Modern Group Theory

Corran Webster

May 3, 2004

Contents

Chapter 1

Introduction

Algebraic structures of various types occur naturally in many different areas of mathematics. The most straightforward examples arise in arithmetic, but there are numerous other examples which are not as obvious. In this chapter we start our study of group theory by looking at a number of concrete situations where an algebraic structure arises naturally. We will see that all these algebraic structures share common features, and these common features will lead us to the definition of a group in Chapter 2.

1.1 Symmetry

You are familiar, at least in an informal way, with the idea of symmetry from Euclidean geometry and calculus. For example, the letter "A" has reflective symmetry in its vertical axis, "E" has reflective symmetry in its horizontal axis, "N" has rotational symmetry of π radians about its centre, "H" has all three types of symmetry, and the letter "F" has none of these symmetries.

Symmetry is also important in understanding real world phenomena. As some examples:

- The symmetries of molecules can affect possible chemical reactions. For example, many proteins and amino acids (the basic building blocks of life) have "left-handed" and "right-handed" versions which are reflections of one-another. Life on earth uses the "left-handed" versions almost exclusively.

- Crystals have very strong symmetries, largely determined by the symmetries of the atoms or molecules of which the crystal is built.

- Most animals and plants have some sort of symmetry in their body-shapes, although they are never perfectly symmetrical. Most animals have bilateral symmetry, while plants often have five-fold or six-fold rotational symmetry.

- In art and design, symmetrical patterns are often found to be more pleasing to the eye than asymmetrical patterns, or simply more practical.
- Waves in fluids, and the vibrations of a drumhead or string are often symmetrical, or built out of symmetric components. These symmetries are usually inherent in the underlying equations that we use to model such systems, and understanding the symmetry can be crucial in finding solutions to these equations.

But what, precisely, do we mean by symmetry?

Definition 1.1
Let Ω be a subset of $\mathbb{R}^n$. A ***symmetry*** *of Ω is a function $T : \mathbb{R}^n \to \mathbb{R}^n$ such that*

(i) $\{T(x) : x \in \Omega\} = \Omega$, and

(ii) T preserves distances between points: if $d(x, y)$ is the distance between the points x and y, then $d(T(x), T(y)) = d(x, y)$.

We denote the set of all symmetries of Ω by $\mathrm{Sym}(\Omega)$. Every set Ω has at least one symmetry, the ***identity symmetry*** *$I(x) = x$.*

Functions which preserve distance are called ***isometries****, so every symmetry is an isometry.*

Proposition 1.1
Let Ω be a subset of $\mathbb{R}^n$, and let S and T be symmetries of Ω. Then

(i) T is one-to-one and onto.

(ii) the inverse function T^{-1} is a symmetry of Ω

(iii) the composition $T \circ S$ is a symmetry of Ω

(iv) the compositions $T \circ T^{-1}$ and $T^{-1} \circ T$ always equal the identity symmetry I.

Proof:
(i) This follows immediately from the technical result that every isometry from $\mathbb{R}^n$ to $\mathbb{R}^n$ is one-to-one and onto (this is proved in Lemma 1.11 at the end of this chapter).

(ii) Since T is one-to-one and onto, it has an inverse function T^{-1}. We observe that $T^{-1}(\Omega) = T^{-1}(T(\Omega)) = \Omega$, and also that $d(T^{-1}(x), T^{-1}(y)) = d(T(T^{-1}(x)), T(T^{-1}(y))) = d(x, y)$. Hence T^{-1} is a symmetry of Ω.

Parts (iii) and (iv) are left as a simple exercise. ■

We will usually write the composed symmetry $T \circ S$ as simply TS. Remember that because function composition works from right to left, TS means that the symmetry S is applied first, followed by the symmetry T.

Notation: *Many algebra texts write ST for $T \circ S$, because S is applied first, then T. In these notes, however, we will remain consistent with the traditional function composition order, but you must keep this clear in your head to avoid confusion. Another commonly used convention in algebra is to apply functions on the right, so $T(x)$ is written as xT, so that $S(T(x))$ would be written as xTS.*

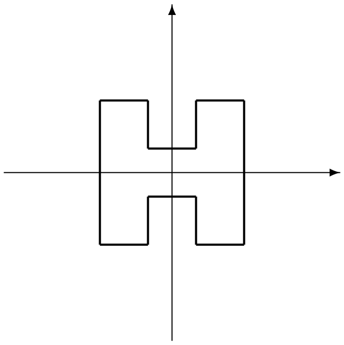


Figure 1.1: The set Ω of Example 1.1

You should also recall that composition of functions is associative (see Proposition 1.2) so composition of symmetries is always associative. In other words if S, T and $U \in \mathrm{Sym}(\Omega)$, then $S(TU) = (ST)U$. However, composition of functions is not usually commutative, so without additional evidence, we cannot conclude that $ST = TS$.

Example 1.1

Let $\Omega \subseteq \mathbb{R}^2$ be the H-shaped set illustrated in Figure 1.1. Then Ω has percisely the following symmetries:

$$\begin{aligned} I(x,y) &= (x,y) && \text{(Identity)} \\ H(x,y) &= (x,-y) && \text{(Reflection in the } x\text{-axis)} \\ V(x,y) &= (-x,y) && \text{(Reflection in the } y\text{-axis)} \\ R(x,y) &= (-x,-y) && \text{(Rotation by } \pi \text{ radians about the origin)} \end{aligned}$$

We can confirm by direct calculation that $I^{-1} = I$, $H^{-1} = H$, $V^{-1} = V$ and $R^{-1} = R$. In other words, each of these transformations is its own inverse. These symmetries compose in the following ways:

$$\begin{array}{lll} H \circ H = I & H \circ V = R & H \circ R = V \\ V \circ H = R & V \circ V = I & V \circ R = H \\ R \circ H = V & R \circ V = H & R \circ R = I \end{array}$$

In fact we can summarize this using a "multiplication table":

$\circ$	I	H	V	R
I	I	H	V	R
H	H	I	R	V
V	V	R	I	H
R	R	V	H	I

This sort of "multiplication table" is called a ***Cayley table*** for the operation.

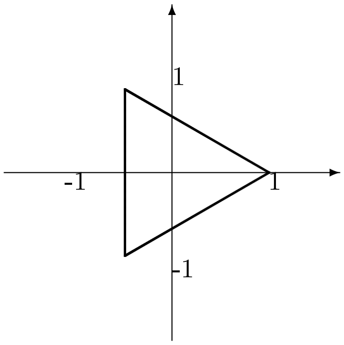


Figure 1.2: The equilateral triangle of Example 1.2

The composition of symmetries in this example is commutative. You can verify this by simply checking every possible product. For example, from the Cayley table we have $HR = V$, and $RH = V$, so $HR = RH$. ◇

There is nothing really special about the set Ω in the previous example, other than the fact that composition is commutative for this set. As the following example shows, we should not expect composition of symmetries to be commutative in every case.

Example 1.2

Let $\Omega \subseteq \mathbb{R}^2$ be an equilateral triangle with veritces $(1, 0)$, $(-1/2, \sqrt{3}/2)$ and $(-1/2, -\sqrt{3}/2)$. Then Ω has the following symmetries:

I	Identity
R_1	Rotation by $2\pi/3$ radians clockwise
R_2	Rotation by $2\pi/3$ radians anticlockwise
H_0	Reflection in the x-axis
H_1	Reflection in the line through $(0, 0)$ and $(-1/2, \sqrt{3}/2)$
H_2	Reflection in the line through $(0, 0)$ and $(-1/2, -\sqrt{3}/2)$

The precise formulas for these symmetries are an exercise. A little thought tells us that $I^{-1} = I$, $R_1^{-1} = R_2$, $R_2^{-1} = R_1$, $H_1^{-1} = H_1$, $H_2^{-1} = H_2$, and $H_3^{-1} = H_3$. The Cayley table for these symmetries is:

$\circ$	I	R_1	R_2	H_0	H_1	H_2
I	I	R_1	R_2	H_0	H_1	H_2
R_1	R_1	R_2	I	H_1	H_2	H_0
R_2	R_2	I	R_1	H_2	H_0	H_1
H_0	H_0	H_2	H_1	I	R_2	R_1
H_1	H_1	H_0	H_2	R_1	I	R_2
H_2	H_2	H_1	H_0	R_2	R_1	I

This operation is associative, but it is clearly *not* commutative: $H_0 \circ H_1 = R_1$, but $H_1 \circ H_0 = R_2$, for example. ◇

Some sets have infinite collections of symmetries, but even in these cases we can still understand how composition works.

Example 1.3
Let $\Omega = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}$ be the unit circle. Then Ω has infinitely many symmetries, which fall into two classes:

R_θ	Rotation by θ radians clockwise, $0 \leq \theta < 2\pi$
H_φ	Reflection in the line which makes an angle φ to the x-axis at the origin, $0 \leq \varphi < \pi$.

The identity is R_0, rotation by 0 radians. We can also check that the inverse of R_θ is $R_{2\pi-\theta}$ for $0 < \theta < 2\pi$, and the inverse of H_φ is H_φ.

Because the set of symmetries is infinite, we can't write down a Cayley table, but we can list how the generic symmetries compose:

$$\begin{aligned} R_\theta \circ R_\omega &= R_{\theta+\omega} & R_\theta \circ H_\varphi &= H_{\varphi-\theta/2} \\ H_\varphi \circ R_\theta &= H_{\varphi+\theta/2} & H_\varphi \circ H_\psi &= R_{2\psi-2\varphi} \end{aligned}$$

where all angles are reduced to lie in the appropriate ranges. The easiest way to verify this table is to note that $H_\varphi = H_0 \circ R_{2\varphi} = R_{-2\varphi} \circ H_0$, which greatly simplifies calculations involving H_φ. ◇

All the examples so far have used rotational and reflective symmetries, but some sets also have translational symmetry.

Example 1.4
Let $\Omega\{(x, y) \in \mathbb{R}^2 : y = 0\}$ be the x-axis in $\mathbb{R}^2$. Then Ω has symmetries of the form

$$T_c(x, y) = (x + c, y),$$

ie. right translation by c, for any $c \in \mathbb{R}$, and

$$S_c(x, y) = (-x + c, y),$$

ie. reflection about 0, followed by right translation by c, for any $c \in \mathbb{R}$ (which is equal to reflection about the point $c/2$).

The identity symmetry is T_0, the inverse symmetry of T_c is T_{-c}, and the inverse symmetry of S_c is S_c. The symmetries of this set compose by the rules

$$\begin{aligned} T_a \circ T_b &= T_{a+b} & T_a \circ S_b &= S_{a+b} \\ S_a \circ T_b &= S_{a-b} & S_a \circ S_b &= T_{a-b} \end{aligned}$$

◇

Exercises

1.1.1. Find the set of symmetries for each capital letter of the alphabet (assume uniform, sans serif letter shapes).

1.1.2. Prove Proposition 1.1 (iii-iv).

1.1.3. Write down formulas for each of the symmetries in Example 1.2.

Hint 1: the point $(x, y) \in \mathbb{R}^2$ rotated clockwise by an angle θ about the origin is $(x \cos\theta + y \sin\theta, -x \sin\theta + y \cos\theta)$.

Hint 2: from the Cayley table, we have $H_1 = R_1 \circ H_0$ and $H_2 = R_2 \circ H_0$, and it is easy to find the formula of a composition of functions.

1.1.4. Let $\Omega \subseteq \mathbb{R}^2$ be a square, centred at the origin, with side length 1. Find all 8 symmetries of Ω, and write down the formula for each. Find the inverses of each symmetry. Write out the Cayley table for the symmetries of a square.

1.1.5. (*) Let $\Omega \subseteq \mathbb{R}^3$ be a regular tetrahedron centred at the origin. Show that Ω has 24 symmetries.

1.1.6. (*) Let $\Omega = \mathbb{Z}^2 \subseteq \mathbb{R}^2$ be the integer lattice in the plane, ie.

$$\mathbb{Z}^2 = \{(m, n) \in \mathbb{R}^2 : m, n \in \mathbb{Z}\}.$$

Classify the symmetries of $\mathbb{Z}^2$. Find the inverses of each symmetry. As in Example 1.3, find the product of typical symmetries.

1.2 Review: Sets

Group theory does not require a great deal of mathematical background to get started: we really only need the concepts of sets and functions to present the basics of the theory. You should have come across the formal definitions of these concepts in previous courses, such as a typical discrete mathematics course. A large part of the discussion in this section and the next will be to fix notation and terminology.

A ***set*** is a collection of mathematical objects. We do not care about the order that the objects are presented, nor any potential duplication of elements. The mathematical objects contained in a set S are called the ***elements*** or ***members*** of a set, and write $x \in S$ to say that x is an element of S. We say that two sets are equal if they have exactly the same elements.

The simplest way to present a set is as a list of all the elements of the set enclosed in braces, such as the set $\{1, 2, 3\}$. For sets with large numbers of elements, or infinite sets, this presentation is tedious (or impossible!), so there are two alternatives. If there is a clear pattern to the elements, one can use ellipses to elide the majority of the set, leaving just enough to make the pattern of elements clear:

$$\{2, 4, 6, \ldots, 100\} \qquad \text{and} \qquad \{2, 3, 5, 7, 11, 13, 17 \ldots\}$$

are clearly meant to represent the set of all even numbers from 2 to 100, and the set of all prime numbers respectively. However some sets are too complicated for this sort of presentation, and for these we use "set builder" notation. In set builder notation we simply specify the set by some property P which defines the set:

$$\{x|x \text{ satisfies } P\} \qquad \text{or} \qquad \{x : x \text{ satisfies } P\}.$$

For example, one could write the set of all prime numbers as

$$\{x|x \text{ is prime}\},$$

or the set of all numbers greater than 2 and less than or equal to 10 as

$$\{x : 2 < x \leq 10\}.$$

This last example illustrates an ambiguity: which collection of numbers do we mean? Integers? Rational numbers? Real numbers? To resolve this ambiguity, we usually specify the set S from which we take our elements, and use the notation

$$\{x \in S|x \text{ satisfies } P\} \qquad \text{or} \qquad \{x \in S : x \text{ satisfies } P\}.$$

Therefore the interval of all real numbers greater than 2 and less than or equal to 10 would most clearly be represented by

$$\{x \in \mathbb{R} : 2 < x \leq 10\}.$$

There are several special sets that come up with sufficient frequency to deserve their own notation. The most important is the ***empty set*** $\emptyset = \{\}$, the set which contains no elements. The next most important are the various sets of numbers:

$\mathbb{N} = \{1, 2, 3, 4, \ldots\}$	***natural numbers***
$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$	***integers***
$\mathbb{Q} = \{p/q : p \in \mathbb{Z}, q \in \mathbb{N}, p \text{ and } q \text{ coprime}\}$	***rational numbers***
$\mathbb{R} = \{x : x \text{ is an infinite decimal}^1\}$	***real numbers***
$\mathbb{C} = \{x + iy : x, y \in \mathbb{R}\}$	***complex numbers***

We say that a set A is a ***subset*** of another set B, and write $A \subseteq B$, if every element of A is an element of B. For example, $\{2, 4, 6\} \subseteq \{1, 2, 3, 4, 5, 6\}$. Note that if A is equal to B, it is still a subset of B, and that the empty set is always a subset of any other set. We say that A is a ***proper subset*** of B if $A \subset B$ and $A \neq B$, and we denote this by $A \subset B$.

We can combine sets using a number of different ***set operations***. The ***union*** of two sets A and B is the set containing all the elements of both sets combined, ie.

$$A \cup B = \{x : x \in A \text{ or } x \in B\}.$$

Proving Equality of Sets: *Often we have two sets, A and B, which we want to show are equal. A very common technique to show that this is in fact the case is to show that each set is a subset of the other. We can then conclude that they are equal. In summary:*

$\boxed{A \subseteq B \text{ and } B \subseteq A \text{ implies } A = B}$

The ***intersection*** of A and B is the set containing the objects that are elements of both of the sets, ie.

$$A \cap B = \{x : x \in A \text{ and } x \in B\}.$$

Intersection and union are both ***commutative*** and ***associative*** operations, and are ***distributive*** with respect to one another:

$$\begin{aligned} A \cup B &= B \cup A \\ A \cap B &= B \cap A \\ A \cup (B \cup C) &= (A \cup B) \cup C = A \cup B \cup C \\ A \cap (B \cap C) &= (A \cap B) \cap C = A \cap B \cap C \\ A \cup (B \cap C) &= (A \cup B) \cap (A \cup C) \\ A \cap (B \cup C) &= (A \cap B) \cup (A \cap C) \\ A \cup \emptyset &= A \\ A \cap \emptyset &= \emptyset \end{aligned}$$

If there is some natural ***universal set*** U of elements which we are considering, we can define the ***complement*** of a set A as the set of all things in U not in A, ie.

$$A^c = \{x \in U : x \notin A\}.$$

The complement of the complement is the original set, and complements interact with union and intersection via ***DeMorgan's laws***:

$$\begin{aligned} (A^c)^c &= A \\ (A \cup B)^c &= A^c \cap B^c \\ (A \cap B)^c &= A^c \cup B^c \\ \emptyset^c &= U \\ U^c &= \emptyset. \end{aligned}$$

Note that sometimes the notation $\overline{A}$ is used for complements.

Even in the absence of a universal set, we can define the ***set difference*** operation: $A \setminus B$ is everything in A which is not in B. That is

$$A \setminus B = \{x \in A : x \notin B\}.$$

If complements make sense, then we have $A \setminus B = A \cap B^c$. We can also define the ***symmetric difference*** of A and B as the set of all things in either A or B, but not in both,

$$A \bigtriangleup B = \{x \in A \cup B : x \notin A \cap B\}$$

or equivalently

$$A \bigtriangleup B = (A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A).$$

Clearly $A \triangle B = B \triangle A$.

Perhaps the most important set operation for our purposes, since it appears in just about every core definition in abstract algebra, is the ***Cartesian product***. The product of two sets, $A \times B$ is the set consisting of tuples (x, y), where $x \in A$ and $y \in B$, ie.

$$A \times B = \{(x, y) : x \in A, y \in B\}.$$

More generally, we define a product of n sets to be the set of n-tuples:

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) : a_k \in A_k, k = 1, 2, \ldots, n\}.$$

We also define

$$A^n = \underbrace{A \times A \times \cdots \times A}_{n \text{ times}}$$

to be the set of all n-tuples of elements of A. This notation is familiar from calculus, where $\mathbb{R}^n$ is the set of all n-tuples of real numbers. Note that $A \times B$ is not equal to $B \times A$ in general, although they are clearly closely related.

If $A \subseteq C$, and $B \subseteq D$ it is straightforward to see that $A \times B \subseteq C \times D$.

We denote the ***cardinality*** of a set A by $|A|$. For sets with a finite number of elements, the cardinality of A is simply the number of elements in the set. For infinite sets, cardinality is a more complicated matter, but for the purposes of this course it really only matters whether a set is infinite or not. You should, however, be aware that there are countably infinite sets (such as $\mathbb{N}^n$, $\mathbb{Z}^n$ and $\mathbb{Q}^n$) and uncountably infinite sets (such as $\mathbb{R}^n$ and $\mathbb{C}^n$) and that countable and uncountable sets have different cardinality.

For finite sets, we have the following facts from basic counting theory: the inclusion-exclusion principle

$$|A \cup B| = |A| + |B| - |A \cap B|,$$

and the multiplication principle

$$|A \times B| = |A||B|.$$

Both of these will be of importance when exploring the structure of finite groups.

Exercises

1.2.1. In this section many identities are stated without proof. Pick 8 of them and show why they hold. Be careful not to use any identity or fact which is dependent on what you are proving.

1.2.2. Show that $|A \setminus B| = |A| - |A \cap B|$.

1.3 Review: Functions

A ***function*** f from A to B is a rule which relates every element x of A to some unique element y of B. What is key here is that the function associates x with *precisely* one element of B. We write $y = f(x)$. More formally, we denote the function with the notation

$$\begin{aligned} f : A &\to B \\ x &\mapsto y. \end{aligned}$$

The set A is the ***domain***, the set B the ***codomain***, while the set

$$f(A) = \{f(x) : x \in A\}$$

is the ***range*** of the function. The ***graph*** of the function is the subset

$$\mathcal{G}_f = \{(x, f(x)) : x \in A\}$$

of $A \times B$.

From time to time, we will wish to specify an abstract function without specifying an exact formula or rule. In this case, we will just write $f : A \to B$, specifying the domain and codomain, but nothing else. We will also write $\mathcal{F}(A, B)$ for the set of all functions from A to B. Some texts use B^A instead for this set.

Given a function $f : A \to B$, and a subset $X \subseteq A$, we define the ***image*** of X to be the subset of B given by

$$f(X) = \{f(x) : x \in B\}.$$

If $Y \subseteq B$, we also define the ***inverse image*** of Y to be the subset of A given by

$$f^{-1}(Y) = \{x \in A : f(x) \in Y\}.$$

In other words $f^{-1}(Y)$ is the set of elements of A whose value lies in the set Y.

Given a function $g : A \to B$ and another function $f : B \to C$, we define the ***composition*** of f and g to be the function $f \circ g : A \to C$ defined by $(f \circ g)(x) = f(g(x))$.

A function is ***one-to-one*** or ***injective*** if it satisfies the condition

$$f(x_1) = f(x_2) \text{ implies } x_1 = x_2.$$

A function is ***onto*** or ***surjective*** if the range equals the entire codomain, or equivalently

$$f(A) = B.$$

A function which is both injective and surjective is called a ***bijective*** function.

A bijective function automatically has an ***inverse function*** $f^{-1} : B \to A$ defined by $f^{-1}(b) = a$ if and only if $f(a) = b$. The fact that f is onto guarantees that f^{-1} is defined on all of B, while the fact that f is injective ensures that f^{-1} is a function. It follows from the definition that $(f \circ f^{-1})(x) = x$ and $(f^{-1} \circ f)(x) = x$.

Proposition 1.2
Let A, B C and D be sets, and $f : A \to B$, $g : B \to C$ and $h : C \to D$ be functions. Then we have:

(i) Composition of functions satisfies an associative law: $(h \circ g) \circ f = h \circ (g \circ f)$.

(ii) If f and g are both one-to-one, then so is $g \circ f$.

(iii) If f and g are both onto, then so is $g \circ f$.

(iv) If f and g are both bijections, then so is $g \circ f$.

(v) If f is a bijection, then so is f^{-1}.

(vi) If f is a bijection $|A| = |B|$.

Proof:
The proof is left as an exercise. ■

Example 1.5
We could formally write the function $f(x) = \sqrt{x} + 1$ as:

$$\begin{aligned} f : [0, \infty) &\to \mathbb{R} \\ x &\mapsto \sqrt{x} + 1. \end{aligned}$$

As you would expect, the domain is $[0, \infty)$, the codomain is $\mathbb{R}$, the range is $[1, \infty)$, and the graph is the set of points

$$\{(x, \sqrt{x} + 1) : x \in [0, \infty)\}.$$

The function is one-to-one, but is not surjective or bijective. ◇

Exercises

1.3.1. Prove Proposition 1.2.

1.4 Permutations

A ***permutation*** of a set X is simply a re-arrangement of the elements, or more precisely a function p that maps each element of X to an element of X with no two distinct elements being mapped to the same element (and for infinite sets, we also need $p(X) = X$). Another way of saying this is that a permutation of X is simply a bijection $p : X \to X$.

Normally we are interested only in permutations of finite sets, and we really only care how many elements there are to permute. Hence it is customary to consider permutations of the set $\{1, 2, 3, ..., n\}$.

Since permutations are just functions,we can define them as we would any other function, by specifying the value that the function takes at each point in the domain. Unfortunately, unlike the usual functions you see in a calculus course, you usually can't specify permutations using a formula.

Example 1.6
The following function p is a permutation of the set $\{1, 2, 3, 4, 5, 6, 7, 8\}$:

$$\begin{array}{llll} p(1) = 2 & p(2)= 4 & p(3) = 6 & p(4)= 8 \\ p(5) = 7 & p(6)= 5 & p(7) = 3 & p(8)= 1 \end{array}$$

$\diamond$

A more compact way of writing down a permutation is to write it as an array of numbers, with 1, through n on the top row, and the respective image of each in the second row, like so:

$$p = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ p(1) & p(2) & p(3) & \dots & p(n) \end{pmatrix}$$

Example 1.7
The permutation p of the previous example can be written as follows:

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 4 & 6 & 8 & 7 & 5 & 3 & 1 \end{pmatrix}$$

$\diamond$

We denote the set of all permutations of $\{1, 2, 3, \dots, n\}$ by S_n.

Example 1.8
The set S_3 is

$$\left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}$$

$\diamond$

Note that, as in the above example, the ***identity permutation*** $p(k) = k$ is always a permutation.

Since every permutation is a one-to-one and onto function, there is an inverse function p^{-1} associated with every permutation p.

We can "multiply" two permutations by applying the first permutation, and then using the second permutation to permute the result. If p and q are permutations of the same set, $pq(k)$ is the what you get from applying q to $p(k)$, ie. $pq(k) = q(p(k))$, so $pq = q \circ p$ (note the reversal of terms in the product versus the composition).

Proposition 1.3
Let X be any set, and p and q be permutations of X, then

(i) p^{-1} *is a permutation of* X,

(ii) pq *is a permutation of* X,

(iii) the product satisfies an associative law: $(pq)r = p(qr)$.

Proof:
These follow immediately from Proposition 1.2: the inverse function of a bijection is a bijection, proving (i); the composition of bijective functions is a bijective function, proving (ii); and composition of functions is associative, so

$$(pq)r = r \circ (q \circ p) = (r \circ q) \circ p = p(qr),$$

proving (iii). ■

Example 1.9
Let

$$p = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \qquad \text{and} \qquad q = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

We can find pq fairly easily: for example if $k = 1$, we know that $p(1) = 3$, and $q(3) = 2$, so $pq(1) = 2$. Repeating for $k = 2$ and 3, we get So we have

$$pq = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

◇

Example 1.10
We listed all the elements of S_3 in Example 1.8. To simplify notation we will give each of these a symbol to identify it:

$$p_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad p_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \qquad p_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$
$$p_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \qquad p_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \qquad p_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

It is easy to verify that $p_0^{-1} = p_0$, $p_1^{-1} = p_2$, $p_2^{-1} = p_1$, $p_3^{-1} = p_3$, $p_4^{-1} = p_4$, and $p_5^{-1} = p_5$.

Just as with symmetries, we can write out a Cayley table for the products of these permutations:

	p_0	p_1	p_2	p_3	p_4	p_5
p_0	p_0	p_1	p_2	p_3	p_4	p_5
p_1	p_1	p_2	p_0	p_4	p_5	p_3
p_2	p_2	p_0	p_1	p_5	p_3	p_4
p_3	p_3	p_5	p_4	p_0	p_2	p_1
p_4	p_4	p_3	p_5	p_1	p_0	p_2
p_5	p_5	p_4	p_3	p_2	p_1	p_0

This product is not commutative.

It's probably not immediately obvious, but if you look closely you will see that the pattern of this Cayley table is exactly the same as the pattern of the Cayley table of Example 1.2, with the correspondences $p_0 \leftrightarrow I$, $p_1 \leftrightarrow R_1$, $p_2 \leftrightarrow R_2$, $p_3 \leftrightarrow H_0$, $p_4 \leftrightarrow H_1$, $p_5 \leftrightarrow H_2$. Indeed, the inverses of each element have the same pattern under these same correspondences.

In other words, if we look at these two examples abstractly, we seem to be getting the same underlying mathematical object.

This correspondence can be made even more concrete in the following way: if we label the vertices of the equilateral triangle of Example 1.2 with the numbers 1, 2 and 3, starting at $(0,0)$ and working clockwise, we find that the symmetries of the triangle permute the vertices in exactly the same way that the corresponding permutations permute the corresponding numbers. ◇

1.4.1 Cycles

Even with the current notation, expressing and working with permutations can be cumbersome. There is another, alternative, notation which can speed up the process of working with permutations. This notation works by looking at the ***cycles*** withing a permutation. If p is a permutation of the set X, the cycle of an element k of X in p is the sequence of elements $(k, p(k), p^2(k), \ldots, p^m(k))$ (where p^l is the product of p with itself l times) such that m is the smallest number such that, $p^{m+1}(k) = k$.

Note that the order of the elements in a cycle is important, but not where we start in the cycle. For example, we regard $(k, p(k), p^2(k), \ldots, p^m(k))$, $(p(k), p^2(k), \ldots, p^m(k), k)$, $(p^2(k), \ldots, p^m(k), k, p(k))$, etc. as representing the same cycle. If X is the set $\{1, 2, \ldots n\}$, it is usual to write a cycle starting with the smallest number in the cycle.

A cycle with m elements is called an m***-cycle***. A 2-cycle is sometimes called a ***transposition***, since it transposes two elements.

Example 1.11

In the following permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 4 & 6 & 8 & 7 & 5 & 3 & 1 \end{pmatrix}$$

we have $1 \to 2$, $2 \to 4$, $4 \to 8$ and $8 \to 1$, so $(1, 2, 4, 8)$ is a cycle. We could also write this cycle as $(2, 4, 8, 1)$, $(4, 8, 1, 2)$, or $(8, 1, 2, 4)$.

The smallest element not in this cycle is 3, and we have $3 \to 6$, $6 \to 5$, $5 \to 7$ and $7 \to 3$, so $(3, 6, 5, 7)$ is another cycle.

Since every element is in one of these two cycles, these are the only cycles in this permutation. ◇

If we find all of the cycles of a permutation, we can represent the permutation as a whole as a product of its cycles. But to do that we need to understand how to multiply cycles.

To work out how a product of cycles permutes a particular element k, all you need do is work from left to right until you find the element in a cycle, and then find the element which follows it in that cycle. You continue from left to right starting with the the next cycle looking for an occurrence of the new element. If there is, then you find the element which follows it in the cycle. Continue on in this fashion until you run out of cycles. The final value of the element is the image of k under the product of cycles.

Example 1.12

Consider the permutation $p = (1,3,5)(2)(4,6)$ of the set $\{1,2,3,4,5,6\}$. We can calculate $p(1)$ be looking at the first cycle, where we see that the element after 1 in that cycle is 3, and we also note that 3 does not occur in any cycle after the first, so $p(1) = 3$. Similarly, we have $p(2) = 2$, $p(3) = 5$, $p(4) = 6$, $p(5) = 1$ and $p(6) = 4$. This permutation could also be written as

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 5 & 6 & 1 & 4 \end{pmatrix}.$$

◇

Notice that there would be no difference in the above example if the cycle (2) was omitted. It is common practise to leave such single-element cycles out, particularly when the set which is being permuted is clear.

Example 1.13

Consider the product of cycles $p = (1,3,5)(2,3)(4,6,5)$ in the set $\{1,2,3,4,5,6\}$. We can calculate $p(1)$ be looking at the first cycle, where we see that the element after 1 in that cycle is 3; however 3 occurs in the second cycle, and the element after it in the cycle is 2; and 2 does not occur in the remaining cycle, so $p(1) = 2$. Similarly, we have $3 \to 5$ in the first cycle, and $5 \to 4$ in the last cycle, so $p(3) = 4$. Calculating everything out, we have $p(2) = 3$, $p(4) = 6$, $p(5) = 1$ and $p(6) = 5$. This permutation could also be written as

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 6 & 1 & 5 \end{pmatrix},$$

or more simply in cycle notation as $(1,2,3,4,6,5)$. ◇

Any permutation can be written as a product of the cycles it contains.

Theorem 1.4

Every permutation of S_n can be written as a product of disjoint cycles. (Two cycles are disjoint if they have not elements in common.)

Proof:

Let p be a permutation of S_n. We let c_1 be the cycle which includes 1,

$$c_1 = \{1, p(1), p^2(1), \ldots, p^{m_1}(1)\},$$

and we let p_1 be the permutation defined by

$$p_1(k) = \begin{cases} k & \text{if } k \in c_1, \\ p(k) & \text{otherwise.} \end{cases}$$

Then it is clear that $p = c_1 p_1$.

Now if we have written $p = c_1 \dots c_l p_l$, where $c_1, \dots,\ c_l$ are disjoint cycles, and p_l is a permutation which satisfies has $p_l(k) = k$ whenever k is in one of the cycles, then one of two things must be true: either every element of $\{1, 2, \dots, n\}$ is an element of one of the cycles, or there is some smallest element k_l which is not in any of the cycles.

In the first case, we have that p_l must be the identity permutation, so $p = c_1 \dots c_l$, and we are done.

In the second case, we let c_{l+1} be the cycle including k_l,

$$c_{l+1} = \{k_l, p(k_l), p^2(k_l), \dots, p^{m_l}(k_l)\},$$

and let p_{l+1} be the permutation defined by

$$p_{l+1}(k) = \begin{cases} k & \text{if } k \text{ is an element of any cycle } c_1,\, c_2, \dots, c_{l+1} \\ p(k) & \text{otherwise.} \end{cases}$$

Then $p = c_1 \dots c_{l+1} p_{l+1}$.

Since $\{1, 2, 3, \dots, n\}$ is a finite set, an induction argument using this construction proves the result. ■

Example 1.14

The permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 4 & 6 & 8 & 7 & 5 & 3 & 1 \end{pmatrix}$$

can be written as $(1, 2, 4, 8)(3, 6, 5, 7)$ or $(3, 6, 5, 7)(1, 2, 4, 8)$, or in many other ways. The first is the standard form. ◇

Example 1.15

The elements of S_3 can be represented in cycle form as follows:

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = (1)(2)(3) \qquad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1, 3, 2) \qquad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1, 2, 3)$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (1)(2, 3) \qquad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1, 2)(3) \qquad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1, 3)(2)$$

◇

It is often convenient to simply always work with the cycle form of a permutation. We can calculate the product of two permutations in cycle notation by writing all long product of cycles, and then reducing to the standard form of the cycles.

Example 1.16

Let $p = (1,4,6)(3,5)$ and $q = (1,2,4)(3,6,5)$. Then pq is given by the product of cycles $(1,4,6)(3,5)(1,2,4)(3,6,5)$.

Starting with 1, we see that $1 \to 4 \to 1$, so the first cycle of the standard form is just (1).

Looking at 2 next, we have $2 \to 4$, so the next cycle starts $(2,4,\ldots)$. Looking at 4, we get $4 \to 6 \to 5$, so 5 is the next entry, and the cycle is starting $(2,4,5,\ldots)$. Now starting with 5 we get $5 \to 3 \to 6$, so 6 is next in the cycle. Continuing in this manner we get $6 \to 1 \to 2$, and 2 is the start of the cycle, so the finished cycle is $(2,4,5,6)$.

The only remaining number is 3, so (3) must be the last cycle.

Hence $pq = (1)(2,4,5,6)(3)$, which we will usually just write as $pq = (2,4,5,6)$.

Similarly we have that $qp = (1,2,4)(3,6,5)(1,4,6)(3,5)$, and we have $1 \to 2$, $2 \to 4 \to 6$, $6 \to 5 \to 3$ and $3 \to 6 \to 1$, so the first cycle is $(1,2,6,3)$. Similarly, we have $4 \to 1 \to 4$, so (4) is a cycle. Finally 5 is the only element remaining, so (5) is a cycle. Hence $qp = (1,2,6,3)(4)(5) = (1,2,6,3)$. ◇

1.4.2 Parity

Informally, if we compare the permuations

$$\begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix} \qquad \text{and} \qquad \begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix},$$

we observe that the first “rotates” the elements to the right, while the second “reflects” the elements. Indeed, if we consider the correspondence between these permutations and the symmetries of a triangle discussed in Example 1.10, we see that the first corresponds to a rotation, and the second to a reflection. In this section, we will generalize this idea to arbitrary permutations.

The starting point of this discussion is a comparison between the following two products: if $p \in S_n$ we define

$$D_n = \prod_{1 \le i < j \le n} (j - i)$$

and

$$D(p) = \prod_{1 \le i < j \le n} (p(j) - p(i)).$$

Given any pair of distinct elements $k, l \in \{1, 2, \ldots, n\}$, both of these products contain exactly one factor which is a difference of k and l. This is easy to see in the product D_n, but a little thought will convince you that it is also the case for $D(p)$. The difference between the two products is that in $D(p)$ it may not necessarily be the larger term minus the smaller term. Hence D_n and $D(p)$ have the same magnitude, but may differ in sign.

Definition 1.2
Let $p \in S_n$. The ***parity*** *of p is*

$$\text{parity}(p) = \frac{D(p)}{D_n}.$$

Clearly the parity of p is 1 if $D(p) > 0$ and -1 if $D(p) < 0$.

Example 1.17
Consider the permutations

$$p = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \qquad \text{and} \qquad q = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

In both cases

$$D_3 = (3-1)(3-2)(2-1) = 2 \times 1 \times 1 = 2.$$

Now

$$\begin{aligned} D(p) &= (p(3)-p(1))(p(3)-p(2))(p(2)-p(1)) = (2-3)(2-1)(1-3) \\ &= -1 \times 1 \times -2 = 2, \end{aligned}$$

so

$$\text{parity}(p) = 2/2 = 1.$$

On the other hand,

$$\begin{aligned} D(q) &= (q(3)-q(1))(q(3)-q(2))(q(2)-q(1)) = (1-3)(1-2)(2-3) \\ &= -2 \times -1 \times -1 = -2, \end{aligned}$$

so

$$\text{parity}(q) = -2/2 = -1.$$

◇

Calculating the parity in the last example was fairly straightforward, but calculating the parity of a general permutation can be quite time consuming: a simple counting argument tells us that if $p \in S_n$ we have $n(n-1)/2$ terms in the product $D(p)$. We need a better way to calculate the parity.

It turns out that there is nothing particularly special about D_n in the definition of parity. Let $(x_1, x_2, \ldots, x_n)$ be a sequence of distinct numbers, and p a permutation of $\{1, 2, \ldots n\}$. We define

$$p(x_1, x_2, \ldots, x_n) = (x_{p(1)}, x_{p(2)}, \ldots, x_{p(n)}), \tag{1.1}$$

and

$$D(x_1, x_2, \dots, x_n) = \prod_{1 \le i < j \le n} (x_j - x_i).$$

The following technical lemma shows that we can use these instead to find the parity of p.

Lemma 1.5
If p is a permutation in S_n, then

$$\text{parity}(p) = \frac{D(x_{p(1)}, x_{p(2)}, \dots, x_{p(n)})}{D(x_1, x_2, \dots, x_n)}.$$

We say that p is an ***even permutation*** *if* $\text{parity}(p) = 1$, *and p is an* ***odd permutation*** *if* $\text{parity}(p) = -1$.

Proof:
See Section 1.6.2. ■

Note that $D_n = D(1, 2, \dots, n)$, and $D(p) = D(p(1), p(2), \dots, p(n))$.
With this lemma in hand, we can easily prove the following important result:

Theorem 1.6
Let p and $q \in S_n$. Then

$$\text{parity}(pq) = \text{parity}(p)\,\text{parity}(q).$$

Proof:
The key observation here is that if we have permutations p and q, then

$$\text{parity}(p) = \frac{D(pq)}{D(q)}.$$

Letting $a_k = q(k)$, so that

$$D(pq) = D(q(p(1)), q(p(2)), \dots, q(p(n))) = D(a_{p(1)}, \dots, a_{p(n)}),$$

and

$$D(q) = D(a_1, \dots, a_n),$$

the lemma tells us that

$$\text{parity}(p) = \frac{D(a_{p(1)}, \dots, a_{p(n)})}{D(a_1, \dots, a_n)} = \frac{D(pq)}{D(q)}.$$

It is immediate form this that

$$\text{parity}(p) \times \text{parity}(q) = \frac{D(pq)}{D(q)} \times \frac{D(q)}{D_n} = \frac{D(pq)}{D_n} = \text{parity}(pq).$$

■

Thinking in terms of cycles also helps us to calculate the parity of a permutation, as this result shows:

Theorem 1.7
Let $c = (k_1, k_2, \ldots, k_m)$ *be a cycle. Then*

$$\text{parity}(c) = \begin{cases} 1 & \textit{if } m \textit{ is odd} \\ -1 & \textit{if } m \textit{ is even.} \end{cases}$$

Proof:

First we observe that if $p = (1, 2)$, then all the factors in $D(p)$ are positive, except for $p(2) - p(1) = 1 - 2 = -1$. Hence $D(p)$ is negative, so $\text{parity}(p) = -1$.

Now if $i, j > 2$, and $i \neq j$, then simple checking shows that $(i, j) = (1, i)(2, j)(1, 2)(1, i)(2, j)$, and, given this fact, the previous theorem tells us

$$\begin{aligned} \text{parity}((i, j)) &= \text{parity}((1, i)(2, j)) \times \text{parity}(1, 2) \times \text{parity}((1, i)(2, j)) \\ &= -\text{parity}((1, i)(2, j))^2 \\ &= -1 \end{aligned}$$

Finally, we observe that

$$c = (k_1, k_2, \ldots, k_m) = (k_1, k_m)(k_2, k_m) \cdots (k_{m-1}, k_m), \tag{1.2}$$

and so

$$\begin{aligned} \text{parity}(c) &= \text{parity}((k_1, k_m)) \times \text{parity}((k_2, k_m)) \times \cdots \times \text{parity}((k_{m-1}, k_m)) \\ &= (-1)^{m-1} \\ &= \begin{cases} 1 & \text{if } m \text{ is odd} \\ -1 & \text{if } m \text{ is even.} \end{cases} \end{aligned}$$

■

Corollary 1.8
A permutation p is even iff when it is expressed as a product of cycles there are an even number of commas in the expression.

Another interesting fact that can be squeezed out of the previous theorem is the following:

Proposition 1.9
Any permutation p can be written as a product of 2*-cycles, and the number of* 2*-cycles is even iff p is even.*

Proof:

The first fact follows from the fact that every permutation can be written as a product of cycles, and equation (1.2) shows that every cycle is a product of 2-cycles.

The second follows from the previous corollary, coupled with the fact that every 2-cycle has a single comma. ■

Example 1.18

Let p_0, $p_1, \ldots, p_5$ be as in Example 1.10. Then $\text{parity}(p_0) = \text{parity}(p_1) = \text{parity}(p_2) = 1$, and $\text{parity}(p_3) = \text{parity}(p_4) = \text{parity}(p_5) = -1$.

Observe that the “reflections” have parity -1, while the “rotations” have parity 1. ◇

Example 1.19

The permutation

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 5 & 2 & 7 & 8 & 6 & 1 & 4 & 10 & 9 \end{pmatrix},$$

can be written as $p = (1,3,2,5,8,4,7)(9,10)$, and since it has 7 commas in the expression, it has parity -1. ◇

1.4.3 Permutation Matrices

Another way of looking at permutations is very closely related to Equation 1.1.

Since $x = (x_1, x_2, \ldots, x_n)$ is a vector in $\mathbb{R}^n$, the function it implicitly defines, $T_p : \mathbb{R}^n \to \mathbb{R}^n$, where

$$T_p x = (x_{p(1)}, x_{p(2)}, \ldots, x_{p(n)})$$

is a linear transformation:

$$\begin{aligned} T_p(x+y) &= (x_{p(1)} + y_{p(1)}, x_{p(2)} + y_{p(2)}, \ldots, x_{p(n)} + y_{p(n)}) \\ &= (x_{p(1)}, x_{p(2)}, \ldots, x_{p(n)}) + (y_{p(1)}, y_{p(2)}, \ldots, y_{p(n)}) = T_p x + T_p y \end{aligned}$$

and

$$\begin{aligned} T_p(\lambda x) &= (\lambda x_{p(1)}, \lambda x_{p(2)}, \ldots, \lambda x_{p(n)}) \\ &= \lambda(x_{p(1)}, x_{p(2)}, \ldots, x_{p(n)}) = \lambda T_p x. \end{aligned}$$

Let e_k be the kth standard orthonormal basis vector in $\mathbb{R}^n$, ie. e_k is the vector with 0 in every entry except the kth entry, which is 1. By looking at the image of each standard basis vector e_k under the transformation T_p, we can find a corresponding $n \times n$ matrix which we will also call T_p. We note that $T_p e_k$ has zeroes in every entry except the $p^{-1}(k)$th entry, which is 1. Hence $T_p e_k = e_{p^{-1}(k)}$, so T_p always takes basis vectors to basis vectors.

Example 1.20

If $p = (1,2,3) \in S_3$, then

$$T_p = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

◇

Proposition 1.10
Let $p \in S_n$ be a permutation. Then

(i) T_p is an orthogonal matrix

(ii) T_p is the matrix with 1s in the $p^{-1}(k)$th row of the kth column, for $k = 1, 2, \ldots, n$, and 0 everywhere else.

(iii) T_p is the matrix with 1s in the $p(k)$th column of the kth row, for $k = 1, 2, \ldots, n$, and 0 everywhere else.

(iv) $T_e = I_n$.

(v) $T_p T_q = T_{pq}$.

(vi) $T_p^{-1} = T_{p^{-1}}$.

Proof:

(i) is immediate since every column of T_p is a standard orthonormal basis vector, and each vector in the basis occurs exactly once.

(ii) this is immediate from the fact that the kth column is the column vector $e_{p^{-1}(k)}$.

(iii) using part (ii), we know that is $k = p^{-1}(j)$, then the entry in the kth row and jth column is 1. But $k = p^{-1}(j)$ if and only if $j = p(k)$, so the $p(k)$th column of the kth row is 1, and all other entries in the row are 0.

(iv) the kth row of T_e is e_k, so T_e has 1 in diagonal entries and 0 everywhere else, so $T_e = I$.

(v) Looking at the standard basis vectors, we have

$$T_{pq} e_k = e_{(pq)^{-1}(k)} = e_{p^{-1}(q^{-1}(k))} = T_p e_{q^{-1}(k)} = T_p T_q e_k.$$

Since any vector v is a linear combination of basis vectors, and the transformations T_p, T_q and T_{pq} are all linear, we have that $T_{pq} v = T_p T_q v$ for any vector v, and so $T_p T_q = T_{pq}$.

(vi) Since T_p is orthogonal, it is invertible, and $T_p^{-1} e_{p^{-1}(k)} = e_k$. Now $j = p^{-1}(k)$ if and only if $k = p(j)$, so

$$T_p^{-1} e_j = e_k = e_{p(j)} = e_{(p^{-1})^{-1}(j)} = T_{p^{-1}} e_j.$$

As in part (v), it is sufficient to show that this occurs for every basis vector to be able to conclude that $T_p^{-1} = T_{p^{-1}}$. ■

Example 1.21

We know that in S_3, if $p = (1, 2, 3)$ and $q = (1, 2)$, then $pq = (2, 3)$. The corresponding permutation matrices are

$$T_p = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \qquad T_q = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \qquad T_{pq} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

and matrix multiplication confirms that $T_p T_q = T_{pq}$. ◇

Exercises

1.4.1. Let

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 2 & 5 & 1 & 6 & 3 \end{pmatrix} \qquad \text{and} \qquad q = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 1 & 2 & 6 \end{pmatrix}.$$

Find pq and qp. Write both permutations using cycle notation. Write down the permutation matrices T_p and T_q. Determine the parity of p and q.

1.4.2. Let $p = (1, 5, 3, 2)(4, 6, 8)$ and $q = (1, 7, 4, 3)(8, 2)(5, 6)$. Find pq and qp. Write both permutations using array notation. Write down the permutation matrices T_p and T_q. Determine the parity of p and q.

1.4.3. How many distinct permutations are there of the set $\{1, 2, \ldots, n\}$? (Hint: they're called *permutations*.)

1.4.4. Let $p \in S_3$. Use the Cayley table for S_3 to show that p^6 is always the identity permutation.

1.4.5. Write down all the elements of S_4 in array, cycle and matrix form. Calculate the parity of each element. Find the inverse of each element. Choose 5 pairs of non-identity elements, and calculate their product.

1.4.6. Let $c = (k_1, k_2, \ldots, k_m)$ be a cycle. What is c^{-1}? Use your answer to calculate the inverse of the permutation $p = (1, 3, 4)(2, 5)$.

1.4.7. Show that $D_n = (n-1)!(n-2)! \ldots 2!1!$.

1.4.8. Show that exactly half the permutations of S_n are even, and half are odd.

1.4.9. (*) Show that S_4 and the set of symmetries of a regular tetrahedron (see Exercise 1.1.5) correspond in the same way as S_3 and the set of symmetries of an equilateral triangle.

Hint: you could do this by calculating all 576 entries in the Cayley table of each, and comparing the two; however it is more practical to find some way to classify the elements of each in a way which makes the correspondence clear.

1.4.10. (*) Let $\Omega \subseteq \mathbb{R}^3$ be the equilateral triangle with vertices $(1, 0, 0)$, $(0, 1, 0)$ and $(0, 0, 1)$. Show that every symmetry $S \in \mathrm{Sym}(\Omega)$ is a linear transformation, and that there is a permutation $p_S \in S_3$ such that $S = T_{p_S}$. Show that the correspondence $S \mapsto p_S$ preserves multiplication and inverses, ie. $T_{p_S p_R} = SR$, $T_{p_S^{-1}} = S^{-1}$.

1.4.11. (*) Let $|A|$ denote the determinant of the matrix A. Prove that $|T_p| = \mathrm{parity}(p)$.

1.4.12. (**) Write a computer program that calculates and prints out the Cayley table for S_4. Generalize it to print out the Cayley table for S_n for any n.

1.5 Modulo Arithmetic

We say that two numbers x and y are ***equal (modulo** m**)*** if x and y differ by a multiple of m, and we write

$$x \equiv y \pmod{m}$$

to denote this situation. Another equivalent (and useful) way to think of this situation is that x and y have the same remainder when you divide by m. Since any number greater than m is equal (modulo m) to a number less than m, it is customary when working modulo m to reduce your answer to a number in the range $[0, m)$.

For example

$$-1 \equiv 7 \equiv 1023 \pmod{8},$$

and we would usually write any of these three numbers as $7 \mod 8$ if it were the solution to a problem.

When we are working modulo m, we can perform the operations of addition, multiplication and subtraction as normal, but we reduce our answers to the range $[0, m)$. Indeed, in complicated expressions, one can reduce at intermediate steps to simplify calculations:

$$7 \times 6 + 4 \times 3 \equiv 42 + 12 \equiv 54 \equiv 6 \pmod{8}$$

could be instead calculated as

$$7 \times 6 + 4 \times 3 \equiv 42 + 12 \equiv 2 + 4 \equiv 6 \pmod{8}.$$

Division is a trickier topic, but since we are usually performing modulo arithmetic with integers the naïve way of defining modulo division does not make sense in most cases. Nevertheless, we will see later on that in some cases division does make sense.

We can write out addition and multiplication tables for operations modulo some base, and we call these Cayley tables, just as before.

Example 1.22

The addition and multiplication tables, modulo 6 are as follows:

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

×	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	2	3	1

◇

Exercises

1.5.1. Write down the addition and multiplication tables modulo 5 and modulo 8.

1.5.2. Recall that two natural numbers p and q are ***coprime*** if their highest common factor is 1. Show that if k and m are coprime, then $xk \equiv 0 \pmod{m}$ if and only if x is an integer multiple of m.

1.6 Addendum: Technical Details

We now provide the technical proofs that were omitted from earlier discussions in this chapter.

1.6.1 Symmetry

In Proposition 1.1 we make use of the following fact.

Lemma 1.11
If T is a function from $\mathbb{R}^n$ to $\mathbb{R}^n$ that preserves distance, then T is one-to-one and onto.

Proof:
If $T(x_1) = T(x_2)$ then $d(T(x_1), T(x_2)) = 0$ so the fact that T preserves distances means that $d(x_1, x_2) = 0$. But this implies that $x_1 = x_2$, so T is one-to-one.

If x, y and $z \in \mathbb{R}^n$ are the vertices of a triangle, then $T(x)$, $T(y)$ and $T(z)$ are vertices of a triangle as well, and since $d(T(x), T(y)) = d(x, y)$, $d(T(x), T(z)) = d(x, z)$, and $d(T(y), T(z)) = d(y, z)$, the triangles are congruent. From this observation, it follows that any parallelogram x,y, z, $w \in \mathbb{R}^n$ is congruent to the corresponding parallelogram $T(x)$,$T(y)$, $T(z)$, $T(w)$.

If $T(0) = 0$ then this means that in particular, the parallelogram 0, x, $x + y$, y is congruent to the parallelogram 0, $T(x)$, $T(x + y)$, $T(y)$. Therefore, comparing opposite sides, $T(y) = T(x + y) - T(x)$, or $T(x + y) = T(x) + T(y)$. Also, the "triangle" with vertices 0, x, λx is congruent to the triangle with vertices 0, $T(x)$, $T(\lambda x)$, but since the vertices of the first triangle are collinear, so must the vertices of the second, so $T(\lambda x)$ is a scalar multiple of $T(x)$, and $d(T(\lambda x), 0) = |\lambda| d(x, 0)$, so $T(\lambda x) = \pm\lambda x$. However, if $T(\lambda x) = -\lambda x$, then looking at the corresponding sides x to λx and $T(x)$ to $T(\lambda x)$, we would have $d(T(\lambda x), T(x)) = |\lambda + 1| d(x, 0)$, rather than $|\lambda - 1| d(x, 0)$.

Hence if $T(0) = 0$, T is a linear transformation, and a linear transformation from $\mathbb{R}^n$ to $\mathbb{R}^n$ which preserves distance is orthogonal and hence onto.

If $T(0) = c$, then the function $S(x) = T(x) - c$ preserves distances, and $S(0) = 0$, so S is orthogonal and hence onto. But then $T(x) = S(x) + c$, so given any y, there is some x such that $S(x) = y - c$, and so $T(x) = S(x) + c = (y - c) + c = y$. Hence T is onto. ■

1.6.2 Parity

Proof (Lemma 1.5):

Given any number $k \in \{1, 2, \ldots, n\}$, let $a_k = p^{-1}(k)$. Then given any $k > l$, we have that $k = p(a_k)$ and $l = p(a_l)$.

If $a_k > a_l$, in which case the corresponding terms in each of the sums D_n, $D(p)$, $D(x_1, \ldots, x_n)$ and $D(x_{p(1)}, \ldots, x_{p(n)})$ are, respectively, $k - l$, $p(a_k) - p(a_l)$, $x_k - x_l$, and $x_{p(a_k)} - x_{p(a_l)}$, with the first two being equal and the second two being equal, and so these terms in the quotients $D(p)/D_n$ and $D(x_{p(1)}, \ldots, x_{p(n)})/D(x_1, \ldots, x_n)$, respectively, cancel each other out.

On the other hand, if $a_k < a_l$, the corresponding terms in each of the sums D_n, $D(p)$, $D(x_1, \ldots, x_n)$ and $D(x_{p(1)}, \ldots, x_{p(n)})$ are, respectively, $k - l$, $p(a_l) - p(a_k)$, $x_k - x_l$, and $x_{p(a_l)} - x_{p(a_k)}$, with the first two being negatives and the second two being negatives, and so these terms in the quotients $D(p)/D_n$ and $D(x_{p(1)}, \ldots, x_{p(n)})/D(x_1, \ldots, x_n)$, respectively, give a factor of -1.

Hence the number of terms giving each of the factors 1 and -1 in each quotient are equal, so

$$\text{parity}(p) = \frac{D(p)}{D_n} = \frac{D(x_{p(1)}, x_{p(2)}, \ldots, x_{p(n)})}{D(x_1, x_2, \ldots, x_n)}.$$

■

Assignment 1

The following exercises are due Friday, Februrary 13.

1.1 Exercises 1, 4.

1.2 Exercise 2.

1.4 Exercises 1, 2, 3, 6.

1.5 Exercise 1.

Chapter 2

Groups

Algebra concerns the abstraction of simple arithmetic operations to situations where the quantities involved are unknown. In this endeavour, we discover that there are certain rules which always apply, such as the commutative and associative laws of addition and multiplication, and that these laws allow us to manipulate and simplify algebraic expressions. As we learn more mathematics, we see similar rules appear over and over again.

In abstract algebra, instead of concentrating on specific algebraic settings (such as algebra with numbers, vectors or, now, permutations or symmetries) we instead look at the *rules* of algebra and ask what we can infer from reasonable collections of such rules. We can then apply the knowledge so gained to a surprisingly wide collection of concrete situations which happen to satisfy such rules.

You may have already seen such an approach in linear algebra, where one eventually considers abstract vector spaces (as opposed to concrete ones, such as $\mathbb{R}^n$). One then finds that, for example, that differentiable functions form a vector space, and that differentiation and integration are linear transformations, giving new (and quite important) insight into calculus.

Our starting point, then will be the ***group***, an object which encapsulates a reasonable set of rules for a single algebraic operation.

2.1 Binary Operations

A ***binary operation*** is a type of function that we shall be using regularly. A binary operation $*$ is simply a function

$$\begin{aligned} * : A \times B &\to C \\ (x, y) &\mapsto x * y. \end{aligned}$$

The distinction lies in that instead of using “function-style” notation $*(x, y)$, it is traditional to write binary operations “in-line” as $x * y$. Often A, B and C

are the same set, in which case we say that a binary operation $* : A \times A \to A$ is a ***binary operation on*** A.

A binary operation on A is ***commutative*** if

$$x * y = y * x$$

for all x, $y \in A$. It is ***associative*** if

$$(x * y) * z = x * (y * z) = x * y * z.$$

for all x, y and $z \in A$.

Lemma 2.1

Let $* : A \times A \to A$ be an associative binary operation. Then no matter where you put parentheses in the product $x_1 * x_2 * \cdots * x_n$, you get the same result.

Proof:

We prove this by induction. Since the operation is associative, it is true for $n \leq 3$ automatically.

Now assume that this is true for all $n < k$. We need to show that for any choice of i and j with $1 \leq i < j < k$, we have

$$(x_1 * \cdots * x_i) * (x_{i+1} * \cdots * x_k) = (x_1 * \cdots * x_j) * (x_{j+1} * \cdots * x_k)$$

(we do not need to worry about where the parentheses go inside each factor, since they are products of less than k terms). Now we know that

$$(x_1 * \cdots * x_i) * (x_{i+1} * \cdots * x_k) = (x_1 * \cdots * x_i) * ((x_{i+1} * \cdots * x_j) * (x_{j+1} * \cdots * x_k))$$

since the second term is a product of less than k terms. Similarly

$$(x_1 * \cdots * x_j) * (x_{j+1} * \cdots * x_k) = ((x_1 * \cdots * x_i) * (x_{i+1} * \cdots * x_j)) * (x_{j+1} * \cdots * x_k).$$

But $*$ is associative, so

$$\begin{aligned}(x_1 * \cdots * x_i) &* ((x_{i+1} * \cdots * x_j) * (x_{j+1} * \cdots * x_k)) \\ &= y_1 * (y_2 * y_3) \\ &= (y_1 * y_2) * y_3 \\ &= ((x_1 * \cdots * x_i) * (x_{i+1} * \cdots * x_j)) * (x_{j+1} * \cdots * x_k),\end{aligned}$$

and we have proven equality of the two expressions.

By induction, the result follows for any k. ■

An element e of A is an ***identity*** for the binary operation if

$$e * x = x \qquad \text{and} \qquad x * e = x$$

for every $x \in A$. More generally, one can have a ***left identity*** e which merely satisfies

$$e * x = x$$

for every x. A ***right identity*** is defined analagously.

Lemma 2.2
If $* : A \times A \to A$ is a binary operation, and e is an identity for $*$, then it is the only identity element.

Proof:
Assume that there is another element e' so that $e' * x = x * e' = x$. Then in particular, if we let $x = e$, we have $e' * e = e$. But by assumption, e is an identity, and so $e' * e = e'$. Hence $e = e'$. ■

Notationally, if $*$ behaves in a "multiplication-like" fashion, or it is clear from context which binary operation we are using, we will often simply write xy for $x * y$.

Example 2.1
The addition operation is a binary operation in the integers

$$\begin{aligned} + : \mathbb{Z} \times \mathbb{Z} &\to \mathbb{Z} \\ (x, y) &\mapsto x + y. \end{aligned}$$

In this case we could write $+(2, 3) = 2 + 3 = 5$. Addition is, of course, both associative and commutative. 0 is an identity for addition. In fact addition is also an associative and commutative binary operation on any of the standard number systems, and if 0 is in the number system, then 0 is an identity. ◇

Example 2.2
Multiplication is a binary operation on the set $\mathbb{R}$, and it is associative and commutative, and 1 is an identity. Again, like addition, multiplication is comuntative and associative on any of the standard number systems, and if 1 is in the number system, then 1 is an identity. ◇

Example 2.3
If we consider the set $M_n(\mathbb{R})$ of $n \times n$ real-valued matrices, then matrix addition and matrix multiplication are binary operations. Both operations are associative, but only matrix addition is commutative. The zero matrix is an identity for addition, the identity matrix I_n (the matrix with 1 down the diagonal and 0 elsewhere) is an identity for matrix multiplication.

We also have scalar multiplication as a binary operation $\mathbb{R} \times M_n(\mathbb{R}) \to M_n(\mathbb{R})$. This cannot be commutative or associative, but it does have 1 as a left identity. ◇

Example 2.4
More generally, the inner or dot product on $\mathbb{R}^n$ is a binary operation $\cdot : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$ which is commutative, but cannot be associative (since the codomain is $\mathbb{R}$, and one cannot take a dot product of an element of $\mathbb{R}$ and an element of $\mathbb{R}^n$). Similarly, there is no identity element of any sort. ◇

Example 2.5

One can define arbitrary binary products which are of little or no interest. For example, $x * y = e^x(x + \sin(y))$ is a binary product. But it is neither associative, commutative, nor has an identity. So clearly simple binary operations are not enough to encapsulate the sorts of rules that we expect algebraic operations to have. ◇

Exercises

2.1.1. Let $* : A \times A \to A$ be a commutative binary operation. If e is a left identity, show that it also a right identity (and hence simply an identity).

2.1.2. Let X be any set, and let $\mathcal{P}(X)$ be the power set of X (ie. the set of all subsets of X). Show that $\cup : \mathcal{P}(X) \times \mathcal{P}(X) \to \mathcal{P}(X)$ is an associative, commutative binary operation, and that $\emptyset$ is an identity for this operation.

Similarly, show that $\cap : \mathcal{P}(X) \times \mathcal{P}(X) \to \mathcal{P}(X)$ is an associative, commutative binary operation, and that X is an identity for this operation.

2.1.3. Let $* : A \times A \to A$ be an associative and commutative binary operation. Show that for any product of n elements $x_1, x_2, \ldots, x_n \in A$, no matter what the order of elements in the product

$$x_1 * x_2 * \cdots * x_n$$

the result is the same.

2.2 Groups

If you look at the discussion of symmetries and permutations, you will note that not only was there a binary operation, but there was an inverse. We should have some model for this additional operation.

A ***group***, $\mathbf{G} = (G, *, e)$, consists of a set G, a binary operation $* : G \times G \to G$, and an element $e \in G$ satisfying the following three conditions:

(i) $*$ is associative

(ii) e is an identity for $*$

(iii) every element $x \in G$ has an ***inverse element*** $x^{-1} \in G$ such that $x * x^{-1} = x^{-1} * x = e$.

We call $*$ the ***group operation***.

Note that there is no requirement that the group operation is commutative. If it does happen to be commutative, then we say that the group is an ***commutative*** or ***Abelian group***.

This means that in general $x * y$ and $y * x$ are distinct elements, but sometimes they are not. If

$$x * y = y * x$$

for a particular x and $y \in G$, we say that x and y ***commute***.

A number of different notations are used when working with groups elements. Most commonly we will omit the group operation entirely and simply write xy for $x * y$, just as is done for multiplication. In this case we use the following clear notation for repeated applications of the group operations:

$$x^k = \underbrace{xxx\cdots x}_{k \text{ times}}$$

for any natural number k. To make this notation mesh nicely with the expected behaviour of power laws, we define

$$x^{-k} = (x^{-1})^k \qquad \text{and} \qquad x^0 = e.$$

When then have the standard power laws

$$x^m x^k = x^{m+k} \qquad \text{and} \qquad (x^m)^k = x^{mk},$$

for any integers m and k. Its also not hard to see that $(x^k)^{-1} = x^{-k}$. However, we have that

$$(xy)^k \neq x^k y^k$$

in general. In the case that x and y commute, then we do have equality.

In the case of Abelian groups, we will sometimes instead use an additive notation. We use $+$ for the group operation, and we customarily write the identity element as 0, and the inverse element of x as $-x$. We then use the notation

$$kx = \underbrace{x + x + \cdots + x}_{k \text{ times}}$$

for any natural number k, and

$$-kx = k(-x) \qquad \text{and} \qquad 0x = 0.$$

We then have the natural rules that

$$kx + mx = (k+m)x, \qquad k(mx) = (km)x \qquad \text{and} \qquad kx + ky = k(x+y)$$

for any integers k and m.

If the set G has a finite number of elements, we say that the ***order*** of the group is the number of elements of G. If G is an infinite set, we say that the group has infinite order. We denote the order of the group by $|G|$.

Example 2.6 (Addition and Multiplication)

Since a principle motivation for the definition of groups are standard algebraic operations, it should be no surprise that the following are all Abelian groups:

- the additive group of real numbers $(\mathbb{R}, +, 0)$

- the additive group of complex numbers $(\mathbb{C}, +, 0)$
- the additive group of rational numbers $(\mathbb{Q}, +, 0)$
- the additive group of integers $(\mathbb{Z}, +, 0)$
- the multiplicative group of real numbers $(\mathbb{R} \setminus \{0\}, \times, 1)$
- the multiplicative group of complex numbers $(\mathbb{C} \setminus \{0\}, \times, 1)$
- the multiplicative group of rational numbers $(\mathbb{Q} \setminus \{0\}, \times, 1)$
- the multiplicative group of integers $(\mathbb{Z} \setminus \{0\}, \times, 1)$
- the multiplicative group of natural numbers $(\mathbb{N}, \times, 1)$

Note that for the multiplicative groups, we need to exclude 0, since 0 has no multiplicative inverse.

All of these groups have infinite order. ◇

Example 2.7 (Modulo Addition)

If m is any natural number, the additive group of integers modulo m is the group $\mathbb{Z}_m = (\{0, 1, 2, \ldots, m-1\}, +, 0)$, where addition is performed modulo m. To confirm that it is a group, we need to check that the axioms hold.

Associativity follows from the fact that regular addition is associative and commutative. Given x, y and z, we have $x + y = a + km$ for some a and k, so $(x + y) + z \equiv a + z \pmod{m}$. But $y = a - x + km$, so $y + z \equiv a - x + z \pmod{m}$, and hence $x + (y + z) \equiv x + a - x + z \equiv a + z \pmod{m}$.

The fact that 0 is an identity is trivial: $0 + x = x$, so $0 + x \equiv x \pmod{m}$ follows immediately.

If $x \in \{1, 2, \ldots, m-1\}$, we know that $-x \equiv m - x \pmod{m}$, and so $(m - x) + x \equiv 0 \pmod{m}$ and $x + (m - x) \equiv 0 \pmod{m}$. Also 0 is its own inverse. So every element has an inverse.

These groups are also clearly Abelian, since regular addition is commutative.

The order of $\mathbb{Z}_m$ is m. ◇

The previous example shows that there are groups of all orders except 0.

Example 2.8

Multiplication modulo m does not, in general, give a group structure. Multiplication modulo m is associative, and 1 is an identity. We have to exclude 0 from the group, because it clearly does not have a multiplicative inverse, but even with this restriction, some other elements may not have multiplicative inverses.

If you consider multiplication modulo 6, as in Example 1.22, you can see that there are no inverses for 2, 3, and 4, since none of them have a number which you can multiply them by to give 1. Indeed, there is a somewhat deeper problem in that some products give 0, which cannot be an element of the group.

Multiplication modulo m *does* sometimes give you a group, however. The multiplication table (omitting 0) for multiplication modulo 5 is as follows:

×	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

A quick check shows that every element has an inverse. Hence $(\{1,2,3,4\},\times,1)$ is a group, where $\times$ is multiplication modulo 5. ◇

Example 2.9 (Symmetries of a Set)

If $\Omega \subseteq \mathbb{R}^n$, then $(\mathrm{Sym}(\Omega), \circ, I)$ is a group. The proof of this is the essential content of Proposition 1.1. ◇

Example 2.10 (Symmetric Group)

The ***symmetric group*** is the group $S_n = (S_n, \cdot, e)$ of all permutations, with the multiplication of permutations being the group operation, and $e(k) = k$ being the identity permutation. That this is a group is largely the content of Proposition 1.3. The only thing that needs to be checked is that the identity permutation is in fact a group identity, and that is fairly straightforward: if p is any permutation in S_n,

$$(pe)(k) = e(p(k)) = p(k) \qquad \text{and} \qquad (ep)(k) = p(e(k)) = p(k),$$

for all k, so $ep = pe = p$, and e is therefore the identity for this group operation. ◇

Example 2.11 (Alternating Group)

Let A_n be the set of all even permutations. The ***alternating group*** is the group $A_n = (A_n, \cdot, e)$ of all even permutations, with the multiplication of permutations being the group operation, and $e(k) = k$ being the identity permutation. We know that the product of two even permutations is an even permutation, and the product is associative, and from the previous example we know that e is an identity. What remains to be checked is that if p is an even permutation, so is p^{-1}. We note that since $\mathrm{parity}(p) = 1$,

$$\mathrm{parity}(p^{-1}) = \mathrm{parity}(p)\,\mathrm{parity}(p^{-1}) = \mathrm{parity}(pp^{-1}) = \mathrm{parity}(e) = 1.$$

Hence p^{-1} is an even permutation.

The group A_n has order $n!/2$. ◇

Example 2.12 (Matrix Groups)

Recall that a matrix A is invertible if and only if $\det(A) \neq 0$. If we are going to find groups of matrices with matrix multiplication as the group operation, then they must be invertible at least.

The following are all groups:

- the ***general linear group*** of $n \times n$ matrices $(GL_n(\mathbb{R}), \times, I_n)$, where
$$GL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) : \det(A) \neq 0\}.$$
- the ***orthogonal group*** of $n \times n$ matrices $(O_n(\mathbb{R}), \times, I_n)$, where $O_n(\mathbb{R})$ is the set of orthogonal matrices (ie. matrices whose columns form an orthonormal basis or, equivalently, which satisfy $A^{-1} = A^t$).
- the ***special linear group*** of $n \times n$ matrices $(SL_n(\mathbb{R}), \times, I_n)$, where
$$SL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) : \det(A) = 1\}.$$
- the ***special orthogonal group*** of $n \times n$ matrices $(SO_n(\mathbb{R}), \times, I_n)$, where $SO_n(\mathbb{R})$ is the set of orthogonal matrices with determinant 1.

There isn't anything particularly special about $\mathbb{R}$-valued matrices in the above. Once can define $GL_n(\mathbb{F})$, $SL_n(\mathbb{F})$, $O_n(\mathbb{F})$, and $SO_n(\mathbb{F})$ for any field $\mathbb{F}$ (such as the complex numbers $\mathbb{C}$, or the rational numbers $\mathbb{Q}$).

A ***unitary matrix*** is a complex-valued matrix which satisfies $A^{-1} = A^*$, where A^* is the conjugate transpose matrix of A. More precisely, if $A = [a_{i,j}]_{i,j=1}^n$, then
$$A^* = [\overline{a_{i,j}}]^t.$$
We then have two additional complex matrix groups

- the ***unitary group*** of $n \times n$ matrices $(U_n(\mathbb{C}), \times, I_n)$, where U_n is the set of unitary matrices.
- the ***special unitary group*** of $n \times n$ matrices $(SU_n(\mathbb{C}), \times, I_n)$, where $SU_n(\mathbb{C})$ is the set of unitary matrices with determinant 1.

In all these cases, we know that matrix multiplication is associative, the identity matrix is an element of each group, and in each case there is a matrix inverse of each matrix. What we need to check in each case is that the product of two elements is an element of the group, and that the inverse of an element is an element of the group.

In each case it is fairly easy to verify these two facts. The key identities that we use are as follows:

(i) $|AB| = |A||B|$. So if $|A|$ and $|B| \neq 0$, then $|AB| \neq 0$. Hence if A and $B \in GL_n(\mathbb{R})$, then so is AB.

Similarly if $|A|$ and $|B| = 1$, then $|AB| = |A||B| = 1$, so if A and $B \in SL_n(\mathbb{R})$, then so is AB.

(ii) $(A^{-1})^{-1} = A$, so if $A \in GL_n(\mathbb{R})$, then so is A^{-1}.

(iii) $|A^{-1}| = |A|^{-1}$, so if $|A| = 1$, $|A^{-1}| = 1^{-1} = 1$. Hence if $A \in SL_n(\mathbb{R})$, then so is A^{-1}.

(iv) if A and $B \in O_n(\mathbb{R})$, then $(AB)^t = B^t A^t = B^{-1}A^{-1} = (AB)^{-1}$. Also $(A^{-1})^t = (A^t)^t = A = (A^{-1})^{-1}$, so $A^{-1} \in O_n(\mathbb{R})$.

This, combined with (1) and (2) also shows that $SO_n(\mathbb{R})$ is a group.

(v) similarly, if A and $B \in U_n(\mathbb{C})$, then $(AB)^* = B^*A^* = B^{-1}A^{-1} = (AB)^{-1}$. Also $(A^{-1})^* = (A^*)^* = A = (A^{-1})^{-1}$, so $A^{-1} \in U_n(\mathbb{C})$.

This, combined with (1) and (2) also shows that $SU_n(\mathbb{C})$ is a group.

◇

Example 2.13

The set of matrices

$$G = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} \right\}$$

is a group when given the standard matrix operations, and the identity is the identity matrix. The easiest way to verify this is simply to show that the group is closed under matrix multiplication and matrix inverse.

Letting

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \qquad A = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \qquad B = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, C = \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix},$$

we have that $I^{-1} = I$, $A^{-1} = A$, $B^{-1} = B$ abd $C^{-1} = C$, and if we draw up the Cayley table for matrix multiplication of these matrices, we get

	I	A	B	C
I	I	A	B	C
A	A	I	C	B
B	B	C	I	A
C	C	B	A	I

Note that the Cayley table and inverses of this group correspond to the Cayley table and inverses of the symmetries of the H-shaped set of Example 1.1, with $I \leftrightarrow I$, $A \leftrightarrow H$, $B \leftrightarrow V$, and $C \leftrightarrow R$. ◇

Example 2.14 (Free Groups)

Let a and b two symbols, and a^{-1} and b^{-1} be the inverse of these two symbols. A ***word*** in the ***letters*** a, b, a^{-1} and b^{-1} is simply a list $w = w_1 w_2 \cdots w_n$, where each w_k is one of the 4 letters. A ***reduced word*** is a word where we have repeatedly cancelled any adjacent occurrences of a letter and its inverse.

For example $w = aba^{-1}ab^{-1}b^{-1}ab^{-1}ba$ is a word. The corresponding reduced word can be found by cancelling: $w = aba^{-1}ab^{-1}b^{-1}ab^{-1}ba = abb^{-1}b^{-1}aa = ab^{-1}aa$.

The empty word e is the word with no letters. The product of two words $v = v_1v_2\cdots v_m$ and $w = w_1w_2\cdots w_n$ is simply the concatenation of the two words:

$$vw = v_1v_2\cdots v_mw_1w_2\cdots w_n$$

The ***free group*** on 2 symbols, F_2, is the set of all reduced words in a, b, a^{-1} and b^{-1}, where the group operation is to multiply two words, and then reduce the product, and the identity is the empty word. The inverse of a word $w = w_1w_2\cdots w_n$ is the word $w^{-1} = w_n^{-1}w_{n-1}^{-1}\cdots w_1^{-1}$.

In a similar manner, one can construct the free group F_n on n symbols. $\diamond$

Exercises

2.2.1. Let $(G, *, e)$ be a group, and let x and y be two elements of G which commute. Prove that for any $k \in \mathbb{Z}$, $(xy)^k = x^ky^k$.

2.2.2. Give an example of a group and two elements of that group such that

$$(xy)^2 \neq x^2y^2.$$

Provide concrete calculations to demonstrate this fact for your example.

2.2.3. Show that in each of the following cases, $(G, *, e)$ is a group.

(i) $G = \mathbb{R}^2$, $(x, y) * (x', y') = (x + x', y + y')$, $e = (0, 0)$.

(ii) $G = \{(x, y) : x, y \in \mathbb{R}, x \neq 0\}$, $(x, y) * (x', y') = (xx', x'y + y')$, $e = (1, 0)$.

(iii) $G = \{x : x \in \mathbb{R}, x \neq -1\}$, $x * y = x + y + xy$, $e = 0$.

(iv) $G = SL_2(\mathbb{Z}) = \left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{Z}, ad - bc = 1\right\}$, $*$ is matrix multiplication, and e is the identity matrix.

(v) $G = \left\{\begin{bmatrix} a & b \\ 0 & a \end{bmatrix} : a, b \in \mathbb{R}, a \neq 0\right\}$, $*$ is matrix multiplication, and e is the identity matrix.

(vi) $G = \mathcal{P}(X)$, the power set of some set X, $* = \triangle$, and $e = \emptyset$.

2.2.4. Let $m \geq 2$ be a natural number, and

$$G = \{k \in \mathbb{Z}_m : k \neq 0,\ k \text{ and } m \text{ are coprime}\}.$$

Show that $(G, \times, 1)$ is a group where $\times$ is performed modulo m. Conclude that $(\mathbb{Z}_p \setminus \{0\}, \times, 1)$ is a group if and only if p is prime.

Hint: Use Exercise 1.5.2.

2.2.5. Explain why $(\mathbb{N}, \times, 1)$ is not a group.

2.2.6. (*) Prove that $SL_n(\mathbb{Z})$ is a group.

2.3 Working With Abstract Groups

A lot of the content of group theory involves proving general facts about groups. The point of this section is to make you familiar with the sorts of techniques and proof methods involved. Unfortunately, even the most “obvious” and basic facts need careful checking, since we have stripped away most of the standard rules of algebra.

Consider the ***cancellation law***:

Proposition 2.3 (Cancellation Law)
Let $(G, *, e)$ be a group, and x, y, and $z \in G$. If $x * z = y * z$, then $x = y$. Similarly, if $z * x = z * y$, then $x = y$.

Normally you would cancel like this in algebra without too much thought: the case $z = 0$ for multiplication is really the only exceptional case in standard algebra. However we need to carefully justify that cancellation in fact works for groups.
Proof:
We have

$$\begin{aligned} x &= x * e && \text{(identity axiom)} \\ &= x * (z * z^{-1}) && \text{(inverse axiom)} \\ &= (x * z) * z^{-1} && \text{(associativity)} \\ &= (y * z) * z^{-1} && \text{(hypothesis)} \\ &= y * (z * z^{-1}) && \text{(associativity)} \\ &= y * e && \text{(inverse axiom)} \\ &= y. && \text{(identity axiom)} \end{aligned}$$

The second part is left as an exercise. ■

Notice how each step is justified in terms of the axioms of a group. Needless to say, once you get more familiar with the way that group operations work, you will not need to justify each step, and you may be able to skip certain trivial steps. In the short term, however, you should be careful that you justify each step in any calculation.

Here is another example: it should be fairly obvious that there can only be one inverse of any particular element. Nevertheless, we need to prove this result.

Proposition 2.4 (The Inverse is Unique)
Let $(G, *, e)$ be a group, and x, $y \in G$. Then if $x * y = e$, $y = x^{-1}$. Similarly, if $y * x = e$, $y = x^{-1}$.

Proof:

We have

$$\begin{aligned} y &= e * y && \text{(identity axiom)} \\ &= (x^{-1} * x) * y && \text{(inverse axiom)} \\ &= x^{-1} * (x * y) && \text{(associativity)} \\ &= x^{-1} * e && \text{(hypothesis)} \\ &= x^{-1}. && \text{(identity axiom)} \end{aligned}$$

The second part is left as an exercise. ■

Once we have basic facts like this, we can use them to simplify the proofs of other facts.

Proposition 2.5
Let $(G, *, e)$ be a group, and x, $y \in G$. Then $(x * y)^{-1} = y^{-1} * x^{-1}$.

Proof:
By Proposition 2.4, we need only show that $(x * y) * (y^{-1} * x^{-1}) = e$.

$$\begin{aligned} (x * y) * (y^{-1} * x^{-1}) &= (x * (y * y^{-1})) * x^{-1} && \text{(associativity)} \\ &= (x * e) * x^{-1} && \text{(inverse axiom)} \\ &= x * x^{-1} && \text{(identity axiom)} \\ &= e. && \text{(inverse axiom)} \end{aligned}$$

Hence $(x * y)^{-1} = y^{-1} * x^{-1}$. ■

Notice in this example that the order of the product is reversed in the inverse. This is necessary if the elements do not commute.

Here is another basic fact that needs to be verified.

Proposition 2.6 (Double Inverse)
Let $(G, *, e)$ be a group, and $x \in G$. Then $(x^{-1})^{-1} = x$.

Proof:
Exercise. ■

As mentioned in the previous section, if we use power-style notation, most of the usual power laws hold.

Proposition 2.7 (Power Laws for Groups)
Let $(G, *, e)$ be a group, and $x \in G$. Then

(i) $x^m x^n = x^{m+n}$,

(ii) $(x^m)^n = x^{mn}$,

(iii) if $y \in G$ *and* $x * y = y * x$, *then* $(x * y)^n = x^n * y^n$.

Let $(G, +, 0)$ is an Abelian group, and x, $y \in G$. Then

(i) $mx + nx = (m + n)x$,

(ii) $m(nx) = (mn)x$,

(iii) $n(x + y) = nx + ny$.

Proof:
Exercise. ■

Exercises

2.3.1. Prove the parts of the proofs from this section that were left as exercises.

2.3.2. Some texts define groups slightly differently (and slightly more efficiently) as follows:

A ***group***, $\mathbf{G} = (G, *, e)$, consists of a set G, a binary operation $* : G \times G \to G$, and an element $e \in G$ satisfying the following three conditions:

(i) $*$ is associative

(ii) e is a (left) identity for $*$, ie. $e * x = x$,

(iii) every element $x \in G$ has an ***inverse element*** $x^{-1} \in G$ such that $x^{-1} * x = e$.

Show that if you use these axioms, you can prove that e is also a right inverse, and $x*x^{-1} = e$, giving you the axioms of our definition of a group.

This means that the two definitions are equivalent, so you can use either one.

2.3.3. Let $(G, *, e)$ be a group, and x, $y \in G$. Show that if $y^{-1}xy = x^k$, then $y^{-n}x^m y^n = x^{mk^n}$.

2.3.4. Let $(G, *, e)$ be a group. Show that $e^{-1} = e$.

2.4 Cayley Tables

As we have seen, there are quite a number of groups around. We would like to develop some way that we can present groups abstractly, without worrying about any potential context.

For finite groups, one way of doing this is by giving a Cayley table for the group.

Definition 2.1
Let $(G, *, e)$ be a finite group of order n, with some particular ordering x_1, $x_2, \ldots, x_n$ chosen for the elements of G. Then a Cayley table of the group is an array where $x_i * x_j$ is in the ith row and jth column.

We do not need to specify the inverse as a separate table, since we can find the inverse of x_i by looking for the j such that the jth entry of the ith row is e, so that $x_i * x_j = e$, and hence $x_j = x_i^{-1}$ by Proposition 2.4.

We have already seen a number of Cayley tables for binary operations which turned out to be groups. Indeed, in a number of situations, the Cayley tables turned out to be essentially the same.

Example 2.15

Consider the Cayley tables of $(\mathbb{Z}_2, +, 0)$ and $(\mathbb{Z}_3 \setminus \{0\}, \times, 1)$.

$+$	0	1
0	0	1
1	1	0

$\times$	1	2
1	1	2
2	2	1

These are the same table is you replace + by ×, 0 by 1 and 1 by 2. ◇

In situations like this, we can agree that the two groups in question are essentially the same.

Definition 2.2

*Two finite groups $(G, *, e)$ and $(H, \circ, i)$ are **isomorphic** if a Cayley table of H can be obtained from a Cayley table of G be replacing all occurrences of each symbol in G by a corresponding symbol of H, and each $*$ by $\circ$.*

We write $G \cong H$ when G and H are isomorphic.

The correspondence between any two isomorphic groups always has the two identities corresponding, and always has the inverse of a symbol in G corresponding to the inverse of the corresponding symbol in H.

Isomorphism is clearly a transitive relation between groups. If G and H are isomorphic, and H and F are isomorphic, than G and F must also be isomorphic.

This is not the final version of the definition of "isomorphic", but it will do for now.

Example 2.16

The groups S_3 and $\mathrm{Sym}(\Omega)$, where Ω is an equilateral triangle, are isomorphic. ◇

Example 2.17

Consider the Cayley tables of $\mathbb{Z}_4$ and the group of symmetries of the H-shaped set of Example 1.1:

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\circ$	I	H	V	R
I	I	H	V	R
H	H	I	R	V
V	V	R	I	H
R	R	V	H	I

These two groups are not isomorphic, since I must correspond to 0, and one of H, V or R must correspond to 1, and $1 + 1 = 2$, but we have $H \circ H = I$, $V \circ V = I$, $R \circ R = I$, so their products cannot correspond to the sum, and so there is no element that can correspond to 1. ◇

It is immediate that for two groups to be isomorphic, they must have the same order, since otherwise the Cayley tables are different sizes, and so the cannot correspond.

Similarly if two groups are isomorphic, either both are Abelian, or both fail to be Abelian, since there is no way the Cayley tables can correspond if one is Abelian and the other not.

Lemma 2.8
If G and H are finite groups, and $G \cong H$, then:

(i) $|G| = |H|$,

(ii) G is Abelian if and only if H is Abelian.

This leads to the following:

Question 1
How many different (ie. non-isomorphic) classes of groups are there for any given order?

This question is one which we will spend a fair amount of time considering.

Cayley tables can be used to answer this question, at least for groups of small order, but we need a few facts about Cayley tables first.

Proposition 2.9
If $(G, *, e)$ is a finite group, then every element of G occurs exactly once in each row and in each column of a Cayley table for G.

Proof:

Let $G = \{x_1, x_2, \ldots, x_n\}$. Assume that x occurs twice in the ith row, so that $x = x_i * x_j$ and $x = x_i * x_k$ for some $j \neq k$. But then we have $x_i * x_j = x_i * x_k$, and the cancellation law tells us that $x_j = x_k$, so $j = k$, which is a contradiction. Hence x can occur at most once.

If x does not occur at all in the ith row, then there must be some other element which occurs 2 or more times by the pidgeonhole principle, which is impossible. Hence x must occur exactly once.

A similar argument proves the result for columns. ■

Another way of saying this is that a Cayley table is a ***Latin square***: a Latin square is an array of symbols in which every symbol occurs exactly once in each row and in each column. Latin squares are significant in experimental design and statistics. However, not every Latin square is a Cayley table for a group.

Example 2.18

The following binary operation does not give a group:

$*$	1	a	b	c	d
1	1	a	b	c	d
a	a	1	d	b	c
b	b	c	1	d	a
c	c	d	a	1	b
d	d	b	c	a	1

The problem is that the operation it determines is not associative: $(a * b) * c = d * c = a$, while $a * (b * c) = a * d = c$. However, this table clearly has the Latin square property. $\diamond$

Theorem 2.10

Let $n = 1$, 2, or 3. Then every group of order n is isomorphic to $(\mathbb{Z}_n, +, 0)$.

Proof:

Case $n = 1$: the group has one element which must be the identity, so $G = \{e\}$. The only possible Cayley table is trivial

$*$	e
e	e

and this clearly is isomorphic to the Cayley table of $\mathbb{Z}_1$

$+$	0
0	0

Case $n = 2$: the group has two elements, one of which must be the identity, so $G = \{e, a\}$. Entering in the elements which are products of the identity element we get

$*$	e	a
e	e	a
a	a	

and clearly the only way to complete this table while keeping the Latin square property is to put an e in the bottom right entry:

$*$	e	a
e	e	a
a	a	e

Again, this is clearly isomorphic to $\mathbb{Z}_2$ when you look at the Cayley table

$+$	0	1
0	0	1
1	1	0

Case $n = 3$: the group has three elements, one of which must be the identity, so $G = \{e, a, b\}$. Entering in the elements which are products of the identity element we get

$*$	e	a	b
e	e	a	b
a	a		
b	b		

To preserve the Latin square property, the second entry of the second column must be b, otherwise the second entry of the third column would be b, which would break the Latin square property for the third column. This then implies that the last entries of the second row and second column must be e, and the final entry of the array must be a.

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Again, the correspondence with the Cayley table for $\mathbb{Z}_3$ is clear:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

■

We know that there are at least two non-isomorphic groups of order 4. It will turn out that these are the only two possibilities. We could prove this by finding all possible Cayley tables of groups of order 4, but as we will see, there are slicker ways to do this.

Exercises

2.4.1. Find another example of a Latin square which is not the Cayley table of a group.

2.4.2. Show that any group of order 4 is isomorphic to one of the two groups in Example 2.17.

2.5 Generators

While Cayley tables have their uses, there are clear limitations to their use once the groups get large, and for infinite groups they at best give a tiny snapshot of the group. Another way of presenting groups is required, which can deal with these larger groups.

Definition 2.3
Let $(G, *, e)$ be a group. We say that a subset $X = \{x_1, x_2, \ldots, x_n\}$ of G ***generates*** *G if every element of G can be written as a product of powers of elements of set X (possibly with repetition). We say that the elements of X are generators of G.*

More generally, given a subset $X = \{x_1, x_2, \ldots, x_n\}$ of G, the set of elements that can be written as a product of powers of elements of X (possibly with repetition) is the set ***generated*** *by X, and we denote it by $\langle x_1, x_2, \ldots, x_n \rangle$ or $\langle X \rangle$.*

Example 2.19
The group S_3 is generated by the permutations $a = (1, 2, 3)$ and $b = (1, 2)$. One can easily verify that the identity permutation is a^0, $a^2 = (1, 3, 2)$, $ab = (2, 3)$ and $a^2 b = (1, 3)$. We could write $S_3 = \langle (1, 2, 3), (1, 2) \rangle$.

The group S_3 is also generated by $x = (1, 2)$ and $y = (2, 3)$. This requires a little bit more checking, but $x^0 = e$, $yx = (1, 2, 3)$, $xy = (1, 3, 2)$, and $xyx = (1, 3)$, so we also have $S_3 = \langle (1, 2), (2, 3) \rangle$.

On the other hand, the permutation $a = (1, 2, 3)$ does not generate the whole group. The only elements we can get using just powers of a are e, a, and a^2, since $a^3 = e$. Hence $\langle (1, 2, 3) \rangle = \{e, (1, 2, 3), (1, 3, 2)\}$. ◇

Example 2.20
The group $(\mathbb{Z}_4, +, 0)$ is generated by 1, since $1 + 1 = 2$, $1 + 1 + 1 = 3$ and $1 + 1 + 1 + 1 = 0$. It is also generated by -1.

However the set generated by 2 is simply $\{0, 2\}$. ◇

We note that the identity element is always in the set generated by any collection of elements.

Generators help us understand the structure of a group by allowing us to represent general elements in terms of fewer symbols.

Example 2.21
If $x = (1, 2)$ and $y = (2, 3)$, then $S_3 = \{e, x, y, xy, yx, xyx\}$. In addition, we can see that $x^2 = e$, $y^2 = e$ and $yxy = xyx$. For example, you could calculate the product of xyx and yx using these facts as follows:

$$\begin{aligned}
(xyx)(yx) &= x(yxy)x && \text{(associativity)} \\
&= x(xyx)x && (yxy = xyx) \\
&= (xx)y(xx) && \text{(associativity)} \\
&= eye && (x^2 = e) \\
&= y && \text{(identity axiom)}
\end{aligned}$$

We can use this information to write the Cayley table of S_3 in terms of x and y as follows:

$\cdot$	e	x	y	xy	yx	xyx
e	e	x	y	xy	yx	xyx
x	x	e	xy	y	xyx	yx
y	y	yx	e	xyx	x	xy
xy	xy	xyx	x	yx	e	y
yx	yx	y	xyx	e	xy	x
xyx	xyx	xy	yx	x	y	e

$\diamond$

Notice how in the above example the identities $x^2 = e$, $y^2 = e$ and $yxy = xyx$ help us calculate. Such identities are called ***relations***. In fact, given the generators x and y and these three relations, we can recover the Cayley table for S_3. This leads us to another way to present a group, which we will make more formal in a later section. In the mean-time we can use it informally as follows:

Example 2.22 (Cyclic Groups)
The group C_n consists of the set $C_n = \{1, a, a^2, \ldots, a^{n-1}\}$ and the group operation is determined by the relation $a^n = 1$.

The group $(C_4, \cdot, 1)$, then has the Cayley table

$\cdot$	1	a	a^2	a^3
1	1	a	a^2	a^3
a	a	a^2	a^3	1
a^2	a^2	a^3	1	a
a^3	a^3	1	a	a^2

Clearly C_4 and $\mathbb{Z}_4$ are isomorphic. $\diamond$

Example 2.23 (Dihedral Groups)
The group D_{2n} consists of the set

$$D_{2n} = \{1, a, a^2, \ldots, a^{n-1}, b, ab, a^2b, \ldots, a^{n-1}b\}$$

and the group operation is determined by the relations $a^n = 1$, $b^2 = 1$ and $ba = a^{n-1}b$. Note that $a^{n-1}a = a^n = 1$, so $a^{n-1} = a^{-1}$, and we could write the third relation as $ba = a^{-1}b$.

For example, we can use these relations to show that

$$ba^k = a^{-1}ba^{k-1} = a^{-1}a^{-1}ba^{k-2} = \cdots = a^{-k}b.$$

The group $(D_8, \cdot, 1)$, then has the Cayley table

$\cdot$	1	a	a^2	a^3	b	ab	a^2b	a^3b
1	1	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	1	ab	a^2b	a^3b	b
a^2	a^2	a^3	1	a	a^2b	a^3b	b	ab
a^3	a^3	1	a	a^2	a^3b	b	ab	a^2b
b	b	a^3b	a^2b	ab	1	a^3	a^2	a
ab	ab	b	a^3b	a^2b	a	1	a^3	a^2
a^2b	a^2b	ab	b	a^3b	a^2	a	1	a^3
a^3b	a^3b	a^2b	ab	b	a^3	a^2	a	1

If you were to write out the symmetry group of a square you would find that it is isomorphic to D_8.

In fact we will prove later that the symmetry group of a regular n-gon is isomorphic to D_{2n}. ◇

Definition 2.4
*Let $(G, *, e)$ be a group, and left $x \in G$. The **order** $o(x)$ is the cardinality of the set it generates, $o(x) = |\langle x \rangle|$.*

*If $G = \langle x \rangle$ for any $x \in G$, we say that G is a **cyclic group**.*

Example 2.24
In S_3, e has order 1, $(1, 2)$, $(2, 3)$ and $(1, 3)$ have order 2, and the elements $(1, 2, 3)$ and $(1, 3, 2)$ have order 3.

In $\mathbb{Z}_4$, 0 has order 1, 2 has order 2, and 1 and -1 have order 4. Since $\mathbb{Z}_4 = \langle 1 \rangle$, it is a cyclic group. ◇

Example 2.25
For every $n \in \mathbb{N}$, $(\mathbb{Z}_n, +, 0)$ is a cyclic group, since $\mathbb{Z}_n = \langle 1 \rangle$. ◇

The orders of elements of a group can be used as a comparatively simple check to see if two groups may not be isomorphic. It is clear that if G and H are isomorphic groups, and $x \in G$ corresponds to $y \in H$, then $o(x) = o(y)$. Turning this idea around, we get the following theorem

Theorem 2.11
If G and H are two groups, then if there is some n such that the number of elements of order n in G is different from the number of elements of order n in H, ie.

$$|\{x \in G : o(x) = n\}| \neq |\{y \in H : o(y) = n\}|$$

then G and H are not isomorphic.

Proof:

Without loss of generality, we may assume that $|\{x \in G : o(x) = n\}| > |\{y \in H : o(y) = n\}|$. If G and H are isomorphic, then there must be some x which corresponds to an element of H which does not have order y, because there are not enough elements of order n in H. But this cannot happen if the groups are isomorphic, giving a contradiction. ■

We will eventually see that the converse of this theorem is not true, so this does not give a good test for isomorphism of groups.

The following simplified version of the theorem is often enough to prove that two groups are not isomorphic.

Corollary 2.12
If G and H are two groups, and there is some $x \in G$ such that $o(x) > o(y)$ for every $y \in H$, then G and H are not isomorphic.

This allows us to see that a couple of groups are not isomorphic very quickly:

Example 2.26
If we look at $C_4 = \{1, a, a^2, a^3\}$, we see that $o(a) = 4$. On the other hand, $D_4 = \{1, a, b, ab\}$ has $o(1) = 1$, and $o(a) = o(b) = o(ab) = 2$. So by the corollary, $C_4 \ncong D_4$. ◇

Example 2.27
If we look at $C_6 = \{1, a, a^2, a^3, a^4, a^5\}$, we see that $o(a) = 6$. On the other hand, $D_6 = \{1, a, b, ab, a^2, a^2b\}$ has $o(1) = 1$, $o(b) = o(ab) = o(a^2b) = 2$, and $o(a) = o(a)^2 = 3$. So by the corollary, $C_6 \ncong D_6$.

One could also show this by simply observing that C_6 is Abelian, but D_6 is not. ◇

Related to the above discussion is the following theorem.

Theorem 2.13
If G is a group of order n and there is some element $x \in G$ of order n, then G is a cyclic group.

Proof:

We have that $\langle x \rangle \subseteq G$, and $|\langle x \rangle| = o(x) = n = |G|$. Hence, since G is finite, $\langle x \rangle = G$ ■

The following theorem is fairly obvious, but needs to be stated and proved.

Theorem 2.14
If G and H are cyclic groups of the same order, then they are isomorphic.

Proof:

We have that $G = \langle a \rangle = \{1 = a^n, a, a^2, \dots a^{n-1}\}$ and $H = \langle b \rangle = \{1 = b^n, b, b^2, \dots, b^{n-1}\}$, and a typical entry in their Cayley tables looks like

	a^k
a^l	a^{k+l}

	b^k
b^l	b^{k+l}

remembering that $a^n = 1$ and $b^n = 1$. In any case, it is clear that we can get from one Cayley table to the other by simply replacing powers of a with corresponding powers of b. $\blacksquare$

Corollary 2.15
Every group of order 1, 2, *or* 3 *is a cyclic group.*

We give one last example, mainly to introduce a name.

Example 2.28
The group V consisting of the elements $\{1, a, b, ab\}$ with the relations $a^2 = 1$, $b^2 = 1$ and $ba = ab$ is called the ***four-group*** or ***vierergruppe*** (which is German for "four-group").

The Cayley table of this group is

$\cdot$	1	a	b	ab
1	1	a	b	ab
a	a	1	ab	b
b	b	ab	1	a
ab	ab	b	a	1

Given the Cayley table, you can see that this is isomorphic to the group of symmetries of the letter H, via the correspondences: $1 \leftrightarrow I$, $a \leftrightarrow H$, $b \leftrightarrow V$, and $ab \leftrightarrow R$.

Also, since $a^2 = 1$ implies $a = a^{-1}$, we could have used the relation $ba = a^{-1}b$ instead of $ba = ab$. Hence V is the same group as D_4. $\diamond$

Exercises

2.5.1. Show that $(1, 2)$ and $(1, 3)$ generate S_3.

2.5.2. Let $(G, *, e)$ be a group, and let x, $y \in G$. Show that

(i) $o(x^{-1}) = o(x)$,

(ii) $o(xy) = o(yx)$,

(iii) if $o(x) = 1$, then $x = e$,

(iv) if $o(x) = n$, then $x^m = e$ if and only if n divides m,

(v) if $o(x) = n$, then n is the smallest natural number such that $x^n = e$.

2.5.3. Show that a^k generates the cyclic group $C_n = \{1, a^1, a^2, \ldots, a^{n-1}\}$ if and only if k and n are coprime.

Show that the order of a^k in C_n is $k/\gcd(k, n)$.

2.5.4. Let $(G, *, e)$ be a group, and x, $y \in G$. Show that if x, y and xy all have order 2, then x and y commute.

2.5.5. Show that D_6 and S_3 are isomorphic groups.

2.5.6. Show that if Ω is a regular n-sided polygon in $\mathbb{R}^2$, then $\mathrm{Sym}(\Omega) \cong D_6$.

2.5.7. Let $G = \{1, a, b, ab, a^2, a^2b\}$ with the relations $a^3 = 1$, $b^2 = 1$, and $ab = ba$. Write out the Cayley table of this group, and show that G is isomorphic to C_6.

2.5.8. Show that $(\mathbb{Z}, +0)$ is generated by the elements 2 and 3.

(*) Show that it is generated by any pair of coprime numbers. (Hint: show that you can get 1 as a sum of multiples of the numbers.)

2.6 Excursion: Introduction to Categories

You may have noticed some similarities between the theory of groups as it has been presented to this point, and the theory of abstract vector spaces. In both cases the objects were defined in terms of axioms which must hold for various binary operations. In both cases we have a concept called isomorphism which tells us when two groups or two vector spaces are essentially the same.

Indeed, if you think about it, the concept of generating sets and spanning sets are somewhat analogous: a set generates G if you can get every element of G by applying the group operations to the elements of the generating set; while a set spans a vector space V if you can get every element of V by applying linear operations (vector addition and scalar multiplication) to the elements of the spanning set.

Clearly we should be careful not to take such analogies too far, since groups and vector spaces *are* different, but the analogies are useful for putting the next few sections into context.

In the theory of vector spaces, there are three concepts we have not yet seen in the context of groups:

- direct sums of vector spaces: if V and W are vector spaces, we have the direct sum $V \oplus W$ which is the set $V \times W$ together with appropriate vector space operations.

- subspaces: a subspace of a vector space is a subset which is also a vector space.

- linear transformations: a linear transformation is a function between vector spaces which preserves the vector space operations.

As you study more algebra you will notice that there are many similarities like these between the theories of various types of algebraic objects. Indeed, we even get such similarities in other areas of pure mathematics, such as analysis, topology and geometry. In many cases the proofs of basic facts in these theories are almost identical, but with appropriate change of terminology.

Whenever you have similarities and patterns like this in mathematics, there must be something going on. Category theory is the theory which deals with and formalizes these similarities. There are a handful of useful results which have come out of category theory, but its primary significance is that it provides a framework for much of modern mathematical theory.

We'll consider categories in more depth later.

2.7 Direct Products

You may recall the definition of a direct sum from linear algebra, if you have two vector spaces V and W over the same scalar field, the direct product is the set $V \times W$ with vector addition

$$(v_1, w_1) + (v_2, w_2) = (v_1 + v_2, w_1 + w_2),$$

scalar multiplication

$$\lambda(v, w) = (\lambda v, \lambda w)$$

and zero vector $(0, 0)$. Note that the vector space operations are defined simply by applying the appropriate vector space operation to each component.

Theorem 2.16
Let $(G, *, e)$ and $(H, \circ, 1)$ be two groups. If we define a binary operation $\bullet$ on $G \times H$ by

$$(g_1, h_1) \bullet (g_2, h_2) = (g_1 * g_2, h_1 \circ h_2),$$

then $G \times H = (G \times H, \bullet, (e, 1))$ is a group, and the inverse of (g, h) is (g^{-1}, h^{-1}).

Proof:
The binary operation $\bullet$ is obviously well defined, so we only need to check that the three axioms hold.

Associativity follows directly from the associativity of G and H:

$$\begin{aligned}((g_1, h_1) \bullet (g_2, h_2)) \bullet (g_3, h_3) &= (g_1 * g_2, h_1 \circ h_2) \bullet (g_3, h_3) \\ &= ((g_1 * g_2) * g_3, (h_1 \circ h_2) \circ h_3) \\ &= (g_1 * (g_2 * g_3), h_1 \circ (h_2 \circ h_3)) \\ &= (g_1, h_1) \bullet (g_2 * g_3, h_2 \circ h_3) \\ &= (g_1, h_1) \bullet ((g_2, h_2) \bullet (g_3, h_3))\end{aligned}$$

It's straightforward to see that $(e, 1)$ is an identity:

$$(g, h) \bullet (e, 1) = (g * e, h \circ 1) = (g, h)$$

and

$$(e, 1) \bullet (g, h) = (e * g, e \circ h) = (g, h).$$

Finally, we observe that

$$(g^{-1}, h^{-1}) \bullet (g, h) = (g^{-1} * g, h^{-1} \circ h) = (e, 1),$$

so by Proposition 2.4, $(g, h)^{-1} = (g^{-1}, h^{-1})$, and so every element of $G \times H$ has an inverse.

So $G \times H$ is a group. ■

If G and H are finite groups, the multiplication principle tells us that $G \times H$ is a finite group, and the order of $G \times H$ is $|G||H|$.

Consider the following examples:

Example 2.29

The group $C_2 \times C_2$ has 4 elements: $(1, 1)$, $(a, 1)$, $(1, a)$ and (a, a). We can draw up the Cayley table:

$\bullet$	$(1,1)$	$(a,1)$	$(1,a)$	(a,a)
$(1,1)$	$(1,1)$	$(a,1)$	$(1,a)$	(a,a)
$(a,1)$	$(a,1)$	$(1,1)$	(a,a)	$(1,a)$
$(1,a)$	$(1,a)$	(a,a)	$(1,1)$	$(a,1)$
(a,a)	(a,a)	$(1,a)$	$(a,1)$	$(1,1)$

Hopefully you can immediately see that this group is isomorphic to the *viergruppe* V via the correspondence $(1, 1) \leftrightarrow 1$, $(a, 1) \leftrightarrow a$, $(1, a) \leftrightarrow b$, and $(a, a) \leftrightarrow ab$. Hence it is also isomorphic to the group of symmetries of the letter H. ◇

Example 2.30

The group $C_2 \times C_3$ has 6 elements: $(1, 1)$, $(a, 1)$, $(1, b)$ (a, b), $(1, b^2)$ and (a, b^2). We note that

$$\begin{aligned}(a, b)^2 &= (1, b^2)\\(a, b)^3 &= (a, 1)\\(a, b)^4 &= (1, b)\\(a, b)^5 &= (a, b^2)\\(a, b)^6 &= (1, 1)\end{aligned}$$

So $C_2 \times C_3 = \langle (a, b) \rangle$, and so it is a cyclic group. Hence $C_2 \times C_3$ is isomorphic to the cyclic group of order 6, C_6. ◇

You may notice that in these example the groups are all Abelian. This is a consequence of the following proposition.

Proposition 2.17
If G and H are Abelian groups, then so is $G \times H$.

Proof:
Exercise. ■

The converse to this proposition is also true, but it requires a lot more theory to get it in its nicest form.

If we have several groups G_1, $G_2, \ldots, G_n$, we can define the direct product $G_1 \times G_2 \times \cdots G_n$ in the obvious way. There is a fairly clear isomorphism between $(G_1 \times G_2) \times G_3$, $G_1 \times (G_2 \times G_3)$, and $G_1 \times G_2 \times G_3$ given by the correspondence

$$((g_1, g_2), g_3) \leftrightarrow (g_1, (g_2, g_3)) \leftrightarrow (g_1, g_2, g_3).$$

So just as we consider the vector spaces $(V_1 \oplus V_2) \times V_3$, $V_1 \oplus (V_2 \times V_3)$ and $V_1 \oplus V_2 \times V_3$ as being the same vector space, we blur the distinction between the above direct products of groups and regard all three as the same group. With this in mind, the direct product is then associative. We will also write

$$G^n = \underbrace{G \times G \times \cdots \times G}_{n \text{ times}}.$$

The following theorem will prove useful when we try to classify all the groups of a given order. It generalizes the isomorphism between V and $C_2 \times C_2$.

Theorem 2.18
Let G be a finite group such that $x^2 = 1$ for every element $x \in G$, and $|G| \geq 2$. Then G is isomorphic to $C_2 \times C_2 \times \cdots \times C_2$.

Proof:
We first observe that G must be Abelian. Given any x and $y \in G$, we have

$$xyxy = (xy)^2 = 1.$$

But then

$$x = x1 = x(xyxy) = x^2yxyx = yxy,$$

and so

$$yx = y(yxy) = y^2xy = xy.$$

We now find elements $a_k \in G$ by the following inductive construction:

(i) Since $|G| \geq 2$, we can find some element $a_1 \neq 1$. So $\langle a_1 \rangle = \{1, a_1\}$, since $a_1^2 = 1$.

(ii) Assume that we have found elements a_1, $a_2, \ldots, a_r$, such that a_k is not in $\langle a_1, \ldots, a_{k-1} \rangle$ for all $k = 2, \ldots, r$.

Then one of two things must be true: either $G = \langle a_1, \ldots, a_r \rangle$, or there is some a_{r+1} which is not in $\langle a_1, \ldots, a_r \rangle$. But then the elements a_1, $a_2, \ldots, a_r, a_{r+1}$ satisfy the condition for $r + 1$.

(iii) Proceeding inductively, we must eventually exhaust all the elements of G.

So we have that $G = \langle a_1, a_2, \ldots, a_n \rangle$ for elements a_1, $a_2, \ldots, a_n$ such that a_k is not in $\langle a_1, \ldots, a_{k-1} \rangle$ for all $k = 2, \ldots, n$. So any element $x \in G$ can be written as a product of powers of the elements a_1, $a_2, \ldots, a_n$, and since G is Abelian, we can move all the powers of a_1 to the front of the product, a_2 to the next term, and so on. So in general

$$x = a_1^{p(1)} a_2^{p(2)} \cdots a_n^{p(n)},$$

where $p(k)$ must be either 0 or 1. Moreover, this is the only way that the element x can be written, since if we also have

$$x = a_1^{r(1)} a_2^{r(2)} \cdots a_n^{r(n)},$$

then

$$\begin{aligned} 1 &= a_1^{p(1)} a_2^{p(2)} \cdots a_n^{p(n)} (a_1^{r(1)} a_2^{r(2)} \cdots a_n^{r(n)})^{-1} \\ &= a_1^{p(1)-r(1)} a_2^{p(2)-r(2)} \cdots a_n^{p(n)-r(n)}. \end{aligned}$$

But this implies that

$$a_n^{p(n)-r(n)} = a_1^{r(1)-p(1)} a_2^{r(2)-p(2)} \cdots a_{n-1}^{r(n-1)-p(n-1)},$$

and so $p(n) - r(n) = 0$, since if $p(n) - r(n) = 1$, then a_n would be generated by a_1, $a_2, \ldots, a_{n-1}$, which contradicts our construction. So

$$1 = a_1^{p(1)-r(1)} a_2^{p(2)-r(2)} \cdots a_n^{p(n-1)-r(n-1)},$$

and the same argument as for n shows that $p(n-1) - r(n-1) = 0$.

Proceeding inductively, we have that $p(k) - r(k) = 0$ for all k. Hence $p(k) = r(k)$ for all k, and so there is only one such way to write x as a product of powers of a_1, $a_2, \ldots, a_n$ in that order.

Now we can think of $C_2 = \{1, a\}$, and so

$$\underbrace{C_2 \times C_2 \times \cdots \times C_2}_{n \text{ times}} = \{(a^{p(1)}, a^{p(2)}, \ldots, a^{p(n)}) : p(k) \in \{0, 1\}\}.$$

But we have a correspondence

$$a_1^{p(1)} a_2^{p(2)} \cdots a_n^{p(n)} \leftrightarrow (a^{p(1)}, a^{p(2)}, \ldots, a^{p(n)}),$$

and if you compare typical entries of the Cayley table you get

	$a_1^{r(1)} a_2^{r(2)} \cdots a_n^{r(n)}$
$a_1^{p(1)} a_2^{p(2)} \cdots a_n^{p(n)}$	$a_1^{p(1)+r(1)} a_2^{p(2)+r(2)} \cdots a_n^{p(n)+r(n)}$

and

	$(a^{r(1)}, a^{r(2)}, \ldots, a^{r(n)})$
$(a^{p(1)}, a^{p(2)}, \ldots, a^{p(n)})$	$(a^{p(1)+r(1)}, a^{p(2)+r(2)}, \ldots, a^{p(n)+r(n)})$

and so the Cayley tables correspond.

Hence $G \cong C_2^n$. ■

Corollary 2.19
Let G be a finite group such that $x^2 = 1$ for every element $x \in G$, and $|G| \geq 2$. Then $|G| = 2^n$ for some n.

Exercises

2.7.1. Show that D_{2n} and $C_2 \times C_n$ are not isomorphic for $n > 2$.

2.7.2. Write down the Cayley tables of $C_2 \times C_2 \times C_2$ and $C_2 \times C_4$. Show that these two groups are not isomorphic.

Show that D_8 and $C_2 \times C_2 \times C_2$ are not isomporhic.

2.7.3. Let p and q be prime numbers. Show that $C_p \times C_q \cong C_{pq}$.

More generally, show that if p and q are coprime, $C_p \times C_q \cong C_{pq}$.

2.7.4. Let G be an Abelian group where $x^3 = 1$ for every $x \in G$. Show that $G \cong C_3 \times C_3 \times \cdots \times C_3$.

2.7.5. (*) Find a group G such that $x^3 = 1$ for every $x \in G$, but $G \ncong C_3 \times C_3 \times \cdots \times C_3$

2.8 Subgroups

Groups often contain other groups. You should be at least intuitively aware of this fact, since the various additive groups of numbers are contained in one another:

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

Knowing the groups which are contained within a particular group can tell you a lot about the group.

Definition 2.5
Let $(G, *, e)$ be a group, and $H \subseteq G$. We say H is a ***subgroup*** *of G if $(H, *, e)$ is a group (where $*$ is restricted to H).*

We denote this relationship by writing $H \leq G$. If $H \subset G$, then we may write $H < G$.

In general, we do not expect an arbitrary subset of a group to be a group. In particular, we have to at least have $e \in H$. Furthermore, for $*$ to be a binary operation when restricted to H, it needs to be closed on H. In other words, the product of elements of H must again be an element of H. Finally, we need that the inverse of every element of H is an element of H. But the good news is that we don't need to check associativity: that is guaranteed by the associativity of $*$ as an operation on G. To summarize:

Theorem 2.20
Let $G = (G, *e)$ be a group, and $H \subseteq G$. If for every x and $y \in H$ we have

(i) $x * y \in H$, and

(ii) $x^{-1} \in H$,

then H is a subgroup.

Proof:
Condition (i) tells us that $* : H \times H \to H$, so $*$ is a binary operation on H. Associativity is simple since $*$ is associative on G, so the axiom still holds for a subset. Since $x^{-1} \in H$, we have both the inverse axiom, and the identity being an element of H, since $e = x^{-1} * x \in H$ by (i). And e is still an identity for $*$ on H, since it satisfies the identity axiom for all elements of G, including those in H. ■

In fact, we can make this theorem even slicker by combining the two conditions into one:

Corollary 2.21
Let $G = (G, *e)$ be a group, and $H \subseteq G$. If for every x and $y \in H$ we have $xy^{-1} \in H$, then H is a subgroup.

Proof:
We note that if $x \in H$, then $xx^{-1} = e \in H$, and hence $x^{-1} = ex^{-1} \in H$, giving condition (i) of the theorem.

Additionally, since $y^{-1} \in H$, $xy = x(y^{-1})^{-1} \in H$, giving condition (ii) of the theorem.

Hence H is a subgroup. ■

Note that if we use additive notation for a group, the conditions of Theorem 2.20 become

(i) $x + y \in H$, and

(ii) $-x \in H$,

while the condition for Corollary 2.21 becomes $x - y \in H$.

We immediately note that a group G is always a subgroup of itself, and the set containing just the identity $\{e\}$ is always a group. These two subgroups are called the ***trivial subgroups*** of G. If H is a subgroup of G which not trivial, we say that H is a ***proper subgroup***.

For finite groups, the Cayley table of a subgroup is simply the Cayley table of the whole group with every row and column corresponding to elements not in the subgroup being removed.

Example 2.31

The cyclic group of order 3 $C_3 = \{1, a, a^2\}$ has the subgroups $\{1\}$, and $\{1, a, a^2\}$. It has no proper subgroups.

You can see that other subsets are not subgroups be inspection. For example, the set $\{1, a^2\}$ is not a subgroup because $a^2 a^2 = a^4 = a$, and a is not an element of the set. ◇

Example 2.32

The cyclic group of order 4 $C_4 = \{1, a, a^2, a^3\}$ has the subgroups $\{1\}$, $\langle a^2 \rangle = \{1, a^2\}$ and $\{1, a, a^2, a^3\}$.

You can verify that $\{1, a^2\}$ is a subgroup by calculating every possible value of xy^{-1} for x and $y \in \{1, a^2\}$:

$$\begin{array}{cc} 1 \cdot 1^{-1} = 1 & 1 \cdot (a^2)^{-1} = a^{-2} = a^2 \\ a^2 \cdot 1^{-1} = a^2 & a^2 \cdot (a^2)^{-1} = 1. \end{array}$$

In fact, we really only need to look at products where neither x nor y is 1, since those always leave the other term alone. We will see shortly that the fact that this is a set generated by an element guarantees that it is a subgroup.

These subgroups are isomorphic to C_1, C_2 and C_4 respectively. ◇

Example 2.33

The vierergruppe $V = \{1, a, b, ab\}$ has the subgroups $\{1\}$, $\langle a \rangle = \{1, a\}$, $\langle b \rangle = \{1, b\}$, $\langle ab \rangle = \{1, ab\}$ and $\{1, a, b, ab\}$.

These subgroups are isomorphic to C_1, C_2, C_2, C_2, and V respectively. ◇

Example 2.34

The cyclic group or order 6, $C_6 = \{1, a, a^2, a^3, a^4, a^5\}$ has the subgroups $\{1\}$, $\langle a^3 \rangle = \{1, a^3\}$, $\langle a^2 \rangle = \{1, a^2, a^4\}$, and C_6.

These subgroups are isomorphic to C_1, C_2, C_3, C_6, and V respectively. ◇

Example 2.35

Let p be a prime number, and C_p the cyclic group of order p. Since a^k generates C_p for all $k \neq 0$, any subgroup which contains any element other than 1 must automatically contain all of C_p. Hence C_p only has the trivial subgroups $\{1\}$ and C_p. ◇

Example 2.36

If $s \in \mathbb{R}$, then the set $\{sn : n \in \mathbb{Z}\}$ is a subgroup of the additive group of real numbers $(\mathbb{R}, +, 0)$. This follows because if we take two typical elements ns and ms, then

$$ns - ms = (n - m)s,$$

and this is an element of the set $\{sn : n \in \mathbb{Z}\}$. ◇

Example 2.37

We have that $SL_n(\mathbb{R})$, $O_n(\mathbb{R})$ and $SO_n(\mathbb{R})$ are all proper subgroups of $GL_n(\mathbb{R})$. In fact $SO_n(\mathbb{R})$ is also a proper subgroup of both $SL_n(\mathbb{R})$ and $O_n(\mathbb{R})$.

We know that these are subgroups, since we showed that they were groups under matrix multiplication in an earlier example. ◇

Example 2.38

The alternating group A_n is a subgroup of the corresponding symmetric group S_n. ◇

Example 2.39

If G and H are groups, then the subset $\{(x, e) : x \in G\}$ of $G \times H$ is a subgroup of $G \times H$. Similarly, $\{(e, y) : y \in H\}$ is a subgroup of $G \times H$. ◇

Example 2.40

If G is any finite group and $x \in G$, the set $\langle x \rangle$ is always a subgroup. This follows since $x^n(x^m)^{-1} = x^{n-m}$, which is a power of x and so is an element of $\langle x \rangle$, and Corollary 2.21 tells us $\langle x \rangle$ is a subgroup. ◇

In fact, we can extend the last example to the set generated by any set of generators.

Theorem 2.22

Let $(G, *, e)$ be a group, and $X \subseteq G$. Then $\langle X \rangle$ is the smallest subgroup of G which contains X.

Finding Subgroups: *To find all the subgroups of a finite group, look at the subgroups generated by each element, then look at the subgroups generated by pairs of elements, then triples of elements, and so on. This procedure works because of Theorem 2.22.*

You can cut down the number of generating sets you need to check by noticing that if an element is in a subgroup, adding it to the set of generators of that subgroup gives nothing new.

Proof:

First we must show that $\langle X \rangle$ is a subgroup. This set consists of all products of powers of elements of X. If we have

$$x = x_1^{p_1} x_2^{p_2} \cdots x_n^{p_n} \qquad \text{and} \qquad y = y_1^{q_1} y_2^{q_2} \cdots y_m^{q_m},$$

where x_k and $y_l \in X$, p_k and $q_l \in \mathbb{Z}$, then we have that

$$\begin{aligned}(x_n^{-p_n} x_{n-1}^{-p_{n-1}} \cdots x_1^{-p_1})x &= x_n^{-p_n} x_{n-1}^{-p_{n-1}} \cdots x_1^{-p_1} x_1^{p_1} x_2^{p_2} \cdots x_n^{p_n} \\ &= x_n^{-p_n} x_{n-1}^{-p_{n-1}} \cdots x_2^{-p_2} x_2^{p_2} \cdots x_n^{p_n} \\ &\vdots \\ &= x_n^{-p_n} x_n^{p_n} = e,\end{aligned}$$

so $x^{-1} = x_n^{-p_n} x_{n-1}^{-p_{n-1}} \cdots x_1^{-p_1}$, which is a product of powers of elements of X, so $x^{-1} \in \langle X \rangle$. Similarly

$$xy = x_1^{p_1} x_2^{p_2} \cdots x_n^{p_n} y_1^{q_1} y_2^{q_2} \cdots y_m^{q_m}$$

is a product of powers of elements of X, so $xy \in \langle X \rangle$.

So $\langle X \rangle$ satisfies conditions (i) and (ii) of Theorem 2.20, so it is a subgroup of G.

Now assume that there is some subgroup H of G with $X \subseteq H \subset \langle X \rangle$. Then we can find some $x \in \langle X \rangle \setminus H$, so

$$x = x_1^{p_1} x_2^{p_2} \cdots x_n^{p_n}$$

where $x_k \in X$, $p_k \in \mathbb{Z}$. A simple induction argument shows that $x_k^{p_k} \in H$ for all k, no matter what power we have of p_k. But this means that $x_1^{p_1} x_2^{p_2} \in H$, since it is a product of elements of the subgroup H, and similarly $x_1^{p_1} x_2^{p_2} x_3^{p_3} \in H$. Proceeding inductively, we have $x_1^{p_1} x_2^{p_2} \cdots x_n^{p_n} \in H$, and so $x \in H$. This is a contradiction, and hence there is no subgroup H.

Therefore $\langle X \rangle$ is the smallest subgroup of G containing X. ■

It is worth noting that some texts actually define $\langle X \rangle$ to be the smallest subgroup of G containing X.

Example 2.41

The dihedral group of order 8, $D_8 = \{1, a, a^2, a^3, b, ab, a^2, a^3\}$ has subgroups

$$\begin{aligned}
\langle 1 \rangle &= \{1\} \cong C_1, & \langle a^2 \rangle &= \{1, a^2\} \cong C_2, \\
\langle b \rangle &= \{1, b\} \cong C_2, & \langle ab \rangle &= \{1, ab\} \cong C_2, \\
\langle a^2 b \rangle &= \{1, a^2 b\} \cong C_2, & \langle a^3 b \rangle &= \{1, a^3 b\} \cong C_2, \\
\langle a \rangle &= \{1, a, a^2, a^3\} \cong C_4, & \langle a^2, b \rangle &= \{1, a^2, b, a^2 b\} \cong V, \\
\langle a^2, ab \rangle &= \{1, a^2, ab, a^3 b\} \cong V, & \langle a, b \rangle &= D_8.
\end{aligned}$$

◇

Example 2.42

Consider $S_3 = \{e, (1,2,3), (1,3,2), (1,2), (2,3), (1,3)\}$. We can find all the subgroups of this group by looking at the sets generated by each element:

$$\begin{aligned}
\langle e \rangle &= e \\
\langle (1,2,3) \rangle = \langle (1,3,2) \rangle &= \{e, (1,2,3), (1,3,2)\} \\
\langle (1,2) \rangle &= \{e, (1,2)\} \\
\langle (2,3) \rangle &= \{e, (2,3)\} \\
\langle (1,3) \rangle &= \{e, (1,3)\}
\end{aligned}$$

Now we need to consider the sets generated by pairs of elements. For example, the set $\langle(1,2,3),(1,2)\rangle$ contains the elements e, $(1,2,3)$, $(1,3,2)$ and $(1,2)$ as well as

$$(2,3) = (1,2,3)(1,2) \qquad (1,3) = (1,2)(1,2,3).$$

So $\langle(1,2,3),(1,2)\rangle = S_3$. In fact, when we look at all possible pairings, we discover that

$$\langle(1,2,3),(1,2)\rangle = \langle(1,2,3),(2,3)\rangle = \langle(1,2,3),(1,3)\rangle = S_3$$

and

$$\langle(1,2),(2,3)\rangle = \langle(1,2),(1,3)\rangle = \langle(2,3),(1,3)\rangle = S_3.$$

So S_3 is the only other subgroup. ◇

Notice in all the above examples of finite groups, the order of any subgroup divides the order of the group. This is always true, but we need some new ideas before we can prove it.

Exercises

2.8.1. Let X be a subset of a group. Show that any one of the following is sufficient to show that X is not a subgroup:

(i) $e \notin X$,

(ii) there is an $x \in X$ with $x^{-1} \notin X$,

(iii) there is an x and $y \in X$ with $xy \notin X$,

(iv) there is an x and $y \in X$ with $xy^{-1} \notin X$.

2.8.2. For each of the following groups, find all its subgroups. For each subgroup, determine if it is isomorphic to a known group.

(i) D_6

(ii) C_8

(iii) $C_2 \times C_4$

(iv) $C_2 \times C_2 \times C_2$

(v) D_{10}

(vi) D_{12}

(vii) A_4

2.8.3. Let $s \in \mathbb{R}$. Show that $\{n + ms : n, m \in \mathbb{Z}\}$ is a subgroup of $\mathbb{R}$.

2.8.4. Show that $\mathbb{N}$ is not a subgroup of $(\mathbb{Z}, +, 0)$.

2.8.5. Show that every subgroup of a cyclic group is a cyclic group.

Show that every subgroup of an Abelian group is an Abelian group.

2.8.6. Show that every group has a cyclic subgroup.

2.9 Homomorphisms

Recall from abstract linear algebra that a linear transformation is a function from one vector space to another which preserves vector addition and scalar multiplication, ie. $T : V \to W$ is a linear transformation if and only if

$$T(v + w) = T(v) + T(w) \qquad \text{and} \qquad T(\lambda v) = \lambda T(v),$$

for all v, $w \in V$ and $\lambda \in \mathbb{F}$.

The analogue for groups should, then, be a function which preserves the group operation.

Definition 2.6
Let $(G, *, e)$ and $(H, \star, 1)$ be groups. A function $\alpha : G \to H$ is a ***(group) homomorphism*** *if*

$$\alpha(x * y) = \alpha(x) \star \alpha(y)$$

for all x, $y \in X$.

When using the multiplicative notation for groups, we will often simply write this condition as

$$\alpha(xy) = \alpha(x)\alpha(y).$$

It is immediate from this definition that group homomorphisms preserve the identity and inverse.

Proposition 2.23
Let G and H be groups and $\alpha : G \to H$ a homomorphism. Then

(i) $\alpha(e_G) = e_H$,

(ii) $\alpha(x^{-1}) = (\alpha(x))^{-1}$ *for all* $x \in X$.

Proof:

(i) Let $y = \alpha(x)$ for some $x \in G$, so that

$$y\alpha(e_G) = \alpha(x)\alpha(e_G) = \alpha(xe_G) = \alpha(x) = y = ye_H.$$

The cancellation law then tells us that $\alpha(e_G) = e_H$.

(ii) Given any $x \in G$, we have that

$$\alpha(x^{-1})\alpha(x) = \alpha(x^{-1}x) = \alpha(e_G) = e_H.$$

So $\alpha(x^{-1}) = \alpha(x)^{-1}$. ■

Using this proposition we can show, using induction if needed, that

$$\alpha(x^n) = \alpha(x)^n$$

for any $n \in \mathbb{Z}$.

Example 2.43

Let $V = \{1, a, b, ab\}$ be the four-group, and $C_4 = \{1, a, a^2, a^3\}$ be the cyclic group of order 4. Consider the function $\alpha : V \to C_4$ definied by the following table:

x	$\alpha(x)$
1	1
a	a^2
b	a^2
ab	1

Checking by hand, we can verify that this is indeed a homomorphism. For example $a^2 = 1$ in V so $\alpha(a^2) = \alpha(1) = 1$, and $\alpha(a)\alpha(a) = a^2a^2 = 1$. ◇

Example 2.44

If we look at the groups $\mathbb{Z}_3$, where the group operation is addition modulo 3, and the group $C_6 = \{1, a, a^2, a^3, a^4, a^5\}$, then we have the following homomorphisms from $\mathbb{Z}_3 \to C_6$:

$$\begin{aligned}\alpha(x) &= 1\\ \beta(x) &= a^{2x}\\ \gamma(x) &= a^{-2x}\end{aligned}$$

To verify that β is a homomoprhism, for example, we need to check that $\beta(x + y) = \beta(x)\beta(y)$:

Note: *Observe here that $\mathbb{Z}_3$ uses additive notation, while C_6 uses multiplicative notation, and we need to use the appropriate form of notation when verifying that we have a homomorphism.*

$$\begin{aligned}\beta(x + y \pmod 3) &= a^{2(x+y \pmod 3)} = a^{2x+2y \pmod 6}\\ \beta(x)\beta(y) &= a^{2x}a^{2y} = a^{2x+2y \pmod 6},\end{aligned}$$

noting that in C_6, $a^x a^y = a^{x+y \text{ (mod 6)}}$. So β is a homomorphism. You could also verify this fact by case-by-case checking of results.

On the other hand, the function $\delta : \mathbb{Z}_3 \to C_6$ defined by $\delta(x) = a^x$ is not a homomorphism, because

$$\delta(1 + 2 \pmod 3) = \delta(0) = a^0 = 1,$$

but

$$\delta(1)\delta(2) = a^1a^2 = a^3 \neq 1.$$

◇

Example 2.45

Let $GL_n(\mathbb{R})$ be the group of all invertible real-valued matrices, and consider the determinant function $\det : GL_n(\mathbb{R}) \to R^\times$ given by

$$\det(A) = |A|.$$

Since

$$\det(AB) = |AB| = |A||B| = \det(A)\det(B),$$

this is a homomorphism. ◇

If we once again consider the analogy with abstract linear algebra, you may recall that the image of a linear subspace under a linear transformation is a subspace of the range. If the analogy with linear algebra is to hold, the same thing ought to be true for subgroups.

Proposition 2.24
If G and H are groups, $\alpha : G \to H$ is a homomorphism, and K is a subgroup of G, then $\alpha(K)$ is a subgroup of H.

Proof:
Let x, $y \in \alpha(K)$, so that there are some u and $v \in K$ such that $x = \alpha(u)$ and $y = \alpha(v)$. Then, noting that $uv^{-1} \in K$,

$$xy^{-1} = \alpha(u)(\alpha(v))^{-1} = \alpha(uv^{-1}) \in \alpha(K).$$

So by Corollary 2.21, $\alpha(K) \leq H$. ■

Example 2.46
We know from Example 2.33 that the subgroups of V are $\{1\}$, $\{1, a\}$, $\{1, b\}$, $\{1, ab\}$ and the whole group V. The images of these sets under the homomorphism α of Example 2.43 are $\{1\}$, $\{1, a^2\}$, $\{1, a^2\}$, $\{1\}$ and $\{1, a^2\}$, respectively. ◇

Since $G \leq G$, the following is an immediate corollary of the proposition.

Corollary 2.25
If G and H are groups, and $\alpha : G \to H$ is a homomorphism, then $\alpha(G)$ is a subgroup of H.

In other words, the image of a homomorphism is a subgroup of the codomain.

We have a similar result for inverse images of subgroups.

Proposition 2.26
If G and H are groups, $\alpha : G \to H$ is a homomorphism, and K is a subgroup of H, then $\alpha^{-1}(K)$ is a subgroup of G.

Proof:
Let x, $y \in \alpha^{-1}(K)$, so that there are some u and $v \in K$ such that $u = \alpha(x)$ and $v = \alpha(y)$. Then,

$$\alpha(xy^{-1}) = \alpha(x)(\alpha(y))^{-1} = uv^{-1} \in K,$$

so $xy^{-1} \in \alpha^{-1}(K)$. Therefore by Corollary 2.21, $\alpha^{-1}(K) \leq G$. ■

You may also recall from linear algebra that the kernel of a linear transformation is a subspace of the domain. This leads us to the following definition and corollary.

Definition 2.7
If G and H are groups, and $\alpha : G \to H$ is a homomorphism, then the ***kernel*** *of α is the set*

$$\ker \alpha = \{x \in X : \alpha(x) = e_H\}$$

of all elements of the group G whose image is the identity.

Corollary 2.27
If G and H are groups, and $\alpha : G \to H$ is a homomorphism, then $\ker \alpha$ is a subgroup of G.

Proof:
Notice that $\ker \alpha = \alpha^{-1}(\{e_H\})$, and $\{e_H\} \leq H$, so by Proposition 2.26, $\ker \alpha \leq G$. ■

Example 2.47
In Example 2.43, the kernel of the homomorphism is $\{1, ab\}$, which is a subgroup of V, and the image of the homomorphism is $\{1, a^2\}$, which is a subgroup of C_4. ◇

Example 2.48
The kernel of the determinant map from the previous example is the set of all matrices whose determinant is 1, ie.

$$\ker \det = SL_n(\mathbb{R}).$$

On the other hand, there are matrices whose determinant is any number you choose, so the image of $GL_n(\mathbb{R})$ under det is all of $\mathbb{R} \setminus \{0\}$. ◇

Example 2.49
Parity can be regarded as a function that takes permutations to elements of the multiplicative group of integers $\mathbb{Z} \setminus \{0\}$. Theorem 1.6 tells us that this is a homomorphism.

The kernel of parity is the subgroup A_n of all permutations whose parity is 1, ie.

$$\ker \text{parity} = A_n.$$

On the other hand, the image of S_n under the parity homomorphism is simply the set $\{1, -1\}$, which is a subgroup of the multiplicative group of integers. ◇

Just as we are particularly interested in functions which are one-to-one, onto, or bijective, we are interested in homomorphisms which are one-to-one, onto, or bijective.

Definition 2.8
Let G and H be groups, and $\alpha : G \to H$ a homomorphism. If α is one-to-one (or injective), then we say that it is a ***monomorphism****. If α is onto (or sujective), then we say that it is an* ***epimorphism****. If α is a bijection, then we say that it is an* ***isomorphism****.*

If $\alpha : G \to G$ is an isomorphism, then we call α an ***automorphism****. The set of all automorphisms of G is denoted* $\mathrm{Aut}(G)$.

This definition of isomorphism agrees with the definition that we have been using, but can also be applied to infinite groups. The concept of "correspondence" of elements that we have been informally using to translate between the two Cayley tables is, formally, a bijection; while the fact that the Cayley tables correspond means that the group operation is preserved by the bijection, giving us a homomorphism. If there is an isomorphism between two groups G and H, then we say that the groups are ***isomorphic*** and write $G \cong H$ as usual.

Example 2.50

Consider the additive group of reals numbers, $(\mathbb{R}, +, 0)$, and the multiplicative group of positive real numbers, $(\mathbb{R}^+, \times, 1)$. The exponential function

$$\exp : x \mapsto e^x$$

is a homomorphism between these two groups, since

$$\exp(x + y) = e^{x+y} = e^x e^y = \exp(x) \exp(y).$$

Furthermore, the exponential function is one-to-one (a fact you should be familiar with from elementary calculus), and the range of the exponential function is all positive real numbers. Hence exp is an isomorphism, and the two groups are isomorphic.

In fact, this isomorphism is not the only possible choice. Any function of the form

$$x \mapsto a^x$$

for $a > 0$ is an isomorphism. Going in the reverse direction, the corresponding logarithms

$$x \mapsto \log_a x,$$

regarded as functions from $\mathbb{R}^+$ to $\mathbb{R}$, are also isomorphisms. ◇

The following proposition collects some useful facts about homomorphisms.

Proposition 2.28
Let G, H and K be groups, and let $\alpha : G \to H$ and $\beta : H \to K$ be homomorphisms.

(i) $\beta \circ \alpha : G \to K$ *is a homomorphism,*

(ii) if α and β are monomorphisms, so is $\beta \circ \alpha$,

(iii) if α and β are epimorphisms, so is $\beta \circ \alpha$,

(iv) if α and β are isomorphisms, so is $\beta \circ \alpha$,

(v) if α is an isomorphism, so is the inverse function α^{-1},

(vi) α is a monomorphism if and only if $\ker \alpha = \{e\}$,

Proof:

(i) We observe that

$$\beta(\alpha(xy)) = \beta(\alpha(x)\alpha(y)) = \beta(\alpha(x))\beta(\alpha(y)),$$

so $\beta \circ \alpha$ is a homomorphism.

(ii–iv) These follow immediately from (i) which tells us that the composition is a homomorphism, and parts (ii–iv) of Proposition 1.2 which tell us that the composition is, respectively, one-to-one, onto, and bijective.

(vi) If α is an isomorphism, then for any x, $y \in H$, we have u and $v \in G$ such that $\alpha(u) = x$ and $\alpha(v) = y$, so

$$xy = \alpha(u)\alpha(v) = \alpha(uv).$$

But $u = \alpha^{-1}(x)$ and $v = \alpha^{-1}(y)$, so

$$\alpha^{-1}(xy) = \alpha^{-1}(\alpha(uv)) = uv = \alpha^{-1}(x)\alpha^{-1}(y).$$

Hence α^{-1} is a homomorphism.

Furthermore, parts (v) of Proposition 1.2 tells us that α^{-1} is a bijection, so α^{-1} is an isomorphism.

(v) If α is a monomorphism and $\alpha(x) = e$, then $\alpha(x) = \alpha(e)$, and since α is injective, $x = e$. So $\ker \alpha = \{e\}$.

On the other hand, if $\ker \alpha = \{e\}$, then if we have x and $y \in G$ such that $\alpha(x) = \alpha(y)$, then

$$\alpha(xy^{-1}) = \alpha(x)\alpha(y)^{-1} = \alpha(x)\alpha(x)^{-1} = e,$$

so $xy^{-1} \in \ker \alpha$, and hence $xy^{-1} = e$. But then

$$x = xy^{-1}y = ey = y,$$

so α is injective and hence a monomorphism. ■

Exercises

2.9.1. Find all the homomorphisms from C_2 to V. Describe the kernel and image of each.

2.9.2. Let $\mathbb{Z}$ be the additive group of integers. Show that for each $m \in \mathbb{Z}$, the function $\alpha_m : \mathbb{Z} \to \mathbb{Z}$, given by

$$\alpha_m(x) = mx$$

is a homomorphism. Show that if $m \neq 0$ then α_m is a monomorphism. Show that it is an epimorphism if and only if $m = \pm 1$.

2.9.3. Let $\mathbb{Q}$ be the additive group of rational numbers. Show that for each $r \in \mathbb{Q}$, the function $\alpha_r : \mathbb{Q} \to \mathbb{Q}$ given by

$$\alpha_r(x) = rx$$

is a homomorphism. Show that if $r \neq 0$ then α_r is an automorphism.

2.9.4. Consider the group $(G, *, e)$, where $G = \{(x, y) : x, y \in \mathbb{R}, x \neq 0\}$, $(x, y) * (x', y') = (xx', xy' + y)$ and $e = (1, 0)$, and the group $(H, \cdot, I_2)$, where

$$H = \left\{ \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} : a, b \in \mathbb{R}, a \neq 0 \right\},$$

$\cdot$ is matrix multiplication, and I_2 is the 2 by 2 identity matrix. Show that G and H are isomorphic.

2.9.5. Show that every isomorphism $\alpha : (\mathbb{R}, +, 0) \to (\mathbb{R}^+, \times, 1)$ satisfies

$$\alpha(x) = a^x$$

for some number $a > 0$.

Show that every isomorphism $\alpha : (\mathbb{R}^+, \times, 1) \to (\mathbb{R}, +, 0)$ satisfies

$$\alpha(x) = \log_a x$$

for some number $a > 0$.

2.9.6. Let G and H be two groups. Show that each of the following is a homomorphism:

(i) $\alpha : G \to G \times H$, where $\alpha(g) = (g, 1)$,
(ii) $\alpha : H \to G \times H$, where $\alpha(h) = (1, h)$,
(iii) $\alpha : G \times H \to G$, where $\alpha(g, h) = g$,
(iv) $\alpha : G \times H \to H$, where $\alpha(g, h) = h$,
(v) $\alpha : G \times H \to H \times G$, where $\alpha(g, h) = (h, g)$,
(vi) $\alpha : G \to G \times G$, where $\alpha(g) = (g, g)$.

Which of these are monomorphisms, which are epimorphisms, and which are isomorphisms?

2.9.7. Find all the automorphisms of V.

2.9.8. Let G be a group. Show that $(\mathrm{Aut}(G), \circ, \mathrm{id})$ is a group, where $\circ$ is composition and $\mathrm{id} : G \to G$ is the identity function $\mathrm{id}(x) = x$ for all $x \in G$.

Assignment 2

The following exercises are due Friday, March 5th.

2.1 Exercises 1, 2.

2.2 Exercises 2, 3, 5.

2.3 Exercises 2, 3, 4.

2.4 Exercises 1.

Assignment 3

The following exercises are due Friday, March 12th.

2.5 Exercises 1, 2, 7.

2.7 Exercises 1, 4.

2.8 Exercises 2, 3.

2.9 Exercises 1, 2, 4, 7.

Chapter 3

The Structure of Groups

We are interested in understanding the structure of groups, particularly finite groups, as a way of potentially distinguishing groups. In this section we will see a number of ways of looking at structure within a group.

3.1 The Subgroup Lattice

At a very coarse level, if two groups are isomorphic then their subgroups must be in bijective correspondence with one another.

Proposition 3.1
Let G and H be two groups, and let $\mathrm{Sub}(G)$ and $\mathrm{Sub}(H)$ be the set of subgroups of G and H respectively. If $G \cong H$ then there is a bijection between $\mathrm{Sub}(G)$ and $\mathrm{Sub}(H)$.

Proof:
Since $G \cong H$ there is an isomorphism $\alpha : G \to H$, and its inverse function $\alpha^{-1} : H \to G$ is also an isomorphism by Proposition 2.28. Since by Proposition 2.24, the image $\alpha(K)$ of a subgroup K of G is a subgroup of H, we can define a function

$$\begin{aligned} \overline{\alpha} : \mathrm{Sub}(G) &\to \mathrm{Sub}(H) \\ K &\mapsto \alpha(K). \end{aligned}$$

The function $\overline{\alpha}$ is one-to-one, since if we have two subgroups K_1 and K_2 of G such that $\overline{\alpha}(K_1) = \overline{\alpha}(K_2)$, then

$$K_1 = \alpha^{-1}(\alpha(K_1)) = \alpha^{-1}(\overline{\alpha}(K_1)) = \alpha^{-1}(\overline{\alpha}(K_{12})) = \alpha^{-1}(\alpha(K_2)) = K_2,$$

since $\alpha^{-1} \circ \alpha$ is the identity function.

The function $\overline{\alpha}$ is onto, since if K is a subgroup of H, then $\alpha^{-1}(K)$ is a subgroup of G, and

$$\overline{\alpha}(\alpha^{-1}(K)) = \alpha(\alpha^{-1}(K)) = K$$

since $\alpha \circ \alpha^{-1}$ is the identity function.

So $\overline{\alpha}$ is a bijection. ■

Corollary 3.2
If G and H are finite groups with different numbers of subgroups, then G and H cannot be isomorphic.

Example 3.1
From Example 2.32 C_4, we know that C_4 has 3 subgroups. On the other hand, Example 2.33 tells us that V has 5 subgroups, so V is not isomorphic to C_4. ◇

However, it is certainly conceivable that two groups may have the same number of subgroups, but fail to be isomorphic. In this case we need to investigate the relationships between subgroups of a group. For instance, if we have a group G and subgroups H and K of G such that $K \subseteq H$, then it is immediate from Corollary 2.21 that K is a subgroup of H. So a good starting point is to consider which subgroups are contained in other subgroups.

Example 3.2
From Example 2.32 $C_4 = \{1, a, a^2, a^3\}$ has the subgroups $\{1\}$, $\langle a^2 \rangle = \{1, a^2\}$ and $\{1, a, a^2, a^3\}$. We can easily see that $\{1\} \leq \langle a^2 \rangle \leq C_4$. ◇

Noting that each of these is subgroups is contained in the next, we can represent this situation diagramatically as follows:

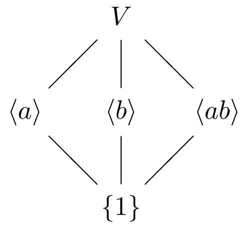
$$\begin{tikzcd}
C_4 \arrow[d, dash] \\
\langle a^2 \rangle \arrow[d, dash] \\
\{1\}
\end{tikzcd}$$

This sort of diagram is a graphical representation of the ***subgroup lattice*** of the group. The idea is that if a subgroup is contained in another, with no intermediate subgroups, we write it higher on the page and join the two subgroups with a line. We also try to draw the diagram so that subgroups with the same number of elements are the same distance up the page.

Here are some more examples.

Example 3.3
From Example 2.33, the vierergruppe $V = \{1, a, b, ab\}$ has the subgroups $\{1\}$, $\langle a \rangle = \{1, a\}$, $\langle b \rangle = \{1, b\}$, $\langle ab \rangle = \{1, ab\}$ and $\{1, a, b, ab\}$.

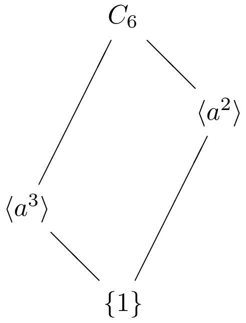
The subgroup lattice of V is:



◇

Example 3.4

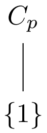
From Example 2.34, the cyclic group or order 6, $C_6 = \{1, a, a^2, a^3, a^4, a^5\}$ has the subgroups $\{1\}$, $\langle a^3\rangle = \{1, a^3\}$, $\langle a^2\rangle = \{1, a^2, a^4\}$, and C_6. The subgroup lattice of C_6 is:



◇

Example 3.5

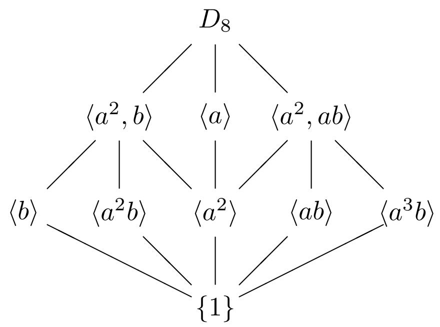
Let p be a prime number, and C_p the cyclic group of order p. From Example 2.35 C_p only has the trivial subgroups $\{1\}$ and C_p. The subgroup lattice of C_p is always:



◇

Example 3.6

From Example 2.41, the dihedral group of order 8, $D_8 = \{1, a, a^2, a^3, b, ab, a^2, a^3\}$ has subgroups $\{1\}$, $\langle a^2\rangle = \{1, a^2\}$, $\langle b\rangle = \{1, b\}$, $\langle ab\rangle = \{1, ab\}$, $\langle a^2 b\rangle = \{1, a^2 b\}$, $\langle a^3 b\rangle = \{1, a^3 b\}$, $\langle a\rangle = \{1, a, a^2, a^3\}$, $\langle a^2, b\rangle = \{1, a^2, b, a^2 b\}$, $\langle a^2, ab\rangle = \{1, a^2, ab, a^3 b\}$, and D_8. The subgroup lattice of D_8 is:



◇

Notice that in these diagrams, there is always a unique smallest subgroup which is bigger than any pair of subgroups. This is a corollary of Theorem 2.22.

Corollary 3.3
If G is a group and H and K are subgroups of G, then $\langle H \cup K\rangle$ is the smallest subgroup which contains both H and K.

This subgroup is usually quite different from the union of the two sets. Indeed, we have the following:

Proposition 3.4
Let H and K be subgroups of G. Then $H \cup K$ is a subgroup if and only if either $H \subseteq K$ or $K \subseteq H$.

Proof:
If $H \subseteq K$, then $H \cup K = K$, so $H \cup K$ is a subgroup. Similarly, if $K \subseteq H$, then $H \cup K = H$, so $H \cup K$ is a subgroup.

Conversely, if neither H nor K is a subset of the other, then there is some $x \in H \setminus K$ and $y \in K \setminus H$. Also $x^{-1} \in H$, since H is a subgroup. But then if $xy \in H$, we have $x^{-1}(xy) = y \in H$, but since $y \in K \setminus H$, this means that $y \notin H$, which is a contradicition. Therefore $xy \notin H$. But a similar argument shows that $xy \notin K$. So $xy \notin H \cup K$. So $H \cup K$ is not a subgroup of G. ■

The following theorem shows us that there is also a subgroup which is contained in both H and K.

Theorem 3.5
Let $(G, *, e)$ be a group, and H and K subgroups of G. Then $H \cap K$ is the largest subgroup of G which is contained in both H and K.

Proof:
We first need to show that $H \cap K$ is a subgroup. If x, $y \in H \cap K$, then $xy^{-1} \in H$, since H is a subgroup, and $xy^{-1} \in K$, since K is a subgroup. Therefore $xy^{-1} \in H \cap K$, and so by Corollary 2.21, $H \cap K$ is a subgroup of G.

Since $H \cap K$ is the largest set contained in both H and K, it must also be the largest subgroup contained in both. ■

We will denote $\langle H \cup K \rangle$ by $H \vee K$ and call it the ***join*** of H and K. We will denote $H \cap K$ by $H \wedge K$, and call it the ***meet*** of H and K. The reason for this terminology will be come clear when we look at abstract lattices.

The significance of the lattice of subgroups is that if two groups do not have similar lattices of subgroups, they cannot be isomorphic, so it provides a nice pictorial way of demonstrating that two groups are distinct. To show this, we first need to show that homomorphisms preserve the relationship of inclusion of subgroups.

Proposition 3.6
If G and H are groups, $\alpha : G \to H$ is a homomorphism, and K_1 and K_2 are subgroups of G with $K_1 \subseteq K_2$, then $\alpha(K_1)$ is a subgroup of $\alpha(K_2)$.

Furthermore, if α is a monomorphism, and $K_1 \subset K_2$, then $\alpha(K_1)$ not equal to $\alpha(K_2)$.

Proof:
We know from Proposition 2.24 that $\alpha(K_1)$ and $\alpha(K_2)$ are subgroups of H, and it is immediate from the definition of the image of a set under a function that $\alpha(K_1) \subseteq \alpha(K_2)$ if $K_1 \subseteq K_2$. So $\alpha(K_1) \leq \alpha(K_2)$.

If α is a monomorphism in addition, then since there is some $g \in K_2$, but not in K_1, we cannot have $\alpha(h) = \alpha(g)$ for any $h \in K_1$ (otherwise α would not be one-to-one). Hence $\alpha(K_1)$ is properly contained in $\alpha(K_2)$. ■

Corollary 3.7
If G and H are groups, $\alpha : G \to H$ is a homomorphism, and K_1 and K_2 are subgroups of G, then $\alpha(K_1 \vee K_2) = \alpha(K_1) \vee \alpha(K_2)$ and $\alpha(K_1 \wedge K_2) = \alpha(K_1) \wedge \alpha(K_2)$.

Proof:
We know that $\alpha(K_1) \vee \alpha(K_2)$ is the smallest subgroup which contains both $\alpha(K_1)$ and $\alpha(K_2)$, but since K_1 and $K_2 \subseteq K_1 \vee K_2$, we have that $\alpha(K_1)$ and $\alpha(K_2) \subseteq \alpha(K_1 \vee K_2)$, hence $\alpha(K_1) \vee \alpha(K_2) \subseteq \alpha(K_1 \vee K_2)$.

Conversely, if $\alpha^{-1}(\alpha(K_1) \vee \alpha(K_2))$ is a subgroup of G which contains both K_1 and K_2, so $K_1 \vee K_2 \subseteq \alpha^{-1}(\alpha(K_1) \vee \alpha(K_2))$, and hence

$$\alpha(K_1 \vee K_2) \subseteq \alpha(\alpha^{-1}(\alpha(K_1) \vee \alpha(K_2))) = \alpha(K_1) \vee \alpha(K_2).$$

Hence $\alpha(K_1) \vee \alpha(K_2) = \alpha(K_1 \vee K_2)$.

The proof of the case for $\wedge$ is left as an exercise. ■

We will say that two groups G and H have corresponding, or isomorphic, subgroup lattices if there is a bijection f from $\mathrm{Sub}(G)$ to $\mathrm{Sub}(H)$ so that $f(K_1) \vee f(K_2) = f(K_1 \vee K_2)$, and $f(K_1) \wedge f(K_2) = f(K_1 \wedge K_2)$.

Corollary 3.8
If G and H are two groups whose subgroup lattices do not correspond, then G and H are not isomorphic.

Proof:
If G and H are isomorphic, then Proposition 3.1 tells us that $\overline{\alpha}$ is a bijection from $\mathrm{Sub}(G)$ to $\mathrm{Sub}(H)$, and Corollary 3.7 says that $\overline{\alpha}(K_1 \vee K_2) = \overline{\alpha}(K_1) \vee \overline{\alpha}(K_2)$ and $\overline{\alpha}(K_1 \wedge K_2) = \overline{\alpha}(K_1) \wedge \overline{\alpha}(K_2)$. So isomorphic groups have corresponding subgroup lattices.

The contrapositive of this result is the corollary. ■

Example 3.7
The groups C_4 and V have different subgroup lattices, so they are not isomorphic. ◇

Note that the converse of the corollary is not true. We know, for example, that if p is prime, the groups C_p all have corresponding subgroup lattices, yet the groups are clearly not isomorphic.

Exercises

3.1.1. Find the subgroup lattice of the group D_6.

3.1.2. Find the subgroup lattice of the group C_8.

3.1.3. Find the subgroup lattice of the group $C_2 \times C_4$.

3.1.4. Find the subgroup lattice of the group $C_2 \times C_2 \times C_2$.

3.1.5. Find the subgroup lattice of the group D_{10}.

3.1.6. Find the subgroup lattice of the group D_{12}.

3.1.7. Find the subgroup lattice of the group A_4

3.1.8. Complete the proof of Corollary 3.7.

3.2 Extension: Lattices

The pattern that subgroups of a group make under inclusion is a particular example of a general phenomenon. The key idea is that we know when one subgroup is “larger” than another, that we can find the largest thing smaller than two subgroups (the meet) and that we can find the smallest thing larger than the two subgroups (the join).

This idea is essentially the same as what happens with general subsets of a set. We know when one subset is “larger” than another, we can find the largest thing smaller than two subsets (the intersection) and we can find the smallest thing larger than the two subsets (the union).

To explore this similarity further, we need to introduce a general concept that we can use to model the idea of one thing being larger then another.

Definition 3.1
Let X and Y be sets. A ***relation*** *between X and Y is a subset R of $X \times Y$, where $x \in X$ and $y \in Y$ are considered to be related by R if and only if $(x, y) \in R$.*

We write xRy if $(x, y) \in R$. If $X = Y$ we say that R is a relation on X.

Note that you should not confuse this definition of relation with the notion of a relation on the elements of a group.

The concept of a relation is extremely general, and can be used to model a great many fundamental mathematical concepts.

Example 3.8
If X is any set, equality can be regarded as the relation $R = \{(x, x) : x \in X\} \subseteq X \times X$. Here xRy if and only if $(x, y) \in R$ if and only if $x = y$. ◇

Example 3.9
If X and Y are any sets and $f : X \to Y$ is a function, the graph $R = \{(x, f(x)) : x \in X\} \subset X \times Y$ is a relation where xRy if and only if $y = f(x)$. In fact functions are sometimes defined in this way as a special case of the concept of a relation. ◇

Example 3.10
In the real numbers, the set $L = \{(x, y) : x \leq y\} \in \mathbb{R} \times \mathbb{R}$ is a relation where xLy if and only if $x \leq y$. ◇

Example 3.11
If $\mathcal{P}(X)$ is the power set of some set X, then the set $\subseteq = \{(A, B) : A \text{ is a subset of } B\}$ is a relation where $A \subseteq B$ if and only if A is a subset of B. ◇

Example 3.12
If G is a group, and X is the set of subgroups of G, then the set $\leq = \{(A, B) : A \text{ is a subgroup of } B\}$ is a relation where $A \leq B$ if and only A is a subgroup of B. ◇

Because of the generality of relations, we need to impose some additional conditions to make them useful in modelling particular situations.

Definition 3.2
Let X and Y be sets, and R a relation on X. Let x, y and $z \in X$.

We say that R is ***reflexive*** *if xRx for all $x \in X$.*

We say that R is ***symmetric*** *if xRy implies yRx.*

We say that R is ***antisymmetric*** *if xRy and yRx implies $x = y$.*

We say that R is ***transitive*** *if xRy and yRz implies xRz.*

A ***partial order*** *on X is a relation on X which is reflexive, transitive and antisymmetric.*

Example 3.13

The $\leq$, $<$, $>$ and $\geq$ relations on any set of numbers. All are antisymmetric and transitive, but not symmetric. The relations $\leq$ and $\geq$ are reflexive, but $<$ and $>$ are not. ◇

Example 3.14

The relation $\subseteq$ of $\mathcal{P}(X)$ is a partial order. ◇

Example 3.15

The relation $\leq$ on the set of subgroups of a group is a partial order. ◇

Notice that if $\preceq$ is a partial order on a set X, and x, $y \in X$, then it may be the case that neither $x \preceq y$ nor $y \preceq x$. If this is the case, we say that x and y are ***incomparable elements*** of X.

Example 3.16

The sets $\{1\}$ and $\{2, 3\}$ are incomparable elements of $\mathcal{P}(\{1, 2, 3\})$ under the subset partial order $\subseteq$. ◇

So a partial order seem to encapsulate the general idea of something being bigger than something else. Now we need to model the idea of a meet and a join.

Definition 3.3

If X is a set, $\preceq$ is a partial order on X, and x and $y \in X$, then $a \in X$ is a ***lower bound*** *for x and y if $a \preceq x$ and $a \preceq y$. We say that a is the* ***greatest lower bound*** *of x and y if given any lower bound z of x and y, we have that $z \preceq a$.*

Similarly, a is an ***upper bound*** *for x and y if $x \preceq a$ and $y \preceq a$. We say that a is the* ***least upper bound*** *of x and y if given any upper bound z of x and y, we have that $a \preceq z$.*

In general, we denote the greatest lower bound of x and y by $x \wedge y$, and the least upper bound of x and y by $x \vee y$.

A ***lattice*** *$(X, \preceq)$ is a set with a partial order such that every pair of elements has a greatest lower bound and a least upper bound.*

The examples of partial orders earlier in this section all have the lattice property.

Example 3.17

The pair $(\mathbb{R}, \leq)$ is a lattice. Since for any x and y, we have $x \leq y$ or $y \leq x$ (or both), then $x \vee y = \min x, y$ and $x \wedge y = \max x, y$. ◇

Example 3.18

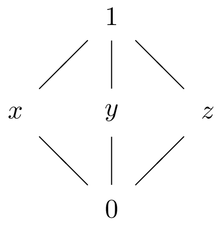
If X is any set, then the pair $(\mathcal{P}(X), \subseteq)$ is a lattice. Given any two subsets A and B of X, we have $A \wedge B = A \cup B$ and $A \vee B = A \cap B$. $\diamond$

Example 3.19

The subgroup relation $\leq$ on the set of subgroups $\mathrm{Sub}(G)$ of a group G makes $(\mathrm{Sub}(G), \leq)$ a lattice, since if H and $K \in \mathrm{Sub}(G)$ we have $H \vee K = \langle H \cup K \rangle$ and $H \wedge K = H \cap K$. $\diamond$

Example 3.20

Let $X = \{0, x, y, 1\}$, and let $\preceq$ be the partial order defined by $0 \preceq x$, $0 \preceq y$, $0 \preceq x$, $0 \preceq 1$, $x \preceq 1$, $y \preceq 1$ and $y \preceq 1$. Then $(X, \preceq)$ is a lattice, and we can represent it diagramatically as



$\diamond$

In the previous section, we showed that if the subgroup lattice of two groups didn't agree, then the groups could not be isomorphic. The heart of the result was showing that the isomorphism α between the groups produced a function between the subgroups $\overline{\alpha}$ which preserved meet and join.

Definition 3.4

Let $(X, \preceq)$ and $(Y, \leq)$ be two partially ordered sets. A function $\alpha : X \to Y$ is an order-preserving function if whenever we have x and $y \in X$ such that $x \preceq y$, we have $\alpha(x) \leq \alpha(y)$.

If $(X, \preceq)$ and $(Y, \leq)$ are lattices, then $\alpha : X \to Y$ is a lattice homomorphism if $\alpha(x \vee y) = \alpha(x) \vee \alpha(y)$, and $\alpha(x \wedge y) = \alpha(x) \wedge \alpha(y)$. If α is a bijective lattice homomorphism, we say that it is a lattice isomorphism.

Example 3.21

Let $(X, \preceq)$ be as in Example 3.20, and V be the four-group. The function $\alpha : X \to \mathrm{Sub}(V)$ defined by the table

t	$\alpha(t)$
0	$\{e\}$
x	$\{e, a\}$
y	$\{e, b\}$
z	$\{e, ab\}$
1	V

is a lattice isomorphism. Perhaps the easiest way to grasp this fact is to observe that the diagrams for each lattice correspond. ◇

Example 3.22

Consider the homomorphism $\alpha : V \to C_4$ of Example 2.43. The corresponding map between subgroups of these groups is $\overline{\alpha}$, and is given by the following table

H	$\overline{\alpha}(H)$
$\{e\}$	$\{e\}$
$\{e, a\}$	$\{e, a^2\}$
$\{e, b\}$	$\{e, a^2\}$
$\{e, ab\}$	$\{e\}$
V	$\{e, a^2\}$

is a lattice homomorphism. ◇

The essential content of Proposition 3.6 and Corollary 3.7 is then:

Proposition 3.9

If G and H are groups, and $\alpha : G \to H$ is a homomorphism, then $\overline{\alpha} : \mathrm{Sub}(G) \to \mathrm{Sub}(H)$ is an order-preserving map.

Corollary 3.10

If G and H are groups, and $\alpha : G \to H$ is a homomorphism, then $\overline{\alpha} : \mathrm{Sub}(G) \to \mathrm{Sub}(H)$ is a lattice homomorphism.

So we can then re-phrase Corollary 3.8 in the following way:

Corollary 3.11

If G and H are groups, and the subgroup lattices of G and H are not isomorphic, then G and H are not isomoprhic.

We can use Exercise 3.2.1 to prove the following proposition.

Proposition 3.12

Let $(X, \preceq)$ and $(Y, \leq)$ be lattices, and $\alpha : X \to Y$ a lattice homomorphism. Then α is an order-preserving function.

Proof:

See Exercise 3.2.2. ■

In fact, we could prove Corollary 3.7 directly, and use this proposition to conclude that Proposition 3.6 must hold.

So the abstract concept of a lattice helps us understand the structure of subgroups within a group, just as the abstract structure of a group helps us understand concrete situations such as the symmetries of a set.

Exercises

3.2.1. Let $\preceq$ be a partial order on X. Show that if $x \preceq y$ that $x \wedge y = x$ and $x \vee y = y$.

3.2.2. Prove Proposition 3.12.

3.2.3. Consider the natural numbers $\mathbb{N}$ with the "divides" relation $x \mid y$ if and only if $y = kx$ for some $k \in \mathbb{N}$ (ie. if x divides y). Show that $\mid$ is a partial order, and that $x \wedge y$ is the greatest common divisor of x and y and $x \vee y$ is the least common multiple of x and y.

3.2.4. Show that if $\preceq$ is a partial order on X, then the reverse relation $\succeq$ defined by $x \succeq y$ if and only if $y \preceq x$ is a partial order. Show that $(X, \preceq)$ is a lattice if and only if $(X, \succeq)$ is a lattice.

3.2.5. Let $F(D, \mathbb{R})$ be the set of real-valued functions on some fixed domain $D \subseteq \mathbb{R}$ (ie. the typical functions considered in calculus). Show that the relation defined by $f \leq g$ if $f(x) \leq g(x)$ for all $x \in D$ is a partial order.

Give an example of two functions which are incomparable.

Show that $(F(D, \mathbb{R}), \leq)$ is a lattice, where $f \wedge g$ and $f \vee g$ are the functions defined by

$$(f \wedge g)(x) = \min f(x), g(x) \qquad \text{and} \qquad (f \vee g)(x) = \max f(x), g(x)$$

respectively.

3.3 The Centre and Centralizers

Abelian groups are much nicer to work with algebraically than non-Abelian groups. However, even in the case of non-Abelian groups there may be large parts of the group which commute with each other.

Recall that two elements x and $y \in G$ commute with one another if

$$xy = yx.$$

Multiplying both sides on the right by x^{-1}, we can state this equivalently as saying that x and y commute if and only if

$$xyx^{-1} = y,$$

or, multiplying on the other side, if and only if

$$x^{-1}yx = y.$$

The set of all elements which commute with every other element of the group is called the ***centre*** of the group, denoted by $Z(G)$. At the very least we have the identity $e \in Z(G)$, but it is potentially much larger.

Example 3.23

The centre of D_6 is $\{1\}$. Clearly 1 always commutes with any element of D_6. For the other elements we can always find an element with which it does not commute. For example, a does not commute with b, since $ba = (a^2)b \neq ab$. The same equation shows that a^2 does not commute with b. So a, a^2 and b are not in the centre. Similarly $(ab)a = a^3b = a^2(ab)$, so ab does not commute with a, and $(a^2b)a = a^4b = a^2(a^2b)$, so a^2b does not commute with a. ◇

Example 3.24

The centre of D_8 is $\{1, a^2\}$. This follows since $a^n a^2 = a^{n+2} = a^2 a^n$ and

$$(a^n b)a^2 = a^n a^3 ba = a^{n+3}a^3 b = a^{n+6}b = a^{n+2}b = a^2(a^n b).$$

for $n = 0, 1, 2, 3$. So $a^2 \in Z(D_8)$.

On the other hand $(a^n b)a = a^n a^3 b = a^3(a^n b)$ for $n = 0, 1, 2, 3$, so a, a^3, and $a^n b$ are not in the centre. ◇

Example 3.25

The centre of $GL_n(\mathbb{R})$ is the set

$$\mathbb{R}^\times I_n = \left\{ \begin{bmatrix} a & 0 & \cdots 0 & \\ 0 & a & \cdots 0 & \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots a & \end{bmatrix} : a \in \mathbb{R}^\times \right\}.$$

It is easy to verify with matrix multiplication that every element of this set commutes with every matrix.

To simplify calculations, we will just look at the case $n = 2$. To see that these are the only possible elements of the centre, we note that if

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in Z(GL_2(\mathbb{R}))$$

then we must have

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix},$$

or,

$$\begin{bmatrix} b & a \\ d & c \end{bmatrix} = \begin{bmatrix} c & d \\ a & b \end{bmatrix}$$

and so we conclude that $a = d$ and $b = c$. We also must have

$$\begin{bmatrix} a & b \\ b & a \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a & b \\ b & a \end{bmatrix},$$

or,

$$\begin{bmatrix} b & -a \\ a & -b \end{bmatrix} = \begin{bmatrix} -b & -a \\ a & b \end{bmatrix}$$

so $b = -b$. Hence $b = 0$, and so a matrix is in the centre only if it is in the set $\mathbb{R}^\times I_2$. ◇

The centre is an extremely nice subset of the group.

Proposition 3.13
Let G be a group. Then $Z(G)$ is an Abelian subgroup of G.

Proof:
Given x, $y \in Z(G)$, we observe that for any $z \in G$ we have

$$(xy)z = xzy = z(xy),$$

so $xy \in Z(G)$. Similarly,

$$x^{-1}z = x^{-1}zxx^{-1} = zx^{-1},$$

so $x^{-1} \in Z(G)$. Hence $Z(G)$ is a subgroup of G.

It is immediate that $Z(G)$ is also Abelian, since every element of $Z(G)$ commutes with every element of G, and $Z(G)$ is a subgroup. ■

You can think of the centre as being a measure of how close the group G is to being Abelian. If $Z(G) = G$, then the group is Abelian, while if $Z(G)$ is a large subgroup, then G can be thought of having a large Abelian component. On the other hand, if $Z(G) = \{e\}$, the group is very far from being Abelian.

Proposition 3.14
Let G and H be isomorphic groups. Then $Z(G)$ and $Z(H)$ are isomorphic groups.

Proof:
We know that there is an isomorphism $\alpha : G \to H$. If $x \in Z(G)$, then for any $y \in H$, we have that there is some unique $u \in G$ such that $\alpha(u) = y$, and

$$\alpha(x)y = \alpha(x)\alpha(u) = \alpha(xu) = \alpha(ux) = \alpha(u)\alpha(x) = y\alpha(x).$$

So $\alpha(x) \in Z(H)$. An identical argument shows that if $x \in Z(H)$, then $\alpha^{-1}(x) \in Z(G)$.

Hence $\alpha(Z(G)) = Z(H)$, and the restriction of α to $Z(G)$ is an isomorphism between the centres. ■

Corollary 3.15
If G and H have centres which are not isomorphic, then G and H are not isomorphic.

More generally, rather than asking which elements commute with the entire group we might ask which elements commute with some subset of the group. If $X \subset G$ is any subset of the group G, then the ***centralizer*** of X is the set of all elements which commute with every element of X, ie.

$$Z_G(X) = \{y \in G : yx = xy\} = \{y \in G : y^{-1}xy = x\} = \{y \in G : yxy^{-1} = x\}.$$

This set always contains at least the identity element e.

Proposition 3.16
Let G be a group, and $X \subset G$. Then $Z_G(X)$ is a subgroup of G. If $Y \subseteq X$, then $Z_G(X)$ is a subgroup of $Z_G(Y)$.

Proof:

The proof of the first part of this proposition is essentially the same as the proof of the first part of Proposition 3.13, but with $z \in X$ rather than $z \in G$.

The second part follows from the fact that if $zx = xz$ for every $x \in X$, then it must also hold for every element of Y, since $Y \subseteq X$. Therefore $Z_G(X) \subseteq Z_G(Y)$. ■

In particular, this proposition implies that $Z(G) = Z_G(G) \subseteq Z_G(X)$ for all X.

The case where X contains a single element g is important enough to have its own, slightly different notation. We define

$$Z_G(g) = \{y \in G : yg = gy\} = \{y \in G : y^{-1}gy = g\} = \{y \in G : ygy^{-1} = g\}.$$

Example 3.26

The consider the element a of D_6. Then $Z_{D_6}(a) = \{e, a, a^2\}$. The elements b, ab and a^2b are not elements of $Z_{D_6}(a)$. Similarly, we have:

$$\begin{aligned} Z_{D_6}(e) &= D_6, \\ Z_{D_6}(a^2) &= \{e, a, a^2\}, \\ Z_{D_6}(b) &= \{e, b\}, \\ Z_{D_6}(ab) &= \{e, ab\}, \\ Z_{D_6}(a^2b) &= \{e, a^2b\}, \end{aligned}$$

◇

Once again, these subsets have very nice properties.

Proposition 3.17
Let G be a group and $g \in G$. Then $\langle g \rangle$ is a subgroup of G. Furthermore, $Z_G(g) = G$ if and only if $g \in Z(G)$

Proof:

We note that $g \in Z_G(g)$, and since $\langle g \rangle$ is the smallest subgroup of G containing g, we have that $\langle g \rangle$ must be a subgroup of $Z_G(g)$.

If $g \in Z(G)$, $gx = xg$ for all $x \in G$, so $Z_G(g) = G$.

On the other hand, if $Z_G(g) = G$, then that implies that for any $x \in G$, $xg = gx$, and so $g \in Z(G)$. ■

You can think of the centralizer of g as measuring how close g is to being an element of the centre, or how close it is to commuting with everything.

The centralizer plays a key role in the discussion of conjugacy later in this chapter. We finish up with one last result which links the centre and centralizers of elements.

Proposition 3.18
Let G be a group. Then $Z(G)$ is the intersection of all the subgroups $Z_G(g)$.

Proof:

We know that $Z(G) \subseteq Z_G(g)$ for every g, so

$$Z(G) \subseteq \bigcap_{g \in G} Z_G(g).$$

On the other hand, if $x \in Z_G(g)$ for every $g \in G$, then $xg = gx$ for every $g \in G$, and so $x \in Z(G)$. Hence

$$\bigcap_{g \in G} Z_G(g) \subseteq Z(G).$$

■

Exercises

3.3.1. Find the centre of the group $C_2 \times D_6$.

3.3.2. Find the centre of the group D_{10}.

3.3.3. Show that $Z(D_{2n}) = \{1\}$ if n is odd, and $Z(D_{2n}) = \{1, a^{n/2}\}$ if n is even.

3.3.4. Find the centralizers of each element of D_8.

3.3.5. Find the centralizers of each element of $C_2 \times D_6$.

3.3.6. Find the centralizers of each element of S_4. What is the center of this group?

3.3.7. Show that $Z_G(X) = Z_G(\langle X \rangle)$.

3.4 Cosets

There are other subsets of groups which it seems should have some significance. For example in S_3, the set of "reflection permutations", ie. those permutations with odd parity, is $\{(1,2),(1,3),(2,3)\}$ and is not a subgroup. Nevertheless, the elements have a commonality. To understand such a situation, we need to introduce some new notation.

If $* : A \times B \to C$ is any binary relation, then given any $x \in X$ and $Y \subseteq B$, we define

$$x * Y = \{x * y : y \in Y\} \subseteq C.$$

Similarly, if $y \in B$ and $X \subseteq A$, we define

$$X * y = \{x * y : x \in X\} \subseteq C.$$

And analagously, we define

$$X * Y = \{x * y : x \in X, y \in Y\} \subseteq C.$$

We will often omit the operation $*$ and simply write xY, Xy and XY respectively.

If $*$ is a binary operation on A, and $X \subseteq A$, we will sometimes write

$$X^n = \underbrace{X * X * \cdots * X}_{n \text{ times}}.$$

This is far from ideal notation, since it conflicts with the Cartesian product

$$X^n = \underbrace{X \times X \times \cdots \times X}_{n \text{ times}}.$$

However, it is usually clear from context which of the two possibilities we mean.

If $(G, *, e)$ is a group, and $X \subseteq G$ then we can also write

$$X^{-1} = \{x^{-1} : x \in X\}.$$

Using this notation, we can write Theorem 2.20 and Corollary 2.21 as follows:

Corollary 3.19
Let $G = (G, *e)$ be a group, and $H \subseteq G$. If $H^2 \subseteq H$ and $H^{-1} \subseteq H$, then $H \leq G$.

Corollary 3.20
Let $G = (G, *e)$ be a group, and $H \subseteq G$. If $HH^{-1} \subseteq H$, then $H \leq G$.

In fact, if H is a finite subset of G, we can use an even weaker condition:

Proposition 3.21
Let $G = (G, *e)$ be a group, and H be a finite subset G. If $H^2 = H$, then $H \leq G$.

To prove this fact, we need a lemma which we will use often in what follows:

Lemma 3.22
Let $G = (G, *e)$ be a group, $H \subseteq G$, and $g \in G$. Then the ***right translation*** *by g function $\rho_g : H \to Hg$ defined by $\rho_g(x) = xg$ is a bijection.*

Similarly, the ***left translation*** *by g function $\lambda_g : H \to gH$ defined by $\lambda_g(x) = gx$ is a bijection.*

We also have $|H| = |gH| = |Hg|$.

Proof:
That ρ_g is onto is trivial, for

$$\rho_g(H) = \{\rho_g(x) : x \in H\} = \{xg : x \in H\} = Hg.$$

On the other hand, if $\rho_g(x_1) = \rho_g(x_2)$, then this means that $x_1 g = x_2 g$, and the cancellation law (Proposition 2.3) says that $x_1 = x_2$. Hence ρ_g is one-to-one, and so ρ_g is a bijection.

The result for λ_g is similar.

Since we have bijections between H and Hg, and H and gH, all three sets must have the same cardinality (Proposition 1.2). ■

With this in hand, the proof is simple.
Proof (Proposition 3.21):
The hypothesis $H^2 = H$ implies that $xy \in H$ for all x, $y \in H$, so we need only prove that $x^{-1} \in H$.

Let $|H| = n$. Lemma 3.22 tells us $|Hx| = |H| = n$. Since H is finite this, together with the fact that $Hx \subseteq H^2 = H$, implies that $Hx = H$.

Hence there must be some element $y \in H$ such that $yx = x$. By the cancellation law, we have $y = e$, so $x \in H$.

But now there must also be some $z \in H$ such that $zx = e$, so $z = x^{-1}$.

Hence H is a subgroup of G. ■

Getting back to the example at the start of this section, if $H = \langle(1,2,3)\rangle = \{e, (1,2,3), (1,3,2)\}$, then we can write

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

In fact, we also have

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

This situation is important enough to give it a name.

Definition 3.5
Let G be a group, and H a subgroup of G. Sets of the form xH are called ***left cosets*** *of H and sets of the form Hx are called* ***right cosets*** *of H, where x is any element of G.*

If G is Abelian, then $Hx = xH$, and we simply call the set a ***coset*** *of H.*

So $\{(1,2),(1,3),(2,3)\}$ is both a left and right coset of $\{e,(1,2,3),(1,3,2)\}$.

Example 3.27

Consider $C_6 = \{1, a, a^2, a^3, a^4, a^5\}$. We know that $H = \langle a^3 \rangle$ is a subgroup, and its cosets are itself $H = a^3H$, $aH = a^4H = \{a, a^4\}$, and $a^2H = a^5H = \{a^2, a^5\}$.

Because cyclic groups are Abelian, the left and right cosets are the same. ◇

Notice in the examples so far that several different choices for x give the same coset. This is typical.

Theorem 3.23

Let G be a group, H a subgroup of G, and x and $y \in H$. Then $xH = yH$ if and only if $x^{-1}y \in H$. On the other hand, $Hx = Hy$ if and only if $xy^{-1} \in H$.

Furthermore, either $xH = yH$ or $xH \cap yH = \emptyset$. Similarly, either $Hx = Hy$ or $Hx \cap Hy = \emptyset$.

Proof:

A typical element of yH is of the form yz, for some $z \in H$. We note that $x^{-1}yz \in H$, as well, and so multiplying on the left by x we have $x(x^{-1}yz) = yz \in xH$. So $yH \subseteq xH$. Similarly, since $(x^{-1}y)^{-1} = y^{-1}x \in H$, given a typical element $xz \in xH$ we have $y^{-1}xz \in H$, and so $y(y^{-1}xz) = yz \in yH$. Hence $xH \subseteq yH$, and we conclude that $xH = yH$.

Conversely, if $x^{-1}y \notin H$, we have that $y \notin xH$, since if that were the case $y = xz$ for some $z \in H$, but $y = xx^{-1}y$, and the cancellation law implies that then $z = x^{-1}y$, so $z \notin H$, which is a contradiction. However, $y = ye \in yH$, so xH and yH are not equal.

Assume that $xH \neq yH$, so that $xy^{-1} \notin H$. If there were some $z \in xH \cap yH$, then we would have $z = xu = yv$ for some u and $v \in H$. So $uv^{-1} \in H$. But

$$uv^{-1} = x^{-1}xuv^{-1} = x^{-1}yvv^{-1} = x^{-1}y \notin H.$$

This is a contradiction, so there can be no such element z.

Analagous arguments show that $Hx = Hy$ if and only if $xy^{-1} \in H$, and either $Hx = Hy$ or $Hx \cap Hy = \emptyset$. ■

Every element of the group must lie in some coset, since $x = xe \in xH$, so the cosets of a subgroup H break the group G up into a collection of disjoint subsets. Furthermore, we know that each of these subsets has the same cardinality. This is nice to know for infinite groups, but it is really useful when dealing with finite groups.

Theorem 3.24 (Lagrange)

If G is a finite group, and $H \leq G$, then the number of left cosets of H and the number of right cosets of H both equal $|G|/|H|$.

Proof:

Assume that there are n left cosets, and that g_1H, $g_2H, \dots, g_nH$ is a complete list of the distinct left cosets of H, so G is a disjoint union of these sets. The inclusion-exclusion principle tells us that when we have a disjoint union of finite sets, the cardinality of the union is the sum of the cardinality of each set, ie.

$$|G| = |g_1H| + |g_2H| + \cdots + |g_nH|.$$

But Lemma 3.22 tells is that $|g_1H| = |g_2H| = \cdots = |g_nH| = |H|$, so

$$|G| = \underbrace{|H| + |H| + \cdots + |H|}_{n \text{ times}} = n|H|.$$

Hence the number of left cosets is $n = |G|/|H|$.

The argument for right cosets is analagous. ■

The number of cosets of a subgroup is significant enough to be given its own name and notation.

Definition 3.6
*If H is a subgroup of a group G, the **index** $[G : H]$ is the number of left (or right) cosets of H.*

The index is sometimes denoted $|G : H|$. The following corollaries of Lagrange's theorem are almost trivial, but they are important enough that we state them explicitly. We will use these some of these facts as much, if not more often, than Lagrange's theorem itself.

Corollary 3.25
If H is a subgroup of a finite group G, $[G : H] = |G|/|H|$.

Corollary 3.26
If H is a subgroup of a finite group G, then both $[G : H]$ and $|H|$ divide $|G|$.

Proof:

The numbers $[G : H] = |G|/|H|$, and $|H| = |G|/[G : H]$ are both natural numbers, so $|H| \mid |G|$ and $[G : H] \mid |G|$. ■

Corollary 3.27
If G is a finite group, and $x \in G$, then the order of the x, $o(x)$, divides $|G|$.

Proof:

We know that $o(x) = |\langle x \rangle|$, and we also know that $\langle x \rangle$ is a subgroup. Hence $|\langle x \rangle|$ divides $|G|$, and so $o(x)$ divides G. ■

This last corollary has some immediate consequences, both for properties of particular elements, and for classifying groups.

Corollary 3.28
If G is a finite group, and $n = |G|$, then given any $x \in G$, $x^n = e$.

Proof:
Assume that $o(x) = k$, so that in particular $x^k = e$. By the previous corollary, $o(x)$ divides n, so we have $n = km$ for some integer m. But then

$$x^n = x^{km} = (x^k)^m = e^m = e.$$

■

Exercises

3.4.1. Identify the cosets of the subgroup $H = \{1, a^2\}$ of the group D_8. What is the index of H in G?

3.4.2. Verify Lagrange's Theorem for D_8.

3.4.3. Show that if $X \subseteq G$ is not a subgroup, then an element may lie in more than one set of the form aX. Show that every element lies in at least one such set.

3.4.4. Let C_n be a cyclic group, and m be a number that divides n. Show that there is an element of order m in C_n.

3.4.5. Show that if G is a finite group, then the function $\alpha : \mathrm{Sub}(G) \to \mathbb{N}$ given by $\alpha(G) = |G|$ is an order-preserving function from the partial ordered set $(\mathrm{Sub}(G), \leq)$ to the partially ordered set $(\mathbb{N}, |)$.

3.5 Classifying Groups of Small Order

We will use the corollaries of Lagrange's theorem to show that groups of low order fall into a few distinct isomorphism classes. The aim of this section is to show that every group of order less than or equal to 8 is isomorphic to one of a few standard groups.

Corollary 3.29
Let G be a group with $|G| = p$, a prime number. Then G has no proper subgroups, and G is cyclic.

Proof:
If H is a subgroup of G, then $|H|$ divides $|G| = p$, so $|H|$ must either be 1 or p. If $|H| = 1$, then $H = \{e\}$, since every subgroup must contain the identity element. On the other hand, if $|H| = p$, then $H = G$, since H must contain every element of the group. So G has no proper subgroups.

Now assume that $x \in G$, and $x \neq e$. Then $H = \langle x \rangle$ is a subgroup of G, and H contains at least two elements x and e. Hence $|H| \neq 1$, and so $|H| = p$, which implies $H = G$. So G is generated by x, and hence is a cyclic group. ■

This last corollary means that every group of prime order is isomorphic to C_p.

We can also show that we have found all groups of order 4.

Proposition 3.30
Let G be a group such that $|G| = 4$. Then either $G \cong C_4$ or $G \cong V \cong C_2 \times C_2$.

Proof:

We know that the order of every element of G divides 4, so the order of an element which is not the idientity must be 2 or 4.

If there is an element x with $o(x) = 4$, then x must generate G. Hence G is cyclic, so $G \cong C_4$.

If there is no element of order 4, then we must have $x^2 = e$ for every $x \in G$. But then Theorem 2.18 tells us that $G \cong C_2 \times C_2$. ■

This table summarizes the typical groups of each order that we have discovered, up to order 12.

Order	**Known Groups**
1	C_1
2	C_2
3	C_3
4	C_4, $C_2 \times C_2$
5	C_5
6	C_6, D_6, ?
7	C_7
8	C_8, $C_2 \times C_2 \times C_2$, $C_4 \times C_2$, D_8, ?
9	C_9, $C_3 \times C_3$, ?
10	C_{10}, D_{10}, ?
11	C_{11}
12	C_{12}, $C_2 \times C_6$, D_{12}, A_3, ?

There may be other groups of order 6, 8, 10 and 12 that we do not yet know of, indicated by the question marks in the table.

The following general result tells us that there are no more groups of order 6 and 10 than the ones listed on the table.

Proposition 3.31
Let G be a group with $|G| = 2p$, where p is a prime number greater than 2. Then either G is cyclic, or $G \cong D_{2p}$.

Proof:

The factors of $2p$ are 1, 2, p and $2p$, so the order of each element must be one of those factors. If G has an element of order $2p$ it is cyclic.

Assume that G does not have an element of order $2p$. If G does not have an element of order p, then every non-identity element of G must have order 2, which means that $x^2 = e$ for every element of G. That imples that G is a product of copies of C_2 by Theorem 2.18, and in particular that $|G| = 2^n$, which is impossible if $p > 2$.

Hence there is some element $a \in G$ with $o(a) = p$. Choose any element $b \notin \langle a \rangle$. Then G breaks into the two right cosets

$$\langle a \rangle = \{1, a, a^2, \ldots, a^{p-1}\},$$
$$\langle a \rangle b = \{b, ab, a^2b, \ldots, a^{p-1}b\}.$$

Therefore b^2 and $(ba)^2$ must lie in one of these two cosets.

If $b^2 \in \langle a \rangle b$, then $b^2 = a^k b$ for some k, and the cancellation law tells us that $b = a^k$, which is a contradiction. Hence $b^2 \in \langle a \rangle$, so $b^2 = a^k$ for some k. If $k \neq 0$, then $b^2 \neq e$, so $o(b) > 2$ and hence b must have order p. But then since p is odd, $p - 1$ is even, and

$$b^p = b^{p-1}b = (b^2)^{(p-1)/2}b = (a^k)^{(p-1)/2}b = a^{k(p-1)/2}b \neq e.$$

So b cannot have order p. Hence $b^2 = e$.

The same argument with ba in the place of b shows that $(ba)^2 = e$. Hence,

$$\begin{aligned} baba &= 1 \\ bab &= a^{-1} = a^{p-1} \\ ba &= a^{p-1}b^{-1} = a^{p-1}b. \end{aligned}$$

So $G = \{1, a, a^2, \ldots, a^{p-1}, b, ab, a^2b, \ldots, a^{p-1}b\}$ and the relations

$$a^p = 1, b = 1, \text{and} ba = a^{p-1}b,$$

hold, which is precisely the definition of D_{2p}. Hence $G \cong D_{2p}$. ■

There may still be groups of order 8, 9 and 12 which we do not know about. We need to introduce a new concept to fully analyse these situations, so we defer them to a later section.

Exercises

3.5.1. Show that every Abelian group of order 8 is isomorphic to one of C_8, $C_4 \times C_2$, or $C_2 \times C_2 \times C_2$.

3.5.2. For any natural number n, define the ***quaternion group*** to be the group

$$Q_{4n} = \{1, a, a^2, \ldots, a^{2n-1}, b, ab, a^2b, \ldots, a^{2n-1}b\}$$

where the Cayley table is determined by the relations $a^{2n} = 1$, $b^2 = a^n$, and $b^{-1}ab = a^{-1}$.

Show that $Q_4 \cong C_2 \times C_2$.

Show that Q_8 is not isomorphic to any one of C_8, $C_2 \times C_2 \times C_2$, $C_2 \times C_4$, or D_8. In other words, Q_8 is a new group of order 8.

Find the subgroup lattice for Q_8.

3.6 Excursion: Equivalence Relations

Underlying the concept of cosets is the notion of an equivalence relation. Equivalence relations are a powerful mathematical concept which occur with regularity throughout abstract mathematics. Moreover, you are familiar with some of them already, even though you may have not seen the concept formally explained.

Definition 3.7
An ***equivalence relation*** *on a set X is a relation R on X which is reflexive, transitive and symmetric. Equivalence relations are often denoted by the symbol $\sim$.*

Example 3.28
The equality relation is an equivalence relation. Indeed, it is the prototypical equivalence relation. ◇

Example 3.29
Let $M_n(\mathbb{R})$ be the set of n by n real-valued matrices. Recall that A and B are equivalent matrices if there is an orthogonal matrix U such that $A = U^{-1}BU$. The relation $\sim$ defined by $A \sim B$ if and only if A and B are equivalence matrices is an equivalence relation. ◇

Example 3.30
Let m be any natural number. The relation $\equiv$ on $\mathbb{Z}$ defined by $x \equiv y$ if and only if m divides $x - y$ is an equivalence relation. Another way of looking at it, is that it holds if and only if

$$x \equiv y \pmod{m}.$$

A third, useful, way of looking at this situation is that the set of all integers divisible by m is the subset $H = m\mathbb{Z} = \{mn : n \in \mathbb{Z}\}$ of $\mathbb{Z}$, and this is a subgroup, so $x \equiv y$ if and only if $x - y \in H$, and $x - y$ is the additive notation for xy^{-1}. So this is the same condition we were using to test whether two elements were in the same coset. ◇

We now get to the key example which links this section with what we have just discussed by generalizing the above example.

Example 3.31
Let G be a group, H a subgroup of G, and x, $y \in G$. We define $x \equiv_R y \pmod{H}$ if $xy^{-1} \in H$.

To prove this, you need to check that each of the three axioms for an equivalence relation hold.

Firstly, $xx^{-1} = e \in H$, so $x \equiv_R x \pmod{H}$, and $\equiv_R \pmod{H}$ is reflexive.

Secondly, if $x \equiv_R y \pmod{H}$, then $xy^{-1} \in H$, then $yx^{-1} = (xy^{-1})^{-1} \in H$, so $y \equiv_R x \pmod{H}$, and $\equiv_R \pmod{H}$ is symmetric.

Finally, if $x \equiv_R y \pmod{H}$ and $y \equiv_R z \pmod{H}$, then xy^{-1} and $yz^{-1} \in H$, so $xz^{-1} = xy^{-1}yz^{-1} \in H$, so $x \equiv_R z \pmod{H}$, and $\equiv_R \pmod{H}$ is transitive.

There is of course the equivalent "left" relation $x \equiv_L y \pmod{H}$ if $x^{-1}y \in H$, and this too is an equivalence relation. ◇

Notice how the three group axioms correspond to the three equivalence relation axioms in the previous example. Notice also that with these equivalence relations, the cosets are precisely the sets of elements which are equivalent to one-another.

Definition 3.8
Let $\sim$ be an equivalence relation on X. The ***equivalence class*** *of $x \in X$ is the set*

$$[x]_\sim = \{y \in X : x \sim y\}.$$

When the equivalence relation is clear, we typically write just $[x]$.

Example 3.32
For equality, the equivalence class $[x]_= = \{x\}$. ◇

Example 3.33
For $\equiv \pmod{m}$, the equivalence class of a number n, $[n]_\equiv$ is the set of all numbers with the same remainder when divided by m, or equivalently,

$$[n] = \{\dots, n - 2m, n - m, n, n + m, n + 2m, \dots\}$$

◇

Example 3.34
The equivalence class of x under the equivalence relation $\equiv_R \pmod{H}$ is the right coset Hx.

The equivalence class of x under the equivalence relation $\equiv_L \pmod{H}$ is the left coset xH. ◇

A key fact about equivalence classes is that they partition the set X into a disjoint collection of subsets whose union is the whole set.

Lemma 3.32
Let $\sim$ be an equivalence relation on X. We have $x \sim y$ if and only if $[x] = [y]$.

Also, either $[x] = [y]$ or $[x] \cap [y] = \emptyset$.

Proof:

Assume that $x \sim y$, then given any $z \in [y]$, we have $y \sim z$, and since $\sim$ is transitive, $x \sim z$, so $z \in [x]$. Hence $[x] \subseteq [y]$. On the other hand, we know that by symmetry $x \sim y$ implies $y \sim x$. If $z \in [x]$, we have $x \sim z$ and since $\sim$ is transitive, $x \sim z$, so $z \in [x]$. Hence $[x] \subseteq [y]$. Hence $[x] = [y]$.

If $[x] = [y]$, then $y \in [y]$, since $y \sim y$ by reflexivity, and so $y \in [x]$. Hence $x \sim y$ by definition.

If $[x] \cap [y] \neq \emptyset$, then there must be some z in both sets, ie. $x \sim z$ and $y \sim z$. Now since $\sim$ is symmetric, $y \sim z$ implies $z \sim y$, and since $\sim$ is transitive, $x \sim y$. The first part of this lemma allows us to conclude that $[x] = [y]$. ■

Theorem 3.23 is now a trivial corollary of this general fact about equivalence relations. Similarly, Lagrange's Theorem follows from the following general fact.

Theorem 3.33

Let X be a finite set, and let $\sim$ be an equivalence relation on X. Choose elements $x_1, x_2, \ldots, x_n \in X$ so that no two are equivalent, and so for every $x \in X$, there is some x_k such that $[x] = [x_k]$ (ie. this is a complete set of equivalence class representatives). Then

$$|X| = \sum_{k=1}^{n} |[x_k]|$$

Proof:

We have that X is the disjoint union of the equivalence classes of the x_k, ie.

$$X = [x_1] \cup [x_2] \cup \cdots \cup [x_n],$$

which follows from the fact that every x lies in one of the $[x_k]$, and if $k \neq j$,

$$[x_j] \cap [x_k] = \emptyset,$$

since $x_k \not\sim x_j$.

Repeated application of the inclusion-exclusion principle then tells us that

$$|X| = |[x_1]| + |[x_2]| + \cdots + |[x_n]|,$$

since the intersections are empty. ■

We will use this general theorem in the next section.

Exercises

3.6.1. Verify that Example 3.30 is an equivalence relation.

3.6.2. Verify that Example 3.29 is an equivalence relation.

3.6.3. Let A and $B \in M_n(\mathbb{R})$, and define a relation by $A \sim B$ if $A = X^{-1}BX$ for some invertible matrix X. SHow that this is an equivalence relation.

3.6.4. Can a relation be symmetric and transitive, but not reflexive? Give a proof or counterexample to justify your position.

3.6.5. (*) Show that if $\sim$ is the equivalence relation of Example 3.29, and

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

then $[A]_\sim$ is the set of all symmetric 2×2 matrices with eigenvalues 1 and 2.

3.7 Conjugacy Classes

There is another equivalence relation which is of interest which is a generalization of the idea of conjugate matrices (see Example 3.29).

Definition 3.9
Let G be a group and let x and $y \in G$. We say that y is a conjugate of x if $y = u^{-1}xu$ for some $u \in G$. In this case, we write $x \sim y$.

Example 3.35
In the group $D_6 = \{1, a, a^2, b, ab, a^2b\}$ we have that $a \sim a^2$, since $b^{-1}ab = bab = a^2bb = a^2$. Similarly, we have that $b \sim ab$ since $a^{-1}ba = a^2ba = a^2a^2b = ab$. ◇

Proposition 3.34
If G is a group, the conjugacy relation $\sim$ is an equivalence relation on G.

Proof:
We need to show that $\sim$ is reflexive, symmetric and transitive.

Since $x = e^{-1}xe$, we have that $x \sim x$, so $\sim$ is reflexive.

If $x \sim y$, then there is an element u such that $y = u^{-1}xu$. But then $x = uu^{-1}xuu^{-1} = uyu^{-1} = (u^{-1})^{-1}yu^{-1}$. So $y \sim x$, and $\sim$ is symmetric.

If $x \sim y$ and $y \sim z$, then $y = u^{-1}xu$ and $z = v^{-1}yv$ for some u and v in G, so $z = v^{-1}u^{-1}xuv = (uv)^{-1}x(uv)$. Hence $x \sim z$, and $\sim$ is transitive. ■

We will call the equivalence class of $x \in G$ the ***conjugacy class*** of x. We will denote the conjugacy class of an element $x \in G$ by $C(x)$. In other words,

$$C(x) = \{y \in G : y = u^{-1}xu \text{ for some } u \in G\}.$$

Example 3.36
The conjugacy classes of the four-group are $\{e\}$, $\{a\}$, $\{b\}$, $\{ab\}$. In other words, each element is in its own conjugacy class. ◇

Example 3.37

The conjugacy classes of the group $D_6 = \{1, a, a^2, b, ab, a^2b\}$ are $\{1\}$, $\{a, a^2\}$, $\{b, ab, a^2b\}$. ◇

The reason that the four-group has a conjugacy class for each element is because it is an Abelian group. In fact if x commutes with everything in G, then the only element of the conjugacy class of x is itself.

Proposition 3.35

Let G be a group and $x \in G$. Then $C(x) = \{x\}$ if and only if $x \in Z(G)$.

Proof:

Assume $x \in Z(G)$. Let $y \in C(x)$, so that there is some $u \in G$ such that $y = u^{-1}xu$. But then, since $xu = ux$,

$$y = u^{-1}xu = u^{-1}ux = x.$$

So $C(x) = \{x\}$.

On the other hand, if $C(x) = \{x\}$, then for every $u \in G$, we have $u^{-1}xu = x$, which means x and u commute. Hence $x \in Z(G)$. ■

Notice in this case that we are saying that $u^{-1}xu = v^{-1}xv$ for every u and $v \in G$. This is not going to be the case in general, but it is of interest to know for which u and v it occurs. For example, if these quantities were never equal for different u and v, it would show that the conjugacy class of x has many different elements.

Proposition 3.36

Let G be a group and $x \in G$. Then $u^{-1}xu = v^{-1}xv$ if and only if $uv^{-1} \in Z_G(x)$.

Proof:

If $u^{-1}xu = v^{-1}xv$, then we have

$$\begin{aligned} u^{-1}xu &= v^{-1}xv \\ xu &= uv^{-1}xv \\ xuv^{-1} &= uv^{-1}x. \end{aligned}$$

So we can see that uv^{-1} commutes with x, and so $uv^{-1} \in Z_G(x)$.

On the other hand, if $uv^{-1} \in Z_G(x)$, we can run the calculation backwards:

$$\begin{aligned} xuv^{-1} &= uv^{-1}x \\ xu &= uv^{-1}xv \\ u^{-1}xu &= v^{-1}xv, \end{aligned}$$

and so we have the result. ■

Recalling Theorem 3.23, this proposition cas the following corollary:

Corollary 3.37
Let G be a group and $x \in G$. Then $u^{-1}xu = v^{-1}xv$ if and only if u and v are in the same right coset of $Z_G(x)$, ie. if $Z_G(x)u = Z_G(x)v$.

Turning this around, it means that $u^{-1}xu \neq v^{-1}xv$ if and only if u and v are in different right cosets of $Z_G(x)$, which means that there is a distinct conjugate of x for each distinct right coset of $Z_G(x)$. If G is finite, then Lagrange's Theorem tells us that there are exactly $|G : Z_G(x)| = |G|/|Z_G(x)|$ distinct right cosets of $Z_G(x)$. This proves the following:

Corollary 3.38
Let G be a finite group and $x \in G$. Then

$$|C(x)| = |G : Z_G(x)|.$$

Note that this agrees with Proposition 3.35, since $x \in Z(G)$ if and only if $Z_G(x) = G$, but this happens if and only if $|C(x)| = |G : Z_G(x)| = |G|/|G| = 1$. In other words, if and only if the only conjugate of x is itself.

Example 3.38
For the group D_6 we know that a has conjugacy class $\{a, a^2\}$, and we know that $Z_{D_6}(a) = \{1, a, a^2\}$. It is simple to verify that

$$|G|/|Z_{D_6}(a)| = 6/3 = 2 = |C(a)|.$$

If we look at the other elements of D_g, we observe that

$$\begin{aligned}
|C(e)| &= 2 & |G|/|Z_{D_6}(e)| &= 6/6 = 1\\
|C(a^2)| &= 2 & |G|/|Z_{D_6}(a^2)| &= 6/3 = 2\\
|C(b)| &= 3 & |G|/|Z_{D_6}(b)| &= 6/2 = 3\\
|C(ab)| &= 3 & |G|/|Z_{D_6}(ab)| &= 6/2 = 3\\
|C(a^2b)| &= 3 & |G|/|Z_{D_6}(a^2b)| &= 6/2 = 3.
\end{aligned}$$

◇

We can now apply Theorem 3.33 to the conjugacy equivalence relation.

Theorem 3.39 (The Class Equation)
Let G be a finite group, and let g_1, g_2, $g_n \in G$ be chosen so that no two are conjugate, and every conjugacy class of G occurs as one of the conjugacy classes $C(g_k)$ (ie. the elements g_k are a complete set of conjugacy class representatives). Then

$$|G| = \sum_{k=1}^{n} |C(g_k)| = \sum_{k=1}^{n} |G : Z_G(g_k)|.$$

In fact, if we assume that $Z(G) = \{g_1, g_2, \ldots, g_m\}$, then

$$|G| = |Z(G)| + \sum_{k=m+1}^{n} |G : Z_G(g_k)|.$$

Proof:

Since conjugacy is an equivalence relation, Theorem 3.33 applies and tells us that

$$|G| = |C(g_1)| + |C(g_2)| + \cdots + |C(g_n)| = \sum_{k=1}^{n} |C(g_k)|.$$

But then Corollary 3.38 tells us that $|C(g_k)| = |G : Z_G(g_k)|$, and so we can re-write the equation as

$$|G| = \sum_{k=1}^{n} |G : Z_G(g_k)|.$$

Now we know that if $g_k \in Z(G)$, then $|C(g_k)| = 1$, so if $Z(G) = \{g_1, g_2, \ldots, g_m\}$, then

$$\begin{aligned} |G| &= |C(g_1)| + |C(g_2)| + \cdots + |C(g_m)| + |C(g_{m+1})| + |C(g_{m+2})| + \cdots + |C(g_n)| \\ &= \underbrace{1 + 1 + \cdots + 1}_{m \text{ times}} + |C(g_{m+1})| + |C(g_{m+2})| + \cdots + |C(g_n)| \\ &= |Z(G)| + \sum_{k=m+1}^{n} |C(g_k)| \\ &= |Z(G)| + \sum_{k=m+1}^{n} |G : Z_G(g_k)|. \end{aligned}$$

■

Example 3.39

For the group D_6 we have that 1, a, and b are representatives of each conjugacy class, and

$$|C(1)| + |C(a)| + |C(b)| = 1 + 2 + 3 = 6 = |D_6|.$$

◇

Example 3.40

For the group D_8, we know from Example 3.24 that the centre $Z(D_8) = \{1, a^2\}$, so $C(1) = \{1\}$ and $C(a^2) = \{a^2\}$.

We know that $Z_{D_8}(a)$ contains $\langle a \rangle$ so

$$|Z_{D_8}(a)| \geq |\langle a \rangle| = o(a) = 4,$$

and from Lagrange's theorem $|Z_{D_8}(a)|$ divides 8, so we conclude that $|Z_{D_8}(a)|$ is 4 or 8. But $a \notin Z(D_8)$, so $Z_{D_8}(a) \neq D_8$, and hence $|Z_{D_8}(a)| = 4$. Hence a has two conjugates, itself, and $b^{-1}ab = bab = a^3b^2 = a^3$. So $C(a) = \{a, a^3\}$.

Now $Z_{D_8}(b)$ contains $\langle b\rangle$, so $|Z_{D_8}(b)| \geq o(b) = 2$, and $|Z_{D_8}(b)|$ divides 8. Also b is not in the centre of D_8, so $|Z_{D_8}(b)| \neq 8$, and hence $|Z_{D_8}(b)|$ is 2 or 4. Now we know that the centre is a subgroup of $Z_{D_8}(b)$, so 1 and a^2 are in the subgroup, as is b itself. Hence $|Z_{D_8}(b)| > 2$, and we conclude that $|Z_{D_8}(b)| = 4$. Hence b has two conjugates, itself and $a^{-1}ba = a^{-1}a^3b = a^2b$. So $C(b) = \{b, a^2b\}$.

Looking at $Z_{D_8}(ab)$, an analagous argument tells us that $|Z_{D_8}(ab)| = 4$, and the conjucacy class is $C(ab) = \{ab, a^3b\}$.

We can verify that the class equation holds in this example: a complete collection of equivalence class representatives is 1, a^2, a, b and ab, and

$$|Z(D_8)| + |C(a)| + |C(b)| + |C(ab)| = 2 + 2 + 2 + 2 = 8 = |D_8|.$$

$\diamond$

We conclude with one last proposition which can help identify which elements are in different conjugacy classes.

Proposition 3.40
Let G be a finite group. If x and $y \in G$ are conjugate, then $o(x) = o(y)$.

Proof:
Let $x = u^{-1}yu$. Then if $o(y) = n$,

$$\begin{aligned} x^n &= (u^{-1}yu)^n \\ &= \underbrace{(u^{-1}yu)(u^{-1}yu)\cdots(u^{-1}yu)} n \text{ times} \\ &= u^{-1}\underbrace{yy\ldots y} n \text{ times} u \\ &= u^{-1}y^n u \\ &= u^{-1}u \\ &= e. \end{aligned}$$

So $o(x)$ divides n. However, if $o(x) = m$, then a similar calculation shows that

$$\begin{aligned} e &= x^m \\ &= u^{-1}y^m u, \end{aligned}$$

so $y^m = uu^{-1}y^m uu^{-1} = ueu^{-1} = e$. Hence n divides m, and so $n = m$. ■

Note that the converse is not true, since in the group D_8, the elements a^2, b and ab all have order 2, but all are in distinct conjugacy classes.

Notice that every term in the class equation divides the order of the group. We can use this to prove the following interesting result that will be useful when we look once again at groups of small order.

Theorem 3.41
Let G be a finite group of prime power order, ie. $|G| = p^n$ where p is prime and $n \geq 1$. Then $|Z(G)| = p^m$ for some $m \geq 1$.

Proof:

Lagrange's theorem tells us that $|Z(G)| = p^m$ for some $m \geq 0$.

Let x_1, $x_2, \ldots, x_k$ be a complete set of conjugacy class representatives, and let $Z(G) = \{x_1, \ldots, x_l\}$. Now let $n_i = |C(x_i)| = |G : Z_G(x_i)|$, so $n_i \mid p^n$. Now for $i > l$, we must have $n_i > 1$, so n_i must be a multiple of p. Therefore,

$$p^n = |G| = |Z(G)| + n_{l+1} + n_{l+2} + \cdots n_k = l + jp$$

for some integer j. But therefore l is a multiple of p, and since $e \in Z(G)$, $|Z(G)| \geq 1$. So we conclude that $|Z(G)| \geq p$, and hence $m \geq 1$. ■

In other words, groups of prime power must have more than just the identity in their centres.

Exercises

3.7.1. In a group of order 15, what does the Class equation say are possible sizes of the conjugacy classes? Potentially how many different ways can a group of order 15 be divided into conjugacy classes of these sizes (remembering that the number of conjugacy classes of size 1 has to equal $|Z(G)|$, which has to divide 15).

Note: in actual fact, there turns out to be only one group of order 15, so there is just one way to do it once this is taken into account; however you should use the class equation to give you all the potentially possible ways that it could be done.

3.7.2. Find the conjugacy classes of D_{10}, and verify that the class equation holds.

3.7.3. Find the conjugacy classes of D_{12}, and verify that the class equation holds.

3.7.4. Find the conjugacy classes of A_4, and verify that the class equation holds.

3.7.5. Let G be a finite group, and $x \in G$. Show that the conjugacy classes $C(x)$ and $C(x^{-1})$ have the same number of elements.

3.7.6. Show that any group G of even order must contain an element of even order, and use the previous exercise to conclude that there is at least one element $x \in G$ other than e such that $C(x) = C(x^{-1})$.

3.8 Normal Subgroups

It turns out that many of the ideas relating to centralizers and conjugacy can be applied to subgroups instead of individual elements.

Proposition 3.42
Let G be a group and H a subgroup of G. Given any $x \in G$, the set

$$x^{-1}Hx = \{x^{-1}yx : y \in H\}$$

of conjugates of elements of H is a subgroup of G.

Proof:
Given any elements u and $v \in x^{-1}Hx$, we have y and $z \in H$ such that $u = x^{-1}yx$ and $v = x^{-1}zx$. Then

$$uv^{-1} = x^{-1}yx(x^{-1}zx)^{-1} = x^{-1}yxx^{-1}z^{-1}x = x^{-1}yz^{-1}x,$$

which is an element of $x^{-1}Hx$, since $yz^{-1} \in H$.
Hence $x^{-1}Hx$ is a subgroup of G. ■

If $x \in H$, then $x^{-1}Hx = H$, but if $x \notin H$ we may potentially get something else.

Example 3.41
In the group D_6, consider the subgroup $H = \{1, b\}$. Since $a^{-1}1a = 1$, and $a^{-1}ba = a^{-1}a^2b = ab$, we have

$$a^{-1}Ha = \{1, ab\}.$$

Similarly, we have

$$\begin{aligned}(a^2)^{-1}Ha^2 &= \{1, a^2b\} \\ b^{-1}Hb &= \{1, b\} \\ (ab)^{-1}H(ab) &= \{1, a^2b\} \\ (a^2b)^{-1}H(a^2b) &= \{1, ab\}\end{aligned}$$

On the other hand, the subgroup $K = \{1, a, a^2\}$ has $x^{-1}Kx = K$ for any x. For example, since $b^{-1}1b = 1$, $b^{-1}ab = bab = a^2b^2 = a^2$, and $b^{-1}a^2b = ba^2b = b^2a = a$, we have $b^{-1}Kb = K$. Similar arguments give the remaining cases. ◇

We will say that two subgroups H and K of G are ***conjugate*** if there is some $x \in G$ such that

$$K = x^{-1}Hx,$$

and we will write $K \sim H$ if this is the case. It is equivalent to say that K and H are conjugate if and only if there is some $x \in G$ such that $xK = Hx$.

Proposition 3.43
Let G be a group. The conjugacy relation $\sim$ is an equivalence relation on the set $\mathrm{Sub}(G)$ of all subgroups of G. Furthermore if two subgroups are conjugate, they are isomorphic.

Proof:

We need to show that $\sim$ is reflexive, symmetric and transitive.

Given a subgroup H, we have $H \sim H$ immediately from the fact that $e^{-1}He = H$.

If K and H are subgroups with $K \sim H$, then there is some $x \in G$ so that $K = x^{-1}Hx$. But then $H = xKx^{-1} = (x^{-1})^{-1}Kx^{-1}$, and so $H \sim K$.

Finally, if H, K and F are subgroups, with $H \sim K$ and $K \sim F$, then there are elements x and $y \in G$ such that $K = x^{-1}Hx$ and $F = y^{-1}Ky$. But then $F = y^{-1}(x^{-1}Hx)y = (xy)^{-1}H(xy)$, and so $F \sim H$.

So conjugacy of subgroups is an equivalence relation.

If K and H are conjugate, with $K = x^{-1}Hx$, we define a function $\alpha : H \to K$ by $\alpha(y) = x^{-1}yx$. This function is a homomorphism, since

$$\alpha(y)\alpha(z) = x^{-1}yxx^{-1}zx = x^{-1}yzx = \alpha(yz).$$

It is also onto, since $K = \alpha(H)$ by definition. Finally, it is one-to-one since if $\alpha(y) = \alpha(z)$, then $x^{-1}yx = x^{-1}zx$, and using the cancellation law on the left and right gives $y = z$.

So α is an isomorphism from H to K, and H and K are isomorphic. ■

Example 3.42

Continuing the example of D_6 from above, we have that $\{1\}$ is only conjugate with itself, $\{1, a, a^2\}$ is only conjugate with itself, $\{1, b\} \sim \{1, ab\} \sim \{1, a^2b\}$, and D_6 is only conjugate with itself. ◇

We recall that elements of a group whose conjugacy class was just themselves were special: they formed the centre of the group. Subgroups which are conjugate only with themselves are also special.

Definition 3.10

Let G be a group and K a subgroup of G. If the only subgroup conjugate to K is K itself, that is, for any $x \in G$

$$x^{-1}Kx = K,$$

*then we say that K is a **normal subgroup**, and we write $K \lhd G$.*

Another way of representing the condition that K is normal is that

$$Kx = xK$$

for every $x \in G$, or in other words that the corresponding left- and right- cosets of K are identical.

Example 3.43

In the group D_6 we have that the subgroups $\{1\}$, $\{1, a, a^2\}$ and D_6 are normal. The subgroups $\{1, b\}$, $\{1, ab\}$ and $\{1, a^2b\}$ are not normal. ◇

Lemma 3.44
If G is a group, then $\{e\}$ and G are always normal subgroups of G.

If G is Abelian, then every subgroup of G is normal.

Proof:
We know $x^{-1}ex = x^{-1}x = e$ for every x, so $x^{-1}\{e\}x = \{e\}$ for all x. We also know that $x^{-1}Gx = G$ for any x, since $x \in G$.

If G is Abelian, we recall that $Kx = xK$ for any subgroup and any $x \in G$ (see Definition 3.5), hence K is always normal. ■

Not every element of a group is in the centre, and not every subgroup is normal. Similarly, just as the centralizer gives us information about the conjugacy classes of elements, we have an analagous concept for conjugacy classes of subgroups.

Definition 3.11
Let G be a group, and H a subgroup of G. We define the ***normalizer*** *of H to be the set*

$$N_G(H) = \{x \in G : H = x^{-1}Hx\}$$

With this definition, we can duplicate most of the key results about centralizers and conjugacy classes.

Theorem 3.45
Let G be a group and H a subgroup of G. Then

(i) $N_G(H)$ is a subgroup of G,

(ii) H and $Z(G)$ are subgroups of $N_G(H)$,

(iii) $N_G(H) = G$ if and only if H is normal,

(iv) $x^{-1}Hx = y^{-1}Hy$ if and only if x and y are in the same right coset of $N_G(H)$,

(v) The number of distinct conjugacy classes of H is $|G : N_G(H)|$.

Proof:
The proofs of these facts are analogous to the proofs of the corresponding results for centralizers, and are left as an exercise. ■

Normal subgroups play a key role in the theory of groups, and we now turn to study them in more detail. We start with some ways of testing whether a subgroup is normal or not, and discovering normal subgroups of a group.

Theorem 3.46
Let G be a group and K a subgroup of G. Then the following are equivalent:

(i) K is normal,

(ii) $x^{-1}Kx = K$ for all $x \in G$,

(iii) $Kx = xK$ *for all* $x \in G$*,*

(iv) $N_G(H) = G$*,*

(v) $x^{-1}yx \in K$ *for all* $y \in K$ *and* $x \in G$*,*

(vi) K *is a union of some of the conjugacy classes of elements of* G*,*

Proof:

We have already seen that (i), (ii), (iii) and (iv) are equivalent.

If K is normal then $x^{-1}Kx = K$, so for any $y \in K$ we have that $x^{-1}yx \in K$. Conversely, if $x^{-1}yx \in K$ for all $y \in K$ and $x \in G$, then if we fix x we have that

$$x^{-1}Kx = \{x^{-1}yx : y \in K\} \subseteq K.$$

On the other hand, given any $y \in K$, we have that $(x^{-1})^{-1}yx^{-1} \in K$, and so

$$x^{-1}((x^{-1})^{-1}yx^{-1})x = x^{-1}xyx^{-1}x = y,$$

and so $K \subseteq x^{-1}Kx$. Hence $x^{-1}Kx = K$ for every $x \in G$ and so K is normal.

So we have just shown that (i) and (v) are equivalent.

Another way of stating (v) is that if $y \in K$ then every conjugate of y is in K, so that $C(y) \subseteq K$. Hence K must be the union of all the conjugacy classes of its elements, ie.

$$K = \bigcup_{y \in K} C(y)$$

So (v) implies (vi).

Conversely, if K is a union of conjugacy classes, then given any element $y \in K$, the conjugacy class $C(y)$ of y must be a subset of K, and so we have that $x^{-1}yx \in C(y) \subseteq K$. Therefore $x^{-1}yx \in K$, and (vi) implies (v). ■

Example 3.44

In the group D_6, we have conjugacy classes $\{1\}$, $\{a, a^2\}$ and $\{b, ab, a^2b\}$. We can clearly see that each of the normal subgroups are unions of conjugacy classes:

$$\begin{aligned} \{1\} &= \{1\} \\ \{1, a, a^2\} &= \{1\} \cup \{a, a^2\} \\ D_6 &= \{1\} \cup \{a, a^2\} \cup \{b, ab, a^2b\}. \end{aligned}$$

Notice that not every union of conjugacy classes gives a normal subgroup, because some unions of conjugacy classes aren't subgroups. For example, the set $\{1, b, ab, a^2b\} = \{1\} \cup \{b, ab, a^2b\}$ is not a subgroup. ◇

Example 3.45

The group D_8 has conjugacy classes

$$\{1\}, \{a^2\}, \{a, a^3\}, \{b, a^2b\}, \{ab, a^3b\}.$$

The trivial subgroups $\{1\}$ and D_8 are automatically normal, but in addition, we have that the subgroups

$$\begin{aligned}
\{1, a^2\} &= \{1\} \cup \{a^2\} \\
\{1, a, a^2, a^3\} &= \{1\} \cup \{a^2\} \cup \{a, a^3\} \\
\{1, a^2, b, a^2b\} &= \{1\} \cup \{a^2\} \cup \{b, a^2b\} \\
\{1, a^2, ab, a^3b\} &= \{1\} \cup \{a^2\} \cup \{ab, a^3b\}
\end{aligned}$$

are all normal, as they can be written as unions of conjugacy classes as shown. These are the only possible normal subgroups. ◇

There are a number of conditions which guarantee that a subgroup is normal.

Theorem 3.47
Let G be a group, and H a subgroup of G. If any of the following holds, H is normal:

(i) $H = \{e\}$ or G,

(ii) $H \subseteq Z(G)$,

(iii) $|G : H| = 2$,

(iv) H is the only subgroup of order $|H|$ in G.

Proof:
We have already seen (i) is true.
(ii) Recall that for any element $x \in Z(G)$, $C(x) = \{x\}$, so if $H \subseteq Z(G)$, then

$$H = \bigcup_{x \in H} \{x\} = \bigcup_{x \in H} C(x),$$

so H is a union of conjugacy classes, and so H is normal.
(iii) If $|G : H| = 2$, then H has two left cosets, H itself and xH, where $x \notin H$. Similarly, it has two right cosets H and Hx. Now since every element of G is either in H or xH, we have that $xH = G \setminus H$. But we similarly have that $Hx = G \setminus H$. Hence $xH = Hx$, and corresponding left and right cosets of H are equal. Hence H is normal.
(iv) We know that every conjugate of H is a subgroup of G, and we must have $|x^{-1}Hx| = |H|$. Hence if H is the only subgroup of order $|H|$, we must have $H = x^{-1}Hx$ for all $x \in G$. So H is normal. ■

Example 3.46
In the dihedral group $D_{2n} = \{1, a, a^2, \ldots, a^{n-1}, b, ab, \ldots, a^{n-1}n\}$, the subgroup $\langle a \rangle = \{1, a, a^2, \ldots, a^{n-1}\}$ has order $|\langle a \rangle| = o(a) = n$. So $|D_{2n} : \langle a \rangle| = |D_{2n}|/|\langle a \rangle| = 2n/n = 2$.
So $\langle a \rangle$ is always a normal subgroup of D_{2n}. ◇

Normal subgroups also have a nice relationship with the lattice structure of subgroups.

Proposition 3.48
Let G be a group, K a normal subgroup of G, and H an arbitrary subgroup of G. Then HK is a subgroup of G, and furthermore $H \vee K = HK = KH$.

Proof:
We start by showing that HK is a group. Given x and $y \in H$ and u and $v \in K$, we have that xu and yv are typical elements of HK. Now

$$xu(yv)^{-1} = xuv^{-1}y^{-1} = xy^{-1}(y^{-1})^{-1}uv^{-1}y^{-1},$$

and we know $xy^{-1} \in H$, and $(y^{-1})^{-1}uv^{-1}y^{-1} \in K$, since it is a conjugate of $uv^{-1} \in K$. So $xu(yv)^{-1} \in HK$, and hence HK is a subgroup of G.

Now we need to show that $\langle H \cup K \rangle = HK$. We do this by showing that HK is the smallest subgroup of G containing both H and K. First observe that since $e \in K$, $H = He \subseteq HK$. Similarly $K = eK \subseteq HK$. So HK contains both H and K. Now assume that F is a subgroup which contains both H and K. Then given any $x \in H$ and $u \in K$, then x and $u \in F$ and so $xu \in F$. Hence $HK \subseteq F$. So HK is the smallest subgroup which contains both H and K.

A similar argument shows that KH is a subgroup of G and that $H \vee K = KH$ as well.

So we have that $HK = \langle H \cup K \rangle = H \vee K = K \vee H = KH$. ■

We can use this fact to show that normal subgroups form a sub-lattice within the lattice of subgroups of a group.

Theorem 3.49
Let G be a group, and let H and K be normal subgroups of G. Then $H \vee K = \langle H \cup K \rangle$ and $H \wedge K = H \cap K$ are both normal.

Proof:
We know that $H \vee K = HK$, so we will show that HK is a normal subgroup of G. If $x \in H$ and $u \in K$ and $z \in G$, then xu is a typical element of HK and we have that

$$z^{-1}xuz = z^{-1}xzz^{-1}uz,$$

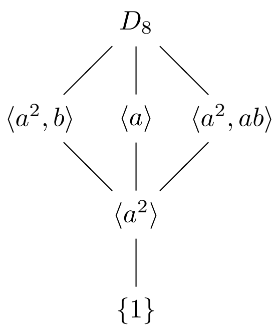
and $z^{-1}xz \in H$, $z^{-1}uz \in K$, and so $z^{-1}xuz \in HK$. Hence HK is normal.

Also, given any $y \in H \cap K$, and any $x \in G$, we have that $x^{-1}yx \in H$ and $x^{-1}yx \in K$, so $x^{-1}yx \in H \cap K$, and so $H \cap K$ is normal. ■

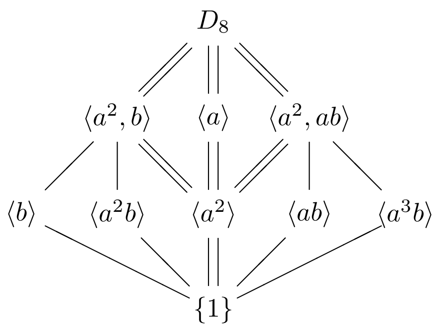
Corollary 3.50
If G is a group, then the set of normal subgroups of G is a lattice.

We will use the symbol $\lhd$ to represent the order that gives this lattice. In other words, $H \lhd K$ if and only if both H and K are normal and $H \leq K$. This extends the use of $\lhd$ to indicate a normal subgroup of a group.

Example 3.47
The normal subgroup lattice of D_8 is:



The lattice diagrams for the subgroup lattice and the normal subgroup lattice are sometimes combined by representing the normal subgroup lattice by thicker lines or double lines.



◇

Part of the importance of normal subgroups is that they are closely related to homomorphisms. In fact every homomorphism gives you a normal subgroup.

Theorem 3.51
Let G and H be groups and $\alpha : G \to H$ a homomorphism. If K is a normal subgroup of H, then $\alpha^{-1}(K)$ is a normal subgroup of G.

In particular, $\ker\alpha$ is always normal.

Proof:
We know that $\alpha^{-1}(K)$ is a subgroup of G. Given any $x \in G$, and any $y \in \alpha^{-1}(K)$, we have that

$$\alpha(x^{-1}yx) = (\alpha(x))^{-1}\alpha(y)\alpha(x),$$

and $\alpha(y) \in K$, so $(\alpha(x))^{-1}\alpha(y)\alpha(x) \in K$. Therefore, $x^{-1}yx \in K$, and so K is normal.

We recall that $\ker\alpha = \alpha^{-1}(\{e\})$, and $\{e\}$ is always normal, so $\ker\alpha$ is normal. ■

Corollary 3.52
If G and H are groups, and $\alpha : G \to H$ is an isomorphism, then a subgroup K of G is normal if and only if $\alpha(K)$ is normal.

Corollary 3.53
If G and H are isomorphic, then the lattice of normal subgroups of G and the lattice of normal subgroups of H are isomorphic.

Example 3.48
Consider the homomorphism $\alpha : D_8 \to V$ defined by $\alpha(a) = a$, and $\alpha(b) = b$. Looking at the image of each element, we see get the following table:

x	$\alpha(x)$
1	1
a	a
a^2	1
a^3	a
b	b
ab	ab
a^2b	b
a^3b	ab

Since V is Abelian, every subgroup is normal, and the inverse images of each subgroup are the normal subgroups

$$\begin{aligned}\alpha^{-1}(\{1\}) &= \{1, a^2\}\\ \alpha^{-1}(\{1, a\}) &= \{1, a, a^2, a^3\}\\ \alpha^{-1}(\{1, b\}) &= \{1, b, a^2, a^2b\}\\ \alpha^{-1}(\{1, ab\}) &= \{1, ab, a^2, a^3b\}\\ \alpha^{-1}(V) &= D_8.\end{aligned}$$

◇

Exercises

3.8.1. Prove Theorem 3.45.

3.8.2. Let $H = \langle X \rangle$ be a subgroup of a group G. Show that H is normal if and only if $g^{-1}xg \in H$ for all $x \in X$.

3.8.3. Find the normal subgroup lattice of D_{10}.

3.8.4. Find the normal subgroup lattice of D_{12}.

3.8.5. Find the normal subgroup lattice of A_4.

3.8.6. Given elements x and $y \in G$, their ***commutator*** is the element

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

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

$$G' = \langle \{[x, y] : x, y \in G\} \rangle$$

(i) Show that if x and y commute, then $[x, y] = e$. Conclude that the commutator subgroup of an Abelian group is always $\{e\}$.

(ii) Show that G' is normal.

(iii) Find the commutator subgroup of D_8.

(iv) If H and K are normal subgroups of G, show that the commutator $[x, y]$ of any pair $x \in H$ and $y \in K$ lies in $H \wedge K$. Show that if $H \wedge K = \{e\}$, then any element of H commutes with any element of K.

3.9 Groups of Small Order, Part II

In previous sections we have discovered that all the groups of order less than 8 are isomorphic to one of a small collection of groups. We do not know what groups there are of order 8, however.

We have identified C_8, $C^2 \times C^4$, $C_2 \times C_2 \times C_2$ and D_8, but there could potentially be more. In fact, in Exercise 3.5.2, there was the following definition.

Definition 3.12
For any natural number n, the **quaternion group** *is the group with elements*

$$Q_{4n} = \{1, a, a^2, \dots, a^{2n-1}, b, ab, a^2b, \dots, a^{2n-1}b\}$$

where the Cayley table is determined by the relations $a^{2n} = 1$, $b^2 = a^n$, and $b^{-1}ab = a^{-1}$.

In Exercise 3.5.2 it was shown that Q_8 is not isomorphic to any other known group of order 8. In fact, Q_8 completes the set of isomorphism classes of groups of order 8.

Theorem 3.54
If G is a group of order 8, then G is isomorphic to one of C_8, $C_2 \times C_4$, $C_2 \times C_2 \times C_2$, D_8 or Q_8.

Proof:
If G has an element of order 8, then Theorem 2.13 tells us that G is cyclic, and so $G \cong C_8$.

If every element of G other then e has order 2, then Theorem 2.18 tells us that G is a direct product of cyclic groups of order 2. So $G \cong C_2 \times C_2 \times C_2$.

If G is not isomorphic to one of these two groups, it must have an element of order 4, and no elements of order 8. Let a be this element of order 4 in G, and let $H = \langle a \rangle$. Since $|G : H| = |G|/|H| = 8/4 = 2$, so if $b \in G \setminus H$, then H has two cosets H and Hb, and G is the disjoint union of H and Hb. So

$$G = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}.$$

If G is Abelian, then $ab = ba$, and b must either be of order 2 or 4. If $b^2 = 1$, then $G \cong C_4 \times C_2$ where the isomorphism is given by $\alpha(u^k, v^l) = a^k b^l$, where $C_4 = \langle u \rangle$ and $C_2 = \langle v \rangle$. If $b^2 \neq e$, then we must have $b^2 = a^k$, since if $b^2 = a^k b$, then the cancellation law tells us that $b = a^k \in H$, which is a contradiction. Furthermore if $k = 1$ or $k = 3$, then $b^4 = a^2 \neq e$, which is a contradiction. So then $b^2 = a^2$. But in this case, ab has order 2, and $G \cong C_4 \times C_2$ where the isomorphism is given by $\alpha(u^k, v^l) = a^k(ab)^l$.

So the only Abelian groups of order 8 are C_8, $C_4 \times C_2$ and $C_2 \times C_2 \times C_2$.

If G is not Abelian, we note that Theorem 3.47 says that since $|G : H| = 2$, H is normal in G, which means that $b^{-1}ab \in H$, so

$$b^{-1}ab = a^k$$

where k is one of 0, 1, 2 or 3. But $k \neq 0$, since otherwise $a \in C(e) = \{e\}$, which cannot happen. If $k = 2$, then

$$b^{-1}a^2b = b^{-1}abb^{-1}ab = a^2a^2 = a^4 = e,$$

so $a^2 \in C(e)$, which is also impossible. If $k = 1$, then $b^{-1}ab = a$ implies $ab = ba$, so G is Abelian. So the only remaining possibility is that $k = 3$.

As before, the order of b must be either 2 or 4. If b has order 2, then $b^2 = 1$. This means that $b = b^{-1}$, and so $b^{-1}ab = a^3$ implies that $ba = a^3b$. So G is determined by the relations $a^4 = 1$, $b^2 = 1$ and $ba = a^3b$, and G is isomorphic to D_8 under the trivial isomorphism $\alpha(a^kb^l) = a^kb^l$.

Finally, if b has order 4, then the same argument as the Abelian case tells us that $b^2 = a^2$. We then observe that since $b^3 = b_{-1}$, we have that G is determined by the relations $a^4 = 1$, $b^2 = a^2$ and $b^{-1}ab = a^{-1}$, and G is isomorphic to Q_8 under the trivial isomorphism $\alpha(a^kb^l) = a^kb^l$. ■

The next lowest order that we don't have full information on is groups of order 9. We know that we have C_9 and $C_3 \times C_3$, but there could potentially be other groups of order 9.

Theorem 3.55
Let G be a group of order 9. Then G is isomorphic to one of C_9 or $C_3 \times C_3$.

Proof:

From Lagrange's theorem, the elements of G all have orders dividing 9, so they have order 1, 3 or 9. If there is an element of order 9, then Theorem 2.13 tells us that $G \cong C_9$. So if G is not isomorphic to C_9, then every element other than the identity must have order 3.

Choosing an element $a \neq e$, we have that the subgroup $H = \langle a \rangle$ has order 3. Now choose $b \notin H$. Now $b^2 \notin H$, since that would imply $b^2 = a^k$, where $k = 1$ or 2, and in either case b would have order 6. Similarly $b^2 \notin Hb$ since then we would have $b^2 = a^k b$, where $k = 1$ or 2, and then since G is Abelian $b^3 = a^k b^2 = a^{2k} b \neq e$, since $b \notin H$. So the right cosets of H are H, Hb and Hb^2, and therefore

$$G = \{e, a, a^2, b, ab, a^2b, b^2, ab^2, a^2b^2\}.$$

Theorem 3.41 tells us that the centre of G has $|Z(G)| = 3$ or $|Z(G)| = 9$. If $|Z(G)| = 9$, then G is Abelian, and $G \cong C_3 \times C_3$ via the isomorphism $\alpha(u^k, u^l) = a^k b^l$, where $C_3 = \langle u \rangle$.

So assume that $|Z(G)| = 3$. Without loss of generality in the above discussion, we could have assumed that we chose $a \in Z(G)$, so that $H = Z(G)$. Therefore a commutes with every element of G, so in particular, $ba = ab$. But since $G = \langle a, b \rangle$, G is Abelian and $|Z(G)| = |G| = 9$. So every group of order 9 is Abelian. ■

At this point we have classified every group of order up to and including 11. It turns out that any group of order 12 is isomorphic to one of C_{12}, $C_6 \times C_2$, D_{12}, Q_{12} or the alternating group A_4. However, the proof of this fact requires considerably more powerful techniques than we have available right now.

Exercises

3.9.1. Show that if p is a prime number, and G is a group with $|G| = p^2$, then G is isomorphic to one of C_{p^2} or $C_p \times C_p$.

Hint: generalize the case of $|G| = 9$.

3.9.2. Explain why there is one group of order 13 and two groups of order 14.

3.9.3. Show that $C_{15} \cong C_5 \times C_3$.

3.10 Extension: Cayley Graphs

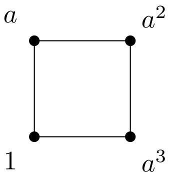
Cayley graphs are closely related to generators, and give a nice way of picturing groups. Unfortunately, they are not that useful in distingishing between groups which are not isomorphic, but they are of some independent interest, particularly when considering how one can computerize calculations involving groups.

Definition 3.13
*Let $(G, *, e)$ be a group, and let $S = \{g_1, a_2, \ldots, g_n\}$ be a finite set which generates G, ie. $G = \langle S \rangle$. The **Cayley graph** of G with the generating set S is the graph $\Gamma_G = (G, E)$ with vertices being the elements of G, and two vertices x and $y \in G$ are connected by an edge if $x = yg$ for some $g \in S \cup S^{-1}$.*

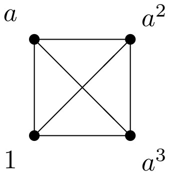
Definitions vary somewhat from source to source. Some may define the Cayley graph as a directed graph with directed edges of the form (x, xg) for $g \in S \cup S^{-1}$, while others allow a double edge (x, y) if both $x = yg$ and $y = xg$.

Example 3.49

The cyclic group $C_4 = \{1, a, a^2, a^3\}$ has a generating set $S = \{a\}$. The Cayley graph of G with this generating set has edges $(1, a)$, (a, a^2), (a^2, a^3) and $(a^3, 1)$. In other words, it looks like this:



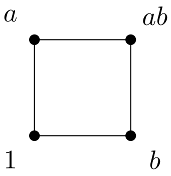
This group is also generated (somewhat redundantly) by the set $S = \{a, a^2\}$. This gives a Cayley graph which looks like this:



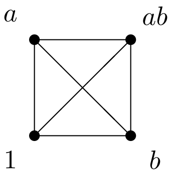
◇

Example 3.50

The four-group $V = \{1, a, b, ab\}$ has a generating set $S = \{a, b\}$. The Cayley graph of G with this generating set has edges $(1, a)$, (a, ab), $(1, b)$ and (b, ab). In other words, it looks like this:



This group is also generated by the set $S = \{a, b, ab\}$. This gives a Cayley graph which looks like this:



◇

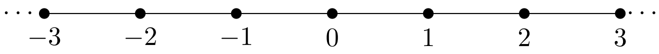
Notice that in each case, the graphs look the same, even though the groups are not isomorphic.

Proposition 3.56
Let G be a finite group. The Cayley graph with generating set taken to be all of G is the complete graph on $|G|$ vertices.

Proof:
Given any pair of vertices x, y, the element $g = y^{-1}x$ is in the generating set G, and $yg = yy^{-1}x = x$, so there is an edge joining x and y. Hence the Cayley graph is a complete graph. ■

With careful selection of the generating set, however, the Cayley graph can reveal a lot about the structure of the group.

Example 3.51
The group of integers $(\mathbb{Z}, +, 0)$ is generated by the element 1. The Cayley graph is infinite, but the region near 0 looks like:



◇

Cayley graphs have some regularities that normal graphs do not.

Proposition 3.57
Let G be a group, and S a finite set which generates G. The Cayley graph of G with generating set S has the following properties:

(i) the graph is connected.

(ii) every vertex is an end of exactly $|S \cup S^{-1}|$ edges

Proof:
(i) Every element x can be written as a product $x = x_1x_2 \cdots x_n$ of elements $x_k \in S \cup S^{-1}$, so $e, x_1, x_1x_2, \dots, x_1x_2 \cdots x_{n-1}, x$ is a path from e to x. So the Cayley graph is connected.
(ii) Given any $x \in G$, if we consider the set

$$X = \{xg : g \in S \cup S^{-1}\},$$

then we note that if $xg_1 = xg_2$, the cancellation law says that $g_1 = g_2$. Therefore every edge (x, xg) is distinct, and $|X| = |S \cup S^{-1}|$. Furthermore, if there is some y such that (y, x) is an edge, then $x = yg$ for some $g \in S \cup S^{-1}$, so $y = xg^{-1} \in X$. So X is exactly the set of all vertices connected to x by one edge. So x is an end of exactly $|S \cup S^{-1}|$ edges. ■

Exercises

3.10.1. Draw the Cayley graph of C_6 with generating set $\{a\}$.

Draw the Cayley graph of C_6 with generating set $\{a^2, a^3\}$.

3.10.2. Draw the Cayley graph of D_6 with generating set $\{a, b\}$.

3.10.3. Draw the Cayley graph of D_8 with generating set $\{a, b\}$.

3.10.4. Draw the Cayley graph of $C_2 \times C_4$ with generating set $\{(a, 1), (1, b)\}$.

3.10.5. Draw the region near 0 of the Cayley graph of $\mathbb{Z}$ with generating set $\{2, 3\}$.

3.10.6. Draw the region near 0 of the Cayley graph of $\mathbb{Z}^2$ with generating set $\{(1, 0), (0, 1)\}$.

Draw the same region if the generating set is $\{(1, 0), (0, 1), (1, 1)\}$.

3.10.7. Draw the region near e of the Cayley graph of the free group F_2 with generating set $\{a, b\}$.

Assignment 4

The following exercises are due Monday, April 19th. Since this is a long assignment, it will be worth twice as much as the other 3 assignments.

3.1 Exercises 2, 4, 6.

3.2 Exercises 1, 3, 5.

3.3 Exercises 1, 3, 5.

3.4 Exercises 1, 4, 5.

3.5 Exercises 2.

3.6 Exercises 4.

3.7 Exercises 1, 2, 5, 6.

3.8 Exercises 2, 3, 6.

3.9 Exercises 1, 2.

3.10 Exercises 1, 2, 5, 6.

Chapter 4

Constructing Groups

In Chapter 2 we saw a simple way that we could combine two groups to get a third group: the direct product. In this chapter we look at other ways to construct new groups from already known groups.

4.1 Quotient Groups

Let G be a group, and N a normal subgroup of G. We can (at least potentially) define a binary operation $*$ on the set of cosets of N by

$$Nx * Ny = Nxy.$$

The difficulty with this definition is that there may be many different choices for x' and y', so that $Nx' = Nx$ and $Ny = Ny'$, and it is not immediate why we should have $Nxy = Nx'y'$. However they are in fact equal since $x' = ux$ and $y' = vy$ for some u and $v \in N$, and since N is normal, we have $z = xvx^{-1} \in N$, so

$$x'y' = uxvy = uxvx^{-1}xy = (uz)xy,$$

so $Nx'y' = N(uz)xy = Nxy$. So $*$ is a well-defined binary operation, and it is only well-defined if N is normal.

Proposition 4.1
Let G be a group and N a normal subgroup of G. Let G/N be the set of all cosets of N in G. Then $(G/N, *, N)$ is a group.

Proof:
We first observe that G/N is associative, since for any right cosets Nx, Ny and $Nz \in G/N$, we have

$$(Nx * Ny) * Nz = Nxy * Nz = Nxyz = Nx * Nyz = Nx * (Ny * Nz).$$

The set N is an identity, since $N = Ne$, and so

$$Ne * Nx = Nex = Nx \qquad \text{and} Nx * Ne = Nxe = Nx.$$

Finally, Nx^{-1} is the inverse of Nx, since

$$Nx * Nx^{-1} = Nxx^{-1} = Ne = N \qquad \text{and} \qquad Nx^{-1} * Nx = Nx^{-1}x = Ne = N.$$

■

In fact, there is another way of looking at this product. If we consider cosets Nx and Ny, then we have that the product of the cosets as sets is

$$(Nx)(Ny) = (xN)(Ny) = (xN^2)y = (xN)y = (Nx)y = Nxy,$$

recalling that $Nx = xN$ since N is normal, and $N^2 = N$ since N is a subgroup. In other words, $Nx * Ny$ is given by the product of sets $(Nx)(Ny)$. In some texts this is used as the definition of the product.

Definition 4.1
*If G is a group, and N a normal subgroup of G, then we call G/N the **quotient group** of N in G.*

Example 4.1
Let $D_6 = \{1, a, a^2, b, ab, a^2b\}$ as usual. If $N = \{1, a, a^2\}$, then N is normal, and the cosets are N and Nb. Then the Cayley table of D_6/N is simply

$*$	N	Nb
N	N	Nb
Nb	Nb	N

Clearly, $D_6/N \cong C_2$. ◇

Example 4.2
The additive group of integers is Abelian, so every subgroup is normal. If we have a subgroup of the form

$$N = m\mathbb{Z} = \{mx : x \in \mathbb{Z}\},$$

then we observed in Example 3.33 that the cosets of this subgroup are the sets of numbers which have the same remainer modulo m, or more concretely,

$$\mathbb{Z}/N = \{N, N+1, N+2, \ldots, N+(m-1)\}.$$

The group operation on these cosets is just

$$(N+x) + (N+y) = N + (x+y) = N + z,$$

where $z = x + y \pmod{m}$. In other words $\mathbb{Z}/m\mathbb{Z} \cong Z_m$. Indeed, this is a common way of defining addition modulo m. ◇

From the theory developed in the previous chapters, we can immediately conclude the following.

Proposition 4.2
Let G be a group, and N a subgroup of G. Then

(i) if $|G|$ is finite, then $|G/N| = |G|/|N|$,

(ii) the function $\alpha(x) = Nx$ is a homomorphism from G to G/N, and $\ker\alpha = N$.

Proof:
(i) This is immediate from the fact that $|G/N| = [G : N]$ and Lagrange's Theorem.

(ii) That α is a homomorphism follows immediately from the fact that

$$\alpha(x) * \alpha(y) = Nx * Ny = Nxy = \alpha(xy).$$

It is immediate that $N \subseteq \ker\alpha$, since if $x \in N$, $\alpha(x) = Nx = N$. Similarly, if $\alpha(x) = N$, then $Nx = N$, which only happens when $x \in N$. So $\ker\alpha = N$. ■

Corollary 4.3
A subgroup N of a group G is normal if and only if it is the kernel of some homomorphism.

The relationship between quotient groups and homomorphisms is significantly deeper than this corollary, however. These relationships are encapsulated in a trilogy of theorems called the Isomorphism Theorems. Unfortunately there is little consensus about which of the three should be first, second and third.

Theorem 4.4 (First Isomorphism Theorem)
Let G and H be groups, and $\alpha : G \to H$ a homomorphism. Then

$$\alpha(G) \cong G/\ker\alpha.$$

Proof:
For simplicity of notation, let $N = \ker\alpha$.

We would like to define a function $\beta : G/\ker\alpha \to \alpha(G)$ by $\beta(Nx) = \alpha(x)$, but it's not clear that this is a well-defined function. To verify that this definition is good, we need to show that if $Nx = Ny$ then $\beta(Nx) = \beta(Ny)$ so that the value of β does not depend on the choice of x.

Now if $Nx = Ny$ we have that $xy^{-1} \in N$, so $\alpha(xy^{-1}) = e$, and hence

$$\alpha(y) = e\alpha(y) = \alpha(xy^{-1})\alpha(y) = \alpha(xy^{-1}y) = \alpha(x).$$

So we conclude that if $Nx = Ny$ then $beta(Nx) = \beta(Ny)$, and so β is well-defined.

Furthermore, β is a homomorphism, since

$$\beta(Nx * Ny) = \beta(Nxy) = \alpha(xy) = \alpha(x)\alpha(y) = \beta(Nx)\beta(Ny).$$

We also have that β is onto, since if $y \in \alpha(G)$, then $y = \alpha(x)$ for some $x \in G$, but then $y = \beta(Nx)$.

Finally, if $\beta(Nx) = \beta(Ny)$, then $\alpha(x) = \alpha(y)$, so

$$\alpha(xy^{-1}) = \alpha(x)(\alpha(y))^{-1} = \alpha(x)(\alpha(x))^{-1} = e.$$

This means that $xy^{-1} \in \ker\alpha = N$, so $Nx = Ny$. Hence β is one-to-one.

So β is an isomorphism, and we conclude that $G/\ker\alpha \cong \alpha(G)$. ■

We will now turn to look at how the subgroup structure of G and the subgroup structure of G/N are related. Letting $\alpha : G \to G/N$ be given by $\alpha(x) = Nx$, we have that if $H \leq G$, then $\alpha(H) \leq G/N$ and if $K \subseteq G/N$ then $\alpha^{-1}(K) \leq G$ from Propositions 2.24 and 2.26. A deeper question is if there is any relationship between normal subgroups of G and normal subgroups of G/N.

Proposition 4.5
Let G be a group and N a normal subgroup of G. Then every subgroup of N is equal to K/N where for some K with $N \leq K \leq G$. Furthermore K/N is normal if and only if K is normal.

Proof:

Let $\alpha : G \to G/N$ be given by $\alpha(x) = Nx$.

Let H be a subgroup of G/N, and let $K = \alpha^{-1}(H)$, so that K is a subgroup of G, and since $N = \alpha^{-1}(\{e\}) \subseteq \alpha^{-1}(H)$, so $N \leq K$. So $H = \alpha(K)$ and if we restrict α to K, the First Isomorphism Theorem tells us that

$$\alpha(K) \cong K/N.$$

Furthermore, recall from the proof of the First Isomorphism Theorem that this isomorphism is given by $\beta(Nx) = \alpha(x)$, and $\alpha(x) = Nx$, so β is just the identity map, and so $H = K/N$.

If K is normal in G, then $x^{-1}Kx = K$ for each $x \in G$, and so

$$(Nx^{-1}) * \alpha(K) * (Nx) = \alpha(x^{-1}) * \alpha(K) * \alpha(x) = \alpha(x^{-1}Kx) = \alpha(K),$$

so $H = \alpha(K)$ is normal in G/N.

Conversely, if $H = K/N$ is normal in G/N, then Theorem 3.51 tells us immediately that $\alpha^{-1}(H) = K$ is normal in G. ■

Now if $N \lhd K \lhd G$, as in the last part of the Proposition, we note that N is normal when regarded as a subgroup of K also, and so we can take three quotients: G/N, G/K and K/N. The Second Isomorphism Theorem gives us a relationship between these three quotients.

Theorem 4.6 (Second Isomorphism Theorem)
Let G be a group and N and K normal subgroups of G with $N \leq K$. Then

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

Proof:

We first note that since K is normal, the previous proposition tells us that K/N is normal in G/N, and so $(G/N)/(K/N)$ is defined.

We would like to define a function $\alpha : G/N \to G/K$ by $\alpha(Nx) = Kx$, but once again we must be careful that this well-defined, since there are multiple possible choices for x which give the same coset Nx. If $Nx = Ny$, then we recall that $xy^{-1} \in N$, and so $xy^{-1} \in K$ as well. So $K = K(xy^{-1})$,

$$\alpha(Ny) = Ky = (Kxy^{-1})y = Kx = \alpha(Ny).$$

So this is a well-defined function.

Furthermore, α is a homomorphism, since

$$\alpha(Nx * Ny) = \alpha(Nxy) = Kxy = Kx * Ky = \alpha(Nx) * \alpha(Ny).$$

We observe that $\alpha(Nx) = K$ if and only if $x \in K$, or equivalently, $Nx \in K/N$. But this means that $\ker \alpha = K/N$. We also have that since every coset of K is of the form Kx for some $x \in G$, we have that $\alpha(G/N) = \{\alpha(Nx) : x \in G\} = \{Kx : x \in G\} = G/K$, so α is onto.

Now the First Isomorphism Theorem tells us that

$$\alpha(G/N) \cong (G/N)/\ker \alpha,$$

But we know that $\alpha(G/N) = G/K$ and $\ker \alpha = K/N$, so

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

■

Note that this theorem essentially says that the quotient operation cancels in the way that you would expect a quotient to cancel: if G, K and N were numbers you would expect the same equation to hold.

We can also ask what happens if K is a general subgroup of G. In this case we can't talk about K/N, since we may not have $N \subseteq K$. However we do know that the meet of K and N is a subgroup of K. Indeed we have that for any $x \in K$, and $y \in K \wedge N$ we have that $x^{-1}yx \in K$, since K is a subgroup. But we also have that $x^{-1}yx \in N$, since N is normal. Hence $K \wedge N$ is a normal subgroup of the subgroup K. So we can consider the quotient group $K/(K \wedge N)$. Similarly, although N is not a subgroup of K, we know that $N \vee K$ contains N, and since N is normal, we can consider the quotient group $(K \vee N)/N$.

Theorem 4.7 (Third Isomorphism Theorem)
Let G be a group, K a subgroup of G and N a normal subgroup of G. Then

$$K/(K \wedge N) \cong (K \vee N)/N.$$

Proof:

Recall from Proposition 3.48 that $K \vee N = NK$ when N is normal.

We define a function $\alpha : K \to G/N$ by $\alpha(x) = Nx$. This is a homomorphism since

$$\alpha(xy) = Nxy = Nx * Ny = \alpha(x) * \alpha(y).$$

The image of α is the set

$$\alpha(K) = \{Nx : x \in K\} = NK/N = (N \vee K)/N.$$

Furthermore, the kernel of α is the set of x such that $\alpha(x) = N$, ie. all $x \in K$ such that $Nx = N$. But $Nx = N$ if ans only if $x \in N$, so $x \in K \cap N = K \wedge N$.

So the First Isomorphism Theorem tells us that

$$\alpha(K) = K/\ker\alpha,$$

and so

$$(N \vee K)/N \cong K/(K \wedge N).$$

■

As you may expect, quotient groups can be used to shed some light on the structure of finite groups.

Theorem 4.8
Let G be a finite group which is not Abelian, and $Z(G)$ the centre of G. Then $G/Z(G)$ cannot be cyclic.

Proof:
We first recall that $Z(G)$ is always normal, so $G/Z(G)$ is defined. If $G/Z(G)$ is cyclic, then we can find an element t so that $Z(G)t$ generates $G/Z(G)$, and so every coset of $Z(G)$ is of the form $Z(G)t^k$ for some k. But then given arbitrary elements x and $y \in G$, we have that $x = ut^k$ and $y = vt^l$ for some u and $v \in Z(G)$. So now, since u and v commute with all elements of G,

$$xy = ut^kvt^l = uvt^kt^l = uvt^lt^k = vt^lut^k = yx.$$

So G is Abelian, which is a contradiction. ■

Corollary 4.9
If p is a prime number and G is a group with order p^2, then G is Abelian.

Proof:
We know from Theorem 3.41 that the order of $Z(G)$ is either p or p^2. But if $|Z(G)| = p$, then G is not Abelian, and we have that $|G/Z(G)| = |G|/|Z(G)| = p^2/p = p$, so $G/Z(G)$ must be a cyclic group of order p. But the previous theorem showed that this cannot happen.

Hence $|Z(G)| = p^2$, and so G is Abelian. ■

This corollary allows us to slightly simplify the proof of Theorem 3.55, since the last paragraph can be replaced by a reference to this corollary. Indeed, one can generalise that theorem to all prime numbers.

Theorem 4.10
If p is a prime number and G is a group with order p^2, then G is isomorphic to one of C_{p^2} or $C_p \times C_p$.

Proof:
The previous corollary tells us that G is Abelian. If G has an element of order p^2, then $G \cong C_{p^2}$.

Otherwise every element of G other then the identity e has order p. Let a be such an element, and let $N = \langle a \rangle = \{1, a, a^2, \ldots, a^{p-1}\}$. Lagrange's Theorem tells us that the quotient group G/N has order p, so $G/N \cong C_p$. So there is some element b with order p, such that G/N is generated by the coset Nb, so $G/N = \{N, Nb, Nb^2, \ldots, Nb^{n-1}\}$. Hence $G = \{a^k b^l : k, l = 0, 1, \ldots, p-1\}$ with $a^p = e$ and $b^p = e$. Hence G is isomorphic to $C_p \times C_p$ via the isomorphism

$$\alpha(u^k, u^l) = a^k b^l.$$

■

Exercises

4.1.1. Consider the group D_8. The subgroup $Z(D_8) = \{1, a^2\}$ is normal, since it is the centre of D_8. Write down the Cayley table of $D_8/Z(D_8)$.

Explain why $D_8/Z(D_8) \cong V$.

4.1.2. Consider the group D_{12}. The subgroup $Z(D_{12}) = \{1, a^3\}$ is normal, since it is the centre of D_{12}. Write down the Cayley table of $D_{12}/Z(D_{12})$.

Explain why $D_{12}/Z(D_{12}) \cong D_6$?

4.1.3. Generalize the above two results, and show that if n is even, then $D_{2n}/Z(D_{2n}) \cong D_n$.

4.1.4. Consider the normal subgroup $N = \{1, a^2, a^4\}$ of the group D_{12}. Write down the Cayley table of D_{12}/N. Show $D_{12}/N \cong V$.

4.1.5. Let G and H be groups. Show that the set

$$K = \{(g, e) : g \in G\}$$

is a normal subgroup of $G \times H$. Let $\pi : G \times H \to H$ be defined by $\pi(g, h) = h$ (this a homomorphism by Exercise 2.9.6). Use this homomorphism to show that

$$(G \times H)/K \cong H.$$

4.1.6. Consider the additive group $\mathbb{Z}^2$. Show that $\alpha(x, y) = 3x + 2y$ is a homomorphism from $\mathbb{Z}^2 \to \mathbb{Z}$, and $\ker \alpha = K = \{(2k, -3k) : k \in \mathit{integers}\}$. Show that

$$\mathbb{Z}^2/K \cong \mathbb{Z}.$$

4.1.7. Let $\alpha : G \to H$ be a homomorphism. Use the first Isomorphism Theorem to show that $|\alpha(G)|$ divides both $|G|$ and $|H|$. Show that if $|G|$ and $|H|$ have a greatest common divisor of 1, then $\alpha(x) = e$ for all $x \in G$.

4.1.8. Let G be a group. Recall the commutator subgroup G' defined in Exercise 3.8.6 is normal. Show that G/G' is Abelian.

4.1.9. Let G be a group, and N be a normal subgroup of G such that G/N is Abelian. Show that the commutator subgroup G' defined in Exercise 3.8.6 is a normal subgroup of N.

4.2 Automorphism Groups

Recall that an automorphism of a group G is an isomorphism from G to itself. The set of all automorphisms of G is denoted by $\mathrm{Aut}(G)$. This set is never empty since at the very least the identity map defined $\mathrm{id}(x) = x$ is always an automorphism.

Proposition 4.11
If G is a group, then $(\mathrm{Aut}(G), \circ, id)$ *is a group, where* $\circ$ *is function composition.*

Proof:
Function composition of two automorphisms gives another automorphism, since if α and $\beta \in \mathrm{Aut}(G)$, then $\beta \circ \alpha : G \to G$ is an isomoprhism by Proposition 2.28, so $\beta \circ \alpha \in \mathrm{Aut}(G)$.

We already know that function composition is associative, so that group axiom holds.

The identity map id is an identity under composition, since for any $x \in G$,

$$(\mathrm{id} \circ \alpha)(x) = \mathrm{id}(\alpha(x)) = \alpha(x) \qquad \text{and} \qquad (\alpha \circ \mathrm{id})(x) = \alpha(\mathrm{id}(x)) = \alpha(x),$$

so we conclude that $\mathrm{id} \circ \alpha = \alpha \circ \mathrm{id} = \alpha$.

Since α is an isomorphism, it has an inverse function which is also an isomorphism from G to G by Proposition 2.28. We know that for any inverse function, $\alpha^{-1} \circ \alpha = \mathrm{id} = \alpha \circ \alpha^{-1}$, so α^{-1} is an inverse for α in the set of automorphisms. ■

Example 4.3
Consider the group C_4. Any automorphism has to preserve the order of each of the elements, and since a^2 is the only element of order 2, $\alpha(a^2) = a^2$ for every automorphism α. However, an automorphism could potentially swap a and a^3. Indeed, there are two automorphisms: id and the function $\alpha(x) = x^{-1}$, or more concretely,

x	$\alpha(x)$
1	1
a	a^3
a^2	a^2
a^3	a

Verifying that this is an isomorphism is easy, since

$$\alpha(a^k a^l) = \alpha(a^{k+l}) = a^{-k-l} = a^{-k}a^{-l} = \alpha(a^k)\alpha(a^l),$$

and it is clearly bijective.

Since there are only two elements, $\mathrm{Aut}(C_4) \cong C_2$. ◇

Example 4.4

Consider the four-group V. V has 3 elements of order 2, a, b and ab, so an isomorphism could possibly interchange those elements. In fact any permutation of these three elements gives rise to a distinct automorphism.

For example, the function α given by

x	$\alpha(x)$
1	1
a	ab
b	b
ab	a

is an automorphism: it is clearly bijective, $\alpha(xx) = 1 = \alpha(x)\alpha(x)$ for any $x \in V$, since $x^2 = 1$ for every element, $\alpha(1x) = \alpha(1)\alpha(x)$ for any $x \in V$, and the remaining cases are covered by

$$\begin{aligned}\alpha(ab) &= a = (ab)b = \alpha(a)\alpha(b)\\ \alpha(a(ab)) &= b = (ab)a = \alpha(a)\alpha(ab)\\ \alpha(b(ab)) &= ab = ba = \alpha(b)\alpha(ab).\end{aligned}$$

So α is indeed an automorphism.

Given that every automorphism corresponds to a permutation of a set with 3 elements, and function composition will correspond to composition of the permutations, we have that $\mathrm{Aut}(V) \cong S_3$. ◇

As the previous example illustrates, finding all the automorphisms of a group can be potentially difficult. However, non-Abelian groups have a collection of automorphisms which are easy to find.

Proposition 4.12

If G is a group, then the conjugation by x function

$$\alpha_x(y) = x^{-1}yx$$

is an automorphism.

Proof:

We first note that

$$\alpha_x(yz) = x^{-1}yzx = x^{-1}yxx^{-1}zx = \alpha(y)\alpha(z),$$

so $\alpha : G \to G$ is a homomorphism. Now $\alpha_x(y) = e$ if and only if

$$x^{-1}yx = e.$$

But this implies that $y = xx^{-1} = e$. So $\ker \alpha = \{e\}$, and so α_x is one-to-one. Finally, G is a normal subgroup of itself, so $x^{-1}Gx = G$, and so $\alpha_x(G) = G$.

Hence α_x is an automorphism. ■

We call such automorphisms ***inner automorphism***, and let $\mathrm{Inn}(G) = \{\alpha_x : x \in G\}$ be the set of all inner automorphisms of G. Of course, not every one of these automorphisms need be distinct, since if $x \in Z(G)$, then

$$\alpha_x(y) = x^{-1}yx = \mathrm{id}(y),$$

for every y, and so $\alpha_x = y$. So in particular, the collection of inner automorphisms is just $\{\mathrm{id}\}$ if G is Abelian. In fact the set of inner automorphisms is very closely related to the centre.

Theorem 4.13
Let G be a group. Then $\mathrm{Inn}(G)$ is a subgroup of $\mathrm{Aut}(G)$, the function $\beta : x \mapsto \alpha_{x^{-1}}$ is a homomorphism from G onto $\mathrm{Inn}(G)$, and

$$\mathrm{Inn}(G) \cong G/Z(G).$$

Proof:

We start by observing that the function β is a homomorphism:

$$\beta(xy)(z) = \alpha_{(xy)^{-1}}(z) = xyzy^{-1}x = x(\alpha_{y^{-1}}(z))x = \alpha_{x^{-1}}(\alpha_{y^{-1}}(z)) = (\beta(x)\circ\beta(y))(z)$$

for all $z \in G$, so $\beta(xy) = \beta(x) \circ \beta(y)$.

Now the image of G under β is precisely $\mathrm{Inn}(G)$, so $\mathrm{Inn}(G)$ is a subgroup. Furthermore, $\beta(x) = \mathrm{id}$ if and only if $\beta(x)(z) = z$ for all $z \in G$, or equivalently,

$$xzx^{-1} = z$$

for all $z \in G$. So $x \in \ker \beta$ if and only if $x \in Z(G)$. Therefore $\ker \beta = Z(G)$.

The First Isomorphism Theorem then tells us that

$$\beta(G) \cong G/\ker \beta,$$

so

$$\mathrm{Inn}(G) \cong G/Z(G).$$

■

Corollary 4.14
If G is a finite group which is not Abelian, then $\mathrm{Inn}(G)$ is never cyclic.

Proof:

This follows immediately from the above theorem and Theorem 4.8. ■

Example 4.5

The group D_6 has centre $Z(D_6) = \{1\}$, so $\mathrm{Inn}(D_6) \cong D_6$. In fact, since D_6 has 2 elements of order 3, and 3 elements of order 2, if $\alpha \in \mathrm{Aut}(D_6)$ we must have

$$\alpha(a) = a \text{ or } a^2$$
$$\alpha(b) = b, ab \text{ or } a^2 b$$

and since $\alpha(a^k b^l) = (\alpha(a))^k(\alpha(b))^l$, these choices completely determine the automorphism. Therefore $|\,\mathrm{Aut}(D_6)| \leq 6$, and since $|\,\mathrm{Inn}(D_6)| = |D_6| = 6$, every automorphism of D_6 is inner. ◇

Example 4.6

The group D_8 has centre $Z(D_8) = \{1, a^2\}$, so $|\,\mathrm{Inn}(G)| = |D_8|/|Z(D_8)| = 8/2 = 4$. But we know that $D_8/Z(D_8)$ cannot be cyclic, so $\mathrm{Inn}(G) \cong V$. ◇

It's worthwhile noting that if H is a normal subgroup of G, then the inner automorphisms of G are automorphisms of H when restricted to just H. This follows because if $x \in G$, we have that

$$H = x^{-1}Hx = \alpha_x(H),$$

so α_x, regarded as a function defined on H, must be a bijective homomorphism onto H, ie. an element of $\mathrm{Aut}(H)$.

A ***characteristic subgroup*** H of a group G is a subgroup which is invariant under every automorphism of G, in other words $\alpha(H) = H$ for all $\alpha \in \mathrm{Aut}(G)$. Every characteristic subgroup is automatically normal, since if $x \in G$, so $\alpha_x \in \mathrm{Inn}(G)$, then

$$H = \alpha_x(H) = x^{-1}Hx.$$

The centre of G is always characteristic, since any isomorphism always maps the centre to the centre. The trivial subgroups G and $\{e\}$ are also always characteristic.

Example 4.7

In the group D_6, the subgroup $H = \langle a \rangle$ is characteristic, since any automorphism must map 1 to 1 and elements of order 3 to elements of order 3, ie. the set $\{a, a^2\}$ maps onto $\{a, a^2\}$. ◇

Proposition 4.15

If G is a group, N is a normal subgroup of G and H is a characteristic subgroup of N, then H is a normal subgroup of G.

Proof:

Since $\alpha_x \in \mathrm{Inn}(G)$ is an automorphism of N, and H is characteristic, then

$$x^{-1}Hx = \alpha_x(H) = H.$$

■

The inner automorphisms which come from characteristic subgroups are also interesting.

Theorem 4.16
Let G be a group, and let H be a characteristic subgroup of G. Then the set of inner automorphisms of the form $\{\alpha_x : x \in H\}$ is a normal subgroup of $\mathrm{Aut}(G)$.

Proof:

We first note that since $\beta(x) = \alpha_{x^{-1}}$ is a homomorphism from G to $\mathrm{Inn}(G)$, $\beta(H) = \{\alpha_x : x \in H\}$ is a subgroup of $\mathrm{Aut}(G)$.

Let $x \in H$. Given any automorphism α, we have that for any $z \in G$,

$$\begin{aligned}(\alpha^{-1} \circ \alpha_x \circ \alpha)(z) &= \alpha^{-1}(\alpha_x(\alpha(z))) \\ &= \alpha^{-1}(x^{-1}\alpha(z)x) \\ &= \alpha^{-1}(x^{-1})\alpha^{-1}(\alpha(z))\alpha^{-1}(x) \\ &= (\alpha^{-1}(x))^{-1}z\alpha^{-1}(x) \\ &= \alpha_{\alpha^{-1}(x)}(z).\end{aligned}$$

But since H is characteristic, $\alpha^{-1}(x) \in H$, so $\alpha^{-1} \circ \alpha_x \circ \alpha \in \beta(H)$. Hence $\beta(H)$ is a normal subgroup of $\mathrm{Aut}(G)$. ■

Corollary 4.17
If G is a group, then $\mathrm{Inn}(G)$ is a normal subgroup of $\mathrm{Aut}(G)$.

Exercises

4.2.1. Find the automorphism group of C_5. Does C_5 have any non-trivial inner automorphisms?

4.2.2. Find the automorphism group of C_6.

4.2.3. Find $\mathrm{Aut}(Q_8)$.

4.2.4. Show that the additive group of integers has only two automorphisms: id and $\iota(x) = -x$. Conclude that $\mathrm{Aut}(\mathbb{Z}) \cong C_2$.

4.2.5. Let $\mathbb{Z}_m$ be the additive group of integers modulo m, and let $\alpha : \mathbb{Z}_m \to \mathbb{Z}_m$ be a homomorphism.

Show that if $\alpha(1) = k$, then $\alpha(x) = kx$.

Show that α is an automorphism if and only if the greatest common divisor of k and m is 1.

Let $\alpha_k(x) = kx$ on $\mathbb{Z}_m$. Show that $\alpha_k \circ \alpha_j = \alpha_{kj}$.

Show that $\operatorname{Aut}(\mathbb{Z}_m)$ is isomorphic to the multiplicative group $\mathbb{Z}_m^* = \{x : \gcd(x,m) = 1\}$.

Show that $\operatorname{Aut}(\mathbb{Z}_8) \cong V$.

Show that if $m = pq$ where p and q are distinct primes, then $|\operatorname{Aut}(\mathbb{Z}_m)| = (p-1)(q-1)$.

4.2.6. Show that if $(G, +, 0)$ is any finite Abelian group (written using additive notation), then the function

$$\alpha_k(x) = \underbrace{x + x + x + \cdots + x}_{k \text{ times}}$$

is a homomorphism from G to G. Show that if k and $|G|$ have a greatest common divisor of 1, then $\alpha_k(x) = 0$ if and only if $x = 0$. Show that in this case, α_k is an automorphism.

Show that $\alpha_k \circ \alpha_j = \alpha_{kj}$, so that the function $\beta : \mathbb{Z}_{|G|}^* \to \operatorname{Aut}(G)$ defined by $\beta(k) = \alpha_k$ is a homomorphism.

4.2.7. Show that if G is a group, the function $\iota(x) = x^{-1}$ is an automorphism if and only if G is Abelian.

4.2.8. Show that if $G \cong H$, then $\operatorname{Aut}(G) \cong \operatorname{Aut}(H)$.

4.2.9. Show that if n is odd then $\operatorname{Inn}(D_{2n}) \cong D_{2n}$, while if n is even then $\operatorname{Inn}(D_{2n}) \cong D_n$ (Hint: you may use Exercise 4.1.3 to prove this).

4.3 Extension: Category Theory

If you think about the basic outlines of the theory which we have developed so far, you should notice some similarities between the theories of groups, vector spaces, partial orders and lattices. At a very abstract level we have:

Sets	Functions
Groups	Homomorphisms
Vector Spaces	Linear Transformations
Partially Ordered Sets	Order-preserving Functions
Lattices	Lattice Homomorphisms

There are also similarities beyond this: in all cases there is the notion of "isomorphism" between appropriate types of sets and the notion of a "sub-" object (like a subgroup or subspace), for example.

The model that we should keep in mind ofr what we are about to define is simply a minimal set of axioms which sets and functions will satisfy:

1. each function has a domain and codomain,

2. if $\operatorname{dom} f = \operatorname{cod} g$ we can compose the functions,
3. function composition is associative,
4. for each set X, there is an identity function $\mathrm{id}_A : X \to X$, and this identity function has the property $f \circ \mathrm{id}_A = f$ and $\mathrm{id}_A \circ g = g$.

Notice that group homomorphisms also satisfy all of these conditions.

Definition 4.2
A ***category*** $\mathcal{C}$ *consists of a set of* ***objects***, $\mathcal{O}$*; a set of* ***arrows*** *or* ***morphisms*** $\mathcal{A}$, *two functions*

$$\operatorname{cod} : \mathcal{A} \to \mathcal{O} \qquad \textit{and} \qquad \operatorname{dom} : \mathcal{A} \to \mathcal{O}$$

which assign to each arrow an object called, respectively, the ***domain*** *and* ***codomain*** *of the arrow; a function*

$$id : \mathcal{O} \to \mathcal{A},$$

which assigns to each object A an ***identity arrow*** id_A*; and a* ***composition*** *operation that assigns each to pair of arrows (α, β) with $\operatorname{dom}\alpha = \operatorname{cod}\beta$ an arrow $\gamma = \alpha \circ \beta$ with $\operatorname{cod}\gamma = \operatorname{cod}\alpha$ and $\operatorname{dom}\gamma = \operatorname{dom}\beta$.*

We will write $f : A \to B$ to denote that an arrow f has domain A and codomain B, or diagramatically, write:

$$A \to B$$

These have to satisfy the following axioms:

(i) Associativity: if $f : B \to A$, $g : C \to B$, and $h : D \to C$, then $(f \circ g) \circ h = f \circ (g \circ h)$,

(ii) Identity: for any $f : A \to B$, $f \circ id_A = f$; and for any $g : B \to A$, $id_A \circ g = g$,

Notice that these axioms are very similar to the definition of a group, but with added complexity because of the neccessity of dealing with the domains and codomains, and with no inverse axiom.

Categories are very closely related to directed graphs, and we can often represent parts of a category graphically. Many key facts in category can be represented by succinctly by ***commuting diagrams***. The key property of a commuting diagram is that any path following the arrows through a diagram that start from the same object and ends at the same object are equal. For example, the associativity axiom can be represented by the following commuting diagram:

XXX Picture

Similarly, the following two diagrams represent the identity axioms:

XXX Picture

As is the case for associative binary operations, the associativity axiom for categories means that it doesn't matter where we put the parentheses in a composition of multiple arrows. We can also show that for each A, id_A is unique.

Example 4.8
The following are all categories:

1. **Set**: the category with objects being all sets contained in some universe U and arrows being all functions on those sets.
2. **Grp**: the category with objects being all groups contained in some universe U, and arrows being all group homomorphisms.
3. **Abl**: the category with objects being all Abelian groups contained in some universe U, and arrows being group homomorphisms between them.
4. **Vec**($\mathbb{F}$): the category with objects being all vector spaces over a field $\mathbb{F}$ (contained in some universe U), and arrows being linear transformations between them.
5. **Lat**: the category with objects being all lattices contained in some universe U, and arrows being lattice homomorphisms.
6. $\mathbf{Set}_*$: the category whose objects are ***pointed sets***: pairs (X, x), where X is a set contained in some universe U, and $x \in X$ is some distinguished point; and whose arrows are functions which map distingushed points to distinguished points: if (X, x) and (Y, y) are pointed sets, then $f : X \to Y$ is a morphism if and only if $f(x) = y$.

◇

There are, of course, many, many other categories. Indeed, whenever you encounter a new mathematical object, particularly in algebra, you should ask yourself "what is the category that goes with this?" If you can establish this, then you can immediately get a number of basic results for free.

For a good theory which encompasses the fundamentals of functions on sets and group homomorphisms, we need to have more than just composition and identity. We also need to determine analogues of injective functions (or group monomorphisms), surjective functions (or group epimorphisms), and most importantly bijection (or group isomorphisms).

Definition 4.3
*Let $\mathcal{C}$ be a category with objects $\mathcal{O}$ and arrows $\mathcal{A}$. An arrow $\alpha : A \to B$ is **invertible** if there is an arrow $\alpha^{-1} : B \to A$ such that $\alpha^{-1} \circ \alpha = \mathrm{id}_A$ and $\alpha \circ \alpha^{-1} = \mathrm{id}_B$. We say that two objects A and B are **isomorphic** if there is an invertible arrow $\alpha : A \to B$.*

*An arrow $\alpha : A \to B$ is **monic** if whenever there are arrows β_1 and $\beta_2 : C \to A$ such that $\alpha \circ \beta_1 = \alpha \circ \beta_2$, then $\beta_1 = \beta_2$ (ie. we can cancel α on the left). An* *arrow $\alpha : A \to B$ is* ***epi*** *if whenever there are arrows β_1 and $\beta_2 : B \to C$ such that $\beta_1 \circ \alpha = \beta_2 \circ \alpha$, then $\beta_1 = \beta_2$ (ie. we can cancel α on the right).*

A ***right inverse*** *of an arrow $\alpha : A \to B$ is an arrow $\rho : B \to A$ such that $\alpha \circ \rho = \mathrm{id}_B$. A* ***left inverse*** *of an arrow $\alpha : A \to B$ is an arrow $\lambda : B \to A$ so that $\lambda \circ \alpha = \mathrm{id}_A$. A right inverse of α is also called a* ***section*** *of α, while a left-inverse is called a* ***retraction*** *of α.*

If an object A has the property that for any object B we have a exactly one arrow $B \to A$, it is said to be ***terminal****. If instead it has the property that there is exactly one arrow from $A \to B$, then it is said to be* ***initial****.*

Example 4.9

In the categories of **Set** and **Grp**, we have that following correspondence:

	Set	**Grp**
invertible arrow	bijective function	isomorphism
monic arrow	injective function	monomorphism
epi arrow	surjective function	epimorphism
terminal object	any set with one element	any group with one element
initial object	the empty set	any group with one element

◇

We can prove a number of facts immediately:

Proposition 4.18

If $\mathcal{C}$ is a category, then

(i) if an arrow α has a right inverse, then it is epi,

(ii) if an arrow α has a left inverse, then it is monic,

(iii) an arrow α has both a left and right inverse if and only if it is invertible,

(iv) if an arrow is invertible, it is both epi and monic.

Proof:

(i) Let $\alpha : A \to B$ and let $\rho : B \to A$ be a right inverse of α. Then given any arrows β_1 and $\beta_2 : B \to C$ such that $\beta_1 \circ \alpha = \beta_2 \circ \alpha$, we have that

$$\begin{aligned}\beta_1 &= \beta_1 \circ \mathrm{id} \\ &= \beta_1 \circ \alpha \circ \rho \\ &= \beta_2 \circ \alpha \circ \rho \\ &= \beta_2 \circ \mathrm{id} \\ &= \beta_2.\end{aligned}$$

So α is epi.

(ii) The proof of this is left as an exercise.

(iii) If α is invertible, then the inverse is both a left and right inverse, so α has both a left and right inverse.

On the other hand, if $\alpha : A \to B$ and $\rho : B \to A$ and $\lambda : B \to A$ be right and left inverses of α, respectively, then

$$\begin{aligned} \rho &= \mathrm{id} \circ \rho \\ &= \lambda \circ \alpha \circ \rho \\ &= \lambda \circ \mathrm{id} \\ &= \lambda \end{aligned}$$

So $\rho = \lambda$ is an inverse for α.

(iv) This follows immediately from the first three parts.

■

In the previous chapter, key results came from looking at an object in another category which corresponded to the group, such as looking at the subgroup lattice of a group in the category of lattices. These sorts of correspondences between categories were first recognised in the study of algebraic topology, and are extremely powerful. Indeed, in some sense they are what justifies the study of categories as a distinct topic.

Definition 4.4
Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be two categories with object sets $\mathcal{O}_1$ and $\mathcal{O}_2$, and arrow sets $\mathcal{A}_1$ and $\mathcal{A}_2$, respectively. A ***functor*** *$\mathcal{F} : \mathcal{C}_1 \to \mathcal{C}_2$ is a pair of functions $\mathcal{F}_\mathcal{O} : \mathcal{O}_1 \to \mathcal{O}_2$ and $\mathcal{F}_\mathcal{A} : \mathcal{A}_1 \to \mathcal{A}_2$ such that if $A \in \mathcal{O}_\infty$, α and $\beta \in \mathcal{A}_\infty$, then*

$$\begin{aligned} &\operatorname{dom} \mathcal{F}_\mathcal{A}(\alpha) = \mathcal{F}_\mathcal{O}(\operatorname{dom} \alpha) &\qquad &\operatorname{cod} \mathcal{F}_\mathcal{A}(\alpha) = \mathcal{F}_\mathcal{O}(\operatorname{cod} \alpha) \\ &\mathcal{F}_\mathcal{A}(\alpha \circ \beta) = (\mathcal{F}_\mathcal{A}(\alpha) \circ \mathcal{F}_\mathcal{A}(\beta) &\qquad &\mathcal{F}_\mathcal{A}(id_A) = id_{\mathcal{F}_\mathcal{O}}(A) \end{aligned}$$

whenever $\alpha \circ \beta$ is defined.

We usually don't distinguish between the functor, and the functions on the sets of objects and arrows, simply representing each of them by a single symbol $\mathcal{F}$.

Example 4.10
Let **Grp** and **Lat** be the categories of groups and lattices defined earlier. Then we know that the function $\mathcal{F}_\mathcal{O}$ defined by $\mathcal{F}_\mathcal{O}(G) = \mathrm{Sub}(G)$ is a function from the objects of **Grp** to the objects of **Lat**. Corollary 3.10 tells us that if we have a group homomorphism $\alpha : G \to H$, then we have a corresponding lattice homomorphism $\overline{\alpha} : \mathrm{Sub}(G) \to \mathrm{Sub}(H)$. So we define $\mathcal{F}_\mathcal{A}(\alpha) = \overline{\alpha}$. This gives the first two of the four conditions that we need for $\mathcal{F}$ to be a functor.

It is easily verified that $\mathcal{F}_\mathcal{A}(\mathrm{id}_G) = \mathrm{id}_{\mathcal{F}_\mathcal{O}(G)}$, while it is a little more work to check the remaining composition condition. They do hold, however, so we have a functor between the categories.

This is not the only possible functor between these two categories, since we could also consider a functor which maps a group G to the lattice consisting of the power set $\mathcal{P}(G)$ with meet and join being intersection and union. ◇

Example 4.11

The maps $\mathcal{F}(G) = G$ and $\mathcal{F}(\alpha) = \alpha$ give a functor $\mathcal{F} : \mathbf{Grp} \to \mathbf{Set}$. $\diamond$

Functors such as the one in the last example are called ***forgetful functors*** because we are forgetting about all the extra structure that a group has and treating it just as a set, and regarding homomoprhisms simply as functions. Whenever we have a category whose objects and arrows are specializations of another categories objects and arrows we get a forgetful functor which strips this additional structure away.

Example 4.12

There is a forgetful functor $\mathcal{F} : \mathbf{Abl} \to \mathbf{Grp}$, since Abelian groups are simply groups with an additional requirement of commutativity, and homomorphisms between Abelian groups are still homomoprhisms. $\diamond$

When looking at the question of whether or not two objects within a category are isomorphic or not, functors can help us say that that the two objects are not isomorphic.

Proposition 4.19

Let $\mathcal{C}$ be a category, and let A and B be two objects in $\mathcal{C}$. If there is another category $\mathcal{D}$ and a functor $\mathcal{F} : \mathcal{C} \to \mathcal{D}$ such that $\mathcal{F}(A)$ and $\mathcal{F}(B)$ are not isomorphic in $\mathcal{D}$, then A and B are not isomorphic in $\mathcal{C}$.

Proof:

If A and B are isomorphic, then we have an invertible arrow $\alpha : A \to B$ and its inverse $\alpha^{-1} : B \to A$. If $\mathcal{F} : \mathcal{C} \to \mathcal{D}$ is any functor, then

$$\mathcal{F}(\alpha) \circ \mathcal{F}(\alpha^{-1}) = \mathcal{F}(\alpha \circ \alpha^{-1}) = \mathcal{F}(\mathrm{id}_B) = \mathrm{id}_{\mathcal{F}(B)}.$$

Similarly $\mathcal{F}(\alpha^{-1}) \circ \mathcal{F}(\alpha) = \mathrm{id}_{\mathcal{F}(A)}$, and so $\mathcal{F}(\alpha) : \mathcal{F}(A) \to \mathcal{F}(B)$ has an inverse arrow $\mathcal{F}(\alpha^{-1})$, and hence $\mathcal{F}(A)$ is isomorphic to $\mathcal{F}(B)$.

Hence if $\mathcal{F}(A)$ is not isomorphic to $\mathcal{F}(B)$, then A and B are not isomorphic.
■

This very general result is at the core of many of the techniques we have for distinguishing groups which are not isomorphic. For example, the fact that two groups with different subgroup lattices are not isomorphic is an immediate corollary of this proposition, together with the functor of Example 4.10. The fact that two groups of different orders are not isomorphic is an immediate corollary of this proposition, using the forgetful functor from **Grp** to **Set**.

Unfortunately, this doesn't help us in showing when two groups are isomorphic, since there are many functors available, so checking every possible functor is impossible.

The category of groups is not the only category of interest in mathematics, of course, so it is useful to observe that in every category we find many naturally occurring groups:

Proposition 4.20
Let $\mathcal{C}$ be a category, and A an object in $\mathcal{C}$. Then the triple $(\mathrm{Aut}(A), \circ, id_A)$, *where* $\mathrm{Aut}(A)$ *is the set of invertible arrows from A to A, is a group. We call this the* ***automorphism group*** *of A.*

Proof:
From the definition of a category, when $\circ$ is restricted to $\mathrm{Aut}(A)$, it is an associative binary operation, and id_A is an identity. So the only thing that needs to be checked is that there is an inverse for every element, but this is guaranteed by the assumption that our arrows are all invertible. ■

Example 4.13
In the category Grp, $\mathrm{Aut}(G)$ is precisely the automorphism group of G, as discussed earlier. ◇

Example 4.14
In the category of finite dimensional real vector spaces and linear transformations, we have that $\mathrm{Aut}(V)$ is the set of all invertible linear transformations from V to V. If V has dimension n, then this group is isomorphic to $GL_n(\mathbb{R})$. ◇

Example 4.15
In the category Set, the group $\mathrm{Aut}(X)$ consists of all bijections of X onto itself, or in other words, the group of all permutations of X. If $|X| = n$, then $\mathrm{Aut}(X) \cong S_n$. ◇

Example 4.16
One can consider a category whose objects are all subsets of $\mathbb{R}^n$, and whose arrows are isometries which map one subset onto another.

In this category, the automorphism group of an object is the set of all symmetries of the object. ◇

As the above examples illustrate, the concept of an automorphism group generalises the concept of symmetries that we first introduced in Chapter 1. Whenever you see a new type of mathematical object being introduced, there is usually a category associated with it, and hence there is some sort of automorphism group associated with each object. Given the wide variety of categories that are of interest in mathematics, this underlines the importance of group theory.

Proposition 4.21
Let $\mathcal{C}$ be a category, and A and B two objects in $\mathcal{C}$. If A and B are isomorphic, then $\mathrm{Aut}(A)$ *and* $\mathrm{Aut}(B)$ *are isomorphic.*

Proof:

Let $\alpha : A \to B$ be an invertible arrow. Then we define a function $\overline{\alpha} : \mathrm{Aut}(A) \to \mathrm{Aut}(B)$ by

$$\overline{\alpha}(\beta) = \alpha \circ \beta \circ \alpha^{-1}.$$

One can easily verify that $\overline{\alpha}(\beta)$ is an invertible arrow, and hence the function is indeed into $\mathrm{Aut}(B)$, and furthermore

$$\overline{\alpha}(\beta) \circ \overline{\alpha}(\gamma) = \alpha \circ \beta \circ \alpha^{-1} \circ \alpha \circ \gamma \circ \alpha^{-1} = \alpha \circ \beta \circ \gamma \circ \alpha^{-1} = \overline{\alpha}(\beta \circ \gamma),$$

so $\overline{\alpha}$ is a homomorphism. Similarly, $\overline{\alpha^{-1}} : \mathrm{Aut}(B) \to \mathrm{Aut}(A)$ is a homomorphism, and furthermore $\overline{\alpha} \circ \overline{\alpha^{-1}} = \mathrm{id}_{\mathrm{Aut}(B)}$ and $\overline{\alpha^{-1}} \circ \overline{\alpha} = \mathrm{id}_{\mathrm{Aut}(A)}$, so $\overline{\alpha}$ is an isomorphism. ■

This means that in any time you have a category, you can use the automoprhism groups to distinguish non-isomoprhic objects in the category via the contrapositive of this result: if the automorphism groups are not isomorphic, the objects are not isomorphic.

Definition 4.5
*If $\mathcal{C}$ is a category, and A is an object in $\mathcal{C}$, then an **action** of a group G on A is a homomorphism $\alpha : G \to \mathrm{Aut}(A)$.*

For most categories of interest the objects of the category are sets with additional structure and the arrows are functions with additional conditions that they must satisfy. This means that $\alpha(g)$ is a function of some sort from A to A. To avoid confusion, it is common to write $\alpha(g) = \alpha_g$, so that we can use the less confusing notation $\alpha_g(x)$ instead of $(\alpha(g))(x)$ to represent the image of an element of A under this automorphism. In this case we have that $\alpha_{gh} = \alpha_g \circ \alpha_h$.

Example 4.17
Given a group G, the map $\alpha : G \to \mathrm{Aut}(G)$ defined by $\alpha(g) = \alpha_g$, where $\alpha_g(x) = g^{-1}xg$ is an action of G on itself. The image of the homomorphism is $\mathrm{Inn}(G)$, and the kernel is $Z(G)$. ◇

Example 4.18
Given a group G then for each $g \in G$ we have bijective functions $\lambda_g(x) = g^{-1}x$ and $\rho_g(x) = xg$. Since $\lambda_{gh} = \lambda_g \circ \lambda_h$, and $\rho_{gh} = \rho_g \circ \rho_h$, the functions $\lambda : g \mapsto \lambda_g$ and $\rho : g \mapsto \rho_g$ are actions of G on itself, when we consider it as an object in the category Set. We call these the ***left*** and ***right actions*** of G on itself, respectively. ◇

In a category in which the objects are sets with additional structure, and the arrows are functions which satisfy some additional conditions, we define the ***orbit*** of an element x under an action of a group G to be the set

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

We can define an equivalence relation using an action by $x \sim y$ if and only if $y = \alpha_g(x)$ for some $g \in G$. It is easy to verify that this is indeed an equivalence relation, since the facts that $x = \alpha_e(x)$; that if $x = \alpha_g(y)$ then $y = \alpha_{g^{-1}}(x)$; and that if $x = \alpha_g(y)$ and $y = \alpha_g(z)$, then

$$x = \alpha_g(y) = \alpha_g(\alpha_h(z)) = \alpha_{gh}(z)$$

give reflexivity, symmetry and transitivity, respectively. We then have that the orbit of x is simply the equivalence class of x, ie.

$$O(x) = [x]_\sim.$$

Example 4.19

The orbit of an element $x \in G$ under the action of Example 4.17 is the conjugacy class of x, ie. $O(x) = C(x)$. ◇

Example 4.20

The orbit of an element $x \in G$ under the left action of G is G.

However if we restrict the left action to some subgroup H of G, so we only consider functions of the form λ_h for $h \in H$, then λ is an action of H on G, and then $O(x)$ is the right coset Hx. ◇

Example 4.21

In the category of Example 4.16, consider closed disc of radius 1 with centre at the origin as the object A. The automorphism group of this object consists of rotations R_θ and reflections H_ψ of the disc, as discussed in Example 1.3. There is an action of the additive group of real numbers $\alpha : \mathbb{R} \to \mathrm{Aut}(A)$ given by $\alpha_x = R_y$, where $x = 2\pi k + y$, with $k \in \mathbb{Z}$ and $y \in [0, 2\pi)$.

In this case the orbit of the point $(1, 0)$ is the unit circle, since we can find a rotation that maps that point to any other on the unit circle, and every rotation is in the image of the action.

Indeed, the orbit of any point in the disc will be a circle. ◇

The previous example should help you understand why an orbit is called an orbit.

4.4 Semidirect Products

Group automorphisms and the actions of groups allow us to generalise the notion of the direct product introduced in Chapter 2. Let G and H be groups, and let α be an action of H on G. We supply a binary operation $*$ for the set

$$G \times H = \{(g, h) : g \in G, h \in H\}$$

by

$$(g_1, h_1) * (g_2, h_2) = (\alpha_{h_2}(g_1)g_2, h_1h_2).$$

Proposition 4.22
Let G and H be groups, and let α be an action of H on G. The binary operation $*$ defined above makes $(G \times H, *, (e, e))$ a group. We call this group a ***semidirect product*** *of G and H, and denote it symbolically by $G \rtimes_\alpha H$. If H is a subgroup of $\mathrm{Aut}(G)$ acting in the obvious way, then we call this group the* ***extension*** *of G by H.*

Moreover

(i) the subset $G' = \{(g, e) : g \in G\}$ is a characteristic subgroup of the semidirect product which is isomorphic to G;

(ii) $(G \rtimes_\alpha H)/G' \cong H$;

(iii) the subset $H' = \{(e, h) : h \in H\}$ is a subgroup of the semidirect product which is isomorphic to H;

(iv) the conjugate of an element (g, e) of G' by an element (e, h) of H' is the element $(\alpha_h(g), e)$ of G'. In other words, conjugation by elements of H' is equivalent to the action α on G.

Proof:

Showing that the semidirect product is a group is left as an easy exercise. It is also left as an exercise to show that $G' \cong G$ and $H' \cong H$.

We note that the inverse of the element (g, h) is the element $(\alpha_{h^{-1}}(g^{-1}), h^{-1})$.

The function $\beta(g, h) = h$ from $G \rtimes_\alpha H$ to H is a homomorphism, since

$$\begin{aligned} \beta((g_1, h_1) * (g_2, h_2)) &= \beta(\alpha_{h_2}(g_1)g_2, h_1h_2) \\ &= h_1h_2 \\ &= \beta(g_1, h_1)\beta(g_2, h_2)). \end{aligned}$$

Now

$$\ker \beta = \{(g, h) : \beta(g, h) = h = e\} = \{(g, e) : g \in G\} = G',$$

so G' is a normal subgroup, and furthermore the First Isomorphism Theorem says that since β is onto,

$$H \cong (G \rtimes_\alpha H)/\ker \beta = (G \rtimes_\alpha H)/G'$$

Finally, by calculation,

$$\begin{aligned} (e, h)^{-1} * (g, e) * (e, h) &= (e, h^{-1}) * (g, e) * (e, h) \\ &= (\alpha_e(e)g, h^{-1}e) * (e, h) \\ &= (g, h^{-1}) * (e, h) \\ &= (\alpha_h(g)e, h^{-1}h) \\ &= (\alpha_h(g), e). \end{aligned}$$

■

Example 4.22

For any G and H, there is always the trivial action $\alpha_h(g) = g$. Under this action, the semidirect product $G \rtimes_\alpha H$ has product

$$(g_1, h_1) * (g_2, h_2) = (\alpha_{h_2}(g_1)g_2, h_1h_2) = (g_1g_2, h_1h_2).$$

In other words, this is simply the direct product of the two groups. $\diamond$

Example 4.23

If G is any Abelian group, there is an action of the multiplicative group $\{1, -1\} \cong C_2$ given by $\alpha_1(g) = g$ and $\alpha_{-1}(g) = g^{-1}$. It is trivial that α_1 is a homomorphism, and $\alpha_{-1}(gh) = (gh)^{-1} = h^{-1}g^{-1} = g^{-1}h^{-1} = \alpha_{-1}(g)\alpha_{-1}(h)$, since G is Abelian.

The semidirect product of G and this group with this action is a group of order $2|G|$, and if G has any element of order greater than 2, this is distinct from the direct product. Indeed, if it is distinct from the direct product, the semidirect product is not Abelian, since if g_1 is an element of order greater than 2, we have

$$(g_1, 1) * (e, -1) = (g_1^{-1}, -1),$$

but

$$(e, -1) * (g_1, 1) = (g_1, -1),$$

and these are only equal if $g_1^{-1} = g_1$, which implies that g_1 has order 2. So these elements do not commute.

One can show that as a particular example of this action giving a semidirect product, we have $D_{2n} \cong C_n \rtimes_\alpha C_2$, where the generators a and b of D_{2n} correspond to the elements $(u, 1)$ and $(1, -1)$, respectively. $\diamond$

Assignment 5

The following exercises are due on day of final.

4.1 Exercises 1, 2, 4, 5, 7.

4.2 Exercises 1, 4, 5, 8, 9.

Index