Part I

Groups

1

Preliminaries

1.1 Introduction

Notation. From now on, we will often use the abbreviations:

$\Longrightarrow$	implies
$\Longleftarrow$	is implied by
iff (or $\Longleftrightarrow$)	if and only if
$\forall$	for every
$\exists$	there exists
$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$	the integers, rationals, reals, complex numbers, respectively

We will not review the basics of proofs here. Hopefully you have figured out the basics, either from a high school plane geometry class or a college class introducing the subject of mathematical proof. See K. H. Rosen [93] for an introduction to proof. We will discuss proof by mathematical induction soon. There is an interesting book [60] by Steven Krantz on the subject of proof. Edna E. Kramer's history book [59] gives more perspective on the subject of proof. Another place to find a discussion of mathematical proof is Wikipedia. A cautionary tale concerns K. Gödel's incompleteness theorems from 1931, the first of which says that for any consistent formal system for the positive integers $\mathbb{Z}^+$, there is a statement about $\mathbb{Z}^+$ that is unprovable within this system.

There are those who argue against proofs. I have heard this at conferences with physicists. Nature will tell us the truth of a statement they argue. Ramanujan felt the goddess would inspire him to write true formulas. However, I have no such help myself and really need to see a proof to know what is true and what is false. This makes me very bad at real life, where there is rarely a proof of any statement. Thus I have grown to be happier writing an algebra book than a book on politics.

If you need more convincing about the need for proofs, look at the following two exercises, once you know what a prime is – an integer $p > 1$ such that $p = ab$, with positive integers a, b implies either a or $b = 1$. These exercises are silly if you can use your computer and Mathematica or some other similar program.

Exercise 1.1.1 *Show that $x^2 - x + 41$ is prime for all integers x such that $0 \leq x \leq 40$, but is not a prime when $x = 41$. Feel free to use a computer.*

Number theory has multitudes of statements like that in Exercise 1.1.1 that have been checked for a huge number of cases, but yet fail to be true in all cases. Of course, now

computers can do much more than the puny 41 cases in the preceding exercise. For example, Mersenne primes are primes of the form $M_p = 2^p - 1$, where p is a prime. Mersenne compiled a list of Mersenne primes in the 1600s, but there were some mistakes after $p = 31$. Much computer time has been devoted to the search for these primes. Always bigger ones are found. In January, 2017 the biggest known prime was found to be $M_{77\,232\,917}$. It is conjectured that there are infinitely many Mersenne primes, but the proof has eluded mathematicians. See Wikipedia or Shanks [103] for more information on this subject and other unsolved problems in number theory. Wikipedia notes that these large primes have a cult following – moreover they have applications to random number generators and cryptography.

In the 1800s – before any computers existed – there was a conjecture by E. C. Catalan that M_{M_p} is prime, assuming that M_p is a Mersenne prime. Years passed before Catalan's conjecture was shown to be false. In 1953 the ILLIAC computer (after 100 hours of computing) showed that M_{M_p} is not prime when $p = 11$. M_{M_p} is prime for $p = 2, 3, 5, 7$. It was subsequently found that the conjecture is false for $p = 17, 19, 31$ as well. The next case is too large to test at the moment. Wikipedia conjectures that the four known M_{M_p} that are prime are the only ones. Anyway, hopefully, you get the point that you can find a large number of cases of some proposition that are true without the general proposition being valid. Stark gives many more examples in the introduction to [110].

Exercise 1.1.2 ***(Mersenne Primes).*** *Show that $2^p - 1$ is prime for $p = 2, 3, 5, 7, 13$, but not for $p = 11$.*

Hint. *The Mathematica command below will do the problem for the first 10 primes.*

```
Table[{Prime[n],FactorInteger[(2^Prime[n])-1]},{n,1,10}]
```

We assume that you can write down the **converse** of the statement "proposition A implies proposition B." Yes, it is "proposition B implies proposition A." Recall that $A \implies B$ is not equivalent to $B \implies A$. However $A \implies B$ is equivalent to its **contrapositive:** (not B) $\implies$ (not A).

We will sometimes use proof by contradiction. There are those who would object. In proof by contradiction of $A \implies B$ we assume A and (not B) and deduce a contradiction of the form R and (not R). Those who would object to this and to any sort of "non-constructive" proof have a point, and so we will try to give constructive proofs when possible. See Krantz [60] for a bit of the history of constructive proofs in mathematics.

It is also possible that you can prove something that may at first be unbelievable. See the exercise below, which really belongs to an analysis course covering the geometric series – the formula for which follows from Exercise 1.4.7 below. If you accept the axioms of the system of real numbers, then you have to believe the formula.

Exercise 1.1.3 *Show that* $0.999\,999\ldots = 1$.

Hint. *See Exercise 1.4.7. The ... conceals an infinite series.*

A controversial method of proof is proof by computer. First you have to believe that the computer has been programmed correctly. This has not always been the case; e.g., the problem with the Pentium chip. Here I will choose to believe what my computer tells me

when I use Mathematica to say whether an integer is a prime, or when used to compute eigenvalues of matrices, or graphs of functions, or to multiply elements of finite fields. There are more elaborate computer proofs that are hard to verify without even faster computers than the cheap laptop (vintage 2011) that I am using – for example, the proof of the four color problem in the 1970s or the recent proof of the Kepler conjecture on the densest packing of spheres in 3-space. See Krantz [60] for more information.

We are also going to assume that you view the following types of numbers as old friends:

the integers	$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \ldots\}$,
the rationals	$\mathbb{Q} = \left\{ \frac{m}{n} \mid m, n \in \mathbb{Z}, n \neq 0 \right\}$,
the reals	$\mathbb{R} = \{\text{all decimals}\}$,
the complex numbers	$\mathbb{C} = \{x + iy \mid x, y \in \mathbb{R}\}$, for $i = \sqrt{-1}$.

We will list the axioms for $\mathbb{Z}$ in Chapter 1 and will construct $\mathbb{Q}$ from $\mathbb{Z}$ in Chapter 6. Of course, the construction of $\mathbb{Q}$ from $\mathbb{Z}$ just involves the algebra of fractions and could be done in Chapter 1 – minus the verbiage about fields and integral domains. We should define the real numbers as limits of Cauchy sequences of rationals rather then to say real numbers are represented by all possible decimals, but that would be calculus and we won't go there. Such a construction can be found for example in the book by Leon Cohen and Gertrude Ehrlich [17]. A serious student should really prove that $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ exist by constructing them from scratch, sort of like a serious chef makes a pie, but we will not do that here.

In contemplating the lower rows of our table of number systems, philosophers have found their hair standing on end. Around 500 BC the Pythagoreans were horribly shocked to find that irrational numbers like $\sqrt{2}$ existed. You will be asked to prove that $\sqrt{2} \notin \mathbb{Q}$ in Section 1.6. What was the problem for the Pythagoreans? You can read about it in Shanks [103, Chapter III]. What would they have thought about transcendental numbers like π? Later the complex numbers were so controversial that people called numbers like $i = \sqrt{-1}$ "imaginary." Non-Euclidean geometry was so upsetting that Gauss did not publish his work on the subject.

Warning. This course is like a language course. It is extremely important to memorize the vocabulary – the definitions. If you neglect to do this, after a week or so, the lectures – or the reading – will become meaningless. One confusing aspect of the vocabulary is the use of everyday words in a very different but precise way. Then one needs the axioms, the rules of constructing proofs. Those are our rules of grammar for the mathematical language. These too must be memorized. We should perhaps add that it is folly to argue with the definitions or axioms – unless you have found the equivalent of non-Euclidean geometry. To some our subject appears arcane. But they should remember that it is just a language – there is no mystery once you know the vocabulary and grammar rules.

Practice doing proofs. This means practice speaking or writing the language. One can begin by imitating the proofs in the text or other texts or those given by your professor. It is important to practice writing proofs daily. In particular, one must do as many exercises as possible. If your calculus class did not include proofs, this may be something of a shock. Mathematics seemed to be just calculations in those sad proof-less classes. And we will have a few calculations too. But the main goal is to be able to derive "everything" from a few basic definitions and axioms – thus to understand the subject. One can do this for calculus too. That is advanced calculus. If you do not practice conversations in a language, you are extremely unlikely to become fluent. The same goes with mathematics.

You should also be warned that sometimes when reading a proof you may doubt a statement and then be tempted to stop reading. Sadly, often the next sentence explains why that unbelievable statement is true. So always keep reading. This happens to "real" mathematicians all the time so do not feel bad. I have heard a story about a thesis advisor who told a student he did not understand the proof of a lemma in the student's thesis. The student almost had a heart attack worrying about that important lemma. But it turned out that the advisor had not turned the page to find the rest of the proof.

Our second goal is to apply the algebra we derive so carefully. We will not be able to go too deeply into any one application, but hopefully we will give the reader a taste of each one.

1.2 Sets

We first review a bit of set theory. Georg Cantor (1845–1918) developed the theory of infinite sets. It was controversial. There are paradoxes for those who throw caution to the winds and consider sets whose elements are sets. For example, consider **Russell's paradox**. It was stated by B. Russell (1872–1970). We use the notation: $x \in S$ to mean that x is an element of the set S; $x \notin S$ means x is not an element of the set S. The notation $\{x | x \text{ has property } P\}$ is read as the set of x such that x has property P. Consider the set X defined by

$$X = \{\text{sets } S \mid S \notin S\}.$$

Then $X \in X$ implies $X \notin X$ and $X \notin X$ implies $X \in X$. This is a paradox. The set X can neither be a member of itself nor not a member of itself. There are similar paradoxes that sound less abstract. Consider the barber who must shave every man in town who does not shave himself. Does the barber shave himself? A mystery was written inspired by the paradox: *The Library Paradox* by Catharine Shaw. There is also a comic book about Russell, *Logicomix* by A. Doxiadis and C. Papadimitriou (see [26]). A nice reference for set theory illustrated by pictures and stories is the book by Vilenkin [122].

We will hopefully avoid paradoxes by restricting consideration to sets of numbers, vectors, and functions. This would not be enough for "constructionists" such as Errett Bishop who was on the faculty at the University of California San Diego. until his premature death. I am still haunted by his probing questions of colloquium speakers. Anyway, for applied mathematics, one can hope that paradoxical sets and barbers do not appear. Thus we will be using proof by contradiction, as we have already promised.

Most books on calculus do a little set theory. We assume you are familiar with the notation which we are about to review. We will draw pictures in the plane. We write $A \subset B$ (or $B \supset A$) if A is a **subset** of B: that is, $x \in A$ implies $x \in B$. We might also say B **contains** A. If $A \subset B$, the **complement** of A in B is $B - A = \{x \in B \,|\, x \notin A\}$.[1] The **empty set** is denoted $\emptyset$. It has no elements. The **intersection** of sets A and B is

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

The **union** of sets A and B is

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

[1] We will not use the other common notation B/A for set complement since it conflicts with our later notation for quotient groups.

Here – as is usual in mathematics – "or" means either or both. See Figure 1.1. Sets A and B are said to be **disjoint** iff $A \cap B = \emptyset$.

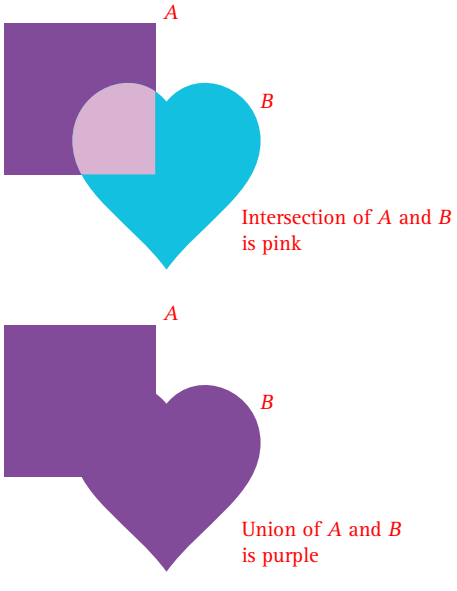

Figure 1.1 Intersection and union of square A and heart B

The easiest way to do the following exercises on the equality of various sets is to show first that the set on the left is contained in the set on the right and second that the set on the right is contained in the set on the left.

Exercise 1.2.1

(a) Prove that

$$A - (B \cup C) = (A - B) \cap (A - C).$$

(b) Prove that

$$A - (B \cap C) = (A - B) \cup (A - C).$$

Exercise 1.2.2 *Prove that* $A \cup (B \cup C) = (A \cup B) \cup C$. *Then prove the analogous equation with* $\cup$ *replaced by* $\cap$.

Exercise 1.2.3 *Prove that* $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Definition 1.2.1 *If A and B are sets, the* ***Cartesian product*** *of A and B is the set of ordered pairs (a, b) with $a \in A$ and $b \in B$: that is,*

$$A \times B = \{(a, b) \mid a \in A, b \in B\}.$$

It is understood that we have equality of two ordered pairs $(a, b) = (c, d)$ iff $a = c$ and $b = d$.

Example 1. Suppose A and B are both equal to the set of all real numbers; $A = B = \mathbb{R}$. Then $A \times B = \mathbb{R} \times \mathbb{R} = \mathbb{R}^2$. That is, the Cartesian product of the real line with itself is the set of points in the plane. ▲

Example 2. Suppose C is the interval $[0, 1]$ and D is the set consisting of the point $\{2\}$. Then $C \times D$ is the line segment of length 1 at height 2 in the plane. See Figure 1.2 below. ▲

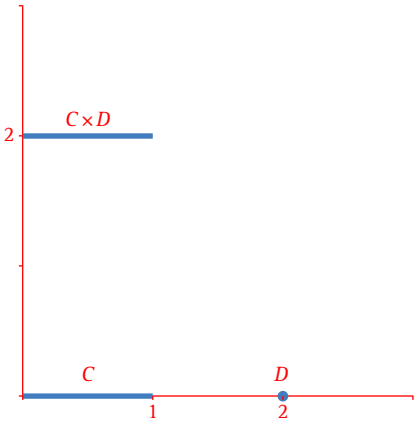

Figure 1.2 Cartesian product $[0, 1] \times \{2\}$

Of course you can also define the Cartesian product of any number of sets – even an infinite number of sets. We mostly restrict ourselves to a finite number of sets here. Given n sets S_i, $i \in \{1, 2, \ldots, n\}$, define the Cartesian product $S_1 \times S_2 \times \cdots \times S_n$ to be the set of ordered n-tuples $(s_1, s_2, \ldots, s_n)$ with $s_i \in S_i$, for all $i = 1, 2, \ldots, n$.

Example 3. $[0, 1] \times [0, 1] \times [0, 1] = [0, 1]^3$ is the unit cube in 3-space. See Figure 1.3. ▲

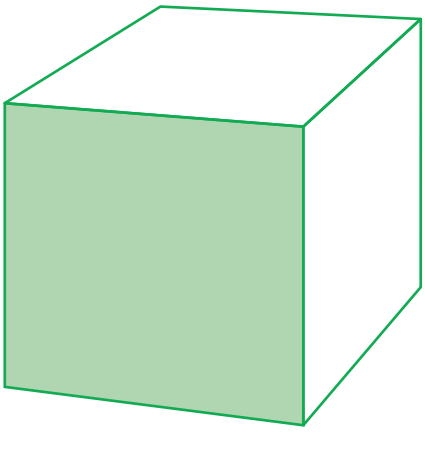

Figure 1.3 $[0, 1]^3$

Example 4. $[0, 1] \times [0, 1] \times [0, 1] \times [0, 1] = [0, 1]^4$ is the four-dimensional cube or tesseract. Draw it by "pulling out" the three-dimensional cube. See T. Banchoff [6]. Figure 1.4 below shows the edges and vertices of the four-dimensional cube or tesseract (actually more of

a 4-rectangular solid) as drawn by Mathematica. Of course both Figures 1.3 and 1.4 are really projections of the cube and hypercube onto the plane. ▲

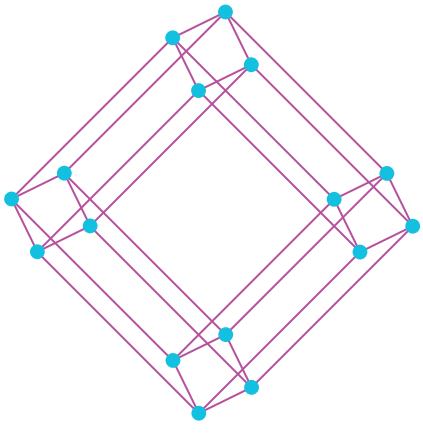

Figure 1.4 Graph representing the hypercube $[0, 1]^4$

Exercise 1.2.4 *Show that* $A \times (B \cap C) = (A \times B) \cap (A \times C)$. *Does the same equality hold when you replace* $\cap$ *with* $\cup$?

Exercise 1.2.5 *State whether the following set-theoretic equalities are true or false and give reasons for your answers.*

(a) $\{2, 5, 7\} = \{5, 2, 7\}$.
(b) $\{(2, 1), (2, 3)\} = \{(1, 2), (3, 2)\}$.
(c) $\emptyset = \{0\}$.

Exercise 1.2.6 *Prove the following set-theoretic identities:*

(a) $(A - C) \cap (B - C) = (A \cap B) - C$;
(b) $A \times (B - C) = (A \times B) - (A \times C)$.

1.3 The Integers

Notation.

$\mathbb{Z}^+$	$\{1, 2, 3, 4, \ldots\}$	the positive integers
$\mathbb{Z}$	$\{0, \pm 1, \pm 2, \pm 3, \ldots\}$	the integers

We assume that you have been familiar with the basic facts about the integers since childhood. Despite that familiarity, we must list the 10 basic axioms for $\mathbb{Z}$ in order to be able to prove anything about $\mathbb{Z}$. By an axiom, we mean a basic unproved assumption. We must deduce everything we say about $\mathbb{Z}$ from our 10 axioms – forgetting what we know from elementary school. In Section 5.3 we will find that much of what we do here – especially in the pure algebra part (R1 to R6) – works for any integral domain and not just $\mathbb{Z}$. Sometimes $\mathbb{Z}^+$ or $\mathbb{Z}^+ \cup \{0\}$ is referred to as the "**natural numbers**." This seems somewhat prejudicial to the other types of numbers one may use and so we will try to avoid that terminology.

Algebra Axioms for $\mathbb{Z}$

For every $n, m \in \mathbb{Z}$ there is a unique integer $m+n$ and a unique integer $n \cdot m$ such that the following laws are valid for all $m, n, k \in \mathbb{Z}$. This says the set of integers is **closed** under addition and multiplication.

R1 **Commutative laws:** $m+n=n+m$ and $m \cdot n = n \cdot m$.
R2 **Associative laws:** $k+(m+n)=(k+m)+n$ and $k \cdot (m \cdot n) = (k \cdot m) \cdot n$.
R3 **Identities:** There are two special elements of $\mathbb{Z}$, namely
0 (identity for addition) and 1 (identity for multiplication) in $\mathbb{Z}$
such that $0+n=n$, $1 \cdot n = n$, for all $n \in \mathbb{Z}$, and $0 \neq 1$.
R4 **Inverse for addition:** For every $m \in \mathbb{Z}$ there exists an element
$x \in \mathbb{Z}$ such that $m+x=0$. Write $x=-m$, once you know x is unique.
R5 **Distributive law:** $k \cdot (m+n) = k \cdot m + k \cdot n$.
R6 **No zero divisors:** $m \cdot n = 0$ implies either m or n is 0.

We sometimes write $n \cdot m = n * m = nm$. Thanks to the associative laws, we can leave out parentheses in sums like $k+m+n$ or in products like kmn. Of course we still need those parentheses in the distributive law.

As a result of axioms R1–R5, we say that $\mathbb{Z}$ is a "commutative ring with identity for multiplication." As a result of the additional axiom R6 we say that $\mathbb{Z}$ is an "integral domain." Rings will be the topic for the last half of this book – starting with Chapter 5.

Exercise 1.3.1

(a) Show that the identities 0 and 1 in R3 are unique.
(b) Show that the inverse x of the element m in R4 is unique once m is fixed.

Exercise 1.3.2 *Show that $a \cdot 0 = 0$ for any $a \in \mathbb{Z}$.*

Exercise 1.3.3 *In axiom R4, we can write $1+u=0$ and then define $u=-1$. Show that then, for any $m \in \mathbb{Z}$, if x is the integer such that $m+x=0$, we have $x=(-1) \cdot m$. Thus $x=-m=(-1) \cdot m$. Prove that $-(-m)=m$.*

Exercise 1.3.4 ***(Cancellation Laws).*** *Show that if $a, b, c \in \mathbb{Z}$, then we have the following laws.*
(a) If $a+b=a+c$, then $b=c$.
(b) If $a \neq 0$ and $ab=ac$, then $b=c$.

Exercise 1.3.5 *Prove the other distributive law: $(m+n) \cdot k = m \cdot k + n \cdot k$.*

Exercise 1.3.6 *Prove that for any $a, b \in \mathbb{Z}$ we can solve the equation $a+x=b$ for $x \in \mathbb{Z}$.*

Additional axioms for $\mathbb{Z}$ involve the ordering $<$ of $\mathbb{Z}$ which behaves well with respect to addition and multiplication. The properties of inequalities can be derived from three simple axioms for the set $P=\mathbb{Z}^+$ of positive integers.

Order Axioms for $\mathbb{Z}$

O1 $\mathbb{Z} = P \cup \{0\} \cup (-P)$, where $-P = \{-x | x \in P\}$. Moreover this is a disjoint union. That is,

$$0 \notin P, \quad 0 \notin -P, \quad P \cap (-P) = \emptyset.$$

O2 $n, m \in P \Longrightarrow n + m \in P$.
O3 $n, m \in P \Longrightarrow n \cdot m \in P$.

As a result of the nine axioms R1–R6 and O1–O3, we say that $\mathbb{Z}$ is an **ordered integral domain**. There is still one more axiom needed to define $\mathbb{Z}$, but we discuss this below – after saying more about the order relation $a < b$.

Definition 1.3.1 *If $a, b \in \mathbb{Z}$ we say that $a < b$ (b is **greater than** a or a is **less than** b) iff $b - a \in P = \mathbb{Z}^+$. One can also write $b > a$ in this situation.*

Examples. By this definition, the set P consists of integers that are greater than 0. We can see that $0 < 1$ since otherwise, by O1, $0 < -1$. But then, according to axiom O3 it follows that $(-1)(-1) = 1 \in P$. This contradicts $P \cap (-P) = \emptyset$.

It follows from our axioms that $P = \mathbb{Z}^+ = \{1, 2, 3, 4, \ldots\}$, using O2 and the last axiom (well-ordering) which we are about to state. This axiom will allow us to prove infinite lists of statements by checking two items (mathematical induction). See Exercise 1.3.13. ▲

We can use our axioms to prove the following facts about order.

Facts about Order. $\forall\ x, y, z, c \in \mathbb{Z}$

(1) **Transitivity.** $x < y$ and $y < z$ implies $x < z$.
(2) **Trichotomy.** For any $x, y, z \in \mathbb{Z}$ exactly one of the following inequalities is true:

$$x < y, \quad y < x, \quad \text{or} \quad x = y.$$

(3) **Addition.** $x < y$ implies $x + z < y + z$ for any $z \in \mathbb{Z}$.
(4) **Multiplication by a positive number.** If $0 < c$ and $x < y$, then $cx < cy$.
(5) **Multiplication by a negative number.** If $c < 0$ and $x < y$, then $cy < cx$.

Proof. We will leave most of these proofs to the reader as an exercise. But we will do (1) and (3).
Fact (1): $x < y$ means $y - x \in P$. $y < z$ means $z - y \in P$. Then by O2 and the axioms for arithmetic in $\mathbb{R}$, we have $y - x + z - y = z - x \in P$. This says $x < z$.
Fact (3): Since $x < y$ we know that $y - x \in P$. Then $(y + z) - (x + z) = y - x \in P$ which is what we needed to show. ▲

More Definitions. Of course we will write $a \leq b$ if either $a = b$ or $a < b$. We may also write $b \geq a$ in this case.

Exercise 1.3.7 *Prove the rest of the facts about order.*