The Basics of Abstract Algebra

John Bamberg and Alice C. Niemeyer

Contents

CHAPTER 1

Introduction

The purpose of this handout is to summarise some basic concepts used in Algebra. A more detailed account can be found in Fraleigh's book [1]. For each of the algebra units taught in third year, we have listed some recommended books and suggestions for reading this text.

3P5

Recommended Reading:

- *A course in group theory* , J. F. Humphreys
- *An introduction to abstract algebra*, T. Whitelaw
- *Modern algebra*, J. R. Durbin
- *Groups*, C. R. Jordan and D. A. Jordan
- *Rings, fields, and groups*, R. B. J. T. Allenby
- *Introduction to abstract algebra*, Elbert A. Walker
- *Abstract algebra; a first undergraduate course*, A. P. Hillman and G. C. Alexanderson.

All parts of this handbook, except possibly Section 3 would be recommended if you are a student in 3P5.

3P7

Recommended Reading:

- *Introduction to Modern Algebra*, N. H. McCoy and G.J. Janusz
- *Topics in Algebra*, I.N. Herstein
- *Contemporary Abstract Algebra*, J.A. Gallian
- *Elementary Number Theory and its Applications*, K.H. Rosen
- *An Introduction to the Theory of Numbers*, I. Niven, H.S. Zuckerman and H.L. Montgomery,
- *A Classical Introduction to Modern Number Theory*, K. Ireland and M. Rosen

Reading the following parts of this handbook is recommended if you are a student in 3P7:

- Chapter 2, except Section 5
- Chapter 4, skip anything about Permutations.

3CC

Recommended Reading:

- *Public-key cryptography*, Arto Salomaa
- *Cipher systems : the protection of communications,London : Northwood Books*, Henry Beker and Fred Piper
- *The code book*, Simon Singh
- *An introduction to error correcting codes with applications*, Scott A. Vanstone and Paul C. van Oorschot
- *Introduction to the theory of error-correcting codes*, Vera Pless,
- *Coding and information theory*, S. Roman

The following parts of this handbook would be recommended if you are a student in 3CC:

- Chapter 2,
- Chapter 3,
- Sections 1-4,
- Section 6, and
- Section 8.

[1] John B. Fraleigh, *A first course in abstract algebra*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., fifth edition, 1994.

CHAPTER 2

Relations, Functions, and Permutations

An important idea in mathematics is that of a *set* of objects. From the theory of sets, we can establish the notions of a *binary relation* and a *function*.

1. Binary Relations

Intuitively, a binary relation is some rule on two objects. For example, "$10 < 20$", "Collingwood is better than Carlton", and "Pacino and de Niro have been in the same movie". On the integers, things like "less than", "is a factor of", or "not equal to" are examples of binary relations. We abstract this notion as follows:

DEFINITION 1.1. A *binary relation* from a set X to a set Y is a subset of the set of ordered pairs

$$\{(x, y) : x \in X, y \in Y\}.$$

By *ordered pair* we mean that (x, y) is not necessarily equal to (y, x), that is, it matters that x is in the first coordinate and y is in the second coordinate. The set of *all* ordered pairs is known as the *Cartesian*[1] product of X and Y. We denote this set by $X \times Y := \{(x, y) : x \in X, y \in Y\}$.

Example 1.2.

- If $X = Y$, we call a binary relation from X to Y also a binary relation on X.
- Equality is a binary relation on any set. If X is a set, then $R_=$ on X is precisely the subset of $X \times X$ given by $\{(x, x) : x \in X\}$. So two elements $x, y \in X$ are equal if $(x, y) \in R_=$. This looks a bit strange doesn't it? You might be asking, don't you mean $x = y$? See below for the answer.
- "Less than" is a binary relation on the real numbers. So $(1, 2) \in R_<$ and $(\pi, 4) \in R_<$. Again, this looks very strange if you are familiar with infix notation.
- The "blood type" binary relation BT is defined on the sets of human beings and blood types. So if Fred has $A+$ blood, then $(Fred, A+) \in BT$.
- The "grand-father" binary relation GF is defined on the set of human beings. So if Bill is Fred's grandfather, then $(Fred, Bill) \in GF$.

.....

Instead of writing $(x, y) \in R$ all the time, we will often write $x\,R\,y$ to mean $(x, y) \in R$. So in the first example above, $(x, y) \in R_=$ is the same as $x = y$.

EXERCISES 1.3. Which of the following are binary relations?

(1) Football team x is better than football team y.
(2) Politicians are stupid.
(3) Town x is a suburb of Perth.
(4) The integer x is a divisor of the integer y.
(5) Person x is wearing the same hat as person y.

---

[1] 

The *Cartesian Product* was named after Renè Descartes (1596-1650), the famous French philosopher and mathematician.

2. Functions

In high school, the first functions we saw were something like $f(x) = x^2$ or $f(x) = 3x+1$, but yet a function was never defined. What is a function? One can think of a function as a machine which takes an input and spits out an output. Another way to think of a function, is that it is a binary relation on the input and output of this machine. So for example, if we take the above example $f(x) = x^2$ on the real numbers, we say that 2 and 4 are related since $f(2) = 4$. So a function is a relation, but is it special in anyway? Note that $f(2)$ is always equal to 4, but the same can't be said of $<$, where $2 < 4$ but $2 < 5$ as well! We have the following abstract definition of a function:

DEFINITION 2.1. A *function* f from X to Y is a binary relation from X to Y where for each (a, b) and (a, c) in f, if $(a, b) = (a, c)$ then $b = c$. In other words, for anything in the first coordinate of an ordered pair of f, there is a *unique* entry in the second coordinate.

Example 2.2.

(1) The squaring function $f(x) = x^2$ on the real numbers, can be thought of as the set of pairs (x, x^2) (like $(2, 4)$, $(5, 25)$, $(-1, 1)$, $(\sqrt{6}, 6)$, etc).
(2) Equality is a function. In fact, we usually call it the *identity* function. So if X is a set, the function defined by $f(x) = x$ (for all $x \in X$) is actually the equality relation!
(3) Notice that $R_<$ is not a function since $(2, 4) \in R_<$ and $(2, 5) \in R_<$.
(4) The "grandfather" relation is also not a function since it is possible to have two different grandfathers!
(5) The "blood-type" relation is a function, since everyone has a unique blood type.

. . . . . .

DEFINITION 2.3 (One-to-One).
A function $f : X \to Y$ is *one-to-one* if for each element of $y \in Y$, there is at most one element $x \in X$ such that $f(x) = y$.

Example 2.4.

- The function f defined by $f(x) = x^2$ is not one-to-one since $f(-1) = f(1)$ but $1 \neq -1$.
- The identity function on a set X is one-to-one since for all $y \in X$, there is just one element, namely itself, that is mapped to y by the identity function.
- The "blood type" function is not one-to-one, since one of the author's blood type is the same as his mother's!
- Pictorially, a function f on the reals is one-to-one if every horizontal line drawn on the graph of f intersects the values of f at most once. You should picture "$f(x) = x^2$" and imagine drawing horizontal lines on the graph.

. . . . . .

To prove a function $f : X \to Y$ is one-to-one:
Suppose $f(x_1) = f(x_2)$ for some $x_1, x_2 \in X$. Show that $x_1 = x_2$.

Example 2.5. Show that the function $f : \{x \in \mathbb{R} : x > -1\} \to \mathbb{R}$ defined by $f(x) = \sqrt{x+1}$ for all real numbers $x > -1$, is one-to-one.

PROOF. Let x_1, x_2 be real numbers greater than -1, and suppose $f(x_1) = f(x_2)$. Then $\sqrt{x_1+1} = \sqrt{x_2+1}$ and hence squaring gives $x_1 + 1 = x_2 + 1$. So $x_1 = x_2$ and hence f is one-to-one. □

. . . . . .

DEFINITION 2.6 (Onto).
A function $f : X \to Y$ is *onto*, if for each element $y \in Y$, there is at least one element $x \in X$ such that $f(x) = y$.

Example 2.7.

- The function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$ (for all $x \in \mathbb{R}$) is not onto since no element maps to -1 under f. If however we restricted the definition of f by defining $f : \mathbb{R} \to \mathbb{R}^+ \cup \{0\}$, then it would be onto.
- The "blood-type" function is onto, since for every blood type, there is at least one person in the world who has that blood type.

.....

To prove a function $f : X \to Y$ is onto:
Let y be any element of Y. Find an element $x \in X$ such that $f(x) = y$.

Example 2.8. Show that the function $f : \{x \in \mathbb{R} : x > -1\} \to [1, \infty)$ defined by $f(x) = \sqrt{x+1}$ for all real numbers $x > -1$, is onto.

PROOF. Let $y \in [1, \infty)$. We must find a real number x greater than -1 such that $f(x) = y$. Choose $x = y^2 - 1$. First note that $y \geq 1$, which implies that $y^2 - 1 \geq 0$ and hence x is certainly greater than -1. So $f(x) = \sqrt{x+1} = \sqrt{y^2 - 1 + 1} = |y| = y$ and hence f is onto. □

.....

Counting is one of the most central ideas of mathematics, and it wasn't until Cantor's[2] work in the 19th century that we began to understand fully what it means to count. To say that one set has more elements then another is a trivial problem in the finite context, but what about infinite sets? Are there more integers than even numbers? What Cantor realised, is that counting can be thought of pairing elements in a unique and exhaustive way. For example, we can pair up the integers and even numbers in the following way:

$$\ldots, (-6, -3), (-4, -2), (-2, -1), (0, 0), (2, 1), (4, 2), (6, 3), \ldots.$$

You can see here that every even number will appear in the first coordinate in precisely one of these pairs and every integer will appear in the second coordinate in just one of these pairs. So what we require is that there is a function from the even numbers to the integers that is one-to-one and onto. We call this a *bijection*.

DEFINITION 2.9 (Bijection). A function is *bijective* if it is both one-to-one and onto.

Example 2.10.

(1) The function f from the even numbers to the integers defined by $f(x) = x/2$ is a bijection. So essentially, we think of the integers and even numbers as having the *same* amount of elements.
(2) There is no bijection from the integers to the real numbers. We will not prove this here, but will remark that according to Cantor's theory of cardinality, the real numbers are infinite in a different way to the integers.

.....

To prove two functions $f : X \to Y$ and $g : X \to Y$ are equal:
Let $x \in X$. Show that $f(x) = g(x)$. A common mistake by students is that they prove that two functions are equal for a specific element of X. You must prove that they compute the same value for EVERY element of the domain!

---

[2] 

Georg Cantor (1845-1918) was born in Russia, but lived most of his life in Germany. He is best known as one of the founders of modern analysis and number theory.

EXERCISES 2.11.

(1) Which of the following relations are functions?
   (a) $\{(x, y) \in \mathbb{R} \times \mathbb{R} : y = \cos(x)\}$,
   (b) $\{(x, y) \in \mathbb{Z} \times \mathbb{Z} : y \neq 0\}$,
   (c) $\{(x, y) \in \mathbb{Z} \times \mathbb{Z} : y = 0\}$,
   (d) The relation $R : \mathbb{Q} \times \mathbb{Z} \to \mathbb{Z}$ defined by qRa where a is the numerator of q.
(2) Prove or disprove that the following functions are one-to-one or onto:
   (a) $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^3$ for all $x \in \mathbb{R}$,
   (b) $f : [-1, 1] \to \mathbb{R}$, $f(x) = \sin(x\pi/2)$ for all $x \in [-1, 1]$,
   (c) $f : \mathbb{R}\backslash\{0\} \to \mathbb{R}$, $f(x) = x^2 - 1/x$ for all $x \in \mathbb{R}\backslash\{0\}$,
   (d) $f : \mathbb{R}^+ \to \mathbb{R}^+ \cup \{0\}$, $f(x) = x - \log(x)$ for all $x \in \mathbb{R}^+$.

3. Composition of functions

In algebra, we often want to create new things from old things. In this section, we look at a way of creating a function from two old ones. This operation is called *function composition*.

DEFINITION 3.1 (Function Composition). Let g be a function from a set A to a set B and let f be a function from a set B to a set C. Then the *composition* of f and g, denoted $f \circ g$ is the function defined by $(f \circ g)(a) = f(g(a))$ for all $a \in A$.

Example 3.2.

- The function h defined by $h(x) = \sin^2(x)$ (for all $x \in \mathbb{R}$) is the composition of the two functions f and g defined by $f(x) = x^2$ and $g(x) = \sin(x)$. So $h = f \circ g$. Note that $g \circ f$ is a completely different function which maps an element $x \in \mathbb{R}$ to $\sin(x^2)$.
- Let X and Y be sets and let $f : X \to Y$ be a function. Then $f \circ \mathrm{id}_X = f$ and $\mathrm{id}_Y \circ f = f$ where id_X and id_Y are the identity functions on X and Y, respectively.
- Let $\mathbb{R}^+$ denote the positive real numbers, and let $f : \mathbb{R}^+ \to \mathbb{R}^+$ be defined by $f(x) = x^2$ (for all $x \in \mathbb{R}^+$). Let $g : \mathbb{R}^+ \to \mathbb{R}^+$ be defined by $g(y) = \sqrt{y}$ (for all $y \in \mathbb{R}^+$). Then $f \circ g = \mathrm{id}_{\mathbb{R}^+}$ and $g \circ f = \mathrm{id}_{\mathbb{R}^+}$.

EXERCISES 3.3.

(1) Let $f : \mathbb{R} \to \mathbb{R}$ and $g : \mathbb{R}^+ \to \mathbb{R}$ be defined by $f(x) = x(x - 1)$ and $g(y) = \log(y^2)$ for all $x \in \mathbb{R}$ and $y \in \mathbb{R}^+$. What is $f \circ g$? Is it O.K to write $g \circ f$?
(2) Show that the composition of two one-to-one functions is one-to-one.

4. Image, preimage, and inverses

Modern mathematics and its language have evolved into a reasonably stable and uniform state. The words "one-to-one", "onto", and "real number" are universally understood. We present here some more notions that are fundamental to the communication of mathematics.

DEFINITION 4.1 (Image and Preimage).
Let ϕ be a function from a set X into a set Y, and let $A \subseteq X$ and $B \subseteq Y$.

- The *image* $\phi(A)$ of A under ϕ is the subset $\{\phi(a) : a \in A\}$ of Y.
- The *preimage* $\phi^{\leftarrow}(B)$ of B under ϕ is the subset $\{a \in X : \phi(a) \in B\}$.

Example 4.2.

- Warning! The object $\phi^{\leftarrow}$ may not be a function!
- Consider the sine function $\sin : \mathbb{R} \to \mathbb{R}$. The image of $\mathbb{R}$ under this function is $\sin(\mathbb{R}) = [-1, 1]$. The preimage of $\{0\}$ under sine is the set

$$\sin^{\leftarrow}(\{0\}) = \{x \in \mathbb{R} : \sin(x) = 0\} = \{\pi x : x \in \mathbb{Z}\}.$$

EXERCISES 4.3. Let A and B be sets, let $f : A \to B$ be a function, let $U, V \subseteq A$, and let $X, Y \subseteq B$. Prove the following:

(1) $U \subseteq V \implies f(U) \subseteq f(V)$
(2) $X \subseteq Y \implies f^{\leftarrow}(X) \subseteq f^{\leftarrow}(Y)$
(3) $U \subseteq f^{\leftarrow}(f(U))$
(4) if f is one-to-one, then $U = f^{\leftarrow}(f(U))$
(5) $f(f^{\leftarrow}(X)) \subseteq X$
(6) if f is onto, then $f(f^{\leftarrow}(X)) = X$

DEFINITION 4.4 (Invertibility).
A function $f : X \to Y$ is said to be *invertible* if there exists a function $g : Y \to X$ such that $f \circ g = \mathrm{id}_Y$ and $g \circ f = \mathrm{id}_X$. If such a g exists, we call it the *inverse* of f, and denote it by f^{-1}.

Example 4.5.

- The squaring function from $\mathbb{R}$ to $\mathbb{R}$ is not invertible. However the squaring function on $\mathbb{R}^+$ is invertible!
- The inverse of the identity function is itself, since for any set X, $\mathrm{id}_X \circ \mathrm{id}_X = \mathrm{id}_X$.

. . . . . .

THEOREM 4.6. *A function $f : X \to Y$ is invertible if and only if it is bijective.*

PROOF. We have to prove both directions. Suppose first that f is invertible. Then by definition, there exists a function $g : Y \to X$ such that $f \circ g = \mathrm{id}_Y$ and $g \circ f = \mathrm{id}_X$. We must show that f is one-to-one and onto. Suppose $f(x_1) = f(x_2)$ for some $x_1, x_2 \in X$. Then

$$x_1 = \mathrm{id}_X(x_1) = (g \circ f)(x_1) = g(f(x_1)) = g(f(x_2)) = (g \circ f)(x_2) = \mathrm{id}_X(x_2) = x_2$$

and hence f is one-to-one. It remains to show that f is onto. Let $y \in Y$. We must find an element $x \in X$ such that $f(x) = y$. Choose $x = g(y)$. Then

$$f(x) = f(g(y)) = (f \circ g)(y) = \mathrm{id}_Y(y) = y$$

and hence f is onto. Therefore f is bijective.

Now we prove the converse. Suppose f is bijective, that is, f is one-to-one and onto. Then for every element $y \in Y$, there exists $x \in X$ such that $y = f(x)$. Moreover, x is unique, since if there was another element x' such that $y = f(x')$, then $f(x) = f(x')$ and hence $x = x'$ as f is one-to-one. So we can define a function $g : Y \to X$ where for each $y \in Y$, $g(y)$ is the unique element of X such that $y = f(x)$. We will prove now that g is the inverse of f. For all $x \in X$, $(g \circ f)(x) = g(f(x)) = x = \mathrm{id}_X(x)$ and hence $g \circ f = \mathrm{id}_X$. Similarly, for all $y \in Y$, $(f \circ g)(y) = f(g(y)) = y = \mathrm{id}_Y(y)$ and hence $f \circ g = \mathrm{id}_Y$. Therefore f is invertible. □

EXERCISES 4.7. Which of the following functions are invertible?

(1) The "Blood Type" function.
(2) Equality.
(3) $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^4$ for all $x \in \mathbb{R}$.
(4) $f : \mathbb{R}^+ \to \mathbb{R}$, $f(x) = x^4$ for all $x \in \mathbb{R}$.
(5) $f : \mathbb{R}^+ \to \mathbb{R}^+$, $f(x) = x^4$ for all $x \in \mathbb{R}$.

5. Permutations

We can think of a *rearrangement* of a set as just being a bijection from the set to itself. Formally, we call this a *permutation*.

DEFINITION 5.1 (Permutation). A *permutation* on a set X is a bijection from X onto X.

We denote the set of all permutations of a set X by $\mathrm{Sym}(X)$. If $X = \{1, \ldots, n\}$, then we write $\mathrm{Sym}(X) = S_n$. Consider S_4 the set of permutations of $\{1, 2, 3, 4\}$. Then we can write down specifically what each permutation does. For example, the map which takes 1 to 4, 2 to 1, 3 to 2, and 4 to 3, is indeed a permutation of $\{1, 2, 3, 4\}$, and we can write it as:

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

The top line represents the domain elements and the bottom line represents the image of the elements. This is called *double-bar* notation. But this notation can be a bit cumbersome, so we have the following way of writing this permutation:

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

This means, "1 goes to 4", "4 goes to 3", "3 goes to 2", and "2 goes to 1". Similarly, the permutation given by $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$ can be written as

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

So within each pair of parentheses, a number is sent to the number on its right in a cyclic way. So $(1\,4)$ sends 4 to 1 and 1 to 4. The permutation $(1\,2\,3\,4)$ sends 1 to 2, 2 to 3, and so on. This is called *cycle notation*.

Example 5.2. Here are some equivalent ways of writing some permutations in S_6:

- $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 1 \end{pmatrix} \leftrightarrow (1\,2\,3\,4\,3\,6)$,
- $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 4 & 2 & 5 & 6 \end{pmatrix} \leftrightarrow (1)(2\,3\,4)(5)(6)$,
- $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} \leftrightarrow (1)(2)(3)(4)(5)(6)$.

Generally, parentheses with just one number in them will be disregarded and we write the second permutation as $(2\,3\,4)$ and the identity permutation (in the third example) as $()$.

. . . . . .

A permutation is called a *cycle* if when written in cycle notation we get only one parenthesis with more than one number in it. The permutation $(1\,3\,6)$ is a cycle, but $(1\,2)(3\,4)$ is not. So not every permutation is a cycle, but we can write permutations as products of cycles. For example, the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 6 & 7 & 4 & 1 & 5 & 2 \end{pmatrix} \in S_8$$

can be written as

$$(1\,3\,6)(2\,8)(4\,7\,5).$$

To compute elements with this permutation, we apply the permutation to the right of the variable. For example, if $\sigma = (1\,2\,3)(2\,4)(3\,5) \in S_5$, then $(1)\sigma = 2$, $(2)\sigma = 3$, and so on.

> WARNING! As a function, when we compute the values of a permutation, we are actually applying it to the *right* of a variable, rather than the left.

DEFINITION 5.3 (Disjoint Cycles). Two cycles in S_n are *disjoint* if they do not move a common point.

The cycles $(1\,2\,3)$ and $(1\,4\,5)$ are not disjoint since they have a 1 in common.

THEOREM 5.4. *Every permutation of a finite set is a product of disjoint cycles.*

PROOF. Let $X = \{1, 2, \ldots, n\}$ and let σ be a permutation of X. For each $i \in X$, let $\Delta_i = \{(i)\sigma^r : r \in \mathbb{Z}\}$. This is the set of all iterated images of i under σ. Now for all $i \in X$, define $\mu_i : X \to X$ by

$$(x)\mu_i = \begin{cases} (x)\sigma & \text{if } x \in \Delta_i \\ x & \text{otherwise} \end{cases}.$$

Note that μ_i is a permutation of X for all $i \in X$ and that $\sigma = \mu_1 \circ \mu_2 \circ \cdots \circ \mu_n$. Now some of the μ_i will be equal, so it suffices to show that Δ_i and Δ_j are either equal or disjoint. We leave this as an exercise. □

DEFINITION 5.5 (Transposition). A *transposition* is a cycle of length 2.

Notice that $(1\,2\,3\,4\,5\,6) = (1\,2)(1\,3)(1\,4)(1\,5)(1\,6)$. So we have the following important observation.

THEOREM 5.6. *Every permutation of a finite set with more than one element, is a product of transpositions.*

EXERCISES 5.7.

(1) (a) Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{pmatrix}$ and let $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix}$. Calculate $\sigma \circ \tau$.
(b) So what is $(1)\sigma \circ \tau$ equal to?

(2) (a) How many possible permutations are there of n elements?
(b) Consider the following permutations on $\{1, 2, 3\}$:

$$r_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

Calculate $r_2 := r_1^2$, $r_0 := r_1^3$, $f_2 := r_1 \circ f_1$, and $f_3 := f_1 \circ r_1$.

(3) Which of the following functions are elements of $\mathrm{Sym}(\mathbb{R})$:
(a) $f_1 : \mathbb{R} \to \mathbb{R}$ defined by $f_1(x) = x + 1$
(b) $f_2 : \mathbb{R} \to \mathbb{R}$ defined by $f_2(x) = x^2$
(c) $f_3 : \mathbb{R} \to \mathbb{R}$ defined by $f_3(x) = -x^3$
(d) $f_4 : \mathbb{R} \to \mathbb{R}$ defined by $f_4(x) = e^x$
(e) $f_5 : \mathbb{R} \to \mathbb{R}$ defined by $f_5(x) = x^3 - x^2 - 2x$

6. Binary Operations

As children, one of the first mathematical ideas we learnt was how to count and how to add or multiply numbers. Addition and multiplication are in fact functions. More generally, matrix multiplication, addition, cross products of vectors, composition of functions, and the greatest common divisor function all have at least one thing in common – they are binary operations.

DEFINITION 6.1 (Binary Operation).
A *binary operation* $*$ on a set X is a function from $X \times X$ to X.

Example 6.2.

- "+" is a binary operation on $\mathbb{R}$.
- "−" is not a binary operation on $\mathbb{N}$.
- The "cross product" is a binary operation on $\mathbb{R}^3$,
- Matrix multiplication is a binary operation on the set of $n \times n$ matrices.
- The "dot product" is not a binary operation on $\mathbb{R}^3$.
- Function composition is a binary operation on $\mathrm{Sym}(X)$, for any set X.

. . . . . .

DEFINITION 6.3 (Commutative, Associative).
A binary operation $*$ on a set X is...

- *commutative* if $a * b = b * a$ for all $a, b \in X$.
- *associative* if $(a * b) * c = a * (b * c)$ for all $a, b, c \in X$.

Example 6.4.

- Matrix multiplication is associative but not commutative,
- Function composition is associative but not commutative.
- The cross product is neither commutative, nor associative, on $\mathbb{R}^3$,
- "−" is not commutative, nor associative on $\mathbb{R}$.

. . . . . .

EXERCISES 6.5. Of the following functions, state whether they are binary operations or not, and if so, are they commutative or associative?

(1) $\times$ on the integers.
(2) The function defined by $f(x, n) = x^n$ where $x, n \in \mathbb{Z}$.
(3) Function composition on the set of linear functions on $\mathbb{R}$.
(4) Function composition on the set of polynomials on $\mathbb{R}$.

7. Equivalence Relations

Recall from calculus that if $f : \mathbb{R} \to \mathbb{R}$ is a differentiable function, then the function $g : \mathbb{R} \to \mathbb{R}$ defined by $g(x) = f(x) + c$, where c is some constant in $\mathbb{R}$, has the same derivative as f. So the functions $x \mapsto f(x) + 1$, $x \mapsto f(x) - 50$, and $x \mapsto f(x) + \pi$ all have the same derivative. So if all we care about is the derivative of a function, then we might say that f and g are *equivalent*. Along with this concept of equivalence is that of a partition. For example, if we take the set of all differentiable functions on $\mathbb{R}$, we could lump altogether those functions which have the same derivative into separate compartments of the "differentiable functions on $\mathbb{R}$". So one part of the partition would contain the cosine function and all "translations" of it. In general, we define a partition as follows.

Definition 7.1 (Partition). Let A be a set. A collection $\mathcal{B}$ of subsets of A is called a *partition* of A provided

(1) every element of $\mathcal{B}$ is nonempty,
(2) for every element $x \in A$, there is a set $B \in \mathcal{B}$ such that $x \in B$ (union covers A),
(3) every pair of elements of $\mathcal{B}$ are either equal or disjoint.

The elements of the partition are sometimes called *cells* or *parts* of the partition.

Example 7.2. Let

$$A_0 = \{5z : z \in \mathbb{Z}\} = \{\ldots, -15, -10, -5, 0, 5, 10, 15, \ldots\},$$

and let

$$A_i = \{x + i : x \in A_0\}$$

for $i = 1, 2, 3, 4$. For example,

$$A_3 = \{\ldots, -12, -7, -2, 3, 8, 13, \ldots\}.$$

So A_0 is the set of multiples of 5, and the A_i are translates of A_0. Let $\mathcal{B} = \{A_0, A_1, A_2, A_3, A_4\}$. We claim that $\mathcal{B}$ is a partition of the integers.

(1) Every element of $\mathcal{B}$ is nonempty, since $0 \in A_0$ and $i \in A_i$ for all $i \in \{1, 2, 3, 4\}$.
(2) Every integer belongs to at least one of the elements $\mathcal{B}$. To see this, let z be an integer and let i be the remainder of z divided by 5. Then $z \in A_i$.
(3) Every pair of distinct elements in $\mathcal{B}$ are disjoint. This is clear from the definition of the A_i.

. . . . . .

As promised in the introduction to this section, we show that the idea of a partition is strongly connected to that of an equivalence relation.

Definition 7.3 (Equivalence Relation).
A relation $\sim$ on a set S satisfying the following axioms, is called an *equivalence relation*.

(1) (Reflexive) $(\forall x \in S)\, x \sim x$,
(2) (Symmetric) $(\forall x, y \in S)\, x \sim y \implies y \sim x$,
(3) (Transitive) $(\forall x, y, z \in S)\, x \sim y$ and $y \sim z \implies x \sim z$.

Definition 7.4 (Equivalence Class).
Let $\sim$ be an equivalence relation on a set S. Then for all $x \in S$, the set

$$[x] = \{y \in S : y \sim x\}$$

is called an *equivalence class* (with representative x).

Example 7.5. Let's check that "has the same derivative" is an equivalence relation on the set of differentiable functions.

(1) Reflexive: every function has the same derivative as its own derivative!
(2) Symmetric: if f has the same derivative as g, then g has the same derivative as f.
(3) Transitive: if f has the same derivative as g and g has the same derivative as h, then f has the same derivative as h.

The equivalence class of the identity function is the set of all functions which have "$g(x) = 1$" as their derivative. So any function of the form $f(x) = x + c$ for some constant c, is in the equivalence class of the identity function.

. . . . . .

Example 7.6.

- Equality is an equivalence relation.
- "$<$" is not an equivalence relation as it is not reflexive.
- "$\leq$" is not an equivalence relation as it is not symmetric (but it is reflexive and transitive!),
- "friendship" is an equivalence relation (at least it should be!), since everyone is a friend of themselves (reflexivity), if I'm a friend of you then you're a friend of me (symmetry), and a friend of a friend is a friend (transitivity). The equivalence class of me under the equivalence relation "friendship", is the set of all friends of mine!

. . . . . .

THEOREM 7.7. *The equivalence classes of an equivalence relation partition the set S. On the other hand, each partition of S determines an equivalence relation.*

PROOF.

($\Rightarrow$) We need to show each element is in exactly one equivalence class. Certainly $a \in S$ is in $[a]$. Suppose $a \in [b]$. Then $a \sim b$ and if $d \in [a]$ then $d \sim a$ and $a \sim b$ so $d \sim b$ and hence $[a] \subseteq [b]$. On the other hand $[b] \subseteq [a]$ by similar proof. So $[a] = [b]$.

($\Leftarrow$) Define a relation $\equiv$ on S by $a \equiv b$ if a and b lie in the same cell. Then $\equiv$ is an equivalence relation.

(1) reflexive: $a \equiv a$ as a lies in the same cell as a.
(2) symmetric: $a \equiv b$ then $b \equiv a$ if a lies in the same cell as b then b lies in the same cell as a.
(3) transitive: $a \equiv b$ and $b \equiv c$ then $a \equiv c$. a lies in the same cell as b and b lies in the same cell as c then a lies in the same cell as c.

□

Example 7.8. The rational numbers are just like a partition of $\mathbb{Z} \times \mathbb{Z}$. Let $K = \{(m, n) : m \in \mathbb{Z}, n \in \mathbb{Z} \backslash \{0\}\}$. Define $\sim$ to be the relation

$$(m_1, n_1) \sim (m_2, n_2) \iff m_1 n_2 = m_2 n_1$$

for all $(m_1, n_1), (m_2, n_2) \in K$. Is this an equivalence relation?

Reflexive: Let $(m, n) \in K$. Clearly, $mn = mn$ (since $=$ is reflexive) and hence $(m, n) \sim (m, n)$.

Symmetric: Suppose $(m_1, n_1) \sim (m_2, n_2)$ for some $(m_1, n_1), (m_2, n_2) \in K$. Then $m_1 n_2 = m_2 n_1$. Since $=$ is symmetric, $m_2 n_1 = m_1 n_2$ and hence $(m_2, n_2) \sim (m_1, n_1)$.

Transitive: Suppose $(m_1, n_1) \sim (m_2, n_2)$ and $(m_2, n_2) \sim (m_3, n_3)$ for some $(m_1, n_1), (m_2, n_2), (m_3, n_3) \in K$. Then $m_1 n_2 = m_2 n_1$ and $m_2 n_3 = m_3 n_2$. So $m_1 n_3 = \frac{m_1 n_2 n_3}{n_2}$ since n_2 is nonzero, and hence $m_1 n_3 = \frac{m_2 n_1 n_3}{n_2}$ (we used the fact that "$=$" is transitive here). So $m_1 n_3 = \frac{m_3 n_2 n_1}{n_2} = m_3 n_1$, and hence $(m_1, n_1) \sim (m_3, n_3)$.

Therefore $\sim$ is an equivalence relation on K. So

$$[(1, 2)] = \{\ldots, (-3, -6), (-2, -4), (-1, -2), (1, 2), (2, 4), (3, 6), \ldots\}.$$

This is what *one-half* means. It is an equivalence class!

. . . . . .

EXERCISES 7.9.

(1) (a) Show that the following relation is an equivalence relation on the set of integers:

$$x \, R \, y \iff x + y \text{ is an even number.}$$

(b) What is the equivalence class of 1 under this relation?
(c) What is the equivalence class of 2 under this relation?
(d) What is the partition of the integers induced by this relation?

(2) (a) Show that the following relation is an equivalence relation of the set of Australian politicians:

$$x \, R \, y \iff x \text{ and } y \text{ belong to the same political party}$$

(b) What is the equivalence class of John Howard?
(c) What is the partition of the set of politicians induced by this relation?

8. The Issue of "Well-Defined"

It is a common trait of mathematicians to "define" a function before actually proving that it is a function. Ideally, we should define a set, show it is a binary relation, and then show it is a function. As you can imagine, this can be quite a cumbersome task in most situations. So mathematicians have become accustomed to writing functions down before verifying that they are indeed functions. When we prove that a binary relation is a binary relation or a function is a function, we say that the object in question is "well-defined". Not until now have you needed to deal with this issue, but you will find, especially when defining functions with a partition as their domain, that you must take a minute to prove that what you've claimed is a function actually is!

Example 8.1.

"Let $f(x) : \mathbb{Q} \to \mathbb{Z}$ be the function defined by $f(q) = a$ where a is the numerator of q."

This is BAD! What we've written is not a function, since $f(1/2) = 1$ and $f(2/4) = 2$ but $1/2 = 2/4$. The rational numbers are like a partition of $\mathbb{Z} \times (\mathbb{Z}\backslash\{0\})$, and so we must be extra careful when defining functions when there are equivalence relations hanging about!

. . . . . .

CHAPTER 3

Some Elementary Number Theory

Number theory has traditionally been called the *queen of mathematics* for it's elegance and prominence in mathematics. Even in modern mathematics, the old theory of numbers plays an ever present role. Often a complex problem in algebra, analysis, or geometry can be reduced to a problem in number theory. The most popular open questions in the last 100 years have been number theory problems; Collatz's conjecture, the Riemann Hypothesis, Goldbach's conjecture, and Fermat's Last Theorem, just to name a few.

1. Arithmetic properties of numbers

We begin this section by defining a natural relation on the integers.

DEFINITION 1.1 (The "Divides" Relation).
A non-zero integer x is said to *divide* another integer y if there exists an integer n such that $y = nx$. We write $x|y$ to mean "x divides y".

So for example, 3 divides 6, 8 divides 24, and -3 divides 3.

LEMMA 1.2 (Division Algorithm). *If m is a positive integer and n is an integer, then there exist unique integers q and r such that*

$$n = mq + r \quad \text{and} \quad 0 \leq r < m.$$

The integer r is called the remainder and q is called the quotient.

Example 1.3.

- If we take $m = 4$ and $n = 23$, then $q = 5$ and $r = 3$ are the only integers which satisfy the Division Algorithm. That is, $23 = 4 \times 5 + 3$.
- Warning: r must be between 0 and m, or equal to 0.

. . . . . .

DEFINITION 1.4 (Greatest Common Divisor).
The *greatest common divisor* of two positive integers x and y is defined by

$$\gcd(x, y) = \max\{i \in \mathbb{N} : i|x \text{ and } i|y\}.$$

Example 1.5.

- The divisors of 8 are $1, 2, 4, 8$ and the divisors of 20 are $1, 2, 4, 5, 10, 20$. So $\gcd(8, 20) = 4$.
- The gcd of two distinct primes is always 1.

. . . . . .

THEOREM 1.6. *The greatest common divisor of two non-zero integers a and b, can be expressed as a linear combination of a and b:*

$$\gcd(a, b) = am + bn \text{ for some integers } m \text{ and } n.$$

DEFINITION 1.7. The *least common multiple* of two positive integers x and y is defined by

$$\text{LCM}(x, y) = \min\{i \in \mathbb{N} : x|i \text{ and } y|i\}.$$

LEMMA 1.8. *For all non-zero integers x and y,*

$$\text{LCM}(x, y) = \frac{xy}{\gcd(x, y)}.$$

DEFINITION 1.9. Two positive integers are *relatively prime* if their gcd is equal to 1.

Example 1.10.

- Any two distinct primes are relatively prime.
- 15 and 8 are relatively prime.

2. Euclidean Algorithm in $\mathbb{Z}$

In this section we demonstrate a method for finding the gcd of two integers. We show by example the routine.

Example 2.1. Consider 558 and 423. We put the biggest one on the left (in this case 558 and write it as a linear combination involving 423 (via the Division Algorithm).

$$558 = \mathbf{1} \cdot 423 + 125.$$

We will write the *quotient* of 423 in bold to keep track of this number. Next we take the number adjacent to the bold number, and write it as a linear combination of the remainder:

$$423 = \mathbf{3} \cdot 135 + 18$$

We continue this process until we get 0 as a remainder:

$$\begin{aligned} 558 &= \mathbf{1} \cdot 423 + 135 \\ 423 &= \mathbf{3} \cdot 135 + 18 \\ 135 &= \mathbf{7} \cdot 18 + 9 \\ 18 &= \mathbf{2} \cdot 9 + 0 \end{aligned}$$

Then the last non-zero remainder is 9 so it will turn out that $9 = \gcd(558, 423)$. Now we do the reverse substitution and get

$$\begin{aligned} 9 &= 135 - 7 \cdot 18 \\ &= 135 - 7(423 - 3 \cdot 135) \\ &= 22 \cdot 135 - 7 \cdot 423 \\ &= 22 \cdot (558 - 423) - 7423 \\ &= 22 \cdot 558 - 29 \cdot 423 \end{aligned}$$

Example 2.2. We use the Euclidean[1] Algorithm to find the gcd of 56 and 1450.

$$\begin{aligned} 1450 &= \mathbf{25} \cdot 56 + 50 \\ 56 &= \mathbf{50} \cdot 1 + 6 \\ 50 &= \mathbf{6} \cdot 8 + 2 \\ 6 &= \mathbf{2} \cdot 3 + 0 \end{aligned}$$

Therefore $\gcd(56, 1450) = 2$.

Exercises 2.3.

(1) List all the positive divisors of each of the following integers:
12, 20, 32, 63, -101.
(2) For each pair a and b below, find the unique integers q and r such that $a = bq + r$ with $0 \leq r < b$,
(a) $a = 19, b = 5$

[1] 

Euclid of Alexandria (abt.325 BC - abt.265 BC) is the most prominent mathematician of antiquity best known for his treatise on mathematics "The Elements".

(b) $a = -7, b = 5$
(c) $a = 30, b = 1$

(3) Find the gcd of the following pairs of numbers:
(a) $4, 6$
(b) $5, 8$
(c) $24, 32$
(d) $9, 18$

(4) Use the Euclidean Algorithm to find the gcd of:
(a) 1001 and 357
(b) 56 and 126

3. Linear Congruences

In this section, we introduce an equivalence relation on the integers that in some sense preserves arithmetic on the integers.

Definition 3.1 (Congruence Modulo n).
Let $n \in \mathbb{N}$. Integers a and b are said to be *congruent modulo* n if n divides $a - b$. We denote this relation by $a \equiv b \pmod{n}$.

Example 3.2.

- $14 \equiv 4 \pmod{5}$ since $14 - 4 = 10$ is a multiple of 5.
- $-7 \equiv 2 \pmod{3}$ since $-7 - 2 = -9$ is a multiple of 3.

Lemma 3.3. *For $n \in \mathbb{N}$, congruence modulo n is an equivalence relation on the integers.*

Proof.

(1) Reflexivity: Note for all $a \in \mathbb{Z}$ that n divides $a - a = 0$ and hence $a \equiv a \pmod{n}$.
(2) Symmetry: If $a \equiv b \pmod{n}$, then n divides $a - b$, which is the same as $b - a$, and hence $b \equiv a \pmod{n}$.
(3) Transitivity: Suppose $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ for some integers a, b, and c. Then n divides $a - b$ and n divides $b - c$. So n divides the sum of $a - b$ and $b - c$, which is $a - c$, and hence $a \equiv c \pmod{n}$.

Since congruence modulo n is a reflexive, symmetric, and transitive relation on the integers, it is also an equivalence relation. □

Here are some properties of congruences:

- If $a \equiv b \pmod{n}$ and $a' \equiv b' \pmod{n}$, then $a + a' \equiv b + b' \pmod{n}$ and $aa' \equiv bb' \pmod{n}$.
- If $d > 0$, d divides n, and $a \equiv b \pmod{n}$, then $a \equiv b \pmod{d}$.

We now define addition and multiplication modulo n.

Definition 3.4 (Arithmetic Modulo n).
Let $n \in \mathbb{N}$. Then we define the binary operations $\oplus_n$ and $\otimes_n$ on the integers by

$$x \oplus_n y = (x + y) \pmod{n}$$
$$x \otimes_n y = xy \pmod{n}$$

for all $x, y \in \mathbb{Z}$.

Example 3.5.

- $5 \oplus_4 3 = 8 \pmod{4} = 0$,
- $-7 \oplus_5 13 = 6 \pmod{5} = 1$,
- $50 \otimes_{233} 233 = 50.233 \pmod{233} = 0$.

Definition 3.6 (Ceiling and Floor).
Let x be a real number. Then the *ceiling* of x, denoted $\lceil x \rceil$ is the smallest integer bigger than x. The *floor* of x, denoted $\lfloor x \rfloor$ is the largest integer smaller than x.

Example 3.7.

- $\lfloor 3.6 \rfloor = 4$,

. . . . . .

Exercises 3.8.

(1) Find the solutions of the following sums:
   (a) $5 \oplus_3 7$
   (b) $50 \oplus_{20} 2$
   (c) $-19 \oplus_5 8$
(2) Show that $\oplus_n$ and $\otimes_n$ are indeed binary relations. (Hint: use the Division Algorithm).
(3) Prove the "properties of congruences" stated above.
(4) Find the day of the week you were born on by using the following formula:

$$W = (D + \lfloor 2.6((M+9) \bmod 12) + 2.4 \rfloor - 2\mathrm{C} + \lfloor 5\mathrm{Y}/4 \rfloor + \lfloor \mathrm{C}/4 \rfloor - \lfloor ((\mathrm{M}+9) \bmod 12)/10 \rfloor) \bmod 7$$

   where
   - D is the day (1 to 31),
   - M is the month (1 to 12),
   - C is the century (2003 has $C = 20$),
   - Y is the year (2003 has $Y = 3$),
   - W is the week day (Sunday=0,. . . ,Saturday=6).

(5) Prove that a number is divisible by three if and only if the sum of its digits is divisible by three.

CHAPTER 4

An Introduction to Group Theory

What do we know about the set of permutations (bijections) of a set X? Well we know, that if we compose two permutations, we get another permutation. So "composition" is a binary operation on the set of permutations of X. We also know that there is a special function called the "identity map" which when composed with any permutation, returns the same permutation. That is $f \circ \mathrm{id} = \mathrm{id} \circ f = f$ for all permutations f of X. The last property to note is that every permutation has an inverse permutation. So this set of permutations we have been considering obeys the algebraic laws of what is abstractly known as a "group".

1. The Axioms

DEFINITION 1.1 (Group). A *group* is a set G together with a binary operation $*$ on G, such that the following axioms are satisfied:

(1) $*$ is associative, (associativity axiom)
(2) There is an element $e \in G$ such that $x * e = e * x = x$ for all $x \in G$.
We call e the[1] "identity element" of G; (identity axiom)
(3) For each $a \in G$, there is an element $b \in G$ such that $a * b = b * a = e$. We call b the[2] "inverse" of a. (inverse axiom)

Note that to show $(G, *)$ is a group for a set G and a binary operation $*$, we have to prove each of these axioms.

Often we use the usual multiplication symbol $\cdot$ instead of $*$. In this case we denote the identity of $(G, \cdot)$ by 1 and denote the inverse of an element $a \in G$ by a^{-1}. We also use the convention a^n for $n \in \mathbb{Z}^+$ to mean $a \cdots a$ where the product contains n copies of a. Sometimes we also use the symbol $+$ instead of $*$. Generally, we do that if the group is commutative, i.e. if $a * b = b * a$ for all $a, b \in G$. In this case we write $(G, +)$ for our group, the identity is denoted by 0 and the inverse of an element $a \in G$ is denoted $-a$. The convention na for $n \in \mathbb{Z}^+$ means $a + \ldots + a$, where the sum contains n copies of a.

LEMMA 1.2. *Let G be a group with binary operation $*$. Then*

- *the identity of G is unique,*
- *each non-identity element in G has a unique inverse,*
- *for $a, b \in G$ holds $(a * b)^{-1} = b^{-1} * a^{-1}$ and $(a^{-1})^{-1} = a$,*
- *$a * b = a * c \implies b = c$, and $b * a = c * a \implies b = c$ (cancellation laws),*
- *$a * b = a \implies b = e$.*

PROOF. Exercise. □

2. Examples of Groups

EXERCISES 2.1.

(1) For each of the following either prove or disprove that the given set together with the binary operation is a group.
   (a) $(\mathbb{Z}, +)$;
   (b) $(\mathbb{Z}^+, +)$;
   (c) $(\mathbb{Z}, \times)$;
   (d) $(\mathbb{R}, +)$;
   (e) $(\mathbb{R} \backslash \{0\}, \times)$;
   (f) The set $GL(2, \mathbb{R})$ of 2×2 invertible matrices with real entries, together with matrix multiplication;

[1] We prove in Lemma 1.2 that there is a unique such element e with this property. So we can say *the identity element* here.
[2] Again, we prove in Lemma 1.2 that there is a unique such element b with this property. So we can say *the inverse* here.

(g) The *Klein 4-group* $V_4 = \{(), (1,2)(3,4), (1,4)(2,3), (1,3)(2,4)\}$. Show that V_4 under permutation multiplication;
(h) The symmetric group on 3 letters $S_3 = \{(), (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}$. under permutation multiplication;
(i) $C_5 = \{(), (1,2,3,4,5), (1,3,5,2,4), (1,4,2,5,3), (1,5,4,3,2)\}$ under permutation multiplication;
(j) The *circle group* $S^1 = \{z \in \mathbb{C} : |z| = 1\}$ under multiplication.

(2) Let $n \in \mathbb{N}$ and let $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$. Show that $\mathbb{Z}_n$ is a group under $\oplus_n$. Is it a group under $\otimes_n$?
(3) Let G be a group and for all $g \in G$, let $\tau_g : G \to G$ be the map defined by $\tau_g(x) = gx$ for all $x \in G$. Show that τ_g is a permutation (for all $g \in G$) and that the set of all τ_g is a subgroup of $\mathrm{Sym}(G)$.

3. Abelian Groups

Recall that a binary operation $*$ on a set X is commutative if $x * y = y * x$ for all $x, y \in X$. We have a special name for groups with a commutative binary operation.

Definition 3.1 (Abelian Group).
A group G with binary operation $*$, is said to be *abelian*[3] if $*$ is commutative.

> To show that a group is not abelian, find two elements in the group that do not commute. Do not attempt to give a general "proof". Whenever you need to show that a statement is not true in general, give a concrete counterexample.

For most groups we use, if it is clear what the binary operation is, we will use the juxtaposition ab to represent $a * b$. For abelian groups, we may use $a + b$ to mean $a * b$.

Exercises 3.2. For each group in Exercise 2.1 decide whether or not the group is abelian.

4. Subgroups

Everyone knows what "subset" means, and it is helpful to use this term when we are talking about sets. In Linear Algebra, it is common to use the term "subspace" for a subset of a vector space that is also a vector space. Recall that to prove that a subset V of a vector space W is a vector space, we needed to show that "+" was *closed* on W, and scalar multiplication was also closed. Similarly, for groups we have the notion of a "subgroup", but first we give the defintion of *closure* of a binary operation.

Definition 4.1 (Closure).
Let $*$ be a binary operation on a set X and let S be a subset of X. If $a * b \in S$ for each $a, b \in S$, then we say that S is *closed under* $*$. The operation $*$ restricted to S is called the *induced* binary operation on S.

Definition 4.2 (Subgroup).
Let G be a group and let H be a subset of G. If H is closed under the binary operation of G, and is a group under the induced binary operation of G, then H is a *subgroup* of G. We write $H \leq G$ to mean "H is a subgroup of G", and $H < G$ if $H \leq G$ but $H \neq G$.

Two obvious examples of a subgroup of a group G are $\{1\}$ and G itself.

Definition 4.3. We say that a subgroup H of G is *trivial* if $H = \{1\}$. We call H a proper subgroup of G if $H \neq \{1\}$ and $H \neq G$.

Now we give a lemma which will assist us in proving that a subset of a group is a subgroup.

---

[3] 

Commutative groups are called abelian after Niels Henrik Abel (1802-1829). In 1824, at the age of 22, Abel proved that it is impossible to solve algebraically the general equation of the fifth degree. By the time he died he had written many influential papers in mathematics.

LEMMA 4.4. *Let G be a group with binary operation $*$ and identity element 1, and let H be a subset of G. Then the following are equivalent:*

(1) *H is a subgroup of G,*
(2) *H satisfies...*
   (a) $1 \in H$,
   (b) $a, b \in H \implies ab \in H$,
   (c) $a \in H \implies a^{-1} \in H$.
(3) *H satisfies the "subgroup criterion"...*
   (a) $1 \in H$,
   (b) $a, b \in H \implies ab^{-1} \in H$.

Note: "$1 \in H$" is equivalent to "H is nonempty".

Example 4.5.

(1) $(\mathbb{Q}, +)$ is a subgroup of $(\mathbb{R}, +)$, which in turn is a subgroup of $(\mathbb{C}, +)$.
(2) $(\mathbb{Q}, \cdot)$ is not a subgroup of $(\mathbb{R}, +)$. Why not?

. . . . . .

EXERCISES 4.6.

(1) Prove that the circle group S^1 is a subgroup of $\mathbb{C}$.
(2) Prove that $\{(), (1,2)\}$ is a subgroup of S_3.
(3) Prove that $\{(), (1,2)\}$ is a subgroup of V_4.
(4) Prove that $\{0, 1\}$ is a subgroup of $\mathbb{Z}_n$ under $\oplus_n$.
(5) Is $\{0, 2, 4\}$ a subgroup of $\mathbb{Z}_6$ under $\oplus_6$?
(6) Is $\{1, 3, 5\}$ a subgroup of $\mathbb{Z}_6$ under $\oplus_6$?
(7) Is $\{2n \mid n \in \mathbb{Z}\}$ a subgroup of $(\mathbb{Z}, +)$?

5. Orders

DEFINITION 5.1 (Order of a Group).
The *order* of a group G is the cardinality (or size) of the set G. If G is finite, then we say that G has *finite order* and denote $|G|$ the order of G.

Just as we have "power laws" for real numbers, we can define power laws for elements of a group.

LEMMA 5.2 (Power laws).
Let G be a group and let $a \in G$. Then for all $m, n \in \mathbb{Z}$ we have (in multiplicative notation):

$$a^{m+n} = a^m a^n \text{ and } (a^m)^n = a^{mn}.$$

PROOF. Exercise (hint: use induction). □

DEFINITION 5.3 (Order of an element).
Let G be a group and let $g \in G$. We say that g has *finite order* if there is a positive integer n such that $g^n = 1$. If n is the smallest integer such that $g^n = 1$, then we say that g has *order* n.

EXERCISES 5.4.
(1) What is the order of $(\mathbb{R}, +)$?
(2) What is the order of V_4? What are the orders of all the elements of V_4?
(3) What is the order of S_3? What are the orders of all the elements of S_3?
(4) Given $n \in \mathbb{Z}^+$. What is the order of $(\mathbb{Z}_n, \oplus_n)$?
(5) What are the orders of all the elements in $\mathbb{Z}_5$ and in $\mathbb{Z}_6$?

6. Cyclic Groups

We have seen a few examples of groups thus far, many of which are quite complicated in structure. Here, we investigate cyclic groups, which are the most basic of classes of groups.

THEOREM 6.1 (Fraleigh, Theorem 1.5).
Let $(G, *)$ be a group and $a \in G$. Then

$$H = \{a^n \mid n \in \mathbb{Z}\}$$

is a subgroup of G and is the smallest subgroup containing a, that is every subgroup of G that contains a also contains H. We write this subgroup as $\langle a \rangle$.

The group H of the previous theorem is called a *cyclic* group. The element a is called a *generator* of H.

DEFINITION 6.2 (Cyclic Subgroups).
An element g of a group G *generates* G if $G = \{g^n \mid n \in \mathbb{Z}\}$, i.e. if $G = \langle g \rangle$. If a group G is equal to $\langle g \rangle$ for some $g \in G$, then we say that G is *cyclic*.

Example 6.3.

(1) $(\mathbb{Z}, +)$ is a cyclic group. A generator for this group is 1. Note that here we are using additive notation, so a^n in multiplicative notation becomes na in additive notation. Then $\langle 1 \rangle = \{n \cdot 1 \mid n \in \mathbb{Z}\} = \mathbb{Z}$.
(2) Are there any other generators for $(\mathbb{Z}, +)$?
(3) 3 is not a generator for $(\mathbb{Z}, +)$, because $\langle 3 \rangle = \{3n \mid n \in \mathbb{Z}\} = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$. In particular, $1 \notin \langle 3 \rangle$. As $\langle 3 \rangle \neq \{0\}$ it is a proper subgroup of $(\mathbb{Z}, +)$.
(4) Prove that if G is a group and each element of G has order at most 2, then G is abelian.

. . . . . .

Note that if g has finite order, then the "order" of g is equal to the "order" of $\langle g \rangle$. Both uses of the word "order" here mean different things!

EXERCISES 6.4.

(1) Which of the groups in Exercise 2.1 are cyclic?
(2) Find a generator for $\mathbb{Z}_6$.

We said that a cyclic group is basic in structure. In fact, cyclic groups are abelian!

THEOREM 6.5. *Every cyclic group is abelian.*

PROOF. Let G be a cyclic group. Then $G = \langle g \rangle$ for some $g \in G$. Now suppose $a, b \in G$. Then there are integers $i, j \in \mathbb{Z}$ such that $a = g^i$ and $b = g^j$. Thus

$$ab = g^i g^j = g^{i+j} = g^{j+i} = g^j g^i = ba$$

and so G is abelian. □

EXERCISES 6.6.

(1) Let G be a group and $a \in G$. Suppose that a has order n. Show that
   (a) $a^k = 1 \Leftrightarrow n$ divides k.
   (b) The order of a^k is $n/\gcd(n, k)$.
(2) Let G be an abelian group group and $a, b \in G$. Suppose that a has order n and b has order m. Show that if $\gcd(n, m) = 1$ then the order of ab is nm.

7. Isomorphism and Homomorphism

What does it mean for two groups to be the same? For example, $\{-1, 1\}$ under multiplication looks just like $\{0, 1\}$ under binary addition if we just change the labelling of elements. But relabelling alone does note ensure our groups behave the same way. We must make sure that the basic algebraic properties are preserved as well. For example, consider the two functions defined by $f(x) = 1/x$ and $g(x) = -x$ on the set of all nonzero real numbers. The set $V = \{\text{id}, f, g, f \circ g\}$ forms a group under composition of functions (check this!). Another group of four elements is the set of permutations $V_4 = \{(1), (1,2)(3,4), (1,3)(2,4), (1,4)(3,2)\}$. Every element of V is equal to its own inverse, and the same holds for V_4. We say two groups are the same if we can relabel the elements, that is there is a bijection between the groups such that the binary operation is preserved. It turns out that V and V_4 are the *same* group up to relabelling of elements. Formally, we define the following equivalence relation on groups.

Definition 7.1 (Isomorphism).
Let G and H be groups with binary operations $\diamond$ and $\star$ respectively. A function $\Phi : G \to H$ is an *isomorphism* if it is a bijection and preserves the group operation as follows:

$$\Phi(g_1 \diamond g_2) = \Phi(g_1) \star \Phi(g_2), \quad \text{for all } g_1, g_2 \in G.$$

We say that two groups G and H are *isomorphic* if there exists an isomorphism from G onto H, and we write $G \cong H$ to mean "G is isomorphic to H".

The next theorem, first demonstrated by Arthur Cayley[4] can turn a difficult group with a difficult binary operation into a nice group of permutations under the nice binary operation of function composition.

Theorem 7.2 (Cayley's Theorem). *Every group is isomorphic to a group of permutations.*

Proof. Let G be a group (with identity element 1) and let $f : G \to \text{Sym}(G)$ be the function defined by $f(g) = \tau_g$ where τ_g is the permutation defined by $\tau_g(x) = gx$ for all $x \in G$. We showed in a previous exercise that $f(G)$ is a subgroup of $\text{Sym}(G)$. Now we will prove that f is a one-to-one function from G onto $f(G)$ that preserves the binary operation and hence show that G is isomorphic to $f(G)$. Suppose $f(g_1) = f(g_2)$. Then $\tau_{g_1} = \tau_{g_2}$. So $\tau_{g_1}(1) = \tau_{g_2}(1)$ and hence $g_1 = g_2$. Therefore f is one-to-one. Now for all $g_1, g_2 \in G$, we have $f(g_1 g_2) = \tau_{g_1 g_2}$. But for all $x \in G$, $(\tau_{g_1} \circ \tau_{g_2})(x) = \tau_{g_1}(\tau_{g_2})(x) = \tau_{g_1}(g_2 x) = g_1 g_2 x = \tau_{g_1 g_2}(x)$. So $\tau_{g_1} \circ \tau_{g_2} = \tau_{g_1 g_2}$ and hence $f(g_1 g_2) = f(g_1) \circ f(g_2)$. Therefore f is a homomorphism and thus G is isomorphic to $f(G)$. □

In linear algebra, not only do we study invertible linear maps, but we are also interested in the non-invertible one's as well. There are some interesting properties of vector spaces that are preserved by linear maps, but that do not require that our vector spaces look exactly the same. Analogously, we generalise the notion of *isomorphism* to that of a *homomorphism* so that we can study similarity properties of non-isomorphic groups.

Definition 7.3 (Homomorphism). Let G and H be groups with binary operations $\diamond$ and $\star$ respectively. A function $\Psi : G \to H$ is a *homomorphism* if it preserves the group operation. That is,

$$\Psi(g_1 \diamond g_2) = \Psi(g_1) \star \Psi(g_2), \quad \text{for all } g_1, g_2 \in G.$$

A one-to-one homomorphism is called an *embedding*, or sometimes it is called a *monomorphism*. An onto homomorphism is called an *epimorphism*.

Now we give some important properties of homomorphisms.

Theorem 7.4. *Let Ψ be a homomorphism from a group G into a group H. Then*

1. *if e is the identity of G, then $\Psi(e)$ is the identity of H,*
2. *if $g \in G$, then $\Psi(g^{-1}) = (\Psi(g))^{-1}$,*
3. *if A is a subgroup of G, then $\Psi(A)$ is a subgroup of H,*
4. *if B is a subgroup of H, then $\Psi^{\leftarrow}(B)$ is a subgroup of G.*

Proof.

1. Let e be the identity of G. Now $\Psi(e)\Psi(e) = \Psi(ee) = \Psi(e)$, and hence $\Psi(e)$ is the identity element of H.

---

[4] 

Arthur Cayley (1821-1895) was a child prodigy who showed impressive ability in numerical calculations at an early age. At the age of 25, he began a 14 year career in the legal profession and solved mathematics problems in his spare time. Even though he was seen as an amateur mathematician, he was one of the most prolific during his time as a lawyer. He eventually took a cut in pay to become a mathematician, and remained so until his death.

(2) Let $g \in G$. Then $\Psi(g)\Psi(g^{-1}) = \Psi(gg^{-1}) = \Psi(e)$. By (1), $\Psi(e)$ is the identity of H, and so $\Psi(g^{-1})$ is the inverse of $\Psi(g)$.
(3) Let A be a subgroup of G. Since $e \in A$ and $\Psi(e) \in \Psi(A)$, by (1), the identity of H belongs to $\Psi(A)$. Let $\Psi(a)$ and $\Psi(b)$ be arbitrary elements of $\Psi(A)$. Then $\Psi(a)\Psi(b^{-1}) = \Psi(ab^{-1}) \in \Psi(A)$. So by the "subgroup criterion", $\Psi(A)$ is a subgroup of H.
(4) Exercise.

□

A homomorphism Ψ preserves the identity, inverses, and subgroups.

DEFINITION 7.5 (Kernel). Let Ψ be a homomorphism from a group G into a group H, and let 1_H be the identity element of H. The set

$$\ker \Psi := \{g \in G : \Psi(g) = 1_H\}$$

is called the *kernel* of Ψ.

Note that $\ker \Psi = \Psi^{\leftarrow}(1_H)$.

EXERCISES 7.6.

(1) Let Ψ be a homomorphism from a group G into a group H. Show $\ker \Psi$ is a subgroup of G.
(2) Prove that a group homomorphism $\phi : G \to H$ is one-to-one if and only if $\ker \phi$ is trivial.
(3) Let $n \in \mathbb{Z}^+$. Prove that $\varphi : (\mathbb{Z}, +) \to \mathbb{Z}_n$ defined by $\varphi(a) = a \pmod n$ is a homomorphism. Is φ one-to-one? Is φ onto? What is $\ker \varphi$?
(4) Are the groups $\mathbb{Z}_4$ and V_4 isomorphic?
(5) Let G, H be groups and φ an isomomorphism from G to H. Prove that if G is abelian, then so is H.
(6) Let G, H be groups and φ a homomorphism from G to H. Prove that if $g \in G$ has order n then $\varphi(g) \in H$ has order dividing n.

8. Lagrange's Theorem

In this section we prove that the order of a subgroup of a finite group always divides the order of the group. We also introduce the important concept of cosets.

THEOREM 8.1. *Let $(G, \cdot)$ be a group and let H be a subgroup of G. Define binary relations $\sim_L$ and $\sim_R$ on G by*

$$\begin{aligned} a \sim_L b &\Leftrightarrow a^{-1}b \in H \\ a \sim_R b &\Leftrightarrow ba^{-1} \in H. \end{aligned}$$

Then $\sim_L$ and $\sim_R$ are both equivalence relations on G.

PROOF. Exercise! □

Note that by Theorem 7.7 both equivalence relations define partitions of the set G. What do the parts of these partitions look like? Let us consider the equivalence relation $\sim_L$ first. Then the set of all elements of G equivalent to a particular element $a \in G$ is a part. Let us denote this part by aH. We can see that this part is

$$\begin{aligned} aH &= \{b \in G \mid b \sim_L a\} \\ &= \{b \in G \mid a^{-1}b \in H\} \\ &= \{b \in G \mid b = ah \text{ for some } h \in H\} \\ &= \{ah \mid h \in H\}. \end{aligned}$$

Similarly, if we denote by Ha the part containing a when we use the equivalence relation $\sim_R$, we can see that $Ha = \{ha \mid h \in H\}$.

DEFINITION 8.2 (Coset).
Let H be a subgroup of a group G. The part $aH = \{ah \mid h \in H\}$ is called the *left coset* of H containing a in G and $Ha = \{ha \mid h \in H\}$ is called the *right coset* of H containing a. We call a a *representative* of the coset aH.

Example 8.3. The left coset of the subgroup $3\mathbb{Z} = \langle 3 \rangle$ containing a of $\mathbb{Z}$ is $a + \langle 3 \rangle = \{a + 3n : n \in Z\}$. Thus all left cosets are (taking $a = 0, 1, 2$)

$$\begin{aligned} 3\mathbb{Z} &= \{\ldots, -6, -3, 0, 3, 6, \ldots\} \\ 1 + 3\mathbb{Z} &= \{\ldots, -5, -2, 1, 4, 7, \ldots\} \\ 2 + 3\mathbb{Z} &= \{\ldots, -4, -1, 2, 5, 8, \ldots\}. \end{aligned}$$

We see that these three cosets already partition $\mathbb{Z}$ thus we have found all left cosets of $\langle 3 \rangle$ in $\mathbb{Z}$. Note that $3 + 3\mathbb{Z} = 3\mathbb{Z}$.

. . . . . .

Example 8.4. Let $G = (\mathbb{R}^2, +)$ and let v be an element of $\mathbb{R}^2$. Then $\langle v \rangle$ is a line in $\mathbb{R}^2$ passing through v and the origin $(0, 0)$ (which is the identity element of $\mathbb{R}^2$). By definition, $\langle v \rangle$ is a subgroup of G. What do the cosets of $\langle v \rangle$ look like? They are just the lines in $\mathbb{R}^2$ parallel to $\langle v \rangle$ (see below).

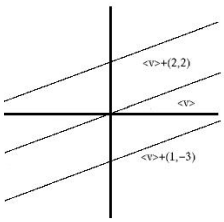

FIGURE 1. Two cosets of $\langle v \rangle$.

. . . . . .

EXERCISES 8.5.

(1) Find all cosets of the subgroup $\langle 5 \rangle$ of $\mathbb{Z}$.
(2) Show that if $aH = bH$ then $Ha^{-1} = Hb^{-1}$.
(3) Consider again the homomorphism $\varphi : \mathbb{Z} \to Z_n$ defined by $\varphi(a) = a \pmod{n}$. Find all cosets of $\ker \varphi$ in $\mathbb{Z}$.

LEMMA 8.6. *Let H be a subgroup of G. Then every left coset and every right coset of H in G have the same number of elements.*

PROOF. We show that every left coset and every right coset of H in G has the same number of elements as H. Let's start with a left coset aH. Define a map $\psi : H \to aH$ defined by $\psi(h) = ah$. Then it is clear that ψ is onto. Let us now show it is one-to-one. Suppose $\psi(h) = \psi(k)$ for $h, k \in H$. Then $ah = ak$. By the cancellation law, it follows that $h = k$. Therefore, ψ is one-to-one. In particular this means H and aH have the same number of elements. The same can be shown for any right coset Ha. □

THEOREM 8.7 (Lagrange[5]).
Let H be a subgroup of a finite group G. Then the order of H is a divisor of the order of G.

PROOF. See Theorem 2.5 in Fraleigh. □

From this it follows immediately that the order of an element in a finite group divides the order of the group.

EXERCISES 8.8.

(1) Let $G = \langle a \rangle$ be a cyclic group of order n. Show that every subgroup of G is cyclic of order d for some d dividing n.
(2) For each d dividing n show that there is a unique subgroup of G of order d. Can you list the elements of this subgroup in terms of a?

---

5 

Joseph-Louis Lagrange was born in 1736 in Turin, Italy under the name Giuseppe Lodovico Lagrangia. He was mostly self taught and published papers on a wide variety of topics. He died 1813 in Paris, France.

Index