 is central, $\langle \Delta^2 \rangle \trianglelefteq B_3$. In the quotient $B_3/\langle \Delta^2 \rangle$, show that the images of Δ and $\sigma_1\sigma_2$ satisfy

$$\Delta^2 = e \qquad \text{and} \qquad (\sigma_1\sigma_2)^3 = e.$$

4. A theorem from topology says that when the boundary of the disk is capped off by adding a fourth marked point, the full twist becomes invisible. This gives

$$B_3/\langle \Delta^2 \rangle \cong \mathrm{PSL}_2(\mathbb{Z}),$$

which is also the mapping class group of a sphere with four marked points. Explain why this quotient has the flavor of "forgetting the boundary twist."

Exercise (3.4.5). Let G be a group and let A be an abelian group. Show that every group homomorphism

$$f : G \to A$$

factors uniquely through the abelianization $G_{ab} = G/[G, G]$.

Exercise (3.4.6). Prove that if $G/Z(G)$ is cyclic, then G is abelian.

The third isomorphism theorem considers the question of taking quotient groups of quotient groups. In short, they cancel like fractions and we gain no new structural information from taking quotients of a quotient group.

Theorem 3.4.14 (Third Isomorphism Theorem)**.** *Let* G *be a group and suppose*

$$M \leq N \leq G, \qquad M \trianglelefteq G, \qquad N \trianglelefteq G.$$

Then $M \trianglelefteq N$, $N/M \trianglelefteq G/M$, *and there is an isomorphism*

$$(G/M)/(N/M) \cong G/N.$$

Proof. Since $M \trianglelefteq G$, we have $M \trianglelefteq N$. Consider the canonical projection

$$\pi : G \twoheadrightarrow G/N.$$

Since $M \leq N = \ker \pi$, the universal mapping property gives a homomorphism

$$\overline{\pi} : G/M \to G/N, \qquad \overline{\pi}(gM) = gN.$$

This map is surjective, and its kernel is $\ker(\overline{\pi}) = N/M$. Therefore $N/M \trianglelefteq G/M$, and the First Isomorphism Theorem gives

$$(G/M)/(N/M) \cong G/N. \qquad \blacksquare$$

3.5 Composition Series and the Hölder Program

The isomorphism theorems tell us how to understand a group by passing to quotients. Composition series push this idea as far as it can reasonably go: break a group into simple quotient groups, in the same spirit that an integer is broken into prime factors.

Definition 3.5.1. A nontrivial group G is called *simple* if its only normal subgroups are

$$\{e_G\} \qquad \text{and} \qquad G.$$

Simple groups are the groups which cannot be broken down further using normal subgroups and quotients. They are the "atoms" or "prime numbers" of group theory.

Example 3.5.2. If p is prime, then $\mathbb{Z}/p\mathbb{Z}$ is simple. Indeed, its only subgroups are

$$\{\overline{0}\} \qquad \text{and} \qquad \mathbb{Z}/p\mathbb{Z},$$

and every subgroup of an abelian group is normal. ◇

Proposition 3.5.3. *The simple abelian groups are exactly the cyclic groups of prime order.*

Proof. We have already seen that $\mathbb{Z}/p\mathbb{Z}$ is simple when p is prime.

Conversely, let G be a simple abelian group, and choose a nonidentity element $g \in G$. Since G is abelian, every subgroup of G is normal. The subgroup $\langle g \rangle$ is nontrivial, so simplicity forces

$$G = \langle g \rangle.$$

Thus G is cyclic. If G were infinite cyclic, then it would have a proper nontrivial subgroup, for example $\langle g^2 \rangle$. Hence G is finite cyclic. If $|G|$ were composite, then G would have a proper nontrivial subgroup. Therefore $|G|$ is prime. ■

If simple groups are the "primes", we would wish for a "unique factorization theorem" for finite groups. We now describe this program, which was initiated by Hölder in 1889.

Definition 3.5.4. A *composition series* for a group G is a finite chain of subgroups

$$\{e_G\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$$

such that each quotient G_i/G_{i-1} is simple. The simple groups G_i/G_{i-1} are called the *composition factors* of the series.

The notation $G_{i-1} \trianglelefteq G_i$ is important. We do not require every G_i to be normal in all of G; we only require it to be normal in the next group in the chain.

Example 3.5.5. If G is simple, then

$$\{e_G\} \trianglelefteq G$$

is a composition series. Its only composition factor is G itself. ◇

Example 3.5.6. In $\mathbb{Z}/12\mathbb{Z}$, one composition series is

$$\{\overline{0}\} \trianglelefteq \langle\overline{6}\rangle \trianglelefteq \langle\overline{3}\rangle \trianglelefteq \mathbb{Z}/12\mathbb{Z}.$$

The composition factors are

$$\mathbb{Z}/2\mathbb{Z}, \quad \mathbb{Z}/2\mathbb{Z}, \quad \mathbb{Z}/3\mathbb{Z}.$$

Another composition series is

$$\{\overline{0}\} \trianglelefteq \langle\overline{4}\rangle \trianglelefteq \langle\overline{2}\rangle \trianglelefteq \mathbb{Z}/12\mathbb{Z},$$

whose composition factors occur in the order

$$\mathbb{Z}/3\mathbb{Z}, \quad \mathbb{Z}/2\mathbb{Z}, \quad \mathbb{Z}/2\mathbb{Z}.$$

Note: the order changed, but the list of factors did not. ◇

Example 3.5.7. Note that in D_8, we have two composition series

$$1 \trianglelefteq \langle r^2\rangle \trianglelefteq \langle r\rangle \trianglelefteq D_8 \qquad \text{and} \qquad 1 \trianglelefteq \langle s\rangle \trianglelefteq \langle r^2, s\rangle \trianglelefteq D_8.$$

In each series there are three composition factors, each of which is isomorphic to the simple group $\mathbb{Z}/2\mathbb{Z}$. ◇

Proposition 3.5.8. *Every finite group has a composition series.*

Proof. We argue by induction on $|G|$. If G is simple, then $\{e_G\} \trianglelefteq G$ is a composition series. If G is not simple, choose a proper normal subgroup $N \trianglelefteq G$ which is maximal among proper normal subgroups of G. Such an N exists because G is finite. By the Lattice Isomorphism Theorem, the quotient G/N has no nontrivial proper normal subgroups, so G/N is simple.

Since $|N| < |G|$, the induction hypothesis gives a composition series

$$\{e_G\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_k = N$$

for N. Appending G gives

$$\{e_G\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_k = N \trianglelefteq G,$$

and the new final quotient G/N is simple. Therefore this is a composition series for G. ■

Theorem 3.5.9 (Jordan–Hölder theorem)**.** *Let G be a finite group. Any two composition series for G have the same length, and after reordering their factors, the two lists of composition factors are isomorphic term-by-term.*

We will not prove the Jordan–Hölder theorem here. The proof is a refinement argument: one compares two normal chains by cutting each chain with the subgroups in the other chain, then uses the isomorphism theorems to identify the new quotient factors.

Remark 3.5.10. Composition factors behave like prime factors of an integer. A composition series is not unique, just as a factorization can be written in different orders. The Jordan–Hölder theorem says that the simple factors themselves are unique up to reordering.

Remark 3.5.11. The analogy with prime factorization is useful but imperfect. Knowing the composition factors of a group does not determine the group. For example, both

$$\mathbb{Z}/4\mathbb{Z} \qquad \text{and} \qquad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

have two composition factors, both isomorphic to $\mathbb{Z}/2\mathbb{Z}$, but the groups are not isomorphic. Composition factors describe the simple pieces; they do not describe all the ways those pieces can be glued together.

After this, the Hölder program was to:

1. classify all finite simple groups, and
2. find all ways of putting them together to form other groups.

Step (1) was completely in about 1980, 100 years after the program was launched. The efforts of over 100 matehamticians covering about 5000-10000 pages of journal pages over 300-500 individual papers.

Theorem 3.5.12. *There is a list consisting of 18 infinite families of simple groups and 26 simple groups not belonging to this family (the* sporadic groups*) such that every finite simple group is isomorphic to one of the groups in the list.*

Definition 3.5.13. A finite group G is called *solvable* if it has a composition series whose composition factors are all cyclic of prime order.

By the Jordan–Hölder theorem, if one composition series for a finite group has only cyclic prime-order factors, then every composition series does. Thus solvability is a property of the group, not of the chosen composition series.

Example 3.5.14. Every finite abelian group is solvable. Indeed, every composition factor of a finite abelian group is abelian and simple, hence cyclic of prime order. ◇

Remark 3.5.15. The name "solvable" points back to Galois's original goal: understanding when polynomial equations can be solved by radicals.

Very roughly, a polynomial has a group attached to it, called its *Galois group*. This group records the permutations of the roots that preserve all algebraic relations among those roots. For example, the roots of a polynomial may be labeled

$$\alpha_1, \ldots, \alpha_n,$$

and the Galois group is a subgroup of S_n describing which permutations of these roots are compatible with the algebraic structure of the equation.

Solving a polynomial by radicals means building its roots by repeatedly adjoining expressions such as square roots, cube roots, and more generally mth roots. On the group-theoretic side, these radical adjunctions contribute only cyclic prime-order composition factors. Thus Galois theory proves the following fundamental principle:

$$\text{solvable by radicals} \quad \Longrightarrow \quad \text{solvable Galois group.}$$

This turns the existence of radical formulas into a group-theoretic question. The general quintic has Galois group S_5. In the following exercise, you will show that S_5 is not solvable, achieving Galois's goal.

Exercise (3.5.1). A fact that we will not prove A_5 is simple – this is easy, but messy. Using this fact, prove that S_5 is not solvable.

Exercise (3.5.2). Let

$$V = \{e, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}.$$

Prove that

$$\{e\} \trianglelefteq \langle (1\,2)(3\,4)\rangle \trianglelefteq V \trianglelefteq A_4 \trianglelefteq S_4$$

is a composition series, and list its composition factors.

THE CLASSIFICATION OF FINITELY GENERATED ABELIAN GROUPS

For finite abelian groups, composition factors are especially simple: they are all cyclic groups of prime order. The Jordan–Hölder theorem then records the primes that appear, counted with multiplicity. For instance, every abelian group of order 12 has composition factors

$$\mathbb{Z}/2\mathbb{Z}, \quad \mathbb{Z}/2\mathbb{Z}, \quad \mathbb{Z}/3\mathbb{Z}$$

in some order.

But now we need to understand goal (2); how these can be glued together. Fortunately, we know how to do this in this case.

Theorem 3.5.16. *Every finitely generated abelian group is isomorphic to a group of the form*

$$\mathbb{Z}^r \oplus \mathbb{Z}/n_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n_k\mathbb{Z},$$

where $r \geq 0$, *each* $n_i > 1$, *and*

$$n_1 \mid n_2 \mid \cdots \mid n_k.$$

Moreover, the integer r *and the integers* $n_1, \ldots, n_k$ *are uniquely determined by the group.*

Example 3.5.17. What are all the possible finite abelian groups of order 12? The prime factorization is

$$12 = 2^2 \cdot 3^1.$$

The 2-part of the group can be either $\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, and the 3-part of the group is $\mathbb{Z}/3\mathbb{Z}$. Therefore the two possible abelian groups of order 12 are

$$\mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \qquad \text{and} \qquad \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}. \qquad \diamond$$

CHAPTER 4

GROUP ACTIONS

In this chapter we'll consider some of the consequences of an object acting on a set. It is an important and recurring idea in mathematics to study how one object acts on another, and if we have enough time, we'll more fully explore this with representation theory.

4.1 ORBITS AND STABILIZERS

In the first chapter we introduced group actions as a way for a group to act by symmetries or transformations of a set. We now return to them more systematically.

Recall the definition of a group action: A group action of G on a set X (sometimes denoted $G \curvearrowright X$) is a rule that assigns, for every $g \in G$ and $x \in X$ an element $g \cdot x \in X$ so that the identity acts trivially and the action is compatible with the group operation:

$$e \cdot x = x \text{ for all } x \in X \qquad \text{and} \qquad g \cdot (h \cdot x) = (gh) \cdot x \text{ for all } g, h \in G \text{ and } x \in X.$$

We learned that equivalently, it is a homomorphism $\rho : G \to \mathrm{Sym}(X)$ from G to the group of permutations of X, called the *permutation representation* of the action. This was because if you fix g, the map $x \mapsto g \cdot x$ is a bijection of X to itself, and the compatibility condition ensures that ρ is a homomorphism.

Perhaps the first question you should ask about a group action is: where do points go? That is, if I keep applying elements of G to a point $x \in X$, what are all the possible places I can get to? This leads us to the notion of an orbit.

Definition 4.1.1. Let $G \curvearrowright X$ be a group action. The *orbit* of an element $x \in X$ is

$$\mathrm{Orb}_G(x) = \{g \cdot x \mid g \in G\}.$$

We will think of an orbit as an equivalence class: two points $x, y \in X$ are in the same orbit if there is some $g \in G$ such that $g \cdot x = y$. The set of orbits is denoted X/G.

This means that the orbit of an action breaks X apart into orbits, and we can for example, count $|X|$ by counting the number of orbits and the size of each orbit.

Definition 4.1.2. Let $G \curvearrowright X$ be a group action. The *stabilizer* of an element $x \in X$ is the set of group elements that fix x under the action:

$$\mathrm{Stab}_G(x) = \{g \in G \mid g \cdot x = x\}.$$

Example 4.1.3. Let G act on S. An element $s \in S$ is a *fixed point* of the action if $g \cdot s = s$ for every $g \in G$. Equivalently, s is a fixed point if $\mathrm{Orb}_G(s) = \{s\}$, or if $\mathrm{Stab}_G(s) = G$. $\diamond$

So the orbit measures how much the point moves; the stabilizer measures how much symmetry remains after we pin down the point. One important difference is that the orbit is a subset of X, while the stabilizer is a subgroup of G.

Lemma 4.1.4. *Let* G *act on* X*, and let* $x \in X$*. Then* $\mathrm{Stab}_G(x)$ *is a subgroup of* G*.*

Proof. The stabilizer is nonempty because $e_G \cdot x = x$, so $e_G \in \mathrm{Stab}_G(x)$. We use the one-step subgroup test. Suppose $a, b \in \mathrm{Stab}_G(x)$. Since $b \cdot x = x$, note that the inverse b^{-1} also fixes x:

$$b^{-1} \cdot x = b^{-1} \cdot (b \cdot x) = (b^{-1}b) \cdot x = e_G \cdot x = x.$$

Therefore

$$(ab^{-1}) \cdot x = a \cdot (b^{-1} \cdot x) = a \cdot x = x.$$

Thus $ab^{-1} \in \mathrm{Stab}_G(x)$, and hence $\mathrm{Stab}_G(x) \leq G$. ■

The main counting theorem for actions says that the size of an orbit is controlled by the size of a stabilizer. A useful mnemonic is

LOIS = Length of the Orbit Is the index of the Stabilizer.

Theorem 4.1.5 (LOIS)**.** *Let* G *act on a set* X*. For every* $x \in X$*,*

$$|\mathrm{Orb}_G(x)| = [G : \mathrm{Stab}_G(x)].$$

Proof. Let $H = \mathrm{Stab}_G(x)$, and let $\mathcal{L}$ be the set of left cosets of H in G. We'll show that there is a bijection

$$\Phi : \mathcal{L} \to \mathrm{Orb}_G(x), \qquad \Phi(gH) = g \cdot x.$$

We first check that this is well-defined. If $gH = kH$, then $k^{-1}g \in H$, so

$$(k^{-1}g) \cdot x = x.$$

Applying k to both sides gives $g \cdot x = k \cdot x$.

The same calculation also proves injectivity. If $\Phi(gH) = \Phi(kH)$, then $g \cdot x = k \cdot x$. Applying k^{-1} gives

$$(k^{-1}g) \cdot x = x,$$

so $k^{-1}g \in H$, and therefore $gH = kH$.

Finally, Φ is surjective by the definition of the orbit: every element of $\mathrm{Orb}_G(x)$ has the form $g \cdot x$ for some $g \in G$. Thus Φ is a bijection, so the number of elements in the orbit is the number of left cosets of the stabilizer. ■

Exercise (4.1.1). Let G act transitively on a set X, and fix $x \in X$. Let $H = \mathrm{Stab}_G(x)$. Prove that

$$G/H \longrightarrow X, \qquad gH \mapsto g \cdot x$$

is a well-defined bijection that respects the G-actions.

Note that one consequence of LOIS is that for each x in an orbit, the size of the stabilizer is the same. More explicitly, if $y = g \cdot x$, then

$$\mathrm{Stab}_G(y) = \mathrm{Stab}_G(g \cdot x) = g \,\mathrm{Stab}_G(x) g^{-1}.$$

Corollary 4.1.6 (Orbit-Stabilizer Theorem)**.** *Let G be a finite group acting on a set X. For every $x \in X$,*

$$|G| = |\mathrm{Orb}_G(x)| \cdot |\mathrm{Stab}_G(x)|.$$

Proof. By LOIS,

$$|\mathrm{Orb}_G(x)| = [G : \mathrm{Stab}_G(x)].$$

Since G is finite, Lagrange's theorem gives

$$[G : \mathrm{Stab}_G(x)] = \frac{|G|}{|\mathrm{Stab}_G(x)|}.$$

Rearranging gives the result. ∎

Remark 4.1.7. Let G act on a finite set X. Choose one representative $x_1, \ldots, x_m$ from each orbit that has more than one element. Then

$$|X| = |\{x \in X \mid x \text{ is fixed}\}| + \sum_{i=1}^{m} |\mathrm{Orb}_G(x_i)|.$$

Using LOIS, we can also write this as

$$|X| = |\{x \in X \mid x \text{ is fixed}\}| + \sum_{i=1}^{m} [G : \mathrm{Stab}_G(x_i)].$$

This is often called the *orbit formula*. We will use it soon in the special case where a group acts on itself by conjugation.

Exercise (4.1.2). Let S_n act on $\mathbb{C}^n$ by permuting coordinates. For $(a_1, \ldots, a_n) \in \mathbb{C}^n$, define the *elementary symmetric polynomials*

$$\begin{aligned} e_1(a_1, \ldots, a_n) &= a_1 + \cdots + a_n, \\ e_2(a_1, \ldots, a_n) &= \sum_{i<j} a_i a_j, \\ &\vdots \\ e_n(a_1, \ldots, a_n) &= a_1 a_2 \cdots a_n. \end{aligned}$$

Show that $e_1, \ldots, e_n$ are constant on S_n-orbits. Then prove the converse: two points of $\mathbb{C}^n$ have the same values of $e_1, \ldots, e_n$ if and only if they lie in the same S_n-orbit.

Interpret this as saying that the orbit space $\mathbb{C}^n/S_n$ parametrizes monic degree n polynomials by their roots:

$$(a_1, \ldots, a_n) \longmapsto \prod_{i=1}^{n} (t - a_i).$$

There is also a neat way to count the number of orbits of a group action, called Burnside's lemma, though it is more accurately due to Cauchy and Frobenius.

Theorem 4.1.8 (Burnside's lemma)**.** *Let* G *be a finite group acting on a finite set* X*. For* $g \in G$*, let*

$$\mathrm{Fix}(g) = \{x \in X \mid g \cdot x = x\}.$$

be all the fixed points of g*. Then the number of orbits is*

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

Proof. Count the set

$$P = \{(g, x) \in G \times X \mid g \cdot x = x\}$$

enumerating all fixed pairs in two ways. First, if we fix $g \in G$, then the possible x are exactly the elements of $\mathrm{Fix}(g)$. Thus

$$|P| = \sum_{g \in G} |\mathrm{Fix}(g)|.$$

Now count by fixing $x \in X$. The possible g are exactly the elements of $\mathrm{Stab}_G(x)$, so

$$|P| = \sum_{x \in X} |\mathrm{Stab}_G(x)|.$$

Now group the sum by orbits. If O is an orbit and $x \in O$, then every point of O has a stabilizer of the same size as $\mathrm{Stab}_G(x)$. Thus the contribution of this orbit to the sum is

$$|O| \cdot |\mathrm{Stab}_G(x)| = |G|$$

by LOIS. Hence each orbit contributes $|G|$, and since there are $|X/G|$ orbits, we get

$$|P| = |G| \cdot |X/G|.$$

Using the first equality for $|P|$ gives the formula. ∎

Example 4.1.9. How many ways are there to color the vertices of a square black or white, up to rotation? Let $C_4 = \langle r \mid r^4 = 1 \rangle$ act on the set X of all $2^4 = 16$ colorings by rotating the square. The answer will be the number of orbits – since the orbits identify colorings that are equivalent under rotation.

The identity fixes all 16 colorings. The rotations r and r^3 each fix only the two constant colorings. The rotation r^2 fixes the colorings where opposite vertices have the same color, so it fixes $2^2 = 4$ colorings. By Burnside's lemma,

$$|X/C_4| = \frac{1}{4}(16 + 2 + 4 + 2) = 6.$$

Thus there are 6 colorings up to rotation. ◇

Exercise (4.1.3). Use Burnside's lemma to count the number of ways to color the vertices of a regular pentagon with three colors, up to all symmetries of the pentagon.

We can now use these facts to compute with concrete symmetry groups. First, let's get some definitions:

Definition 4.1.10. An action of G on X is *transitive* if there is only one orbit, i.e., for every $x, y \in X$, there is some $g \in G$ such that $g \cdot x = y$.

Definition 4.1.11. An action of G on X is *faithful* if the only group element that fixes every element of X is the identity. Equivalently, the associated homomorphism $\varphi : G \to \mathrm{Sym}(X)$ has trivial kernel.

Exercise (4.1.4). Let

$$O(k) = \{Q \in GL_k(\mathbb{R}) \mid Q^T Q = I\}$$

be the orthogonal group. Let $O(m) \times O(n)$ act on the set $M_{m\times n}(\mathbb{R})$ of real $m \times n$ matrices by

$$(U, V) \cdot A = UAV^T.$$

1. Show that this defines a group action. Why does it correspond to rotating the rows and columns of A?
2. Show that the eigenvalues of $A^T A$, and hence the singular values of A, are constant on orbits.
3. Use singular value decomposition to show that two matrices lie in the same $O(m) \times O(n)$-orbit if and only if they have the same singular values.

Lemma 4.1.12. *Let G act on a set X, and let $\varphi : G \to \mathrm{Sym}(X)$ be the associated permutation representation. Then*

$$\ker(\varphi) = \bigcap_{x \in X} \mathrm{Stab}_G(x).$$

In particular, the action is faithful if and only if

$$\bigcap_{x \in X} \mathrm{Stab}_G(x) = \{e\}.$$

Proof. An element $g \in G$ lies in $\ker(\varphi)$ if and only if g acts trivially on every element of X. This means exactly that

$$g \cdot x = x$$

for every $x \in X$, or equivalently, that $g \in \mathrm{Stab}_G(x)$ for every $x \in X$. ■

Example 4.1.13. Let G be the group of rotational symmetries of a cube. We can count G by imagining that we pick up the cube and put it back in the same place. How many ways are there to do this?

G acts on the six faces of the cube. This action is transitive, because I can pick up the cube and rotate it so that any face is on top. The stabilizer of a face consists of the four rotations by $0, \pi/2, \pi$, and $3\pi/2$ around the axis passing through the center of F and the center of the opposite face. So

$$|G| = |\mathrm{Orb}_G(F)| \cdot |\mathrm{Stab}_G(F)| = 6 \cdot 4 = 24.$$

The cube has four long diagonals joining opposite vertices. Every rotational symmetry permutes these four diagonals, so we get a homomorphism

$$\rho : G \to S_4.$$

We claim this is actually an isomorphism. This action is faithful: a rotational symmetry that fixes all four long diagonals must fix the whole cube. To see this, consider a line $L = \{A, B\}$ joining two opposite vertices A and B. Any $g \in G$ that fixes all four long diagonals must fix L as a set, and thus either fixes both A and B or swaps them. If it fixes A and B, rotating around L fixes the other lines. If it swaps A and B, this is a rotation around another line L and therefore fixes all the lines. Therefore ρ is injective. Since $|G| = 24 = |S_4|$, the map ρ is an isomorphism. Thus the rotational symmetry group of the cube is isomorphic to S_4. ◇

Example 4.1.14. Let Y be a regular dodecahedron centered at the origin in $\mathbb{R}^3$, and let G be the group of orientation-preserving isometries of $\mathbb{R}^3$ that send Y to itself:

$$G = \{\alpha : \mathbb{R}^3 \to \mathbb{R}^3 \mid \alpha \text{ is an isometry, } \alpha \text{ preserves orientation, and } \alpha(Y) = Y\}.$$

The group G acts on the set of 12 faces of Y. This action is transitive, since any face can be rotated to any other face. If F is a face, then

$$|\mathrm{Orb}_G(F)| = 12.$$

The stabilizer of F consists of the five rotations around the axis through the center of F and the center of the opposite face:

$$0, \frac{2\pi}{5}, \frac{4\pi}{5}, \frac{6\pi}{5}, \frac{8\pi}{5}.$$

Therefore $|\mathrm{Stab}_G(F)| = 5$, and the Orbit-Stabilizer Theorem gives

$$|G| = |\mathrm{Orb}_G(F)| \cdot |\mathrm{Stab}_G(F)| = 12 \cdot 5 = 60.$$ ◇

4.2 THE CLASS EQUATION

The main goal of this section is to apply the Orbit-Stabilizer Theorem to the action of a group on itself by conjugation. Recall that every group G acts on itself by

$$g \cdot x = gxg^{-1}.$$

Definition 4.2.1. Let G be a group. Two elements $g, g' \in G$ are *conjugate* if there exists $h \in G$ such that

$$g' = hgh^{-1}.$$

The *conjugacy class* of $g \in G$ is

$$[g]_c = \{hgh^{-1} \mid h \in G\}.$$

Thus the conjugacy class of g is exactly the orbit of g under conjugation.

Remark 4.2.2. For any group G, we have

$$geg^{-1} = e$$

for every $g \in G$. Therefore $[e]_c = \{e\}$.

Let us first understand conjugacy classes in symmetric groups. Remember that in symmetric groups, every permutation factors uniquely into a product of disjoint cycles. The key fact is that conjugation relabels cycles.

Lemma 4.2.3. *Let $\sigma \in S_n$, and let $i_1, \ldots, i_k$ be distinct elements of $\{1, \ldots, n\}$. Then*

$$\sigma(i_1\, i_2 \cdots i_k)\sigma^{-1} = (\sigma(i_1)\, \sigma(i_2) \cdots \sigma(i_k)).$$

Proof. Let $\tau = (i_1\, i_2 \cdots i_k)$. If $1 \leq j < k$, then

$$\sigma\tau\sigma^{-1}(\sigma(i_j)) = \sigma\tau(i_j) = \sigma(i_{j+1}).$$

Similarly, $\sigma\tau\sigma^{-1}(\sigma(i_k)) = \sigma(i_1)$. If a is not one of the elements $\sigma(i_1), \ldots, \sigma(i_k)$, then $\sigma^{-1}(a)$ is not one of $i_1, \ldots, i_k$, so τ fixes $\sigma^{-1}(a)$ and hence $\sigma\tau\sigma^{-1}$ fixes a. Therefore $\sigma\tau\sigma^{-1}$ is the cycle $(\sigma(i_1)\, \sigma(i_2) \cdots \sigma(i_k))$. ∎

Definition 4.2.4. The *cycle type* of a permutation is the list of lengths of the cycles in its disjoint cycle decomposition, ignoring cycles of length 1.

Theorem 4.2.5. *Two elements of S_n are conjugate if and only if they have the same cycle type.*

Proof. Suppose $\alpha, \beta \in S_n$ are conjugate, say $\beta = \sigma\alpha\sigma^{-1}$. Write α as a product of disjoint cycles:

$$\alpha = \alpha_1 \alpha_2 \cdots \alpha_m.$$

Then

$$\beta = \sigma\alpha\sigma^{-1} = (\sigma\alpha_1\sigma^{-1})(\sigma\alpha_2\sigma^{-1})\cdots(\sigma\alpha_m\sigma^{-1}).$$

By Lemma 4.2.3, each $\sigma\alpha_i\sigma^{-1}$ is a cycle of the same length as α_i. These cycles are still disjoint, because σ is a bijection. Hence α and β have the same cycle type.

Conversely, suppose α and β have the same cycle type. Write

$$\alpha = \alpha_1 \cdots \alpha_m \qquad \text{and} \qquad \beta = \beta_1 \cdots \beta_m,$$

where, after reordering if necessary, α_j and β_j have the same length for every j.

If

$$\alpha_j = (i_{j,1}\, i_{j,2} \cdots i_{j,k_j}) \qquad \text{and} \qquad \beta_j = (\ell_{j,1}\, \ell_{j,2} \cdots \ell_{j,k_j}),$$

choose a permutation $\sigma \in S_n$ such that

$$\sigma(i_{j,t}) = \ell_{j,t}$$

for all j and t. This can be done because the cycles in the two decompositions are disjoint and have matching lengths; define σ arbitrarily on any remaining fixed points. Then Lemma 4.2.3 gives

$$\sigma\alpha_j\sigma^{-1} = \beta_j$$

for every j, so $\sigma\alpha\sigma^{-1} = \beta$. Thus α and β are conjugate. ■

Example 4.2.6. The conjugacy classes of S_4 are determined by cycle type:

- the identity class $\{e\}$;
- the class of $(1\,2)$, consisting of all transpositions, with $\binom{4}{2} = 6$ elements;
- the class of $(1\,2\,3)$, consisting of all 3-cycles, with $4 \cdot 2 = 8$ elements;
- the class of $(1\,2\,3\,4)$, consisting of all 4-cycles, with $3! = 6$ elements;
- the class of $(1\,2)(3\,4)$, consisting of products of two disjoint transpositions, with 3 elements.

The sizes add to

$$1 + 6 + 8 + 6 + 3 = 24 = |S_4|.$$ ◇

Example 4.2.7. The conjugacy classes of S_5 are:

- the identity class $\{e\}$;
- the class of $(1\,2)$, consisting of all transpositions, with $\binom{5}{2} = 10$ elements;
- the class of $(1\,2\,3)$, consisting of all 3-cycles, with $\binom{5}{3} \cdot 2! = 20$ elements;

- the class of $(1\,2\,3\,4)$, consisting of all 4-cycles, with $5 \cdot 3! = 30$ elements;
- the class of $(1\,2\,3\,4\,5)$, consisting of all 5-cycles, with $4! = 24$ elements;
- the class of $(1\,2)(3\,4)$, consisting of products of two disjoint transpositions, with $5 \cdot 3 = 15$ elements;
- the class of $(1\,2)(3\,4\,5)$, consisting of products of a transposition and a disjoint 3-cycle, with $\binom{5}{2} \cdot 2! = 20$ elements.

Again, the sizes add to

$$1 + 10 + 20 + 30 + 24 + 15 + 20 = 120 = |S_5|. \qquad \diamond$$

Remark 4.2.8. If G is a nontrivial group, then no conjugacy class is all of G. Indeed, $[e]_c = \{e\}$, and the conjugacy classes partition G.

Definition 4.2.9. Let G be a group and let $S \subseteq G$. The *centralizer* of S in G is

$$C_G(S) = \{x \in G \mid xs = sx \text{ for all } s \in S\}.$$

If $S = \{a\}$, we write $C_G(a)$ instead of $C_G(\{a\})$.

Definition 4.2.10. Let G be a group and let $S \subseteq G$. The *normalizer* of S in G is

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

Exercise (4.2.1). Let G be a group and let $S \subseteq G$. Prove that $C_G(S)$ and $N_G(S)$ are subgroups of G.

Lemma 4.2.11. *Let* $S \subseteq G$. *Then* $C_G(S) \leq N_G(S)$.

Proof. Let $x \in C_G(S)$. For every $s \in S$, we have $xs = sx$, so

$$xsx^{-1} = s \qquad \text{and} \qquad x^{-1}sx = s.$$

Therefore $xSx^{-1} \subseteq S$ and $x^{-1}Sx \subseteq S$. To prove the reverse containment, let $s \in S$. Since $x^{-1}sx \in S$, we can write

$$s = x(x^{-1}sx)x^{-1} \in xSx^{-1}.$$

Hence $S \subseteq xSx^{-1}$, so $xSx^{-1} = S$. Thus $x \in N_G(S)$. ■

Remark 4.2.12. If G is abelian, then $C_G(S) = G = N_G(S)$ for every subset $S \subseteq G$.

Exercise (4.2.2). Let $H \leq G$, and let $S \subseteq H$. Prove that

$$C_H(S) = C_G(S) \cap H \qquad \text{and} \qquad N_H(S) = N_G(S) \cap H.$$

Exercise (4.2.3). Let G be a group and let $H \leq G$.

1. Prove that $N_G(H)/C_G(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$.
2. Deduce that if $H \trianglelefteq G$, then $C_G(H) \trianglelefteq G$, and $G/C_G(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$.

Lemma 4.2.13. *Let G act on itself by conjugation. For every $g \in G$,*

$$\mathrm{Orb}_G(g) = [g]_c, \qquad \mathrm{Stab}_G(g) = C_G(g), \qquad |[g]_c| = [G : C_G(g)].$$

Proof. The first equality is the definition of the conjugacy class. For the stabilizer,

$$h \in \mathrm{Stab}_G(g) \iff hgh^{-1} = g \iff hg = gh \iff h \in C_G(g).$$

The final equality follows from Theorem 4.1.5. ■

Corollary 4.2.14. *If G is finite, then the size of every conjugacy class divides $|G|$.*

Proof. By Lemma 4.2.13, a conjugacy class is an orbit. By the Orbit-Stabilizer Theorem, the size of the orbit always divides the size of the group. ■

Exercise (4.2.4). Let G be a finite group. The *commuting probability* of G is the probability that two randomly chosen elements of G commute:

$$\mathrm{cp}(G) = \frac{|\{(x,y) \in G \times G \mid xy = yx\}|}{|G|^2}.$$

If $k(G)$ is the number of conjugacy classes of G, prove that

$$\mathrm{cp}(G) = \frac{k(G)}{|G|}.$$

Compute $\mathrm{cp}(S_3)$ and $\mathrm{cp}(D_4)$.

We now apply the orbit formula to the conjugation action. First we identify the fixed points.

Lemma 4.2.15. *Let G act on itself by conjugation. An element $g \in G$ is a fixed point of this action if and only if $g \in Z(G)$.*

Proof. Suppose $g \in Z(G)$. Then g commutes with every $h \in G$, so

$$hgh^{-1} = (hg)h^{-1} = g(hh^{-1}) = g.$$

Thus g is fixed by every element of G under conjugation.

Conversely, suppose g is fixed by every element of G under conjugation. Then for every $h \in G$,

$$hgh^{-1} = g.$$

Multiplying on the right by h gives $hg = gh$. Hence $g \in Z(G)$. ■

Theorem 4.2.16 (The Class Equation)**.** *Let* G *be a finite group. For each conjugacy class of size greater than* 1*, choose exactly one representative, and call the resulting list* $g_1, \ldots, g_r$*. Then*

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

Proof. The conjugacy classes are the orbits of the conjugation action. By Lemma 4.2.15, the fixed points of this action are exactly the elements of $Z(G)$.

Theorem 4.1.5 gives

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

For each chosen representative g_i, Lemma 4.2.13 gives

$$|[g_i]_c| = [G : C_G(g_i)].$$

Substituting these equalities into the orbit formula proves the class equation. ■

Remark 4.2.17. If G is abelian, then $Z(G) = G$, so the class equation is not saying much: there are no conjugacy classes of size greater than 1. The theorem becomes most useful when G is nonabelian, because it forces noncentral conjugacy classes to account for the part of G outside the center.

Exercise (4.2.5). Prove that if G is a nonabelian group of order 21, then there is only one possible class equation for G, up to reordering the noncentral conjugacy-class sizes.

Exercise (4.2.6). Let p be prime, and let G be a finite group of order p^m for some $m > 0$. Show $Z(G)$ is not the trivial group.

Lemma 4.2.18. *Let* G *be a group and let* $N \trianglelefteq G$*. The conjugation action of* G *on itself restricts to an action of* G *on* N*. In particular,* N *is a disjoint union of conjugacy classes of* G*.*

Proof. Define $g \cdot n = gng^{-1}$ for $g \in G$ and $n \in N$. Since N is normal in G, the element gng^{-1} lies in N, so this rule is well-defined as an action on N. The action axioms are inherited from the conjugation action of G on itself.

The orbit of an element $n \in N$ under this restricted action is

$$\{gng^{-1} \mid g \in G\} = [n]_c,$$

its conjugacy class in G. The orbits of an action partition the set being acted on, so N is a disjoint union of conjugacy classes of G. ■

Remark 4.2.19. Lemma 4.2.18 says that if $N \trianglelefteq G$, then every conjugacy class of G that touches N is completely contained in N.

This should not be confused with the conjugation action of N on itself. If two elements of N are conjugate by an element of N, then they are certainly conjugate by an element of G. The converse need not hold: two elements of N might be conjugate in G only by elements outside of N.

Exercise (4.2.7). Using the conjugacy classes of S_4, prove that the only normal subgroups of S_4 are

$$\{e\}, \qquad V = \{e, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}, \qquad A_4, \qquad S_4.$$

4.3 Other Group Actions with Applications

The action on left cosets

Let G be a group and let $H \leq G$. Let $\mathcal{L}$ be the set of left cosets of H in G:

$$\mathcal{L} = \{xH \mid x \in G\}.$$

When H is normal, this is the quotient group G/H. Here we do not assume that H is normal; we are only using $\mathcal{L}$ as a set.

The group G acts on $\mathcal{L}$ by left multiplication. This action is transitive, since every coset is obtained from H by $x \cdot H$. The stabilizer of the coset H is

$$\mathrm{Stab}_G(H) = \{g \in G \mid gH = H\} = H.$$

This is consistent with LOIS:

$$|\mathrm{Orb}_G(H)| = |\mathcal{L}| = [G : H], \qquad [G : \mathrm{Stab}_G(H)] = [G : H].$$

The associated permutation representation is

$$\varphi : G \to \mathrm{Sym}(\mathcal{L}), \qquad \varphi(g)(xH) = (gx)H.$$

If $[G : H] = n < \infty$, then after choosing a bijection $\mathcal{L} \cong \{1, \ldots, n\}$, we may view this as a homomorphism $\varphi : G \to S_n$.

Lemma 4.3.1. *Let G be a group and let $H \leq G$. Consider the action of G on the set $\mathcal{L}$ of left cosets of H, and let $\varphi : G \to \mathrm{Sym}(\mathcal{L})$ be the corresponding permutation representation. Then*

$$\ker(\varphi) = \bigcap_{x \in G} xHx^{-1}.$$

In particular, $\ker(\varphi) \leq H$.

Proof. An element $g \in G$ lies in $\ker(\varphi)$ if and only if it fixes every left coset of H. Thus

$$\begin{aligned} g \in \ker(\varphi) &\iff (gx)H = xH \text{ for every } x \in G \\ &\iff x^{-1}gx \in H \text{ for every } x \in G \\ &\iff g \in xHx^{-1} \text{ for every } x \in G \\ &\iff g \in \bigcap_{x \in G} xHx^{-1}. \end{aligned}$$

Taking $x = e$ shows that this intersection is contained in H. ∎

The subgroup

$$\bigcap_{x \in G} xHx^{-1}$$

is the largest normal subgroup of G contained in H. It is often called the *core* of H in G.

Remark 4.3.2. The action of G on the left cosets of H may or may not be faithful. By Lemma 4.3.1, it is faithful if and only if

$$\bigcap_{x \in G} xHx^{-1} = \{e\}.$$

If $H \trianglelefteq G$, then $xHx^{-1} = H$ for all $x \in G$, so the kernel is H. Thus, for normal H, this action is faithful if and only if $H = \{e\}$.

Example 4.3.3. Let $G = S_3$ and let $H = \langle (1\,2) \rangle$. The action of S_3 on the left cosets of H is faithful. Indeed, if $\omega = (1\,3)$, then

$$\omega H \omega^{-1} = \{e, (2\,3)\}.$$

Hence

$$H \cap \omega H \omega^{-1} = \{e\}.$$

By Lemma 4.3.1, the kernel of the coset action is contained in this intersection, so the kernel is trivial. ◇

Theorem 4.3.4. *Let G be a finite group, and let $H \leq G$ have index p, where p is the smallest prime divisor of $|G|$. Then $H \trianglelefteq G$.*

Proof. Let $\mathcal{L}$ be the set of left cosets of H in G. Since $[G : H] = p$, the action of G on $\mathcal{L}$ gives a homomorphism $\varphi : G \to S_p$. Let $N = \ker(\varphi)$. By Lemma 4.3.1, we have $N \leq H$.

By the First Isomorphism Theorem,

$$[G : N] = |G/N| = |\operatorname{im}(\varphi)|.$$

Since $\operatorname{im}(\varphi) \leq S_p$, Lagrange's theorem implies that $[G : N]$ divides $p!$. Also $[G : N]$ divides $|G|$. Therefore $[G : N]$ divides $\gcd(|G|, p!)$. Because p is the smallest prime divisor of $|G|$, this greatest common divisor is p. Hence

$$[G : N] = 1 \qquad \text{or} \qquad [G : N] = p.$$

The first option is impossible because $N \leq H < G$. Thus $[G : N] = p$. Since $N \leq H$ and $[G : H] = p$, we must have $N = H$. Therefore $H = \ker(\varphi)$, so H is normal in G. ■

This generalizes the earlier exercise that every subgroup of index 2 is normal.

THE ACTION ON SUBGROUPS BY CONJUGATION

Another useful action comes from conjugating subgroups. If $H \leq G$ and $g \in G$, then

$$gHg^{-1} = \{ghg^{-1} \mid h \in H\}$$

is again a subgroup of G, and the map $H \to gHg^{-1}$ given by $h \mapsto ghg^{-1}$ is a bijection. Thus conjugate subgroups have the same cardinality. In particular, if H is the unique subgroup of G of order $|H|$, then $gHg^{-1} = H$ for every $g \in G$, so $H \trianglelefteq G$.

Let

$$\mathcal{S}(G) = \{H \mid H \leq G\}$$

be the set of all subgroups of G. Then G acts on $\mathcal{S}(G)$ by

$$g \cdot H = gHg^{-1}.$$

Definition 4.3.5. Two subgroups A and B of a group G are *conjugate* if there exists $g \in G$ such that

$$A = gBg^{-1}.$$

Equivalently, two subgroups are conjugate if they lie in the same orbit for the action of G on $\mathcal{S}(G)$ by conjugation.

Lemma 4.3.6. *Let G be a group and let $H \leq G$. The number of subgroups of G conjugate to H is $[G : N_G(H)]$.*

Proof. The subgroups conjugate to H are exactly the elements in the orbit of H under the conjugation action of G on $\mathcal{S}(G)$. The stabilizer of H under this action is

$$\{g \in G \mid gHg^{-1} = H\} = N_G(H).$$

By LOIS, the size of the orbit is $[G : N_G(H)]$. ∎

The normalizer $N_G(H)$ is the largest subgroup of G in which H is normal. Indeed, $H \trianglelefteq N_G(H)$, and if $H \trianglelefteq K \leq G$, then every element of K normalizes H, so $K \leq N_G(H)$. In particular,

$$H \trianglelefteq G \qquad \text{if and only if} \qquad N_G(H) = G.$$

These actions on cosets and subgroups both turn group-theoretic structure into permutation representations. In the next chapter we linearize this idea: an action on a finite set gives a representation by letting G permute basis vectors.

CHAPTER 5

REPRESENTATION THEORY

Representation theory is a way of studying groups by letting them act on vector spaces. The point is that linear algebra gives us tools that are very concrete: matrices, eigenvalues, traces, dimensions, and decompositions.

In this chapter we follow the beginning of Serre's *Linear Representations of Finite Groups*. We will work with finite groups and finite-dimensional complex vector spaces. This is already a rich setting, and it is the setting where the basic structure theorems have their cleanest form.

5.1 DEFINITIONS AND EXAMPLES

Let G be a group and let V be a finite-dimensional vector space over $\mathbb{C}$.

Definition 5.1.1. A (complex) *representation* of G in V is a group homomorphism

$$\rho : G \to \mathrm{GL}(V).$$

As a reminder, $\mathrm{GL}(V)$ is the group of linear automorphisms of V called the *general linear group*, or if $\dim V = d$, the group of invertible $d \times d$ matrices.

In other words, a representation of G is a pair (V, ρ), which associates to each element $g \in G$ an invertible linear map $\rho(g)$ in such a way that

$$\rho(gt) = \rho(g)\rho(t) \quad \text{for } g, t \in G.$$

After choosing a basis of V, each $\rho(g)$ becomes an invertible matrix. In this way, we are trying to *represent* the abstract group G by matrices. Most people will abuse notation supress ρ from the notation when its understood, and say that V is a representation of G.

Example 5.1.2. Let V be any finite-dimensional complex vector space. The rule $\rho(g) = I_V$ for every $g \in G$ defines a representation of G. This is called the *trivial representation*. ◇

Example 5.1.3. Suppose $\dim V = 1$. In this case, a representation is a map

$$\rho : G \to \mathbb{C}^\times.$$

Since G is finite, every element $g \in G$ has finite order. If $g^n = e_G$, then

$$\rho(g)^n = \rho(g^n) = \rho(e_G) = 1.$$

Thus $\rho(g)$ is a root of unity for every $g \in G$. ◇

Exercise (5.1.1). This exercise will complete a classification of one-dimensional representations of a finite group G.

1. Show that ρ uniquely factors through the abelianization $G^{ab} = G/[G, G]$. (Hint: look at previous exercises...)
2. Show that if G is a cyclic group, then the one-dimensional representations of G are in bijection with the n-th roots of unity, where $n = |G|$.
3. Use the classification of finite abelian groups to describe all one-dimensional representations of G.

Example 5.1.4. The *sign representation* of S_n is the one-dimensional representation

$$\operatorname{sgn} : S_n \to \{\pm 1\} \subseteq \mathbb{C}^\times.$$

Even permutations act by multiplication by 1, and odd permutations act by multiplication by -1. This is a representation because if you multiply two even permutations, you get an even permutation, and if you multiply two odd permutations, you get an even permutation. If you multiply an even and an odd permutation, you get an odd permutation. In all cases, the sign of the product is the product of the signs. ◇

Example 5.1.5. Recall that S_n acts naturally on the set $X = \{1, 2, \ldots, n\}$ by permutating the elements. There is an extremely natural representation here on the n-dimensional vector space $\mathbb{C}^n$. Let $e_1, \ldots, e_n$ be the standard basis of $\mathbb{C}^n$, one for each element in X. For each permutation $\sigma \in S_n$, define

$$\rho(\sigma)(e_i) = e_{\sigma(i)}.$$

So for example, if $n = 3$ and $\sigma = (1\,2\,3)$, then

$$\rho(\sigma) = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}.$$

We call this the *permutation representation* associated with $S_n \curvearrowright X$. ◇

Example 5.1.5 extends to a general construction for *any* group action $G \curvearrowright X$ on a finite set X.

Definition 5.1.6. Let V be the complex vector space with basis $(e_x)_{x\in X}$. For each $g \in G$, define the *permutation representation* of $G \curvearrowright X$ by

$$\rho(g)(e_x) = e_{g\cdot x} \qquad \text{for all } g \in G,\ x \in X.$$

Since the action satisfies $g(tx) = (gt)x$, the maps $\rho(g)$ satisfy $\rho(gt) = \rho(g)\rho(t)$.

Recall that every finite group G acts on itself by left multiplication. This gives a permutation representation of G on a vector space of dimension $|G|$ with basis $(e_g)_{g\in G}$. This is called the *regular representation* of G.

Example 5.1.7. If $G = S_3$, then the regular representation is 6-dimensional, with one basis vector for each permutation in S_3. Order the basis as

$$e_{\mathrm{id}},\ e_{(1\,2)},\ e_{(1\,3)},\ e_{(2\,3)},\ e_{(1\,2\,3)},\ e_{(1\,3\,2)}.$$

In this basis, the matrix for $\rho((1\,2\,3))$ is

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}. \qquad \diamond$$

Example 5.1.8. If $G = \mathbb{Z}/3\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}\}$, then the regular representation of G is a representation in a three-dimensional vector space with basis $e_{\overline{0}}, e_{\overline{1}}, e_{\overline{2}}$, and the group elements act as follows:

$$\begin{aligned} &\rho(\overline{0})(e_{\overline{0}}) = e_{\overline{0}}, && \rho(\overline{0})(e_{\overline{1}}) = e_{\overline{1}}, && \rho(\overline{0})(e_{\overline{2}}) = e_{\overline{2}}, \\ &\rho(\overline{1})(e_{\overline{0}}) = e_{\overline{1}}, && \rho(\overline{1})(e_{\overline{1}}) = e_{\overline{2}}, && \rho(\overline{1})(e_{\overline{2}}) = e_{\overline{0}}, \\ &\rho(\overline{2})(e_{\overline{0}}) = e_{\overline{2}}, && \rho(\overline{2})(e_{\overline{1}}) = e_{\overline{0}}, && \rho(\overline{2})(e_{\overline{2}}) = e_{\overline{1}}. \end{aligned}$$

So as a matrix, $\rho(\overline{1})$ is the matrix

$$\begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}.$$

Note that this is the same matrix as the natural permutation representation of $(1\,2\,3) \in S_3$, after identifying $\overline{0}, \overline{1}, \overline{2}$ with $1, 2, 3$. $\diamond$

Exercise (5.1.2). Let G be a finite group. The *group algebra* $\mathbb{C}[G]$ is the complex vector space with basis $(e_g)_{g\in G}$. Define multiplication on basis vectors by

$$e_g e_h = e_{gh}$$

and extend this rule bilinearly, so that

$$\left(\sum_{g\in G} a_g e_g\right)\left(\sum_{h\in G} b_h e_h\right) = \sum_{g,h\in G} a_g b_h e_{gh}.$$

1. Show that this multiplication is associative and has identity element e_{e_G}.

2. Show that $\mathbb{C}[G]$ is commutative if and only if G is abelian.

3. For each $s \in G$, left multiplication by e_s sends e_g to e_{sg}. Explain why this recovers the regular representation described above.

As usual, we have a notion for when objects are the isomorphic to each other. As usual, it means that there is a homomorphism that respects the structure of the objects.

Definition 5.1.9. Two representations (V, ρ) and (W, τ) of G are called *isomorphic* if there is an isomorphism of vector spaces $f : V \to W$ such that

$$\tau(g) \circ f = f \circ \rho(g)$$

for all $g \in G$. In other words, the following diagram commutes for all $g \in G$:

$$\begin{array}{ccc} V & \xrightarrow{\rho(g)} & V \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f} \\ W & \xrightarrow{\tau(g)} & W \end{array}$$

People call such a map f a G-equivariant linear map. More generally, a homomorphism from one G-representation to another is a homomorphism respecting the G-action in the same way.

Isomorphic representations are the same representation written in different coordinates. If bases are chosen for V and W, then the condition above says that the matrices for one representation are obtained from the matrices for the other by a single change of basis.

Remark 5.1.10. There is a pattern here that appears throughout modern mathematics. Once we decide what kinds of objects we want to study, we also have to decide what the structure-preserving maps between them should be. For representations of G, the objects are representations, and the structure-preserving maps are G-equivariant linear maps. The isomorphisms are exactly the invertible G-equivariant linear maps. The subject that studies this general pattern of objects and morphisms is called category theory.

5.2 SUBREPRESENTATIONS AND IRREDUCIBILITY

A representation is a vector space together with a compatible action of G. Therefore the right analogue of a subgroup is not just a subset, but a linear subspace that is preserved by the action.

Definition 5.2.1. Let (V, ρ) be a representation of G. A subspace $W \subseteq V$ is called a *subrepresentation* if

$$\rho(g)(W) \subseteq W$$

for every $g \in G$. Sometimes we call W G-*stable* or *invariant* under G.

This is what is needed in order for the restriction

$$\rho_W(g) = \rho(g)|_W : W \to W$$

defines a representation of G on W. Since $\rho(g)$ is invertible, the condition $\rho(g)(W) \subseteq W$ is equivalent to $\rho(g)(W) = W$ for every $g \in G$.

Example 5.2.2. Let G act on a finite set X, and let V be the associated permutation representation with basis $(e_x)_{x \in X}$. The vector

$$u = \sum_{x \in X} e_x$$

is fixed by every element of G, because each $s \in G$ only permutes the basis vectors. Therefore the line $\mathbb{C}u$ is a subrepresentation, and G acts trivially on it. ◇

Lemma 5.2.3. *Let $f : V \to W$ be a G-equivariant linear map between representations of G. Then $\ker(f)$ is a subrepresentation of V, and $\operatorname{im}(f)$ is a subrepresentation of W.*

Proof. Let $v \in \ker(f)$, so $f(v) = 0$. Then for any $g \in G$,

$$f(\rho(g)(v)) = \tau(g)(f(v)) = \tau(g)(0) = 0,$$

so $\rho(g)(v) \in \ker(f)$. Therefore $\ker(f)$ is a subrepresentation of V.

Let $w \in \operatorname{im}(f)$, so $w = f(v)$ for some $v \in V$. Then for any $g \in G$,

$$\tau(g)(w) = \tau(g)(f(v)) = f(\rho(g)(v)) \in \operatorname{im}(f),$$

so $\operatorname{im}(f)$ is a subrepresentation of W. ■

Example 5.2.4. Every representation V has two automatic subrepresentations:

$$0 \qquad \text{and} \qquad V.$$

These are called the trivial subrepresentations. ◇

Definition 5.2.5. A nonzero representation V of G is called *irreducible* if its only subrepresentations are 0 and V.

Later, Maschke's theorem will tell us that every finite-dimensional complex representation of a finite group can be built as a direct sum of irreducible representations. Irreducible representations are therefore the basic building blocks of representation theory. They are the "simple groups" of representation theory.

Example 5.2.6. Every one-dimensional representation is irreducible. Indeed, a one-dimensional vector space has only two subspaces: 0 and the whole space. ◇

Example 5.2.7. If G is nontrivial, then the regular representation of G is not irreducible. The line

$$\mathbb{C}\left(\sum_{t\in G} e_t\right)$$

is a one-dimensional subrepresentation, and it is not the whole regular representation because $\dim V = |G| > 1$. ◇

Proposition 5.2.8. *All irreducible representations of $\mathbb{Z}/n\mathbb{Z}$ are one-dimensional.*

Proof. Let γ be a generator for $\mathbb{Z}/n\mathbb{Z}$, and let V be an irreducible representation. Let v be an eigenvector for γ, so $\gamma v = \lambda v$. Consider the complex line $\mathbb{C}v$; it is preserved by γ and by all of its powers and thus $\mathbb{C}v$ is preserved by every group element. Therefore its a subrepresentation of V and must be irreducible since its 1-dimensional. ■

There are also multiple ways to create representations from existing ones. The most basic is to take their direct sum.

Definition 5.2.9. Let V_1 and V_2 be representations of G. Their *direct sum representation* is the representation on $V_1 \oplus V_2$ defined by

$$s(v_1, v_2) = (sv_1, sv_2)$$

for every $s \in G$, $v_1 \in V_1$, and $v_2 \in V_2$.

Example 5.2.10. Let us return to the natural action of S_n on the set $\{1, \ldots, n\}$. The corresponding permutation representation is the representation on $\mathbb{C}^n$ with standard basis $e_1, \ldots, e_n$ given by

$$\rho(\sigma)(e_i) = e_{\sigma(i)}.$$

There is a one-dimensional subspace

$$L = \operatorname{span}\{e_1 + \cdots + e_n\}$$

on which every permutation acts trivially. There is also an $(n-1)$-dimensional subspace

$$W = \{a_1 e_1 + \cdots + a_n e_n \mid a_1 + \cdots + a_n = 0\}.$$

This subspace is preserved by every permutation, and the resulting representation on W is called the *standard representation* of S_n.

In fact,

$$\mathbb{C}^n = L \oplus W.$$

To see this, write $v = a_1 e_1 + \cdots + a_n e_n$ and let

$$\overline{a} = \frac{a_1 + \cdots + a_n}{n}.$$

Then

$$v = \overline{a}(e_1 + \cdots + e_n) + \sum_{i=1}^{n} (a_i - \overline{a}) e_i,$$

where the first term lies in L and the second lies in W. ◇

Exercise (5.2.1). This exercise shows that for $n \geq 2$, the standard representation of S_n is irreducible. Suppose U is a nonzero subrepresentation of the standard representation

1. Let $v = a_1 e_1 + \cdots a_n e_n$ be a nonzero vector in U. Show that there must be i, j such that $a_i \neq a_j$.

2. Show that the transposition $\tau = (i\,j)$ satisfies $v - \tau v \in U$. Conclude that $e_p - e_q \in U$ for any $p \neq q$.

3. Show that the vectors $e_p - e_q$ for $p \neq q$ span the standard representation. Conclude that U is the whole standard representation.

5.3 Schur's Lemma and Maschke's Theorem

We now prove the first structural theorems about finite-dimensional complex representations. Maschke's theorem says that every representation can be broken apart into irreducible pieces. Schur's lemma says that maps between irreducible representations are very rigid.

More precisely, Maschke's theorem says that over $\mathbb{C}$, every finite-dimensional representation is assembled from irreducible ones by direct sums. The key point is that every subrepresentation has an invariant complement.

Lemma 5.3.1 (Invariant complements)**.** *Let V be a finite-dimensional complex representation of a finite group G, and let $W \subseteq V$ be a subrepresentation. Then there is a subrepresentation $W' \subseteq V$ such that*

$$V = W \oplus W'.$$

Proof. Start by choosing any linear complement U to W, so that $V = W \oplus U$ as vector spaces. Equivalently, choose a linear projection $p : V \to W$ onto W – this chooses a complement $U = \ker(p)$.

The projection p does not have to respect the G-action. We fix this by averaging it over the group. Define

$$P(v) = \frac{1}{|G|} \sum_{s \in G} s\, p(s^{-1}v).$$

Since W is a subrepresentation, each term $s\, p(s^{-1}v)$ lies in W, so $P(v) \in W$.

First, P is still a projection onto W. If $w \in W$, then $s^{-1}w \in W$, so $p(s^{-1}w) = s^{-1}w$. Therefore

$$P(w) = \frac{1}{|G|} \sum_{s \in G} s(s^{-1}w) = \frac{1}{|G|} \sum_{s \in G} w = w.$$

Next, P is G-equivariant. Let $t \in G$. Then

$$P(tv) = \frac{1}{|G|} \sum_{s \in G} s\, p(s^{-1}tv).$$

As s runs through G, we may write $s = tr$ with r running through G. Thus

$$\begin{aligned} P(tv) &= \frac{1}{|G|} \sum_{r \in G} tr\, p(r^{-1}v) \\ &= t \left(\frac{1}{|G|} \sum_{r \in G} r\, p(r^{-1}v) \right) \\ &= tP(v). \end{aligned}$$

Now let

$$W' = \ker(P).$$

Since P is G-equivariant, W' is a subrepresentation of V. Finally, every $v \in V$ can be written as

$$v = P(v) + (v - P(v)).$$

The first term lies in W. The second lies in $\ker(P)$, because P is the identity on W and $P(v) \in W$. Also, $W \cap \ker(P) = 0$, since if $w \in W$ and $P(w) = 0$, then $w = 0$. Hence

$$V = W \oplus W'. \qquad \blacksquare$$

Theorem 5.3.2 (Maschke's theorem)**.** *Let G be a finite group. Every finite-dimensional complex representation of G is a direct sum of irreducible subrepresentations.*

Proof. We use induction on $\dim V$. If $\dim V = 0$, there is nothing to prove. If V is irreducible, then V is already a direct sum with one irreducible summand.

Otherwise, V has a nonzero proper subrepresentation W. By Lemma 5.3.1, there is a subrepresentation W' such that

$$V = W \oplus W'.$$

Both W and W' have dimension smaller than $\dim V$. By induction, each of them is a direct sum of irreducible subrepresentations. Therefore V is also a direct sum of irreducible subrepresentations. ■

Maschke's theorem is the structural foundation of finite representation theory over $\mathbb{C}$. It tells us that the main problem is to understand the irreducible representations and then understand how often each one appears inside a given representation. Characters will give us an efficient way to answer that multiplicity question.

Now we turn to Schur's lemma, which says that maps between irreducible representations are very rigid. In particular, if two irreducible representations are not isomorphic, then there are no nonzero maps between them. If they are isomorphic, then the only maps from one to the other are scalar multiples of the isomorphism.

Theorem 5.3.3 (Schur's lemma)**.** *Let V and W be irreducible complex representations of G. Any nonzero G-equivariant map $T : V \to W$ is an isomorphism.*

In particular, if V is irreducible, then every G-equivariant linear map $T : V \to V$ is scalar multiplication by some complex number.

Proof. By Lemma 5.2.3, $\ker(T)$ is a subrepresentation of V, and $\mathrm{im}(T)$ is a subrepresentation of W. Since V is irreducible, $\ker(T)$ is either 0 or V. If $\ker(T) = V$, then $T = 0$. If $\ker(T) = 0$, then T is injective.

Similarly, since W is irreducible, $\mathrm{im}(T)$ is either 0 or W. If $T \neq 0$, then $\mathrm{im}(T) \neq 0$, so $\mathrm{im}(T) = W$. Therefore every nonzero G-equivariant map $T : V \to W$ is both injective and surjective, hence an isomorphism.

Now suppose $V = W$, and let $T : V \to V$ be G-equivariant. Since V is a finite-dimensional complex vector space, T has an eigenvalue $\lambda \in \mathbb{C}$. The map

$$T - \lambda I_V$$

is still G-equivariant. It is not injective, because it has a nonzero eigenvector in its kernel. By the first part of the theorem, it cannot be a nonzero map. Therefore $T = \lambda I_V$. ■

Corollary 5.3.4. *Let V and W be irreducible complex representations of G. Then*

$$\mathrm{Hom}_G(V, W) = \begin{cases} 0, & V \ncong W \\ \mathbb{C}, & V \cong W. \end{cases}$$

Intuitively, Maschke's theorems say that all representations break apart into irreducible pieces, and then Schur's lemma says that any maps between representations do not "mix" these irreducible pieces. In the next section, we will use this to find the irreducible decomposition of a representation.

5.4 CHARACTERS

Reminder: the *trace* of a matrix is the sum of its diagonal entries. Equivalently, the trace is the sum of the eigenvalues of the matrix or the second coefficient of the characteristic polynomial. This is independent of the choice of basis, so it is a well-defined invariant of a linear transformation. Recall that $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$ and $\mathrm{Tr}(A+B) = \mathrm{Tr}(A) + \mathrm{Tr}(B)$.

Definition 5.4.1. Let (V, ρ) be a finite-dimensional complex representation of G. The *character* of V is the function $\chi_V : G \to \mathbb{C}$ defined by

$$\chi_V(s) = \mathrm{Tr}(\rho(s)).$$

The character records one number for each group element: the trace of the linear transformation by which that element acts. One immediate thing is that if two representations are isomorphic, they have the same character.

Lemma 5.4.2. *Isomorphic representations have the same character.*

Proof. If V and W are isomorphic representations, then $W = PVP^{-1}$ for some invertible matrix P. That is, it is the same linear transformation written in a different basis. Therefore $\mathrm{Tr}(W) = \mathrm{Tr}(PVP^{-1}) = \mathrm{Tr}(V)$, so the characters are the same. ■

Remark 5.4.3. The observation that $\chi(uv) = \chi(vu)$ is equivalent to $\chi(uvu^{-1}) = \chi(v)$ is called being a *class function*. In other words, the character is constant on conjugacy classes.

As we will show, the important deeper point is that the converse is also true: if two representations have the same character, then they are isomorphic. Therefore we can reduce the study of representations to that of their characters, and in general, a finite-dimensional representation is specified by a set of $|G|$ numbers.

Example 5.4.4. If V is the trivial representation of dimension n, then every $s \in G$ acts as the identity map I_V. Therefore

$$\chi_V(s) = \mathrm{Tr}(I_V) = n$$

for every $s \in G$. ◇

Example 5.4.5. Let G act on a finite set X, and let V be the associated permutation representation with basis $(e_x)_{x \in X}$. For $s \in G$, the matrix of $\rho(s)$ has a 1 in the diagonal entry corresponding to x exactly when $sx = x$, and has 0 in that diagonal entry otherwise. Therefore

$$\chi_V(s) = |\{x \in X \mid sx = x\}|.$$

So the character of a permutation representation counts fixed points. ◇

Example 5.4.6. Let V be the regular representation of G. This is the permutation representation associated to the action of G on itself by left multiplication. If $s = e_G$, then every element of G is fixed, so

$$\chi_V(e_G) = |G|.$$

If $s \neq e_G$, then left multiplication by s has no fixed points: $st = t$ would imply $s = e_G$. Hence

$$\chi_V(s) = 0 \qquad \text{for } s \neq e_G.$$

Thus the character of the regular representation is

$$\chi_V(s) = \begin{cases} |G| & \text{if } s = e_G, \\ 0 & \text{if } s \neq e_G. \end{cases} \quad \diamond$$

Example 5.4.7. Let S_n act on $\mathbb{C}^n$ by permuting the standard basis. Let P be this permutation representation, let L be the trivial subrepresentation spanned by $e_1 + \cdots + e_n$, and let W be the standard representation. We showed earlier that

$$P = L \oplus W.$$

The character of P counts fixed points, and the character of L is identically 1. Therefore

$$\chi_W(\sigma) = |\{i \in \{1, \ldots, n\} \mid \sigma(i) = i\}| - 1.$$

Thus the character of the standard representation of S_n is "number of fixed points minus one." $\diamond$

Example 5.4.8. So far, we've introduced three different irreducible representations of S_3: the trivial representation, the sign representation, and the standard representation. Lets compute their characters.

$\chi_V(g)$	e	$(1\,2)$	$(1\,3)$	$(2\,3)$	$(1\,2\,3)$	$(1\,3\,2)$
χ_{triv}	1	1	1	1	1	1
χ_{sgn}	1	-1	-1	-1	1	1
χ_{std}	2	0	0	0	-1	-1

We will soon be able to show that these are *all* the irreducible representations of S_3. This is called the *character table* for S_3. $\diamond$

Here are the important properties about characters and character tables:

1. The value of $\chi_V(g)$ only depends on the conjugacy class of g.
2. The number of rows equals the number of conjugacy classes of G.
3. The sum of the absolute squares of any row, summed over all group elements, equals $|G|$.

4. The "dot product" of any row with itself is 1.
5. The "dot product" of any two different rows, summed over all group elements, is 0.

Most of these we will prove later.

Proposition 5.4.9. *If V and W are representations of G, then $\chi_{V\oplus W} = \chi_V + \chi_W$.*

Proof. With respect to bases adapted to the direct sum $V \oplus W$, the matrix for the action of $s \in G$ has block form

$$\begin{bmatrix} \rho_V(s) & 0 \\ 0 & \rho_W(s) \end{bmatrix}.$$

The trace of a block diagonal matrix is the sum of the traces of the diagonal blocks. Therefore

$$\chi_{V\oplus W}(s) = \chi_V(s) + \chi_W(s)$$

for every $s \in G$. ■

Lemma 5.4.10. *If χ_V is a character, then $\chi(s^{-1}) = \overline{\chi(s)}$ for every $s \in G$.*

Proof. Since s has finite order, the eigenvalues of $\rho(s)$ are roots of unity. Therefore the eigenvalues of $\rho(s^{-1})$ are the complex conjugates of the eigenvalues of $\rho(s)$. Since the trace is the sum of the eigenvalues, we have

$$\chi_V(s^{-1}) = \mathrm{Tr}(\rho(s^{-1})) = \overline{\mathrm{Tr}(\rho(s))} = \overline{\chi_V(s)}.$$ ■

5.5 CHARACTERS AND CLASS FUNCTIONS

Recall from the previous section that characters are class functions on G. We can define an inner product on the vector space of all class functions on G.

Definition 5.5.1. If $f_1, f_2 : G \to \mathbb{C}$ are functions, define

$$\langle f_1, f_2\rangle = \frac{1}{|G|}\sum_{s\in G} f_1(s)\overline{f_2(s)}.$$

This is the usual Hermitian inner product on the vector space of functions $G \to \mathbb{C}$, normalized by the factor $|G|$.

Remark 5.5.2. If f_1 and f_2 are class functions, then the inner product can be computed by summing over conjugacy classes. If $C_1, \ldots, C_r$ are the conjugacy classes of G and $c_i \in C_i$ is a representative, then

$$\langle f_1, f_2\rangle = \frac{1}{|G|}\sum_{i=1}^{r} |C_i|\, f_1(c_i)\overline{f_2(c_i)}.$$

This is one reason conjugacy classes become the columns of a character table.

We now prove the main orthogonality theorem for irreducible characters. The proof is a little complicated, but combining the result with Schur's lemma gives a very clean and useful result.

Proposition 5.5.3. *Let V and W be finite-dimensional complex representations of G. Then*

$$\langle \chi_V, \chi_W \rangle = \dim \mathrm{Hom}_G(W, V).$$

Proof. Let $E = \mathrm{Hom}(W, V)$. We make E into a representation of G by

$$(sT)(w) = sT(s^{-1}w),$$

for $T \in \mathrm{Hom}(W, V)$ and $w \in W$. Its character is

$$\chi_E(s) = \chi_V(s)\chi_W(s^{-1}).$$

Indeed, after choosing bases, the action of s on E has the form

$$T \longmapsto ATB^{-1},$$

where A is the matrix of s on V, and B is the matrix of s on W. A direct calculation on matrix units E_{ij} shows that the trace of the map $T \mapsto ATB^{-1}$ is $\mathrm{Tr}(A)\,\mathrm{Tr}(B^{-1})$. This proves the displayed formula for $\chi_E(s)$.

Now average the action of G on E. Define

$$P : E \to E, \qquad P(T) = \frac{1}{|G|} \sum_{s \in G} sT.$$

This is a projection onto the fixed subspace E^G. Indeed, if $U \in E$, then for any $t \in G$,

$$tP(U) = \frac{1}{|G|} \sum_{s \in G} tsU = \frac{1}{|G|} \sum_{r \in G} rU = P(U),$$

so $P(U) \in E^G$. If $U \in E^G$, then

$$P(U) = \frac{1}{|G|} \sum_{s \in G} U = U.$$

Thus P is a projection onto E^G, and therefore $\mathrm{Tr}(P) = \dim E^G$ since Tr of a projection is the dimension of its image. By linearity of trace,

$$\begin{aligned} \mathrm{Tr}(P) &= \frac{1}{|G|} \sum_{s \in G} \chi_E(s) \\ &= \frac{1}{|G|} \sum_{s \in G} \chi_V(s)\overline{\chi_W(s)} \\ &= \langle \chi_V, \chi_W \rangle. \end{aligned}$$

Finally, the fixed subspace E^G is exactly $\mathrm{Hom}_G(W, V)$. Indeed, $T \in E^G$ means

$$sT(s^{-1}w) = T(w)$$

for every $s \in G$ and $w \in W$. Replacing w by sw gives

$$sT(w) = T(sw),$$

which is exactly the condition that T is G-equivariant. Thus

$$\langle \chi_V, \chi_W \rangle = \mathrm{Tr}(P) = \dim E^G = \dim \mathrm{Hom}_G(W, V). \qquad \blacksquare$$

The proof of Proposition 5.5.3 gives an intuitive picture of inner products between characters. The inner product between characters is the quantity

$$\frac{1}{|G|} \sum_{s \in G} \chi_V(s) \overline{\chi_W(s)},$$

which is is an average correlation between the two representations, or how much they have in common. This is the same as the dimension of the space of G-equivariant maps between the two representations. By adding Schur's lemma, we get the following orthogonality theorem for irreducible characters.

Theorem 5.5.4 (Orthogonality of irreducible characters)**.** *Let V and W be irreducible complex representations of G. Then*

$$\langle \chi_V, \chi_W \rangle = \begin{cases} 1 & \text{if } V \cong W, \\ 0 & \text{if } V \ncong W. \end{cases}$$

Proof. By Proposition 5.5.3,

$$\langle \chi_V, \chi_W \rangle = \dim \mathrm{Hom}_G(W, V).$$

By Schur's lemma, $\mathrm{Hom}_G(W, V) = 0$ if V and W are not isomorphic. If $V \cong W$, then $\mathrm{Hom}_G(W, V)$ is one-dimensional: after choosing one isomorphism $W \to V$, every other G-equivariant map differs from it by a scalar. This proves the theorem. $\blacksquare$

This theorem says that irreducible characters form an orthonormal set in the space of class functions. In particular, they are linearly independent. But in fact, they form an orthonormal *basis* for the space of class functions.

Theorem 5.5.5 (Completeness of irreducible characters)**.** *The irreducible characters of G form an orthonormal basis for the vector space of class functions on G. In particular, the number of irreducible complex representations of G is equal to the number of conjugacy classes of G.*

We will not prove this here because it requires a little more machinery I don't want to introduce.[1] As a direct consequence, we can compute the decomposition of the regular representation into irreducible representations, which gives a very useful formula for the order of a finite group.

Corollary 5.5.6. *Let $V_1, \dots, V_r$ be the irreducible complex representations of G. Then the regular representation decomposes as*

$$V_{\text{reg}} \cong (\dim V_1)V_1 \oplus \cdots \oplus (\dim V_r)V_r.$$

Consequently,

$$|G| = \sum_{i=1}^{r} (\dim V_i)^2.$$

Proof. Let χ_{reg} be the character of the regular representation. We computed earlier that

$$\chi_{\text{reg}}(e) = |G|, \qquad \chi_{\text{reg}}(s) = 0 \text{ for } s \neq e.$$

Therefore the multiplicity of V_i in the regular representation is

$$\begin{aligned} \langle \chi_{\text{reg}}, \chi_{V_i} \rangle &= \frac{1}{|G|} |G| \chi_{V_i}(e) \\ &= \dim V_i. \end{aligned}$$

This proves the decomposition. Taking dimensions of both sides gives the result. ∎

Now suppose a finite-dimensional complex representation V decomposes as

$$V \cong m_1 V_1 \oplus \cdots \oplus m_r V_r,$$

where $V_1, \dots, V_r$ are pairwise nonisomorphic irreducible representations, and where $m_i V_i$ means a direct sum of m_i copies of V_i. Maschke's theorem guarantees that such a decomposition exists after collecting isomorphic irreducible summands together. The integers m_i are called the *multiplicities* of the irreducible representations in V.

Theorem 5.5.7 (Multiplicity formula)**.** *With notation as above,*

$$m_i = \langle \chi_V, \chi_{V_i} \rangle.$$

[1] One way to prove this is through the group algebra $\mathbb{C}[G]$. The center of $\mathbb{C}[G]$ has a basis given by the conjugacy-class sums $\sum_{g \in C} g$, so its dimension is the number of conjugacy classes of G. On the other hand, Schur's lemma implies that a central element acts by a scalar on each irreducible representation, so the center has one independent scalar parameter for each irreducible representation. Thus the number of irreducible representations equals the number of conjugacy classes.

Proof. By additivity of characters under direct sums,

$$\chi_V = m_1\chi_{V_1} + \cdots + m_r\chi_{V_r}.$$

Taking the inner product with χ_{V_i} gives

$$\begin{aligned}\langle \chi_V, \chi_{V_i}\rangle &= \sum_{j=1}^{r} m_j \langle \chi_{V_j}, \chi_{V_i}\rangle \\ &= m_i,\end{aligned}$$

by the orthogonality of irreducible characters. ∎

Corollary 5.5.8. *Two finite-dimensional complex representations of* G *have the same character if and only if they are isomorphic.*

Proof. If $V \cong W$, then $\chi_V = \chi_W$. Conversely, suppose $\chi_V = \chi_W$. Write

$$V \cong m_1V_1 \oplus \cdots \oplus m_rV_r \qquad \text{and} \qquad W \cong n_1V_1 \oplus \cdots \oplus n_rV_r,$$

where $V_1, \ldots, V_r$ are the irreducible representations that occur in either decomposition. The multiplicity formula gives

$$m_i = \langle \chi_V, \chi_{V_i}\rangle = \langle \chi_W, \chi_{V_i}\rangle = n_i$$

for every i. Thus V and W have the same irreducible summands with the same multiplicities, so $V \cong W$. ∎

Remark 5.5.9. This is the first major computational payoff of characters. To find how many times an irreducible representation V_i occurs inside V, we do not have to find all of the subrepresentations by hand. We compute one inner product of class functions.

Proposition 5.5.10 (Burnside's lemma revisited)**.** *Let* G *act on a finite set* X*, and let* χ_{perm} *be the character of the associated permutation representation. Then*

$$\langle \chi_{\text{perm}}, 1\rangle = \frac{1}{|G|}\sum_{s\in G} |\{x \in X \mid sx = x\}| = |X/G|.$$

Proof. The first equality is just the definition of the inner product together with the fact that $\chi_{\text{perm}}(s)$ counts the fixed points of s. The last expression is Burnside's lemma. ∎

We can also see the representation-theoretic meaning directly. The inner product $\langle \chi_{\text{perm}}, 1\rangle$ is the multiplicity of the trivial representation inside the permutation representation. The fixed subspace consists of the vectors

$$\sum_{x\in X} a_x e_x$$

whose coefficients are constant on each orbit. Therefore the dimension of this fixed subspace is the number of orbits of the action.

5.6 Computing Character Tables

As we've seen, a character table is a compact way to record the irreducible characters of a finite group. The columns are indexed by conjugacy classes of G. This makes sense because characters are class functions. The rows are indexed by the irreducible characters of G. If $C_1, \ldots, C_r$ are the conjugacy classes and $c_i \in C_i$ is a representative, then the character table records the values $\chi(c_i)$ as χ runs through the irreducible characters.

Remark 5.6.1. The choice of representative c_i does not matter, since characters are constant on conjugacy classes. In a character table we usually label a column by a convenient representative, such as $(1\,2)$ for the class of all transpositions in S_n.

The row orthogonality relation says that distinct irreducible rows are orthogonal using the weighted inner product

$$\langle \chi, \psi \rangle = \frac{1}{|G|} \sum_{i=1}^{r} |C_i| \chi(c_i) \overline{\psi(c_i)}.$$

Thus each irreducible row has norm 1, and two different irreducible rows have inner product 0.

There is also a column orthogonality relation for a complete character table. Let g and h be elements of a finite group G, and let $V_1, \ldots, V_r$ be irreps of G. Then

$$\sum_{i=1}^{r} \chi_{V_i}(g) \overline{\chi_{V_i}(h)} = \begin{cases} |C_G(g)| = |G|/|C_g| & \text{if } g, h \text{ are conjugate,} \\ 0 & \text{otherwise.} \end{cases}$$

So the columns are orthogonal too, but with a different normalization.

Exercise (5.6.1). Let $C_n = \langle a \rangle$ be a cyclic group of order n. Write the character table of C_n.

Example 5.6.2. Let us return to the symmetric group S_3. The conjugacy classes of S_3 are:

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

Their sizes are 1, 3, and 2. We can rewrite the character table with columns as conjugacy classes:

	e	$(1\,2)$	$(1\,2\,3)$
class size	1	3	2
χ_{triv}	1	1	1
χ_{sgn}	1	-1	1
χ_{std}	2	0	-1

Since S_3 has three conjugacy classes, Theorem 5.5.5 says that there are three irreducible characters. Thus this is the complete character table of S_3.

Now let R be the regular representation of S_3. From our earlier computation of the character of the regular representation,

$$\chi_R = (6, 0, 0)$$

on these three conjugacy classes. The multiplicities are

$$\langle \chi_R, \chi_{\text{triv}} \rangle = 1, \qquad \langle \chi_R, \chi_{\text{sgn}} \rangle = 1, \qquad \langle \chi_R, \chi_{\text{std}} \rangle = 2.$$

Therefore

$$R \cong V_{\text{triv}} \oplus V_{\text{sgn}} \oplus 2V_{\text{std}}.$$

The dimensions check out: $1 + 1 + 2 \cdot 2 = 6$, which is the dimension of the regular representation. ◇

Exercise (5.6.2). Let S_4 act on the set X of all two-element subsets of $\{1, 2, 3, 4\}$. Let P be the corresponding permutation representation.

1. Compute the character χ_P on the five conjugacy classes

$$e, \quad (1\,2), \quad (1\,2)(3\,4), \quad (1\,2\,3), \quad (1\,2\,3\,4).$$

2. Compute

$$\langle \chi_P, \chi_{\text{triv}} \rangle \qquad \text{and} \qquad \langle \chi_P, \chi_{\text{std}} \rangle.$$

   Conclude that P contains one copy of the trivial representation and one copy of the standard representation.

3. By Maschke's theorem, write $P \cong V_{\text{triv}} \oplus V_{\text{std}} \oplus U$ for some representation U. Compute χ_U and show that it is irreducible. What is the dimension of U?

Example 5.6.3. Let us compute the character table of S_4. By Theorem 4.2.5, conjugacy classes in S_n are determined by cycle type. The conjugacy classes of S_4 are represented by

$$e, \qquad (1\,2), \qquad (1\,2)(3\,4), \qquad (1\,2\,3), \qquad (1\,2\,3\,4),$$

and their sizes are

$$1, \qquad 6, \qquad 3, \qquad 8, \qquad 6.$$

Since there are five conjugacy classes, there are five irreducible characters.

We immediately have the trivial character and the sign character. The dimension formula from Corollary 5.5.6 tells us that if the remaining dimensions are d_1, d_2, d_3, then

$$d_1^2 + d_2^2 + d_3^2 = 24 - 1^2 - 1^2 = 22.$$

The only possibility is

$$\{d_1, d_2, d_3\} = \{2, 3, 3\}.$$

One of the 3-dimensional irreducible representations is the standard representation of S_4. Its character is the number of fixed points minus one:

$$\chi_{\text{std}} = (3, 1, -1, 0, -1).$$

Exercise (5.6.2) gives the remaining 2-dimensional irreducible character

$$\chi_2 = (2, 0, 2, -1, 0).$$

We only need the last irreducible character, which we can compute via the orthogonality relations. That is, we can use the row orthogonality relations and linear algebra to solve for the last row, or some of the column orthogonality relations. We get

$$\chi_{\text{sgn}\cdot\text{std}} = (3, -1, -1, 0, 1).$$

Note that this is the character χ_{std} multiplied entrywise by the sign character χ_{sgn}.

Thus the character table of S_4 is

S_4	e	$(1\,2)$	$(1\,2)(3\,4)$	$(1\,2\,3)$	$(1\,2\,3\,4)$
class size	1	6	3	8	6
χ_{triv}	1	1	1	1	1
χ_{sgn}	1	-1	1	1	-1
χ_{std}	3	1	-1	0	-1
χ_2	2	0	2	-1	0
$\chi_{\text{sgn}\cdot\text{std}}$	3	-1	-1	0	1

One quick check is

$$1^2 + 1^2 + 3^2 + 3^2 + 2^2 = 24 = |S_4|. \qquad \diamond$$

Exercise (5.6.3). Show that if V and W are irreps of G with $\dim W = 1$, then $\chi_V \chi_W$ is the character of an irreducible representation (where multiplication happens entrywise). We didn't have time in the course, but this is the character of the *tensor product* $V \otimes W$. This is the "product" analog of the direct sum construction and has dimension $\dim V \cdot \dim W$.

Exercise (5.6.4). Let W be the standard representation of S_4 and let $E = \text{End}(W) = \text{Hom}(W, W)$.

1. Show that $\sigma \cdot T = \sigma T \sigma^{-1}$ defines a representation of S_4 on E.
2. Show that $\dim E = 9$ and compute the character of E. (Hint: For the latter, look at the proof that $\langle \chi_V, \chi_W \rangle = \dim \text{Hom}_G(W, V)$.)
3. Decompose E into irreducible representations of S_4.

Example 5.6.4. Let $D_4 = \langle r, s \mid r^4 = e,\ s^2 = e,\ srs = r^{-1} \rangle$ be the symmetry group of a square. Its conjugacy classes are

$$\{e\}, \qquad \{r^2\}, \qquad \{r, r^3\}, \qquad \{s, r^2 s\}, \qquad \{rs, r^3 s\}.$$

Thus D_4 has five irreducible characters.

Using the earlier exercise about one-dimensional representations, the one-dimensional characters of D_4 are exactly the homomorphisms $D_4^{ab} \to \mathbb{C}^\times$. Recall the presentation

$$D_4 = \langle r, s \mid r^4 = e,\ s^2 = e,\ srs = r^{-1} \rangle.$$

The abelianization is what you get by forcing s and r to commute, thus $srs = r^{-1}$ becomes $r = r^{-1}$, so $r^2 = e$. Thus

$$D_4^{ab} = \langle r, s \mid r^2 = e,\ s^2 = e,\ rs = sr \rangle \cong C_2 \times C_2.$$

Therefore there are four one-dimensional characters, which we can denote by $\chi_{++}, \chi_{+-}, \chi_{-+}$, and χ_{--}, where the signs indicate the values of the character on r and s.

This leaves one last 2-dimensional character, which we *could* find via the orthogonality relations. However, its very natural: consider the 2-dimensional geometric representation coming from the action of D_4 on the square in the plane. In that representation, the identity has trace 2, the half-turn r^2 has trace -2, and every quarter-turn or reflection has trace 0. Therefore the character table is

D_4	e	r^2	r	s	rs
class size	1	1	2	2	2
χ_{++}	1	1	1	1	1
χ_{+-}	1	1	1	-1	-1
χ_{-+}	1	1	-1	1	-1
χ_{--}	1	1	-1	-1	1
χ_{geom}	2	-2	0	0	0

The dimensions again check out:

$$1^2 + 1^2 + 1^2 + 1^2 + 2^2 = 8 = |D_4|. \qquad \diamond$$

Exercise (5.6.5). This exercise computes the character table of the quaternion group

$$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}.$$

1. Show that the conjugacy classes of Q_8 are

$$\{1\}, \qquad \{-1\}, \qquad \{\pm i\}, \qquad \{\pm j\}, \qquad \{\pm k\}.$$

2. Show that the abelianization of Q_8 is $Q_8/\{\pm 1\} \cong C_2 \times C_2$. Use this to find four one-dimensional characters of Q_8.

3. Use orthogonality with the trivial character to show that this final character is

$$(2, -2, 0, 0, 0)$$

on the conjugacy classes above.

4. Write the full character table of Q_8 and compare it with the table of D_4. What does this show about character tables as invariants of groups?

BIBLIOGRAPHY

[DF03] D. S. Dummit and R. M. Foote, *Abstract algebra*, Wiley, 2003. ↑i

INDEX OF DEFINED TERMS