Numbers and Polynomials

Notes for a course, Third edition

Kermit Sigmon
Department of Mathematics
University of Florida, Gainesville

Department of Mathematics • University of Florida • Gainesville, FL 32611
revised June 2001, corrections Nov 2005

Preface to Second Edition

The mathematics you will learn in this course is part of what every mathematically mature person should know. The course is designed neither for learning computational skills nor for learning many "facts" about number systems and polynomials over these number systems. It is rather to provide you with the opportunity to examine the "structure" of these systems and to learn the art of careful mathematical reasoning. It is expected that this experience will help you in the linear algebra (MAS 4105) and abstract algebra (MAS 4301) courses which most of you will subsequently take.

You are expected to work through the notes, proving the theorems and working the exercises. Collaboration between class members in this regard is fine, indeed encouraged, but keep in mind that independent work builds self-confidence. You should work ahead to the extent that you have worked through the material *prior* to its discussion in class. In this way, you can compare your work with that discussed in class and develop a confidence that you can independently attack a question. This is a do-it-yourself course in which you are expected to take your turn presenting your work to the class and to actively participate in class discussion.

To give you this opportunity for independent discovery, the notes contain neither proofs of the theorems, nor solutions to the exercises. It is important, therefore, for you to keep a carefully organized record of such obtained from your work as modified after class discussion; a ring-binder is suggested for this. The process of carefully rewriting your notes after class discussion is an important part of the learning process in the course. Answers to exercises marked with an asterisk, '$*$', are at the end of the notes.

Enjoy yourself!

Kermit Sigmon
Department of Mathematics
University of Florida
(5-96)

[0]Thanks go to all the instructors of the course whose many suggestions which have improved these notes.

[0]These notes were typeset using TEX. Thanks go to Jean Larson for creating the figures in Chapter 6 with TEX.

[0]These notes were revised in 1999.

Introduction

We adopt the viewpoint that the real number system is known. More specifically, we will assume the existence of a set $\mathbb{R}$, the real numbers, equipped with two binary operations "$+$" and "$\cdot$" satisfying certain axioms and an order relation "$<$" satisfying further axioms. You are to deduce (prove) properties of the real numbers from these axioms — and these axioms alone.

The natural numbers, integers, rational numbers, and irrational numbers will be defined as certain distinguished subsets of the real numbers. Their properties will be deduced, therefore, from properties of the real numbers. The complex numbers will be constructed from the real numbers and their properties deduced from properties of the real numbers. Finally, the notion of a polynomial over a number system will be built on properties of the number system. Thus, all "truth" about these number systems and polynomials over them ultimately has its source in the algebraic and order axioms for the real numbers which we will assume.

An alternate approach to the development of these number systems, which we do not adopt, is to first assume the existence of the natural numbers (or even more primitively, the Peano axioms). One then constructs successively the integers, rational numbers, real numbers, and complex numbers. This route presents considerable technical difficulty, especially in building the reals from the rationals. We choose the first approach because it permits one to focus on the central properties of the number systems with a minimum of distractions.

Contents

1. Algebraic Properties of the Real Numbers

1.1 Axioms (Algebraic Axioms for the Real Numbers ("Field Axioms")). We assume that the real numbers consists of a set $\mathbb{R}$ equipped with two binary operations " $+$ " and " $\cdot$ " satisfying the following axioms:

AC (Commutativity of Addition)
$$a + b = b + a \text{ for all } a, b \in \mathbb{R}.$$

AA (Associativity of Addition)
$$a + (b + c) = (a + b) + c \text{ for all } a, b, c \in \mathbb{R}.$$

AID (Existence of Additive Identity) There is a number $0 \in \mathbb{R}$ satisfying
$$a + 0 = a = 0 + a \text{ for all } a \in \mathbb{R}.$$

AIV (Existence of Additive Inverses) Corresponding to each $a \in \mathbb{R}$, there is a unique number $-a \in \mathbb{R}$ satisfying
$$a + (-a) = 0 = (-a) + a.$$

MC (Commutativity of Multiplication)
$$ab = ba \text{ for all } a, b \in \mathbb{R}.$$

MA (Associativity of Multiplication)
$$a(bc) = (ab)c \text{ for all } a, b, c \in \mathbb{R}.$$

MID (Existence of Multiplicative Identity) There is a number 1 (different from 0) in $\mathbb{R}$ satisfying
$$1a = a = a1 \text{ for all } a \in \mathbb{R}.$$

MIV (Existence of Multiplicative Inverses) Corresponding to each a (except 0) in $\mathbb{R}$, there is a unique number $a^{-1} \in \mathbb{R}$ satisfying
$$aa^{-1} = 1 = a^{-1}a.$$

D (Distributivity)
$$a(b + c) = ab + ac \text{ and } (a + b)c = ac + bc \text{ for all } a, b, c \in \mathbb{R}.$$

1.2 Remark. Some other basic facts will be used in proofs without being formally stated here and without citation (except as needed to clarify the exposition). These can be divided into two categories:

1. **Laws of logic.**

2. **Laws of equality.** First, we have three basic axioms: For all a, b and c we have (i) $a = a$, (ii) if $a = b$ then $b = a$, and (iii) if $a = b$ and $b = c$ then $a = c$. In addition there is a general principle which we may call *substitution of equals*, stating that if $a = b$ then we may freely substitute the symbol b for a in any expression. Thus, if $a = b$ and $c = d$ then $a + c = b + d$ and $ac = bd$. The principle here is that $a = b$ means that the symbols a and b are *names for the same object*. All of the properties with which we are concerned are properties of the underlying object, not of the name, and hence are unaffected by the name we happen to use for the object.

1.3 Definition/Remark. A *binary operation* on a set S is a function that assigns to every ordered pair of elements of S a unique element of S. Familiar examples of binary operations on $\mathbb{R}$ are ordinary addition, subtraction, and multiplication. In particular, if we write $a+b = c$, we are assigning the real number c (the "answer") to the ordered pair (a, b) of real numbers.

One immediate consequence of this definition is the familiar "equals added to equals are equal". In other words, if $a = b$ and $c = d$, then $a + c = b + d$. The justification for this is that our binary operation of addition assigns to the ordered pair (a, c) some real number e, let's say. But since $a = b$ and $c = d$, the ordered pair (b, d) is the *same* ordered pair as (a, c), and since the operation of addition assigns a *unique* number e to this ordered pair, we must have $b + d = e$. But since $a + c = e$ we have $a + c = b + d$. In summary, we can say that the definition of binary operation justifies the implication that if $a = b$ and $c = d$, then $a + c = b + d$. Similar considerations apply to subtraction, multiplication, and division.

We will use the familiar rule that multiplication takes precidence over addition, so that $ab + cd$ means $(ab) + (cd)$.

1.4 Theorem. *Suppose $a, b, c, d \in \mathbb{R}$. Then*

a). *If $a + c = b + c$, then $a = b$.*

b). *The additive identity is unique.*
That is, if $e \in \mathbb{R}$ and $a + e = a = e + a$ for all $a \in \mathbb{R}$, then $e = 0$.

c). *If $ac = bc$ and $c \neq 0$, then $a = b$.*

d). *The multiplicative identity is unique.*
That is, if $e \in \mathbb{R}$ and $a \cdot e = a = e \cdot a$ for all $a \in \mathbb{R}$, then $e = 1$.

e). *$(a + b) + (c + d) = (a + c) + (b + d)$ and $(ab)(cd) = (ac)(bd)$.*

f). *$a0 = 0 = 0a$.*

g). *If $ab = 0$, then $a = 0$ or $b = 0$.*

h). *$(-1)a = -a$.*

i). *$-(-a) = a$ and $-(a + b) = (-a) + (-b)$.*
Warning: You cannot use the identity "$(-1)(-1) = 1$" in the proof of clause (i), since you will not have proved it until clause (j).

j). $a(-b) = -(ab) = (-a)b$ *and* $(-a)(-b) = ab$.

k). If $a \neq 0$, *then* $a^{-1} \neq 0$.

l). If $a \neq 0$, *then* $(a^{-1})^{-1} = a$; *also if* $a \neq 0$ *and* $b \neq 0$, *then* $(ab)^{-1} = a^{-1}b^{-1}$.

1.5 Theorem. *Suppose* $a, b \in R$.

a). The equation $b + x = a$ *has one and only one solution.*

b). If $b \neq 0$, *then the equation* $bx = a$ *has one and only one solution.*

1.6 Definition. We define subtraction and division as follows.

a). For $a, b \in \mathbb{R}$, $a - b$ denotes that number x such that $b + x = a$.

b). For $a, b \in \mathbb{R}$ with $b \neq 0$, $\dfrac{a}{b}$ denotes that number x such that $bx = a$.

1.7 Theorem. *Suppose* $a, b, c, d \in R$.

a). $a - b = a + (-b)$; *also, if* $b \neq 0$, *then* $\dfrac{a}{b} = ab^{-1}$.

b). $a(b - c) = ab - ac$ *and* $-(a - b) = b - a$.

c). If $a \neq 0$, *then* $\dfrac{1}{a}$ *is the multiplicative inverse of* a .

d). $\dfrac{a}{1} = a$; *also, if* $a \neq 0$, *then* $\dfrac{a}{a} = 1$.

e). If $b \neq 0$, *then* $\dfrac{-a}{b} = \dfrac{a}{-b} = -\left(\dfrac{a}{b}\right)$ *and* $\dfrac{-a}{-b} = \dfrac{a}{b}$.

f). If $b \neq 0$ *and* $d \neq 0$, *then* $\dfrac{a}{b}\dfrac{c}{d} = \dfrac{ac}{bd}$.

g). If $b \neq 0$, $c \neq 0$ *and* $d \neq 0$, *then* $\dfrac{\frac{a}{b}}{\frac{c}{d}} = \dfrac{ad}{bc}$.

h). If $b \neq 0$ *and* $d \neq 0$, *then* $\dfrac{a}{b} + \dfrac{c}{d} = \dfrac{ad + bc}{bd}$.

1.8 Exercise. (Limitations on definitions, axioms)

a). Explain **why**, in Definition 1.6, $\dfrac{a}{b}$ was not given meaning when $b = 0$.

b). Explain why, in **MID**, one would wish to require that $1 \neq 0$ by showing that, if not, then $\mathbb{R} = \{0\}$.

c). Explain **why**, in **MIV**, one would not wish to require that 0 have a multiplicative inverse.

1.9 Exercise. (Redundancy of axioms)

a). Show that Axiom **AC** is redundant; i.e., it can be proved from the other axioms. [Hint: Expand $(1+1)(a+b)$ in two ways]

b). Show that the uniqueness of the additive inverse in Axiom **AIV** is redundant; i.e., show from the other axioms that $a \in \mathbb{R}$ has at most one additive inverse.

c). Show that the uniqueness of the multiplicative inverse in Axiom **MIV** is redundant; i.e., show from the other axioms that a non-zero $a \in \mathbb{R}$ has at most one multiplicative inverse.

1.10 Exercise. Show that for $a, b, c, d \in R$, one has

a). $(a+b)(c+d) = (ac+ad)+(bc+bd)$

b). $(a+b)^2 = a^2+(2ab+b^2)$ and $a^2-b^2 = (a-b)(a+b)$ ($a^2 := aa$, $b^2 := bb$, $2ab := ab+ab$).

1.11 Notation. $A := B$ means that the new symbol "A" is defined by "B".

1.12 Remark. This illustrates how one deduces a few of the familiar algebraic properties of $\mathbb{R}$ from the axioms. You may henceforth use any other (valid!) ones as long as you can verify them upon demand. In view of the commutative and associative properties you may also omit parenthesis; e.g., $a^2+(2ab+b^2) = a^2+2ab+b^2$, etc.

1.13 Axioms (Order Axioms for the Real Numbers). We assume that there is a binary relation " $<$ " on $\mathbb{R}$ satisfying the following axioms:

OTC (Trichotomy)
For any $a, b \in R$, exactly one of $a < b$, $a = b$, and $b < a$ holds.

OTR (Transitivity)
If $a < b$ and $b < c$, then $a < c$.

OA (Compatibility with Addition)
If $a < b$, then $a + c < b + c$.

OM (Compatibility with Multiplication)
If $a < b$ and $0 < c$, then $ac < bc$.

The axioms above, together with those in 1.1, assert that the reals are an example of what is known as an *ordered field*. One more axiom will be presented later as Axiom 4.7. With this axiom, the *least upper bound axiom* (**LUB**), the reals are a *complete ordered field*.

1.14 Notation. "$a > b$" means "$b < a$", "$a \leq b$" means "$a < b$ or $a = b$", etc.

1.15 Theorem. *Suppose $a, b, c \in \mathbb{R}$. Then*

a). If $a > 0$ and $b > 0$, then $a + b > 0$.

b). If $a < b$, then $-a > -b$.

c). If $a < b$ and $c < 0$, then $ac > bc$.

d). $a > 0, b > 0$ imply $ab > 0$; $a > 0, b < 0$ imply $ab < 0$; and $a < 0, b < 0$ imply $ab > 0$.

e). $ab > 0$ implies that either $a > 0$ and $b > 0$ or else $a < 0$ and $b < 0$.

f). $0 < 1$.

g). $a - 1 < a < a + 1$.

h). Suppose $a \neq 0$. Then $a > 0$ iff $\dfrac{1}{a} > 0$.

i). Suppose $b \neq 0$. Then $\frac{a}{b} > 0$ iff either $a > 0$ and $b > 0$ or $a < 0$ and $b < 0$.

j). Suppose a and b are either both positive or both negative. Then $a < b$ iff $\dfrac{1}{a} > \dfrac{1}{b}$.

k). If $a^2 < b^2$ and $a, b \geq 0$, then $a < b$.

1.16 Exercise. Prove or disprove each of the following.

a). If $a < b$ and $c < d$, then $a + c < b + d$.

b). If $a < b$ and $c < d$, then $ac < bd$.

c). Formulate true versions of the statements you disproved.

1.17 Theorem. *Suppose $a, b \in \mathbb{R}$. Then*

a). If $a^2 = b^2$ and $a, b \geq 0$, then $a = b$.

b). If $a^3 = b^3$, then $a = b$ ($a^3 := a^2 a$).

1.18 Exercise. Suppose $a, b \in \mathbb{R}$ (and $2 := 1 + 1$). Show that:

a). If $a < b$, then $a < \dfrac{a+b}{2} < b$. (Arithmetic mean)

b). If $0 < a < b$, then $a < \sqrt{ab} < b$. (Geometric mean) [You may assume 4.16.]

c). If $0 < a < b$, then $a < \dfrac{2}{\frac{1}{a} + \frac{1}{b}} < b$. (Harmonic mean)

1.19 Definition. The absolute value of a number a in $\mathbb{R}$ is:

$$|a| := \begin{cases} a & \text{if } a \geq 0 \\ -a & \text{if } a < 0. \end{cases}$$

Geometrically, we can think of the absolute value $|a|$ as giving the length of the line segment of the number line whose ends are a and 0. The definition by cases given above enables us to use algebra, e.g. $|-1| := -(-1)$ by definition, and hence $|-1| = 1$ by 1.4i)

1.20 Theorem. *Suppose that $a, b, c, \in \mathbb{R}$. Then*

a). $|a| \geq 0$.

b). $|-a| = |a|$ and $|b - a| = |a - b|$.

c). $|a|^2 = a^2 \geq 0$.

d). $-|a| \leq a \leq |a|$.

e). For $c \geq 0$, $|a| \leq c$ iff $-c \leq a \leq c$.

f). $|ab| = |a||b|$, and if $b \neq 0$ then $\left|\dfrac{a}{b}\right| = \dfrac{|a|}{|b|}$. [Hint: Consider using clause (c).]

g). $|a + b| \leq |a| + |b|$ (Triangle inequality).

h). $|a - b| \geq ||a| - |b||$.

i). $|a - c| \leq |a - b| + |b - c|$.

The importance of the notion of absolute value lies in the fact that $|a-b|$ gives the distance between points a and b on the real number line independent of their order.

1.21 Exercise. Solve the following inequalities, using ordinary arithmetic on real numbers.

a). $|x + 1| > 6$.

b). $|1 - 4x| = 13$.

c). $|2x - 9| \leq 1$.

d). $|2x + 1| = x - 4$.

e). $x^2 - x - 6 > 0$.

f). $\dfrac{x-1}{x+1} < 1$.

2. The Natural Numbers Induction

2.1 Notation. We use the notation $a \in B$ to mean that B is a set, and a is a member of that set. We write $A \subset B$ to mean that A is a subset of B, that is, $\forall x\,(x \in A \implies x \in B)$. Thus if A and B are two sets then $A = B$ if and only if $A \subset B$ and $B \subset A$.

2.2 Definition. We introduce a new symbol $\mathbb{N}$. Intuitively, $\mathbb{N}$ will be the set of *natural* numbers, $\mathbb{N} = \{0, 1, 2, \dots\}$. As we all know, every natural number is also a real number, that is, $\mathbb{N}$ is a subset of the real numbers. We will introduce three new axioms for the natural numbers:

1. Every member of $\mathbb{N}$ is a member of $\mathbb{R}$.
2. (a) $0 \in \mathbb{N}$
   (b) $n + 1 \in \mathbb{N}$ for all numbers $n \in \mathbb{N}$.
   (c) $n - 1 \in \mathbb{N}$ for all $n \in \mathbb{N}$ such that $n \neq 0$.
3. (The well ordering Principle **WO**). Every nonempty subset of $\mathbb{N}$ has a least member. That is, if A is a set with at least one member, such that every member of A is in $\mathbb{N}$, then there is some number $n \in A$ such that $m \notin A$ for all $m < n$.

2.3 Theorem. *1. If n is any member of $\mathbb{N}$ then $n \geq 0$. (*Hint: *$\mathbb{N}$ is a nonempty subset of $\mathbb{N}$, and hence has a least member by **WO**.)*

2. If n is any member of $\mathbb{N}$, and $a \in R$ satisfies $n < a < n + 1$, then $a \notin \mathbb{N}$.

2.4 Exercise. Suppose that $\mathbb{N}'$ is a subset of the real numbers which also satisfies the axioms for $\mathbb{N}$. Show that $\mathbb{N}' = \mathbb{N}$.
*Hint: Show that every member of $\mathbb{N}$ is in $\mathbb{N}'$ by assuming the contrary and applying axiom **WO** to $A = \mathbb{N} \setminus \mathbb{N}' = \{n : n \in \mathbb{N}$ and $n \notin \mathbb{N}'\}$ to get a contradiction. Then use the same argument, applying **WO** for $\mathbb{N}'$, to show that every member of $\mathbb{N}'$ is in $\mathbb{N}$.*

2.5 Definition. The set of *integers* $\mathbb{Z}$ is defined by $\mathbb{Z} := \mathbb{N} \cup \{\, -n \mid n \in \mathbb{N} \,\}$. (Intuitively $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$.)

2.6 Theorem. *(Connections between $\mathbb{N}$ and $\mathbb{Z}$)*

a). A number n is in $\mathbb{N}$ if and only if $n \in \mathbb{Z}$ and $n \geq 0$.

b). If $z \in \mathbb{Z}$, then $|z| \in \mathbb{N}$.

Since $\mathbb{N} \subset \mathbb{R}$, all of the operations defined on members of $\mathbb{R}$ are automatically defined on members of $\mathbb{N}$. However they are not all defined as *operations on* $\mathbb{N}$, since the result of the operation may not be in $\mathbb{N}$. Thus, for example, $1 - 2 \notin \mathbb{N}$ even though 1 and 2 are in $\mathbb{N}$, and $1/2$ is not even in $\mathbb{Z}$. Hence some of the "Field Axioms" from 1.1 are not true in $\mathbb{N}$: for example, **MIV** is not true in $\mathbb{N}$, since there is no number 2^{-1} *in* $\mathbb{N}$ such that $2 \cdot 2^{-1} = 1$. On the other hand, many of the Field axioms automatically hold in $\mathbb{N}$ because they hold in $\mathbb{R}$: for example, **AC** is true because if n and m are any two members of $\mathbb{N}$ then definition 2.2(1) implies that n and m are also members of $\mathbb{R}$. Since we have already assumed that **AC** holds for $\mathbb{R}$, it follows that $n + m = m + n$.

The following theorem states which operations, and which axioms, can be transfered from $\mathbb{R}$ to $\mathbb{N}$ and to $\mathbb{Z}$.

2.7 Theorem. *(Field and order axioms)*

a). $\mathbb{N}$ *is closed under addition and multiplication, that is, if* n *and* m *are any two members of* $\mathbb{N}$ *then* $n + m \in \mathbb{N}$ *and* $nm \in \mathbb{N}$.
Hint: Assume by way of contradiction that there are $n, m \in \mathbb{N}$ such that $n + m \notin \mathbb{N}$. Then the set $A = \{\, r \in \mathbb{N} : n + r \notin \mathbb{N} \,\} \subset \mathbb{N}$ is nonempty, since $m \in A$. It follows by **WO** that A has a least member. Call this least member r_0, and reach a contradiction by showing that r_0 cannot satisfy axiom 2.2(2c).

b). Each of the "Field Axioms" (see 1.1) holds in $\mathbb{N}$*, except* **AIV** *and* **MIV***; and each of the "Order Axioms"* **OTC**, **OTR**, **OA** *and* **OM** *(see 1.13) holds in* $\mathbb{N}$.
[Hint: They hold in $\mathbb{R}$*, so they hold in* $\mathbb{N}$ *as long as the relevant quantities are in* $\mathbb{N}$*].*

c). $\mathbb{Z}$ *is closed under addition and multiplication. In addition,* $\mathbb{Z}$ *is closed under additive inverse and subtraction.*
[Hint: We know the desired sums and products exist in $\mathbb{R}$*. Use Definition 2.5, a case analysis, 2.5a, and algebra to show that they must also be in* $\mathbb{Z}$*.]*

d). Each of the "Field Axioms" holds in $\mathbb{Z}$ *except* **MIV***; and each of the "Order Axioms"* **OTC**, **OTR**, **OA** *and* **OM** *(see 1.13) holds in* $\mathbb{Z}$.

The following proposition lists a few more of the familiar algebraic properties of $\mathbb{N}$ and $\mathbb{Z}$. You may want to prove some of them as intermediate results in the course of proving clauses (c) and (d) of theorem 2.7.

2.8 Theorem. *1. If* $a \in \mathbb{Z}$ *then* $a - 1 \in \mathbb{Z}$.

2. If $a, b \in \mathbb{Z}$ *then* $a - b \in \mathbb{Z}$.

3. If $z \in \mathbb{Z}$, $a \in \mathbb{R}$ *and* $z < a < z + 1$, *then* $a \notin \mathbb{Z}$.

4. The following holds in each of $\mathbb{N}$ *and* $\mathbb{Z}$: $ab = 0$ *implies* $a = 0$ *or* $b = 0$.
(Thus neither $\mathbb{N}$ *nor* $\mathbb{Z}$ *has "divisors of zero.")*

You may henceforth use any other of the familiar (valid!) algebraic properties of $\mathbb{N}$ and $\mathbb{Z}$, as long as you can verify them upon demand using algebra and order properties learned in the previous chapter.

Mathematical induction. You may have noticed that almost all proofs using the axiom **WO** are proofs by contradiction. Mathematical induction can be viewed as a positive way of giving essentially the same proof.

2.9 Lemma. *Suppose that $a \in \mathbb{N}$ and that B is a subset of $\mathbb{N}$ which satisfies the following two properties:*

a) $a \in B$, and

b) $k+1 \in B$ whenever $k \in B$ and $k \geq a$.

Then $x \in B$ for all natural numbers $x \geq a$.

Hint: Try indirect proof (i.e., proof by contradiction) using **WO**.

2.10 Theorem (First Principle of Mathematical Induction (**MI1**)). *Suppose that $a \in \mathbb{N}$ and that, for each natural number $n \geq a$, Φ_n is a statement associated with n. Suppose further that the statements Φ_n satisfy the following two properties:*

a) Φ_a is true.

b) If k is any natural number with $k \geq a$, and Φ_k is true, then Φ_{k+1} is also true.

Then Φ_n holds for each natural number $n \geq a$.

2.11 Theorem (Second Principle of Mathematical Induction (**MI2**)). *Suppose for each natural number n, Φ_n is a statement associated with n and the statements Φ_n have the following property:*

a) If Φ_k is true whenever Φ_j holds for all natural numbers $j < k$, then Φ_n holds for all natural numbers n.

Hint: One way to prove this is to let Ψ_k be the statement that "Φ_j is true for all $j < k$", and apply **MI1** to the statements Ψ_k.

Notice that, although **MI2** does not have an explicit base case, it does have an implicit one which will often—but not always—need to be treated as a special case. If $k = 0$ then the condition "Φ_j holds for all natural numbers $j < k$" is true for the trivial reason that there *are* no natural numbers $j < k$. Hence proving clause 2.11(a) for given statements Φ_n will always require proving Φ_0, without any (nontrivial) assumptions.

Sample proofs using MI1.

2.12 Theorem. *If x is any real number greater than -1 and n is any natural number greater than 0 then $(1+x)^n \geq 1+nx$.*

Proof. Fix an arbitrary real number $x > -1$. Let Φ_k be the statement

$$(1+x)^k \geq 1+kx. \qquad (\Phi_k)$$

We use **MI1** (with $a = 1$) to prove by induction on k that Φ_k holds for all $k \in \mathbb{N}$ with $k \geq 1$.

1. For $k = 1$ we have $(1 + x)^k = 1 + x = 1 + kx$ so $(1 + x)^k \geq 1 + kx$. Hence Φ_1 holds.

2. Suppose that Φ_k is true. Then $(1 + x)^{k+1} = (1 + x)(1 + x)^k$. But $1 + x > 0$ since $x > -1$, and $(1 + x)^k \geq 1 + kx$ by Φ_k. Thus by **OM** we have $(1 + x)^{k+1} = (1 + x)(1 + x)^k \geq (1 + x)(1 + kx) = 1 + (k + 1)x + kx^2$. But $kx^2 > 0$ since $k > 0$ and $x > 0$, so $(1 + x)^{k+1} \geq 1 + (k + 1)x$. This is just Φ_{k+1} so, we have shown that Φ_k implies Φ_{k+1}.

By **MI1**, (1) and (2) implies that Φ_k holds for all natural numbers $k > 0$. ⊣

What about the following proof by mathematical induction?

2.13 Theorem(?). All horses have the same color.

Proof. Let Φ_k, for $k \geq 1$ a natural number, be the statement that in any herd H of exactly k horses, every horse in H has the same color. We will apply **MI1** with $a = 1$ to show that Φ_k holds for all $k \geq 1$.

1. If a herd H has only one horse, then H can't have horses of different colors. Thus Φ_1 holds.

2. Suppose Φ_k holds. Since $k + 1 \geq 2$ we can choose two horses h_1 and h_2 from H. Consider the two herds H_1, obtained by removing h_2 from H, and H_2 obtained by removing h_1 from H. Each of these herds has k members, so by the induction hypothesis Φ_k any two horses, both from H_1 or both from H_2, have the same color. Thus any two horses in

H, with the possible exception of the pair (h_1, h_2), have the same color. Thus we will have finished the induction step if we can show that h_1 and h_2 have the same color. To this end, pick any horse in the herd other than h_1 and h_2. Call this horse Misty. Then Misty has the same color as h_1 because both h_1 and Misty are members of H_1. Similarly, Misty has the same color as h_2 because they are both members of H_2. But then h_1 and h_2 both have the same color as Misty. Since H was arbitrary, we have shown that Φ_k implies Φ_{k+1}.

By (1), (2) and **MI1** we conclude that Φ_k holds for all natural numbers $k \geq 1$. Hence all horses have the same color.[1] ⊣

2.14 Exercise. Use mathematical induction to show that, for each positive integer n,

a). If $0 \leq a < b$, then $a^n < b^n$.

b). $1 + 2 + 3 + \cdots + n = \dfrac{n(n + 1)}{2}$.

c). $1 + 3 + 5 + \cdots + (2n - 1) = n^2$.

[1] Here is the rest of the story:

THEOREM: All horses have an infinite number of legs. *Proof* (by intimidation) Everyone would agree that all horses have an even number of legs. It is also well-known that horses have fore-legs in front and two legs in back. But $4 + 2 = 6$ legs is certainly an odd number of legs for a horse to have! Now the only number that is both even and odd is infinity; therefore all horses have an infinite number of legs. However, suppose that there is a horse somewhere that does not have an infinite number of legs. Well, that would be a horse of a different color; and by the Lemma, it doesn't exist. QED

d). $1 + 2^2 + 3^2 + \cdots + n^2 = \dfrac{n(n+1)(2n+1)}{6}$.

e). $1 + 2^3 + 3^3 + \cdots + n^3 = \dfrac{n^2(n+1)^2}{4}$.

f). (a) $1 \cdot 2 + 2 \cdot 3 + \cdots + n(n+1) = n(n+1)(n+2)/3$

(b) $1 \cdot 2 \cdot 3 + 2 \cdot 3 \cdot 4 + \cdots + n(n+1)(n+2) = n(n+1)(n+2)(n+3)/4$

(c) Find and prove the next statement in the series above.

(d) Find and prove the k^{th} statement in the series above, for any natural number k.

g). if $n \geq 4$, then $2^n < n!$. ($n! := 1 \cdot 2 \cdot 3 \cdot \cdots \cdot n$).

2.15 Exercise. 1. Let $F_0 := 1, F_1 := 1, F_2 := 1 + 1 = 2, F_3 := 1 + 2 = 3, \ldots$; in general, let $F_{n+1} := F_{n-1} + F_n$. This sequence lists the Fibonacci numbers. Show that for all natural numbers n, $F_n \leq 2^n$.

2. Define by recursion a sequence b_n as follows:

$$\begin{aligned} b_0 &= 0; \\ b_1 &= 3; \\ b_n &= 7b_{n-1} - 10b_{n-2} \text{ for } n > 1. \end{aligned}$$

Use MI2 to prove that for all natural numbers n, $b_n = 5^n - 2^n$.

2.16 Exercise. Use mathematical induction to show that, for each natural number n,

a). $n \leq 1$ or n has a prime factor.
You may use the following facts, which will be proved later: a natural number $n > 1$ is prime iff it has no factors other that itself and 1; if d is any factor of n (other than 1 or n) then $d < n$; and if d' is a factor of d, and d is a factor of n, then d' is a factor of n.

b). n has a binary expansion,

$$n = \sum_{i=0}^{\infty} a_i 2^i,$$

where each a_i is either 0 or 1 and $a_i = 0$ for all but finitely many $i \in N$.
*Hint: One way to do this is by **MI2**: if n is odd then you can get an expansion of n from an expansion of $n-1$, while if n is even you can get an expansion of n from that of $n/2$. You may assume without proof that every natural number n is either even or odd.*

c). n has a ternary expansion,

$$n = \sum_{i=0}^{\infty} a_i 3^i,$$

where each a_i is either 0, 1 or 2, and $a_i = 0$ for all but finitely many $i \in N$.

d).

$$(1-r)(1+r^1+\cdots+r^n)=1-r^{n+1}.$$

(Recall that $r^0=1$.)

e). the nth partial sum of the geometric series is

$$S_n := \sum_{i=0}^{n} ar^i = \frac{a(1-r^{n+1})}{(1-r)}.$$

3. Elementary Number Theory

3.1 Definition. For $a, b \in \mathbb{Z}$, we say a *divides* b (in symbols; $a|b$) if there exists a $c \in \mathbb{Z}$ such that $b = ac$. In this case, we say that a is a *divisor* of b, that a is a *factor* of b and that b is a *multiple* of a.

3.2 Theorem. *Suppose* $a, b, c \in \mathbb{Z}$.

a). $1|a$ *and* $a|0$ *for all* $a \in \mathbb{Z}$.

b). If $a|b$, *then* $ac|bc$.

c). If $a|b$ *and* $a|c$, *then* $a|(b+c)$.

d). If $a|b$, *then* $a|bc$.

e). If $a|b$ *and* $a|c$, *then* $a|(mb+nc)$ *for all* $m, n \in \mathbb{Z}$.

f). If $a|b$ *and* $b|c$, *then* $a|c$.

g). If $a \neq 0$, *then* $a|b$ *if and only if* $a^{-1}b \in \mathbb{Z}$.

h). If $a|b$ *and* $b \neq 0$, *then* $|a| \leq |b|$.

3.3 Theorem (Division Algorithm). *For* $a, b \in \mathbb{N}$ *with* $b > 0$, *there exist unique natural numbers* q *and* r *satisfying* $a = bq + r$ *and* $0 \leq r < b$.

Hint: Set $R := \{\, s \in \mathbb{N} : \exists\, q \in \mathbb{N} \text{ such that } a = qb + s \,\}$, show $R \neq \emptyset$, and apply **WO** to get a least element r.

I. Ideals, gcd's and the Euclidean Algorithm

3.4 Definition. A non-empty subset J of $\mathbb{Z}$ is called an *ideal* of $\mathbb{Z}$ if it satisfies:

(i). $x \in J, y \in J$ implies $x + y \in J$, and

(ii). $x \in J, n \in \mathbb{Z}$ implies $nx \in J$.

(What is the smallest possible ideal? The largest?)

3.5 Lemma. *If* J *is an ideal of* $\mathbb{Z}$, *then*

a). $x \in J$ *implies* $-x \in J$;

b). $0 \in J$; *and*

c). for all $x \in \mathbb{Z}$, $x \in J$ *if and only* $|x| \in J$.

3.6 Theorem. *For any $a \in \mathbb{N}$, define the set J_a by $J_a := \{ka \,|\, k \in \mathbb{Z}\}$.*

a). For any $a \in \mathbb{N}$, the set J_a is an ideal of $\mathbb{Z}$.

b). $J_0 = \{0\}$ and $J_1 = \mathbb{Z}$.

c). Suppose J is an ideal of $\mathbb{Z}$ and $a \in J \cap \mathbb{N}$. Then $J_a \subseteq J$.

d). Suppose J is an ideal of $\mathbb{Z}$. Then there exists some $b \in \mathbb{N}$, such that $J = J_b$.

Hint for d): For $J \neq \{0\}$, let $A := \{\, x \in J \mid x > 0 \,\}$. Show $A \subseteq \mathbb{N}$ and $A \neq \emptyset$; apply **WO** to get b. Then for $x \in J$, use the Division Algorithm to show $|x| \in J_b$, and use this claim to show $J \subseteq J_b$.

3.7 Definition. If $a, b \in \mathbb{N}$, then an integer c is called a *common divisor* of a and b if $c|a$ and $c|b$. If d is a common divisor of a and b such that $d \geq c$ for every common divisor of a and b, then d is called the *greatest common divisor* of a and b, and one writes $d = \gcd(a, b)$.

3.8 Theorem. *Suppose $a, b \in \mathbb{N}$ with not both a and b zero. Then there is a unique integer d such that d is the greatest common divisor of a and b.*

[Hint: Set $A := \{\, a/c : c \in \mathbb{N}, c|a \text{ and } c|b \,\}$. Show that $A \subset \mathbb{N}$ and $A \neq \emptyset$, and then apply WO to A.]

3.9 Exercise. a). Show that $\gcd(0, 0)$ does not exist.

b). Show that $\gcd(0, a) = |a|$, for all $a \neq 0$.

c). Show that if $c = \gcd(a, b)$, then $\gcd\left(\frac{a}{c}, \frac{b}{c}\right) = 1$.

3.10 Theorem. *Suppose $a, b \in \mathbb{N}$, not both zero, and set*

$$J_{a,b} := \{ka + \ell b \,|\, k \in \mathbb{Z}, \ell \in \mathbb{Z}\}.$$

a). $J_{a,b}$ is an ideal of $\mathbb{Z}$, and

b). $J_{a,b} = J_d$ where $d := \gcd(a, b)$.

[Hint (for b)): We know $J_{a,b} = J_e := \{ke \,|\, k \in \mathbb{Z}\}$ for some $e \in \mathbb{N}$ by Theorem 3.6(d). Show $e = d$.]

3.11 Corollary. *If $a, b \in \mathbb{N}$, not both zero, and $d = \gcd(a, b)$, then there exist integers x and y such that $ax + by = d$.*

3.12 Exercise. Prove or disprove:

a). $a|bc$ implies $a|b$ or $a|c$.

b). $a|c$ and $b|c$ imply $ab|c$.

3.13 Definition. Natural numbers a and b are called *relatively prime* if $\gcd(a, b) = 1$.

3.14 Theorem. *Suppose* $a, b, c \in \mathbb{N}$.

a). a and b are relatively prime iff there exist integers x and y such that $ax + by = 1$.

b). If $a|bc$ *and a and b are relatively prime, then* $a|c$.

c). If a and b are relatively prime and $a|c$ *and* $b|c$, *then* $ab|c$.

d). If each of a and b is relatively prime to c, then so is ab.

e). If $e|a$ *and* $e|b$, *then* $e|\gcd(a, b)$.

f). If $c, d, q, r \in \mathbb{N}$ *(*$d \neq 0$*) satisfy* $c = dq + r$, *then* $\gcd(c, d) = \gcd(d, r)$.

3.15 Exercise (Reduction to lowest terms). Prove that every fraction whose numerator and denominator are positive integers can be reduced to lowest terms. That is, suppose m and n are positive integers. Prove that there are positive integers k and ℓ so that k and ℓ are relatively prime and $\dfrac{m}{n} = \dfrac{k}{\ell}$.

3.16 Theorem (Euclidean Algorithm). *Suppose* $a, b \in \mathbb{N}$ *with* $b > 0$. *Then* $\gcd(a, b)$ *is the last non-zero remainder* r_k *obtained from the following applications of the division algorithm, unless* $b|a$, *in which case* $\gcd(a, b) = b$. *[Hint: 3.14f)]*

$$a = bq_1 + r_1; \qquad 0 \leq r_1 < b$$

$$b = r_1q_2 + r_2; \qquad 0 \leq r_2 < r_1$$

$$r_1 = r_2q_3 + r_3; \qquad 0 \leq r_3 < r_2$$
$$\vdots \qquad \vdots$$
$$r_{k-2} = r_{k-1}q_k + r_k; \quad 0 \leq r_k < r_{k-1}$$

$$r_{k-1} = r_kq_{k+1}.$$

[[wjm 8/23/01 — Is this clearer?]]

Consider the following algorithm, which defines a function GCD:

$$\mathrm{GCD}(a, b) = \begin{cases} a & \text{if } b = 0. \\ \mathrm{GCD}(b, r) & \text{if } a = bq + r \text{ with } 0 \leq r < |b|. \end{cases}$$

Thus, for example

$$\begin{aligned} \mathrm{GCD}(55, 15) &= \mathrm{GCD}(15, 10) && \text{since } 55 = 3 \cdot 45 + 10 \\ &= \mathrm{GCD}(10, 5) && \text{since } 15 = 1 \cdot 10 + 5 \\ &= \mathrm{GCD}(5, 0) && \text{since } 10 = 2 \cdot 5 + 0 \\ &= 5 && \text{since } b = 0. \end{aligned}$$

Show that this algorithm computes $\gcd(a, b)$. That is, show that if a, b are any two members of $\mathbb{N}$ with $a \neq 0$ then the computation of $\mathrm{GCD}(a, b)$ will eventually stop, and that the value of $\mathrm{GCD}(a, b)$ so obtained is $\gcd(a, b)$.

3.17 Exercise. Use the Euclidean algorithm to compute the gcd of the following pairs of numbers.

a). 1001, 1815

b). 391, 403

c). 4960, 9200

d). 8316, 26208

e). If you have access to a microcomputer or programmable calculator, construct a program to compute $\gcd(a, b)$ for any positive integers a and b.

f). Extend the algorithm GCD above to obtain a function xGCD such that whenever a, b are in $\mathbb{N}$ and $a \neq 0$ then $\text{xGCD}(a, b) = (x, y, d)$ where $d = \gcd(a, b)$ and $d = xa + by$.

II. Prime and Composite Numbers

3.18 Definition. A natural number greater than 1 is called

(i). *prime* if its only positive divisors are 1 and itself.

(ii). *composite* if it is not prime.

3.19 Theorem. *Suppose $a, b \in \mathbb{N}$. Then*

a). If p is prime and $p|ab$, then $p|a$ or $p|b$.

b). If $p, q_1, q_2, \ldots, q_k$ are prime and $p|q_1 q_2 \ldots q_k$, then $p = q_i$ for some i.

3.20 Definition. For a natural number $n > 1$, a product of primes $p_1 p_2 \ldots p_k$ is a *prime factorization* of n if

(i). $n = p_1 p_2 \ldots p_k$ and

(ii). $p_1 \leq p_2 \leq \cdots \leq p_k$.

3.21 Example. $21 = 3 \cdot 7, \quad 252 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 7, \quad 104 = 2 \cdot 2 \cdot 2 \cdot 13.$]
One often groups equal primes: $252 = 2^2 \cdot 3^2 \cdot 7, \quad 104 = 2^3 \cdot 13.$
So $n = {q_1}^{e_1} {q_2}^{e_2} \ldots {q_l}^{e_l}$, where $q_1 < q_2 < \cdots < q_l$ with $e_i \geq 0$.

3.22 Theorem (Fundamental Theorem of Arithmetic). *Every natural number greater than 1 has exactly one prime factorization.*

3.23 Corollary. *Every natural number greater than 1 has a prime factor.*

3.24 Theorem. *(Primes and perfect squares)*

a). If $a, b,$ and n are positive integers with $n = ab$, then either $a^2 \leq n$ or $b^2 \leq n$.

b). A natural number $n > 1$ is prime iff it has no prime divisor p with $p^2 \leq n$.

3.25 Exercise. (Prime factorizations and lists of primes)

a). Determine the prime factorization of the following natural numbers: 391, 403, 1815, 8316, 26208, 997.

b). Describe a method for finding all prime numbers up to a fixed natural number k. Apply your method for $k = 150$, $k = 500$. [Sieve of Eratosthenes]

3.26 Theorem. *(Distribution of primes)*

a). There are arbitrarily large gaps in the primes. That is, for any natural number $k > 1$, there exist k consecutive composite integers.
[Hint: $6! + 2$, $6! + 3$, $6! + 4$, $6! + 5$, $6! + 6$ are each composite.]

b). There are infinitely many prime numbers.
[Hint: Suppose not; consider $N := p_1 p_2 \dots p_k + 1$.]

3.27 Theorem. *Let $a = {p_1}^{e_1} {p_2}^{e_2} \dots {p_k}^{e_k}$ and $b = {p_1}^{f_1} {p_2}^{f_2} \dots {p_k}^{f_k}$ where $p_1, \dots, p_k$ are distinct primes and $e_i, f_i \in \mathbb{N}$ for $1 \leq i \leq k$. (Allowing $e_i = 0$ or $f_i = 0$ permits the use of the same p_i's for each of a and b). Then*

a). $a|b$ iff $e_i \leq f_i$ for each i.

b). $\gcd(a, b) = {p_1}^{m_1} {p_2}^{m_2} \dots {p_k}^{m_k}$, where $m_i = \min\{e_i, f_i\}$.

c). $\operatorname{lcm}(a, b) = {p_1}^{M_1} {p_2}^{M_2} \dots {p_k}^{M_k}$, where $M_i = \max\{e_i, f_i\}$.

In Clause c, $\operatorname{lcm}(a, b)$ is the least positive common multiple of a and b.

3.28 Exercise. Use the method of Theorem 3.27 to compute the gcd and lcm of the pairs of integers in Exercise 3.17. The results from Exercise 3.25 may help.

3.29 Remark. Although there is no known local pattern to the occurrence of the primes, it is known that they become rarer among large integers - as one would expect since more prime divisors become available. In fact, the function $\dfrac{n}{\ln(n)}$ is a global model for the distribution of the primes as the following theorem shows (we will not prove it).

3.30 Theorem (The Prime Number Theorem). *For a positive integer n, let $P(n)$ denote the number of primes not greater than n. Then*

$$\lim_{n \to \infty} \frac{P(n)}{\frac{n}{\ln(n)}} = 1.$$

4. Rational and Irrational Numbers

4.1 Definition. a). The set of *rational numbers* is the set $\mathbb{Q} := \{\frac{m}{n} \mid m, n \in \mathbb{Z}, n \neq 0\}$.

b). A real number which is not rational is called *irrational*.

4.2 Theorem. *The rational numbers $\mathbb{Q}$ are closed under addition and multiplication and satisfy all the "Field Axioms" (See 1.1) and the order axioms given in 1.13.*

I. Algebraic Irrationals

In 4.3 through 4.17, we *assume* temporarily that for each positive integer n and each $a \in \mathbb{R}$ with $a \geq 0$, there is exactly one $b \geq 0$ such that $b^n = a$; this b is denoted by $\sqrt[n]{a}$. This fact rests on the axiom LUB (4.7) and is proved for the case $n = 2$ in 4.16.

4.3 Theorem. *(Irrational square roots)*

a). $\sqrt{2}$ *is irrational.*
[Hint: Suppose not, and apply Exercise 3.15.]

b). $\sqrt{12}$ *is irrational.*

c). $\sqrt[3]{2}$ *is irrational.*

d). $\sqrt[4]{8}$ *is irrational.*

e). Suppose that $0 < n, k \in \mathbb{N}$ *and that* $\sqrt[k]{n}$ *is rational. Then there is some* $m \in \mathbb{N}$ *so that* $n = m^k$.

f). $\sqrt{2}\sqrt{3}$ *and* $\sqrt{2} + \sqrt{3}$ *are irrational.*

4.4 Exercise. Suppose $a, b \in \mathbb{R}$.

a). Suppose that $a \neq 0$ is rational and b is irrational. Can you tell whether $a+b$ is rational or irrational? What about ab?

b). Suppose that a and b are both irrational. Can you tell whether $a + b$ is rational or irrational? What about ab?

4.5 Theorem. a). *There are no* $a, b \in \mathbb{Q}$ *such that* $\sqrt[3]{2} = a\sqrt{2} + b$.

b). *If* $a(\sqrt[3]{2})^2 + b\sqrt[3]{2} + c = 0$ *with* $a, b, c \in \mathbb{Q}$, *then* $a = b = c = 0$

II. More order properties of real numbers

4.6 Definition. A number $b \in \mathbb{R}$ is an *upper bound* for a subset A of $\mathbb{R}$ if $b \geq x$ for all $x \in A$. A *lower bound* for A is defined analogously. Note that b is not an upper bound for A iff there is some $x \in A$ with $b < x$.

We now supply the missing order axiom for $\mathbb{R}$ which was promised in 1.13:

4.7 Axiom (Least Upper Bound Axiom (LUB)). Each non-empty subset A of $\mathbb{R}$ which has an upper bound has a least upper bound u. (Notation: $u = \text{lub } A$)

4.8 Example. The least upper bound of a set may be an element of that set but it need not be: for example, $\text{lub}[0,1) = \text{lub}[0,1] = \text{lub}\{1 - \frac{1}{n} \,|\, n = 1, 2, 3, \dots\} = 1$.

Here is the property for the natural numbers corresponding to LUB.

4.9 Theorem. *(**DWO**, the Order Dual of **WO**) If a non-empty subset $A \subseteq \mathbb{N}$ has an upper bound $v \in \mathbb{N}$, then it has a* greatest element *t ($t \in A$ and $a \leq t$ for all $a \in A$).*
Hint: apply **WO** to $U = \{\, u \in \mathbb{N} : u \text{ is an upper bound of } A \,\}$ to find t.

We note that the **LUB** axiom does not hold in $\mathbb{Q}$. (See 4.17)

Warning! Do not confuse **LUB** and **DWO**!

While they may at first glance appear similar, **LUB** is quite different from the **DWO**. The **DWO** is based on the **WO** and addresses the ordering of $\mathbb{N}$. It implies, among other things that the ordering of of $\mathbb{N}$: is "discrete", that is, for each natural number n there must be a next greatest one (namely the least element of $\{k \in \mathbb{N} \,|\, k > n\}$, whose existence is guaranteed by **WO**).

The **LUB**, on the other hand, addresses the ordering of $\mathbb{R}$, and implies (as noted below in 4.18) that there are *no gaps* (not even infinitely small ones) in the ordering of $\mathbb{R}$. Hence, **LUB** assures that the ordering of $\mathbb{R}$ is a continuum, just the opposite of the discrete ordering of $\mathbb{N}$ assured by WO.

4.10 Theorem. *For every real number b, there is some $n \in \mathbb{N}$ so that $b < n$. Indeed, for every real number $b \geq 0$ there is a natural number k so that $k \leq b < k + 1$.*
Hint: For the first sentence, assume the sentence is false and apply **LUB** to the set $\mathbb{N} \subset \mathbb{R}$.

4.11 Corollary (Archimedian Property). *For each $a, b \in \mathbb{R}$ with $a > 0$, there exists an integer n such that $na > b$.*

4.12 Theorem (Order Dual of LUB). *Each non-empty subset A of $\mathbb{R}$ which has a lower bound has a greatest lower bound v. [Notation: $v = \text{glb}(A)$]*

Hint: Let B be the set of lower bounds of A; apply **LUB** to B.

4.13 Exercise. Show that

a). $\lim_{n\to\infty} \frac{1}{n} = 0$; i.e., for each $\epsilon > 0$, there is an integer M such that if $n \geq M$, then $0 < \frac{1}{n} < \epsilon$. (See a calculus book for a definition of limit of a sequence.)

b). If $0 < a < 1$, then $\lim_{n\to\infty} a^n = 0$.

Hint for b): Write $\frac{1}{a} = 1 + x$ $(x > 0)$ and use 2.12.

4.14 Theorem. *Between any two distinct real numbers there is both a rational number and an irrational number – and hence infinitely many of each type.*

Hint: Consider multiples of $\frac{1}{n}$ and $\frac{\sqrt{2}}{n}$ for suitable n. Assume (though it has not yet been proven) that $\sqrt{2}$ exists.

4.15 Exercise. Use the technique of the proof of 4.14 to exhibit a rational number and an irrational number between:

a). $\sqrt{11}$ and $\sqrt{13}$.

b). $\dfrac{4}{7}$ and $\dfrac{5}{7}$.

c). 3 and $\sqrt{11}$.

Finally we show that $\sqrt{2}$ exists:

4.16 Theorem. *For each $a \in \mathbb{R}$, $a \geq 0$, there exists exactly one $b \geq 0$ such that $b^2 = a$. (This b is denoted by $\sqrt{a}$.)*

Hint: Set $u := \text{lub}(A)$, where $A := \{x \in \mathbb{R} \mid 0 \leq x^2 \leq a\}$, and show $u^2 = a$, using an indirect proof.
If $u^2 < a$, exhibit $\epsilon > 0$ such that $(u + \epsilon)^2 < a$, etc.

4.17 Theorem. *The* **LUB** *axiom does not hold in $\mathbb{Q}$.*
Hint: Consider the set $A \cap \mathbb{Q}$ (for $a = 2$) from theorem 4.16.

4.18 Remark. The set A from the hint for Theorem 4.17, paired with $B = \{\, y \in \mathbb{Q} : y \geq 0 \text{ and } y^2 > 2 \,\}$, gives one example of a "Dedekind cut". With Dedekind cuts one can more clearly see the role of **LUB** and how the rational and irrational numbers intermix. Suppose A and B are disjoint subsets of $\mathbb{Q}$ whose union is $\mathbb{Q}$ and for which $x < y$ for each $x \in A$ and $y \in B$. Such a pair (A, B) of sets is called a *Dedekind cut*. Each such pair corresponds to a real number: if either A has a greatest element r or B has a least element r, the pair (A, B) corresponds to the *rational* number r; a pair in which A has no greatest element and B has no least element corresponds to an *irrational* number. The irrational numbers can, therefore, be viewed as those numbers created to "plug the holes" between pairs of sets in Dedekind cuts of the second type. Note that **LUB** asserts the existence of numbers to "plug" all such "holes."

This is what we meant earlier when we said that **LUB** asserted that there are no gaps in the ordering of $\mathbb{R}$.

III. Decimal Expansions of Real Numbers

4.19 Remark. In 4.20 through 4.32 we explore the decimal expansion of a non-negative real number less than one – in particular the form of the expansion for a positive rational number that can be represented as a proper fraction. Since, by Corollary 4.10, every non-negative real number can be expressed as the sum of a natural number and a non-negative real number less than one, this exploration yields a lot of information about the entire set of real numbers.

In this section, formal proofs of the theorems are not expected. One should, however, be able to illustrate why Theorems 4.26, 4.27, 4.29, and 4.31 hold through an analysis of general examples.

4.20 Theorem. *If $|r| < 1$, then the geometric series $a + ar + ar^2 + \cdots + ar^n + \ldots$ converges to $\frac{a}{1-r}$.*

[Recall that "$c_1 + c_2 + c_3 + \ldots$ converges to b" means $\lim_{n\to\infty}(c_1 + c_2 + \cdots + c_n) = b$; in this case we write $b = c_1 + c_2 + c_3 + \ldots$. You may wish to consult a calculus book for the definition of the sequence of partial sums and the definition of convergence of a series.]

4.21 Definition. A *decimal expansion* of a non-negative real number $b < 1$ is a series

$$\frac{a_1}{10} + \frac{a_2}{10^2} + \cdots + \frac{a_k}{10^k} + \cdots$$

which converges to b, where $a_i \in \{0, 1, 2, \ldots, 8, 9\}$ for each i, and not all a_i's are 9 from some point on. One usually writes $b = 0.a_1a_2a_3\ldots$.

4.22 Example. By 4.20, $\frac{1}{3} = 0.333\ldots$ since $\frac{3}{10} + \frac{3}{10^2} + \cdots$ converges to $\dfrac{\frac{3}{10}}{1 - \frac{1}{10}} = \frac{1}{3}$; $0.25000\ldots$ is a decimal expansion for $\frac{1}{4}$ but $0.24999\ldots$ is not.

4.23 Theorem. *(Convergence, existence and uniqueness of decimal expansions)*

a). Each series $\frac{a_1}{10} + \frac{a_2}{10^2} + \ldots$, as described in 4.21, must converge to some non-negative real number less than one. That is, each decimal expansion represents a non-negative real number less than one.
[Hint: Compare with $1 = \frac{9}{10} + \frac{9}{10^2} + \frac{9}{10^3} + \ldots$; see a calculus book for a suitable Comparison Theorem.]

b). Conversely, each non-negative real number less than one has a decimal expansion.

c). The decimal expansion of a non-negative real number less than one is unique.

Hint for c): Suppose $r = 0.a_1a_2a_3\ldots = 0.b_1b_2b_3\ldots$. Multiply by 10 to obtain $10r = a_1.a_2a_3\ldots = b_1.b_2b_3\ldots$. Use Theorem 4.10 to argue that $a_1 = b_1$. Note that $.a_2a_3\ldots = 10r - a_1 = 10r - b_1 = .b_2b_3\ldots$. Continue by induction.

We now explore the decimal expansion of a positive rational number which can be represented by a proper fraction.

4.24 Exercise. Compute, via long division, the decimal representations of

$$\frac{5}{8}, \quad \frac{5}{11}, \quad \frac{13}{88}, \quad \frac{201}{444}, \quad \frac{3}{7}, \quad \frac{5}{7}, \text{ and } \frac{5}{13}.$$

Examine the form of these decimal expansions: length of repeating blocks and delay before such begins. Do you see any connection between this form and the denominators of the rational numbers?

4.25 Definition. A decimal expansion $0.a_1a_2a_3\ldots$ is

a). *Periodic* if, after some point, a block of digits repeats itself indefinitely:

$$0.a_1a_2\ldots a_s a_{s+1}\ldots a_{s+t}a_{s+1}\ldots a_{s+t}\ldots.$$

In this case we write $0.a_1a_2\ldots a_s\overline{a_{s+1}\ldots a_{s+t}}$.
For example, $\frac{7}{22} = 0.3181818\cdots = 0.3\overline{18}$. [The smallest such s is called the *pre-period* and the smallest such t the *period* of the expansion.]

b). *Terminating* if all a_i from some point on are zero:

$$0.a_1a_2\ldots a_s000\ldots.$$

Observe that every terminating decimal expansion is periodic of period 1.

4.26 Theorem. *(Normal forms of decimal expansions of rationals)*

a). The decimal expansion of each positive rational number $q < 1$ is periodic.

b). Conversely, each non-zero periodic decimal expansion of a non-negative real number $b < 1$ represents a positive rational number.

Hint for a): What are the possible remainders in each step of performing the long division $n\overline{)\mathrm{m}}$?
Hint for b): Generalize this computation: $b = 0.123\overline{45}$ implies $10^3b = 123.\overline{45}$ and $10^5b = 12345.\overline{45}$. Hence $10^5b - 10^3b = 12345 - 123$ so that

$$b = \frac{12222}{10^5 - 10^3} = \frac{12222}{99000} = \frac{1358}{11000}.$$

Call a fraction $\frac{m}{n}$ a *proper, reduced rational number* if $m < n$ are positive integers with $\gcd(m, n) = 1$. [Recall that in Exercise 3.15 we showed fractions could be reduced.]

4.27 Theorem. *The decimal expansion of the proper, reduced rational number $\frac{m}{n}$ is terminating exactly when $n = 2^\alpha 5^\beta$ for some $\alpha, \beta \geq 0$. In this case the length of the terminating decimal expansion is* $\max\{\alpha, \beta\}$.

Hint: $\frac{11}{40} = \frac{11}{2^3 5} = \frac{11\cdot 5^2}{2^3 5^3} = \frac{275}{10^3} = 0.275$.

4.28 Exercise. Express as a reduced quotient of integers.

a) * $0.21\overline{522}$

b) * $0.444\overline{1332}$

c) * 0.34612

d) Exhibit explicitly a decimal expansion of an irrational number.

4.29 Theorem. *Assume $\frac{m}{n}$ is proper and reduced with no 2 or 5 in the prime factorization of n. Then the pre-period of its decimal expansion is zero and the period is the smallest integer t so that $n|(10^t-1)$; i.e., t is the number of digits in the smallest of $9, 99, 999, 9999, \ldots$ which n divides.*

Hint: $b = 0.\overline{393}$ implies $10^3 b = 393.\overline{393}$. Then $(10^3 - 1)b = 393$, so that

$$b = \frac{393}{10^3 - 1} = \frac{393}{999} = \frac{131}{333}.$$

4.30 Remark. It can be shown that for any such n, a t exists such that $n|(10^t - 1)$.

4.31 Theorem. *Suppose $\frac{m}{n}$ is proper and reduced and $n = 2^\alpha 5^\beta n'$, where n' has no 2 or 5 in its prime factorization. Then the pre-period of the decimal expansion of $\frac{m}{n}$ is $\max\{\alpha, \beta\}$ and the period is the smallest t such that $n'|(10^t - 1)$.*

4.32 Exercise. Determine, without dividing out, the form of the decimal expansion of the following.

a)* $\frac{27}{56}$ b)* $\frac{7}{13}$ c)* $\frac{154}{1680}$ d)* $\frac{111}{148}$

5. Countable and Uncountable Sets

We now explore briefly "how many" natural numbers, integers, rational numbers, irrational numbers, and real numbers there are.

5.1 Definition. 1. If A and B are sets, then a *function f from A to B* is an object which specifies, for each element $a \in A$, an element $f(a) \in B$. We use the notation $f\colon A \to B$ to say that f is a function from A to B.

We will not attempt here to say what sort of an "object" a function is, or precisely what we mean by the word "specifies".

2. A function $f\colon A \to B$ is *onto B* if for each $b \in B$ there is at least one $a \in A$ such that $b = f(a)$.

3. A function $f\colon A \to B$ is *one-to-one* (frequently written 1–1) if for each $b \in B$ there is at most one $a \in A$ such that $b = f(a)$.

Note that this definition can be equivalently stated as "$f\colon A \to B$ is 1–1 if for every $a, a' \in A$ such that $a \neq a'$ we have $f(a) \neq f(a')$."

For an example of a function, consider a shepherd who has made a list of the names of the sheep in his herd. Assuming that no two sheep have the same name, the shepherd has defined a function S which assigns to each name n on the list the sheep $S(n)$ having that name. The function is one to one provided that no sheep has more than one name: if the list includes nicknames along with the official names, then it would not be one to one. It is onto if every sheep has a name: during lambing season the function would not be onto until all of the newborn lambs had been given names.

We say that there is a one-to-one correspondence between two sets A and B if there if is a one-to-one function from A *onto* B. In the case of the sheep there is (assuming no nicknames) a one-to-one correspondence between the set of names on the list and the set of named sheep. Clearly, this correspondence shows (assuming no nicknames) that there are at least as many sheep as names. If every sheep has a name then it shows that the sets have the same size, but if this is lambing season then the set of named sheep may be a proper subset of the set of all sheep, so we could conclude that there are fewer names than there are sheep.

5.2 Definition. a). Two sets A and B have the *same cardinal number*, written $A \equiv B$, if there is a one-to-one correspondence between A and B. [Example: The one-to-one correspondence $n \leftrightarrow 2n$ shows that the set of all natural numbers has the same cardinal number as the set of even natural numbers.]

b). We say that A has at most as many members as B, written $A \preceq B$, if there is a one-to-one correspondence between A and a subset of B. [Example: the identity function, defined by $\mathrm{id}(n) = n$ for each $n \in \mathbb{N}$, shows that $\mathbb{N} \preceq \mathbb{N}$, $\mathbb{N} \preceq \mathbb{Q}$ and $\mathbb{N} \preceq \mathbb{R}$. The function $f\colon \mathbb{N} \to \mathbb{Q}$ defined by $f(n) = 1/(n+1)$ is another map showing that $\mathbb{N} \preceq \mathbb{Q}$.]

c). A has *fewer elements* than B (written $A \prec B$) if $A \preceq B$ but $A \not\equiv B$.

d). A set is *countable* if it is either finite or has the same cardinal number as $\mathbb{N}$, the set of natural numbers. Otherwise, it is said to be *uncountable*.

e). A set is *countably infinite* if it is countable but not infinite.

5.3 Remark. Notice that the function $D(n) = 2n$ of clause (a) is a 1–1 function from $\mathbb{N}$ to the set of even numbers, which is a proper subset of $\mathbb{N}$. This is an important difference between finite and infinite sets. The set of sheep is (presumably) finite, so if there are sheep without names then the set of named sheep must be strictly smaller than the set of all sheep. In the case of the infinite set $\mathbb{N}$, however, the function D shows that the set of even numbers has the same size as the full set $\mathbb{N}$.

5.4 Remark. Mathematicians often write $|A|$ for the *cardinal number of* A, the "number of elements of A". Thus $A \preceq B$ could be written $|A| \leq |B|$. However, you should not use the concept of "the cardinal number of A" in the proofs below. In the first place, we really have no idea what the "cardinal number" of an infinite set would be: clearly the cardinal number of the set $\{\text{Buttercup}, \text{Silvy}, \text{Misty}\}$ is the natural number 3, but what sort of an object is $|\mathbb{R}|$, the cardinal number of the set of reals? In the second place, Remark 5.3 shows that in at least one important aspect the cardinal numbers of infinite sets behave quite differently from finite numbers. It seems that we should be careful not to trust the analogy too far until we have a better understanding of the properties of the cardinal numbers.

5.5 Theorem. *The relation $A \equiv B$ is an equivalence relation. That is, for all sets A, B and C:*

a). (Reflexivity) $A \equiv A$.

b). (Symmetry) *If $A \equiv B$ then $B \equiv A$.*

c). (Transitivity) *If $A \equiv B$ and $B \equiv C$ then $A \equiv C$.*

5.6 Theorem. $\mathbb{N} \equiv \{1, 3, 5, 7, \dots\} \equiv \mathbb{Z} \equiv \mathbb{Q}$.
That is, each of $\mathbb{N}$, $\{1, 3, 5, \dots\}$, $\mathbb{Z}$, and $\mathbb{Q}$ is countably infinite.

5.7 Theorem. $\mathbb{N} \prec \mathbb{R}$. *That is, $\mathbb{R}$ is uncountable.*

Hint: Let $A := \{x \in \mathbb{R} : 0 < x < 1\}$ and show $\mathbb{N} \prec A$ indirectly. Suppose to the contrary $\mathbb{N} \equiv A$ with a one-to-one correspondence between $\mathbb{N}$ and A given by

$$\begin{array}{ccc} 0 & \longleftrightarrow & 0.a_{0,0}\, a_{0,1}\, a_{0,2}\, a_{0,3}\, a_{0,4} \dots \\ 1 & \longleftrightarrow & 0.a_{1,0}\, a_{1,1}\, a_{1,2}\, a_{1,3}\, a_{1,4} \dots \\ 2 & \longleftrightarrow & 0.a_{2,0}\, a_{2,1}\, a_{2,2}\, a_{2,3}\, a_{2,4} \dots \\ \vdots & & \vdots \end{array}$$

where $0.a_{k,0}\,a_{k,1}\,a_{k,2}\,\ldots$ is the decimal expansion of the real number r_k corresponding to the natural number k.

Now let $b := 0.b_0\,b_1\,b_2\,b_3\,\ldots$, where $b_i := \begin{cases} 1 & \text{if } a_{i,i} \neq 1 \\ 2 & \text{if } a_{i,i} = 1. \end{cases}$

To what natural number can b correspond?
This argument is called the Cantor Diagonalization Process.

5.8 Theorem.

a). The union of two disjoint, countably infinite sets is countably infinite.

b). There are uncountably many irrational numbers.

5.9 Theorem. *For any set A, $A \prec \mathcal{P}(A)$, where $\mathcal{P}(A)$ denotes the set of all subsets of A, called the power set of A.*

Hint: Indirect proof! Suppose to the contrary that $f\colon A \to \mathcal{P}(A)$ is a one-to-one correspondence between A and $\mathcal{P}(A)$, and consider the set $B := \{x \in A : x \notin f(x)\}$. Then $B \in P(A)$, so it must correspond to some element $b \in A$. Is $b \in B$?

5.10 Exercise. Give examples of infinitely many infinite sets no two of which have the same cardinal number.

Theorem 5.5, stating that $\equiv$ is (like $=$) an equivalence relation, suggests asking the question whether the relation $\preceq$ is an order relation. In fact it is, as the following theorem asserts. We will not prove parts (b) and (c).

5.11 Theorem. a). *For all sets A, B and C, if $A \preceq B$ and $B \preceq C$ then $A \preceq C$.*

b). *For all sets A and B, if $A \preceq B$ and $B \preceq A$ then $A \equiv B$.*

c). *For all sets A and B, either $A \preceq B$ or $B \preceq A$.*

The proof of the first clause is essentially the same as clause (c) of theorem 5.5. The proof of the second, which is known as the Cantor-Bernstein theorem, is somewhat more challenging. The proof of the third requires a new axiom: the Axiom of Choice.

To get a start on the theory of arithmetic for infinite cardinal numbers, notice that if O is the set of odd natural numbers and E is the set of even natural numbers, then $\mathbb{N} = O \cup E$ and hence we must have $|\mathbb{N}| = |O| + |E|$. But $|O| = |E| = |\mathbb{N}|$, so it follows that $|N| = |N| + |N|$. In fact one can prove, using the axiom of choice, that for *any* infinite cardinal number κ we have $\kappa + \kappa = \kappa$ and $\kappa \cdot \kappa = \kappa$.

6. Fields and Subfields

6.1 Definition. A *field* is a set F equipped with binary operations $+$ and $\cdot$ satisfying the "field axioms" given in 1.1: **AC**, **AA**, **AID**, **AIV**, **MC**, **MA**, **MID**, **MIV**, and **D**. A subset K of a field F is a *subfield* of F if K itself forms a field under the operations defined on F.

Recall that the closure of a set under an operation follows from the meaning of a binary operation on the set (see 1.3)]

6.2 Example. (Revisiting $\mathbb{R}$ and $\mathbb{Q}$)

a). We began by assuming that the real numbers $\mathbb{R}$ form a field.

b). The rational numbers $\mathbb{Q}$ form a field (see 4.2), and $\mathbb{Q}$ is a subfield of $\mathbb{R}$.

I. Subfields, Surd Fields, and Ordered Fields

6.3 Theorem. *Suppose that F is a field. If a subset K of F satisfies the hypotheses*

(i) *K is closed under addition and multiplication;*

(ii) $0, 1 \in K$*;*

(iii) $a \in K$ *implies* $-a \in K$*; and*

(iv) $0 \neq a \in K$ *implies* $a^{-1} \in K$*;*

then K is a subfield of F.

6.4 Exercise. (Sample surd fields)

a). Any subfield of $\mathbb{R}$ must contain $\mathbb{Q}$ as a subset.

b). Show that $\mathbb{Q}[\sqrt{2}] := \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ is a proper subfield of $\mathbb{R}$ which properly contains $\mathbb{Q}$.
Notice that $\mathbb{Q}[\sqrt{2}]$ is the smallest subfield of $\mathbb{R}$ which contains $\mathbb{Q}$ and $\sqrt{2}$. That is, if F is any subfield of $\mathbb{R}$ such that $\mathbb{Q} \subset F$ and $\sqrt{2} \in F$ then $\mathbb{Q}[\sqrt{2}] \subset F$.

c). Show the same for $\mathbb{Q}[\sqrt{3}] := \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\}$.

d). Neither of $\mathbb{Q}[\sqrt{2}]$ and $\mathbb{Q}[\sqrt{3}]$ is a subset of the other.

e). Show that $\mathbb{Q}[\sqrt[3]{2}] := \{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 \mid a, b, c \in \mathbb{Q}\}$ is a subfield of $\mathbb{R}$.
[Hint: Compute $[a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2][d + e\sqrt[3]{2} + f(\sqrt[3]{2})^2]$,
where $d := a^2 - 2bc$, $e := 2c^2 - ab$, and $f := b^2 - ac$. To show that the product is nonzero, use 1.4g).

f). Give examples of infinitely many proper subfields K of $\mathbb{R}$ which properly contain $\mathbb{Q}$.

[Note: A is a *proper subset* of B if $A \subset B$ but $A \neq B$.]

6.5 Definition. A field F is an *ordered field* if it satisfies the order axioms OTC, OTR, OA, and OM given in 1.13. An ordered field is called *completely ordered* if, in addition, it satisfies the least upper bound axiom (4.7). (We have **assumed** that the real numbers $\mathbb{R}$ form a completely ordered field.)

6.6 Theorem. *(Ordered fields and subfields)*

a). A subfield of an ordered field is an ordered field.

b). $\mathbb{Q}$, $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{3}]$, *and* $\mathbb{Q}[\sqrt[3]{2}]$ *are ordered fields.*

c). $\mathbb{Q}$ *is not completely ordered. [See theorem 4.17.]*

II. Modular Arithmetic

6.7 Definition. For each positive integer $n \geq 2$, we set $\mathbb{Z}_n := \{0, 1, 2, 3, \ldots, n-1\}$ and definite operations + and $\cdot$ on $\mathbb{Z}_n$ by:

$a + b :=$ remainder after division of the usual sum by n.

$ab :=$ remainder after division of the usual product by n.

For example, in $\mathbb{Z}_7$, $3 + 6 = 2$, $3 \cdot 6 = 4$ and $6^2 = 1$.

6.8 Remark. One can show (and we will assume) that, for each n, all of the field axioms hold in $\mathbb{Z}_n$, except possibly MIV.

Note that for $n = 12$, the operations defined above form the arithmetic of a clock.

6.9 Exercise. (Sample computations)

a). Compute in $\mathbb{Z}_8$: $5 + 7^*$, $\quad 5 \cdot 7$, $\quad 7^{2\,*}$.

b). Compute in $\mathbb{Z}_5$: -2^*, $\quad 2 - 4$, $\quad 2^{-1\,*}$, $\quad \frac{2}{3}^*$.

c). Which elements of $\mathbb{Z}_{10}$ have a multiplicative inverse? Compute those that exist*.

6.10 Theorem. *Let* $n \geq 2$.

a). The set of those elements of $\mathbb{Z}_n$ which are relatively prime to n is closed under multiplication.
Hint: See 3.14(d), 3.14(f).

b). An element a in $\mathbb{Z}_n$ has a multiplicative inverse iff a and n are relatively prime. Hint: See 3.14(a) and 6.11 below.

c). $\mathbb{Z}_n$ is a field iff n is a prime.

d). No order relation can be placed on $\mathbb{Z}_n$ so that $\mathbb{Z}_n$ becomes an ordered field.

6.11 Exercise. If $a \in \mathbb{Z}_n$ with a relatively prime to n, then, using the Euclidean algorithm one can find integers r and k such that $ar + nk = 1$. If r is then reduced via the division algorithm, $r = nq + b, \quad 0 \leq b < n$, then b is the multiplicative inverse of a in $\mathbb{Z}_n$. Show that this is indeed true and then use this method to compute:

a). The multiplicative inverse of 7 in ${\mathbb{Z}_{31}}^*$.

b). The multiplicative inverse of 11 in ${\mathbb{Z}_{125}}^*$.

7. Complex Numbers

7.1 Definition. The *complex numbers* is the set

$$\mathbb{C} := \{a + bi \mid a, b \in \mathbb{R}\}$$

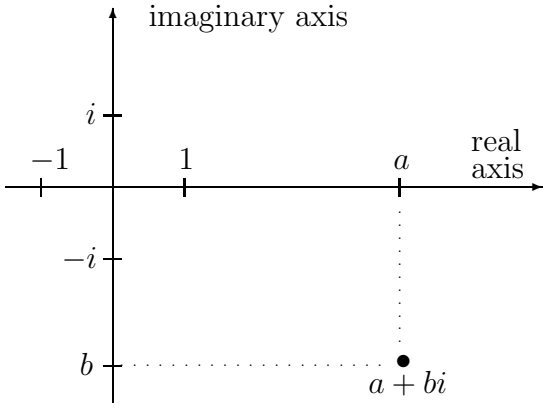
on which equality, multiplication, and addition are defined as follows:

Equality: $a + bi = c + di$ means $a = c$ and $b = d$.

Addition: $(a + bi) + (c + di) := (a + c) + (b + d)i$.

Multiplication: $(a + bi)(c + di) := (ac - bd) + (ad + bc)i$.

For a complex number $z = a + bi$, a is called the *real part* of z and b is called the *imaginary part* of z. The complex numbers are represented geometrically by the Cartesian coordinate plane: $z = a + bi$ is paired with the point having coordinates (a, b) as indicated below.



7.2 Exercise. (Complex arithmetic)

a). Show that the sum and product of complex numbers defined above is the same as if one treated the numbers as polynomials in i and let $i^2 = -1$. Hence by an abuse of notation, we write, for example, $2 - 3i$ for $2 + (-3)i$.

b). Find the sum, product and quotient (See 7.5d) of:
(i) $2 + 3i$ and $-2 - 5i$ * (ii) 5 and $-2 + i$ (iii) $4i$ and $6i$.

c). Locate in the complex plane: $3 - i$, $-4 + 3i$, $-2i$, 2.

d). Compute $(-\frac{1}{2} + \frac{1}{2}\sqrt{3}\,i)^3$ *.

e). Interpret complex number addition geometrically in the plane.

7.3 Definition. For $z = a + bi$ in $\mathbb{C}$,

a). $\bar{z} := a - bi$, the *conjugate* of z.

b). $|z| := \sqrt{a^2 + b^2}$, the *absolute value* of z.

7.4 Exercise. (Geometric interpretations of conjugate and absolute value)

a). What are the relative positions of z, $-z$, $\bar{z}$, and $-\bar{z}$ in the complex plane?

b). Interpret $|z|$ geometrically.

7.5 Theorem. *If z, z_1, and z_2, are in $\mathbb{C}$, then*

a). $\overline{z_1 + z_2} = \overline{z}_1 + \overline{z}_2$.

b). $\overline{z_1 z_2} = \overline{z}_1 \overline{z}_2$.

c). z is real iff $z = \bar{z}$.

d). $z\bar{z} = |z|^2$. *Hence* $\dfrac{z_1}{z_2} = \dfrac{z_1}{z_2}\dfrac{\bar{z}_2}{\bar{z}_2} = \dfrac{z_1 \bar{z}_2}{|z_2|^2}$.
[Use definition 1.6 for division of complex numbers: that is, $\frac{z_1}{z_2}$ is the unique number w such that $z_1 = z_2 w$.]

e). $|z| = |-z| = |\bar{z}|$.

f). $|z_1 z_2| = |z_1||z_2|$ *and* $\left|\dfrac{z_1}{z_2}\right| = \dfrac{|z_1|}{|z_2|}$. *[Hint: Consider using d) above.]*

g). $|z_1 + z_2| \leq |z_1| + |z_2|$. *(triangle inequality)*
[Hint: First show the Schwarz inequality: $(ac + bd)^2 \leq (a^2 + b^2)(c^2 + d^2)$.]

7.6 Theorem. $\mathbb{C}$ *forms a field.*

7.7 Theorem (Complex subfields). *a). There exists no subfield K of $\mathbb{C}$ with $\mathbb{R} \subset K \subset \mathbb{C}$ and $\mathbb{R} \neq K \neq \mathbb{C}$.*

b). There is, however, a proper subfield of $\mathbb{C}$ that is not a subset of $\mathbb{R}$.
(Give an example of such.)

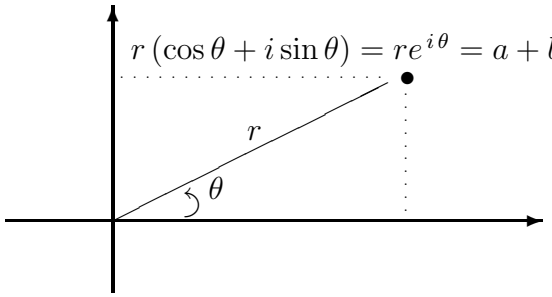
c). No order relation can be placed on $\mathbb{C}$ so that $\mathbb{C}$ becomes an ordered field.

7.8 Remark. In doing arithmetic with complex numbers it is useful to have the exponential function e^z (for real and complex numbers) and the trigonometric functions $\sin(x)$ and $\cos(x)$ for real numbers.

In the following, assume that these functions have been defined for real numbers and assume (without proof) that they have their familiar properties *for real numbers*. We will use this assumption in order to extend the definition of e^z to complex numbers z and to prove that it still satisfies the familiar properties for complex numbers z.

7.9 Definition. For $z = a + bi \in \mathbb{C}$, one can write $a = r\cos\theta$ and $b = r\sin\theta$, where r and θ are as shown below. Hence $z = r(\cos\theta + i\sin\theta)$, the *polar form* of z. Notice that $r = |z|$ and $\theta = \tan^{-1}(\frac{b}{a})$ (or, if $a < 0$, then $\theta = \pi + \tan^{-1}(\frac{b}{a})$). The angle θ is called the *argument* of z.

The exponential function can be extended from $\mathbb{R}$ to $\mathbb{C}$ by defining $e^{i\theta} := \cos(\theta) + i\sin(\theta)$. Thus can write $z = r(cos(\theta) + i\sin(\theta)) = re^{i\theta}$.



Examples:

$$\begin{aligned} 2 - 2i &= 2\sqrt{2}(\cos(-\tfrac{\pi}{4}) + i\sin(-\tfrac{\pi}{4})) \\ -1 + \sqrt{3}i &= 2(\cos\tfrac{2\pi}{3} + i\sin\tfrac{2\pi}{3}) \\ i &= 1(\cos\tfrac{\pi}{2} + i\sin\tfrac{\pi}{2}). \end{aligned}$$

7.10 Theorem. *If $z_1 = r(\cos\theta + i\sin\theta)$ and $z_2 = s(\cos\phi + i\sin\phi)$, then*

a). $z_1 z_2 = rs(\cos(\theta + \phi) + i\sin(\theta + \phi)) = rse^{i(\theta+\phi)}$ *and*

b). $\dfrac{z_1}{z_2} = \dfrac{r}{s}(\cos(\theta - \phi) + i\sin(\theta - \phi)) = \frac{r}{s}e^{i(\theta-\phi)}$.

c). $e^{(z_1+z_2)} = e^{z_1}e^{z_2}$.

7.11 Exercise. (Polar form and geometric interpretation of multiplication)

a). Write in polar form: $2 + 2i$ *, $-\frac{1}{2} + \frac{\sqrt{3}}{2}i$, $-2i$ *, -3.

b). Interpret complex number multiplication geometrically in the plane.

7.12 Theorem (DeMoivre's Theorem). *If $z = r(\cos\theta + i\sin\theta)$ and n is a positive integer, then $z^n = r^n(\cos n\theta + i\sin n\theta)$.*

7.13 Theorem. *Let $z = r(\cos\theta + i\sin\theta)$ be a nonzero complex number.*
Then z has exactly n n-th roots; namely:

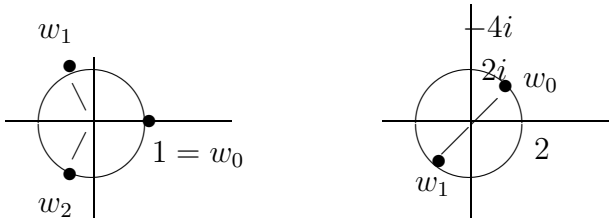
$$w_k := \sqrt[n]{r}\left(\cos\left(\frac{\theta}{n} + \frac{2\pi}{n}k\right) + i\sin\left(\frac{\theta}{n} + \frac{2\pi}{n}k\right)\right), \qquad \textit{for } k = 0, 1, 2, ..., n-1.$$

7.14 Example. (Some complex roots in Cartesian and polar form)

a). The square roots of 1 are:
$w_0 = 1 = \cos 0 + i \sin 0$
$w_1 = -1 = \cos \pi + i \sin \pi$.

b). The cube roots of 1 are (see figure at left below):
$w_0 = 1 = \cos 0 + i \sin 0$
$w_1 = -\frac{1}{2} + \frac{\sqrt{3}}{2} i = \cos \frac{2\pi}{3} + i \sin \frac{2\pi}{3}$
$w_2 = -\frac{1}{2} - \frac{\sqrt{3}}{2} i = \cos \frac{4\pi}{3} + i \sin \frac{4\pi}{3}$.

c). The square roots of $4i$ are (see figure at right below):
$w_0 = 2(\cos \frac{\pi}{4} + i \sin \frac{\pi}{4})$
$w_1 = 2(\cos \frac{5\pi}{4} + i \sin \frac{5\pi}{4})$.



7.15 Exercise. Determine and graph in the complex plane all

a). 4th roots of -1 *

b). 5th roots of i

c). Cube roots of -8

d). 4th roots of $16i$ *

e). Square roots of $1 + \sqrt{3}\, i$ *

f). 4th roots of $-1 - \sqrt{3}\, i$.

7.16 Exercise. Determine all solutions in $\mathbb{C}$ of

a). $x^4 - 16 = 0$

b). $x^6 + 64 = 0$ *

c). $x^3 + 8i = 0$

d) $x^3 - 64i = 0$ *

e) $x^4 + 81 = 0$

f) $x^5 - 243 = 0$.

8. Polynomials

8.1 Definition. (Polynomials and their arithmetic)

a). A *polynomial $P(x)$ over a field F* (or over $\mathbb{Z}$) is a symbol

$$P(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n + \dots$$

in which $a_i \in F$ (or $a_i \in Z$) for each i and $a_i = 0$ for all i from some point on. The set of all polynomials over F (or over $\mathbb{Z}$) is denoted by $F[x]$ (or $\mathbb{Z}[x]$) and is called the *polynomial ring* over F.

Examples: $2 + \sqrt{2}x + x^2$ is in $R[x]$ and $C[x]$ but not in $Q[x]$ or $\mathbb{Z}[x]$;
$1 + x + 2x^2 + 3x^3 + \cdots + nx^n + \dots$ is not a polynomial (why?).

b). The *degree* of a non-zero polynomial $P(x) = a_0 + a_1x + \cdots + a_nx^n + \dots$ is the largest n such that $a_n \neq 0$ (Notation: $\deg P(x) := n$).
The zero polynomial (all $a_i = 0$) is not assigned a degree.

Examples: $4 + 3x^2 + 5x^4$ has degree 4;
nonzero constant polynomials $P(x) = a_0$ ($a_0 \neq 0$) have degree zero.

c). Addition and multiplication of polynomials are defined as follows:
For $P(x) = a_0+a_1x+a_2x^2+\cdots+a_nx^n+\dots$ and $Q(x) = b_0+b_1x+b_2x^2+\cdots+b_nx^n+\cdots$,

(i) $P(x) + Q(x) := (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_n + b_n)x^n + \dots$

(ii) $P(x)Q(x) := c_0 + c_1x + c_2x^2 + \cdots + c_nx^n + \dots$, where for each n,

$$c_n := \sum_{i+j=n} a_ib_j = a_0b_n + a_1b_{n-1} + a_2b_{n-2} + \cdots + a_{n-1}b_1 + a_nb_0.$$

8.2 Exercise. If $P(x) = 1 + 4x + 2x^2$ and $Q(x) = 4 - x + x^2 + 3x^3$, compute $P(x) + Q(x)$ and $P(x)Q(x)$

a). Using the formal definitions given in 8.1c).

b). As you did in high school algebra.

[Compare the computations, not just the results.]

8.3 Theorem (Closure under + and ×). *The sum and product of two polynomials over a field F (or over $\mathbb{Z}$) are polynomials (rather than just power series). Moreover, if $P(x)$ and $Q(x)$ are nonzero polynomials over a field F (or over $\mathbb{Z}$), then*

a). $\deg(P(x)+Q(x)) \le \max\{\deg P(x), \deg Q(x)\}$, *provided* $P(x)+Q(x) \neq 0$. *[Give an example to show that strict inequality can hold.]*

b). $\deg P(x)Q(x) = \deg P(x) + \deg Q(x)$.

8.4 Theorem. *For any field* F, $F[x]$ *(and* $\mathbb{Z}[x]$*)*

a). Satisfies all the field axioms except **MIV**.

b). Has no divisors of zero. That is, $P(x)Q(x) = 0$ *implies* $P(x) = 0$ *or* $Q(x) = 0$.

c). $P(x)Q(x) = P(x)R(x)$ *(*$P(x) \neq 0$*) implies* $Q(x) = R(x)$.

8.5 Theorem (Division Algorithm). *Let* $P(x)$ *and* $D(x)$ *be polynomials over a field* F *with* $D(x) \neq 0$. *Then there exist unique polynomials* $Q(x)$ *and* $R(x)$ *such that* $P(x) = D(x)Q(x) + R(x)$ *with either* $\deg R(x) < \deg D(x)$ *or* $R(x) = 0$.

8.6 Exercise. Compute via long division $Q(x)$ and $R(x)$ in the division algorithm if

a). $P(x) = x^4 - 3x^2 + x + 3$ and $D(x) = 2x^2 - 1$. *

b). $P(x) = 5x^4 - 2x^3 + 12x - 6$ and $D(x) = x^2 + 4$.

c). $P(x) = 2x^4 + 2x^3 + 3x^2 + x + 1$ and $D(x) = 2x^2 + 1$.

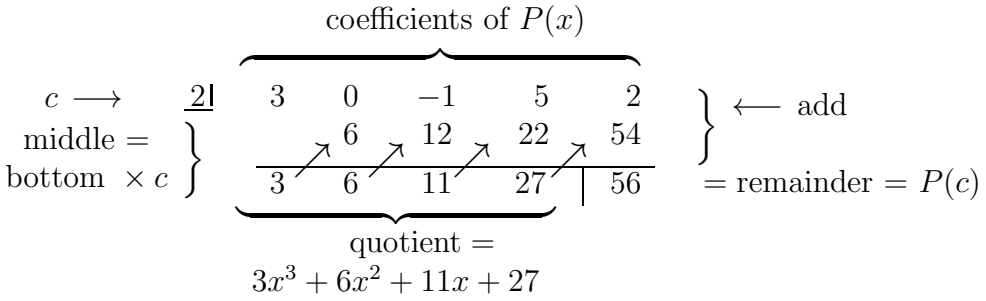
8.7 Definition. Suppose that $P(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ is a polynomial over a field F and $c \in F$.

a). The *value of* $P(x)$ *at* c is defined to be $P(c) := a_0 + a_1c + a_2c^2 + \cdots + a_nc^n \in F$.

b). c is called a *zero* of $P(x)$ (or a *root* of $P(x) = 0$) if $P(c) = 0$.

8.8 Theorem (Remainder Theorem). *If the polynomial* $P(x)$ *over a field* F *is divided by* $x - c$ *(*$c \in F$*) to give* $P(x) = (x-c)Q(x) + R$, *then* $R = P(c)$. *[*$R = R(x)$ *is constant. Why?]*

8.9 Notation (Synthetic Division/Substitution). The computations involved in dividing a polynomial $P(x)$ by $x - c$ can be placed in a convenient format (synthetic division). For example, to divide $3x^4 - x^2 + 5x + 2$ by $x - 2$ one can write:



Notice that this process computes the remainder R, which by theorem 8.8 is equal to $P(c)$. Hence the process of synthetic division is also a convenient method for computing $P(c)$. When used in this way, it can be called synthetic substitution.

8.10 Exercise. (Practice with synthetic division/substitution)

a). Use synthetic division to divide $4x^5 - 3x^4 + 5x^2 + 9$ by $x + 2$.

b). Use synthetic substitution to compute $P(3)$ if $P(x) = 7x^4 - 6x^3 + 2x^2 - 12$.

c). Use synthetic substitution to compute $P(\frac{1}{3})$ if $P(x) = 3x^4 - x^3 - 3x^2 + 4x - 1$.

8.11 Definition. Suppose $P(x)$, $Q(x)$ are in $F[x]$ (or $\mathbb{Z}[x]$). One says that $P(x)$ *divides* $Q(x)$ in $F[x]$ (or $\mathbb{Z}[x]$) (written $P(x)|Q(x)$) if there is a polynomial $R(x)$ in $F[x]$ (or $\mathbb{Z}[x]$) such that $Q(x) = P(x)R(x)$.

8.12 Example. $(x - \sqrt{2})|(x^2 - 2)$ in $\mathbb{R}[x]$ but not in $\mathbb{Q}[x]$.
$3|(2x + 5)$ in $\mathbb{Q}[x]$ but not in $\mathbb{Z}[x]$.

8.13 Theorem (Factor Theorem). *Suppose $P(x)$ is in $F[x]$ and $c \in F$.*
Then $(x - c)|P(x)$ iff $P(c) = 0$.

8.14 Corollary. *A polynomial of degree n over a field can have at most n distinct zeros in the field.*

8.15 Theorem (Rational Root Theorem). *Let $P(x) = a_0 + a_1x + \cdots + a_nx^n$ ($a_n \neq 0$) be a polynomial over $\mathbb{Z}$. If $\frac{p}{q}$ is a reduced rational zero of $P(x)$, then $p|a_0$ and $q|a_n$.*
[When searching for zeros of a polynomial over $\mathbb{Z}$, this narrows the search for rational zeros to finitely many possibilities.]

8.16 Example. Any rational zeros of $P(x) = 2x^3 - x^2 - 4x + 2$ must occur among 1, -1, 2, -2, $\frac{1}{2}$, $-\frac{1}{2}$ (why?). Evaluating $P(x)$ at these numbers reveals that $P(\frac{1}{2}) = 0$; hence $(x - \frac{1}{2})|P(x)$. Synthetic division then yields $P(x) = (x - \frac{1}{2})(2x^2 - 4)$. What are the other zeros of $P(x)$?]

8.17 Exercise. (Applications of the Rational Root Theorem)

a). Find all rational zeros of $P(x)$ and a factorization in $\mathbb{Q}[x]$ of $P(x)$ if $P(x) =$

(i) $x^5 - 3x^4 - 3x^3 + 9x^2 - 4x + 12$

(ii) $3x^4 - 11x^3 + 10x - 4$

(iii) $x^4 + 2x^3 + 2x^2 - 4x - 8$ *

b). Use the rational root theorem to show that

(i) $\sqrt{2}$ is irrational.

(ii) $\sqrt[3]{4}$ is irrational.

8.18 Theorem (Quadratic Formula). *The zeros in $\mathbb{C}$ of the quadratic polynomial ax^2+bx+c ($a \neq 0$) over $\mathbb{R}$ are*

$$\frac{-b + \sqrt{b^2 - 4ac}}{2a} \quad \textit{and} \quad \frac{-b - \sqrt{b^2 - 4ac}}{2a}, \qquad \textit{if } b^2 - 4ac \geq 0, \textit{ and}$$

$$\frac{-b}{2a} + \frac{\sqrt{4ac - b^2}}{2a}\, i \quad \textit{and} \quad \frac{-b}{2a} - \frac{\sqrt{4ac - b^2}}{2a}\, i, \qquad \textit{if } b^2 - 4ac < 0.$$

[Hint: Divide by a, then complete the square to get $\left(x + \frac{b}{2a}\right)^2 = \frac{b^2 - 4ac}{4a^2}$.]

8.19 Exercise. (Zeros of polynomials in $\mathbb{C}[x]$)

a). Find all zeros in $\mathbb{C}$ of

(i) $x^2 + 4x + 13$ *

(ii) $x^2 - 6x + 4$

(iii) $2x^3 + x^2 + x - 1$ *

b). Use the method suggested by the hint in 8.18 to find all zeros in $\mathbb{C}$ of the following polynomials over $\mathbb{C}$.

(i) $x^2 + 4x + (4 + 9i)$

(ii) $x^2 - 4ix - 13$ *.

8.20 Theorem (Fundamental Theorem of Algebra). *Every polynomial over $\mathbb{C}$ of positive degree has at least one zero in $\mathbb{C}$.*

[We will assume this important theorem. Its proof involves concepts well beyond the scope of this course. It tells us that in order to ensure that all polynomial equations have roots, there is no need to extend our number system beyond $\mathbb{C}$.]

8.21 Corollary. *Every polynomial $P(x)$ over $\mathbb{C}$ of positive degree can be factored in $\mathbb{C}[x]$ into a product of linear (= first degree) factors:*

$$P(x) = a_n(x - r_1)(x - r_2)\cdots(x - r_n).$$

8.22 Definition. A polynomial over a field F of positive degree is called *irreducible over F* if it is not the product of two polynomials in $F[x]$ of lesser degree.

8.23 Example. $x^2 - 2$ is irreducible over $\mathbb{Q}$ but not over $\mathbb{R}$. $x^2 + 1$ is irreducible over $\mathbb{R}$ but not over $\mathbb{C}$.

8.24 Theorem. *(Irreducible polynomials)*

a). Every linear polynomial is irreducible.

b). The only irreducible polynomials over $\mathbb{C}[x]$ are the linear ones.

c). A quadratic polynomial $ax^2 + bx + c$ ($a \neq 0$) over $\mathbb{R}$ is irreducible over $\mathbb{R}[x]$ iff $b^2 - 4ac < 0$.

d). There exist irreducible polynomials in $\mathbb{Q}[x]$ of degree three.

8.25 Lemma. *Suppose $P(x)$ is in $\mathbb{R}[x]$ and $z \in \mathbb{C}$. If z is a zero of $P(x)$, then so is $\bar{z}$. Thus, the nonreal zeros of a polynomial over $\mathbb{R}$ must occur in complex conjugate pairs.*

[Hint: First show $\overline{P(z)} = P(\bar{z})$.]

8.26 Theorem. *Every polynomial over $\mathbb{R}$ is the product of polynomials over $\mathbb{R}$ of degree at most 2. [Hint: First factor in $\mathbb{C}[x]$; $(x-z)(x-\bar{z})$ =?]*

8.27 Exercise. (Irreducible polynomials)

a). Describe all irreducible polynomials over $\mathbb{C}$. Over $\mathbb{R}$.

b). Write the following polynomials as a product of irreducible polynomials over $\mathbb{C}$. Over $\mathbb{R}$.

(i) $x^4 - 2x^3 + 9x^2 + 2x - 10$

(ii) $x^5 - 3x^4 + 8x^3 - 8x^2 + 7x - 5$ *

(iii) $3x^5 - 13x^4 + 22x^3 - 30x^2 + 32x - 8$

(iv) $x^4 + 1$ *

c). Are the following irreducible over $\mathbb{Q}$? Explain.

(i) $x^3 + x^2 - x + 1$ *

(ii) $x^4 - x^2 - 2$ *

(iii) $x^4 + 1$ *

(iv) $x^6 - 2$ *

d). Are there irreducible polynomials in $\mathbb{Q}[x]$ of arbitrarily large degree?

e). Can you describe all irreducible polynomials in $\mathbb{Q}[x]$ of degree 2?
Of degree 3? Of any degree?

9. Answers to selected exercises

1.21 a) $x < -7$ or $x > 5$ c) $4 \leq x \leq 5$ d) no real number f) $x > -1$

3.17 a) 11 b) 1 c) 80 d) 252

3.25 a) $403 = 13 \cdot 31$, $1815 = 3 \cdot 5 \cdot 11^2$, $26208 = 2^5 \cdot 3^2 \cdot 7 \cdot 13$

4.24 $\frac{5}{11} = 0.\overline{45}$, $\frac{3}{7} = 0.\overline{428571}$, $\frac{13}{88} = 0.147\overline{72}$, $\frac{5}{13} = 0.\overline{384615}$

4.28 a $\frac{2389}{11100}$ b $\frac{61679}{138875}$ c $\frac{8653}{25000}$

4.28 4.32 $s = 3, t = 6$ 4.32 $s = 0, t = 6$ 4.32 $s = 3, t = 1$ 4.32 $x = 2, t = 0$

6.9

a) $5 \cdot 7 = 3$, $7^2 = 1$

b) $-2 = 3$, $\frac{2}{3} = 4$, $2^{-1} = 3$

c) 1, 3, 7, 9; $3^{-1} = 7$, $9^{-1} = 9$

6.11 a) 9 b) 91

7.2 b) $(2 + 3i)(-2 - 5i) = 11 - 16i$ d) 1

7.11 a) $2 + 2i = 2\sqrt{2}(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4})$, $-2i = 2(\cos\frac{3\pi}{2} + i\sin\frac{3\pi}{2})$

7.15

a) $|w| = 1$; $\theta = \frac{\pi}{4}, \frac{3\pi}{4}, \frac{5\pi}{4}, \frac{7\pi}{4}$

d) $|w| = 2$; $\theta = \frac{\pi}{8}, \frac{5\pi}{8}, \frac{9\pi}{8}, \frac{13\pi}{8}$

e) $|w| = 2$; $\theta = \frac{\pi}{6}, \frac{7\pi}{6}$

7.16

b) $|x| = 2$; $\theta = \frac{\pi}{6}, \frac{\pi}{2}, \frac{5\pi}{6}, \frac{7\pi}{6}, \frac{3\pi}{2}, \frac{11\pi}{6}$

a) $|x| = 4$; $\theta = \frac{\pi}{6}, \frac{5\pi}{6}, \frac{3\pi}{2}$

8.6 a) $Q(x) = \frac{1}{2}x^2 - \frac{5}{4}$, $R(x) = x + \frac{5}{4}$.

8.17 (a)iii. No rational zeros, yet reducible over $\mathbb{Q}$.

8.19

a)i $-2+3i, \quad -2-3i$ a)iii $\frac{1}{2}$ is a zero

b)ii $3+2i, \quad -3+2i$

8.27

b)ii three irreducible factors over $\mathbb{Q}$. b)iv reducible over $\mathbb{R}$.

c)i yes c)ii no c)iii yes c)iv yes