Math 112
Numbers:
From $2 \cdot 0 = 0$ to $e^{2\pi i} = 1$

R. Mayer

Spring 2006

"Then, my dear Glaucon, it is proper to lay down that study by law, and to persuade those who are to share in the highest things in the city to go for and tackle the art of calculation, and not as amateurs; they must keep hold of it until they are led to contemplate the very nature of numbers by thought alone, practising it not for the purpose of buying and selling like merchants or hucksters, but for war, and for the soul itself, to make easier the change from the world of becoming to real being and truth."[38, Republic 525c]

***

Contents

Acknowledgements

I want to thank Cathy D'Ambrosia for converting my handwritten version of these notes into LaTeX. I also thank Joe Buhler, Albyn Jones, David Perkinson Rao Potluri, Joe Roberts and Jerry Shurman for many discussions about Math 112, and for helpful comments on earlier drafts of these notes. I also thank Kelsey Alford-Jones for pointing out numerous typographical errors in an earlier draft of these notes.

Introduction

Remembrance of Things Past

You have been working with numbers for most of your life, and you know hundreds of facts about them. The first numbers you encountered were probably the positive integers $1, 2, 3, \cdots$. You learned that multiplication was repeated addition, and that $3 \times 4 = 12$, because 3 groups of apples, each of which contains 4 apples combine to give a group of 12 apples. Later you learned that $\sqrt{12} \cdot \sqrt{12} = 12$. This did not mean that $\sqrt{12}$ groups of apples, each of which contained $\sqrt{12}$ apples combine to give a group of 12 apples. The definition had changed, but whatever it meant, you knew how to get the "right answer". At some point you met decimals. Since $\frac{1}{4} = \frac{25}{100}$, you knew that $\frac{1}{4} = .25$. However $\frac{1}{3}$ was more of a problem. Although .33333333 was close to $\frac{1}{3}$, the two numbers were not equal. Perhaps you considered *infinite decimals*, so

$$\frac{1}{3} = .3333333 \cdots.$$

Then

$$3 \times \frac{1}{3} = .9999999 \cdots.$$

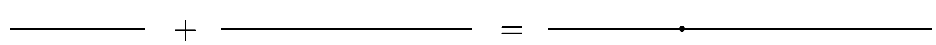
But $3 \times \frac{1}{3} = 1$, So $.9999999 \cdots$ must be equal to 1. They don't look equal, but .9999999 was probably close enough. At first the fact that $(-1) \times (-1) = +1$ was probably rather puzzling, but you got used to it after a while. You may have encountered the *imaginary number* i such that $i^2 = -1$ and $\sqrt{-a} = \sqrt{a}\, i$ when a is positive. Then you found that

$$\sqrt{-4} \times \sqrt{-9} = \sqrt{(-4)(-9)} = \sqrt{36} = 6,$$

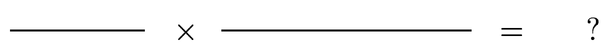
and

$$\sqrt{-4} \times \sqrt{-9} = 2i \cdot 3i = i^2\, 6 = -6.$$

This may have been unnerving. At some time numbers became identified with points on a line. Addition is straightforward: to add two numbers, you just slide the lines so that they share a common end, and combine them into one line.



but what does multiplication mean?



The Goal of the Course

In this course we will reorganize all of the number facts with which you are familiar. We will make a small number of assumptions or *axioms* about numbers, (thirteen assumptions in all, in definitions (2.48), (2.100), and (5.21)). The first twelve assumptions will be familiar number facts. The last assumption may not look familiar, but I hope it will seem as plausible as things you have assumed about numbers in the past. You will not be permitted to assume any facts about numbers other than the thirteen stated assumptions. For example, we will not assume that $3 \cdot 0 = 0$, or that $2 \cdot 2 = 4$, so you will not be allowed to assume this. (These facts will be proved in theorems 2.66 and 2.84.) You will not be allowed to assume that $(-1) \cdot (-1) = 1$, or that $0 < 1$. (These facts will follow from exercise 2.77c and corollary 2.104.) We will not justify the representation of numbers by points on a line, so no proofs can depend on pictures of graphs of functions. On the basis of our assumptions about real numbers, we will construct a more general class of *complex numbers*, in which -1, and in fact every number, has a square root. Many results about the algebra and calculus of real functions will be shown to hold for complex functions.

Occasionally I will draw pictures to motivate proofs, but the proofs themselves will not depend on the pictures. The goal of the course is to "contemplate the very nature of numbers by thought alone, practising it not for the purpose of buying and selling like merchants and hucksters, but $\cdots$ to make easier the change from the world of becoming to real being and truth."

Sometimes in examples or remarks I will use arguments depending on similar triangles or trigonometric identities, but my theorems and definitions will depend only on my assumptions. I will also refer to integers and rational numbers in examples before I give the formal definitions, but no theorems will involve integers until they have been defined. Nothing in this course will be trivial or obvious or clear. If you come across these words, it probably means that I am engaging in a mild deception. Beware.

On page 34 we will prove the well known fact that $2 \cdot 0 = 0$. On page 245, we will prove the less well known fact that $e^{2\pi i} = 1$. The fact that we can derive the last not-so-obvious result from our thirteen assumptions is somewhat remarkable.

Some General Remarks

The **exercises** in these notes are important. The proofs of many theorems will appear as exercises. You should work on as many exercises as time permits. Do not be discouraged if you cannot do some of the exercises the first time you try them. The important thing is that you should be able to do them after they have been discussed in class. The **entertainments** are supposed to be entertaining. If they do not entertain you, you can ignore them (unless your instructor is so entertained that one gets assigned as a homework problem). There are hints for selected problems at the end of the notes. Do not use them until you have spent some time on the problems. Any method you discover on your own is better than any method suggested in a hint.

The prerequisite for this course is a course in one-variable calculus. From the remarks made above you know that you cannot assume any facts from your calculus course, but many theorems are motivated by calculus. You should know that the derivative $f'(a)$ of a function f at a point a is given by

$$f'(a) = \lim_{x \to a} \frac{f(x) - f(a)}{x - a},$$

and that this represents the slope of the tangent to the graph of f at the point $(a, f(a))$. If you are not familiar with the rules for calculating the derivatives of the sine and cosine and exponential functions from an earlier course, our *definitions* of the sine and cosine and exponential will seem rather meaningless.

In these notes, informal set theory and logic are used. Axioms for set theory and logic can be given, and most mathematicians believe that all of the sorts of informal proofs that we give in the notes can, in principle, be justified by the axioms of set theory and logic. However the sort of informal set theory and logic we use here are typical of the methods used by workers in mathematical analysis at the start of the twenty-first century.

***

These notes are largely based on Joe Buhler's math 112 notes, used at Reed College in spring 1998[13]. The material in Buhler's appendices has been expanded and put into the main text. There are more examples, and some proofs are given in more detail. I've added some pictures, because I think geometrically.

Entertainment 0 Suppose three lines are given, having lengths 1, a, and b.

a) Describe a compass-and-straightedge construction for a line segment of length $a \times b$.

b) Describe a compass-and-straightedge construction for a line segment of length $\sqrt{a}$.

Chapter 1

Notation, Undefined Concepts and Examples

The ideas discussed in this chapter (e.g. *set*, *proposition*, *function*) are so basic that I cannot define them in terms of simpler ideas. Logically they are undefined concepts, even though I give definitions for them. My "definitions" use undefined words (e.g. *collection*, *statement*, *rule*) that are essentially equivalent to what I attempt to define. The purpose of these "definitions" and examples is to illustrate how the ideas will be used in the later chapters. I make frequent use of the undefined terms "true", "false", and "there is". It might be appropriate to spend some time discussing various opinions about the meaning of "truth" and "existence" in mathematics, but such a discussion would be more philosophical than mathematical, and would not be very relevant to anything that follows. If such questions interest you, you might enjoy reading *Philosophy of Mathematics* by Benacerraf and Putnam [7] or the article *Schizophrenia in Contemporary Mathematics* by Errett Bishop [10, pp 1-10]

Some of the terms and notation used in the examples in this chapter will be defined more precisely later in the notes. In this chapter I will assume familiar properties of numbers that you have used for many years.

1.1 Sets

1.1 Definition (Set.) A *set* is a collection of objects. A small set is often described by listing the objects it contains inside curly brackets, e.g.,

$$\{1, 3, 5, 7, 9\}$$

denotes the set of positive odd integers smaller than ten.

1.2 Notation ($\mathbf{N}, \mathbf{Z}, \mathbf{Q}, \emptyset$.) A few sets appear so frequently that they have standard names:

$$\begin{aligned}
\mathbf{N} &= \text{ set of natural numbers } = \{0, 1, 2, 3, \cdots\}. \\
\mathbf{Z} &= \text{ set of integers } = \{0, 1, -1, 2, -2, 3, -3, \cdots\}. \\
\mathbf{Q} &= \text{ set of rational numbers.} \\
&= \text{ set of fractions } \frac{p}{q} \text{ where } p, q \text{ are integers and } q \neq 0. \\
\mathbf{Q}^+ &= \text{ set of positive rational numbers.} \\
\emptyset &= \text{ empty set } = \{\ \} = \text{ set containing no objects.}
\end{aligned}$$

1.3 Notation ($\in, \notin$.) If A is a set and a is an object, we write

$$a \in A$$

(read this as "a is in A") to mean that a is an object in A, and we write

$$a \notin A$$

(read this as "a is not in A") to mean that a is not in A.

1.4 Example. Thus we have

$$\begin{aligned}
2 &\in \mathbf{Z}, \\
-2 &\notin \mathbf{N}, \\
2 &\in \{1, 2, 5\} \\
\{1, 2\} &\notin \{1, 2, 5\}. \qquad (1.5)
\end{aligned}$$

To see why (1.5) is true, observe that the only objects in $\{1, 2, 5\}$ are 1, 2, and 5. Since

$$\{1, 2\} \neq 1 \text{ and } \{1, 2\} \neq 2 \text{ and } \{1, 2\} \neq 5$$

it follows that $\{1, 2\} \notin \{1, 2, 5\}$.

1.6 Definition (Subset, $\subset$.) Let A and B be sets. We say that A *is a subset of* B and write

$$A \subset B$$

if and only if every object in A is also in B.

1.7 Example.

$$\begin{aligned} \mathbf{N} &\subset \mathbf{Z}, \\ \emptyset &\subset \mathbf{Z}, \\ \mathbf{Z} &\subset \mathbf{Z}, \\ \{1,2\} &\subset \{1,2,3\}, \\ \{1\} &\subset \mathbf{Z}, \end{aligned}$$

are all true statements. However

$$1 \subset \mathbf{Z} \tag{1.8}$$

is not a statement, but an ungrammatical phrase, since $A \subset B$ has only been defined when A and B are sets, and 1 is not a set.

1.9 Definition (Set equality.) Two sets A and B are considered to be the same if and only if they contain exactly the same objects. In this case we write

$$A = B.$$

Thus $A = B$ if and only if $A \subset B$ and $B \subset A$.

1.10 Example.

$$\begin{aligned} \{1,2,3\} &= \{3,1,1,2\} \\ \{1,2,3,4\} &= \{1, 2+1, 3+1, 1+1, 2+2\} \end{aligned}$$

1.2 Propositions

1.11 Definition (Proposition.) A *proposition* is a statement that is either true or false.

1.12 Example. Both

$$1+1=2$$

and

$$1+1=3$$

are propositions. The first is true and the second is false. I will consider

$$13 \text{ is a prime number}$$

to be a proposition, because I expect that you know what a prime number is. However, I will not consider

$$13 \text{ is an unlucky number}$$

to be a proposition (unless I provide you with a definition for *unlucky number*).

The proposition

$$\{1\} \subset \mathbf{N}$$

is true, and the proposition

$$\mathbf{N} \in \mathbf{N}$$

is false, but

$$1 \subset \mathbf{N}$$

is not a proposition but rather a meaningless statement (cf (1.8)). Observe that "$x \subset y$" makes sense whenever x and y are sets, and " $x \in y$" makes sense when y is a set, and x is any object. Similarly

$$\frac{1}{0} = 5$$

is meaningless rather than false, since division by zero is not defined., i.e. I do not consider $\frac{1}{0}$ to be a name for any object.

1.13 Definition (and, or, not.) If P and Q are propositions, then

$$P \text{ or } Q \qquad P \text{ and } Q \qquad \text{not } P$$

are propositions, and (P or Q) is true if and only if at least one of P, Q is true; (P and Q) is true if and only if both of P, Q are true; (not P) is true if and only if P is false.

1.14 Example.

$$\begin{array}{ccc}(1+1=2) & \text{and} & (2+2=4),\\ (1+1=2) & \text{or} & (1+1=3),\\ (1+1=2) & \text{or} & (2+2=4),\end{array}$$

are all true propositions.

1.15 Notation ($\neq, \notin$.) We abbreviate

$$\text{not } (a=b) \text{ by } a \neq b,$$

and we abbreviate

$$\text{not } (a \in A) \text{ by } a \notin A.$$

1.16 Notation ($\Longrightarrow$) If P and Q are propositions, we write

$$P \Longrightarrow Q \tag{1.17}$$

to denote the proposition "P implies Q".

1.18 Example. If x, y, z are integers then all of the following are true:

$$(x=y) \quad \Longrightarrow \quad (z \cdot x = z \cdot y). \tag{1.19}$$

$$(x=y) \quad \Longrightarrow \quad (x+z = y+z). \tag{1.20}$$

$$(x \neq y) \quad \Longrightarrow \quad ((z=x) \Longrightarrow (z \neq y)). \tag{1.21}$$

The three main properties of implication that we will use are:

If P is true, and $(P \Longrightarrow Q)$ is true, then Q is true.
If $(P \Longrightarrow Q)$ is true and Q is false, then P is false.
If $(P \Longrightarrow Q)$ is true and $(Q \Longrightarrow R)$ is true, then $(P \Longrightarrow R)$ is true. (1.22)

We denote property (1.22) by saying that $\Longrightarrow$ is *transitive.*

1.23 Example. The meaning of a statement like

$$(1=2) \Longrightarrow (5=7) \tag{1.24}$$

or

$$(1=2) \Longrightarrow (5 \neq 7) \tag{1.25}$$

may not be obvious. I claim that both (1.24) and (1.25) should be true.
"Proof" of (1.24):

$$\begin{aligned}(1=2) &\implies (2\cdot 1 = 2\cdot 2) \text{ (by (1.19))},\\ (2\cdot 1 = 2\cdot 2) &\implies (2\cdot 1+3 = 2\cdot 2+3) \text{ (by (1.20))},\end{aligned}$$

and

$$(2\cdot 1+3 = 2\cdot 2+3) \implies (5=7),$$

so by transitivity of $\implies$,

$$(1=2) \implies (5=7). \;\|$$

"Proof" of (1.25):

$$(1=2) \implies (1+4 = 2+4) \text{ (by (1.20))}$$

so

$$\begin{aligned}(1=2) &\implies (5=6),\\ (5=6) &\implies (5\neq 7) \text{ (by (1.21), since } 6\neq 7),\end{aligned}$$

so

$$(1=2) \implies (5\neq 7) \text{ by transitivity of } \implies. \;\|$$

The previous example is supposed to motivate the following assumption:

A false proposition implies everything,

i.e.

If P is false, then $(P \implies Q)$ is true for all propositions Q.

1.26 Example. For every $x \in \mathbf{Z}$, the proposition

$$x = 2 \implies x^2 = 4$$

is true. Hence all three of the statements below are true:

$$2 = 2 \implies 2^2 = 4, \tag{1.27}$$

$$-2 = 2 \implies (-2)^2 = 4, \tag{1.28}$$

$$3 = 2 \implies 3^2 = 4. \tag{1.29}$$

Proposition (1.28) is an example of a false statement implying a true one, and proposition (1.29) is an example of a false statement implying a false one. Equations (1.27) and (1.28) together provide motivation for the assumption.

Every statement implies a true statement;

i.e.

If Q is true then $(P \implies Q)$ is true for all propositions P.

The following table shows the conditions under which $(P \implies Q)$ is true.

P	Q	$P \implies Q$
true	true	true
true	false	false
false	true	true
false	false	true

Thus a true statement does not imply a false one. All other sorts of implications are valid.

1.30 Notation ($P \implies Q \implies R \implies S$.) Let P, Q, R ,S be propositions. Then

$$P \implies Q \implies R \implies S \tag{1.31}$$

is an abbreviation for

$$((P \implies Q) \text{ and } (Q \implies R)) \text{ and } (R \implies S).$$

It follows from transitivity of $\implies$ that if (1.31) is true, then $P \implies S$ is true.

Note that (1.31) is *not* an abbreviation for

$$((P \text{ and } (P \implies Q)) \text{ and } (Q \implies R)) \text{ and } (R \implies S);$$

i.e., when I write (1.31), I do not assume that P is true.

1.32 Definition (Equivalence of propositions, $\iff$.) Let P, Q be propositions. We say that P and Q are *equivalent* and write

$$P \iff Q$$

(read this "P is equivalent to Q" or "P if and only if Q") to mean

$$(P \implies Q) \text{ and } (Q \implies P) \tag{1.33}$$

If either (P, Q are both true) or (P, Q are both false), then $(P \iff Q)$ is true. If one of P, Q is false, and the other is true, then one of $(P \implies Q)$, $(Q \implies P)$ has the form $\langle\text{true}\rangle \implies \langle\text{false}\rangle$, and hence in this case $(P \iff Q)$ is false. Thus

$$(P \iff Q) \text{ is true if and only if } P, Q \text{ are both true or both false.}$$

1.3 Equality

1.34 Notation (=.) Let x and y be (names of) objects. I write

$$x = y$$

to mean that x and y are names for the same object. I will not make a distinction between an object and its name.

$$\text{For all objects } x, \quad x = x. \tag{1.35}$$

We describe this property by saying that *equality is reflexive.*

$$\text{For all objects } x, y, \quad (x = y) \implies (y = x). \tag{1.36}$$

We describe this property by saying that *equality is symmetric.*

$$\text{For all objects } x, y, z \quad ((x = y) \text{ and } (y = z)) \implies (x = z). \tag{1.37}$$

We describe this property by saying that *equality is transitive.*

Let P be a proposition involving the object x. Let Q be a proposition obtained by replacing any or all occurrences of x in P by y. Then $P \iff Q$. We call this property of equality the *substitution property.*

1.38 Examples. Suppose that x, y are integers, and $x = y$. Then

$$\big((x+3)(x+4) = 28 + x\big) \iff \big((x+3)(y+4) = 28 + y\big),$$

and

$$\big((x+3)(x+4) = 28 + x\big) \iff \big((y+3)(y+4) = 28 + y\big),$$

and

$$\big((x+3)(x+4)=28+x\big) \iff \big((y+3)(x+4)=28+x\big).$$

We will frequently make statements like

$$(x=y) \implies (x+3=y+3).$$

The justification for this is

$$x+3=x+3 \qquad \text{(by reflexivity of } = .)$$

Hence, if $x=y$, then by the substitution property,

$$x+3=y+3.$$

1.39 Warning. Because we are using a vague notion of proposition, the substitution property of equality as stated is not precisely true. For example, although

$$5=2+3 \tag{1.40}$$

and

$$5\cdot 4=20 \tag{1.41}$$

are both true, the result of substituting the 5 in the second equation by $2+3$ yields

$$2+3\cdot 4=20$$

which is false.

The proper conclusion that follows from (1.40) and (1.41) is

$$(2+3)\cdot 4=20.$$

(The use of parentheses is discussed in Remark 2.50.)

1.42 Notation ($a=b=c=d$.) Let a,b,c,d be objects. We write

$$a=b=c=d \tag{1.43}$$

as an abbreviation for

$$((a=b) \text{ and } (b=c)) \text{ and } (c=d).$$

If (1.43) is true, then by several applications of transitivity, we conclude that

$$a=d.$$

1.4 More Sets

1.44 Definition (Proposition Form.) Let S be a set. A *proposition form* P on S is a rule that assigns to each element x of S a unique proposition, denoted by $P(x)$.

1.45 Examples. Let

$$P(n) = \text{“}n^2 - 6n + 8 = 0\text{” for all } n \in \mathbf{Z}.$$

Then P is a proposition form on $\mathbf{Z}$. $P(0)$ is false, and $P(2)$ is true. Note that P is neither true nor false. A proposition form is not a proposition.

Let

$$Q(n) = \text{“}n^2 - 4 = (n-2)(n+2)\text{” for all } n \in \mathbf{Z}. \tag{1.46}$$

Then Q is a propostion form, and $Q(n)$ is true for all $n \in \mathbf{Z}$. Note that Q is not a proposition, but if

$$R = \text{“}n^2 - 4 = (n-2)(n+2) \text{ for all } n \in \mathbf{Z}\text{”} \tag{1.47}$$

then R is a proposition and R is true. Make sure that you see the difference between the right sides of (1.46) and (1.47). The placement of the quotation marks is crucial. When I define a proposition I will often enclose it in quotation marks, to prevent ambiguity. Without the quotation marks, I would not be able to distinguish between the right sides of (1.46) and (1.47). If I see a statement like

$$P(n) = n^2 - 6n + 8 = 0$$

without quotation marks, I immediately think this is a statement of the form $x = y = z$ and conclude that $P(n) = 0$.

1.48 Notation. Let S be a set, and let P be a proposition form on S. Then

$$\{x \in S : P(x)\} \tag{1.49}$$

denotes the set of all objects x in S such that $P(x)$ is true. (Read (1.49) as “the set of all x in S such that $P(x)$”.)

1.50 Examples.

$$\{x \in \mathbf{N} : x^2 - 6x + 8 = 0\} = \{2, 4\}$$

$$\{x \in \mathbf{Z} : x = 2n \text{ for some } n \in \mathbf{Z}\} = \text{ set of even integers.}$$

Variations on this notation are common. For example,

$$\{n^2 + n : n \in \mathbf{Z}\}$$

represents the set of all numbers of the form $n^2 + n$ where $n \in \mathbf{Z}$.

1.51 Definition (Union, intersection, difference.) Let A be a set, let $\mathcal{S}$ be the set of all subsets of A, and let R, T be elements of $\mathcal{S}$. We define the *intersection* $R \cap T$ of R and T by

$$R \cap T = \{x \in A : x \in R \text{ and } x \in T\};$$

we define the *union* $R \cup T$ of R and T by

$$R \cup T = \{x \in A : x \in R \text{ or } x \in T\};$$

and we define the difference $R \setminus T$ by

$$R \setminus T = \{x \in R : x \notin T\}.$$

1.52 Examples. If $R = \{1, 2, 3\}$ and $T = \{2, 3, 4, 5\}$, then

$$\begin{aligned} R \cap T &= \{2, 3\} \\ R \cup T &= \{1, 2, 3, 4, 5\} \\ R \setminus T &= \{1\} \\ T \setminus R &= \{4, 5\}. \end{aligned}$$

1.53 Definition (Ordered pairs and triples.) Let a, b, c be objects (not necessarily all different). The ordered pair (a, b) is a set-like combination of a and b into a single object, in which a is designated as the *first element* and b is designated as the *second element.* The ordered triple (a, b, c) is a similar construction having a for its first element, b for its second element and c for its third element. Two ordered pairs (triples) are equal if and only if they have the same first elements, the same second elements, (and the same third elements). Thus

$$\begin{aligned} (a, b) = (b, a) &\iff b = a. \\ (a, b) = (x, y) &\iff a = x \text{ and } b = y. \\ (a, b, c) = (x, y, z) &\iff (a = x) \text{ and } (b = y) \text{ and } (c = z). \end{aligned}$$

1.54 Warning. Ordered pairs should not be confused with sets.

$$\begin{aligned} \{1,2\} &= \{2,1\}. \\ (1,2) &\neq (2,1). \end{aligned}$$

1.55 Definition (Cartesian product, $\times$.) If A and B are sets, we define the set $A \times B$ by

$$\begin{aligned} A \times B &= \text{ the set of all ordered pairs } (a,b) \text{ where } a \in A \text{ and } b \in B. \\ A^2 &= A \times A. \\ A^3 &= \text{ the set of all ordered triples } (a,b,c) \text{ where } a,b,c \text{ are in } A. \end{aligned}$$

$A \times B$ is called the *Cartesian Product* of A and B.

1.56 Example. If $\mathbf{R}$ is the set of real numbers, then $\mathbf{R}^2$ is the set of all ordered pairs of real numbers. You are familiar with the fact that ordered pairs of real numbers can be represented as points in the plane, so you can think of $\mathbf{R}^2$ or $\mathbf{R} \times \mathbf{R}$ as being the points in the plane.

1.5 Functions

1.57 Definition (Function.) Let A, B be sets, and let f be a rule that assigns to each element a in A a unique element (denoted by $f(a)$) in B. The ordered triple (A, B, f) is called a *function with domain A and codomain B.* We write

$$f\colon A \to B$$

to indicate that (A, B, f) is a function. It follows from the definition that two functions are equal if and only if they have the same domain, the same codomain, and the same rule: If $f\colon A \to B$ and $g\colon A \to B$, I say that the rule f and the rule g are the same if and only if $f(a) = g(a)$ for all $a \in A$. We usually say "the function f" when we mean "the function (A, B, f)," i.e., we name a function by giving just the name for its rule.

1.58 Examples. Let

$$\begin{aligned} &f\colon \mathbf{N} \to \mathbf{Z}, \\ &g\colon \mathbf{Z} \to \mathbf{Z}, \\ &h\colon \mathbf{Z} \to \mathbf{N}, \\ &k\colon \mathbf{Z} \to \mathbf{Z}, \end{aligned}$$

be defined by

$$\begin{aligned} f(n) &= (n-2)(n-3) \text{ for all } n \in \mathbf{N}, \\ g(n) &= (n-2)(n-3) \text{ for all } n \in \mathbf{Z}, \\ h(n) &= (n-2)(n-3) \text{ for all } n \in \mathbf{Z}, \\ k(w) &= w^2 - 5w + 6 \text{ for all } w \in \mathbf{Z}. \end{aligned}$$

Then

$$\begin{aligned} f &\neq g \quad (f \text{ and } g \text{ have different domains }) \\ g &\neq h \quad (g \text{ and } h \text{ have different codomains }) \\ g &= k. \end{aligned}$$

If P is a proposition form on a set S, then P determines a function whose domain is S and whose codomain is the set of all propositions.

1.6 *Russell's Paradox

There are some logical paradoxes connected with the theory of sets. The book *The Foundations of Mathematics* by Evert Beth discusses 17 different paradoxes[9, pp. 481-492]. Here I discuss just one of these which was published by Bertrand Russell in 1903[43, ¶78,¶¶100-106].

Let $\mathcal{S}$ be the set of all sets, let $\mathcal{I}$ be the set of all infinite sets, and let $\mathcal{F}$ be the set of all finite sets. Then we have

$$\begin{array}{ccc} \mathcal{F} \in \mathcal{S} & \mathcal{F} \in \mathcal{I} & \mathcal{F} \notin \mathcal{F} \\ \mathcal{I} \in \mathcal{S} & \mathcal{I} \in \mathcal{I} & \mathcal{I} \notin \mathcal{F} \\ \mathcal{S} \in \mathcal{S} & \mathcal{S} \in \mathcal{I} & \mathcal{S} \notin \mathcal{F} \\ 2 \notin \mathcal{S} & \{2\} \notin \mathcal{I} & \{\mathcal{S}\} \in \mathcal{F} \end{array}$$

Here $\mathcal{F} \in \mathcal{I}$ since there are infinitely many finite sets. $\{\mathcal{S}\} \in \mathcal{F}$ since $\{\mathcal{S}\}$ contains just one element, which is the set of all sets. Also $2 \notin \mathcal{S}$ since 2 is not a set. Next, let

$$\mathcal{R} = \{x \in \mathcal{S} : x \notin x\}.$$

Then for all $x \in \mathcal{S}$ we have

$$x \in \mathcal{R} \iff x \notin x. \tag{1.59}$$

Thus

$$\begin{array}{lll} \mathcal{S} \notin \mathcal{R} & \text{since} & \mathcal{S} \in \mathcal{S}, \\ \mathcal{I} \notin \mathcal{R} & \text{since} & \mathcal{I} \in \mathcal{I}, \\ \mathcal{F} \in \mathcal{R} & \text{since} & \mathcal{F} \notin \mathcal{F}, \\ \mathbf{Z} \in \mathcal{R} & \text{since} & \mathbf{Z} \notin \mathbf{Z}. \end{array}$$

We now ask whether $\mathcal{R}$ is in $\mathcal{R}$. According to (1.59),

$$\mathcal{R} \in \mathcal{R} \iff \mathcal{R} \notin \mathcal{R},$$

i.e., $\mathcal{R}$ is in $\mathcal{R}$ if and only if it isn't!

I believe that this paradox has never been satisfactorily explained. A large branch of mathematics (axiomatic set theory) has been developed to get rid of the paradox, but the axiomatic approaches seem to build a fence covered with "keep out" signs around the paradox rather than explaining it. Observe that the discussion of Russell's paradox does not involve any complicated argument: it lies right on the surface of set theory, and it might cause one to wonder what other paradoxes are lurking in a mathematics based on set theory.

1.60 Warning. Thinking too much about this sort of thing can be dangerous to your health.

> The poet and grammarian Philitas of Cos is even said to have died prematurely from exhaustion, owing to his desperate efforts to solve the paradox.[9, page 493]

Philitas was concerned about a different paradox, but Russell's paradox is probably more deadly.

Chapter 2

Fields

2.1 Binary Operations

2.1 Definition (Binary operation.) Let A be a set. A *binary operation* on A is a function $\circ\colon A \times A \to A$. Binary operations are usually denoted by special symbols such as

$$+, -, \cdot, /, \times, \circ, \wedge, \vee, \cup, \cap$$

rather than by letters. If $\circ\colon A \times A \to A$ is a binary operation, we write $a \circ b$ instead of $\circ(a, b)$. By the definition of function (1.57), a binary operation is a triple $(A \times A, A, \circ)$, but as is usual for functions, we refer to "the binary operation $\circ$" instead of "the binary operation $(A \times A, A, \circ)$".

2.2 Examples. The usual operations of addition $(+)$, subtraction $(-)$ and multiplication $(\cdot)$ are binary operations on $\mathbf{Z}$ and on $\mathbf{Q}$. Subtraction is not a binary operation on $\mathbf{N}$, because $3 - 5$ is not in $\mathbf{N}$. Division is not a binary operation on $\mathbf{Q}$, because division by 0 is not defined. However, division is a binary operation on $\mathbf{Q} \setminus \{0\}$.

Let $\mathcal{S}$ be the set of all sets.[1] Then union $(\cup)$ and intersection $(\cap)$ and set difference $(\setminus)$ are binary operations on $\mathcal{S}$.

[1] Some mathematicians cringe at the mention of the set of all sets, because it occurs in Russell's paradox, and in some other set-theoretic paradoxes. Any cringers can modify this example and the next one however they please.

Let $\mathcal{P}$ be the set of all propositions. Then *and* and *or* are binary operations on $\mathcal{P}$. In mathematical logic, *and* is usually represented by $\wedge$ or &, and *or* is represented by $\vee$ or $\bigvee$.

2.3 Definition (Identity element.) Let $\circ$ be a binary operation on a set A. An element $e \in A$ is an *identity element for* $\circ$ (or just an *identity for* $\circ$) if

$$\text{for all } a \in A, \quad e \circ a = a = a \circ e.$$

2.4 Examples. 0 is an identity for addition on $\mathbf{Z}$, and 1 is an identity for multiplication on $\mathbf{Z}$. There is no identity for subtraction on $\mathbf{Z}$, since for all $e \in \mathbf{Z}$ we have

$$\begin{aligned} e \text{ is an identity for } - &\implies e - 1 = 1 \text{ and } 1 = 1 - e, \\ &\implies e = 2 \text{ and } e = 0, \\ &\implies 0 = 2. \end{aligned} \tag{2.5}$$

Since (2.5) is false, the first statement is also false; i.e., for all $e \in \mathbf{Z}$, e is not an identity for $-$. |||

2.6 Exercise. Let $\mathcal{S}(\mathbf{Z})$ denote the set of all subsets of $\mathbf{Z}$. Then union $\cup$ and intersection $\cap$ are binary operations on $\mathcal{S}(\mathbf{Z})$. Is there an identity element for $\cup$? If so, what is it? Is there an identity element for $\cap$? If so, what is it?

2.7 Theorem (Uniqueness of identities.) *Let $\circ$ be a binary operation on a set A. Suppose that e, f are both identity elements for $\circ$. Then $e = f$. (Hence we usually talk about* the *identity for $\circ$, rather than* an *identity for $\circ$.)*

Proof: Let e, f be identity elements for $\circ$. Then

$$e = e \circ f \qquad \text{(since } f \text{ is an identity for } \circ)$$

and

$$e \circ f = f \qquad \text{(since } e \text{ is an identity for } \circ).$$

It follows that $e = f$. |||

2.8 Remark. The conclusion of the previous proof used transitivity of equality (Cf page 12). I usually use the properties of equality without explicitly mentioning them.

2.9 Definition (Inverse.) Let $\circ$ be a binary operation on a set A, and suppose that there is an identity element e for $\circ$. (We know that this identity is unique.) Let x be an element of A. We say that an element y of A *is an inverse for* x *under* $\circ$ if

$$x \circ y = e = y \circ x.$$

We say that x is *invertible under* $\circ$ if x has an inverse under $\circ$.

2.10 Examples. For the operation $+$ on $\mathbf{Z}$, every element x has an inverse, namely $-x$.

For the operation $+$ on $\mathbf{N}$, the only element that has an inverse is 0; 0 is its own inverse.

For the operation $\cdot$ on $\mathbf{Z}$, the only invertible elements are 1 and -1. Both of these elements are equal to their own inverses.

If $\circ$ is any binary operation with identity e, then $e \circ e = e$, so e is always invertible, and e is equal to its own inverse.

2.11 Exercise. Let $\mathcal{S}(\mathbf{Z})$ be the set of all subsets of $\mathbf{Z}$. In exercise 2.6 you should have shown that both of the operations $\cup$ and $\cap$ on $\mathcal{S}(\mathbf{Z})$ have identity elements.

a Which subsets A of $\mathbf{Z}$ have inverses for $\cup$? What are these inverses?

b Which subsets A of $\mathbf{Z}$ have inverses for $\cap$? What are these inverses?

2.12 Entertainment. Let S be a set, and let $\mathcal{S}(S)$ be the set of all subsets of S. Define a binary operation Δ on $\mathcal{S}(S)$ by

$$A \Delta B = (A \setminus B) \cup (B \setminus A) \text{ for all } A, B \in \mathcal{S}(S).$$

Thus $A\Delta B$ consists of all points that are in exactly one of the sets A, B. We call $A\Delta B$ the *symmetric difference* of A and B. Show that there is an identity element for Δ, and that every element of $\mathcal{S}(S)$ is invertible for Δ.

2.13 Definition (Associative operation.) Let $\circ$ be a binary operation on a set A. We say that $\circ$ is *associative* if

$$\text{for all } a, b, c \in A, \quad a \circ (b \circ c) = (a \circ b) \circ c.$$

2.14 Examples. Both $+$ and $\cdot$ are associative operations on $\mathbf{Q}$. Subtraction $(-)$ is not an associative operation on $\mathbf{Z}$, since

$$(1-1)-1 \neq 1-(1-1).$$

Observe that to show that a binary operation $\circ$ on a set A is not associative, it is sufficient to find one point (a,b,c) in A^3 such that $a \circ (b \circ c) \neq (a \circ b) \circ c$.

You should convince yourself that both $\cap$ and $\cup$ are associative operations on the set $\mathcal{S}$ of all sets. If A, B, C are sets, then

$$\begin{aligned} A \cap (B \cap C) = (A \cap B) \cap C &= \text{set of points in all three of } A, B, C \\ A \cup (B \cup C) = (A \cup B) \cup C &= \text{set of points in at least one of } A, B, C. \end{aligned}$$

2.15 Theorem (Uniqueness of inverses.) *Let $\circ$ be an associative operation on a set A, and suppose that there is an identity e for $\circ$. Let $x, y, z \in A$. If y and z are inverses for x, then $y = z$.*

Proof: Since y and z are inverses for x, we have

$$y \circ x = e = x \circ y$$

and

$$z \circ x = e = x \circ z.$$

Hence,

$$y = y \circ e = y \circ (x \circ z) = (y \circ x) \circ z = e \circ z = z. \ \|$$

2.16 Definition (Invertible element.) Let $\circ$ be a binary operation on a set A, having an identity element e. I will say that an element $x \in A$ is *invertible* for $\circ$, if x has an inverse. If $\circ$ is associative, then every invertible element for $\circ$ has a unique inverse, which I call *the inverse for x under $\circ$*.

2.17 Theorem (Double inverse theorem.) *Let $\circ$ be an associative binary operation on a set A, with identity e, and let $x \in A$. If x is invertible for $\circ$, let x^{-1} denote the (unique) inverse for x. Then x^{-1} is invertible and $(x^{-1})^{-1} = x$.*

Proof: If y is the inverse for x, then

$$y \circ x = e = x \circ y.$$

But this is exactly the condition for x to be the inverse for y. $\|$

2.18 Examples. As special cases of the double inverse theorem, we have

$$-(-x) = x \quad \text{for all } x \in \mathbf{Q}$$

and

$$(x^{-1})^{-1} = x \quad \text{for all } x \in \mathbf{Q} \setminus \{0\}.$$

Here, as usual, x^{-1} denotes the multiplicative inverse for x.

2.19 Theorem (Cancellation law.) *Let $\circ$ be an associative binary operation on a set A, having identity e, and let $v \in A$ be an invertible element for $\circ$. Then*

$$\textit{for all } x, y \in A \ \ (x \circ v = y \circ v) \implies (x = y), \tag{2.20}$$

and

$$\textit{for all } x, y \in A \ \ (v \circ x = v \circ y) \implies (x = y). \tag{2.21}$$

Proof: Let v be invertible, and let w be the inverse for v. Then for all $x, y \in A$,

$$\begin{aligned} x \circ v = y \circ v &\implies (x \circ v) \circ w = (y \circ v) \circ w \\ &\implies x \circ (v \circ w) = y \circ (v \circ w) \\ &\implies x \circ e = y \circ e \\ &\implies x = y. \end{aligned}$$

This proves (2.20). The proof of (2.21) is left to you.

2.22 Exercise. Prove the second half of the cancellation theorem.

2.23 Warning. If $\circ$ is a binary operation on a set A, then an expression such as

$$a \circ b \circ c \circ d$$

is ambiguous, and should not be written without including a way of resolving the ambiguity. For example in $\mathbf{Z}$, $a - b - c - d$ could be interpreted as any of

$$(a - (b - c)) - d, \tag{2.24}$$
$$((a - b) - c) - d, \tag{2.25}$$
$$(a - b) - (c - d), \tag{2.26}$$
$$a - (b - (c - d)), \tag{2.27}$$
$$a - ((b - c) - d). \tag{2.28}$$

2.29 Entertainment. Is it possible to find integers a, b, c, d such that the five numbers (2.24)-(2.28) are all different? If so, find four such integers

2.30 Exercise. Let $\circ$ be an associative binary operation on a set A, and let a, b, c, d be elements of A.

a) Show that there are five different ways to sensibly put parentheses in the expression
$$a \circ b \circ c \circ d,$$
and that all five ways produce the same result. (Each way will use two sets of parentheses, e.g. $(a \circ (b \circ c)) \circ d$ is one way. If you arrange things correctly, you will just need to apply the associative law four times.)

b) Show that if a, b, c, d, e are elements of A, then there are 14 ways to put parentheses in
$$a \circ b \circ c \circ d \circ e,$$
and that all 14 ways lead to the same result. Here each sensible way of inserting parentheses will involve three pairs.

2.31 Entertainment. Show that there are 42 ways to put parentheses in
$$a_1 \circ a_2 \circ a_3 \circ a_4 \circ a_5 \circ a_6.$$
This can be done without actually writing down all the ways (and there isn't much point in writing down all the ways, because no one would read it if you did). If you did part b. of the previous exercise in such a way that really showed that there are just 14 ways, you should be able to do this, and then to calculate the number of ways to parenthesize products with seven factors. There is a simple (but hard to guess) formula for the number of ways to put parentheses in products with n factors. You can find the formula, along with a derivation, in [44].

2.32 Definition (Commutative operation.) Let $\circ$ be a binary operation on a set A. We say that $\circ$ is *commutative* if
$$\text{for all } a, b \in A \quad a \circ b = b \circ a.$$

2.33 Examples. Both $+$ and $\cdot$ are commutative operations on $\mathbf{Q}$. However $-$ is not a commutative operation on $\mathbf{Q}$, because $3 - 2 \neq 2 - 3$.

The operations $\cup$ and $\cap$ are both commutative operations on the set $\mathcal{S}$ of all sets, and *and* and *or* are commutative operations on the set $\mathcal{P}$ of all propositions. The set difference operation ($\setminus$) is not commutative on $\mathcal{S}$, since

$$\{1,2\} \setminus \{2,3\} \neq \{2,3\} \setminus \{1,2\}.$$

2.2 Some Examples

2.34 Example (non-commutative *and*.) Many computer languages support an *and* operation that is not commutative. Here is a script of a Maple session. My statements are shown in `typewriter font`. Maple's responses are shown in *italics*.

```
> P := (x = 1/y);
```

$$P := x = \frac{1}{y}$$

```
> Q := (x*y=1);
```

$$Q := x\,y = 1$$

```
> y:= 0;
```

$$y := 0$$

```
> x := 1;
```

$$x := 1$$

```
> Q and P;
```

false

```
> P and Q;
```

Error, division by zero

When evaluating Q *and* P, Maple first found that Q is false, and then, without looking at P, concluded that Q *and* P must be false. When evaluating P *and* Q, Maple first tried to evaluate P, and in the process discovered that P is not a proposition. Mathematically, both Q *and* P and P *and* Q are errors when $y = 0$ and $x = 1$. Many programmers consider the non-commutativity of *and* to be a *feature* (i.e. good), rather than a *bug* (i.e. bad).

2.35 Example (Calculator operations.) Let $\widetilde{C}$ denote the set of all numbers that can be entered into your calculator. The exact composition of $\widetilde{C}$ depends on the model of your calculator. Let $C = \widetilde{C} \cup \{E\}$ where E is some object not in $\widetilde{C}$. I will call E *the error.* I think of E as the result produced when you enter $1/0$. Define four binary operations $\oplus, \ominus, \odot$, and $\oslash$ on C by

$$\begin{aligned} a \oplus b &= \text{result produced when you calculate } a + b. \\ a \ominus b &= \text{result produced when you calculate } a - b. \\ a \odot b &= \text{result produced when you calculate } a \cdot b. \\ a \oslash b &= \text{result produced when you calculate } a/b. \end{aligned}$$

On my calculator

$$\begin{aligned} &2 \oplus 2 = 4. \\ &10^{50} \odot 10^{50} = E. \\ &1111111111 \odot 1111111111 = 1.2345679 \times 10^{18}. \end{aligned}$$

If $\circ$ denotes any of $\oplus, \ominus, \odot, \oslash$, I define

$$E \circ x = E = x \circ E \text{ for all } x \in C.$$

On all calculators with which I am familiar, $\oplus$ and $\odot$ are commutative operations, 0 is an identity for $\oplus$, 1 is an identity for $\odot$, and every element of C except for E is invertible for $\oplus$. On my calculator

$$1 \oslash 3 = 0.333333333 \tag{2.36}$$

$$0.333333333 \odot 3 = 0.999999999 \tag{2.37}$$

$$0.333333333 \odot 3.000000003 = 1 \tag{2.38}$$

$$0.333333333 \odot 3.000000004 = 1. \tag{2.39}$$

Thus 0.333333333 has two different inverses! It follows from theorem 2.15 that $\odot$ is not associative. Your calculator may give different results for the calculations (2.38) and (2.39) but none of the calculator operations are associative.

2.40 Exercise. Verify that calculator addition ($\oplus$) and calculator multiplication ($\odot$) are not associative, by finding calculator numbers a, b, c, x, y, and z such that $a \oplus (b \oplus c) \neq (a \oplus b) \oplus c$, and $x \odot (y \odot z) \neq (x \odot y) \odot z$.

2.41 Notation. If $n \in \mathbf{N}$, let

$$\mathbf{Z}_n = \{x \in \mathbf{N}: x < n\}.$$

Hence, for example

$$\mathbf{Z}_5 = \{0, 1, 2, 3, 4\}.$$

2.42 Definition ($\oplus_n, \odot_n$.) Let $n \in \mathbf{N}$, with $n \geq 2$. We define two binary operations $\oplus_n$ and $\odot_n$ on $\mathbf{Z}_n$ by:

for all $a, b \in \mathbf{Z}_n$,

$$a \oplus_n b = \text{ remainder when } a + b \text{ is divided by } n$$

and for all $a, b \in \mathbf{Z}_n$,

$$a \odot_n b = \text{ remainder when } a \cdot b \text{ is divided by } n.$$

Thus,

$$\begin{aligned} 4 \oplus_5 4 &= 3 \quad \text{since } 4 + 4 = 1 \cdot 5 + 3, \\ 1 \odot_5 4 &= 4 \quad \text{since } 1 \cdot 4 = 0 \cdot 5 + 4, \end{aligned}$$

and

$$4 \odot_5 4 = 1 \quad \text{since } 4 \cdot 4 = 3 \cdot 5 + 1.$$

The operations $\oplus_n$ and $\odot_n$ are both commutative (since $+$ and $\cdot$ are commutative on $\mathbf{Z}$). Clearly 0 is an identity for $\oplus_n$, and 1 is an identity for $\odot_n$. Every element of $\mathbf{Z}_n$ is invertible for $\oplus_n$ and

$$\text{inverse for } k \text{ under } \oplus_n = \begin{cases} n - k & \text{if } k \neq 0 \\ 0 & \text{if } k = 0. \end{cases}$$

2.43 Definition (Multiplication table.) Let $\circ$ be a binary operation on a finite set $A = \{a_1, a_2, \cdots, a_n\}$ having n elements. We construct a *multiplication table* for $\circ$ as follows: We write down a table with n rows and n columns. Along the top of the table we list the elements of A as labels for the columns. Along the left side of the table we list the elements of A (in the same order) as labels for the rows. (See the figure to see what is meant by this.) If $(x, y) \in A^2$, we write the product $x \circ y$ in the box of our table whose row label is x and whose column label is y.

$\circ$	a_1	a_2	$\cdots$	a_n
a_1	$a_1 \circ a_1$	$a_1 \circ a_2$	$\cdots$	$a_1 \circ a_n$
a_2	$a_2 \circ a_1$	$a_2 \circ a_2$	$\cdots$	$a_2 \circ a_n$
$\vdots$	$\vdots$	$\vdots$		$\vdots$
a_n	$a_n \circ a_1$	$a_n \circ a_2$	$\cdots$	$a_n \circ a_n$

Multiplication table for $\circ$

2.44 Examples. Below are the multiplication tables for $\oplus_5$ and $\odot_5$:

$\oplus_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\odot_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

By looking at the multiplication table for $\odot_5$ we see that

$$\begin{array}{ll} 1 \odot_5 1 = 1 & 2 \odot_5 3 = 1 \\ 4 \odot_5 4 = 1 & 3 \odot_5 2 = 1. \end{array}$$

Hence all the non-zero elements of $\mathbf{Z}_5$ have inverses under $\odot_5$.

Both of the operations $\oplus_n$ and $\odot_n$ are associative. This follows from the fact that $+$ and $\cdot$ are associative operations on $\mathbf{Z}$, by a straightforward but lengthy argument. The details are given in appendix A.

2.45 Exercise. Write down the multiplication table for $\odot_6$ on $\mathbf{Z}_6$. Determine which elements of $\mathbf{Z}_6$ are invertible for $\odot_6$, and find the inverse for each invertible element.

2.46 Exercise. Let $\{x, y, z\}$ be a set containing three distinct elements. ($x \neq y$, $y \neq z$, $z \neq x$). Let $\circ$ be the binary operation on $\{x, y, z\}$ determined by the multiplication table:

	x	y	z
x	x	y	z
y	y	x	x
z	z	x	x

a) Show that there is an identity element for $\circ$. (Which of x, y, z is the identity?)

b) Show that y has two different inverses for $\circ$.

c) Explain why the result of part b does not contradict the theorem on uniqueness of inverses.

2.47 Note. An early example of a binary operation that was not an obvious generalization of one of the operations $+, -, \cdot, /$ on numbers was the use of union and intersection as binary operations on the set of all sets by George Boole[11]. In *Laws of Thought* (1854), Boole introduces the operation $+$ (for union) and $\times$ (for intersection) on "classes" (although he usually writes xy instead of $x \times y$). He explicitly states

$$\begin{aligned} x+y &= y+x \\ xy &= yx \\ x(y+z) &= xy+xz \end{aligned}$$

which he calls commutative and distributive laws. He does not mention associativity, and writes xyz without parentheses. He denotes "Nothing" by 0 and "the Universe" by 1, and notes that 0 and 1 have the usual properties. As an example of the distributive law, Boole gives

European men and women = European men and European women.

Boole's $+$ is not really a binary operation since he only defines $x+y$ when x and y have no elements in common.

The word *associative*, in its mathematical sense, was introduced by William Hamilton[24, p114] in 1843 in a paper on quaternions. According to [14, p284], the words *commutative* and *distributive* were introduced by François -Joseph Servois in 1813.

2.3 The Field Axioms

2.48 Definition (Field.) A *field* is a triple $(F, +, \cdot)$ where F is a set, and $+$ and $\cdot$ are binary operations on F (called *addition* and *multiplication* respectively) satisfying the following nine conditions. (These conditions are called the *field axioms.*)

1. **(Associativity of addition.)** *Addition* $(+)$ *is an associative operation on* F.

2. **(Existence of additive identity.)** *There is an identity element for addition.*

   We know that this identity is unique, and we will denote it by 0.

3. **(Existence of additive inverses.)** *Every element* x *of* F *is invertible for* $+$.

   We know that the additive inverse for x is unique, and we will denote it by $-x$.

4. **(Commutativity of multiplication.)** *Multiplication* $(\cdot)$ *is a commutative operation on* F.

5. **(Associativity of multiplication.)** *Multiplication is an associative operation on* F.

6. **(Existence of multiplicative identity.)** *There is an identity element for multiplication.*

   We know that this identity is unique, and we will denote it by 1.

7. **(Existence of multiplicative inverses.)** *Every element* x *of* F except possibly for 0 *is invertible for* $\cdot$.

   We know that the multiplicative inverse for x is unique, and we will denote it by x^{-1}. We do not assume 0 is not invertible. We just do not assume that it is.

8. **(Distributive law.)** *For all* x, y, z *in* F, $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$.

9. **(Zero-one law.)** *The additive identity and multiplicative identity are distinct; i.e.,* $0 \neq 1$.

We often speak of "the field F" instead of "the field $(F, +, \cdot)$".

2.49 Remark. Most calculus books that begin with the axioms for a field (e.g., [47, p5], [1, p18], [13, p5], [12, p554]) add an additional axiom.

10. **(Commutativity of addition.)** *Addition is a commutative operation on* F.

I have omitted this because, as Leonard Dickson pointed out in 1905[18, p202], it can be proved from the other axioms (see theorem 2.72 for a proof). I agree with Aristotle that

> It is manifest that it is far better to make the principles finite in number. Nay, they should be the fewest possible provided they enable all the same results to be proved. This is what mathematicians insist upon; for they take as principles things finite either in kind or in number[26, p178].

2.50 Remark (Parentheses.) The distributive law is usually written as

$$x \cdot (y + z) = x \cdot y + x \cdot z \tag{2.51}$$

The right side of (2.51) is ambiguous. There are five sensible ways to interpret it:

$$\begin{aligned} &x \cdot ((y + x) \cdot z)\,, \\ &x \cdot (y + (x \cdot z))\,, \\ &(x \cdot y) + (x \cdot z), \\ &((x \cdot y) + x) \cdot z \\ &(x \cdot (y + x)) \cdot z. \end{aligned}$$

The conventions presently used for interpreting ambiguous statements such as $x \cdot y + x \cdot z$ and involving operations $+, -, \cdot, /$ are:

1. Multiplication and division have equal precedence.
2. Addition and subtraction have equal precedence.
3. Multiplication has higher precedence than addition.

This means that to interpret

$$1 \cdot 2/3 + 4 \cdot 5 \cdot 6 - 7 \cdot 8 + 9, \tag{2.52}$$

you first read (2.52) from left to right and perform all the multipliations and divisions as you come to them, getting

$$((1 \cdot 2)/3) + ((4 \cdot 5) \cdot 6) - (7 \cdot 8) + 9. \tag{2.53}$$

Then read (2.53) from left to right performing all additions and subtractions as you come to them, getting

$$((((1 \cdot 2)/3) + ((4 \cdot 5) \cdot 6)) - (7 \cdot 8)) + 9.$$

When I was in high school, multiplication had higher precedence than division, so

$$a \cdot b/c \cdot d/e \cdot f$$

meant

$$((a \cdot b)/(c \cdot d))\,/(e \cdot f),$$

whereas today it means

$$((((a \cdot b)/c) \cdot d)\,/e) \cdot f.$$

In 1713, addition often had higher precedence than multiplication. Jacob Bernoulli [8, p180] wrote expressions like

$$n \cdot n + 1 \cdot n + 2 \cdot n + 3 \cdot n + 4$$

to mean

$$n \cdot (n + 1) \cdot (n + 2) \cdot (n + 3) \cdot (n + 4).$$

2.54 Examples. $\mathbf{Q}$ with the usual operations of addition and multiplication is a field.

$(\mathbf{Z}_5, \oplus_5, \odot_5)$ is a field. (See definition 2.42 for the definitions.) We showed in section 2.2 that $(\mathbf{Z}_5, \oplus_5, \odot_5)$ satisfies all the field axioms except possibly the distributive law. In appendix A, it is shown that the distributive property holds for $(\mathbf{Z}_n, \oplus_n, \odot_n)$ for all $n \in \mathbf{N}$, $n \geq 2$. (The proof assumes that the distributive law holds in $\mathbf{Z}$.)

For a general $n \in \mathbf{N}$, $n \geq 2$, the only field axiom that can possibly fail to hold in $(\mathbf{Z}_n, \oplus_n, \odot_n)$ is the existence of multiplicative inverses, so to determine whether $\mathbf{Z}_n$ is a field, it is just necessary to determine whether every non-zero element in $\mathbf{Z}_n$ is invertible for $\odot_n$.

2.55 Exercise. In each of the examples below, determine which field axioms are valid and which are not. Which examples are fields? In each case that an axiom fails to hold, give an example to show why it fails to hold.

a) $(\mathbf{Z}, +, \cdot)$ where $+$ and $\cdot$ are usual addition and multiplication.

b) $(G, +, \cdot)$ where $G = \mathbf{Q}^+ \cup \{0\}$ is the set of non-negative rational numbers, and $+$ and $\cdot$ are the usual addition and multiplication.

c) $(H, +, \cdot)$ where $H = \{x\}$ is a set with just one element and both $+$ and $\cdot$ are the only binary operation on H; i.e.,

$$x + x = x, \qquad x \cdot x = x.$$

d) $(\mathbf{Q}, \oplus, \odot)$ where both $\oplus$ and $\odot$ are the usual operation of addition on $\mathbf{Q}$, e.g., $3 \oplus 4 = 7$ and $3 \odot 4 = 7$.

2.56 Exercise. Determine for which values of $n = 2, 3, 4, 5, 6$, $(\mathbf{Z}_n, \oplus_n, \odot_n)$ is a field. (You already know that $n = 5$ produces a field.)

2.57 Notation (The field $\mathbf{Z}_n$.) Let $n \in \mathbf{N}$, $n \geq 2$ be a number such that $(\mathbf{Z}_n, \oplus_n, \odot_n)$ is a field. Then "the field $\mathbf{Z}_n$" means the field $(\mathbf{Z}_n, \oplus_n, \odot_n)$. I will often denote the operations in $\mathbf{Z}_n$ by $+$ and $\cdot$ instead of $\oplus_n$ and $\odot_n$.

2.58 Entertainment. Determine for which values of n in $\{7, 8, 9, 10, 11\}$ the system $(\mathbf{Z}_n, \oplus_n, \odot_n)$ is a field. If you do this you will probably conjecture the exact (fairly simple) condition on n that makes the system into a field.

2.4 Some Consequences of the Field Axioms.

2.59 Theorem (Cancellation laws.) *Let $(F, +, \cdot)$ be a field, let x, y, z be elements in F, and let $v \in F \setminus \{0\}$. Then*

$$x + z = y + z \implies x = y. \tag{2.60}$$
$$z + x = z + y \implies x = y. \tag{2.61}$$
$$x \cdot v = y \cdot v \implies x = y. \tag{2.62}$$
$$v \cdot x = v \cdot y \implies x = y. \tag{2.63}$$

(2.60) and (2.61) are called cancellation laws for addition, *and (2.62) and (2.63) are called* cancellation laws for multiplication.

Proof: All of these results are special cases of the cancellation law for an associative operation (theorem 2.19). |||

2.64 Theorem. *In any field* $(F, +, \cdot)$

$$-0 = 0 \text{ and } 1^{-1} = 1.$$

Proof: These are special cases of the remark made earlier that an identity element is always invertible, and is its own inverse. |||

2.65 Theorem (Double inverse theorem.) *In any field* $(F, +, \cdot)$,

$$\begin{array}{rl} \text{for all } x \in F & -(-x) = x, \\ \text{for all } x \in F\backslash\{0\} & (x^{-1})^{-1} = x. \end{array}$$

Proof: These are special cases of theorem 2.17. |||

I will now start the practice of calling a field F. If I say "let F be a field" I assume that the operations are denoted by $+$ and $\cdot$.

2.66 Theorem. *Let* F *be a field. Then*

$$\text{for all } a \in F, \quad a \cdot 0 = 0.$$

Proof: We know that $0 = 0 + 0$, and hence

$$a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0.$$

Also, $a \cdot 0 + 0 = a \cdot 0$, so

$$a \cdot 0 + 0 = a \cdot 0 + a \cdot 0.$$

By the cancellation law for addition, $0 = a \cdot 0$. |||

2.67 Corollary. *Let* F *be a field. Then for all* $a \in F$, $0 \cdot a = 0$.

2.68 Theorem. *Let* F *be a field. Then for all* x, y *in* F

$$\Big(x \cdot y = 0\Big) \implies \Big(x = 0 \text{ or } y = 0\Big). \tag{2.69}$$

Proof:

Case 1: Suppose $x = 0$. Then (2.69) is true because every statement implies a true statement.

Case 2: Suppose $x \neq 0$. By theorem 2.66, $x \cdot 0 = 0$, so

$$x \cdot y = 0 \implies x \cdot y = x \cdot 0.$$

Since $x \neq 0$, we can use the cancellation law for multiplication to get

$$\Big(x \cdot y = x \cdot 0\Big) \implies \Big(y = 0\Big) \implies \Big(x = 0 \text{ or } y = 0\Big),$$

and hence

$$\Big(x \cdot y = 0\Big) \implies \Big(x = 0 \text{ or } y = 0\Big).$$

Thus (2.69) holds in all cases. |||

2.70 Remark. We can combine theorem 2.66, corollary 2.67 and theorem 2.68 into the statement: In any field F,

$$\text{for all } x, y \in F \qquad x \cdot y = 0 \iff (x = 0 \text{ or } y = 0).$$

2.71 Exercise. Let F be a field. Prove that 0 has no multiplicative inverse in F.

2.72 Theorem (Commutativity of addition.) *Let F be any field. Then $+$ is a commutative operation on F.*

Proof: Let x, y be elements in F. Then since multiplication is commutative, we have

$$(1 + x) \cdot (1 + y) = (1 + y) \cdot (1 + x).$$

By the distributive law,

$$((1 + x) \cdot 1) + ((1 + x) \cdot y) = ((1 + y) \cdot 1) + ((1 + y) \cdot x)\,.$$

Since 1 is the multiplicative identity,

$$(1 + x) + ((1 + x) \cdot y) = (1 + y) + ((1 + y) \cdot x)\,,$$

and hence

$$1 + (x + ((1 + x) \cdot y)) = 1 + (y + ((1 + y) \cdot x)).$$

By the cancellation law for addition

$$x + ((1 + x) \cdot y) = y + ((1 + y) \cdot x)\,.$$

By commutativity of multiplication and the distributive law,

$$x + (y \cdot (1 + x)) = y + (x \cdot (1 + y))$$

and

$$x + ((y \cdot 1) + (y \cdot x)) = y + ((x \cdot 1) + (x \cdot y)).$$

Since 1 is the multiplicative identity and addition is associative

$$x + (y + (y \cdot x)) = y + (x + (x \cdot y))$$

and hence

$$(x + y) + (y \cdot x) = (y + x) + (x \cdot y).$$

Since multiplication is commutative

$$(x + y) + (x \cdot y) = (y + x) + (x \cdot y)$$

and by the cancellation law for addition,

$$x + y = y + x.$$

Hence, + is commutative. ‖

2.73 Remark. Let F be a field, and let $x, y \in F$. Then

$$\text{To prove } x = -y, \text{ it is sufficient to prove } x + y = 0. \tag{2.74}$$

$$\text{To prove } x = y^{-1}, \text{ it is sufficient to prove } x \cdot y = 1. \tag{2.75}$$

Proof:

$$\begin{aligned}
x + y = 0 &\implies ((x + y = 0) \text{ and } (y + x = 0)) \\
&\implies y = -x \text{ and } x = -y. \\
x \cdot y = 1 &\implies ((x \cdot y = 1) \text{ and } (y \cdot x = 1)) \\
&\implies x = y^{-1} \text{ and } y = x^{-1}.
\end{aligned}$$ ‖

2.76 Theorem. *Let F be a field. Then*

$$\textit{for all } x, y \in F, \qquad x \cdot (-y) = -(x \cdot y).$$

Proof: Let $x, y \in F$. By (2.74) it is sufficient to prove

$$x \cdot (-y) + x \cdot y = 0.$$

Well,

$$\begin{aligned} x \cdot (-y) + x \cdot y &= x \cdot ((-y) + y) \\ &= x \cdot 0 \\ &= 0. \ \| \end{aligned}$$

2.77 Exercise. Let F be a field, and let $a, b \in F$. Prove that

a) $(-a) \cdot b = -(a \cdot b)$.

b) $a \cdot (-1) = -a$.

c) $(-a) \cdot (-b) = a \cdot b$.

2.78 Exercise. Let F be a field and let b, d be non-zero elements in F. Prove that

$$b^{-1} \cdot d^{-1} = (b \cdot d)^{-1}.$$

2.79 Definition (Digits.) Let F be a field. We define

$$\begin{array}{ll} 2 = 1 + 1, & 6 = 5 + 1, \\ 3 = 2 + 1, & 7 = 6 + 1, \\ 4 = 3 + 1, & 8 = 7 + 1, \\ 5 = 4 + 1, & 9 = 8 + 1, \\ & t = 9 + 1. \end{array}$$

I'll call the set

$$\mathbf{D}_F = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

the set of *digits in* F. If a, b, c are digits, I define

$$ab = t \cdot a + b, \tag{2.80}$$

and

$$abc = t \cdot (ab) + c. \tag{2.81}$$

Here ab should not be confused with $a \cdot b$.

2.82 Example.

$$\begin{aligned} 10 &= t \cdot 1 + 0 = t. \\ 100 &= t \cdot 10 + 0 = t \cdot 10 = 10 \cdot 10. \\ 37 &= t \cdot 3 + 7 = 10 \cdot 3 + 7. \end{aligned}$$

In general, if $x \in F$, I define

$$x^2 = x \cdot x.$$

Then for all digits a, b, c

$$\begin{aligned} abc &= t \cdot (ab) + c = t \cdot (t \cdot a + b) + c = (t \cdot (t \cdot a) + t \cdot b) + c \\ &= ((t \cdot t) \cdot a + t \cdot b) + c \\ &= t^2 \cdot a + t \cdot b + c = 10^2 \cdot a + 10 \cdot b + c, \end{aligned}$$

so, for example

$$375 = 10^2 \cdot 3 + 10 \cdot 7 + 5.$$

2.83 Remark. The set $\mathbf{D}_F$ of digits in F may contain fewer than ten elements. For example, in $(\mathbf{Z}_5, \oplus_5, \odot_5)$,

$$\begin{aligned} 2 &= 1 \oplus_5 1 = 2. \\ 3 &= 2 \oplus_5 1 = 3. \\ 4 &= 3 \oplus_5 1 = 4. \\ 5 &= 4 \oplus_5 1 = 0. \end{aligned}$$

and you can see that $\mathbf{D}_{\mathbf{Z}_5} = \{0, 1, 2, 3, 4\}$.

2.84 Theorem. *In any field F, $2 + 2 = 4$ and $2 \cdot 2 = 4$.*

Proof:

$$\begin{aligned} 2 + 2 &= 2 + (1 + 1) && \text{(by definition of 2)} \\ &= (2 + 1) + 1 && \text{(by associativity of +)} \\ &= 3 + 1 && \text{(by definition of 3)} \\ &= 4 && \text{(by definition of 4).} \end{aligned}$$

Also,

$$2 \cdot 2 = 2 \cdot (1 + 1) = 2 \cdot 1 + 2 \cdot 1 = 2 + 2 = 4. \;\|$$

2.85 Exercise. Prove that in any field F, $3+3=6$ and $3\cdot 2=6$.

2.86 Exercise. Prove that in any field F, $9+8=17$.

2.87 Remark. After doing the previous two exercises, you should believe that the multiplication and addition tables that you learned in elementary school are all theorems that hold in any field, and you should feel free to use them in any field.

2.88 Exercise. Let F be a field and let $x \in F$. Prove that

$$x + x = 2 \cdot x.$$

2.5 Subtraction and Division

2.89 Definition (Subtraction.) In any field F, we define a binary operation $-$ (called subtraction) by

$$\text{for all } x, y \in F \qquad x - y = x + (-y).$$

Unfortunately we are now using the same symbol $-$ for two different things, a binary operation on F, and a symbol denoting additive inverses.

2.90 Exercise (Distributive laws.) Let F be a field, and let $a, b, c \in F$. Prove that

a) $a \cdot (b - c) = (a \cdot b) - (a \cdot c)$.

b) $-(a - b) = b - a$.

2.91 Definition (Division.) Let F be a field. If $a \in F$ and $b \in F\backslash\{0\}$ we define

$$a/b = a \cdot b^{-1}.$$

We also write $\frac{a}{b}$ for a/b. If a, b are both in $F\backslash\{0\}$, then $a \cdot b^{-1} \in F\backslash\{0\}$ so $/$ defines a binary operation on $F\backslash\{0\}$. Also, if $b \neq 0$, then $\frac{1}{b} = 1/b = 1 \cdot b^{-1} = b^{-1}$.

2.92 Example. In the field $(\mathbf{Z}_5, \oplus_5, \odot_5)$, $3^{-1} = 2$ and $4^{-1} = 4$. Hence

$$\frac{1}{3} = 2 \text{ and } \frac{2}{3} = 2 \cdot 2 = 4.$$

Thus,

$$\frac{1}{3} + \frac{2}{3} = 2 + 4 = 1.$$

2.93 Exercise. Let F be a field, and let a, b, c, d be elements of F with $b \neq 0$ and $d \neq 0$. Prove all of the following propositions. In doing any part of this problem, you may assume that all of the earlier parts have been proved.

a) $\dfrac{a \cdot d}{b \cdot d} = \dfrac{a}{b}$.

b) $\dfrac{d \cdot a}{d \cdot b} = \dfrac{a}{b}$.

c) $-\left(\dfrac{a}{b}\right) = \dfrac{-a}{b}$.

d) $\dfrac{a}{b} + \dfrac{c}{b} = \dfrac{a + c}{b}$.

e) $\dfrac{a}{b} + \dfrac{c}{d} = \dfrac{a \cdot d + b \cdot c}{b \cdot d}$.

f) $\dfrac{a}{b} - \dfrac{c}{d} = \dfrac{a \cdot d - b \cdot c}{b \cdot d}$.

g) $\dfrac{a}{b} \cdot \dfrac{c}{d} = \dfrac{a \cdot c}{b \cdot d}$.

h) $\left(\dfrac{b}{d}\right)^{-1} = \dfrac{d}{b}$.

I will now start the practice of using steps in proofs that involve multiple uses of the associative and commutative laws. For example, I'll write statements such as

$$(b - a) + (d - c) = (b + d) - (a + c)$$

with no explanation, because I believe that you recognize that it is correct, and that you can prove it. I'll also write ab for $a \cdot b$ when I believe that no confusion will result, and I'll use distributive laws like

$$(x + y) \cdot z = x \cdot z + y \cdot z$$

and

$$(x - y) \cdot z = x \cdot z - y \cdot z$$

even though we haven't proved them. I will write

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

and assume that you know (because of our conventions about omitting parentheses; cf. Remark 2.50) that the right side of this means

$$(((a \cdot c) + (b \cdot c)) + (a \cdot d)) + (b \cdot d)$$

and you also know (by exercise 2.30) that the parentheses can be rearranged in other sensible orders without changing the value of the expression.

2.94 Exercise. Let F be a field. Show that for all a, b, x in F

a) $(a + b)^2 = a^2 + 2ab + b^2$.

b) $(a - b)^2 = a^2 - 2ab + b^2$.

c) $(a - b) \cdot (a + b) = (a^2 - b^2)$.

d) $(x - a)(x - b) = x^2 - (a + b)x + a \cdot b$.

e) $(2a + b)^2 = 4a^2 + 4ab + b^2$.

2.95 Theorem. *Let F be a field. Then for all $x, y \in F$,*

$$(x^2 = y^2) \iff (x = y \text{ or } x = -y).$$

Proof:

$$\begin{aligned} x^2 = y^2 &\iff x^2 - y^2 = 0 \\ &\iff (x - y)(x + y) = 0 \\ &\iff (x - y = 0) \text{ or } (x + y = 0) \\ &\iff x = y \text{ or } x = -y. \ \| \end{aligned}$$

2.96 Theorem (Quadratic formula.) *Let F be a field such that $2 \neq 0$ in F. Let $A \in F \backslash \{0\}$, and let B, C be elements of F. Then the equation*

$$Ax^2 + Bx + C = 0 \tag{2.97}$$

has a solution x in F if and only if $B^2 - 4AC$ is a square in F (i.e., if and only if there is some element $y \in F$ such that $y^2 = B^2 - 4AC$). If y is any element of F satisfying

$$y^2 = B^2 - 4AC,$$

then the complete set of solutions of (2.97) is

$$\left\{ \frac{-B + y}{2A}, \frac{-B - y}{2A} \right\}.$$

(This corresponds to the familiar quadratic formula

$$x = \frac{-B \pm \sqrt{B^2 - 4AC}}{2A}.)$$

Proof: The proof uses the algebraic identity

$$(px + q)^2 = p^2x^2 + 2pqx + q^2 \text{ for all } p, q, x \in F.$$

Since $A \neq 0$ and $2 \neq 0$, we have $2^2 A \neq 0$ and hence

$$\begin{aligned} Ax^2 + Bx + C = 0 &\iff 2^2 A(Ax^2 + Bx + C) = 0 \\ &\iff (2A)^2 x^2 + 2 \cdot (2A)Bx = -4AC \\ &\iff (2A)^2 x^2 + 2 \cdot (2A)Bx + B^2 = B^2 - 4AC \\ &\iff (2Ax + B)^2 = B^2 - 4AC. \end{aligned}$$

Hence if $B^2 - 4AC$ is not a square, then (2.97) has no solutions. If $B^2 - 4AC = y^2$ for some $y \in F$, then

$$\begin{aligned} Ax^2 + Bx + C = 0 &\iff (2Ax + B)^2 = y^2 \\ &\iff 2Ax + B = y \text{ or } 2Ax + B = -y \\ &\iff x = \frac{-B + y}{2A} \text{ or } x = \frac{-y - B}{2A}. \ \| \end{aligned}$$

2.98 Entertainment. $\mathbf{Z}_7$ is a field. (You can take my word for it or check it for yourself.) Find all solutions to the quadratic equations below in $\mathbf{Z}_7$.

a) $x^2 - x + 2 = 0$.

b) $3x^2 + 5x + 2 = 0$.

c) $2x^2 + x + 5 = 0$.

2.99 Note. The definition of field that we use is roughly equivalent to the definition given by H. Weber in 1893 [48, p526]. Weber does not give the zero-one axiom but he remarks that 0 is different from 1 except in the uninteresting case where the field has only one element. He includes commutativity of addition as an axiom, and he also appears to take $a(-b) = -(ab)$ as an axiom. Individual fields, both finite fields and subfields of the real and complex numbers, had been studied before Weber's paper, but Weber's definition provided an abstraction that included both finite and infinite fields.

There are many other choices we could have made for the field axioms. In [29], Edward Huntington gives eight different sets of axioms that are equivalent to ours. (Two sets of propositions $\mathcal{A}, \mathcal{B}$ are equivalent if every statement in $\mathcal{A}$ can be proved using statements in $\mathcal{B}$, and every statement in $\mathcal{B}$ can be proved from statements in $\mathcal{A}$.)

2.6 Ordered Fields

2.100 Definition (Ordered field axioms.) An *ordered field* is a pair $(F, F^+) = ((F, +, \cdot), F^+)$ where F is a field, and F^+ is a subset of F satisfying the conditions

1. For all $a, b \in F^+$, $\quad a + b \in F^+$.
2. For all $a, b \in F^+$, $\quad a \cdot b \in F^+$.
3. (Trichotomy) For all $a \in F$, exactly one of the statements

$$a \in F^+, \quad -a \in F^+, \quad a = 0$$

is true. The set F^+ is called the set of *positive elements* of F. A field F is *orderable* if it has a subset F^+ such that 1), 2) and 3) are satisfied.

2.101 Example. The rational numbers $(\mathbf{Q}, \mathbf{Q}^+)$ form an ordered field, where $\mathbf{Q}^+$ denotes the familiar set of positive rationals.

2.102 Notation (F^-.) Let (F, F^+) be an ordered field. We let

$$F^- = \{x \in F \colon -x \in F^+\}.$$

We call F^- the set of *negative* elements in F. Thus

$$x \in F^- \iff -x \in F^+,$$

and

$$-x \in F^- \iff -(-x) \in F^+ \iff x \in F^+.$$

We can restate the Trichotomy axiom as: For all $x \in F$, exactly one of the statements

$$x \in F^+, \qquad x = 0, \qquad x \in F^-$$

is true.

2.103 Theorem. *Let (F, F^+) be an ordered field. Then for all $x \in F \backslash \{0\}$, $x^2 \in F^+$.*

Proof: Since $x \neq 0$, we know $x \in F^+$ or $x \in F^-$. Now

$$x \in F^+ \implies x \cdot x \in F^+ \implies x^2 \in F^+,$$

and

$$x \in F^- \implies (-x)(-x) \in F^+ \implies x^2 \in F^+. \; \|$$

2.104 Corollary. *In any ordered field, $1 \in F^+$.*

2.105 Example. The field $\mathbf{Z}_5$ is not orderable.
First Proof: If there were a subset $\mathbf{Z}_5^+$ of $\mathbf{Z}_5$ such that $(\mathbf{Z}_5, \mathbf{Z}_5^+)$ were an ordered field, we would have $4 = 2^2 \in \mathbf{Z}_5^+$. But in $\mathbf{Z}_5$, $4 = -1$ so $-1 \in \mathbf{Z}_5^+$ and $1 \in \mathbf{Z}_5^+$, which contradicts trichotomy. ‖
Second Proof: If $(\mathbf{Z}_5, \mathbf{Z}_5^+)$ were an ordered field, we would have $1 \in \mathbf{Z}_5^+$, so $1+1 = 2 \in \mathbf{Z}_5^+$, so $1+2 = 3 \in \mathbf{Z}_5^+$, so $3+1 = 4 \in \mathbf{Z}_5^+$ so $4+1 = 0 \in \mathbf{Z}_5^+$. This contradicts trichotomy. ‖

2.106 Remark. The method used in the second proof above shows that none of the fields $\mathbf{Z}_n$ are orderable.

2.107 Definition $(<, \leq, >, \geq)$ Let (F, F^+) be an ordered field, and let $a, b \in F$. We define

$$\begin{aligned} a < b &\iff b - a \in F^+. \\ a \leq b &\iff a < b \text{ or } a = b. \\ a > b &\iff a - b \in F^+. \\ a \geq b &\iff a > b \text{ or } a = b. \end{aligned}$$

2.108 Remark. In any ordered field (F, F^+):

$$\begin{aligned} 0 < b &\iff b \in F^+. \\ b < 0 &\iff 0 - b \in F^+ \iff b \in F^-. \end{aligned}$$

2.109 Exercise. Let (F, F^+) be an ordered field, and let $a, b \in F$. Show that exactly one of the statements

$$b < a, \qquad b = a, \qquad b > a$$

is true.

2.110 Theorem (Transitivity of <.) *Let (F, F^+) be an ordered field. Then for all $a, b, c \in F$,*

$$((a < b) \text{ and } (b < c)) \implies (a < c).$$

Proof: For all $a, b, c \in F$ we have

$$\begin{aligned} (a < b) \text{ and } (b < c) &\iff b - a \in F^+ \text{ and } c - b \in F^+ \\ &\implies (c - b) + (b - a) \in F^+ \\ &\implies c - a \in F^+ \\ &\implies a < c. \ \| \end{aligned}$$

2.111 Exercise (Addition of inequalities.) Let (F, F^+) be an ordered field, and let $a, b, c, d \in F$. Show that

$$((a < b) \text{ and } (c < d)) \implies (a + c) < (b + d)$$

and

$$a < b \iff a + c < b + c$$

2.112 Exercise. Let (F, F^+) be an ordered field, and let $a, b \in F$. Show that
$$a < b \iff -b < -a.$$

2.113 Notation. Let (F, F^+) be an ordered field, and let $a, b, c, d \in F$. We use notation like
$$a \leq b < c = d \tag{2.114}$$
to mean $(a \leq b)$ and $(b < c)$ and $(c = d)$, and similarly we write
$$a > b = c \geq d \tag{2.115}$$
to mean $a > b$ and $b = c$ and $c \geq d$. By transitivity of $=$ and of $<$, you can conclude $a < c$ from (2.114), and you can conclude $b \geq d$ and $a > c$ from (2.115). A chain of inequalities involving both $<$ and $>$ shows bad style, so you should not write
$$a < b \geq c.$$

2.116 Exercise (Laws of signs.) Let (F, F^+) be an ordered field, and let $a, b \in F$. Show that

1. $(a \in F^+ \text{ and } b \in F^-) \implies ab \in F^-$
2. $(a \in F^- \text{ and } b \in F^+) \implies ab \in F^-$
3. $(a \in F^- \text{ and } b \in F^-) \implies ab \in F^+$

These laws together with the axiom
$$a \in F^+ \text{ and } b \in F^+ \implies ab \in F^+$$
are called the *laws of signs.*

2.117 Notation. Let F be an ordered field, and let a, b be non-zero elements of F. We say a and b *have the same sign* if either (a, b are both in F^+) or (a, b are both in F^-). Otherwise we say *a and b have opposite signs.*

2.118 Corollary (of the law of signs.) *Let (F, F^+) be an ordered field and let $a, b \in F \backslash \{0\}$. Then*
$$a \cdot b \in F^+ \iff a \text{ and } b \text{ have the same sign },$$
$$a \cdot b \in F^- \iff a \text{ and } b \text{ have opposite signs.}$$

2.119 Notation. I will now start to use the convention that "let F be an ordered field" means "let (F, F^+) be an ordered field"; i.e., the set of positive elements of F is assumed to be called F^+.

2.120 Exercise. Let F be an ordered field and let $a, b, c \in F$. Prove that

$$\begin{aligned} ((a < b) \text{ and } (c < 0)) &\implies ac > bc. \\ ((a < b) \text{ and } (c = 0)) &\implies ac = bc = 0. \\ ((a < b)) \text{ and } (c > 0)) &\implies ac < bc. \end{aligned}$$

2.121 Theorem (Multiplication of inequalities.) *Let F be an ordered field and let a, b, c, d be elements of F. Then*

$$((0 < a < b) \textit{ and } (0 < c < d)) \implies 0 < ac < bd.$$

Proof: By the previous exercise we have

$$\begin{aligned} (0 < a < b) \text{ and } (0 < c < d) &\implies ((ca < da) \text{ and } (ad < bd)) \\ &\implies ((ac < ad) \text{ and } (ad < bd)). \end{aligned}$$

Hence, by transitivity of $<$,

$$(0 < a < b) \text{ and } (0 < c < d) \implies ac < bd. \parallel$$

2.122 Exercise. Let F be an ordered field, and let $a \in F \backslash \{0\}$. Show that a and a^{-1} have the same sign.

2.123 Exercise. Let F be an ordered field, and let $a, b \in F \backslash \{0\}$. Under what conditions (if any) can you say that

$$a < b \implies b^{-1} < a^{-1}?$$

Under what conditions (if any) can you say that

$$a < b \implies a^{-1} < b^{-1}?$$

2.124 Definition (Square root.) Let F be a field, and let $x \in F$. A square root for x is any element y of F such that $y^2 = x$.

2.125 Examples. In $\mathbf{Z}_5$, the square roots of -1 are 2 and 3.
In an ordered field F, no element in F^- has a square root.
In $\mathbf{Q}$, there is no square root of 2. (See theorem 3.45 for a proof.)

2.126 Theorem. *Let F be an ordered field and let $x \in F^+$. If x has a square root, then it has exactly two square roots, one in F^+ and one in F^-, so if x has a square root, it has a unique positive square root.*

Proof: Suppose x has a square root y. Then $y \neq 0$, since $x \in F^+$. If z is any square root of x, then $z^2 = x = y^2$, so, as we saw in theorem 2.95, $z = y$ or $z = -y$. By trichotomy, one of $y, -y$ is in F^+, and the other is in F^-. $\|$

2.127 Theorem. *Let F be an ordered field and let x, y be elements of F with $x \geq 0$ and $y \geq 0$. Then*

$$x < y \iff x^2 < y^2. \tag{2.128}$$

Proof: Let x, y be elements of $F^+ \cup \{0\}$. Then $x + y > 0$, unless $x = y = 0$, so $x^2 < y^2 \implies x + y > 0$. Hence

$$\begin{aligned} x^2 < y^2 &\iff y^2 - x^2 > 0 \\ &\iff (y - x)(y + x) > 0 \\ &\iff y - x \text{ and } y + x \text{ have the same sign.} \\ &\iff y - x > 0 \\ &\iff x < y. \; \| \end{aligned}$$

2.129 Remark. The implication (2.128) is also true when $<$ is replaced by $\leq$ in both positions. I'll leave this to you to check.

2.7 Absolute Value

2.130 Definition (Absolute value.) Let F be an ordered field, and let $x \in F$. Then we define

$$|x| = \begin{cases} x & \text{if } x > 0, \\ 0 & \text{if } x = 0, \\ -x & \text{if } x < 0. \end{cases}$$

2.131 Remark. It follows immediately from the definition that

1. $|x| \geq 0$ for all $x \in F$.
2. $|x| > 0$ for all $x \in F \backslash \{0\}$.
3. $(|x| = 0) \iff (x = 0)$.

2.132 Theorem. *Let F be an ordered field. Then for all $x \in F$,*

$$-|x| \leq x \leq |x|. \tag{2.133}$$

Proof: If $x = 0$ then (2.133) becomes $-0 \leq 0 \leq 0$, which is true. If $x > 0$ then $-|x| < 0 < x = |x|$. If $x < 0$ then $-|x| = -(-x) = x < 0 \leq |x|$. Hence (2.133) holds in all cases. |||

2.134 Exercise. Let F be an ordered field. Prove that $|x| = |-x|$ for all $x \in F$ and $|x|^2 = x^2$ for all $x \in F$.

2.135 Exercise (Product formula for absolute value.) Prove that for all $x, y \in F$,

$$|xy| = |x||y|.$$

2.136 Theorem. *Let F be an ordered field, let $x \in F$, and let $p \in F$ with $p \geq 0$. Then*

$$(|x| \leq p) \iff (-p \leq x \leq p) \tag{2.137}$$

and

$$(|x| > p) \iff ((x < -p) \text{ or } (x > p)). \tag{2.138}$$

Proof: We first show that

$$(|x| \leq p) \implies (-p \leq x \leq p). \tag{2.139}$$

Case 1. If $x > 0$, then

$$|x| \leq p \implies x \leq p \implies -p \leq 0 \leq x \leq p.$$

Case 2. If $x < 0$, then

$$|x| \leq p \implies -x \leq p \implies -p \leq x < 0 \leq p.$$

Case 3. If $x = 0$, then $-p \leq x \leq p$ is true, so (2.139) is true. Hence (2.139) is valid in all cases.

Next we show that

$$(-p \leq x \leq p) \implies (|x| \leq p). \tag{2.140}$$

Case 1. If $x > 0$, then

$$-p \leq x \leq p \implies x \leq p \implies |x| \leq p.$$

Case 2. If $x < 0$, then

$$-p \leq x \leq p \implies -p \leq x \implies -x \leq p \implies |x| \leq p.$$

Case 3. If $x = 0$ then $x \leq p$ is true, so (2.140) is true. Hence (2.140) is true in all cases.

We have proved (2.137).

Since $P \Longleftrightarrow Q$ is true if and only if ((not P)$\Longleftrightarrow$(not Q)) is true,

$$\text{not } (|x| \leq p) \iff \text{not } ((-p \leq x) \text{ and } (x \leq p))\,;$$

i.e.,

$$\begin{aligned} |x| > p &\iff (\text{ not } (-p \leq x)) \text{ or } (\text{ not } (x \leq p)) \\ &\iff -p > x \text{ or } x > p, \\ &\iff x < -p \text{ or } x > p. \end{aligned}$$

This is 2.138. ‖

2.141 Remark. I leave it to you to check that (2.137) holds when $\leq$ is replaced by $<$, and (2.138) holds when $>$ and $<$ are replaced by $\geq$ and $\leq$, respectively.

2.142 Theorem (Triangle inequality.) *Let F be an ordered field. Then*

$$\textit{for all } x, y \in F, \qquad |x + y| \leq |x| + |y|. \tag{2.143}$$

Proof: The obvious way to prove this is by cases. But there are many cases to consider, e.g. ($x < 0$ and $y > 0$ and $x + y < 0$). I will use an ingenious trick to avoid the cases. For all $x, y \in F$, we have

$$-|x| \leq x \leq |x|,$$

and

$$-|y| \le y \le |y|.$$

By adding the inequalities, we get

$$-(|x| + |y|) \le x + y \le (|x| + |y|).$$

By theorem 2.136 it follows that $|x + y| \le |x| + |y|$. |||

2.144 Exercise. Let F be an ordered field. For each statement below, either prove the statement, or explain why it is not true.

a) for all $x, y \in F$, $|x - y| \le |x| + |y|$.

b) for all $x, y \in F$, $|x - y| \le |x| - |y|$.

2.145 Exercise (Quotient formula for absolute value.) Let F be an ordered field. Let $a, b \in F$ with $a \neq 0$. Show that

a) $\left|\dfrac{1}{a}\right| = \dfrac{1}{|a|}$,

b) $\left|\dfrac{b}{a}\right| = \dfrac{|b|}{|a|}$.

2.146 Definition (Distance.) Let F be an ordered field, and let $a, b \in F$. We define the *distance from a to b* to be $|b - a|$.

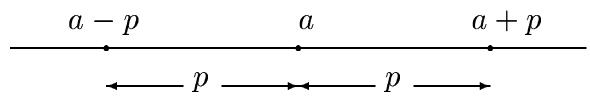
2.147 Remark. If F is the ordered field of real or rational numbers, $|b - a|$ represents the familiar notion of distance between the points a, b on the real line (or the rational line).

2.148 Exercise. Let F be an ordered field. Let $x, a, p \in F$ with $p \ge 0$. Show that

$$(|x - a| \le p) \iff (a - p \le x \le a + p). \tag{2.149}$$

HINT: Use theorem 2.136. Do not reprove theorem 2.136.

2.150 Remark. We can state the result of exercise 2.148 as follows. Let $a \in F$, and let $p \in F^+$. Then the set of points whose distance from x is smaller than p, is the set of points between $a - p$ and $a + p$.



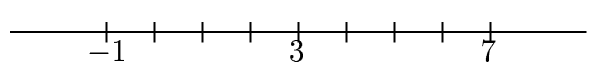
2.151 Definition (Intervals and endpoints.) Let F be an ordered field. Let $a, b \in F$ with $a \le b$. Then we define

$$\begin{aligned}
(a,b) &= \{x \in F\colon a < x < b\}\\
(a,b] &= \{x \in F\colon a < x \le b\}\\
[a,b) &= \{x \in F\colon a \le x < b\}\\
[a,b] &= \{x \in F\colon a \le x \le b\}\\
(-\infty,a] &= \{x \in F\colon x \le a\}\\
(-\infty,a) &= \{x \in F\colon x < a\}\\
(a,\infty) &= \{x \in F\colon x > a\}\\
[a,\infty) &= \{x \in F\colon x \ge a\}\\
(-\infty,\infty) &= F.
\end{aligned}$$

A set that is equal to a set of any of these nine types is called an *interval.* Note that $[a,a) = (a,a] = (a,a) = \emptyset$ and $[a,a] = \{a\}$, so the empty set is an interval and so is a set containing just one point. Sets of the first four types have *endpoints* a and b, except that (a,a) has no endpoints. Sets of the second four types have just one endpoint, namely a. The interval $(-\infty,\infty)$ has no endpoints.

2.152 Examples. Let F be an ordered field. By exercise 2.148 the set of solutions to $|x-3| \le 4$ is

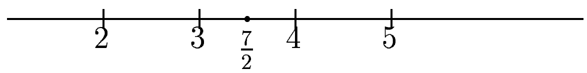
$$\{x \in F\colon 3-4 \le x \le 3+4\} = \{x \in F\colon -1 \le x \le 7\} = [-1,7].$$



I can read this result from the figure by counting 4 units to the left and right of 3. This method is just a way of remembering the result of theorem 2.148.

Now suppose I want to find the solutions in F to

$$|x-2| < |x-5| \tag{2.153}$$



Here, thinking of $|a-b|$ as the distance from a to b, I want to find all elements that are nearer to 2 than to 5. From the picture I expect the answer to be $(-\infty, \frac{7}{2})$. Although this picture method is totally unjustified by anything I've done, it is the method I would use to solve the inequality in practice. If I had to use results we've proved to solve (2.153), I'd say (since $|x-2| \geq 0$)

$$\begin{aligned}
|x-2| < |x-5| &\iff |x-2|^2 < |x-5|^2 \\
&\iff (x-2)^2 < (x-5)^2 \\
&\iff x^2 - 4x + 4 < x^2 - 10x + 25 \\
&\iff 6x < 21 \\
&\iff x < \frac{21}{6} = \frac{7}{2} \\
&\iff x \in (-\infty, \frac{7}{2})
\end{aligned}$$

which agrees with my answer by picture.

2.154 Exercise. Let F be an ordered field, let $x, a, p \in F$ with $p > 0$. Show that

$$|x-a| > p \iff x \in (-\infty, a-p) \cup (a+p, \infty).$$

Interpret the result geometrically on a number line.

2.155 Exercise. Let F be an ordered field. Express each of the following subsets of F as an interval, or a union of intervals. Sketch the sets on a number line.

a) $A = \{x \in F \colon |x-3| < 2\}$

b) $B = \{x \in F \colon |x+2| < 3\}$

c) $C = \{x \in F \colon |x-1| > 1\}$

d) $D = \{x \in F \colon |x+1| \geq 1\}$

2.156 Note. Girolamo Cardano (1501–1576), in an attempt to make sense of the square root of a negative number, proposed an alternate law of signs in which the product of two numbers is negative if at least one factor is negative. He concluded that "plus divided by plus gives plus", and "minus divided by plus gives minus", but "plus divided by minus gives nothing" (i.e. zero), since both of the assertions "plus divided by minus gives plus" and "plus divided by minus gives minus" are contradictory.[40, p 25]

I believe that our axioms for an ordered field are due to Artin and Schreier in 1926 [6, page 259].

Systems satisfying various combinations of algebraic and order axioms were considered by Huntington [28] in 1903.

The notation $|x|$ for absolute value was introduced by Weierstrass in 1841[15, vol.2, page 123]. It was first introduced for complex numbers rather than real numbers.

Chapter 3

Induction and Integers

3.1 Natural Numbers and Induction

3.1 Definition (Inductive set.) Let F be a field. A subset J of F is *inductive* if it satisfies the two conditions:

i) $0 \in J$.

ii) for all $x \in F$, $((x \in J) \implies (x+1) \in J)$.

3.2 Examples. $\mathbf{Z}, \mathbf{N}$ and $\mathbf{Q}$ are inductive sets in $\mathbf{Q}$. Every field is an inductive subset of itself.

If J is an inductive subset of F, then

$$\begin{array}{lll} 1 \in J & \text{since} & 0 \in J \text{ and } 1 = 0+1 \\ 2 \in J & \text{since} & 1 \in J \text{ and } 2 = 1+1 \\ 3 \in J & \text{since} & 2 \in J \text{ and } 3 = 2+1, \end{array}$$

etc. Hence every inductive set contains

$$\{0, 1, 2, 3, 4, 5, \cdots\}.$$

If J is an inductive subset of $\mathbf{Z}_5$, then

$$\mathbf{Z}_5 = \{0, 1, 2, 3, 4\} \subset J \subset \mathbf{Z}_5$$

so the only inductive subset of $\mathbf{Z}_5$ is $\mathbf{Z}_5$ itself. The set

$$\left\{0, \frac{2}{2}, \frac{4}{2}, \frac{5}{2}, \frac{6}{2}, \frac{7}{2}, \frac{8}{2}, \cdots\right\}$$

is an inductive subset in $\mathbf{Q}$.

3.3 Exercise. Which of the following subsets of $\mathbf{Q}$ are inductive?

$$\begin{aligned} A &= \text{The set of even numbers } = \{2n : n \in \mathbf{Z}\} \\ B &= \left\{n + \frac{1}{2} : n \in \mathbf{Z}\right\} \\ C &= \{x \in \mathbf{Z} : x \geq 3\} = \{3, 4, 5, \cdots\} \\ D &= \{x \in \mathbf{Z} : x \geq -3\} = \{-3, -2, -1, \cdots\} \end{aligned}$$

3.4 Exercise.

a) Find an inductive subset J of $\mathbf{Q}$, such that $J \neq \mathbf{Q}$ and $\frac{3}{4} \in J$.

b) Find an inductive subset K of $\mathbf{Q}$, such that $K \neq \mathbf{Z}$ and $\frac{3}{4} \notin K$.

3.5 Definition (Natural numbers in F.) Let F be a field, and let $n \in F$. Then n is a *natural number in* F if n is in every inductive subset of F. The set of all natural numbers in F will be denoted by $\mathbf{N}_F$.

3.6 Example. By the first example in 3.2, for every field F

$$0 \in \mathbf{N}_F, 1 \in \mathbf{N}_F, 2 \in \mathbf{N}_F, 3 \in \mathbf{N}_F, \cdots.$$

If $F = \mathbf{Z}_5$, $\mathbf{N}_F = \mathbf{Z}_5$.

3.7 Remark. By the definition of $\mathbf{N}_F$, $\mathbf{N}_F$ is a subset of every inductive subset of F, i.e.,

$$\text{If } n \in \mathbf{N}_F, \text{ and } J \text{ is inductive, then } n \in J.$$

3.8 Theorem. *Let F be a field. Then the set $\mathbf{N}_F$ of natural numbers in F is an inductive set.*

Proof: Since 0 is in every inductive set, $0 \in \mathbf{N}_F$. Let J be an inductive subset of F. Then for all $n \in F$,

$$\begin{aligned} n \in \mathbf{N}_F &\implies n \in J \text{ (by definition of } \mathbf{N}_F) \\ &\implies n + 1 \in J \text{ (since } J \text{ is inductive)}. \end{aligned}$$

Hence

$$\begin{aligned} n \in \mathbf{N}_F &\implies (n + 1 \in J \text{ for every inductive subset } J \text{ of } F) \\ &\implies n + 1 \in \mathbf{N}_F. \end{aligned}$$

Hence $\mathbf{N}_F$ is inductive. ‖

3.9 Remark. We summarize the previous theorem and remark by saying "$\mathbf{N}_F$ is the smallest inductive subset of F." $\mathbf{N}_F$ is an inductive set, and it's a subset of every other inductive set. You should expect that

$$\mathbf{N_F} = \{0, 1, 2, 3, 4, \cdots\}$$

(whatever "$\cdots$" might mean).

3.10 Theorem (Induction theorem.) *Let F be a field, and let P be a proposition form on $\mathbf{N}_F$. Suppose that*

$$P(0) \text{ is true }. \tag{3.11}$$
$$\text{For all } n \in \mathbf{N}_F, (P(n) \implies P(n+1)) \text{ is true }. \tag{3.12}$$

Then $P(n)$ is true for all $n \in \mathbf{N}_F$.

Proof: Let P be a proposition form on $\mathbf{N}_F$ satisfying (3.11) and (3.12). Let

$$T = \{n \in \mathbf{N}_F \colon P(n) \text{ is true }\}.$$

I want to show that T is inductive. Well, $0 \in T$, by (3.11). Let n be any element in F.

Case 1. $n \in T$:

$$\begin{aligned} n \in T &\implies P(n) \text{ is true} \\ &\implies P(n+1) \text{ is true (by 3.12)} \\ &\implies n+1 \in T. \end{aligned}$$

Case 2. $n \notin T$:

If $n \notin T$, then $n \in T$ is false, so $(n \in T \implies n+1 \in T)$ is true.

Thus for all $n \in F$,

$$n \in T \implies n+1 \in T.$$

This shows that T is inductive. Since every inductive set contains $\mathbf{N}_F$, $\mathbf{N}_F \subset T$; i.e., for all $n \in \mathbf{N}_F$, $P(n)$ is true. ‖

3.13 Theorem. *Let F be a field, and let a, m be natural numbers in F. Then $a + m$ and $a \cdot m$ are in $\mathbf{N}_F$.*

Proof: Let P be the proposition form on $\mathbf{N}_F$ defined by

$$P(n) = \text{“for all } a \in \mathbf{N}_F(a+n \in \mathbf{N}_F)\text{” for all } n \in \mathbf{N}.$$

Then $P(0)$ says “for all $a \in \mathbf{N}_F(a+0 \in \mathbf{N}_F)$” which is true. For all $n \in \mathbf{N}_F$,

$$\begin{aligned} P(n) &\implies \text{for all } a \in \mathbf{N}_F(a+n \in \mathbf{N}_F) \\ &\implies \text{for all } a \in \mathbf{N}_F((a+n)+1 \in \mathbf{N}_F) \text{ (since } \mathbf{N}_F \text{ is inductive)} \\ &\implies \text{for all } a \in \mathbf{N}_F(a+(n+1) \in \mathbf{N}_F) \\ &\implies P(n+1). \end{aligned}$$

By the induction theorem, $P(n)$ is true for all $n \in \mathbf{N}_F$; i.e.,

$$\text{for all } n \in \mathbf{N}_F(\text{ for all } a \in \mathbf{N}_F(a+n \in \mathbf{N}_F)).$$

Now define a proposition form Q on $\mathbf{N}_F$ by

$$Q(n) = \text{“for all } a \in \mathbf{N}_F(a \cdot n \in \mathbf{N}_F)\text{” for all } n \in \mathbf{N}.$$

Then $Q(0)$ says “for all $a \in \mathbf{N}_F(a \cdot 0 \in \mathbf{N}_F)$” which is true. For all $n \in \mathbf{N}_F$,

$$\begin{aligned} Q(n) &\implies \text{for all } a \in \mathbf{N}_F(a \cdot n \in \mathbf{N}_F) \\ &\implies \text{for all } a \in \mathbf{N}_F(a \cdot n + a \in \mathbf{N}_F) \text{ (a sum of things in } \mathbf{N}_F \text{ is in } \mathbf{N}_F) \\ &\implies \text{for all } a \in \mathbf{N}_F(a \cdot (n+1) \in \mathbf{N}_F) \\ &\implies Q(n+1). \end{aligned}$$

By the induction theorem, $Q(n)$ is true for all $n \in \mathbf{N}_F$; i.e.,

$$\text{for all } n \in \mathbf{N}_F(\text{for all } a \in \mathbf{N}_F(a \cdot n \in \mathbf{N}_F)). \;\|$$

3.14 Theorem. *Let F be an ordered field. Then for all $n \in \mathbf{N}_F$, we have*

$$n = 0 \textit{ or } n \geq 1.$$

Proof: Define a proposition form P on $\mathbf{N}_F$ by

$$P(n) = \text{“}n = 0 \text{ or } n \geq 1\text{” for all } n \in \mathbf{N}_F.$$

Clearly $P(0)$ is true. let $n \in \mathbf{N}_F$. To show that $P(n) \implies P(n+1)$, I'll show that $n = 0 \implies P(n+1)$ and that $n \geq 1 \implies P(n+1)$. Well

$$n = 0 \implies n+1 = 1 \implies n+1 \geq 1 \implies P(n+1)$$

and

$$n \geq 1 \implies n+1 \geq 1+1 > 1 \implies n+1 \geq 1 \implies P(n+1).$$

Hence $P(n) \implies P(n+1)$, and by induction $P(n)$ is true for all $n \in \mathbf{N}_F$. $\|$

3.15 Corollary. *Let F be an ordered field. Then there is no element $x \in \mathbf{N}_F$ such that*

$$0 < x < 1.$$

3.16 Lemma. *Let F be an ordered field. Then*

$$\textit{for all } n \in \mathbf{N}_F, (n - 1 \in \mathbf{N}_F \textit{ or } n = 0) \tag{3.17}$$

Proof: Define a proposition form P on $\mathbf{N}_F$ by

$$P(n) = \text{“}(n-1 \in \mathbf{N}_F) \text{ or } (n = 0)\text{” for all } n \in \mathbf{N}_F. \tag{3.18}$$

Then $P(0)$ is true. Let $n \in \mathbf{N}_F$. To show that $P(n) \implies P(n+1)$, I'll show that $(n-1 \in \mathbf{N}_F) \implies P(n+1)$ and that $(n = 0) \implies P(n+1)$. Well,

$$\Big(n-1 \in \mathbf{N}_F\Big) \implies \Big((n-1)+1 \in \mathbf{N}_F\Big) \implies \Big((n+1)-1 \in \mathbf{N}_F\Big) \implies P(n+1),$$

and

$$(n = 0) \implies \Big((n+1) - 1 = 0\Big) \implies \Big((n+1) - 1 \in \mathbf{N}_F\Big) \implies P(n+1).$$

Hence $P(n) \implies P(n+1)$, and by induction, $P(n)$ is true for all $n \in \mathbf{N}_F$. ‖

3.19 Theorem. *Let F be an ordered field and let $p, k \in \mathbf{N}_F$. Then*

$$p - k \in \mathbf{N}_F \textit{ or } p - k < 0.$$

Proof: For each $p \in \mathbf{N}_F$ define a proposition form P_p on $\mathbf{N}_F$ by

$$P_p(n) = \text{“}p - n \in \mathbf{N}_F \text{ or } p - n < 0\text{” for all } n \in \mathbf{N}_F.$$

I'll show that for each $p \in \mathbf{N}_F$, $P_p(n)$ is true for all $n \in \mathbf{N}_F$. Now $P_p(0)$ says “$p \in \mathbf{N}_F$ or $p < 0$” which is true, since $p \in \mathbf{N}_F$. Now let $n \in \mathbf{N}_F$. To show that $P_p(n) \implies P_p(n+1)$, I'll show that

$$p - n \in \mathbf{N}_F \implies P_p(n+1)$$

and that

$$p - n < 0 \implies P_p(n+1).$$

By the previous lemma

$$\begin{aligned} p-n\in \mathbf{N}_F &\implies (p-n)-1\in\mathbf{N}_F \text{ or } p-n=0 \\ &\implies p-(n+1)\in\mathbf{N}_F \text{ or } p-(n+1)=-1 \\ &\implies p-(n+1)\in\mathbf{N}_F \text{ or } p-(n+1)<0 \\ &\implies P_p(n+1). \end{aligned}$$

Also

$$\begin{aligned} p-n<0 &\implies (p-n)-1<-1 \implies p-(n+1)<-1<0 \\ &\implies p-(n+1)<0 \\ &\implies P_p(n+1). \end{aligned}$$

This completes the proof that $P_p(n) \implies P_p(n+1)$, so by induction $P_p(n)$ is true for all $n\in\mathbf{N}_F$. ‖

3.20 Corollary. Let F be an ordered field, and let $p,k\in\mathbf{N}_F$. If $p\geq k$, then $p-k\in\mathbf{N}_F$.

3.21 Theorem. *Let F be an ordered field and let $p\in\mathbf{N}_F$. Then there is no natural number k such that $p<k<p+1$. In other words,*

$$\textit{for all } k,p\in\mathbf{N}_F(k>p \implies k\geq p+1).$$

Proof: Suppose

$$p<k<p+1. \tag{3.22}$$

Then

$$0<k-p<1.$$

Since $k-p>0$, the previous theorem says $k-p\in\mathbf{N}_F$. This contradicts corollary 3.15, so (3.22) is false. ‖

3.23 Theorem (Least Element Principle.) *Let F be an ordered field. Then every non-empty subset S of $\mathbf{N}_F$ contains a least element, i.e. if $S\neq\emptyset$, then there is some element $k\in S$ such that $k\leq n$ for all $n\in S$.*

Proof: I will show that if S is a subset of $\mathbf{N}_F$ having no least element, then $S=\emptyset$.

Let S be a subset of $\mathbf{N}_F$ having no least element. For each $n \in \mathbf{N}_F$ define a proposition $P(n)$ by

$$P(n) = \text{"For all } k \in S, (k > n)\text{"}.$$

Now $0 \notin S$, since if 0 were in S it would be a least element for S. Hence all elements in S are greater than 0, and $P(0)$ is true. Now let n be a generic element of $\mathbf{N}_F$. Then

$$\begin{aligned} P(n) &\implies \text{for all } k \in S, (k > n) \\ &\implies \text{for all } k \in S, (k \geq n+1) \\ &\implies \text{for all } k \in S, (k > n+1) \end{aligned}$$

since if $n+1$ were in S, it would be a least element for S. Thus

$$P(n) \implies P(n+1),$$

and by induction, $P(n)$ is true for all $n \in \mathbf{N}_F$. It follows that $S = \emptyset$, since if S contained an element n, then $P(n)$ would say that $n > n$. |||

3.24 Exercise. Let F be an ordered field. Show that there is a non-empty subset S of F^+ that has no smallest element, i.e. there is a set $S \subset F^+$ such that

for every $a \in S$ there is some $b \in S$ with $b < a$.

3.25 Example. Let F be an ordered field. Let P be the proposition form on $\mathbf{N}_F$ defined by

$$P(n) = \text{"}n^2 > \frac{1}{2}(n^2 + n).\text{"} \tag{3.26}$$

Then for all $n \in \mathbf{N}_F$

$$\begin{aligned} P(n) &\implies n^2 > \frac{1}{2}(n^2+n) \\ &\implies n^2 + (2n+1) > \frac{1}{2}(n^2+n) + (2n+1) \\ &\implies (n+1)^2 > \frac{1}{2}(n^2+n+4n+2) = \frac{1}{2}[(n^2+2n+1)+(n+1)+2n] \\ &\qquad = \frac{1}{2}[(n+1)^2+(n+1)] + n \geq \frac{1}{2}[(n+1)^2+(n+1)] \\ &\implies (n+1)^2 > \frac{1}{2}\left((n+1)^2+(n+1)\right) \\ &\implies P(n+1). \end{aligned}$$

Hence $P(n) \implies P(n+1)$ for all $n \in \mathbf{N}_F$. Now note:

$$\begin{aligned} &P(0) \text{ says } (0 > 0) \text{ so } P(0) \text{ is false!}\\ &P(1) \text{ says } (1 > 1) \text{ so } P(1) \text{ is false!}\\ &P(2) \text{ says } (4 > 3) \text{ so } P(2) \text{ is true.} \end{aligned}$$

Since $P(0)$ is false, I cannot apply the induction theorem. Notice that when I prove $P(n) \implies P(n+1)$ I do *not* assume that $P(n)$ is true. (Although I might as well, since I know $P(n) \implies P(n+1)$ is true if $P(n)$ is false.)

3.27 Theorem (Induction theorem generalization.) *Let F be an ordered field. Let $k \in \mathbf{N}_F$ and let P be a proposition form defined on $\{n \in \mathbf{N}_F : n \geq k\}$. Suppose*

$$P(k) \textit{ is true.} \tag{3.28}$$

$$\textit{For all } n \in \{n \in \mathbf{N}_F : n \geq k\} \qquad P(n) \implies P(n+1). \tag{3.29}$$

Then $P(n)$ is true for all $n \in \{n \in \mathbf{N}_F : n \geq k\}$.

Proof: Let Q be the proposition form on $\mathbf{N}_F$ defined by

$$Q(n) = P(n+k) \text{ for all } n \in \mathbf{N}_F$$

(observe that $n \in \mathbf{N}_F \implies n+k \in \{n \in \mathbf{N}_F : n \geq k\}$ so $Q(n)$ is defined). Then $Q(0) = P(k)$, so $Q(0)$ is true by (3.28). For all $n \in \mathbf{N}_F$,

$$\begin{aligned} Q(n) &\iff P(n+k) \implies P\left((n+k)+1\right)\\ &\iff P\left((n+1)+k\right) \iff Q(n+1) \end{aligned}$$

so

$$Q(n) \implies Q(n+1).$$

By the induction theorem, $Q(n)$ is true for all $n \in \mathbf{N}_F$; i.e., $P(n+k)$ is true for all $n \in \mathbf{N}_F$. To complete the proof, I need to show that

$$\{n+k : n \in \mathbf{N}_F\} = \{n \in \mathbf{N}_F : n \geq k\}.$$

It is clear that

$$\{n+k : n \in \mathbf{N}_F\} \subset \{n \in \mathbf{N}_F : n \geq k\}.$$

To show the opposite inclusion, observe that if $n \in \mathbf{N}_F$ and $n \geq k$, then $n = (n-k)+k$, and by theorem 3.19, $n-k \in \mathbf{N}_F$. ‖

3.30 Example. Let F be an ordered field, and let P be the proposition form on $\mathbf{N}_F$ defined by

$$P(n) = \text{“}n^2 > \frac{1}{2}(n^2+n).\text{”}$$

In example 3.25, we showed that $P(n) \implies P(n+1)$ for all $n \in \mathbf{N}_F$ and that $P(2)$ is true. Hence, by our generalized induction theorem we can conclude that $P(n)$ is true for all $n \in \mathbf{N}_F$ with $n \geq 2$.

3.31 Exercise. Let F be a field and let $x \in \mathbf{N}_F$. We say x is *even* if $x = 2 \cdot y$ for some $y \in \mathbf{N}_F$, and we say x is *odd* if $x = 2 \cdot z + 1$ for some $z \in \mathbf{N}_F$.

a) What are the even numbers in $\mathbf{Z}_5$?

b) What are the odd numbers in $\mathbf{Z}_5$?

3.32 Exercise.

a) Let F be a field. Prove that every element in $\mathbf{N}_F$ is either even or odd. HINT: Let $P(n) =$ “n is even or n is odd”.

b) Let F be an ordered field. Prove that no element of $\mathbf{N}_F$ is both even and odd. Why doesn't this contradict the result of exercise 3.31?

3.33 Note. The question of whether to consider 0 to be a natural number is not settled. Some authors start the natural numbers at 0, other authors start them at 1. It is interesting to note that Aristotle did not consider 1 to be a number.

> ... for “one” signifies a measure of some plurality, and “a number” signifies a measured plurality or a plurality of measures. Therefore, it is also with good reason that unity is not a number; for neither is a measure measures, but a measure is a principle, and so is unity .... [5, page 237, N, 1, 1088a5]

Zero was first recognized to be a number around the ninth century. According to [31, page 185] Mahavira (ninth century) noted that any number multiplied by zero produces zero, and any number divided by zero remains unchanged! Bhaskara (1114–1185) said that a number divided by 0 is called an infinite quantity.

Although arguments that are essentially arguments by induction appear in Euclid, the first clear statement of the induction principle is usually credited to Blaise Pascal (1623-1662) who used induction to prove properties of Pascal's Triangle.[36, page 73]

I believe that the idea of defining the natural numbers to be things that are in every inductive set should be credited to Giuseppe Peano [37, page 94, Axiom 9]. In 1889, Peano gave a set of axioms for natural numbers $\mathbf{N}$ (starting with 1), one of which can be paraphrased as: If K is any set, such that $1 \in K$ and for all $x \in \mathbf{N}$, $(x \in K \implies x+1 \in K)$, then $\mathbf{N} \subset K$.

3.2 Integers and Rationals.

3.34 Definition (Integers in F.) Let F be a field. We define an element z in F to be an *integer in F* if and only if z can be written as the difference of two natural numbers; i.e., if and only if

$$z = q - p \text{ for some } p, q \in \mathbf{N}_F.$$

We denote the set of integers in F by $\mathbf{Z}_F$.

3.35 Exercise. What are the integers in $\mathbf{Z}_5$?

3.36 Exercise. Let F be a field. Show that for all $x, y \in F$,

$$x \in \mathbf{Z}_F \text{ and } y \in \mathbf{Z}_F \implies x + y \in \mathbf{Z}_F$$

and that

$$x \in \mathbf{Z}_F \text{ and } y \in \mathbf{Z}_F \implies x \cdot y \in \mathbf{Z}_F.$$

Also show that $x \in \mathbf{Z}_F \implies -x \in \mathbf{Z}_F$.

3.37 Theorem. *Let F be an ordered field and let $-\mathbf{N}_F = \{-x : x \in \mathbf{N}_F\}$. Then*

$$\mathbf{Z}_F = \mathbf{N}_F \cup (-\mathbf{N}_F) \textit{ and } \mathbf{N}_F \cap (-\mathbf{N}_F) = \{0\}.$$

Proof:

$$n \in \mathbf{N}_F \implies n = n - 0 \in \mathbf{Z}_F$$

and

$$n \in -\mathbf{N}_F \implies -n \in \mathbf{N}_F \implies 0 - (-n) \in \mathbf{Z}_F \implies n \in \mathbf{Z}_F.$$

Hence, $\mathbf{N}_F \subset \mathbf{Z}_F$ and $-\mathbf{N}_F \subset \mathbf{Z}_F$, so

$$\mathbf{N}_F \cup (-\mathbf{N}_F) \subset \mathbf{Z}_F. \tag{3.38}$$

Now suppose $n \in \mathbf{Z}_F$. Then $n = p - q$ where $p, q \in \mathbf{N}_F$. If $p - q \geq 0$, then $p - q \in \mathbf{N}_F$. If $p - q \leq 0$, then $q - p \geq 0$, so $q - p \in \mathbf{N}_F$, so $-(p-q) \in \mathbf{N}_F$, so $-n \in \mathbf{N}_F$, so $n \in -\mathbf{N}_F$. Therefore, $n \in \mathbf{N}_F$ or $n \in -\mathbf{N}_F$; i.e., $n \in \mathbf{N}_F \cup -\mathbf{N}_F$, so

$$\mathbf{Z}_F \subset \mathbf{N}_F \cup (-\mathbf{N}_F).$$

This combined with (3.38) shows that $\mathbf{Z}_F = \mathbf{N}_F \cup (-\mathbf{N}_F)$. Since all elements of $\mathbf{N}_F$ are ≥ 0, and all elements of $-\mathbf{N}_F$ are ≤ 0, it follows that $\mathbf{N}_F \cap (-\mathbf{N}_F) \subset \{0\}$, and clearly $0 \in \mathbf{N}_F \cap -\mathbf{N}_F$, so $\mathbf{N}_F \cap (-\mathbf{N}_F) = \{0\}$. ‖

3.39 Definition (Rational numbers in F.) Let F be a field. Let

$$\mathbf{Q}_F = \left\{ \frac{n}{m} : n, m \in \mathbf{Z}_F \text{ and } m \neq 0 \right\}.$$

The elements of $\mathbf{Q}_F$ will be called *rational numbers* in F. We note $0 = \dfrac{0}{1} \in \mathbf{Q}_F$ and $1 = \dfrac{1}{1} \in \mathbf{Q}_F$.

3.40 Theorem. *Let F be a field. Then the set $\mathbf{Q}_F$ of rational numbers in F form a field (with the operations of F).*

Proof: The various commutative, associative and distributive laws hold in $\mathbf{Q}_F$, because they hold in F, and we've noted that the additive and multiplicative identities of F are in $\mathbf{Q}_F$, and they act as identities in $\mathbf{Q}_F$ because they are identities in F. We note that $+$ and $\cdot$ define binary operations on $\mathbf{Q}_F$; i.e., the sum and product of elements in $\mathbf{Q}_F$ is in $\mathbf{Q}_F$. Let $a, b \in \mathbf{Q}_F$ write $a = \dfrac{p}{q}, b = \dfrac{r}{s}$ where $p, q, r, s \in \mathbf{Z}_F$ and $q \neq 0,\ s \neq 0$. Then

$$\begin{aligned} a + b &= \frac{p}{q} + \frac{r}{s} = \frac{ps + qr}{qs} \\ a \cdot b &= \frac{p}{q} \cdot \frac{r}{s} = \frac{pr}{qs} \end{aligned}$$

and $ps+qr, qs, pr$ are all in $\mathbf{Z}_F$ and $q\cdot s\neq 0$. Hence $a+b$ and $a\cdot b$ are in $\mathbf{Q}_F$. Also, $-a=-\left(\frac{p}{q}\right)=\frac{-p}{q}$ where $-p,q\in\mathbf{Z}_F$, so $-a\in\mathbf{Q}_F$ and

$$\begin{aligned} b\neq 0 &\implies b=\frac{r}{s} \text{ where } r,s\neq 0 \quad r,s\in\mathbf{Z}_F\\ &\implies b^{-1}=\frac{s}{r}\\ &\implies b^{-1}\in\mathbf{Q}_F. \end{aligned}$$

Hence $\mathbf{Q}_F$ is a field. ‖

3.41 Definition (Even and odd.) In exercise 3.31 we defined *even* and *odd* natural numbers. We now extend this definition to integers. Let F be a field and let $x\in\mathbf{Z}_F$. We say x is even if and only if $x=2y$ for some $y\in\mathbf{Z}_F$, and we say x is odd if and only if $x=2z+1$ for some $z\in\mathbf{Z}_F$.

3.42 Remark. In exercise 3.32 you showed that in an ordered field, every element of $\mathbf{N}_F$ is even or odd, and no element of $\mathbf{N}_F$ is both even and odd. Since $\mathbf{Z}_F=\mathbf{N}_F\cup -\mathbf{N}_F$, it follows fairly easily that if F is an ordered field, then every element of $\mathbf{Z}_F$ is even or odd, and no element of $\mathbf{Z}_F$ is both even and odd.

3.43 Exercise.

a) Let F be a field, and let $n\in\mathbf{Z}_F$. Show that

$$n \text{ is even} \implies n^2 \text{ is even},$$

and

$$n \text{ is odd} \implies n^2 \text{ is odd}.$$

b) Let F be an ordered field and let $n\in\mathbf{Z}_F$. Show that

$$\begin{aligned} n^2 \text{ is even} &\implies n \text{ is even}\\ n^2 \text{ is odd} &\implies n \text{ is odd}. \end{aligned}$$

I want to show that in any ordered field F, 2 is not a square in $\mathbf{Q}_F$. To show this I will use the following lemma.

3.44 Lemma. *Let F be an ordered field. Then every element in $\mathbf{Q}_F$ can be written as $\frac{m}{n}$, where $m, n \in \mathbf{Z}_F$ and m, n are not both even.*

Proof: Let F be an ordered field, and let $r \in \mathbf{Q}_F$. Then $r = \frac{m}{n}$ where $m, n \in \mathbf{Z}_F$ and $n \neq 0$. Since $r = \frac{-m}{-n}$, we may assume without loss of generality that $n > 0$. Then $n \in \mathbf{N}_F$ so we can write any element of $\mathbf{Q}_F$ in the form $r = \frac{m}{n}$ where $m \in \mathbf{Z}_F$, $n \in \mathbf{N}_F$ and $n \geq 1$. Let

$$S = \left\{ q \in \mathbf{N}_F : \text{ for some } p \in \mathbf{Z}_F \left(r = \frac{p}{q} \right) \right\}.$$

Then $n \in S$, since $r = \frac{m}{n}$. By the least element principle, S has a least element k. We have

$$r = \frac{p}{k} \text{ for some } p \in \mathbf{Z}_F.$$

Then p and k are not both even, since if $p = 2P$ and $k = 2K$ where P and K are in $\mathbf{Z}_F$, then

$$r = \frac{p}{k} = \frac{2P}{2K} = \frac{P}{K},$$

and hence $K \in S$. But this is impossible because $K = \frac{1}{2}k < k$, i.e. K is less than the least element for S. ‖

3.45 Theorem. *Let F be an ordered field. Then 2 is not a square in $\mathbf{Q}_F$.*

Proof: Suppose there were an element $r \in \mathbf{Q}_F$ such that $r^2 = 2$. By our lemma, we can write $r = \frac{m}{n}$ where $m, n \in \mathbf{Z}_F$, m, n not both even. Now

$$\begin{aligned} r^2 = 2 \implies & \frac{m^2}{n^2} = 2 \\ \implies & m^2 = 2 \cdot n^2 \\ \implies & m \text{ is even (since } n^2 \in \mathbf{Z}_F). \end{aligned}$$

Now

$$m \text{ is even } \implies m = 2k \text{ for some } k \in \mathbf{Z}_F,$$

so

$$\begin{aligned} r^2 = 2 &\implies m^2 = 2 \cdot n^2 \\ &\implies (2k)^2 = 2 \cdot n^2 \\ &\implies 2^2k^2 = 2n^2 \\ &\implies 2k^2 = n^2 \\ &\implies n^2 \text{ is even} \\ &\implies n \text{ is even.} \end{aligned}$$

Thus the statement $r^2 = 2$ implies (m is even and n is even and m, n are not both even), which is false. The theorem follows. ‖

3.46 Note.

When Plato (427?–347B.C.) wrote *The Laws*, he lamented that most Greeks at the time believed that all numbers were rational (i.e. that all lines are commensurable):

> ATHENIAN: My dear Cleinias, even I took a very long time to discover mankind's plight in this business; but when I did, I was amazed, and could scarcely believe that human beings could suffer from such swinish stupidity. I blushed not only for myself, but for Greeks in general.
>
> CLEINIAS: Why so? Go on, sir, tell us what you're getting at.
>
> . . .
>
> ATHENIAN: The real relationship between commensurables and incommensurables. We must be very poor specimens if on inspection we can't tell them apart. These are the problems we ought to keep on putting up to each other, in a competitive spirit, when we've sufficient time to do them justice; and it's a much more civilized pastime for old men then draughts.
>
> CLEINIAS: Perhaps so. Come to think of it, draughts is not radically different from such studies.
>
> ATHENIAN: Well, Cleinias, I maintain that these subjects are what the younger generation should go in for. They do no harm, and are not very difficult: they can be learnt in play, and so far from harming the state, they'll do it some good[39, book vii,820].

However, when Aristotle (384-322 BC) wrote the *Priora Analytica*, he assumed that his reader was familiar with the proof of theorem 3.45 just given. The following quotation would not be understood by anyone who did not know that proof.

> For all who effect an argument *per impossible* infer syllogistically what is false, and prove the initial conclusion hypothetically when something impossible results from the assumption of its contradictory; e.g., that the diagonal of the square is incommensurate with the side, because odd numbers are equal to evens if it is supposed to be commensurate. One infers syllogistically that odd numbers come out equal to evens, and one proves hypothetically the incommensurability of the diagonal since a falsehood results through contradicting this.[4, 1-23, 41a, 23-31]

The meaning of the word "rational" has changed since the time of Euclid. He would have said that a line of length $\sqrt{2}$ was rational, but a rectangle of area $\sqrt{2}$ was irrational. The following quotation is from book X of *The Elements*[19, vol 3, p10, definitions 3 and 4].

> Let then the assigned straight line be called *rational*, and those straight lines which are commensurable with it, whether in length and in square or in square only, *rational*, but those which are incommensurable with it *irrational*.
>
> 4. And let the square on the assigned straight line be called *rational*, and those areas which are commensurable with it *rational*, but those which are incommensurable with it *irrational*.

3.47 Warning. An early commentator on Euclid (quoted in [19, vol III page1]) suggested that perhaps

> $\cdots$ everything irrational and formless is properly concealed, and, if any soul should rashly invade this region of life and lay it open, it would be carried away into the sea of becoming and be overwhelmed by its unresting currents.

3.48 Notation ($\mathbf{N}, \mathbf{Z}, \mathbf{Q}$.) We have defined natural numbers $\mathbf{N}_F$ in any field F, and we've seen that the natural numbers in $\mathbf{Z}_5$ and the natural numbers in $\mathbf{Q}$ are quite different. However, if F is an ordered field, then

$$\mathbf{N}_F = \{0, 1, 2, 3, 4, \cdots\}$$

where the list contains no repetitions, since when we add a new term to the list we get something greater than every element already in the list. Hence if F, G are two ordered fields then $\mathbf{N}_F$ and $\mathbf{N}_G$ are "essentially the same". We will denote the natural numbers in an ordered field by $\mathbf{N}$, and call $\mathbf{N}$ "the natural numbers". Since we defined $\mathbf{Z}_F$ in terms of $\mathbf{N}_F$, and we defined $\mathbf{Q}_F$ in terms of $\mathbf{Z}_F$, the integers in any two ordered fields are "essentially the same" and the rationals in any two ordered fields are "essentially the same". We will denote the integers in any ordered field by $\mathbf{Z}$, and call $\mathbf{Z}$ "the integers".

$$\mathbf{Z} = \mathbf{N} \cup -\mathbf{N} = \{0, 1, -1, 2, -2, 3, -3, \cdots\}.$$

Similarly we will call the rational numbers in an ordered field $\mathbf{Q}$, and call $\mathbf{Q}$ "the rational numbers"

$$\mathbf{Q} = \left\{ \frac{n}{m} : n, m \in \mathbf{Z}, \ , m \neq 0 \right\}.$$

3.49 Remark. One can define formally what it means to say $\mathbf{N}_F$ and $\mathbf{N}_G$ are "essentially the same," and one can prove that if F, G are ordered fields, then $\mathbf{N}_F$ and $\mathbf{N}_G$ are "essentially the same" (e.g., see [35, page 35]).

However, one can also construct ordered fields F and G such that $\mathbf{N}_F$ and $\mathbf{N}_G$ are radically different! (see [41]) The reason that both of these apparently contradictory things can happen is that our definition of $\mathbf{N}_F$ involves looking at the set of all inductive subsets of F, and our vague notions of set and function are just too imprecise to deal with this delicate question. The two quoted contradictory results are proved using different set theories, which are not consistent with each other, but both of which are more or less consistent with everything we've used about sets.

3.3 Recursive Definitions.

Our definition of function $f: A \to B$ involved the undefined word "rule". If I define $f: \mathbf{N} \to \mathbf{N}$ by

$$f(n) = 2 \cdot n + 1 \text{ for all } n \in \mathbf{N}$$

the rule is perfectly clear. I will often want to define functions by "rules" of the following sort: $f: \mathbf{N} \to \mathbf{N}$ is given by

$$\begin{cases} f(0) = 1 \\ f(n+1) = (n+1) \cdot f(n) \quad \text{for all } n \in \mathbf{N}. \end{cases} \tag{3.50}$$

It is not quite so clear that this is a rule, since the right side of (3.50) involves the function I am trying to define. However, if I try to use this rule to calculate $f(4)$, I get

$$\begin{aligned} f(4) &= 4 \cdot f(3) \\ &= 4 \cdot 3 \cdot f(2) \\ &= 4 \cdot 3 \cdot 2 \cdot f(1) \\ &= 4 \cdot 3 \cdot 2 \cdot 1 \cdot f(0) \\ &= 4 \cdot 3 \cdot 2 \cdot 1 \cdot 1 \end{aligned} \tag{3.51}$$

and by this example, you recognize that (3.50) defines the familiar factorial function. In fact, I make this my definition of the factorial function.

3.52 Definition (Factorial function.) We define $f: \mathbf{N} \to \mathbf{N}$ by the rules.

$$\begin{cases} f(0) = 1 \\ f(n+1) = (n+1) \cdot f(n) \quad \text{for all } n \in \mathbf{N}. \end{cases}$$

We call f the *factorial function*, and denote $f(n)$ by $n!$. By definition,

$$\begin{cases} 0! = 1 \\ (n+1)! = (n+1) \cdot n!. \end{cases}$$

I could use the same rule (3.50) to define a factorial function $\mathbf{Z}_5 \to \mathbf{Z}_5$. The calculation (3.51) shows that then

$$f(4) = 4 \cdot 3 \cdot 2 \cdot 1 \cdot 1 = 24 = 4,$$

and

$$f(5) = 5 \cdot f(4) = 5 \cdot 4 = 0.$$

but in $\mathbf{Z}_5$, $5 = 0$ so I have $f(0) = 0$, contradicting $f(0) = 1$. So I see that (3.50) is *not* a "rule". How do I know that (3.50) is a "rule" when considered as a function from $\mathbf{N} \to \mathbf{N}$?; i.e., how do I know that no contradiction arises when I use (3.50) to calculate values for $n \in \mathbf{N}$? I have decided not to worry about this question, and to treat definitions analogous to (3.50) where functions on $\mathbf{N}$ are defined by giving $f(0)$ explicitly, and expressing $f(n+1)$ in terms of n and $f(k)$ for values of $k \leq n$, as valid "rules". Such defintions are called definitions *by recursion*. A discussion of, and justification for definitions by recursion can be found in [27].

3.53 Definition (Powers.) Let F be a field, and let $a \in F$. Define a function

$$f_a : \mathbf{N} \to F$$

by

$$\begin{aligned} f_a(0) &= 1. \\ f_a(n+1) &= f_a(n) \cdot a \text{ for all } n \in \mathbf{N}. \end{aligned} \tag{3.54}$$

Thus,

$$\begin{aligned} f_a(4) &= f_a(3) \cdot a \\ &= f_a(2) \cdot a \cdot a \\ &= f_a(1) \cdot a \cdot a \cdot a \\ &= f_a(0) \cdot a \cdot a \cdot a \cdot a \\ &= 1 \cdot a \cdot a \cdot a \cdot a \\ &= a \cdot a \cdot a \cdot a. \end{aligned}$$

We denote the value of $f_a(n)$ by a^n. Then we can rewrite (3.54) as

$$\begin{cases} a^0 = 1 \\ a^{n+1} = a^n \cdot a \quad \text{for all } n \in \mathbf{N}. \end{cases}$$

Note that $0^0 = 1$ and $a^1 = a$.

3.55 Theorem. *Let F be a field and let $a \in F$. Then for all $p, n \in \mathbf{N}$,*

$$a^{p+n} = a^p \cdot a^n.$$

Proof: Define a proposition form P on $\mathbf{N}$ by

$$P(n) = \text{“for all } p \in \mathbf{N}(a^{p+n} = a^p \cdot a^n)\text{” for all } n \in \mathbf{N}.$$

Then $P(0)$ says "for all $p \in \mathbf{N}(a^{p+0} = a^p \cdot a^0)$" which is true, since both sides of the equation are equal to a^p. For all $n \in \mathbf{N}$,

$$a^{p+n} \cdot a = a^{(p+n)+1} = a^{p+(n+1)},$$

and

$$(a^p a^n) \cdot a = a^p(a^n a) = a^p a^{(n+1)}.$$

Hence for all $n \in \mathbf{N}$,

$$\begin{aligned} P(n) &\implies \text{for all } p \in \mathbf{N}(a^{p+n} = a^p a^n) \\ &\implies \text{for all } p \in \mathbf{N}((a^{p+n}) \cdot a = (a^p a^n) \cdot a) \\ &\implies \text{for all } p \in \mathbf{N}(a^{p+(n+1)} = a^p a^{n+1}) \\ &\implies P(n+1). \end{aligned}$$

By induction, $P(n)$ is true for all $n \in \mathbf{N}$, i.e.

$$\text{for all } n \in \mathbf{N}\Big(\text{for all } p \in \mathbf{N}(a^{p+n} = a^p a^n)\Big). \ \|$$

3.56 Exercise. Let F be a field, and let a, b be elements of F. Show that

$$(ab)^n = a^n b^n \text{ for all } n \in \mathbf{N}.$$

3.57 Exercise. Let F be a field and let $a \in F$. Show that

$$(a^n)^m = a^{(nm)} \text{ for all } m, n \in \mathbf{N}.$$

The following results are easy to show and we will assume them.

$$\begin{aligned} &0^{n+1} = 0 \text{ for all } n \in \mathbf{N}, (\text{ but } 0^0 = 1). \\ &1^n = 1 \text{ for all } n \in \mathbf{N}. \\ &a \neq 0 \implies (a^n \neq 0 \text{ for all } n \in \mathbf{N}). \end{aligned}$$

3.58 Remark. Let F be a field, let $a \in F\backslash\{0\}$ and let $n \in \mathbf{Z}$. We know that $n = p - q$ where $p, q \in \mathbf{N}$. Suppose we also have $n = P - Q$ where $P, Q \in \mathbf{N}$.

$$\begin{aligned} n = n &\implies p - q = P - Q \implies p + Q = q + P \\ &\implies a^{p+Q} = a^{q+P} \implies a^p a^Q = a^q a^P \\ &\implies \frac{a^p}{a^q} = \frac{a^P}{a^Q}. \end{aligned}$$

I need this remark for the following definition to make sense.

3.59 Definition (Integer powers.) Let F be a field. If $a \in F\backslash\{0\}$ and $n \in \mathbf{Z}$, we define

$$a^n = \frac{a^p}{a^q} \text{ where } n = p - q, \quad p, q \in \mathbf{N}.$$

Note that this definition of a^{-1} is consistent with our use of a^{-1} for multiplicative inverse. Also, this definition implies that

$$1^n = 1 \text{ for all } n \in \mathbf{Z}.$$

3.60 Theorem. *Let F be a field and let $a \in F\backslash\{0\}$. Then*

$$\textit{for all } m, n \in \mathbf{Z} \ \ (a^{m+n} = a^m \cdot a^n).$$

Proof: Let $m, n \in \mathbf{Z}$, and write

$$m = p - q, \quad n = r - s \text{ where } p, q, r, s \in \mathbf{N}$$

then $p + r \in \mathbf{N}$ and $q + s \in \mathbf{N}$ and

$$\begin{aligned} a^{m+n} &= a^{(p-q)+(r-s)} = a^{(p+r)-(q+s)} \\ &= \frac{a^{p+r}}{a^{q+s}} = \frac{a^p a^r}{a^q a^s} \\ &= \frac{a^p}{a^q} \cdot \frac{a^r}{a^s} = a^m \cdot a^n. \ \| \end{aligned}$$

3.61 Remark. If F is a field, and $a \in F \setminus \{0\}$, then by definition 3.59 we know that

$$a^{p-q} = \frac{a^p}{a^q} \text{ for all } p, q \in \mathbf{N}.$$

It follows from theorem 3.60 that $a^q a^{p-q} = a^p$ for all $p, q \in \mathbf{Z}$, and hence

$$a^{p-q} = \frac{a^p}{a^q} \text{ for all } p, q \in \mathbf{Z}.$$

3.62 Exercise. Let F be a field, and let $a, b \in F\backslash\{0\}$. Show that

$$(ab)^n = a^n b^n \text{ for all } n \in \mathbf{Z}.$$

3.63 Corollary (to Exercise 3.62) *Let F be a field, and let $a, b \in F \setminus \{0\}$. Then*

$$\left(\frac{a}{b}\right)^n = \frac{a^n}{b^n} \textit{ for all } n \in \mathbf{Z}.$$

Proof: By exercise 3.62

$$\left(\frac{a}{b}\right)^n b^n = \left(\frac{a}{b}\cdot b\right)^n = a^n \text{ for all } n \in \mathbf{Z}.$$

If we multiply both sides of this equation by $(b^n)^{-1}$, we get

$$\left(\frac{a}{b}\right)^n b^n(b^n)^{-1} = a^n(b^n)^{-1},$$

i.e.

$$\left(\frac{a}{b}\right)^n = \frac{a^n}{b^n}.$$

3.64 Exercise. Let F be a field, and let $a \in F\backslash\{0\}$. Show that

$$(a^m)^n = a^{(mn)} \text{ for all } m, n \in \mathbf{Z}.$$

3.4 Summation.

3.65 Notation ($\mathbf{Z}_{\geq k}$.) Let $k \in \mathbf{Z}$. We define

$$\mathbf{Z}_{\geq k} = \{n \in \mathbf{Z}: n \geq k\}.$$

In particular $\mathbf{Z}_{\geq 0} = \mathbf{N}$.

3.66 Definition ($\sum_{j=k}^{p} f(j)$) Let $k \in \mathbf{Z}$ and let $f: \mathbf{Z}_{\geq k} \to F$ be a function from $\mathbf{Z}_{\geq k}$ to a field F. Define a function $S: \mathbf{Z}_{\geq k} \to F$ by the rules

$$\begin{aligned} S(k) &= f(k) \\ S(n+1) &= S(n) + f(n+1) \text{ for all } n \in \mathbf{Z}_{\geq k}. \end{aligned}$$

Hence, for $k = 2$,

$$\begin{aligned} S(5) &= S(4) + f(5) \\ &= S(3) + f(4) + f(5) \\ &= S(2) + f(3) + f(4) + f(5) \\ &= f(2) + f(3) + f(4) + f(5). \end{aligned}$$

We denote $S(p)$ by $\sum_{j=k}^{p} f(j)$ for all $p \in \mathbf{Z}_{\geq k}$. Thus,

$$\sum_{j=k}^{k} f(j) = f(k) \tag{3.67}$$

and

$$\sum_{j=k}^{n+1} f(j) = \left(\sum_{j=k}^{n} f(j)\right) + f(n+1).$$

The letter j in (3.67) has no meaning, and can be replaced by any symbol that has no meaning in the present context. Thus $\sum_{j=3}^{5} f(j) = \sum_{w=3}^{5} f(w)$.

3.68 Example.

$$\begin{aligned}\sum_{j=0}^{4} j^2 &= 0^2 + 1^2 + 2^2 + 3^2 + 4^2 = 30\\ \sum_{j=-3}^{3} j &= (-3) + (-2) + (-1) + 0 + 1 + 2 + 3 = 0.\end{aligned}$$

3.69 Remark. I will sometimes write things like

$$\sum_{j=1}^{2} \frac{1}{3-j} = \frac{1}{3-1} + \frac{1}{3-2} = \frac{1}{2} + 1 = \frac{3}{2}$$

even though my definition of summation is not strictly applicable here (since $\frac{1}{3-j}$ is not defined for all $j \in \mathbf{Z}_{\geq 1}$).

There are many formulas associated with summation notation that are easily proved by induction; e.g., let f, g be functions from $\mathbf{Z}_{\geq k}$ to an ordered field F, and let $c \in F$. Then

$$\sum_{j=k}^{p} f(j) + \sum_{j=k}^{p} g(j) = \sum_{j=k}^{p} [f(j) + g(j)] \text{ for all } p \in \mathbf{Z}_{\geq k}.$$

$$c \sum_{j=k}^{p} f(j) = \sum_{j=k}^{p} (c \cdot f(j)) \text{ for all } p \in \mathbf{Z}_{\geq k}.$$

If $f(j) \geq g(j)$ for all $j \in \mathbf{Z}_{\geq k}$, then $\sum_{j=k}^{p} f(j) \geq \sum_{j=k}^{p} g(j)$ for all $p \in \mathbf{Z}_{\geq k}$.

$\sum_{j=k}^{p} f(j) = \sum_{j=k}^{q} f(j) + \sum_{j=q+1}^{p} f(j)$ for all $q \in \mathbf{Z}_{\geq k}, p \in \mathbf{Z}_{\geq q+1}$.

We will assume these results.

3.70 Remark. Usually induction arguments are presented less formally than I have been presenting them. In the proof of the next theorem I will give a more typical looking induction argument. (I personally find the more formal version – where a proposition is actually named – easier to understand.)

3.71 Theorem (Finite geometric series.) *Let F be a field, and let $r \in F \backslash \{1\}$. Then for all $n \in \mathbf{N}$,*

$$\sum_{j=0}^{n} r^j = \frac{1 - r^{n+1}}{1 - r}. \tag{3.72}$$

Proof: (By induction.) When $n = 0$, (3.72) says $\sum_{j=0}^{0} r^j = \frac{1-r}{1-r}$ which is true since both sides are equal to 1. Now suppose that (3.72) is true for some $n \in \mathbf{N}$. Then

$$\begin{aligned} \sum_{j=0}^{n+1} r^j &= \sum_{j=0}^{n} r^j + r^{n+1} = \frac{1 - r^{n+1}}{1 - r} + r^{n+1} \\ &= \frac{1 - r^{n+1} + r^{n+1}(1 - r)}{1 - r} = \frac{1 - r^{(n+1)+1}}{1 - r} \end{aligned}$$

so

$$\sum_{j=0}^{n+1} r^j = \frac{1 - r^{(n+1)+1}}{1 - r}.$$

Hence, if (3.72) holds for some $n \in \mathbf{N}$, it also holds when n is replaced by $n + 1$. By induction (3.72) holds for all $n \in \mathbf{N}$. ‖

3.73 Remark. I will sometimes denote $\sum_{j=1}^{n} f(j)$ by $f(1) + f(2) + \cdots + f(n)$. I am not going to give a formal definition for $\cdots$, and when you see $\cdots$ written in these notes it is usually an indication that a straightforward induction argument or a recursive definition is being omitted.

3.74 Remark. The previous proof was easy, but in order to use the induction proof, I needed to know the formula. Here I will indicate how one might discover such a formula. For each $n \in \mathbf{N}$, let $S_n = 1 + r + \cdots + r^n$. Then

$$(1 + r + \cdots + r^{n+1}) = (1 + r + \cdots + r^n) + r^{n+1} = S_n + r^{n+1} \tag{3.75}$$

and

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

Hence

$$S_n + r^{n+1} = 1 + rS_n, \tag{3.76}$$

and it follows that

$$S_n(1 - r) = 1 - r^{n+1}$$

i.e.

$$S_n = \frac{1 - r^{n+1}}{1 - r}.$$

Here I have derived the formula (3.72). If you write out the argument from line (3.75) to line (3.76), without using $\cdots$s, and using only properties of sums that we have explicitly proved or assumed, you will probably be surprised at how many implicit assumptions were made above. However all of the assumptions can be justified in a straightforward way.

3.77 Theorem (Factorization of $a^{n+1} - r^{n+1}$.) *Let F be a field, and let a, r be elements of F. Then for all $n \in \mathbf{N}$,*

$$\begin{aligned}(a^{n+1} - r^{n+1}) &= (a - r)(\sum_{j=0}^{n} a^{n-j} r^j) &(3.78)\\ &= (a - r)(a^n + a^{n-1}r^1 + a^{n-2}r^2 + \cdots + a^1 r^{n-1} + r^n).\end{aligned}$$

Proof: Let $n \in \mathbf{N}$. The formula (3.72) for a finite geometric series shows that

$$(1 - r^{n+1}) = (1 - r) \sum_{j=0}^{n} r^j \text{ for all } r \in F \setminus \{1\}. \tag{3.79}$$

This formula also holds when $r = 1$, since then both sides of the equation are equal to zero, so

$$(1 - r^{n+1}) = (1 - r) \sum_{j=0}^{n} r^j \text{ for all } r \in F. \tag{3.80}$$

This proves our formula in the case $a = 1$. When $a = 0$, equation (3.78) says

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

which is true, so we will suppose that $a \neq 0$. Then by (3.80) we have

$$\begin{aligned} a^{n+1} - r^{n+1} &= a^{n+1}\left(1 - \left(\frac{r}{a}\right)^{n+1}\right) \\ &= a^{n+1}\left(1 - \frac{r}{a}\right)\sum_{j=0}^{n}\left(\frac{r}{a}\right)^j = a\left(1 - \frac{r}{a}\right)\left(a^n \sum_{j=0}^{n} \frac{r^j}{a^j}\right) \\ &= (a-r)\sum_{j=0}^{n} \frac{a^n}{a^j} r^j = (a-r)\sum_{j=0}^{n} a^{n-j} r^j \ \| \end{aligned}$$

3.81 Remark. The solution to the problem of "factoring" an expression depends on the field over which we are working. For example, if we work over $\mathbf{Z}_7$, then

$$x^2 + 5 = (x+3)(x+4),$$

whereas if F is an ordered field, then $x^2 + 5$ does not factor in the form $(x+a)(x+b)$, where a and b are in F. (If $x^2+5 = (x+a)(x+b)$ for all $x \in F$, then by taking $x = -a$ we would get $a^2+5 = 0$, which is false since $a^2+5 > 0$ in any ordered field.)

3.82 Exercise. Factor five of the following expressions into at least two factors. Assume that all numbers appearing in your factorization are rational.

a) $a^3 - b^3$.

b) $r^p - 1$. (Here $p \in \mathbf{Z}_{\geq 2}$.)

c) $a^3 + b^3$.

d) $a^4 + b^4$.

e) $x^6 - b^6$.

f) $x^6 + a^6$.

3.83 Entertainment. Let F be a field and let $r \in F\backslash\{1\}$. For all $n \in \mathbf{Z}_{\geq 1}$, let

$$T_n = r + 2r^2 + 3r^3 + \cdots + n \cdot r^n = \sum_{j=1}^{n} jr^j.$$

By looking at $T_{n+1} - r \cdot T_n$ and using the known formula (3.72), derive the formula

$$T_n = \frac{r}{(1-r)^2}\Big(1 + nr^{n+1} - (n+1)r^n\Big).$$

3.84 Exercise. Let

$$S_n = \sum_{j=1}^{n} \frac{1}{j(j+1)} \text{ for all } n \in \mathbf{Z}_{\geq 1}. \tag{3.85}$$

Calculate the values for S_1, S_2, S_3, S_4. Write your answers as fractions in the simplest form you can. Then guess a formula for S_n, and prove that it is valid for all $n \in \mathbf{Z}_{\geq 1}$.

3.86 Exercise. Let

$$T_n = \sum_{j=1}^{n}(2j-1) \text{ for all } n \in \mathbf{Z}_{\geq 1}. \tag{3.87}$$

Calculate the values for T_1, T_2, T_3, and T_4. Then guess a formula for T_n, and prove that your guess is correct.

3.5 Maximum Function

3.88 Definition (max(p, q).) Let F be an ordered field, and let $p, q \in F$. We define

$$\max(p,q) = \begin{cases} p & \text{if } p \geq q \\ q & \text{if } p < q. \end{cases}$$

Then

$$\begin{aligned} p &\leq \max(p,q) \\ q &\leq \max(p,q). \end{aligned}$$

3.89 Definition ($\max_{j\le n\le l} f(n)$.) Let F be an ordered field, let $j \in \mathbf{Z}$ and let $f\colon \mathbf{Z}_{\ge j} \to F$ be a function. Define $M\colon \mathbf{Z}_{\ge j} \to F$ by the rules

$$\begin{aligned} M(j) &= f(j) \\ M(n+1) &= \max\left(f(n+1), M(n)\right) \text{ for all } n \in \mathbf{Z}_{\ge j}. \end{aligned}$$

Hence, e.g., if $f(n) = (n-1)^2$,

$$\begin{aligned} M(0) &= f(0) = 1 \\ M(1) &= \max\left(f(1), M(0)\right) = \max(0,1) = 1 \\ M(2) &= \max\left(f(2), M(1)\right) = \max(1,1) = 1 \\ M(3) &= \max\left(f(3), M(2)\right) = \max(4,1) = 4. \end{aligned}$$

We write

$$M(l) = \max_{j\le m\le l} f(m)$$

where m is a dummy index, and we think of $M(l)$ as the largest of the numbers $\{f(j), f(j+1), \cdots, f(l)\}$. By definition

$$\max_{j\le m\le j} f(m) = f(j)$$

and

$$\max_{j\le m\le l+1} = \max\left(f(j+1), \max_{j\le m\le l} f(m)\right).$$

3.90 Notation ($\mathbf{Z}_{j\le n\le l}$.) Let $j, l \in \mathbf{Z}$ with $j \le l$. Then

$$\mathbf{Z}_{j\le n\le l} = \{n \in \mathbf{Z}\colon j \le n \le l\}.$$

3.91 Theorem. *Let F be an ordered field, let $j \in \mathbf{Z}$ and let $f\colon \mathbf{Z}_{\ge j} \to F$ be a function. Then for all $l \in \mathbf{Z}_{\ge j}$,*

$$\textit{for all } p \in \mathbf{Z}_{j\le m\le l},\ f(p) \le \max_{j\le m\le l} f(m). \tag{3.92}$$

Proof: Let P be the proposition form on $\mathbf{Z}_{\ge j}$ such that $P(l)$ is the proposition (3.92). Then $P(j)$ says

$$\text{for all } p \in \mathbf{Z}_{j\le m\le j},\ f(p) \le \max_{j\le m\le j} f(m);$$

i.e.,

$$\text{for all } p \in \{j\},\ f(p) \leq f(j).$$

Hence $P(j)$ is true.

Now for all $l \in \mathbf{Z}_{\geq j}$,

$$\begin{aligned} P(l) &\implies \text{for all } p \in \mathbf{Z}_{j\leq m \leq l},\ f(p) \leq \max_{j\leq m\leq l} f(m) \\ &\implies \text{for all } p \in \mathbf{Z}_{j\leq m \leq l},\ f(p) \leq \max\Big(f(l+1), \max_{j\leq m\leq l} f(m)\Big) \\ &\qquad\qquad\qquad\qquad\qquad\quad = \max_{j\leq m\leq l+1} f(m). \end{aligned}$$

We also have

$$f(l+1) \leq \max\Big(f(l+1), \max_{j\leq m\leq l} f(m)\Big) = \max_{j\leq m\leq l+1} f(m),$$

so

$$\begin{aligned} P(l) &\implies \text{for all } p \in \mathbf{Z}_{j\leq m \leq l} \cup \{l+1\},\ f(p) \leq \max_{j\leq m\leq l+1} f(m) \\ &\implies \text{for all } j \in \mathbf{Z}_{j\leq m \leq l+1},\ f(p) \leq \max_{j\leq m\leq l+1} \\ &\implies P(l+1). \end{aligned}$$

By induction, $P(l)$ is true for all $l \in \mathbf{Z}_{\geq j}$. |||

3.93 Note. The notation a^n for positive integer powers of a was introduced by Descartes in 1637[15, vol 1,p 346]. Both Maple and Mathematica denote a^n by `a^n`.

The notation $n!$ for the factorial of n was introduced by Christian Kramp in 1808[15, vol 2, p 66].

The use of the Greek letter Σ to denote sums was introduced by Euler in 1755[15, vol 2,p 61]. Euler writes

$$\Sigma x^2 = \frac{x^3}{3} - \frac{x^2}{2} + \frac{x}{6}.$$

The use of limits on sums was introduced by Augustin Cauchy(1789-1857). Cauchy used the notation $\sum_m^n {}_r fr$ to denote what we would write as $\sum_{r=m}^{n} f(r)$[15, vol 2, p 61].

In Maple, the value of $\sum_{i=1}^{n} f(i)$ is denoted by `sum(f(i),i=1..n)` . In Mathematica it is denoted by `Sum[f[i],{i,1,n}]` .

Chapter 4

The Complexification of a Field.

Throughout this chapter, F will represent a field in which -1 is not a square. For example, in an ordered field -1 is not a square, but in $\mathbf{Z}_5$, $(2)^2 = 4 = -1$ so -1 is a square. In $\mathbf{Z}_3$,

$$0^2 = 0, \quad 1^2 = 1, \quad 2^2 = 1, \quad \text{and} \quad -1 = 2,$$

so -1 is not a square in $\mathbf{Z}_3$.

Let F be a field in which -1 is not a square. I am going to construct a new field $\mathbf{C}_F$ which contains (a copy of) F and a new element i such that $i^2 = -1$. The elements of $\mathbf{C}_F$ will all have the form

$$a + bi$$

where a and b are in F. I'll call $\mathbf{C}_F$ the *complexification* of F. Before I start my construction, note that if a, b, c, d are in F and $i^2 = -1$, then by the usual field axioms

$$(a + bi) + (c + di) = (a + c) + (b + d)i, \tag{4.1}$$

and

$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i. \tag{4.2}$$

4.1 Construction of $\mathbf{C}_F$.

Let F be a field in which -1 is not a square. Let $\mathbf{C}_F = F \times F$ denote the Cartesian product of F with itself (Cf. definition 1.55). I define two binary operations $\oplus$ and $\odot$ on $\mathbf{C}_F$ as follows (cf. (4.1) and (4.2)): for all $(a,b),(c,d) \in \mathbf{C}_F$,

$$(a,b) \oplus (c,d) = (a+c, b+d)$$

and

$$(a,b) \odot (c,d) = (ac-bd, ad+bc).$$

We will now show that $(\mathbf{C}_F, \oplus, \odot)$ is a field.

4.3 Theorem (Associativity of $\odot$.) *The operation $\odot$ is associative on $\mathbf{C}_F$.*

Proof: Let $(a,b),(c,d)$ and (e,f) be elements in $\mathbf{C}_F$. Then

$$\begin{aligned} &(a,b) \odot ((c,d) \odot (e,f)) \\ &\quad = (a,b) \cdot (ce-df, cf+de) \\ &\quad = (a(ce-df) - b(cf+de), a(cf+de) + b(ce-df)) \\ &\quad = (ace-adf-bcf-bde, acf+ade+bce-bdf). \qquad (4.4) \end{aligned}$$

Also,

$$\begin{aligned} &((a,b) \odot (c,d)) \odot (e,f) \\ &\quad = (ac-bd, ad+bc) \odot (e,f) \\ &\quad = ((ac-bd)e - (ad+bc)f, (ac-bd)f + (ad+bc)e) \\ &\quad = (ace-bde-adf-bcf, acf-bdf+ade+bce). \qquad (4.5) \end{aligned}$$

Now by using the field properties of F, we see that the (4.4) and (4.5) are equal, and hence

$$(a,b) \odot ((c,d) \odot (e,f)) = ((a,b) \odot (c,d)) \odot (e,f).$$

Hence, $\odot$ is associative on $\mathbf{C}_F$. |||

I expect the multiplicative identity for $\mathbf{C}_F$ to be $1+0i = (1,0)$.

4.6 Theorem (Multiplicative identity for $\mathbf{C}_F$.) *The element $(1,0)$ is an identity for $\odot$ on $\mathbf{C}_F$.*

Proof: For all $(a,b) \in \mathbf{C}_F$, we have

$$(1,0) \odot (a,b) = (1 \cdot a - 0 \cdot b, 1 \cdot b + 0 \cdot a) = (a,b)$$

and

$$(a,b) \odot (1,0) = (a \cdot 1 - b \cdot 0, a \cdot 0 + b \cdot 1) = (a,b). \ |||$$

4.7 Exercise.

a) Show that $\oplus$ is associative on $\mathbf{C}_F$.

b) Show that there is an identity for $\oplus$ on $\mathbf{C}_F$.

c) Show that every element in $\mathbf{C}_F$ has an inverse for $\oplus$.

d) Show that $\odot$ is commutative on $\mathbf{C}_F$.

e) Show that the distributive law holds for $\mathbf{C}_F$.

f) Show that the additive and multiplicative identities for $\mathbf{C}_F$ are different.

As a result of exercise 4.7 and the two previous theorems, we have verified that $(\mathbf{C}_F, \oplus, \odot)$ satisfies all of the field axioms except existence of multiplicative inverses. Note that up to this point we have never used the assumption that -1 is not a square in F.

4.8 Theorem (Existence of multiplicative inverses.) *Let F be a field in which -1 is not a square and let (a, b) be an element in $\mathbf{C}_F \backslash \{(0,0)\}$. Then (a, b) has an inverse for $\odot$.*

Proof: Let $(a, b) \in \mathbf{C}_F \backslash \{(0, 0\}$. I want to find a point $(x, y) \in \mathbf{C}_F$ such that

$$(a, b) \odot (x, y) = (1, 0).$$

Since multiplication is commutative, this shows that $(x, y) \odot (a, b) = (1, 0)$ and hence that (x, y) is a multiplicative inverse for (a, b). I want

$$(ax - by, ay + bx) = (1, 0),$$

so I want

$$bx + ay = 0 \tag{4.9}$$

and

$$ax - by = 1. \tag{4.10}$$

Multiply the first equation by b and the second by a to get

$$\begin{aligned} b^2x + aby &= 0 \\ a^2x - aby &= a. \end{aligned}$$

If we add these equations, we get

$$(a^2+b^2)x = a. \tag{4.11}$$

In the next lemma I'll show that if -1 is not a square then $a^2+b^2 \neq 0$ for all $(a,b) \in \mathbf{C}_F\backslash\{(0,0)\}$, so by (4.11), $x = \dfrac{a}{a^2+b^2}$. Now multiply (4.9) by a and (4.10) by $-b$ to get

$$\begin{aligned} abx + a^2y &= 0 \\ -abx + b^2y &= -b. \end{aligned}$$

If we add these equations, we get

$$(a^2+b^2)y = -b$$

so

$$y = \frac{-b}{a^2+b^2}.$$

I've shown that if $(a,b)\odot(x,y) = (1,0)$, then $(x,y) = \left(\dfrac{a}{a^2+b^2}, \dfrac{-b}{a^2+b^2}\right)$. A direct calculation shows that this works:

$$(a,b)\odot\left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right) = \left(\frac{a^2}{a^2+b^2} + \frac{b^2}{a^2+b^2}, \frac{a(-b)+ba}{a^2+b^2}\right) = (1,0). \;\|$$

4.12 Remark. The above proof shows that for all $(a,b) \in \mathbf{C}\setminus\{(0,0)\}$,

$$(a,b)^{-1} = \left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right).$$

4.13 Lemma. *Let F be a field in which -1 is not a square. Let (a,b) be an element in $\mathbf{C}_F\backslash\{(0,0)\}$. Then $a^2+b^2 \neq 0$.*

Proof: Since $(a,b) \neq (0,0)$, either $a \neq 0$ or $b \neq 0$.

Case 1: Suppose $a \neq 0$, then $a^2 \neq 0$, so

$$\begin{aligned} a^2+b^2 = 0 \implies& a^2\left(1+\left(\frac{b}{a}\right)^2\right) = 0 \\ \implies& 1+\left(\frac{b}{a}\right)^2 = 0 \\ \implies& \left(\frac{b}{a}\right)^2 = -1. \end{aligned}$$

Since -1 is not a square in F, $a^2+b^2 \neq 0$.

Case 2: Suppose $b \neq 0$. Repeat the argument of Case 1 with the roles of a and b interchanged. |||

We now have verified all of the field axioms so we know that $\mathbf{C}_F$ is a field. Hence we can calculate in $\mathbf{C}_F$ using all of the algebraic results that have been proved to hold in all fields.

4.14 Notation **($i, \tilde{a}$)** Let F be a field in which -1 is not a square. We will denote the pair $(0,1) \in \mathbf{C}_F$ by i, and if $a \in F$ we will denote the pair $(a,0) \in \mathbf{C}_F$ by $\tilde{a}$.

We have $\tilde{0} = (0,0)$ is the additive identity for $\mathbf{C}_F$, and $\tilde{1} = (1,0)$ is the multiplicative identity for $\mathbf{C}_F$. If $a \in F$, then $-\tilde{a} = -(a,0) = (-a,0) = \widetilde{-a}$. Also

$$i^2 = (0,1) \odot (0,1) = (0-1,0) = (-1,0) = -\tilde{1},$$

so i is a square root of $-\tilde{1}$.

If $a, b \in F$, then

$$\begin{aligned} \tilde{a} \oplus (\tilde{b} \odot i) &= (a,0) \oplus ((b,0) \odot (0,1)) \\ &= (a,0) \oplus (0,b) = (a,b), \end{aligned}$$

and hence every element $(a,b) \in \mathbf{C}_F$ can be written in the form $\tilde{a} \oplus (\tilde{b} \odot i)$. We have

$$\begin{aligned} \tilde{a} \odot \tilde{b} &= (a,0) \odot (b,0) = (ab,0) = \widetilde{ab} \\ \tilde{a} \oplus \tilde{b} &= (a,0) \oplus (b,0) = (a+b,0) = \widetilde{a+b}. \end{aligned}$$

Hence $\mathbf{C}_F$ contains a "copy of F". Each element a in F corresponds to a unique $\tilde{a}$ in $\mathbf{C}_F$ in such a way that addition in $\mathbf{C}_F$ corresponds to addition in F and multiplication in $\mathbf{C}_F$ corresponds to multiplication in F. We will henceforth drop the tildes, and we'll denote $\oplus$ by $+$ and $\odot$ by $\cdot$ as is usual in fields. Then every element in $\mathbf{C}_F$ can be written uniquely as $a + bi$ where $a, b \in F$ and $i^2 = -1$.

We consider F to be a subset of $\mathbf{C}_F$. An element $z = (a,b) = a + bi$ of $\mathbf{C}_F$ is in F if and only if $b = 0$. If $a, b, c, d \in F$, then

$$a + bi = c + di \iff (a,b) = (c,d) \iff a = c \text{ and } b = d.$$

4.15 Examples. I will find the square roots of $2i$ in $\mathbf{C}_{\mathbf{Q}}$. Let $a, b \in \mathbf{Q}$. Then

$$\begin{aligned}(a+bi)^2 = 2i &\iff a^2 - b^2 + 2abi = 2i \\ &\iff a^2 - b^2 = 0 \text{ and } 2ab = 2 \\ &\iff a^2 = b^2 \text{ and } ab = 1 \\ &\iff (a = b \text{ and } ab = 1) \text{ or } (a = -b \text{ and } ab = 1).\end{aligned}$$

Now

$$(a = b \text{ and } ab = 1) \iff (a = b \text{ and } a^2 = 1) \iff a + bi = \pm(1+i)$$

and

$$(a = -b \text{ and } ab = 1) \implies -b^2 = 1 \implies b^2 = -1$$

which is impossible. The only possible square roots of $2i$ are $\pm(1+i)$. You can easily verify that these are square roots of $2i$.

4.16 Example. I can solve the quadratic equation

$$z^2 - 4z + 4 - \frac{1}{2}i = 0 \tag{4.17}$$

in $\mathbf{C}_{\mathbf{Q}}$ by using the quadratic formula for $Az^2 + Bz + C = 0$.
$B^2 - 4AC = 16 - 4\left(4 - \frac{1}{2}i\right) = 2i = (1+i)^2$ (by the previous example). Since $B^2 - 4AC$ is a square, the equation has the solution set

$$\left\{\frac{4+(1+i)}{2}, \frac{4-(1+i)}{2}\right\} = \left\{\frac{5}{2} + \frac{1}{2}i, \frac{3}{2} - \frac{1}{2}i\right\}.$$

4.18 Exercise. Check that $\frac{5}{2} + \frac{1}{2}i$ and $\frac{3}{2} - \frac{1}{2}i$ are solutions to (4.17).

4.19 Exercise.

a) Write $\dfrac{1}{1-2i}$ in the form $a + bi$ where $a, b \in \mathbf{Q}$.

b) Find all solutions to

$$(1-2i)z^2 - 2z + 1 = 0$$

in $\mathbf{C}_{\mathbf{Q}}$. (You may want to use the result of example 4.15.) Write your solutions in the form $a + bi$ where $a, b \in \mathbf{Q}$.

4.20 Entertainment. We noted earlier that -1 is not a square in $\mathbf{Z}_3$, so $\mathbf{Z}_3$ has a complexification, which is a field with 9 elements. Show that if $z = 1 + i$, then the 9 elements in $\mathbf{C}_{\mathbf{Z}_3}$ are

$$\{0, z, z^2, z^3, z^4, z^5, z^6, z^7, z^8\}.$$

Can you figure out before you make any calculations which of these elements is 1?

4.2 Complex Conjugate.

4.21 Definition (Complex conjugate.) Let F be a field in which -1 is not a square. Let $z = (a, b) = a + bi$ be an element of $\mathbf{C}_F$. We define

$$z^* = (a, -b) = a - bi.$$

z^* is called the *conjugate* of z.

The following remark will be needed somewhere in the proof of the next exercise.

4.22 Remark. If F is a field in which -1 is not a square, then $2 \neq 0$ in F, since

$$\begin{aligned} 2 = 0 &\implies 1 + 1 = 0 \\ &\implies -1 = 1 \\ &\implies -1 = 1^2 \\ &\implies -1 \text{ is a square .} \end{aligned}$$

4.23 Exercise. Let F be a field in which -1 is not a square. Let $z, w \in \mathbf{C}_F$. Show that

a) $(z + w)^* = z^* + w^*$.

b) $(z \cdot w)^* = z^* \cdot w^*$.

c) $\left(\dfrac{z}{w}\right)^* = \dfrac{z^*}{w^*}$ if $w \neq 0$.

d) $z^* = 0 \iff z = 0$.

e) If $z = a + bi \in \mathbf{C}_F$, then $zz^* = a^2 + b^2 \in F$. If $z \neq 0$ then $zz^* \neq 0$.

f) $z^* = z \iff z \in F$.

g) $z^{**} = z$.

4.24 Example. The results of the previous exercise provide a way to write expressions of the form $\dfrac{z}{w}$ in the form $a + bi$. Write

$$\frac{z}{w} = \frac{z}{w} \cdot \frac{w^*}{w^*}$$

and calculate away. For example, in $\mathbf{C}_{\mathbf{Q}}$, we have

$$\begin{aligned} \frac{2+i}{(3-i)(4+5i)} &= \frac{(2+i)}{(3-i)(4+5i)} \cdot \frac{(3+i)(4-5i)}{(3+i)(4-5i)} \\ &= \frac{(2+i)(17-11i)}{(3^2+1^2)(4^2+5^2)} = \frac{45-5i}{10 \cdot 41} = \frac{5(9-i)}{5 \cdot 82} \\ &= \frac{9}{82} - \frac{1}{82}i. \end{aligned}$$

4.25 Exercise. Write each of the following elements of $\mathbf{C}_{\mathbf{Q}}$ in the form $a+bi$ where $a, b \in \mathbf{Q}$.

a) $\dfrac{(4-2i)(1+2i)}{(1-3i)(-1+3i)}$

b) $(1+i)^{10}$

4.26 Note. The first appearance of complex numbers is in *Ars Magna* (1545) by Girolamo Cardano (1501-1576).

> If it should be said, Divide 10 into two parts the product of which is 30 or 40, it is clear that this case is impossible. Nevertheless, we will work thus: $\cdots$ [16, page 219].

He then proceeds to calculate that the parts are $5 + \sqrt{-15}$ and $5 - \sqrt{-15}$, and says

> Putting aside the mental tortures involved, multiply $5 + \sqrt{-15}$ by $5 - \sqrt{-15}$ making $25 - (-15)$ which is $+15$. Hence this product is $40 \cdots$. So progresses arithmetic subtlety the end of which, as is said, is as refined as it is useless [16, page 219–220].

Around 1770, Euler wrote

> 144. All such expressions as $\surd$-1, $\surd$-2, $\surd$-3, $\surd$-4 &c are consequently impossible, or imaginary numbers, since they represent roots of negative quantities; and of such numbers we may truly assert that they are neither nothing nor greater than nothing, nor less than nothing; which necessarily constitutes them imaginary, or impossible.
>
> 145. But notwithstanding this, these numbers present themselves to the mind; they exist in our imagination, and we still have a sufficient idea of them; since we know that by $\surd$-4 is meant a number which, multiplied by itself, produces -4; for this reason also, nothing prevents us from making use of these imaginary numbers, and employing them in calculation. [20, p 43]

The use of the letter i to represent $\sqrt{-1}$ was introduced by Euler in 1777.[15, vol 2, p 128] Both Maple and Mathematica use `I` to denote $\sqrt{-1}$.

The first attempts to "justify" the complex numbers appear around 1800. The early descriptions were geometrical rather than algebraic. The algebraic construction of $\mathbf{C}_F$ used in these notes follows the ideas described by William Hamilton circa 1835 [25, page 83].

You will often find the complex conjugate of z denoted by $\overline{z}$ instead of z^*. The notion of complex conjugate seems to be due to Cauchy[45, page 26], who called $a + bi$ and $a - bi$ conjugates of each other.

Chapter 5

Real Numbers

5.1 Sequences and Search Sequences

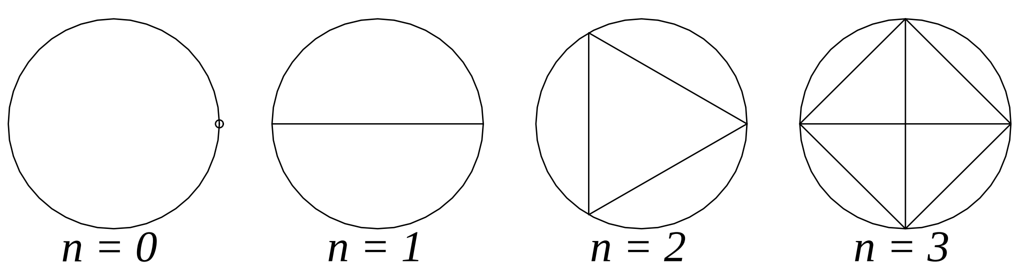
5.1 Definition (Sequence.) Let A be a set. A *sequence in* A is a function $f\colon \mathbf{N} \to A$. I sometimes denote the sequence f by $\{f(n)\}$ or $\{f(0), f(1), f(2), \cdots\}$. For example, if $f\colon \mathbf{N} \to \mathbf{Q}$ is defined by $f(n) = \frac{1}{n+1}$, I might write

$$f = \left\{\frac{1}{n+1}\right\} = \left\{1, \frac{1}{2}, \frac{1}{3}, \cdots\right\}.$$

5.2 Warning. The notation $\{f(0), f(1), f(2), \cdots\}$ is always ambiguous. For example,

$$\{1, 2, 4, 8, 16, \cdots\}$$

might denote $\{2^n\}$. It might also denote $\{\phi(n)\}$ where $\phi(n)$ is the number of regions into which a circle is divided when all the segments joining the vertices of an inscribed regular $(n+1)$-gon are drawn.



5.3 Entertainment. Show that $\phi(4) = 2^4$, but that it is not true that $\phi(n) = 2^n$ for all $n \in \mathbf{N}$.

5.4 Warning. The notation for a sequence and a set are the same, but a sequence is not a set. For example, as sets,

$$\{1,2,3,4,5,6,\cdots\} = \{2,1,4,3,6,5,\cdots\}.$$

But as sequences,

$$\{1,2,3,4,5,6,\cdots\} \neq \{2,1,4,3,6,5,\cdots\}.$$

5.5 Notation ($\mathbf{Z}_{\geq k}$) Recall from section 3.65, that If $k \in \mathbf{Z}$, then

$$\mathbf{Z}_{\geq k} = \{n \in \mathbf{Z}\colon n \geq k\}.$$

Thus, $\mathbf{Z}_{\geq 0} = \mathbf{N}$. Occasionally I will want to consider sequences whose domain is $\mathbf{Z}_{\geq k}$ where $k \neq 0$. I will denote such a sequence by

$$\{f(n)\}_{n \geq k}.$$

Hence, if

$$f = \{1,2,3,\cdots\},$$

then $f(n) = n+1$ for all $n \in \mathbf{N}$, and if

$$g = \{1,2,3,\cdots\}_{n \geq 1},$$

then $g(n) = n$ for all $n \in \mathbf{Z}_{\geq 1}$.

5.6 Remark. Most of the results we prove for sequences $\{f(n)\}$ have obvious analogues for sequences $\{f(n)\}_{n \geq k}$, and I will assume these analogues without explanation.

5.7 Examples. $\{i^n\} = \{1, i, -1, -i, 1, i, \cdots\}$ is a sequence in $\mathbf{C}_{\mathbf{Q}}$.

$$\left\{\left[0, \frac{1}{n}\right]\right\}_{n \geq 1} = \left\{[0,1], \left[0, \frac{1}{2}\right], \left[0, \frac{1}{3}\right], \cdots\right\}$$

is a sequence of intervals in an ordered field F.

5.8 Definition (Open and closed intervals.) An interval J in an ordered field is *closed* if it contains all of its endpoints. J is *open* if it contains none of its endpoints. Thus,

$$\emptyset, [a,b], (-\infty, a], [a, \infty), (-\infty, \infty) \text{ are closed intervals.}$$

$$\emptyset, (a,b), (-\infty, a), (a, \infty), (-\infty, \infty) \text{ are open intervals.}$$

$$(a,b], [a,b) \text{ where } a < b \text{ are neither open nor closed.}$$

5.9 Definition (Binary search sequence.) Let F be an ordered field. A *binary search sequence* $\{[a_n, b_n]\}$ in F is a sequence of closed intervals with end points a_n, b_n in F such that

1) $[a_{n+1}, b_{n+1}] \subset [a_n, b_n]$ for all $n \in \mathbf{N}$, and

2) $b_n - a_n = \dfrac{b_0 - a_0}{2^n}$ for all $n \in \mathbf{N}$.

Condition 1) is equivalent to

$$a_n \leq a_{n+1} \leq b_{n+1} \leq b_n \text{ for all } n \in \mathbf{N}.$$

5.10 Warning. Note that the intervals in a binary search sequence are closed. This will be important later.

5.11 Definition (Convergence of search sequence.) Let F be an ordered field, let $\{[a_n, b_n]\}$ be a binary search sequence in F, and let $x \in F$. We say $\{[a_n, b_n]\}$ *converges* to x and write $\{[a_n, b_n]\} \to x$ if $x \in [a_n, b_n]$ for all $n \in \mathbf{N}$. We say $\{[a_n, b_n]\}$ *converges*, if there is some $x \in F$ such that $\{[a_n, b_n]\} \to x$. We say $\{[a_n, b_n]\}$ *diverges* if there is no such x.

5.12 Example. Let F be an ordered field. Then $\left\{\left[0, \dfrac{1}{2^n}\right]\right\}$ is a binary search sequence and $\left\{\left[0, \dfrac{1}{2^n}\right]\right\} \to 0$.

5.13 Exercise. Let F be an ordered field, let $a, b \in F$ with $a < b$. Let $m = \dfrac{a+b}{2}$. Show that

1) $a < m < b$.

2) $m - a = b - m = \dfrac{1}{2}(b - a)$.

(Conditions 1) and 2) say that m is the midpoint of a and b.)

5.14 Exercise. Let F be an ordered field and let $a, b \in F$ with $a \leq b$ and let c, d be points in $[a, b]$. Show that

$$|c - d| \leq b - a;$$

i.e., if two points lie in an interval then the distance between the points is less than or equal to the length of the interval.

5.15 Exercise. Show that $2^n \geq n$ for all $n \in \mathbf{N}$.

5.16 Example (A divergent binary search sequence.) Define a binary search sequence $\{[a_n, b_n]\}$ in $\mathbf{Q}$ by the rules

$$\begin{aligned} [a_0, b_0] &= [1, 2]. \\ [a_{n+1}, b_{n+1}] &= \begin{cases} \left[a_n, \frac{a_n+b_n}{2}\right] & \text{if } \left(\frac{a_n+b_n}{2}\right)^2 \geq 2, \\ \left[\frac{a_n+b_n}{2}, b_n\right] & \text{if } \left(\frac{a_n+b_n}{2}\right)^2 < 2. \end{cases} \end{aligned}$$

Thus,

$$\frac{a_0+b_0}{2} = \frac{1+2}{2} = \frac{3}{2}; \quad \left(\frac{a_0+b_0}{2}\right)^2 = \frac{9}{4} > 2, \text{ so } [a_1, b_1] = \left[\frac{2}{2}, \frac{3}{2}\right];$$

$$\frac{a_1+b_1}{2} = \frac{\frac{2}{2}+\frac{3}{2}}{2} = \frac{5}{4}; \quad \left(\frac{a_1+b_1}{2}\right)^2 = \frac{25}{16} < 2, \text{ so } [a_2, b_2] = \left[\frac{5}{4}, \frac{6}{4}\right];$$

$$\frac{a_2+b_2}{2} = \frac{\frac{5}{4}+\frac{6}{4}}{2} = \frac{11}{8}; \quad \left(\frac{a_2+b_2}{2}\right)^2 = \frac{121}{64} < 2, \text{ so } [a_3, b_3] = \left[\frac{11}{8}, \frac{12}{8}\right].$$

Since $\dfrac{a_n+b_n}{2}$ is the midpoint of $[a_n, b_n]$, we have

$$[a_{n+1}, b_{n+1}] \subset [a_n, b_n]$$

and

$$b_{n+1} - a_{n+1} = \frac{1}{2}(b_n - a_n) \tag{5.17}$$

It follows from (5.17) that

$$b_n - a_n = \frac{1}{2^n}(b_0 - a_0) \text{ for all } n \in \mathbf{N}.$$

Hence $\{[a_n, b_n]\}$ is a binary search sequence. For each $n \in \mathbf{N}$, let $P(n)$ be the proposition

$$P(n) = \text{“}a_n^2 < 2 \leq b_n^2.\text{”}$$

Then $P(0)$ says $1^2 < 2 \leq 2^2$, so $P(0)$ is true. Let $n \in \mathbf{N}$.
If $\left(\dfrac{a_n+b_n}{2}\right)^2 \geq 2$, then

$$\begin{aligned} P(n) &\implies a_n^2 < 2 \leq b_n^2 \implies a_{n+1}^2 = a_n^2 < 2 \leq \left(\frac{a_n+b_n}{2}\right)^2 = b_{n+1}^2 \\ &\implies a_{n+1}^2 < 2 \leq b_{n+1}^2 \\ &\implies P(n+1). \end{aligned}$$

If $\left(\frac{a_n + b_n}{2}\right)^2 < 2$, then

$$\begin{aligned} P(n) &\implies a_n^2 < 2 \le b_n^2 \implies a_{n+1}^2 = \left(\frac{a_n + b_n}{2}\right)^2 < 2 \le b_n^2 = b_{n+1}^2 \\ &\implies a_{n+1}^2 < 2 \le b_{n+1}^2 \\ &\implies P(n+1). \end{aligned}$$

Hence, in all cases, $P(n) \implies P(n+1)$, and by induction, $a_n^2 < 2 \le b_n^2$ for all $n \subset \mathbf{N}$. Since $x^2 \neq 2$ for all $x \in \mathbf{Q}$, we have

$$a_n^2 < 2 < b_n^2 \text{ for all } n \in \mathbf{N}. \tag{5.18}$$

I now will show that $\{[a_n, b_n]\}$ diverges. Suppose, in order to get a contradiction, that for some $x \in \mathbf{Q}$, $\{[a_n, b_n]\} \to x$. Then

$$0 \le a_n \le x \le b_n \text{ for all } n \in \mathbf{N},$$

so

$$a_n^2 \le x^2 \le b_n^2.$$

Combining this with (5.18), we get

$$|x^2 - 2| \le b_n^2 - a_n^2 = (b_n - a_n)(b_n + a_n) \le \left(\frac{b_0 - a_0}{2^n}\right)(b_0 + b_0) = \frac{4}{2^n} \tag{5.19}$$

for all $n \in \mathbf{N}$. Since 2 is not a square in $\mathbf{Q}$, $x^2 - 2 \neq 0$. Write $|x^2 - 2| = \frac{p}{q}$, where $p, q \in \mathbf{Z}_{\ge 1}$. Then

$$\text{for all } n \in \mathbf{N},\ \frac{p}{q} \le \frac{4}{2^n},$$

so

$$\text{for all } n \in \mathbf{N},\ 2^n \le \frac{4q}{p} \le 4q.$$

By exercise 5.15, for all $n \in \mathbf{N}$,

$$n \le 2^n \le 4q. \tag{5.20}$$

Statement (5.20) is false when $n = 4q + 1$, and hence our assumption that $\{[a_n, b_n]\} \to x$ was false. ‖

5.2 Completeness

5.21 Definition (Completeness axiom.) Let F be an ordered field. We say that F is *complete* if it satisfies the condition:

Every binary search sequence in F converges to a unique point in F.

5.22 Example. The field $\mathbf{Q}$ is not complete, since in example 5.16 we found a binary search sequence in $\mathbf{Q}$ that does not converge.

5.23 Definition (Real field, R.) A *real field* is a complete ordered field. We will use the name $\mathbf{R}$ to denote a real field.

5.24 Remark. It is not at all clear that any real fields exist. If real fields do exist, there is a question of uniqueness; i.e., is it the case that any two real fields are "essentially the same"? I don't want to worry about what mathematical existence means, so let me formulate the questions: Are the axioms for a real field consistent; i.e., is it the case that no contradictions can be derived from them? Note that we are not entirely free to throw axioms together. If I were to make a definition that a *3-field* is an ordered field in which $3 = 0$, I would immediately get a contradiction: $3 = 0$ and $3 > 0$. All I can say about consistency is that no contradictions have been found to follow from the real field axioms. There exist proofs that any two real fields are essentially the same, cf. [35, page 129]. (This source uses a different statement for the completeness axiom than we have used, but the axiom system is equivalent to ours.) There also exist constructions of pairs of very different real fields, cf. [41].

In what follows, I am going to assume that there is a real field $\mathbf{R}$ (which I'll call *the real numbers*). Any theorems proved will be valid in all real fields.

5.25 Theorem (Archimedean property 1.) *Let* $\mathbf{R}$ *be a real field, and let* $x \in \mathbf{R}$. *Then there is an integer* $n \in \mathbf{N}$ *such that* $n > x$.

Proof: Let $x \in \mathbf{R}$, and suppose (in order to get a contradiction) that there is no $n \in \mathbf{N}$ with $n > x$. Then $x \geq n$ for all n. Now $\left\{\left[0, \frac{x}{2^n}\right]\right\}$ is a binary search sequence in $\mathbf{R}$. Since $x \geq 2^n$, I have $1 \leq \frac{x}{2^n}$ for all $n \in \mathbf{N}$. We see that $\left\{\left[0, \frac{x}{2^n}\right]\right\} \to 1$, but clearly $\left\{\left[0, \frac{x}{2^n}\right]\right\} \to 0$. Since completeness of $\mathbf{R}$ implies that a binary search sequence has a unique limit, this yields a contradiction, and proves the theorem. |||

5.26 Corollary (Archimedean property 2.) *Let $x \in \mathbf{R}\backslash\{0\}$. Then there is some $n \in \mathbf{Z}_{\geq 1}$ such that $\frac{1}{n} < |x|$.*

Proof: By the theorem, there is some $n \in \mathbf{Z}_{\geq 1}$ with $n > \frac{1}{|x|}$. Then $\frac{1}{n} < |x|$. ‖

5.27 Corollary (Archimedean property 3.) *Let x be a real number, and let C be a positive real number. Suppose*

$$|x| \leq \frac{C}{n} \text{ for all } n \in \mathbf{Z}_{\geq 1}. \tag{5.28}$$

Then $x = 0$.

Proof: Let $x \in \mathbf{R}$, and let $C \in \mathbf{R}^+$ satisfy

$$|x| \leq \frac{C}{n} \text{ for all } n \in \mathbf{Z}_{\geq 1}. \tag{5.29}$$

Suppose, in order to get a contradiction, that $x \neq 0$. Then by Archimedian property 2 there is some $n \in \mathbf{Z}_{\geq 1}$ such that $\frac{1}{n} < \frac{|x|}{C}$, i.e. $\frac{C}{n} < |x|$. This contradicts (5.29). ‖

5.30 Theorem. *If $t \in \mathbf{R}$, then there is an integer n and a number $\varepsilon \in [0, 1)$ such that $t = n + \varepsilon$.*

In order to prove this theorem, I will use the following lemma.

5.31 Lemma. *If $t \in \mathbf{R}$, then the interval $(t, t+1]$ contains an integer.*

Proof:

Case 1. $t \in [0, \infty)$: Suppose $t \in [0, \infty)$ and $(t, t+1]$ does not contain an integer. I will show that $t \geq n$ for all $n \in \mathbf{N}$. This contradicts the Archimedean property, so no such t can exist. For each $n \in \mathbf{N}$, let $P(n) =$ "$n \leq t$". Then $P(0)$ is true, since I assumed that $t \in [0, \infty)$. Let $n \in \mathbf{N}$ be a number such that $P(n)$ is true; i.e., $n \leq t$. If $n+1$ were $> t$, we'd have $t < n+1 \leq t+1$, and this cannot happen, since $(t, t+1]$ contains no integers. Hence,

$$P(n) \implies n+1 \leq t \implies P(n+1),$$

and by induction, $t \geq n$ for all $n \in \mathbf{N}$. This gives the desired contradiction.

Case 2. $t \in \mathbf{R}^-$: If $t \in \mathbf{R}^-$, then by Case 1 there is an integer n with

$$-t < n \leq -t + 1.$$

Then

$$t \leq -n + 1 < t + 1.$$

If $t < -n + 1$, then $(t, t+1]$ contains $-n + 1$. If $t = -n + 1$, then $(t, t+1] = (-n+1, -n+2]$ contains $-n + 2$. |||

Proof of theorem 5.30. Let $t \in \mathbf{R}$. By the lemma, there is an integer n with $t < n \leq t + 1$. Then

$$0 \leq t - n + 1 < 1,$$

and $t = (n-1) + (t - n + 1)$ gives the desired decomposition. |||

5.32 Theorem. *There is a number $x \in \mathbf{R}$ such that $x^2 = 2$.*

Proof: Let $\{[a_n, b_n]\}$ be the binary search sequence constructed in example 5.16. We know there is a unique $x \in \mathbf{R}$ such that $0 \leq a_n \leq x \leq b_n$ for all n. Then $0 \leq a_n^2 \leq x^2 \leq b_n^2$, and by our construction $0 \leq a_n^2 \leq 2 \leq b_n^2$ for all $n \in \mathbf{N}$, so

$$|2 - x^2| \leq b_n^2 - a_n^2 = (b_n - a_n)(b_n + a_n) \leq \frac{1}{2^n} \cdot 4 \leq \frac{4}{n} \tag{5.33}$$

for all $n \in \mathbf{Z}_{\geq 1}$.

By Archimedean property 3, we conclude that $2 - x^2 = 0$, i.e., $x^2 = 2$. |||

5.34 Theorem. *Let $x \in \mathbf{R}$. Then there is a binary search sequence $\{[a_n, b_n]\}$ in $\mathbf{R}$ such that $a_n \in \mathbf{Q}$ and $b_n \in \mathbf{Q}$ for all n, and such that $\{[a_n, b_n]\} \to x$.*

Proof: I will suppose $x \geq 0$. The case where $x \leq 0$ is left to you. By the Archimedean property of $\mathbf{R}$, there is an integer N such that $N > x$, so $x \in [0, N]$. Now build a binary search sequence $\{[a_n, b_n]\}$ as follows:

$$\begin{aligned} [a_0, b_0] &= [0, N] \\ [a_{n+1}, b_{n+1}] &= \begin{cases} \left[a_n, \frac{a_n + b_n}{2}\right] & \text{if } x \leq \left[\frac{a_n + b_n}{2}\right] \\ \left[\frac{a_n + b_n}{2}, b_n\right] & \text{if } x > \left[\frac{a_n + b_n}{2}\right]. \end{cases} \end{aligned}$$

From the construction, we have $a_n \leq a_{n+1} \leq b_{n+1} \leq b_n$ and $b_n - a_n = \dfrac{b_0 - a_0}{2^n}$. A simple induction argument shows that $a_n \in \mathbf{Q}$ and $b_n \in \mathbf{Q}$ for all $n \in \mathbf{N}$, and an induction proof similar to the one in example 5.16 shows that $a_n \leq x \leq b_n$ for all $n \in \mathbf{N}$ so $\{[a_n, b_n]\} \to x$. |||

5.3 Existence of Roots

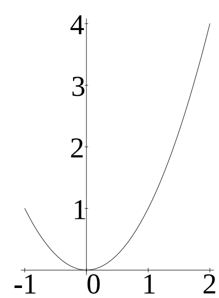
5.35 Definition (Graph.) Let $f: A \to B$ be a function. The *graph of f* is

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

5.36 Remark. If f is a function from $\mathbf{R}$ to $\mathbf{R}$, then graph f is

$$\{(x, y) \in \mathbf{R}^2: y = f(x)\}.$$

You may find it useful to think of $\mathbf{R}$ as points on a line, and $\mathbf{R}^2$ as points in a plane and to represent the graph by a picture. Any such picture is outside the scope of our formal development, but I will draw lots of such pictures informally.



graph of f where $f(x) = x^2$ for $x \in (-1, 2)$.

5.37 Definition (Sum and product of functions.) Let F be a field, and let $\alpha \in F$. Let A, B be sets and let $f: A \to F, g: B \to F$ be functions. We define functions $f + g$, $f - g$, $f \cdot g$, αf and $\dfrac{f}{g}$ by:

$f + g: A \cap B \to F$	$(f + g)(a) = f(a) + g(a)$ for all $a \in A \cap B$.
$f - g: A \cap B \to F$	$(f - g)(a) = f(a) - g(a)$ for all $a \in A \cap B$.
$f \cdot g: (A \cap B) \to F$	$(f \cdot g)(a) = f(a) \cdot g(a)$ for all $a \in A \cap B$.
$\alpha f: A \to F$	$(\alpha f)(a) = \alpha \cdot f(a)$ for all $a \in A$.
$\dfrac{f}{g}: D \to F$	$\left(\dfrac{f}{g}\right)(a) = \dfrac{f(a)}{g(a)}$ for all $a \in D$.

where $D = \{x \in A \cap B: g(x) \neq 0\}$.

5.38 Remark. Let F be a field, let S be a set, and let $f\colon S \to F$, $g\colon S \to F$ be functions with the same domain. Then the operations $+, \cdot, -$ are binary operations on the set $\mathcal{S}$ of all functions from S to F. These operations satisfy the same commutative, associative and distributive laws that the corresponding operations on F satisfy; e.g.,

$$f \cdot (g + h) = f \cdot g + f \cdot h \text{ for all } f, g, h \in \mathcal{S}. \tag{5.39}$$

Proof of (5.39). For all $x \in S$,

$$\begin{aligned}(f \cdot (g+h))\,(x) &= f(x)(g+h)(x)\\ &= f(x)\,(g(x)+h(x))\\ &= f(x)g(x) + f(x)h(x)\\ &= (f \cdot g)(x) + (f \cdot h)(x)\\ &= ((f \cdot g) + (f \cdot h))\,(x).\end{aligned}$$

Hence, $f \cdot (g+h) = (f \cdot g) + (f \cdot h)$. (Two functions are equal when they have the same domain, the same codomain, and the same rule.) ‖

5.40 Definition (Increasing and decreasing.) Let J be an interval in $\mathbf{R}$ and let $f\colon J \to \mathbf{R}$. We say

f is increasing on J if for all $s, t \in J\,(s \le t \implies f(s) \le f(t))$.

f is strictly increasing on J if for all $s, t \in J\,(s < t \implies f(s) < f(t))$.

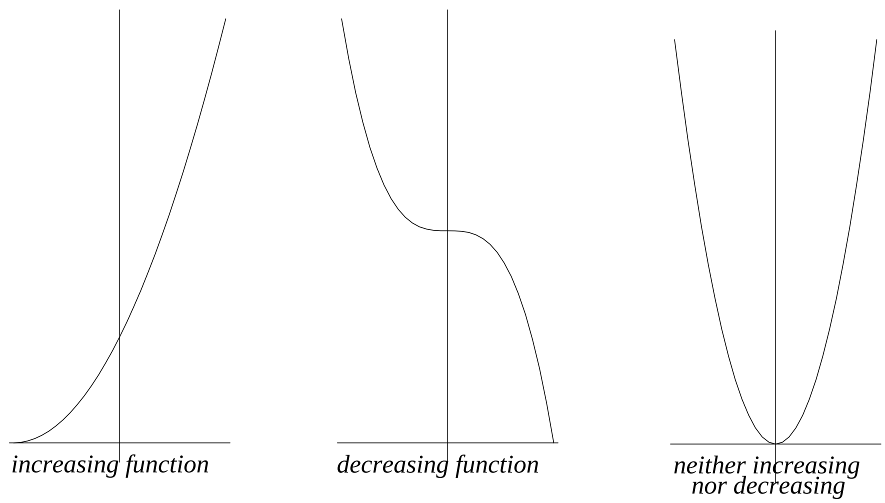
f is decreasing on J if for all $s, t \in J\,(s \le t \implies f(s) \ge f(t))$.

f is strictly decreasing on J if for all $s, t \in J\,(s < t \implies f(s) > f(t))$.

5.41 Remark. Since $s = t \implies f(s) = f(t)$, we can reformulate the definitions of increasing and decreasing as follows:

f is increasing on J if for all $s, t \in J\,(s < t \implies f(s) \le f(t))$.

f is decreasing on J if for all $s, t \in J\,(s < t \implies f(s) \ge f(t))$.



5.42 Exercise. Is there a function $f: \mathbf{R} \to \mathbf{R}$ that is both increasing and decreasing? If the answer is yes, give an example. If the answer is no, explain why not.

5.43 Exercise. Give an example of a function $f: \mathbf{R} \to \mathbf{R}$ such that f is increasing, but not strictly increasing.

5.44 Exercise. Let $f: \mathbf{R} \to \mathbf{R}$ and $g: \mathbf{R} \to \mathbf{R}$ be increasing functions. Either prove that $f + g$ is increasing or give an example to show that $f + g$ is not necessarily increasing

5.45 Exercise. Let $f: \mathbf{R} \to \mathbf{R}$ and $g: \mathbf{R} \to \mathbf{R}$ be increasing functions. Either prove that $f \cdot g$ is increasing or give an example to show that $f \cdot g$ is not necessarily increasing.

5.46 Theorem. *Let $m \in \mathbf{Z}_{\geq 1}$, let $a \in \mathbf{R}$, $a \geq 1$. Then $a^m \geq a$.*

The proof is by induction, and is omitted.

5.47 Theorem. *Let $m \in \mathbf{Z}_{\geq 1}$. Let $f_m(x) = x^m$ for all $x \in [0, \infty)$ in $\mathbf{R}$. Then f_m is strictly increasing on $[0, \infty)$.*

Proof: The proof follows from induction on m or by factoring $x^m - y^m$, and is omitted.

5.48 Exercise. Let J be an interval in $\mathbf{R}$ and let $f\colon J \to \mathbf{R}$ be a strictly increasing function on J. Show that for each $a \in \mathbf{R}$ the equation $f(x) = a$ has at most one solution x in J.

5.49 Theorem. *Let $p \in \mathbf{Z}_{\geq 1}$ and let $a \in [0, \infty)$ in $\mathbf{R}$. Then there is a unique $c \in [0, \infty)$ in $\mathbf{R}$ such that*

$$c^p = a.$$

Proof: First I will construct a binary search sequence $\{[a_n, b_n]\}$ in $\mathbf{R}$ such that

$$a_n^p \leq a \leq b_n^p \text{ for all } n \in \mathbf{N}.$$

By completeness of $\mathbf{R}$, I'll have $\{[a_n, b_n]\} \to c$ for some $c \in \mathbf{R}$. I'll show $c^p = a$, and the proof will be complete.

Let $[a_0, b_0] = [0, (1 + a)]$. Then

$$a_0^p = 0 \leq a < (1 + a) \leq (1 + a)^p = b_0^p.$$

For $n \in \mathbf{N}$, define

$$[a_{n+1}, b_{n+1}] = \begin{cases} \left[a_n, \frac{a_n+b_n}{2}\right] & \text{if } \left(\frac{a_n+b_n}{2}\right)^p \geq a \\ \left[\frac{a_n+b_n}{2}, b_n\right] & \text{if } \left(\frac{a_n+b_n}{2}\right)^p < a. \end{cases}$$

The proof that $\{[a_n, b_n]\}$ is a binary search sequence and that $a_n^p \leq a \leq b_n^p$ for all $n \in \mathbf{N}$ is the same as the proof given in example 5.16 for $a = p = 2$, and will not be repeated here. By completeness $\{[a_n, b_n]\} \to c$ for some $c \in \mathbf{R}$. Since $0 \leq a_n \leq c \leq b_n$, we have $a_n^p \leq c^p \leq b_n^p$. It follows that

$$|a - c^p| \leq b_n^p - a_n^p \text{ for all } n \in \mathbf{N}.$$

By the formula for factoring $b^p - a^p$ (cf. (3.78)), we have

$$\begin{aligned} |a - c^p| &\leq (b_n - a_n) \sum_{j=0}^{p-1} b_n^j a_n^{p-1-j} \leq (b_n - a_n) \sum_{j=0}^{p-1} b_n^j b_n^{p-1-j} \\ &= (b_n - a_n) p b_n^{p-1} \leq \frac{b_0 - a_0}{2^n} \cdot p b_0^{p-1} \leq \frac{(b_0 - a_0) p b_0^{p-1}}{n} \end{aligned}$$

for all $n \in \mathbf{Z}_{\geq 1}$. By Archimedean property 3 (cf corollary 5.28), it follows that $a - c^p = 0$, i.e $c^p = a$.

Let $f_p(x) = x^p$. Since f_p is strictly increasing on $\mathbf{R}$, it follows from exercise 5.48 that $x^p = a$ has at most one solution in $\mathbf{R}^+$ and this completes the proof of the theorem. $\|$

5.50 Notation ($a^{\frac{1}{p}}$.) If $p \in \mathbf{Z}_{\geq 1}$ and $a \in [0, \infty)$, then the unique number c in $[0, \infty)$ such that $c^p = a$ is denoted by $a^{\frac{1}{p}}$, and is called the *pth root of* a. An alternative notation for $a^{\frac{1}{2}}$ is $\sqrt{a}$.

5.51 Exercise. Let $a \in [0, \infty)$, let $q, r \in \mathbf{Z}_{\geq 1}$, and let $p, s \in \mathbf{Z}$.

a) Show that $\left(a^{\frac{1}{q}}\right)^p = (a^p)^{\frac{1}{q}}$.

b) Show that if $\dfrac{p}{q} = \dfrac{s}{r}$, then $\left(a^{\frac{1}{q}}\right)^p = \left(a^{\frac{1}{r}}\right)^s$.

5.52 Definition (a^r.) If $a \in \mathbf{R}^+$ and $r \in \mathbf{Q}$ we define $a^r = \left(a^{\frac{1}{q}}\right)^p$ where $q \in \mathbf{Z}_{\geq 1}$, $p \in \mathbf{Z}$ and $r = \dfrac{p}{q}$. The previous exercise shows that this definition does not depend on what representation we use for writing r.

5.53 Theorem (Laws of exponents.) *For all $a, b \in [0, \infty)$ and all $r, s \in \mathbf{Q}$,*

a) $(ab)^r = a^r b^r$.

b) $a^r a^s = a^{r+s}$.

c) $(a^r)^s = a^{(rs)}$.

Proof: [of part b)] Let $r = \dfrac{p}{q}$, $s = \dfrac{u}{v}$ where u, v are integers and q, v are positive integers. Then (by laws of exponents for integer exponents),

$$\begin{aligned}(a^r a^s)^{q\cdot v} &= \left(a^{\frac{p}{q}} \cdot a^{\frac{u}{v}}\right)^{q\cdot v} = \left(a^{\frac{p}{q}}\right)^{(q\cdot v)} \cdot \left(a^{\frac{u}{v}}\right)^{(q\cdot v)} \\ &= \left(\left((a^p)^{\frac{1}{q}}\right)^q\right)^v \cdot \left(\left((a^u)^{\frac{1}{v}}\right)^v\right)^q = (a^p)^v \cdot (a^u)^q = a^{(pv)} a^{(uq)} \\ &= a^{pv+uq}.\end{aligned}$$

Also,

$$\begin{aligned}(a^{r+s})^{q\cdot v} &= \left(a^{\left(\frac{p}{q}+\frac{u}{v}\right)}\right)^{q\cdot v} \\ &= \left(a^{\left(\frac{pv+uq}{qv}\right)}\right)^{(qv)} = \left(\left(a^{(pv+uq)}\right)^{\frac{1}{qv}}\right)^{qv} \\ &= a^{pv+uq}.\end{aligned}$$

Hence, $(a^r a^s)^{q\cdot v} = (a^{r+s})^{q\cdot v}$, and hence $a^r a^s = a^{r+s}$ by uniqueness of $q \cdot v$ roots.

5.54 Exercise. Prove parts a) and c) of theorem 5.53.

5.55 Entertainment. Show that of the two real numbers

$$\sqrt{\tfrac{9}{2}+\sqrt{8}}+\sqrt{\tfrac{9}{2}-\sqrt{8}}, \quad \sqrt{\tfrac{9}{2}+\sqrt{8}}-\sqrt{\tfrac{9}{2}-\sqrt{8}},$$

one is in $\mathbf{Q}$, and the other is not in $\mathbf{Q}$.

5.56 Note. The Archimedean property was stated by Archimedes in the following form:

> $\cdots$ the following lemma is assumed: that the excess by which the greater of (two) unequal areas exceeds the less can, by being added to itself, be made to exceed any given finite area. The earlier geometers have also used this lemma.[2, p 234]

Euclid indicated that his arguments needed the Archimedean property by using the following definition:

> Magnitudes are said to *have a ratio* to one another which are capable, when multiplied, of exceeding one another.[19, vol 2, p114]

Here "multiplied" means "added to itself some number of times", i.e. "multiplied by some positive integer".

Rational exponents were introduced by Newton in 1676.

> Since algebraists write a^2, a^3, a^4, etc., for $aa, aaa, aaaa$, etc., so I write $a^{\frac{1}{2}}, a^{\frac{3}{2}}, a^{\frac{5}{3}}$, for $\sqrt{a}, \sqrt{a^3}, \sqrt{ca^5}$; and I write a^{-1}, a^{-2}, a^{-3}, etc. for $\frac{1}{a}, \frac{1}{aa}, \frac{1}{aaa}$, etc.[14, vol 1, p355]

Here $\sqrt{ca}$ denotes the cube root of a.

Buck's *Advanced Calculus*[12, appendix 2] gives eight different characterizations of the completeness axiom and discusses the relations between them.

The term *completeness* is a twentieth century term. Older books speak about the *continuity* of the real numbers to describe what we call completeness.

Chapter 6

The Complex Numbers

Many of the results in this chapter are informal and geometrical, and do not follow logically from our assumptions. I will freely use properties of similar triangles, parallelograms, and trigonometric functions. Some of the results (e.g., those involving trigonometric identities) will be rederived later in a more rigorous form. Every statement labeled **Theorem** or **Definition** is part of our logical development.

6.1 Absolute Value and Complex Conjugate

6.1 Definition (Complex Numbers, C.) We denote the complexification of $\mathbf{R}$ by $\mathbf{C}$, and we call $\mathbf{C}$ the *complex numbers*.

6.2 Definition (Absolute value.) In exercise 4.23 we showed that (for any field F in which -1 is not a square), if $z = a + bi = (a, b) \in \mathbf{C}_F$, then

$$z^* z = a^2 + b^2 \in F.$$

If we are working in $\mathbf{C}$, then $a^2 + b^2 \in [0, \infty)$ and hence zz^* has a unique square root in $[0, \infty)$, which we denote by $|z|$ and call the *absolute value* of z.

$$|z| = (z^* z)^{1/2} \text{ for all } z \in \mathbf{C}.$$

We note that

$$|z| \in \mathbf{R}^+ \cup \{0\} \text{ for all } z \in \mathbf{C}.$$
$$|z| = 0 \iff z = 0.$$

Also note that for $z \in \mathbf{R}$, this definition agrees with our old definition of absolute value in $\mathbf{R}$.

6.3 Definition (Real and imaginary parts.) Let $z \in \mathbf{C}$ and write $z = x + iy$ where $x, y \in \mathbf{R}$. We call x the *real part of* z, and we call y the *imaginary part of* z (note that the imaginary part of z is real), and we write

$$x = \mathrm{Re}(z), \quad y = \mathrm{Im}(z) \text{ if } z = (x, y) = x + iy.$$

6.4 Theorem. *Let z, w be complex numbers. Then*

a) $|zw| = |z|\,|w|$.

b) $\left|\dfrac{z}{w}\right| = \dfrac{|z|}{|w|}$ *if* $w \neq 0$.

c) $\mathrm{Re}(z) = \dfrac{z + z^*}{2}$.

d) $\mathrm{Im}(z) = \dfrac{z - z^*}{2i}$.

e) $|\mathrm{Re}(z)| \leq |z|$.

f) $|\mathrm{Im}(z)| \leq |z|$.

g) $|z^*| = |z|$.

h) $\mathrm{Re}(z + w) = \mathrm{Re}(z) + \mathrm{Re}(w)$.

i) $\mathrm{Im}(z + w) = \mathrm{Im}(z) + \mathrm{Im}(w)$.

Proof: By using properties of the complex conjugate proved in exercise 4.23, we have

$$|zw|^2 = (zw)^*(zw) = z^* w^* z w = z^* z w^* w = |z|^2 |w|^2.$$

Hence by uniqueness of square roots, $|zw| = |z|\,|w|$. The proofs of b), c), d), e), f), g), h) and i) are left to you. |||

6.5 Exercise. Prove parts b), c), d), e), f), g), h) and i) of Theorem 6.4.

6.6 Theorem (Triangle inequality.) *Let $z, w \in \mathbf{C}$. Then*

$$|z+w| \le |z| + |w|.$$

Proof: For all $z, w \in \mathbf{C}$,

$$\begin{aligned} |z+w|^2 &= (z+w)^* \cdot (z+w) = (z^*+w^*) \cdot (z+w) \\ &= z^*z + z^*w + w^*z + w^*w \\ &= |z|^2 + z^*w + w^*z + |w|^2. \end{aligned} \tag{6.7}$$

Now since $z^{**} = z$, we have

$$\begin{aligned} z^*w + w^*z &= (z^*w) + (z^*w)^* \\ &= 2\text{Re}(z^*w) \le 2|\text{Re}(z^*w)| \\ &\le 2|z^*w| = 2|z^*|\ |w| = 2|z|\ |w|. \end{aligned}$$

Hence, from (6.7),

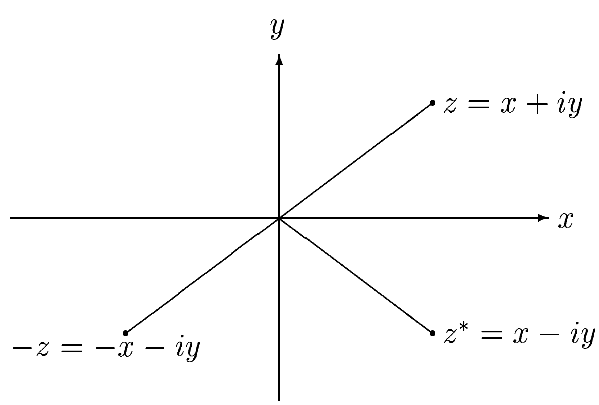
$$|z+w|^2 \le |z|^2 + 2|z|\ |w| + |w|^2 = (|z| + |w|)^2,$$

and it follows that

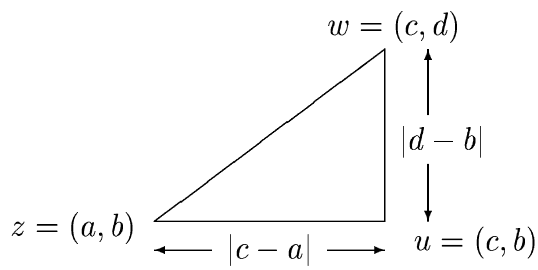
$$|z+w| \le |z| + |w|. \ \|$$

6.2 Geometrical Representation

Since $\mathbf{C} = \mathbf{R} \times \mathbf{R}$, we can identify complex numbers with points in a plane.



Then $\mathbf{R}$ is identified with the x-axis, and points on the y-axis are of the form iy where y is real. I will call the x-axis the *real axis*, and I'll call the y-axis the *imaginary axis*. If $z \in \mathbf{C}$, then z^* represents the result of reflecting z about the real axis. Also $-z$ represents the result of reflecting z through the origin.



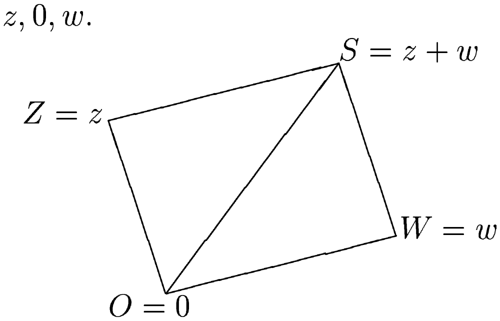
If $z = (a, b)$ and $w = (c, d)$ are two points in $\mathbf{C}$, and $u = (c, b)$, then z, u, w are the vertices of a right triangle having legs of length $|c - a|$, and $|d - b|$. By the Pythagorean theorem, the distance from w to z is $\sqrt{(c-a)^2 + (d-b)^2}$. Also,

$$\begin{aligned} |w - z| &= |(c + id) - (a + ib)| \\ &= |(c - a) + i(d - b)| \\ &= \sqrt{(c-a)^2 + (d-b)^2} \\ &= \text{distance from } w \text{ to } z, \end{aligned}$$

and in particular, for $z = 0$,

$$|w| = \text{ distance from } w \text{ to } 0.$$

Claim: If $z, w \in \mathbf{C}$, then $z + w$ is the fourth vertex of the parallelogram having consecutive vertices $z, 0, w$.



To make this look like a geometry proof, I'll denote points by upper case letters, and let AB denote the distance from A to B. Let $O = 0$, $W = w$, $Z = z$, $S = z + w$. Then

$$ZS = |(z + w) - z| = |w| = |w - 0| = OW$$

$$WS = |(z + w) - w| = |z| = |z - 0| = OZ.$$

Hence, since the quadrilateral $OWSZ$ has opposite sides equal, it is a parallelogram.

We can now give a geometrical interpretation for the triangle inequality (which motivates its name). In the figure above,

$$|z + w| \leq |z| + |w|$$

says

$$OS \leq OZ + ZS;$$

i.e, the sum of two sides of a triangle is greater than or equal to the third side. This is proposition 20 of book 1 of Euclid [19] "In any triangle, two sides taken together in any manner are greater than the remaining one." (Euclid did not consider triangles in which all three vertices lie on a line.)

> It was the habit of the Epicureans, says Proclus ... to ridicule this theorem as being evident even to an ass, and requiring no proof, and their allegation that the theorem was "known" ($\gamma\nu\acute{\omega}\rho\iota\mu o\nu$) even to an ass was based on the fact that, if fodder is placed at one angular point and the ass at another, he does not, in order to get his food, traverse the two sides of the triangle but only the one side separating them [19, vol. I page 287].

6.8 Definition (Circle, disc.) Let $\alpha \in \mathbf{C}, r \in \mathbf{R}^+$. The *circle* with center α and radius r is

$$\begin{aligned} C(\alpha, r) &= \{z \in \mathbf{C}: |z - \alpha| = r\} \\ &= \text{set of points whose distance from } a \text{ is } r. \end{aligned}$$

The *open disc* with center α and radius r is

$$D(\alpha, r) = \{z \in \mathbf{C}: |z - \alpha| < r\},$$

and the *closed disc* with center α and radius r is

$$\bar{D}(\alpha, r) = \{z \in \mathbf{C}: |z - \alpha| \leq r\}.$$

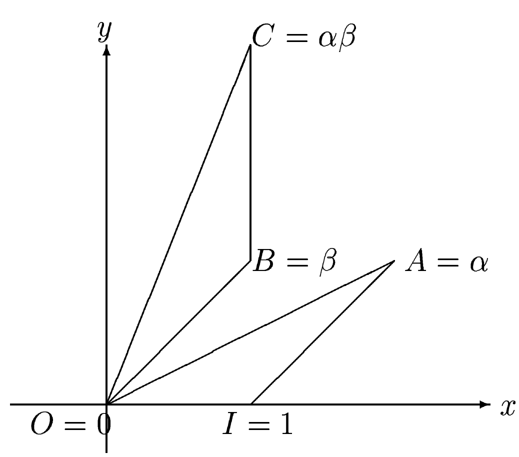
$C(0,1)$ is called the *unit circle*, and $D(0,1)$ is called the *unit disc*. A complex number z is in the unit circle if and only if $|z| = 1$.

6.9 Warning. The word "circle" is sometimes used to mean "disc", although the word "disc" is never used to mean "circle". When you see the word "circle" used in a mathematical statement, you should determine from the context which of the two words is meant. For example, in the statement "the area of the unit circle is π", the word "circle" means "disc", since the unit circle is, in fact, a zero-area set. In these notes the word "circle" always means "circle" except on page 92.

6.10 Theorem. *The product of two numbers in the unit circle is in the unit circle.*

Proof: Let $\alpha, \beta \in C(0,1)$; i.e., $|\alpha| = |\beta| = 1$. Then $|\alpha\beta| = |\alpha||\beta| = 1 \cdot 1 = 1$, so $\alpha\beta \in C(0,1)$. $\|$

We can also give a geometrical interpretation to the product of two complex numbers. Let $\alpha = A$ and $\beta = B$ be complex numbers and let $C = \alpha\beta$. Let $O = 0$ and let $I = 1$.

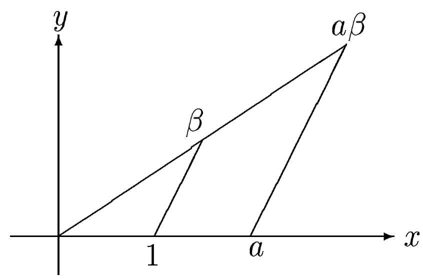


Then $\triangle OIA$ is similar to $\triangle OBC$. The proof consists in showing that

$$\frac{OI}{OB} = \frac{IA}{BC} = \frac{OA}{OC}. \tag{6.11}$$

6.12 Exercise. Prove the equalities listed in (6.11). Assume $\alpha \notin \{0, 1\}$ and $\beta \neq 0$.

From the similarity of $\triangle OIA$ and $\triangle OBC$, we have $\angle IOA = \angle BOC$. In particular, if we take $\alpha = a \in \mathbf{R}^+$, we get the picture



where

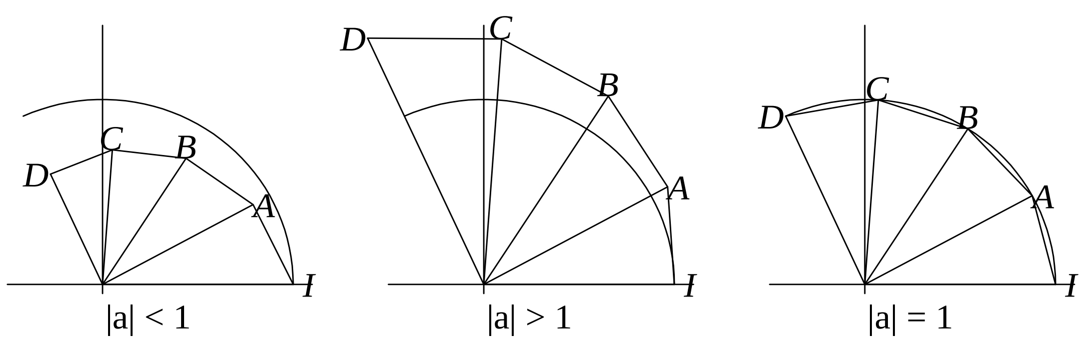
angle(1-0-a)= angle (β-0-$a\beta$),

which indicates that $a\beta$ lies on the line through 0 that passes through β. Also

$$|a\beta| = |a|\ |\beta| = a|\beta|$$

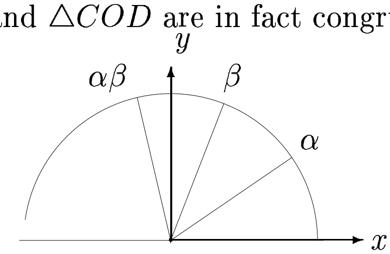
so the length of $a\beta$ is obtained by multiplying the length of β by a.

The figure below shows the powers of a complex number a.



Powers of a: $I = 1$, $A =$ a, $B =$a^2, $C =$ a^3, $D =$ a^4.

In each case the four triangles $\triangle IOA$, $\triangle AOB$, $\triangle BOC$, and $\triangle COD$ are all similar. In the third figure, where a is in the unit circle, the triangles $\triangle IOA, \triangle AOB, \triangle BOC$ and $\triangle COD$ are in fact congruent.



If α, β are points on the unit circle, then

$$\text{angle}(\beta\text{-}0\text{-}\alpha\beta) = \text{angle}(1\text{-}0\text{-}\alpha),$$

which indicates that $\alpha\beta$ is the point in the unit circle such that

$$\text{angle}(1\text{-}0\text{-}\alpha\beta) = \text{angle}(1\text{-}0\text{-}\alpha) + \text{angle}(1\text{-}0\text{-}\beta).$$

From trigonometry, you know that the point on the unit circle making angle θ with the segment OI is $(\cos\theta, \sin\theta) = \cos\theta + i\sin\theta$.

The previous geometrical argument suggests that

$$(\cos\theta + i\sin\theta)(\cos\phi + i\sin\phi) = (\cos(\theta+\phi) + i\sin(\theta+\phi)) \,. \tag{6.13}$$

6.14 Exercise. Using standard trigonometric identities, prove (6.13), and show that $(\cos\theta + i\sin\theta)^{-1} = \cos\theta - i\sin\theta$ for all $\theta \in \mathbf{R}$.

6.15 Exercise. Let $\theta \in \mathbf{R}$. Let $n \in \mathbf{N}$. Prove that

$$(\cos\theta + i\sin\theta)^n = \cos(n\theta) + i\sin(n\theta). \tag{6.16}$$

Then show that formula (6.16) is in fact valid for all $n \in \mathbf{Z}$. (Formula (6.16) is called *De Moivre's Formula*.)

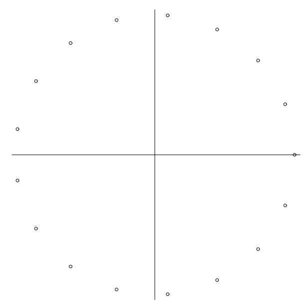
6.3 Roots of Complex Numbers

I expect from (6.16) that every point $(\cos\theta, \sin\theta)$ in the unit circle has nth roots for all $n \in \mathbf{Z}_{\geq 1}$, and that in fact

$$\left(\cos\left(\frac{\theta}{n}\right) + i\sin\left(\frac{\theta}{n}\right)\right)^n = \cos\theta + i\sin\theta.$$

In particular, each vertex of the regular n-gon inscribed in the unit circle and having a vertex at 1 will be an nth root of 1.

6.17 Exercise. The figure below shows the seventeen points
$\left\{\left(\cos\frac{2\pi j}{17}+i\sin\frac{2\pi j}{17}\right):0\leq j<17\right\}$.



Let $w=\left(\cos\frac{4\pi}{17}+i\sin\frac{4\pi}{17}\right)$ and $u=\left(\cos\frac{10\pi}{17}+i\sin\frac{10\pi}{17}\right)$. Draw the polygons 1-$w$-$w^2$-$\cdots$-$w^{17}$ and 1-u-u^2-$\cdots$-u^{17} on different sets of axes, (i.e. draw segments connecting 1 to w, w to w^2, $\cdots$, w^{16} to w^{17}, and segnents joining 1 to u, $\cdots$, u^{16} to u^{17}.)

6.18 Exercise. The sixth roots of 1 are the vertices of a regular hexagon having one vertex at 1. Find these numbers (by geometry or trigonometry) in terms of rational numbers or square roots of rational numbers, and verify by direct calculation that all of them do, in fact, have sixth power equal to 1.

6.19 Theorem (Polar decomposition.) *Let $z\in\mathbf{C}\backslash\{0\}$. Then we can write $z=ru$ where $r\in\mathbf{R}^+$ and $u\in C(0,1)$. In fact this representation is unique, and*

$$r=|z|,\qquad u=\frac{z}{|z|}.$$

I will call the representation

$$z=ru \textit{ where } r\in\mathbf{R}^+,\ u\in C(0,1)$$

the polar decomposition *of z, and I'll call r the* length of z*, and I'll call u the* direction of z*.*

Proof: If $z=ru$ where $r\in\mathbf{R}^+$ and $|u|=1$, then we have

$$|z|=|ru|=|r|\;|u|=r\cdot 1=r.$$

This shows that $r = |z|$, and it then follows that $u = \frac{z}{r} = \frac{z}{|z|}$. Since $\left|\frac{z}{|z|}\right| = \frac{|z|}{||z||} = 1$, we see $\frac{z}{|z|} \in C(0,1)$ and $z = |z|\left(\frac{z}{|z|}\right)$ gives the desired decomposition. ‖

6.20 Notation (Direction.) I will refer to any number in $C(0,1)$ as a *direction.*

6.21 Example. The polar decomposition for $-1+i$ is

$$\begin{aligned}(-1+i) &= |-1+i|\left(\frac{-1+i}{|-1+i|}\right)\\ &= \sqrt{2}\left(-\frac{1}{\sqrt{2}}+\frac{i}{\sqrt{2}}\right).\end{aligned}$$

I recognize from trigonometry that $\left(-\frac{1}{\sqrt{2}}+\frac{i}{\sqrt{2}}\right) = \left(\cos\frac{3\pi}{4} + i\sin\frac{3\pi}{4}\right)$.

6.22 Remark. Let $z, w \in \mathbf{C}\backslash\{0\}$. Let $z = ru$ and $w = sv$ be the polar decompositions of z, w, respectively, so $r, s \in \mathbf{R}^+; u, v \in C(0,1)$. Then $zw = rusv = (rs)(uv)$ where $rs \in \mathbf{R}^+$ and $uv \in C(0,1)$. Hence we have

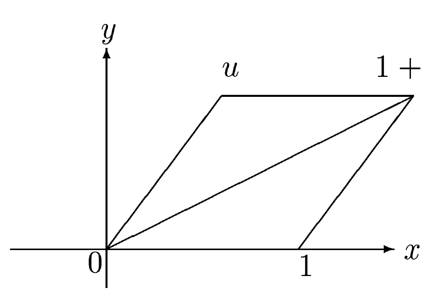
length of product = product of lengths

and

direction of product = product of directions.

6.4 Square Roots

Let u be a direction in $C(0,1)$, with $u \neq -1$. Then we know that $1, 0, u, 1+u$ are the vertices of a parallelogram.



Since $|u| = |1| = 1$, all four sides of the parallelogram are equal, and thus the parallelogram is a rhombus. Since the diagonals of a rhombus bisect its angles, the segment from 0 to $1+u$ bisects angle (1-0-u). Hence I expect that the direction of $1+u$ (i.e., $\dfrac{1+u}{|1+u|}$) is a square root of u. I can prove that this is the case without using any geometry.

6.23 Theorem. *Let u be a direction in $\mathbf{C}$ with $u \neq -1$. Then $\dfrac{1+u}{|1+u|}$ is a square root of u.*

Proof: I just need to square $\dfrac{1+u}{|1+u|}$. Well,

$$\left(\frac{1+u}{|1+u|}\right)^2 = \frac{(1+u)^2}{|1+u|^2} = \frac{(1+u)^2}{(1+u)(1+u)^*} = \frac{1+u}{1+u^*}.$$

Now since u is a direction, we know that $uu^* = 1$, and hence

$$\frac{1+u}{1+u^*} = \frac{uu^*+u}{1+u^*} = \frac{u(u^*+1)}{(1+u^*)} = u. \ \|$$

6.24 Corollary. *Every complex number has a square root.*

Proof: Let $\alpha \in \mathbf{C}$. If $\alpha = 0$, then clearly α has a square root. If $\alpha \neq 0$, let ru be the polar decomposition for α. If $u \neq -1$, then $\pm r^{\frac{1}{2}}\left(\dfrac{1+u}{|1+u|}\right)$ are square roots of α. If $u = -1$, then $\pm r^{\frac{1}{2}} i$ are square roots of α. $\|$

6.25 Example. We will find the square roots of $21-20i$. Let $\alpha = 21-20i$. Then

$$|\alpha| = \sqrt{21^2+20^2} = \sqrt{441+400} = \sqrt{841} = 29.$$

Hence the polar decomposition for α is

$$\alpha = 29\left(\frac{21-20i}{29}\right) = ru \text{ where } r = 29 \text{ and } u = \frac{21-20i}{29}.$$

The square roots of α are

$$\begin{aligned} \pm r^{\frac{1}{2}}\left(\frac{1+u}{|1+u|}\right) &= \pm\sqrt{29}\left(\frac{1+\frac{21}{29}-\frac{20i}{29}}{|1+\frac{21}{29}-\frac{20i}{29}|}\right) \\ &= \pm\sqrt{29}\left(\frac{50-20i}{|50-20i|}\right) = \pm\sqrt{29}\left(\frac{5-2i}{|5-2i|}\right). \end{aligned}$$

Now $|5-2i| = \sqrt{25+4} = \sqrt{29}$, so the square roots of α are $\pm(5-2i)$.

6.26 Exercise. Find the square roots of $12+5i$. Write your answers in the form $a+bi$, where a and b are real.

Let $a, b \in \mathbf{R}$. There is a formula for the square root of $a+bi$ that allows you to say

$$\text{the square roots of } 2+4i \text{ are } \pm\left(\sqrt{\sqrt{5}+1}+i\sqrt{\sqrt{5}-1}\right) \tag{6.27}$$

and

$$\text{the square roots of } 6-2i \text{ are } \pm\left(\sqrt{\sqrt{10}+3}-i\sqrt{\sqrt{10}-3}\right). \tag{6.28}$$

6.29 Exercise. Verify that assertions (6.27) and (6.28) are correct.

6.30 Entertainment. Find the square root formula, and prove that it is correct. (There are at least three ways to do this. Method c) is probably the easiest.)

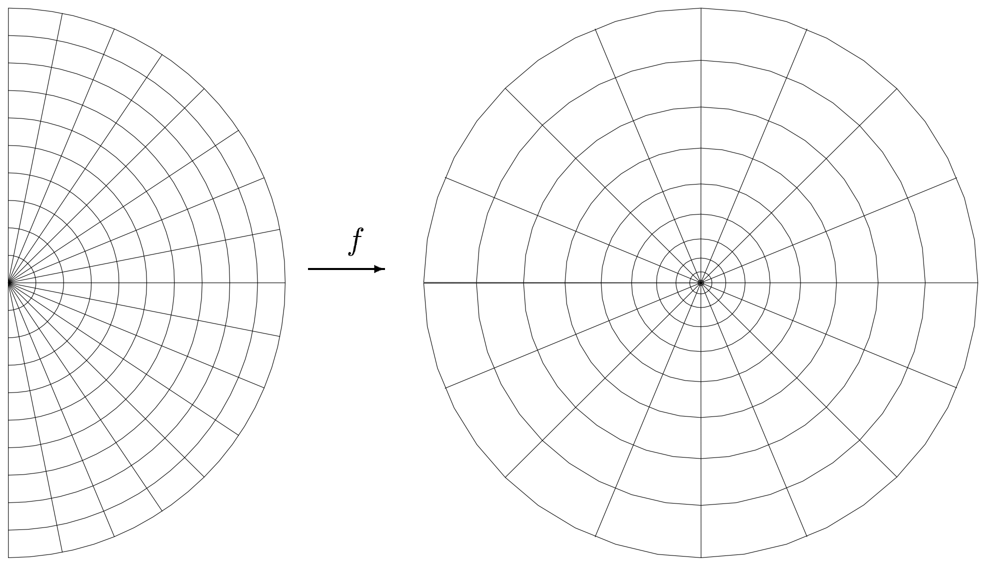
a) Suppose the square root is $c+di$, and equate the real and imaginary parts of $(c+di)^2$ and $a+bi$. Then solve for c and d and show that your solution works.

b) Let ru be the polar decomposition of $a+bi$. You know how to find a square root v for u, and $r^{\frac{1}{2}}v$ will be a square root of $a+bi$. Write this in the form $c+di$.

c) On the basis of (6.27) and (6.28), guess the formula, and show that it works.

6.5 Complex Functions

When one studies a function f from $\mathbf{R}$ to $\mathbf{R}$, one often gets information by looking at the graph of f, which is a subset of $\mathbf{R}\times\mathbf{R}$. If we consider a function $g\colon \mathbf{C}\to\mathbf{C}$, the graph of g is a subset of $\mathbf{C}\times\mathbf{C} = (\mathbf{R}\times\mathbf{R})\times(\mathbf{R}\times\mathbf{R})$, and $\mathbf{C}\times\mathbf{C}$ is a “4-dimensional” object which cannot be visualized. We will now discuss a method to represent functions from $\mathbf{C}$ to $\mathbf{C}$ geometrically.



Geometrical Representation of the Function $f(z) = z^2$.

6.31 Example ($f(z) = z^2$.) Let $f\colon \mathbf{C} \to \mathbf{C}$ be defined by $f(z) = z^2$. If z is a point in the circle $C(0, r)$, then $z = ru$ where u is a direction, and $f(z) = r^2u^2$ is a point in the circle $C(0, r^2)$ with radius r^2. Thus f maps circles of radius r about 0 into circles of radius r^2 about 0. Let u_0 be a direction in $\mathbf{C}$. If z is on the ray from 0 passing through u_0, then $z = ru_0$ for some $r \in \mathbf{R}^+$ so $f(z) = r^2u_0^2$, which is on the ray from 0 passing through u_0^2. Hence the ray making an angle θ with the positive real axis gets mapped by f to the ray making an angle 2θ with the positive x-axis.

The left part of the figure shows a network formed by semicircles of radius

$$r \in \{.1, .2, .3, \cdots, .9, 1\},$$

and rays making angles

$$\theta \in \left\{0, \pm\frac{\pi}{16}, \pm\frac{2\pi}{16}, \cdots, \pm\frac{8\pi}{16}\right\}$$

with the positive x-axis. The right part of the figure shows the network formed by circles of radius

$$r^2 \in \{.1^2, .2^2, \cdots, .9^2, 1\}$$

and rays making angles

$$2\theta \in \left\{0, \pm\frac{\pi}{8}, \pm\frac{2\pi}{8}, \cdots, \pm\frac{8\pi}{8}\right\}$$

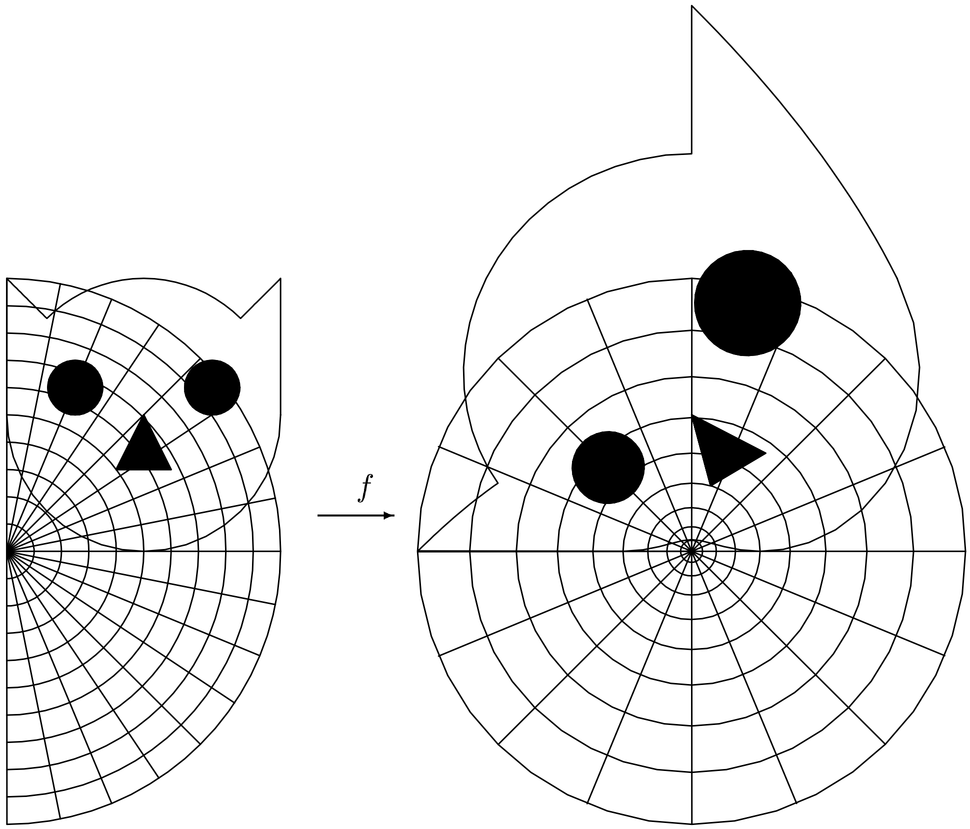
with the positive x-axis. f maps each semicircle in the left part of the figure to a circle in the right part, and f maps each ray in the left part to a ray in the right part. Also f maps each curvilinear rectangle on the left to a curvilinear rectangle on the right. Notice that $f(i) = f(-i)$, and in general $f(z) = f(-z)$, so if we know how f maps points in the right half plane, we know how it maps points in the left half plane. The function f maps the right half plane $\{x > 0\}$ onto $\mathbf{C} \setminus \big((\text{ negative real axis }) \cup \{0\}\big)$.

6.32 Definition (Image of a function.) Let S, T be sets, let $f: S \to T$, and let A be a subset of $\text{dom}(f)$. We define

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

and we call $f(A)$ the *image of A under f*. We call $f(\text{dom}(f))$ the *image of f*.

6.33 Example ($f(z) = z^2$, continued) In the figure on page 118, the right half of the figure is the image of the left half under the function f. The figure on page 120, shows the image of a cat-shaped set under f. The cat on the left lies in the first quadrant, so its square lies in the first two quadrants. The tip of the right ear is $1 + i = \sqrt{2}\left(\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\right)$, with length $\sqrt{2}$, and with direction making an angle $\frac{\pi}{4}$ with the positive real axis. The image of the right ear has length $(\sqrt{2})^2 = 2$ and makes an angle $\frac{\pi}{2}$ with the positive x-axis. You should examine how the parts of the cat in each curvilinear rectangle on the left part of the figure correspond to their images on the right part.



The Square of a Cat

6.34 Exercise. Let C be the cat shown in the left part of the above figure. Sketch the image of C under each of the functions g, h, k below:

a) $g(z) = 2z$.

b) $h(z) = iz$.

c) $k(z) = 2iz$.

6.35 Exercise. Let C be the cat shown in the left part of the above figure. Sketch the image of C under G, where $G(z) = -z^2$.

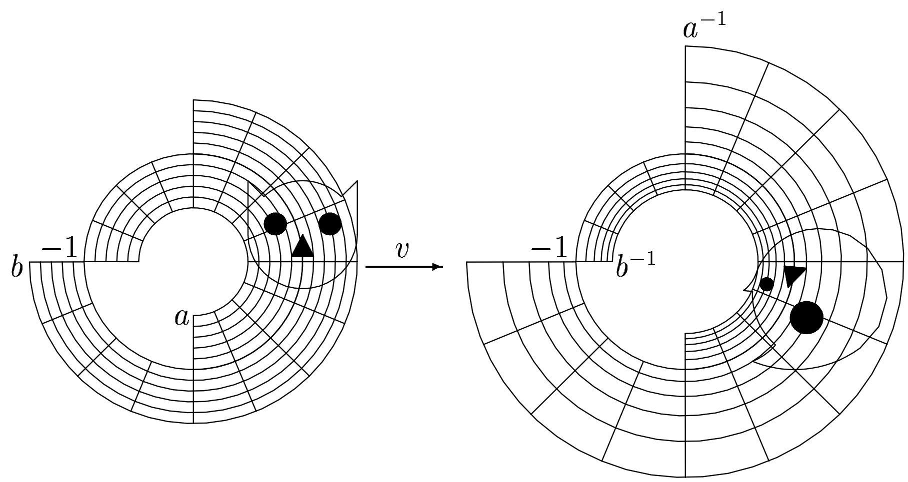
6.36 Exercise. Let z be a direction in $\mathbf{C}$; i.e., let $z \in C(0,1)$. Show that $z^* = z^{-1}$.

6.37 Example. Let $v(z) = \frac{1}{z}$ for all $z \in \mathbf{C}\backslash\{0\}$. If z is in the circle of radius r, then $z = ru$ for some direction u, and $|v(z)| = \left|\frac{1}{ru}\right| = \frac{1}{|r|\ |u|} = \frac{1}{|r|}$, so v takes points in the circle of radius r about 0 to points in the circle of radius $\frac{1}{r}$ about 0.

Let u_0 be a direction. If z is in the ray from 0 through u_0, then $z = ru_0$ for some $r \in \mathbf{R}^+$, so $v(z) = \frac{1}{r}u_0^{-1} = \frac{1}{r}u_0^*$. We noted earlier that u_0^* is the reflection of u_0 about the real axis, so v maps the ray making angle θ with the positive real axis into the ray making angle $-\theta$ with the positive real axis. Thus v maps the network of circles and lines in the left half of the figure into the network on the right half.

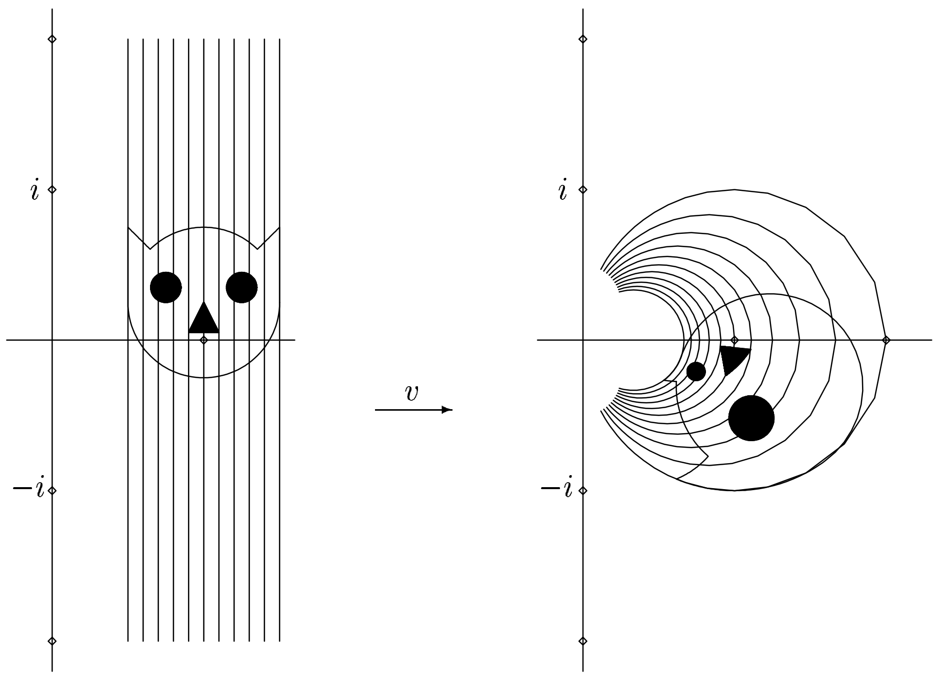
The circular arcs in the left half of the figure have radii

$$r \in \{.5, .6, .7, \cdots, 1.4, 1.5\}.$$



The Inverse of a Cat

Let's see how v maps the vertical line $x = a$ $(a \neq 0)$, $a \in \mathbf{R}$. We know that $v(a) = \frac{1}{a}$ and v maps points in the upper half plane to points in the lower half plane. Points far from the origin get mapped to points near to the origin. I claim that v maps the line $x = a$ into the circle with center $\frac{1}{2a}$ and radius $\frac{1}{2|a|}$.



v maps vertical lines to circles

Let $L_a = \{z\colon \mathrm{Re}(z) = a\} = \{a + iy\colon y \in \mathbf{R}\}$, so L_a is the set of points in the line $x = a$. Then

$$\begin{aligned} z \in L_a &\iff z = a + iy \text{ for some } y \in \mathbf{R} \\ &\implies \frac{1}{z} - \frac{1}{2a} = \frac{2a - z}{2az} = \frac{2a - (a + iy)}{2a(a + iy)} = \frac{a - iy}{2a(a + iy)} \\ &\implies \left|\frac{1}{z} - \frac{1}{2a}\right| = \left|\frac{1}{2a} \cdot \frac{a - iy}{a + iy}\right| = \frac{1}{|2a|}\frac{|a - iy|}{|a + iy|} = \frac{1}{|2a|}, \end{aligned}$$

since $|w| = |w^*|$ for all $w \in \mathbf{C}$. Hence,

$$z \in L_a \implies \left|\frac{1}{z} - \frac{1}{2a}\right| = \frac{1}{|2a|} \implies \frac{1}{z} \in C\left(\frac{1}{2a}, \frac{1}{|2a|}\right),$$

and v maps every point in L_a into $C\left(\frac{1}{2a}, \frac{1}{|2a|}\right)$. Now I claim that every point in $C\left(\frac{1}{2a}, \frac{1}{|2a|}\right)$ (except for 0) is equal to $v(z)$ for some $z \in L_a$.

Since $w = v\,(v(w))$, it will be sufficient to show that if $w \in C\left(\frac{1}{2a}, \frac{1}{|2a|}\right)\backslash\{0\}$, then $v(w) \in L_a$. I want to show

$$\left(\left|w - \frac{1}{2a}\right| = \frac{1}{|2a|} \text{ and } w \neq 0\right) \implies \frac{1}{w} = a + iy \text{ for some } y \in \mathbf{R}.$$

Well, suppose $\left|w - \frac{1}{2a}\right| = \frac{1}{|2a|}$, and let $\frac{1}{w} = A + iB$ where $A, B \in \mathbf{R}$. Then $w = \frac{1}{A+iB} = \frac{A-iB}{A^2+B^2}$, so

$$\begin{aligned}
\left|w - \frac{1}{2a}\right| = \frac{1}{|2a|} &\implies \left|w - \frac{1}{2a}\right|^2 = \frac{1}{4a^2} \\
&\implies \left|\frac{A-iB}{A^2+B^2} - \frac{1}{2a}\right|^2 = \frac{1}{4a^2} \\
&\implies \left|\left(\frac{A}{A^2+B^2} - \frac{1}{2a}\right) - \frac{iB}{A^2+B^2}\right|^2 = \frac{1}{4a^2} \\
&\implies \frac{A^2}{(A^2+B^2)^2} - \frac{A}{a(A^2+B^2)} + \frac{1}{4a^2} + \frac{B^2}{(A^2+B^2)^2} = \frac{1}{4a^2} \\
&\implies \frac{A^2+B^2}{(A^2+B^2)^2} = \frac{A}{a(A^2+B^2)} \\
&\implies A = a,
\end{aligned}$$

so (by definition of A)

$$\left|w - \frac{1}{2a}\right| = \frac{1}{2a} \implies \frac{1}{w} = a + iB \text{ where } B \in \mathbf{R}. \; \|$$

6.38 Exercise. The argument above does not apply to the vertical line $x = 0$. Let $L_0 = \{iy \colon y \in \mathbf{R}\}$. Where does the reciprocal function v map $L_0\backslash\{0\}$?

6.39 Entertainment. Let $v(z) = \frac{1}{z}$ for all $z \in \mathbf{C}\backslash\{0\}$. Show that v maps horizontal lines $y = c$ ($c \neq 0$) into circles that pass through the origin. Sketch the images of the lines

$$x = j, \text{ where } j \in \{0, \pm 1, \pm 2, \pm 3\}$$

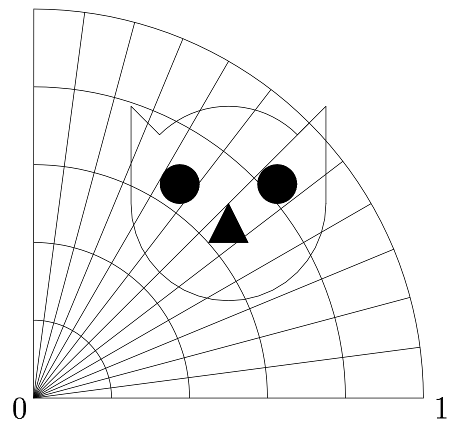
and the lines

$$y = j, \text{ where } j \in \{0, \pm 1, \pm 2, \pm 3\}$$

on one set of axes using a compass. If you've done this correctly, the circles should intersect at right angles.

6.40 Exercise.

a) Sketch the image of the network of lines and circular arcs shown below under the function g, where $g(z) = z^3$ for all $z \in \mathbf{C}$.



b) Cube the cat in the picture.

6.41 Note. De Moivre's formula $(\cos(\theta) + i \sin\theta)^n = \cos(n\theta) + i \sin(n\theta)$, was first stated in this form by Euler in 1749 ([46, pp. 452-454]). Euler named the formula after Abraham De Moivre (1667-1754) who never explicitly stated the formula, but used its consequences several times ([46, pp. 440-450]).

The method for finding mth roots of complex numbers:

$$[r(\cos\theta + i\sin\theta)]^{\frac{1}{m}} = r^{\frac{1}{m}}\left[\cos\frac{\theta}{m} + i\sin\frac{\theta}{m}\right]$$

was introduced by Euler in 1749 [46, pp.452-454].

The idea of illustrating functions from the plane to the plane by distorting cat faces is due to Vladimir Arnold (1937-??), and the figures are sometimes called "Arnold Cats". Usually Arnold cats have black faces and white eyes and noses, as in [3, pp.6-9].

Chapter 7

Complex Sequences

In definition 5.1, we defined a sequence in $\mathbf{C}$ to be a function $f: \mathbf{N} \to \mathbf{C}$. Since we are identifying $\mathbf{R}$ with a subset of $\mathbf{C}$, every sequence in $\mathbf{R}$ is also a sequence in $\mathbf{C}$, and all of our results for complex sequences are applicable to real sequences.

7.1 Some Examples.

7.1 Notation ($\mapsto$) I will say "consider the sequence $n \mapsto 2^n$" or "consider the sequence $f: n \mapsto 2^n$" to mean "consider the sequence $f: \mathbf{N} \to \mathbf{C}$ such that $f(n) = 2^n$ for all $n \in \mathbf{N}$". The arrow $\mapsto$ is read "maps to".

7.2 Definition (Geometric sequence.) For each $\alpha \in \mathbf{C}$, the sequence

$$n \mapsto \alpha^n$$

is called the *geometric sequence with ratio* α.

I will often represent a sequence f in $\mathbf{C}$ by a polygonal line with vertices $f(0), f(1), f(2), \cdots$. The two figures below represent geometric sequences with ratios $\dfrac{1+i}{2}$ and $\dfrac{2+i}{3}$ respectively.

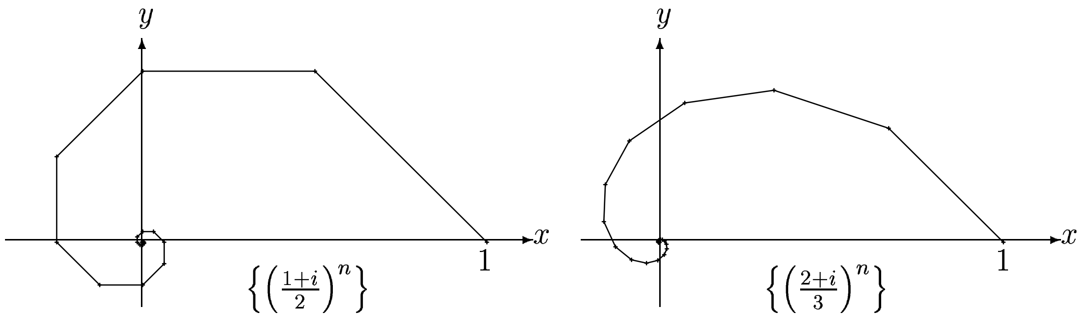


Figure a. Geometric Sequences

7.3 Definition (Geometric series.) If $\alpha \in \mathbf{C}$, then the sequence $g_\alpha : n \mapsto \sum_{j=0}^{n} \alpha^j$ is called the *geometric series with ratio* α.

$$g_\alpha = \{1, 1+\alpha, 1+\alpha+\alpha^2, 1+\alpha+\alpha^2+\alpha^3, \cdots\}$$

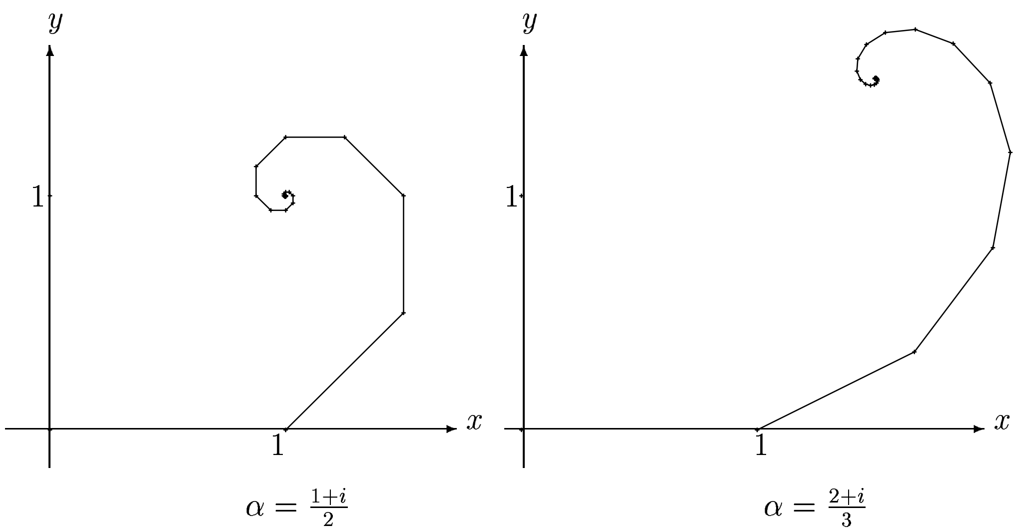


Figure b. Geometric Series $\left\{\sum_{j=0}^{n} \alpha^j\right\}$

Figure b shows the geometric series corresponding to the geometric sequences in figure a. If you examine the figures you should notice a remarkable similarity between the figure representing $\{\alpha^n\}$ and the figure representing $\{\sum_{j=0}^{n} \alpha^j\}$.

7.4 Entertainment. Describe the apparent similarity between the figure for $\{\alpha^n\}$ and the figure for $\{\sum_{j=0}^{n} \alpha^j\}$. Then prove that this similarity is really present for all $\alpha \in \mathbf{C}\backslash\{1\}$.

7.5 Definition (Constant sequence.) For each $\alpha \in \mathbf{C}$, let $\tilde{\alpha}$ denote the constant sequence $\tilde{\alpha}: n \mapsto \alpha$; i.e., $\tilde{\alpha} = \{\alpha, \alpha, \alpha, \alpha, \cdots\}$.

7.2 Convergence

7.6 Definition (Convergent sequence.) Let f be a complex sequence, and let $L \in \mathbf{C}$. We will say f *converges to* L and write $f \to L$ if for every disc $D(L, r)$ there is a number $N \in \mathbf{N}$ such that

$$\text{for every } n \in \mathbf{Z}_{\geq N}, \quad (f(n) \in D(L, r)).$$

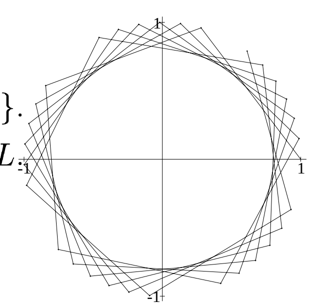
We say f *converges* if there is some $L \in \mathbf{C}$ such that $f \to L$. We say f *diverges* if and only if f does not converge.

It appears from figure a on page 126 that for every disc $D(0, r)$ centered at 0 the terms of the sequence $\left\{\left(\frac{1+i}{2}\right)^n\right\}$ eventually get into $D(0, r)$; i.e., it appears that $\left\{\left(\frac{1+i}{2}\right)^n\right\} \to 0$. Similarly, it appears that $\left\{\left(\frac{1+2i}{3}\right)^n\right\} \to 0$.

From figure b, it appears that there are numbers P, Q such that $\left\{\sum_{j=0}^{n}\left(\frac{1+i}{2}\right)^j\right\} \to P$, and $\left\{\sum_{j=0}^{n}\left(\frac{1+2i}{3}\right)^j\right\} \to Q$. You should be able to put your finger on P and Q, and maybe to guess what their exact values are. We will return to these examples later.

Let $w = \frac{7+24i}{25}$. The figure in the margin represents the sequence $\{w^n\}$. It appears from the figure that there is no number L such that $\{w^n\} \mapsto L$. The following theorem shows that this is the case.

(Note that $\left|\frac{7+24i}{25}\right| = \sqrt{\frac{49+576}{625}} = 1$.)



$\left\{\left(\frac{7+24i}{25}\right)^n\right\}$

7.7 Theorem. *Let $w \in \mathbf{C}$ satisfy $|w| \geq 1$ and $w \neq 1$. Then $\{w^n\}$ diverges.*

Proof: Suppose that $|w| \geq 1$ and $w \neq 1$. Then for all $n \in \mathbf{N}$,

$$|w^n - w^{n+1}| = |w^n(1-w)| = |w|^n|1-w| \geq |1-w| > 0. \tag{7.8}$$

Now suppose, to get a contradiction, that there is a number $L \in \mathbf{C}$ such that $\{w^n\} \to L$. Then corresponding to the disc $D\left(L, \dfrac{|1-w|}{2}\right)$, there is a number $N \in \mathbf{N}$ such that

$$n \in \mathbf{Z}_{\geq N} \implies w^n \in D\left(L, \frac{|1-w|}{2}\right).$$

In particular,

$$w^N \in D\left(L, \frac{|1-w|}{2}\right) \text{ and } w^{N+1} \in D\left(L, \frac{|1-w|}{2}\right)$$

so

$$|w^N - L| < \frac{|1-w|}{2} \text{ and } |w^{N+1} - L| < \frac{|1-w|}{2}.$$

By the triangle inequality,

$$\begin{aligned} |w^N - w^{N+1}| &= |(w^N - L) + (L - w^{N+1})| \\ &\leq |w^N - L| + |L - w^{N+1}| \\ &< \frac{|1-w|}{2} + \frac{|1-w|}{2} = |1-w|. \end{aligned}$$

Combining this result with (7.8), we get

$$|1-w| \leq |w^N - w^{N+1}| < |1-w|,$$

so $|1-w| < |1-w|$. This contradiction shows that $\{w^n\}$ diverges. ‖

We can also show that constant sequences converge.

7.9 Theorem. *Let $\alpha \in \mathbf{C}$. Then the constant sequence $\tilde{\alpha}$ converges to α.*

Proof: Let $\alpha \in \mathbf{C}$. Let $D(\alpha, r)$ be a disc centered at α. Then

$$\tilde{\alpha}(n) = \alpha \in D(\alpha, r) \text{ for all } n \in \mathbf{Z}_{\geq 0},$$

Hence, $\tilde{\alpha} \to \alpha$. ‖

For purposes of calculation it is sometimes useful to rephrase the definition of convergence. Since the disc $D(\alpha, r)$ is determined by its radius r, and for all $z \in \mathbf{C}$, $z \in D(\alpha, r) \iff |z - \alpha| < r$, we can reformulate definition 7.6 as

7.10 Definition (Convergence.) Let f be a sequence in $\mathbf{C}$, and let $L \in \mathbf{C}$. Then $f \to L$ if and only if for every $r \in \mathbf{R}^+$ there is some $N \in \mathbf{N}$ such that

$$\text{for every } n \in \mathbf{Z}_{\geq N}, \quad (|f(n) - L| < r).$$

7.3 Null Sequences

Sequences that converge to 0 are simpler to work with than general sequences, and many of the convergence theorems for general sequences can be easily deduced from the properties of sequences that converge to 0. In this section we will just consider sequences that converge to 0.

7.11 Definition (Null sequence.) Let f be a sequence in $\mathbf{C}$. We will say f is a *null sequence* if and only if for every $\varepsilon \in \mathbf{R}^+$ there is some $N \in \mathbf{N}$ such that for every $n \in \mathbf{Z}_{\geq N}$, $(|f(n)| < \varepsilon)$.

By comparing this definition with definition 7.10, you see that

$$(f \text{ is a null sequence }) \iff (f \to 0).$$

Definition 7.11 is important. You should memorize it.

7.12 Definition (Dull sequence.) Let f be a sequence in $\mathbf{C}$. We say f is a *dull sequence* if and only if there is some $N \in \mathbf{N}$ such that for every ε in $\mathbf{R}^+$, and for every $n \in \mathbf{Z}_{\geq N}$ $(|f(n)| < \varepsilon)$.

The definitions of null sequence and dull sequence use the same words, but they are not in the same order, and the definitions are not equivalent.

If f satisfies condition (7.12), then whenever $n \geq N$,

$$\text{for every } \varepsilon \text{ in } \mathbf{R}^+ \quad (|f(n)| < \varepsilon)\,.$$

If $|f(n)| \in \mathbf{R}^+$, this condition would say $|f(n)| < |f(n)|$, which is false. Hence if $n \geq N$, then $|f(n)| \notin \mathbf{R}^+$; i.e., if $n \geq N$, then $f(n) = 0$. Hence a dull sequence has the property that there is some $N \in \mathbf{N}$ such that $f(n) = 0$ for all $n \geq N$. Thus every dull sequence is a null sequence. The sequence

$$\left\{1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, 0, 0, 0, 0, 0, \cdots\right\}$$

is a dull sequence, but

$$\left\{\frac{1}{n}\right\}_{n\geq 1} = \left\{1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{5}, \frac{1}{6}, \frac{1}{7}, \cdots\right\}$$

is not a dull sequence. In the next theorem we show that $\{\frac{1}{n}\}_{n\geq 1}$ is a null sequence, so null sequences are not necessarily dull.

7.13 Theorem. *For all $a \in \mathbf{C}$, $\left\{\frac{a}{n}\right\}_{n\geq 1}$ is a null sequence .*

Proof: Let $\varepsilon \in \mathbf{R}^+$. By the Archimedean property for $\mathbf{R}$, there is an $N \in \mathbf{Z}^+$ such that $N > \frac{|a|}{\varepsilon}$. Then for all $n \in \mathbf{Z}^+$,

$$n \geq N \implies n > \frac{|a|}{\varepsilon} \implies \frac{|a|}{n} < \varepsilon,$$

so for all $n \in \mathbf{Z}_{\geq N}$ $\left(\left|\frac{a}{n}\right| < \varepsilon\right)$. ‖

The difference between a null sequence and a dull sequence is that the "N" in the definition of null sequence can (and usually does) depend on ε, while the "N" in the definition of dull sequence depends only on f. To emphasize that N depends on ε (and also on f), I will often write $N(\varepsilon)$ or $N_f(\varepsilon)$ instead of N.

Here is another reformulation of the definition of null sequence.

7.14 Definition (Precision function.) Let f be a complex sequence. Then f is a null sequence if and only if there is a function $N_f\colon \mathbf{R}^+ \to \mathbf{N}$ such that

$$\text{for all } \varepsilon > 0 \text{ and all } n \in \mathbf{N};\ (n \geq N_f(\varepsilon) \implies |f(n)| < \varepsilon).$$

I will call such a function N_f a *precision function for f*.

This formulation shows that in order to show that a sequence f is a null sequence, you need to find a *function* $N_f\colon \mathbf{R}^+ \to \mathbf{N}$ such that

$$\text{for all } n \in \mathbf{N}\ (n \geq N_f(\varepsilon) \implies |f(n)| < \varepsilon).$$

In the proof of theorem 7.13, for the sequence $g\colon n \mapsto \dfrac{a}{n}$ we had

$$N_g(\varepsilon) = \left(\text{some integer } N \text{ such that } \frac{|a|}{N} < \varepsilon\right).$$

This description for N_g could be made more precise, but it is good enough for our purposes.

7.15 Theorem. *If $\alpha \in \mathbf{C}\backslash\{0\}$, then the constant sequence $\tilde{\alpha}$ is not a null sequence.*

Proof: If $\alpha \neq 0$, then $\frac{1}{2}|\alpha| \in \mathbf{R}^+$. Suppose, to get a contradiction, that $\tilde{\alpha}$ is a null sequence. Then there is a number $N \in \mathbf{N}$ such that for all $n \in \mathbf{N}$ $\left(n \geq N \implies |\tilde{\alpha}(n)| < \frac{1}{2}|\alpha|\right)$. Then for all $n \in \mathbf{N}$,

$$\left(n \geq N \implies |\alpha| < \frac{1}{2}|\alpha| \implies 1 < \frac{1}{2}\right). \tag{7.16}$$

If $n = N+1$ then (7.16) is false and this shows that $\tilde{\alpha}$ is not a null sequence. ‖

7.17 Theorem (Comparison theorem for null sequences.) *Let f, g be complex sequences. Suppose that f is a null sequence and that*

$$|g(n)| \leq |f(n)| \text{ for all } n \in \mathbf{N}.$$

Then g is a null sequence.

Proof: Since f is a null sequence, there is a function $N_f\colon \mathbf{R}^+ \to \mathbf{N}$ such that for all $n \in \mathbf{N}$,

$$n \geq N_f(\varepsilon) \implies |f(n)| < \varepsilon.$$

Then

$$n \geq N_f(\varepsilon) \implies |g(n)| \leq |f(n)| < \varepsilon \implies |g(n)| < \varepsilon.$$

Hence, we can let $N_g = N_f$. ‖

7.18 Example. We know that $n \leq 2^n$ for all $n \in \mathbf{N}$, so $\dfrac{1}{2^n} \leq \dfrac{1}{n}$ for all $n \in \mathbf{Z}_{\geq 1}$. Since $\left\{\dfrac{1}{n}\right\}_{n\geq 1}$ is a null sequence, it follows from the comparison theorem that $\left\{\dfrac{1}{2^n}\right\}_{n\geq 1}$ is a null sequence. Also, since $\dfrac{1}{n^2+n} \leq \dfrac{1}{n}$ for all $n \in \mathbf{Z}_{\geq 1}$, we see that $\left\{\dfrac{1}{n^2+n}\right\}_{n\geq 1}$ is a null sequence.

7.19 Theorem (Root theorem for null sequences.)
Let $f: \mathbf{N} \to [0, \infty)$ be a null sequence, and let $p \in \mathbf{Z}_{\geq 1}$. Then $f^{\frac{1}{p}}$ is a null sequence where $f^{\frac{1}{p}}(n) = (f(n))^{\frac{1}{p}}$ for all $n \in \mathbf{N}$.

Scratchwork: Let $g = f^{\frac{1}{p}}$. I want to find N_g so that for all $n \in \mathbf{N}$ and all $\varepsilon \in \mathbf{R}^+$,

$$n \geq N_g(\varepsilon) \implies |g(n)| \leq \varepsilon$$

i.e.

$$n \geq N_g(\varepsilon) \implies \left|f^{\frac{1}{p}}(n)\right| \leq \varepsilon$$

i.e.

$$n \geq N_g(\varepsilon) \implies f(n) \leq \varepsilon^p.$$

This suggests that I should take $N_g(\varepsilon) = N_f(\varepsilon^p)$.

Proof: Let f be a null sequence in $[0, \infty)$ and let N_f be a precision function for f. Define $N_g: \mathbf{R}^+ \to \mathbf{N}$ by $N_g(\varepsilon) = N_f(\varepsilon^p)$ for all $\varepsilon \in \mathbf{R}^+$. Then for all $n \in \mathbf{N}$,

$$\begin{aligned} n \geq N_g(\varepsilon) &\implies n \geq N_f(\varepsilon^p) \\ &\implies |f(n)| < \varepsilon^p \\ &\implies 0 \leq f(n) < \varepsilon^p \\ &\implies f(n)^{1/p} < \varepsilon \\ &\implies g(n) < \varepsilon. \end{aligned}$$

Hence N_g is a precision function for g. |||

7.20 Examples. Let $c \in \mathbf{R}^+$. Then $\left\{\dfrac{c^2}{n}\right\}_{n\geq 1}$ is a null sequence in $[0, \infty)$, so it follows that $\left\{\dfrac{c}{\sqrt{n}}\right\}_{n\geq 1}$ is a null sequence.

Consider the sequence $f: \mathbf{Z}_{\geq 1} \to \mathbf{C}$, $f : n \mapsto n + \dfrac{1}{2} - \sqrt{n^2 + n}$. For all $n \in \mathbf{Z}_{\geq 1}$,

$$\begin{aligned} f(n) &= \left(\left(n + \frac{1}{2}\right) - \sqrt{n^2 + n}\right) \frac{\left(\left(n + \frac{1}{2}\right) + \sqrt{n^2 + n}\right)}{\left(\left(n + \frac{1}{2}\right) + \sqrt{n^2 + n}\right)} \\ &= \frac{\left(n^2 + n + \frac{1}{4}\right) - (n^2 + n)}{n + \frac{1}{2} + \sqrt{n^2 + n}} = \frac{1}{4\left(n + \frac{1}{2} + \sqrt{n^2 + n}\right)}. \end{aligned}$$

Hence $|f(n)| \leq \frac{1}{4n} \leq \frac{1}{n}$, so it follows from the comparison theorem that f is a null sequence.

Since $\left\{\frac{1}{2^n}\right\}_{n\geq 1}$ is a null sequence, it follows from the root theorem that $\left\{\left(\frac{1}{\sqrt{2}}\right)^n\right\}_{n\geq 1}$ is a null sequence. Now $.7^2 = .49 < \frac{1}{2}$, so $.7 < \sqrt{\frac{1}{2}} = \frac{1}{\sqrt{2}}$ so $(.7)^n \leq \left(\frac{1}{\sqrt{2}}\right)^n$ for all $n \in \mathbf{Z}_{\geq 1}$, and by another comparison test, $\{.7^n\}$ is a null sequence. Since $\Big((|\alpha| \leq .7) \implies (|\alpha^n| \leq .7^n)\Big)$, it follows that $\{\alpha^n\}_{n\geq 1}$ is a null sequence for all $\alpha \in \mathbf{C}$ with $|\alpha| \leq .7$.

You probably suspect that $\{\alpha^n\}$ is a null sequence for all $\alpha \in \mathbf{C}$ with $|\alpha| < 1$. This is correct, but we will not prove it yet.

7.21 Exercise. Show that the geometric sequences $\left\{\left(\frac{1+i}{2}\right)^n\right\}$ and $\left\{\left(\frac{2+i}{3}\right)^n\right\}$ that are sketched on page 126 are in fact null sequences.

7.22 Exercise. Which, if any, of the sequences below are null sequences? Justify your answers.

a) $\{\sqrt{n+10000} - \sqrt{n}\}_{n\geq 1}$

b) $\left\{\frac{n^2+1}{n^3+3n}\right\}_{n\geq 1}$

c) $\left\{\frac{n^2+6}{n^3+3n}\right\}_{n\geq 1}$

7.23 Entertainment. Show that

$$\{(1-10^{-20})^n\} = \{.99999999999999999999^n\}$$

is a null sequence. (If you succeed, you will probably find a proof that $\{\alpha^n\}$ is a null sequence whenever $|\alpha| < 1$.) NOTE: If you use calculator operations, then $\{(1-10^{-20})^n\}$ is not a null sequence on most calculators.

It follows from remark 5.38 that we can add, subtract and multiply complex sequences, and that the usual associative, commutative, and distributive laws hold. If $f = \{f(n)\}$ and $g = \{g(n)\}$ then $f + g = \{f(n) + g(n)\}$ and $(fg)(n) = \{f(n) \cdot g(n)\}$. If $\alpha, \beta \in \mathbf{C}$ then the constant sequences $\tilde{\alpha}, \tilde{\beta}$ satisfy

$$\widetilde{\alpha + \beta} = \tilde{\alpha} + \tilde{\beta}, \quad \widetilde{\alpha\beta} = \tilde{\alpha}\tilde{\beta}.$$

7.24 Exercise. Which of the field axioms are satisfied by addition and multiplication of sequences? Does the set of complex sequences form a field? (You know that the associative, distributive and commutative laws hold, so you just need to consider the remaining axioms.

7.25 Notation. If f is a complex sequence, we define sequences f^*, $\text{Re}f$, $\text{Im}f$, and $|f|$ by

$$\begin{aligned} f^*(n) &= (f(n))^* \text{ for all } n \in \mathbf{N}, \\ (\text{Re}f)(n) &= \text{Re}\,(f(n)) \text{ for all } n \in \mathbf{N}, \\ (\text{Im}f)(n) &= \text{Im}\,(f(n)) \text{ for all } n \in \mathbf{N}, \\ |f|(n) &= |f(n)| \text{ for all } n \in \mathbf{N}. \end{aligned}$$

7.26 Theorem. *Let f be a complex null sequence. Then f^*, $\text{Re}f$, $\text{Im}f$ and $|f|$ are all null sequences.*

Proof: All four results follow by the comparison theorem. We have, for all $n \in \mathbf{N}$:

$$\begin{aligned} |f^*(n)| &= |(f(n))^*| = |f(n)|, \\ |(\text{Re}f)(n)| &= |\text{Re}(f(n))| \le |f(n)|, \\ |(\text{Im}f)(n)| &= |\text{Im}(f(n))| \le |f(n)|, \\ ||f|(n)| &= |f(n)|. \ \| \end{aligned}$$

7.4 Sums and Products of Null Sequences

7.27 Theorem (Sum theorem for null sequences.) *Let f, g be complex null sequences and let $\alpha \in \mathbf{C}$. Then $f + g$, $f - g$, and αf are null sequences.*

Scratchwork for αf: I want to find $N_{\alpha f}$ so that

$$n \geq N_{\alpha f}(\varepsilon) \implies |\alpha f(n)| < \varepsilon$$

i.e.

$$n \geq N_{\alpha f}(\varepsilon) \implies |f(n)| < \frac{\varepsilon}{|\alpha|}.$$

This suggests that I take $N_{\alpha f}(\varepsilon) = N_f\left(\frac{\varepsilon}{|\alpha|}\right)$.

Scratchwork for $f+g$: I want to find N_{f+g} so that

$$n \geq N_{f+g}(\varepsilon) \implies |f(n)+g(n)| < \varepsilon.$$

Now $|f(n)+g(n)| \leq |f(n)| + |g(n)|$, and I can make $|f(n)| + |g(n)| < \varepsilon$ by making $|f(n)| < \varepsilon/2$ and $|g(n)| < \varepsilon/2$. Hence I want $N_{f+g}(\varepsilon) > N_f(\varepsilon/2)$ and $N_{f+g}(\varepsilon) > N_g\left(\frac{\varepsilon}{2}\right)$. This suggests that I take $N_{f+g}(\varepsilon) = \max\left(N_f(\varepsilon/2), N_g(\varepsilon/2)\right)$.

Proof: Let f, g be null sequences, and let $\alpha \in \mathbf{C}$. Define $N_{f+g}\colon \mathbf{R}^+ \to \mathbf{N}$ by

$$N_{f+g}(\varepsilon) = \max\left(N_f(\varepsilon/2), N_g(\varepsilon/2)\right).$$

Then for all $n \in \mathbf{N}$,

$$\begin{aligned} n \geq N_{f+g}(\varepsilon) &\implies n \geq N_f(\varepsilon/2) \text{ and } n \geq N_g(\varepsilon/2) \\ &\implies |f(n)| < \varepsilon/2 \text{ and } |g(n)| < \varepsilon/2 \\ &\implies |f(n)+g(n)| \leq |f(n)| + |g(n)| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} \\ &\implies |(f+g)(n)| < \varepsilon. \end{aligned}$$

Hence, N_{f+g} is a precision function for $f+g$, and $f+g$ is a null sequence.

If $\alpha = 0$ then $\alpha f = \tilde{0}$ is a null sequence. Suppose $\alpha \neq 0$, and define $N_{\alpha f}\colon \mathbf{R}^+ \to \mathbf{N}$ by

$$N_{\alpha f}(\varepsilon) = N_f\left(\frac{\varepsilon}{|\alpha|}\right).$$

Then for all $n \in \mathbf{Z}$,

$$\begin{aligned} n \geq N_{\alpha f} &\implies n \geq N_f\left(\frac{\varepsilon}{|\alpha|}\right) \\ &\implies |f(n)| \leq \frac{\varepsilon}{|\alpha|} \\ &\implies |\alpha|\,|f(n)| \leq \varepsilon \\ &\implies |\alpha f(n)| \leq \varepsilon. \end{aligned}$$

Hence $N_{\alpha f}$ is a precision function for αf, and hence αf is a null sequence. Since $f - g = f + (-1)g$ it follows that $f - g$ is a null sequence. ‖

7.28 Exercise (Product theorem for null sequences.) Let f, g be complex null sequences. Prove that fg is a null sequence.

7.5 Theorems About Convergent Sequences

7.29 Remark. *Let f be a complex sequence, and let $L \in \mathbf{C}$. Then the following three statements are equivalent.*

a) $f \to L$

b) $f - \tilde{L}$ *is a null sequence.*

c) $|f - \tilde{L}|$ *is a null sequence.*

Proof: By definition 7.10, "$f \to L$" means

$$\text{for every } r \in \mathbf{R}^+ \text{ there is some } N \in \mathbf{N} \text{ such that} \\ \text{for every } n \in \mathbf{Z}_{\geq N},\ (|f(n) - L| < r).$$

By definition 7.11, "$f - \tilde{L}$ is a null sequence" means

$$\text{for every } \varepsilon \in \mathbf{R}^+ \text{ there is some } N \in \mathbf{N} \text{ such that} \\ \text{for every } \ n \in \mathbf{Z}_{\geq N}, |(f - \tilde{L})(n)| < \varepsilon. \tag{7.30}$$

Both definitions say the same thing. If we write out the definition for "$|f - \tilde{L}|$ is a null sequence" we get (7.30) with "$|(f - \tilde{L})(n)| < \varepsilon$" replaced by "$\Big||f - \tilde{L}|(n)\Big| < \varepsilon$." Since

$$|(f - \tilde{L})(n)| = |f(n) - L| = \Big||f - \tilde{L}|(n)\Big|,$$

conditions b) and c) are equivalent. ‖

7.31 Theorem (Decomposition theorem.) *Let f be a convergent complex sequence. Then we can write*

$$f = k + \tilde{c}$$

where k is a null sequence, and $\tilde{c}$ is a constant sequence. If $f \to L$, then $c = L$.

Proof: $f = (f - \tilde{L}) + \tilde{L}$. ‖

7.32 Theorem (Sum theorems for convergent sequences.) *Let $\alpha \in \mathbf{C}$ and let f, g be convergent complex sequences. Say $f \to L$ and $g \to M$. Then $f + g$, $f - g$ and αf are convergent and*

$$\begin{aligned} f + g &\to L + M \\ f - g &\to L - M \\ \alpha f &\to \alpha L. \end{aligned}$$

Proof: Suppose $f \to L$ and $g \to M$. By the decomposition theorem, we can write

$$f = k + \tilde{L} \text{ and } g = p + \tilde{M}$$

where k and p are null sequences. Then

$$(f \pm g) - (\widetilde{L \pm M}) = (k + \tilde{L}) \pm (p + \tilde{M}) - (\tilde{L} \pm \tilde{M}) = k \pm p.$$

By the sum theorem for null sequences, $k \pm p$ is a null sequence, so $(f \pm g) - \widetilde{L \pm M}$ is a null sequence, and hence $f \pm g \to L \pm M$. ‖

7.33 Exercise. Prove the last statement in theorem 7.32; i.e., show that if $f \to L$ then $\alpha f \to \alpha L$ for all $\alpha \in \mathbf{C}$.

7.34 Theorem (Product theorem for convergent sequences.) *Let f, g be convergent complex sequences. Suppose $f \to L$ and $g \to M$. Then fg is convergent and $fg \to LM$.*

Proof: Suppose $f \to L$ and $g \to M$. Write $f = k + \tilde{L}$, $g = p + \tilde{M}$ where k, p are null sequences. Then

$$\begin{aligned} fg &= (k + \tilde{L})(p + \tilde{M}) \\ &= kp + \tilde{L}p + \tilde{M}k + \tilde{L}\tilde{M} \\ &= kp + Lp + Mk + \widetilde{LM}. \end{aligned}$$

Now kp, Lp and Mk are null sequences by the product theorem and sum theorem for null sequences, and $\widetilde{LM} \to LM$, so by several applications of the sum theorem for convergent sequences,

$$fg \to 0 + 0 + 0 + LM; \text{ i.e. } fg \to LM. \; \|$$

7.35 Theorem (Uniqueness theorem for convergent sequences.) *Let f be a complex sequence, and let $L, M \in \mathbf{C}$. If $f \to L$ and $f \to M$, then $L = M$.*

Proof: Suppose $f \to L$ and $f \to M$. Then $f - \tilde{L}$ and $f - \tilde{M}$ are null sequences, so $(f - \tilde{L}) - (f - \tilde{M}) = \tilde{M} - \tilde{L} = \widetilde{M - L}$ is a null sequence. Hence, by theorem 7.15, $M - L = 0$; i.e., $L = M$. ‖

7.36 Definition (Limit of a sequence.) Let f be a convergent sequence. Then the unique complex number L such that $f \to L$ is denoted by $\lim f$ or $\lim\{f(n)\}$.

7.37 Remark. It follows from the sum and product theorems that if f and g are convergent sequences, then

$$\lim(f \pm g) = \lim f \pm \lim g$$

and

$$\lim(f \cdot g) = \lim f \cdot \lim g$$

and

$$\lim cf = c \lim f.$$

7.38 Warning. We have only defined $\lim f$ when f is a convergent sequence. Hence $\lim\{i^n\}$ is ungrammatical and should not be written down. (We showed in theorem 7.7 that $\{i^n\}$ diverges.) However, it is a standard usage to say "$\lim f$ does not exist" or "$\lim\{f(n)\}$ does not exist" to mean that the sequence f has no limit. Hence we may say "$\lim\{i^n\}$ does not exist".

7.39 Theorem. *Let f be a complex sequence. Then f is convergent if and only if both* Ref *and* Imf *are convergent. Moreover,*

$$\begin{aligned} \lim f &= \lim \mathrm{Re} f + i \lim \mathrm{Im} f, && (7.40) \\ \lim \mathrm{Re} f &= \mathrm{Re}(\lim f), \\ \lim \mathrm{Im} f &= \mathrm{Im}(\lim f). \end{aligned}$$

Proof: If Ref and Imf are convergent, then it follows from the sum theorem for convergent sequences that f is convergent and (7.40) is valid.

Suppose that $f \to L$. Then $f - \tilde{L}$ is a null sequence, so Re$(f - \tilde{L})$ is a null sequence (by Theorem 7.26). For all $n \in \mathbf{N}$,

$$\text{Re}(f - \tilde{L})(n) = \text{Re}\,(f(n) - L) = \text{Re}f(n) - \text{Re}L = (\text{Re}f - \widetilde{\text{Re}L})(n)$$

so $(\text{Re}f - \widetilde{\text{Re}L}) = \text{Re}(f - \tilde{L})$ is a null sequence and it follows that Ref converges to ReL. A similar argument shows that Im$f \to$ ImL. |||

7.41 Definition (Bounded sequence.) A sequence f in $\mathbf{C}$ is *bounded*, if there is a disc $\overline{D}(0, B)$ such that $f(n) \in \overline{D}(0, B)$ for all $n \in \mathbf{N}$; i.e., f is bounded if there is a number $B \in [0, \infty)$ such that

$$|f(n)| \leq B \text{ for all } n \in \mathbf{N}. \tag{7.42}$$

Any number B satisfying condition (7.42) is called a *bound for f*.

7.43 Examples. $\left\{\dfrac{i^n n}{n+1}\right\}$ is bounded since $\left|\dfrac{i^n n}{n+1}\right| = \dfrac{n}{n+1} \leq 1$ for all $n \in \mathbf{N}$. The sequence $\{n\}$ is not bounded since the statement $|n| \leq B$ for all $n \in \mathbf{N}$ contradicts the Archimedean property of $\mathbf{R}$. Every constant sequence $\{\tilde{L}\}$ is bounded. In fact, $|L|$ is a bound for $\tilde{L}$.

7.44 Exercise (Null-times-bounded theorem.) Show that if f is a null sequence in $\mathbf{C}$, and g is a bounded sequence in $\mathbf{C}$ then fg is a null sequence.

The next theorem I want to prove is a quotient theorem for convergent sequences. To prove this, I will need some technical results.

7.45 Theorem (Reverse triangle inequality.) *Let $\alpha, \beta \in \mathbf{C}$, then*

$$|\alpha - \beta| \geq |\alpha| - |\beta|.$$

Proof: By the triangle inequality.

$$|\alpha| = |(\alpha - \beta) + \beta| \leq |\alpha - \beta| + |\beta|.$$

Hence,

$$|\alpha| - |\beta| \leq |\alpha - \beta|. \quad |||$$

7.46 Lemma. *Let f be a convergent sequence that is not a null sequence; i.e., $f \to L$ where $L \neq 0$. Suppose $f(n) \neq 0$ for all $n \in \mathbf{N}$. Then $\frac{1}{f}$ is a bounded sequence.*

Proof: Since $f \to L$, we know that $f - \tilde{L}$ is a null sequence. Let $N_{f-\tilde{L}}$ be a precision function for $f - \tilde{L}$. Then for all $n \in \mathbf{N}$,

$$\begin{aligned} n \geq N_{f-\tilde{L}}\left(\frac{|L|}{2}\right) &\implies |f(n) - L| < \frac{|L|}{2} \\ &\implies \frac{|L|}{2} > |L - f(n)| \geq |L| - |f(n)| \\ &\implies |f(n)| \geq |L| - \frac{|L|}{2} = \frac{|L|}{2} > 0 \\ &\implies \left|\frac{1}{f(n)}\right| \leq \frac{2}{|L|}; \end{aligned}$$

i.e., if $M = N_{f-\tilde{L}}\left(\frac{|L|}{2}\right)$, then

$$n \geq M \implies \left|\frac{1}{f(n)}\right| \leq \frac{2}{|L|}.$$

Let

$$B = \max\left(\frac{2}{|L|}, \max_{0 \leq m \leq M}\left|\frac{1}{f(m)}\right|\right).$$

Then $\left|\frac{1}{f(m)}\right| \leq B$ for $m \in \mathbf{Z}_{0 \leq m \leq M}$ and $\left|\frac{1}{f(m)}\right| \leq B$ for $m \in \mathbf{Z}_{\geq M}$, so $\left|\frac{1}{f(m)}\right| \leq B$ for all $m \in \mathbf{Z}_{\geq 0} = \mathbf{N}$, and hence $\frac{1}{f}$ is bounded. |||

7.47 Theorem (Reciprocal theorem for convergent sequences.) *Let g be a complex sequence. Suppose that $g \to L$ where $L \neq 0$, and that $g(n) \neq 0$ for all $n \in \mathbf{N}$. Then $\frac{1}{g}$ is convergent, and $\frac{1}{g} \to \frac{1}{L}$.*

Proof: By the preceding lemma, $\dfrac{1}{g}$ is a bounded sequence, and since $g \to L$, we know that $g - \tilde{L}$ is a null sequence. Hence $(g - \tilde{L}) \cdot \dfrac{1}{g} = \tilde{1} - \dfrac{L}{g}$ is a null sequence, and it follows that $\dfrac{L}{g} \to 1$. Then we have

$$\frac{1}{g} = \frac{1}{L} \cdot \frac{L}{g} \to \frac{1}{L} \cdot 1 = \frac{1}{L};$$

i.e., $\dfrac{1}{g} \to \dfrac{1}{L}$. ‖

7.48 Exercise (Quotient theorem for convergent sequences.) The following statement isn't quite true. Supply the missing hypotheses and prove the corrected statement.

Let f, g be convergent complex sequences. If $f \to L$ and $g \to M$, then $\dfrac{f}{g}$ is convergent and $\dfrac{f}{g} \to \dfrac{L}{M}$.

7.49 Exercise.

a) Let f, g be complex sequences. Show that if f converges and g diverges, then $f + g$ diverges.

b) Show that if f converges and g diverges, then fg does not necessarily diverge.

7.50 Exercise. Let f be a divergent complex sequence. Show that if $c \in \mathbf{C}\backslash\{0\}$, then cf is divergent.

7.51 Example. Let $f \colon \mathbf{Z}_{\geq 1} \to \mathbf{C}$ be defined by

$$f(n) = \frac{n^2 + in + 1}{3n^2 + 2in - 1}. \tag{7.52}$$

Then

$$f(n) = \frac{n^2\left(1 + \frac{i}{n} + \frac{1}{n^2}\right)}{n^2\left(3 + \frac{2i}{n} - \frac{1}{n^2}\right)} = \frac{1 + \frac{i}{n} + \frac{1}{n^2}}{\left(3 - \frac{1}{n^2}\right) + \frac{2i}{n}}. \tag{7.53}$$

Hence f can be written as a quotient of two sequences:

$$h\colon n \mapsto 1 + \frac{i}{n} + \frac{1}{n^2}$$

and

$$g\colon n \mapsto \left(3 - \frac{1}{n^2}\right) + \frac{2i}{n}$$

where $g(n) \neq 0$ for all $n \in \mathbf{Z}_{\geq 1}$. Since

$$h = \tilde{1} + i\left\{\frac{1}{n}\right\}_{n\geq 1} + \left\{\frac{1}{n}\right\}_{n\geq 1} \cdot \left\{\frac{1}{n}\right\}_{n\geq 1}$$

and

$$g = \tilde{3} - \left\{\frac{1}{n}\right\}_{n\geq 1} + 2i\left\{\frac{1}{n}\right\}_{n\geq 1},$$

it follows from numerous applications of product and sum rules that $h \to 1$ and $g \to 3 \neq 0$ and hence $f = \dfrac{h}{g} \to \dfrac{1}{3}$. Once I have expressed $f(n)$ in the final form in (7.53), I can see what the final result is, and I will usually just write

$$\{f(n)\} = \left\{\frac{1 + \frac{i}{n} + \frac{1}{n^2}}{3 - \frac{1}{n^2} + \frac{2i}{n}}\right\} \to \frac{1+0+0}{3-0+0} = \frac{1}{3}.$$

7.54 Example. Let $g\colon \mathbf{N} \to \mathbf{C}$ be the sequence

$$g = \left\{\frac{2^n + 4^n}{4^n + 6^n}\right\}. \tag{7.55}$$

Then for all $n \in \mathbf{N}$,

$$g(n) = \frac{2^n + 4^n}{4^n + 6^n} = \frac{4^n\left(\frac{2^n}{4^n} + 1\right)}{6^n\left(\frac{4^n}{6^n} + 1\right)} = \left(\frac{2}{3}\right)^n \left(\frac{\left(\frac{1}{2}\right)^n + 1}{\left(\frac{2}{3}\right)^n + 1}\right).$$

Since $\left|\dfrac{2}{3}\right| < .7$, I know $\left\{\left(\dfrac{2}{3}\right)^n\right\} \to 0$ and $\left\{\left(\dfrac{1}{2}\right)^n\right\} \to 0$ so

$$\{g(n)\} = \left\{\left(\frac{2}{3}\right)^n \frac{\left(\left(\frac{1}{2}\right)^n + 1\right)}{\left(\left(\frac{2}{3}\right)^n + 1\right)}\right\} \to 0 \cdot \frac{0+1}{0+1} = 0.$$

In the last two examples, I was motivated by the following considerations. I think: In the numerator and denominator for (7.52), for large n the "n^2" term overwhelms the other terms – so that's the term I factored out. In the numerator of (7.55), the overwhelming term is 4^n, and in the denominator, the overwhelming term is 6^n so those are the terms I factored out.

7.56 Exercise. Let $\{f(n)\}$ be a sequence of non-negative numbers and suppose $\{f(n)\} \to L$ where $L > 0$. Prove that $\{\sqrt{f(n)}\} \to \sqrt{L}$. (NOTE: The case $L = 0$ follows from the root theorem for null sequences.

7.57 Exercise. Investigate the sequences below, and find their limits if they have any.

a) $f = \left\{\dfrac{1 + 3n + 3in^2}{1 + 2in + 5n^2}\right\}_{n\geq 1}$

b) $g = \left\{\dfrac{n^2 + 3in + 1}{n^3 + n + i}\right\}_{n\geq 1}$

c) $h = \left\{\dfrac{\left(4 + \frac{1}{n}\right)^2 - 16}{\left(3 + \frac{i}{n}\right)^2 - 9}\right\}_{n\geq 1}$

d) $k = \left\{\sqrt{1 + \dfrac{1}{n}}\right\}_{n\geq 1}$

e) $l = \left\{\sqrt{n^2 + n} - n\right\}_{n\geq 1}$

7.58 Exercise. Show that the sum of two bounded sequences is a bounded sequence.

7.59 Theorem (Convergent sequences are bounded.) *Let $\{\alpha_n\}$ be a convergent complex sequence. Then $\{\alpha_n\}$ is bounded.*

Proof: I will show that null sequences are bounded and leave the general case to you. Let f be a null sequence and let N_f be a precision function for f.

Let

$$B = \max\left(1, \max_{0\leq j\leq N_f(1)} (|f(j)|)\right).$$

I claim that B is a bound for f. If $n \in \mathbf{Z}_{0 \leq j \leq N_f(1)}$, then

$$|f(n)| \leq \max_{0 \leq j \leq N_f(1)} (|f(j)|) \leq B.$$

If $n \in \mathbf{Z}_{\geq N_f(1)}$, then $n \geq N_f(1)$, so $|f(n)| \leq 1 \leq B$. Hence

$$|f(n)| \leq B \text{ for all } n \in \mathbf{Z}_{0 \leq j \leq N_f(1)} \cup \mathbf{Z}_{\geq N_f(1)},$$

i.e., $|f(n)| \leq B$ for all $n \in \mathbf{N}$. ‖

7.60 Exercise. Complete the proof of theorem 7.59; i.e., show that if $\{\alpha_n\}$ is a convergent complex sequence, then $\{\alpha_n\}$ is bounded.

7.61 Example. It follows from the fact that convergent sequences are bounded, that $\{n\}$ is not a convergent sequence.

7.62 Exercise. Give an example of a bounded sequence that is not convergent.

7.6 Geometric Series

7.63 Theorem ($\left\{r^{\frac{1}{n}}\right\} \to 1$.) *If $r \in \mathbf{R}^+$, then $\{r^{\frac{1}{n}}\} \to 1$.*

Proof:

Case 1: $[r \geq 1]$. By the formula for factoring $s^n - a^n$ (3.78), we have for all $n \in \mathbf{Z}_{\geq 1}$ and all $s \geq 1$

$$(s^n - 1) = (s-1)\sum_{j=0}^{n-1} s^j \geq (s-1)\sum_{j=0}^{n-1} 1^j = n(s-1)$$

so

$$(s-1) \leq \frac{1}{n}(s^n - 1).$$

If we let $s = r^{\frac{1}{n}}$ in this formula, we get

$$|r^{\frac{1}{n}} - 1| = r^{\frac{1}{n}} - 1 \leq \frac{1}{n}(r-1).$$

Since $\left\{\dfrac{r-1}{n}\right\}$ is a null sequence, it follows from the comparison theorem for null sequences that $\{r^{1/n} - 1\} \to 0$; i.e., $\left\{r^{\frac{1}{n}}\right\} \to 1$.

Case 2: $[0 < r < 1.]$ Let $R = \dfrac{1}{r}$. Then $R > 1$, so by Case 1, $\left\{R^{\frac{1}{n}}\right\} \to 1$. By the reciprocal theorem $\left\{\dfrac{1}{R^{\frac{1}{n}}}\right\} \to 1$; i.e., $\left\{r^{\frac{1}{n}}\right\} \to 1$.

We have shown that the theorem holds in all cases. ‖

7.64 Theorem (Convergence of geometric sequences.) *Let $\alpha \in \mathbf{C}$. Then*

$$\begin{aligned}&\{\alpha^n\} \to 0 \textit{ if } |\alpha| < 1\\ &\{\alpha^n\} \to 1 \textit{ if } \alpha = 1\\ &\{\alpha^n\} \textit{ diverges if } |\alpha| \geq 1 \textit{ and } \alpha \neq 1.\end{aligned}$$

Proof: The last assertion was shown in theorem 7.7, and the second statement is clear, and it is also clear that $\{\alpha^n\} \to 0$ if $\alpha = 0$.

Suppose that $0 < |\alpha| < 1$. I will show that

$$|\alpha^k| \leq \frac{1}{2} \text{ for some } k \in \mathbf{N}. \tag{7.65}$$

It will then follow that

$$|\alpha^n|^k = (|\alpha|^k)^n \leq \left(\frac{1}{2}\right)^n = \frac{1}{2^n} \text{ for all } n \in \mathbf{N}.$$

Since $\{\frac{1}{2^n}\}$ is a null sequence, it follows from the comparison theorem for null sequences that $\{|\alpha^n|^k\}$ is a null sequence, and then by the root theorem for null sequences (Theorem 7.19), it follows that $\{\alpha^n\}$ is a null sequence.

To prove (7.65), let N be a precision function for $\left\{\left(\frac{1}{2}\right)^{\frac{1}{n}} - 1\right\}$, and let $k = N(1 - |\alpha|)$. Then $\left|\left(\frac{1}{2}\right)^{\frac{1}{k}} - 1\right| < 1 - |\alpha|$, so $1 - \left(\frac{1}{2}\right)^{\frac{1}{k}} < 1 - |\alpha|$, so $|\alpha| < \left(\frac{1}{2}\right)^{\frac{1}{k}}$. and hence $|\alpha^k| \leq \frac{1}{2}$, which is what we wanted to show. ‖

7.66 Theorem (Geometric series.) *Let $\alpha \in \mathbf{C}$. If $|\alpha| < 1$, then the geometric series*

$$g_\alpha : n \mapsto \sum_{j=0}^{n} \alpha^j$$

converges to $\dfrac{1}{1-\alpha}$. If $|\alpha| \geq 1$, then g_α diverges.

Proof: We saw in theorem 3.71 that $g_\alpha(n) = \sum_{j=0}^{n} \alpha^j = \frac{1-\alpha^{n+1}}{1-\alpha}$ for all $\alpha \neq 1$. If $\alpha = 1$, $g_\alpha(n) = n+1$. This sequence diverges, since it is not bounded. If $|\alpha| < 1$, then by the previous theorem $\{\alpha^n\} \to 0$, so

$$\{g_\alpha(n)\} = \left\{\frac{1}{1-\alpha} - \frac{\alpha}{1-\alpha} \cdot \alpha^n\right\} \to \frac{1}{1-\alpha} - \frac{\alpha}{1-\alpha} \cdot 0 = \frac{1}{1-\alpha}.$$

Suppose now $|\alpha| \geq 1$ and $\alpha \neq 1$. Then for all $n \in \mathbf{N}$ we have

$$\begin{aligned} \alpha^n &= \frac{1}{\alpha} \cdot \alpha^{n+1} = \frac{1}{\alpha}\left(1 - (1-\alpha) \cdot \frac{1-\alpha^{n+1}}{1-\alpha}\right) \\ &= \frac{1-(1-\alpha)g_\alpha(n)}{\alpha}. \end{aligned}$$

Hence for all $L \in \mathbf{C}$ we have

$$\{g_\alpha(n)\} \to L \implies \{\alpha^n\} \to \frac{1-(1-\alpha)L}{\alpha}.$$

By theorem 7.7, if $|\alpha| \geq 1$ and $\alpha \neq 1$, then $\{\alpha^n\}$ diverges, and hence $\{g_\alpha(n)\} \to L$ is false for all $L \in \mathbf{C}$; i.e., g_α diverges. ‖

7.67 Notation. If $\{a_j\}_{j \geq 1}$ is a sequence of digits, then we denote $\sum_{j=1}^{n} \frac{a_j}{10^j}$ by $.a_1 a_2 \cdots a_n$. Thus

$$.14159 = \frac{1}{10} + \frac{4}{10^2} + \frac{1}{10^3} + \frac{5}{10^4} + \frac{9}{10^5}$$

and

$$\begin{aligned} &.351351351 \\ &= \left(\frac{3}{10} + \frac{5}{100} + \frac{1}{1000}\right) + \left(\frac{3}{10^4} + \frac{5}{10^5} + \frac{1}{10^6}\right) + \left(\frac{3}{10^7} + \frac{5}{10^8} + \frac{1}{10^9}\right) \\ &= \left(\frac{351}{1000}\right)\left[1 + \frac{1}{10^3} + \frac{1}{10^6}\right] \\ &= \frac{351}{1000} \sum_{j=0}^{2} \frac{1}{10^{3j}}. \end{aligned}$$

7.68 Example. Let a, b, c be digits, and let

$$\{x_n\} = \left\{ \frac{abc}{1000} \sum_{j=0}^{n} \frac{1}{10^{3j}} \right\}$$

so informally, $x_n = \underbrace{.abcabc\cdots abc}_{3(n+1) \text{ digits}}$. Then $\{x_n\}$ is a convergent sequence, and

$$\{x_n\} \to \frac{abc}{1000} \cdot \frac{1}{1 - \frac{1}{1000}} = \frac{abc}{999}.$$

As an example, we have

$$\{.351, .351351, .351351351, \cdots\} \to \frac{351}{999} = \frac{39}{111} = \frac{13}{37}.$$

7.69 Exercise. Let

$$\{a_n\} = \{.672, .67272, .6727272, .672727272, \cdots\}_{n \geq 1}.$$

Show that $\{a_n\}$ converges to a rational number.

7.70 Exercise.

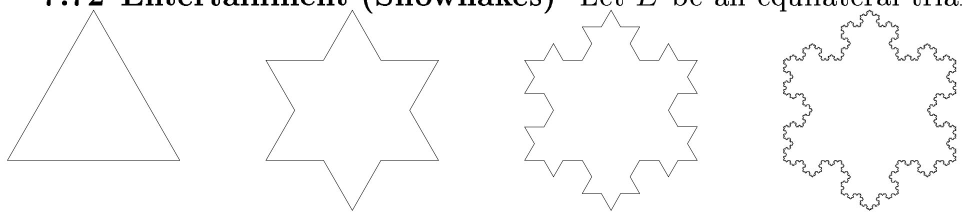
a) Let $\{a_n\} = \left\{ \sum_{j=0}^{n} \left(\left(\frac{3}{5}\right)^j + \left(\frac{4}{5}\right)^j i \right) \right\}$. Does $\{a_n\}$ converge? If it does, find $\lim\{a_n\}$ in the form $a + bi$ where $a, b \in \mathbf{R}$.

b) Let $\{b_n\} = \left\{ \sum_{j=0}^{n} \left(\frac{3+4i}{5}\right)^j \right\}$. Does $\{b_n\}$ converge? If it does, find $\lim\{b_n\}$ in the form $a + bi$ where $a, b \in \mathbf{R}$.

c) Let $\{c_n\} = \left\{ \sum_{j=0}^{n} \left(\left(\frac{3}{5}\right)^j + \left(\frac{4i}{5}\right)^j \right) \right\}$. Does $\{c_n\}$ converge? If it does, find $\lim\{c_n\}$ in the form $a + bi$ where $a, b \in \mathbf{R}$.

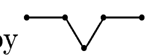
7.71 Exercise. Show that the sequences $\left\{ \sum_{j=0}^{n} \left(\frac{1+i}{2}\right)^j \right\}$ and $\left\{ \sum_{j=0}^{n} \left(\frac{2+i}{3}\right)^j \right\}$ (which are drawn on page 126) converge, and that the limits appear to be in agreement with Figure b) on page 126.

7.72 Entertainment (Snowflakes) Let E be an equilateral triangle with



Snowflakes

area A, and side s. Note that an equilateral triangle with side $\frac{s}{3}$ has area $\frac{A}{9}$. Starting with E, we will now construct a sequence $\{S_n\}$ of polygons. S_n will have $4^n \cdot 3$ sides, all having length $\frac{s}{3^n}$. We let $S_0 = E$ (so S_0 has $4^0 \cdot 3$ sides of length $\frac{s}{3^0}$). To construct S_{n+1} from S_n we attach an equilateral triangle with side of length $\frac{1}{3} \cdot$ side (S_n) to the middle third of each side of S_n.

The bottom side of S_n will be replaced by . Each side of S_n is replaced by 4 sides of length $\frac{1}{3}\left(\frac{s}{3^n}\right)$, so S_{n+1} will have $4 \cdot (4^n 3) = 4^{n+1} \cdot 3$ sides of length $\frac{s}{3^{n+1}}$. The figure shows some of these polygons. I will call the polygons S_n *snowflake polygons*. We have $S_n \subset S_{n+1}$ for all n. The *snowflake* S is the union of all of the sets S_n; i.e., a point x is in S if and only if it is in S_n for some $n \in \mathbf{N}$.

Find the area of S_n (in terms of the area A of E), for example

$$\text{area}(S_1) = A + 3\left(\frac{A}{9}\right) = \frac{4}{3}A.$$

Then find the area of S in terms of A. Make any reasonable assumptions that you need. What is the perimeter of S?

7.7 The Translation Theorem

7.73 Theorem. *Let f be a real convergent sequence, say $f \to L$. If $f(n) \geq 0$ for all $n \in \mathbf{N}$, then $L \geq 0$.*

Proof: I note that $L \in \mathbf{R}$, since if $f \to L$, then $\text{Re}f \to \text{Re}L$. Suppose, to get a contradiction, that $L < 0$, (so $-\frac{L}{2} > 0$), and let $N_{f-\tilde{L}}$ be a precision function for the null sequence $f - \tilde{L}$. Let $N = N_{f-\tilde{L}}\left(-\frac{L}{2}\right)$. Then $|(f - \tilde{L})(N)| \leq -\frac{L}{2}$, so $|f(N) - L| \leq -\frac{L}{2}$, and hence $f(N) < L - \frac{L}{2} = \frac{L}{2} < 0$. This contradicts the assumption that $f(N) \geq 0$ for all $n \in \mathbf{N}$. $\|$

7.74 Exercise (Inequality theorem.) Let f, g be convergent real sequences. Suppose that $f(n) \leq g(n)$ for all $n \in \mathbf{N}$. Prove that $\lim f \leq \lim g$.

7.75 Exercise. Prove the following assertion, or give an example to show that it is not true. Let f, g be convergent real sequences. Suppose that $f(n) < g(n)$ for all $n \in \mathbf{N}$. Then $\lim f < \lim g$.

7.76 Definition (Translate of a sequence.) Let f be a sequence and let $p \in \mathbf{N}$. Then the sequence $f_p: n \mapsto f(n+p)$ is called a *translate of* f.

7.77 Example. If $f = \left\{\frac{1}{2^2}, \frac{1}{3^2}, \frac{1}{4^2}, \cdots, \frac{1}{(n+2)^2}, \cdots\right\}$, then $f_3 = \left\{\frac{1}{5^2}, \frac{1}{6^2}, \frac{1}{7^2}, \cdots, \frac{1}{(n+5)^2}, \cdots\right\}$. A translate of a sequence is a sequence obtained by ignoring the first few terms.

7.78 Theorem (Translation theorem.) *If $\{f(n)\}$ is a convergent complex sequence, and $p \in \mathbf{N}$, then $\{f(n+p)\}$ converges, and $\lim\{f(n)\} = \lim\{f(n+p)\}$. Conversely, if $\{f(n+p)\}$ converges, then $\{f(n)\}$ converges to the same limit.*

Proof: Let $f \to L$, let $f_p(n) = f(n+p)$ and let $N_{f-\tilde{L}}$ be a precision function for $f - \tilde{L}$. I claim $N_{f-\tilde{L}}$ is also a precision function for $f_p - \tilde{L}$. In fact, for all $n \in \mathbf{N}$, and all $\varepsilon \in \mathbf{R}^+$,

$$n \geq N_{f-\tilde{L}}(\varepsilon) \implies n + p \geq N_{f-\tilde{L}}(\varepsilon) \implies |f(n+p) - L| < \varepsilon.$$

Conversely, suppose

$$\{f_p(n)\} = \{f(n+p)\} \to L$$

and let $N_{f_p-\tilde{L}}$ be a precision function for $f_p - \tilde{L}$. Let $N(\varepsilon) = p + N_{f_p-\tilde{L}}(\varepsilon)$ for all $\varepsilon \in \mathbf{R}^+$. I claim N is a precision function for $N_{f-\tilde{L}}$. For all $n \in \mathbf{N}$,

$$\begin{aligned} n > N(\varepsilon) &\implies n > p + N_{f_p-\tilde{L}}(\varepsilon) \\ &\implies n - p > N_{f_p-\tilde{L}}(\varepsilon) \\ &\implies |(f_p - \tilde{L})(n-p)| < \varepsilon \\ &\implies |f_p(n-p) - L| < \varepsilon \\ &\implies |f(n) - L| < \varepsilon. \ \| \end{aligned}$$

7.79 Example. Let the sequence f be defined by

$$\begin{aligned} f(0) &= 1, \\ f(n+1) &= \frac{1}{1+f(n)} \text{ for all } n \in \mathbf{N}. \end{aligned}$$

Then

$$\begin{aligned} f(1) &= \frac{1}{1+1} = \frac{1}{2} \\ f(2) &= \frac{1}{1+\frac{1}{1+1}} = \frac{1}{1+\frac{1}{2}} = \frac{2}{3} \\ f(3) &= \frac{1}{1+\frac{1}{1+\frac{1}{1+1}}} = \frac{1}{1+\frac{2}{3}} = \frac{3}{5}. \end{aligned}$$

Suppose I knew that f converged to a limit L. It is clear that $f(n) > 0$ for all n, so L must be ≥ 0. By the translation theorem

$$L = \lim\{f(n+1)\} = \lim\left\{\frac{1}{1+f(n)}\right\} = \frac{1}{1+\lim f(n)} = \frac{1}{1+L}$$

so $L(1+L) = 1$; i.e., $L^2+L-1 = 0$. Hence $L \in \left\{\frac{-1+\sqrt{1+4}}{2}, \frac{-1-\sqrt{1+4}}{2}\right\}$, and since $L \geq 0$, we conclude $L = \frac{\sqrt{5}-1}{2}$. I've shown that the only thing that f can possibly converge to is $\frac{\sqrt{5}-1}{2}$. Now

$$0 < L < \frac{3-1}{2} = 1, \quad \text{so} \quad |1-L| < 1.$$

Since $L = \frac{1}{1+L}$, we have for all $n \in \mathbf{N}$,

$$\begin{aligned} |f(n+1) - L| &= \left|\frac{1}{1+f(n)} - \frac{1}{1+L}\right| = \left|\frac{L - f(n)}{(1+f(n))(1+L)}\right| \leq \frac{|L - f(n)|}{1+L} \\ &= L|L - f(n)| = L|f(n) - L|. \end{aligned}$$

Hence

$$\begin{aligned} |f(1) - L| &\leq L|f(0) - L| = L|1 - L| \leq L, \\ |f(2) - L| &\leq L|f(1) - L| \leq L^2, \\ |f(3) - L| &\leq L|f(2) - L| \leq L^3, \end{aligned}$$

and by induction,

$$|f(n) - L| \leq L^n \text{ for all } n \in \mathbf{Z}_{\geq 1}.$$

By theorem 7.64 $\{L^n\}$ is a null sequence, and by the comparison theorem for null sequences, it follows that $\{f(n) - L\}$ is a null sequence. This completes the proof that $f \to L$. |||

7.80 Exercise. Let

$$\begin{aligned} f(0) &= -2 \\ f(n+1) &= \frac{f(n)^2 + 2}{2f(n)} \text{ for all } n \in \mathbf{N}. \end{aligned}$$

a) Assume that f converges, and determine the value of $\lim\{f(n)\}$.

b) Calculate $f(1), f(2), f(3), f(4)$, using all of the accuracy of your calculator. Does the sequence appear to converge?

7.81 Entertainment. Show that the sequence f defined in the previous exercise converges. We will prove this result in Example 7.97, but you can prove it now, using results you know.

7.82 Exercise. Let g be the sequence defined by

$$\begin{aligned} g(0) &= 1, \\ g(1) &= 1, \\ g(n+2) &= \frac{1 + g(n+1)}{g(n)} \text{ for all } n \in \mathbf{N}. \end{aligned}$$

a) Assume that g converges, and determine the value of $\lim\{g(n)\}$.

b) Calculate $g(1), g(2), g(3), g(4), g(5), g(6)$, using all of the accuracy of your calculator. Does this sequence converge?

7.83 Theorem (Divergence test.) *Let f, g be complex sequences such that $g(n) \neq 0$ for all $n \in \mathbf{N}$. Suppose that $g \to 0$ and $f \to L$ where $L \neq 0$. Then $\frac{f}{g}$ diverges.*

Proof: Suppose, to get a contradiction, that $\frac{f}{g}$ converges to a limit M. Then by the product theorem, $g \cdot \frac{f}{g}$ converges to $0 \cdot M = 0$; i.e., $f \to 0$. This contradicts our assumption that f has a non-zero limit. |||

7.84 Exercise. Prove the following assertion or give an example to show that it is not true: Let f, g be complex sequences such that $g(n) \neq 0$ for all $n \in \mathbf{N}$, but $g \to 0$. Then $\frac{f}{g}$ diverges.

7.85 Example. Let $f(n) = \left\{\frac{n^3+3n}{n^2+1}\right\}$ for all $n \in \mathbf{Z}_{\geq 1}$. Then

$$f(n) = \frac{n^3\left(1+\frac{3}{n^2}\right)}{n^2\left(1+\frac{1}{n}\right)} = \frac{\left(1+\frac{3}{n^2}\right)}{\frac{1}{n}\left(1+\frac{1}{n}\right)}.$$

Since

$$\lim\left\{\left(1+\frac{3}{n^2}\right)\right\}_{n\geq 1} = 1+0 \neq 0,$$

and

$$\lim\left\{\frac{1}{n}\left(1+\frac{1}{n}\right)\right\}_{n\geq 1} = 0\cdot(1+0) = 0,$$

it follows that f diverges.

7.86 Exercise. Let A, B, a, b be complex numbers such that $an+b \neq 0$ for all $n \in \mathbf{Z}_{\geq 1}$. Discuss the convergence of $\left\{\frac{An+B}{an+b}\right\}_{n\geq 1}$. Consider all possible choices for A, B, a, b.

7.8 Bounded Monotonic Sequences

7.87 Theorem. *Let $\{[a_n, b_n]\}$ be a binary search sequence in $\mathbf{R}$. Suppose $\{[a_n, b_n]\} \to c$ where $c \in \mathbf{R}$. Then $\{b_n - a_n\}$ is a null sequence. Also $\{a_n\} \to c$ and $\{b_n\} \to c$.*

Proof: We know that $b_n - a_n = \dfrac{b_0 - a_0}{2^n}$, and that $\{\frac{1}{2^n}\}$ is a null sequence, so $\{b_n - a_n\}$ is a null sequence. Since $\{[a_n, b_n]\} \to c$ we know that $a_n \leq c \leq b_n$ for all $n \in \mathbf{N}$, and hence

$$0 \leq |b_n - c| \leq |b_n - a_n| \qquad \text{and} \qquad 0 \leq |c - a_n| \leq |b_n - a_n|$$

for all $n \in \mathbf{N}$. By the comparison theorem for null sequences it follows that $\{c - a_n\}$ and $\{b_n - c\}$ are null sequences, and hence $\{a_n\} \to c$ and $\{b_n\} \to c$. ‖

7.88 Definition (Increasing, decreasing, monotonic) Let f be a real sequence. We say f is *increasing* if $f(n) \leq f(n+1)$ for all $n \in \mathbf{N}$, and we say f is *decreasing* if $f(n) \geq f(n+1)$ for all $n \in \mathbf{N}$. We say that f is *monotonic* if either f is increasing or f is decreasing.

7.89 Theorem. Let f be an increasing real sequence. Then for all $k, n \in \mathbf{N}$

$$f(k) \leq f(k+n).$$

Proof: Define a proposition form P on $\mathbf{N}$ by

$$P(n) = \text{“for all } k \in \mathbf{N}(f(k) \leq f(k+n))\text{”}, \text{ for all } n \in \mathbf{N}.$$

Then $P(0)$ says “for all $k \in \mathbf{N}(f(k) \leq f(k))$”, so $P(0)$ is true. Since f is increasing, we have for all $n \in \mathbf{N}$,

$$\begin{aligned} P(n) \implies & \text{ for all } k \in \mathbf{N}\Big(f(k) \leq f(k+n) \leq f((k+n)+1)\Big) \\ \implies & \text{ for all } k \in \mathbf{N}\Big(f(k) \leq f(k+(n+1))\Big) \\ \implies & P(n+1). \end{aligned}$$

By induction, we conclude that $P(n)$ is true for all $n \in \mathbf{N}$, i.e.

$$\text{for all } n \in \mathbf{N}\Big(\text{for all } k \in \mathbf{N}(f(k) \leq f(k+n))\Big). \ \|$$

7.90 Corollary. Let f be an increasing real sequence. Then for all $k, n \in \mathbf{N}$,

$$k \leq n \implies f(k) \leq f(n). \tag{7.91}$$

Proof: For all $k, n \in \mathbf{N}$

$$k \leq n \implies n - k \in \mathbf{N} \implies f(k) \leq f(k + (n-k)) = f(n). \;\|$$

7.92 Definition (Upper bound, lower bound.) Let f be a real sequence. We say that f has an *upper bound* if there is a number $U \in \mathbf{R}$ such that $f(n) \leq U$ for all $n \in \mathbf{N}$. Any such number U is called an *upper bound for* f. We say that f has a *lower bound* if there is a number $L \in \mathbf{R}$ such that $L \leq f(n)$ for all $n \in \mathbf{N}$. Any such number L is called a *lower bound for* f.

7.93 Examples. If $f(n) = \frac{(-1)^n n}{n+1}$ for all $n \in \mathbf{N}$ then 1 (or any number greater than 1) is an upper bound for f, and -1 (or any number less than -1) is a lower bound for f. The sequence $g : n \mapsto n$ has no upper bound, but 0 is a lower bound for g.

7.94 Exercise. In definition 7.41, we defined a complex sequence f to bounded if there is a number $B \in [0, \infty)$ such that $|f(n)| \leq B$ for all $n \in \mathbf{N}$. Show that a real sequence is bounded if and only if it has both an upper bound and a lower bound.

7.95 Theorem (Bounded monotonic sequences converge.) *Let f be an increasing sequence in $\mathbf{R}$, and suppose f has an upper bound. Then f converges. (Similarly, decreasing sequences that have lower bounds converge.)*

Proof: Let B be an upper bound for f. We will construct a binary search sequence $\{[a_n, b_n]\}$ satisfying the following two conditions:

i. For every $n \in \mathbf{N}$, b_n is an upper bound for f,

ii. For every $n \in \mathbf{N}$, a_n is not an upper bound for f.

Let

$$\begin{aligned} [a_0, b_0] &= [f(0) - 1, B] \\ [a_{n+1}, b_{n+1}] &= \begin{cases} \left[a_n, \frac{a_n + b_n}{2}\right] & \text{if } \frac{a_n+b_n}{2} \text{ is an upper bound for } f \\ \left[\frac{a_n+b_n}{2}, b_n\right] & \text{if } \frac{a_n+b_n}{2} \text{ is not an upper bound for } f. \end{cases} \end{aligned}$$

A straightforward induction argument shows that $\{[a_n, b_n]\}$ satisfies conditions i) and ii).

Let c be the number such that $\{[a_n, b_n]\} \to c$. I will show that $f \to c$.

We know that $\{b_n - a_n\} = \{\frac{b_0 - a_0}{2^n}\}$ is a null sequence. Let N be a precision function for $\{b_n - a_n\}$, so that for all $\varepsilon \in \mathbf{R}^+$,

$$n \geq N(\varepsilon) \implies |b_n - a_n| < \varepsilon.$$

I will use N to construct a precision function K for $f - \tilde{c}$.

Let $\varepsilon \in \mathbf{R}^+$. Since $a_{N(\varepsilon)}$ is not an upper bound for f, there is a number $K(\varepsilon) \in \mathbf{N}$ such that $f(K(\varepsilon)) > a_{N(\varepsilon)}$. By condition i), I know that $f(n) \leq b_{N(\varepsilon)}$ for all $n \in \mathbf{N}$. Hence, since f is increasing, we have for all $n \in \mathbf{N}$:

$$\begin{aligned} n \geq K(\varepsilon) &\implies a_{N(\varepsilon)} < f(K(\varepsilon)) \leq f(n) \leq b_{N(\varepsilon)} \\ &\implies f(n) \in [a_{N(\varepsilon)}, b_{N(\varepsilon)}]. \end{aligned}$$

Since $\{[a_n, b_n]\} \to c$ we also have

$$c \in [a_{N(\varepsilon)}, b_{N(\varepsilon)}].$$

Hence

$$|f(n) - c| \leq b_{N(\varepsilon)} - a_{N(\varepsilon)} < \varepsilon \text{ for all } n \geq K(\varepsilon).$$

This says that K is a precision function for $\{f(n) - c\}$, and hence $f \to c$ |||

7.96 Corollary. *Let f be a real sequence. If f has an upper bound, and there is some $N \in \mathbf{N}$ such that*

$$f(n+1) \geq f(n) \text{ for all } n \in \mathbf{Z}_{\geq N}$$

then f converges. Similarly, if f has a lower bound, and there is some $N \in \mathbf{N}$ such that

$$f(n+1) \leq f(n) \text{ for all } n \in \mathbf{Z}_{\geq N}$$

then f converges.

7.97 Example. Let $a \in \mathbf{R}^+$. Define a sequence $\{x_n\}$ by

$$\begin{aligned} x_0 &= a + 1 \\ x_{n+1} &= \frac{x_n^2 + a}{2x_n} \text{ for all } n \in \mathbf{N}. \end{aligned}$$

We have $x_n > 0$ for all n. Suppose $\{x_n\}$ converges to a limit L. Since $2x_n x_{n+1} = x_n^2 + a$ for all $n \in \mathbf{N}$, we can use the translation theorem to show that

$$2L^2 = 2\lim\{x_n\}\lim\{x_{n+1}\} = \lim\{x_n^2 + a\} = L^2 + a,$$

so $2L^2 = L^2 + a$, and hence $L^2 = a$, so L must be $\pm\sqrt{a}$. Since $x_n \geq 0$ for all n, it follows from the inequality theorem that $L \geq 0$, and hence if $\{x_n\}$ converges, it must converge to $\sqrt{a}$. In order to show that $\{x_n\}$ converges, it is sufficient to show that $\{x_n\}$ is decreasing. (We've already noted that 0 is a lower bound.)

Well,

$$x_n - x_{n+1} = x_n - \frac{x_n^2 + a}{2x_n} = \frac{2x_n^2 - x_n^2 - a}{2x_n} = \frac{x_n^2 - a}{2x_n},$$

so if I can show that $x_n^2 - a \geq 0$ for all $n \in \mathbf{N}$, then I'll know that $\{x_n\}$ is decreasing. Now

$$\begin{aligned} x_{n+1}^2 - a &= \left(\frac{x_n^2 + a}{2x_n}\right)^2 - a = \frac{x_n^4 + 2ax_n^2 + a^2}{4x_n^2} - a \\ &= \frac{x_n^4 + 2ax_n^2 + a^2 - 4ax_n^2}{4x_n^2} = \frac{(x_n^2 - a)^2}{4x_n^2} \geq 0. \end{aligned}$$

I also note that $x_0^2 - a = a^2 + a + 1 > 0$, so I finally conclude that $\{x_n\}$ is decreasing, and hence $\{x_n\} \to \sqrt{a}$. In fact, this sequence converges very fast, and is the basis for the square root algorithm used on most computers.

7.98 Example ($\{n^{\frac{1}{n}}\}$) We will show that $\{n^{\frac{1}{n}}\}_{n\geq 1} \to 1$.
Claim: $\{n^{\frac{1}{n}}\}_{n\geq 3}$ is a decreasing sequence.
Proof: For all $n \in \mathbf{Z}_{\geq 1}$,

$$\begin{aligned} (n+1)^{\frac{1}{n+1}} \leq n^{\frac{1}{n}} &\iff (n+1)^n \leq n^{n+1} \\ &\iff \left(\frac{n+1}{n}\right)^n \leq n. \end{aligned} \tag{7.99}$$

We will show by induction that (7.99) holds for all $n \in \mathbf{Z}_{\geq 3}$. Let

$$P(n) = \text{“}\left(\frac{n+1}{n}\right)^n \leq n\text{” for all } n \in \mathbf{Z}_{\geq 3}.$$

Then $P(3)$ says $(\frac{4}{3})^3 \le 3$, which is true since $64 < 81$. For all $n \in \mathbf{Z}_{\ge 3}$,

$$\begin{aligned}
P(n) &\implies \left(\frac{n+1}{n}\right)^n \le n \\
&\implies \left(\frac{n+2}{n+1}\right)^{n+1} = \left(\frac{n+1}{n}\right)^{n+1}\left(\frac{n(n+2)}{(n+1)^2}\right)^{n+1} \\
&\qquad = \left(\frac{n+1}{n}\right)^n \cdot \frac{n+1}{n}\left(\frac{n^2+2n}{n^2+2n+1}\right)^{n+1} \le n \cdot \frac{n+1}{n} \cdot 1 \\
&\implies \left(\frac{n+2}{n+1}\right)^{n+1} \le n+1 \\
&\implies P(n+1).
\end{aligned}$$

By induction, $P(n)$ is true for all $n \in \mathbf{Z}_{\ge 3}$, and the claim is proved.

Let $L = \lim\{n^{\frac{1}{n}}\}$. Then $\{(2n)^{\frac{1}{2n}}\} \to L$, since any precision function for $\{n^{\frac{1}{n}}\}$ is also a precision function for $\{(2n)^{\frac{1}{2n}}\}$. Hence

$$L^2 = \lim\{\left((2n)^{\frac{1}{2n}}\right)^2\} = \lim\{2^{\frac{1}{n}}n^{\frac{1}{n}}\} = 1 \cdot L = L.$$

Thus $L^2 = L$, and hence $L \in \{0, 1\}$. Since $n^{\frac{1}{n}} \ge 1$ for all $n \in \mathbf{Z}_{\ge 3}$ it follows from the inequality theorem that $L \ge 1$, and hence $L = 1$. ‖

7.100 Exercise. Show that the sequence

$$\left\{\frac{60^n}{n!}\right\} = \{1, 60, 1800, 36000, \cdots\}$$

is a null sequence.

7.101 Exercise. Criticize the following argument.

We know that $\left\{1 + \frac{1}{n}\right\}_{n \ge 1} \to 1 + 0 = 1.$

Hence $\left\{\left(1 + \frac{1}{n}\right)^n\right\}_{n \ge 1} \to 1^n = 1.$ ‖

7.102 Note. I got the idea of using precision functions from a letter by Jan Mycielski in the *Notices of the American Mathematical Society*[34, p 569]. Mycielski calls precision functions *Skolem functions.*

The snowflake was introduced by Helge von Koch(1870–1924) who published his results in 1906 [32]. Koch considered only the part of the boundary corresponding to the bottom third of our polygon, which he introduced as an example of a curve not having a tangent at any point.

The sequence g from Exercise 7.82 is taken from [12, page 55, ex 20]

Chapter 8

Continuity

8.1 Compositions with Sequences

8.1 Definition (Composition) Let $a: n \mapsto a(n)$ be a complex sequence. Let $g: S \to \mathbf{C}$ be a function such that $\mathrm{dom}(g) = S \subset \mathbf{C}$, and $a(n) \in S$ for all $n \in \mathbf{N}$. Then the *composition* $g \circ a$ is the sequence such that $(g \circ a)(n) = g\left(a(n)\right)$ for all $n \in \mathbf{N}$. If a is a sequence, I will often write a_n instead of $a(n)$. Then

$$a = \{a_n\} \implies g \circ a = \{g(a_n)\}.$$

8.2 Examples. If

$$f = \left\{\frac{1}{2^n}\right\} = \left\{1, \frac{1}{2}, \frac{1}{4}, \cdots\right\}$$

and $g(z) = \dfrac{1}{1+z}$ for all $z \in \mathbf{C} \setminus \{-1\}$, then

$$g \circ f = \left\{\frac{1}{1+\frac{1}{2^n}}\right\} = \left\{\frac{2^n}{2^n+1}\right\} = \left\{\frac{1}{2}, \frac{2}{3}, \frac{4}{5}, \cdots\right\}.$$

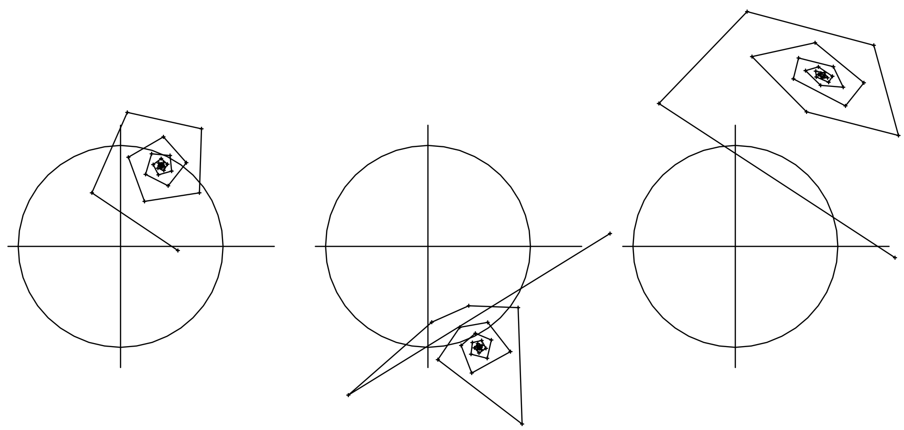
Figure a) below shows representations of $x, v \circ x$ and $K \circ x$ where

$$\begin{aligned} x(n) &= x_n = \frac{2}{5} + \frac{4}{5}i + \left(\frac{4-21i}{25}\right)^{n+1} \text{ for all } n \in \mathbf{N}, \\ v(z) &= \frac{1}{z} \text{ for all } z \in \mathbf{C}\setminus\{0\}, \\ K(z) &= z + \frac{z}{|z|} \text{ for all } z \in \mathbf{C}\setminus\{0\}. \end{aligned} \tag{8.3}$$

I leave it to you to check that $\{x_n\} \to \frac{2}{5} + \frac{4}{5}i$, and $\{v(x_n)\} \to v\left(\frac{2}{5} + \frac{4}{5}i\right)$, and $\{K(x_n)\} \to K\left(\frac{2}{5} + \frac{4}{5}i\right)$. Figure b) shows representations for a and $K \circ a$ where

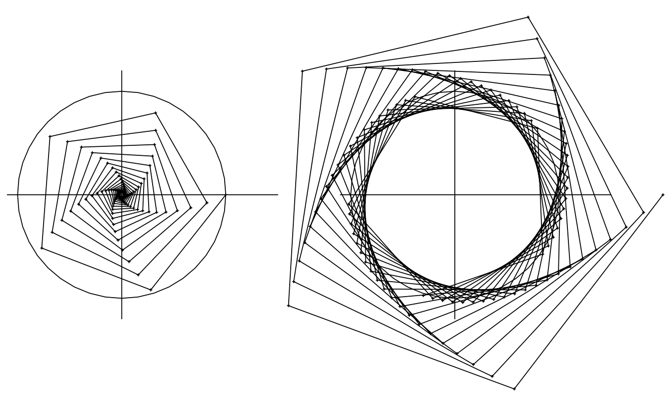
$$a(n) = a_n = \left(\frac{7 - 23i}{25}\right)^n,$$

and K is defined as in (8.3). Here it is easy to check that $\{a_n\} \to 0$. From the figure, $\{K(a_n)\}$ doesn't appear to converge.



$\{x_n\}$ $\{v(x_n)\}$ $\{K(x_n)\}$

figure a) Sequence and compositions



$\{a_n\}$ $\{K(a_n)\}$

figure b) Sequence and composition

8.4 Exercise. Let α be a non-zero complex number with $0 < |\alpha| < 1$. Let

$$f_\alpha(n) = \alpha^n + \frac{\alpha^n}{|\alpha^n|} \text{ for all } n \in \mathbf{N}.$$

Under what conditions on α does f_α converge? What does it converge to? (Your answer should show that the sequence $\{K(a_n)\}$ from the previous example does not converge.)

8.5 Definition (Complex function.) By a *complex function* I will mean a function whose domain is a subset of $\mathbf{C}$, and whose codomain is $\mathbf{C}$. I will consider functions from $\mathbf{R}$ to $\mathbf{R}$ to be complex functions by identifying a function $f: S \to \mathbf{R}$ with a function $f: S \to \mathbf{C}$ in the expected manner.

8.2 Continuity

8.6 Definition (Continuous) Let f be a complex function and let $p \in \text{dom}(f)$. We say *f is continuous at p* if

$$\text{for every sequence } x \text{ in } \text{dom}(f) \quad (x \to p \implies f \circ x \to f(p))\,;$$

i.e., if

$$\text{for every sequence } \{x_n\} \text{ in } \text{dom}(f) \quad (\{x_n\} \to p \implies \{f(x_n)\} \to f(p))\,.$$

Let B be a subset of S. We say *f is continuous on B* if f is continuous at q for all $q \in B$. We say f is *continuous* if f is continuous on $\text{dom}(f)$; i.e., if f is continuous at every point at which it is defined.

8.7 Examples. If $f(z) = z$ for all $z \in \mathbf{C}$, then f is continuous. In this case $f \circ x = x$ for every sequence x so the condition for continuity at p is

$$x \to p \implies x \to p.$$

If $a \in \mathbf{C}$, then the constant function $\tilde{a}$ is continuous since for all $p \in \mathbf{C}$, and all complex sequences x,

$$x \to p \implies \tilde{a} \circ x = \tilde{a} \to a = \tilde{a}(p).$$

Notice that Re and Im (Real part and imaginary part) are functions from **C** to **R**. In theorem 7.39 we showed if x is any complex sequence and $L \in \mathbf{C}$, then

$$x \to L \implies \text{Re}(x) \to \text{Re}(L)$$

and

$$x \to L \implies \text{Im}(x) \to \text{Im}(L).$$

Hence Re and Im are continuous functions on **C**.

8.8 Theorem. *If* abs *and* conj *are functions from* **C** *to* **C** *defined by*

$$\begin{aligned} \text{abs}(z) &= |z| \textit{ for all } z \in \mathbf{C} \\ \text{conj}(z) &= z^* \textit{ for all } z \in \mathbf{C}, \end{aligned}$$

then abs *and* conj *are continuous.*

Proof: Let $a \in \mathbf{C}$ and let x be any sequence in **C** such that $\{x_n\} \to a$; i.e., $\{x_n - a\}$ is a null sequence. By the reverse triangle inequality,

$$|x_n - a| \geq |x_n| - |a|$$

and

$$|x_n - a| = |a - x_n| \geq |a| - |x_n|,$$

so we have

$$-|x_n - a| \leq |x_n| - |a| \leq |x_n - a|$$

and hence

$$||x_n| - |a|| \leq |x_n - a|.$$

It follows by the comparison theorem that $\{|x_n| - |a|\}$ is a null sequence; i.e., $\{|x_n|\} \to |a|$. Hence abs is continuous.

Since $|x_n^* - a^*| = |(x_n - a)^*| = |x_n - a|$, the comparison theorem shows that

$$\{x_n\} \to a \implies \{x_n^*\} \to a^*;$$

i.e., conj is continuous. |||

8.9 Example. If

$$f(z) = \begin{cases} z & \text{for } z \in \mathbf{C}\backslash\{0\}, \\ 1 & \text{for } z = 0, \end{cases}$$

then f is not continuous at 0, since

$$\left\{\frac{1}{n}\right\} \to 0$$

but

$$\left\{f\left(\frac{1}{n}\right)\right\} = \left\{\frac{1}{n}\right\} \to 0 \neq f(0).$$

Notice that to show that a function f is *not* continuous at a point a in its domain, it is sufficient to find *one* sequence $\{x_n\}$ in $\text{dom}(f)$ such that $\{x_n\} \to a$ and either $\{f(x_n)\}$ converges to a limit different from $f(a)$ or $\{f(x_n)\}$ diverges.

8.10 Theorem (Sum and Product theorems.) *Let f, g be complex functions, and let $a \in \text{dom}(f) \cap \text{dom}(g)$. If f and g are continuous at a, then $f+g$, $f-g$, and $f \cdot g$ are continuous at a.*

Proof: Let $\{x_n\}$ be a sequence in domain $(f+g)$ such that $\{x_n\} \to a$. Then $x_n \in \text{dom}(f)$ for all n and $x_n \in \text{dom}(g)$ for all n, and by continuity of f and g at a, it follows that

$$\{f(x_n)\} \to f(a) \text{ and } \{g(x_n)\} \to g(a).$$

By the sum theorem for sequences,

$$\{(f+g)(x_n)\} = \{f(x_n) + g(x_n)\} \to f(a) + g(a) = (f+g)(a).$$

Hence $f+g$ is continuous at a. The proofs of continuity for $f-g$ and $f \cdot g$ are similar.

8.11 Theorem (Quotient theorem.) *Let f, g be complex functions and let $a \in \text{dom}\left(\frac{f}{g}\right)$. If f and g are continuous at a, then $\frac{f}{g}$ is continuous at a.*

8.12 Exercise. Prove the quotient theorem. Recall that

$$\text{dom}\left(\frac{f}{g}\right) = (\text{dom}(f) \cap \text{dom}(g)) \backslash \{z \in \text{dom}(g) \colon g(z) = 0\}.$$

8.13 Theorem (Continuity of roots.) *Let $p \in \mathbf{Z}_{\geq 1}$ and let $f_p(x) = x^{\frac{1}{p}}$ for all $x \in [0, \infty)$. Then f_p is continuous.*

Proof: First we show f_p is continuous at 0. Let $\{x_n\}$ be a sequence in $[0, \infty)$ such that $\{x_n\} \to 0$; i.e., such that $\{x_n\}$ is a null sequence. Then by the root theorem for null sequences (Theorem 7.19), $\left\{x_n^{\frac{1}{p}}\right\}$ is a null sequence; i.e., $\{f_p(x_n)\} = \left\{x_n^{\frac{1}{p}}\right\} \to 0 = f_p(0)$, so f_p is continuous at 0.

Next we show that f_p is continuous at 1. By the formula for a finite geometric series (3.72), we have for all $x \in [0, \infty)$

$$|x^p - 1| = \left|(x-1)\sum_{j=0}^{p-1} x^j\right| = |x-1|\sum_{j=0}^{p-1} x^j \geq |x-1|. \tag{8.14}$$

If we replace x by $y^{\frac{1}{p}}$ in (8.14), we get $|y-1| = |(y^{\frac{1}{p}})^p - 1| \geq |y^{\frac{1}{p}} - 1|$, i.e.,

$$|y^{\frac{1}{p}} - 1| \leq |y - 1| \text{ for all } y \in [0, \infty).$$

Let $\{y_n\}$ be a sequence in $[0, \infty)$. Then

$$|(y_n)^{\frac{1}{p}} - 1| \leq |y_n - 1| \text{ for all } n \in \mathbf{N},$$

so

$$\begin{aligned}
\{y_n\} \to 1 \implies & |y_n - 1| \to 0 \\
\implies & |(y_n)^{\frac{1}{p}} - 1| \to 0 \text{ (by comparison theorem for null sequences)} \\
\implies & \{(y_n)^{\frac{1}{p}}\} \to 1 \\
\implies & \{f_p(y_n)\} \to f_p(1).
\end{aligned}$$

Hence f_p is continuous at 1.

Finally we show that f_p is continuous at arbitrary $a \in (0, \infty)$. Let $a \in [0, \infty)$, and let $\{z_n\}$ be a sequence n $[0, \infty)$. Then

$$\begin{aligned}
\{z_n\} \to a \implies & \frac{1}{a}\{z_n\} \to \frac{1}{a}a = 1 \\
\implies & \left\{\frac{z_n}{a}\right\} \to 1
\end{aligned}$$

$$\begin{aligned}
&\implies \left\{\left(\frac{z_n}{a}\right)^{\frac{1}{p}}\right\} \to 1 \text{ (since } f_p \text{ is continuous at 1)}\\
&\implies a^{\frac{1}{p}}\left\{\left(\frac{z_n}{a}\right)^{\frac{1}{p}}\right\} \to a^{\frac{1}{p}}\cdot 1\\
&\implies \{(z_n)^{\frac{1}{p}}\} \to a^{\frac{1}{p}}\\
&\implies \{f_p(z_n)\} \to f_p(a).
\end{aligned}$$

Thus f_p is continuous at a. ‖

8.15 Definition (Composition of functions.) Let A, B, C, D be sets, and let $f{:}\, A \to B$, $g{:}\, C \to D$ be functions. We define a function $g \circ f$ by the rules:

$$\begin{aligned}
\text{domain } (g \circ f) &= \{x \in \text{dom} f{:}\, f(x) \in \text{dom}(g)\}\\
(g \circ f)(x) &= g\left(f(x)\right) \text{ for all } x \in \text{dom}(g \circ f).
\end{aligned}$$

8.16 Examples. Let $f{:}\,\mathbf{C} \to \mathbf{C}$, $g{:}\,\mathbf{C} \to \mathbf{C}$ be defined by

$$\begin{aligned}
f(z) &= z^2 + 1 \text{ for all } z \in \mathbf{C}\\
g(z) &= (1 + z^*) \text{ for all } z \in \mathbf{C}.
\end{aligned}$$

Then

$$\begin{aligned}
(f \circ g)(z) &= f\left(g(z)\right) = (1 + z^*)^2 + 1 = 1 + 2z^* + (z^*)^2 + 1\\
&= 2 + 2z^* + (z^*)^2,
\end{aligned}$$

and

$$(g \circ f)(z) = g\left(f(z)\right) = 1 + (z^2 + 1)^* = 1 + (z^*)^2 + 1 = 2 + (z^*)^2.$$

If $f{:}\,\mathbf{R} \to \mathbf{R}$ and $g{:}\,[-1, \infty) \to \mathbf{R}$ are defined by

$$f(x) = x^2 - 1 \text{ for all } x \in \mathbf{R}$$

and

$$g(x) = \sqrt{1 + x} \text{ for all } x \in [-1, \infty),$$

then

$$\begin{aligned}
(f \circ g)(x) &= (\sqrt{1 + x})^2 - 1 \text{ for all } x \in [-1, \infty)\\
&= 1 + x - 1 \text{ for all } x \in [-1, \infty)\\
&= x \text{ for all } x \in [-1, \infty)
\end{aligned}$$

and

$$(g \circ f)(x) = \sqrt{1 + (x^2 - 1)} = \sqrt{x^2} = |x| \text{ for all } x \in \mathbf{R}.$$

8.17 Theorem (Compositions of continuous functions.) *Let f, g be complex functions. If f is continuous at $a \in \mathbf{C}$, and g is continuous at $f(a)$, then $g \circ f$ is continuous at a.*

Proof: Let $\{x_n\}$ be a sequence in $\operatorname{dom}(g \circ f)$ such that $\{x_n\} \to a$. Then for all $n \in \mathbf{N}$, we have $x_n \in \operatorname{dom}(f)$ and $f(x_n) \in \operatorname{dom}(g)$. By continuity of f at a, $\{f(x_n)\} \to f(a)$, and by continuity of g at $f(a)$, $\{g(f(x_n))\} \to g(f(a))$. $\|$

8.18 Example. If $f(x) = \sqrt{x^2+3}$ for all $x \in \mathbf{R}$, then f is continuous (i.e., f is continuous at a for all $a \in \mathbf{R}$.)

8.19 Exercise. Let $f\colon \mathbf{N} \to \mathbf{C}$ be defined by $f(n) = n!$ for all $n \in \mathbf{N}$. Is f continuous?

8.3 Limits

8.20 Definition (Limit point.) Let S be a subset of $\mathbf{C}$ and let $a \in \mathbf{C}$. We say a is a *limit point* of S if there is a sequence f in $S \backslash \{a\}$ such that $f \to a$.

8.21 Example. Let $D(0,1) = \{z \in \mathbf{C}\colon |z| < 1\}$ be the unit disc, and let $\alpha \in \mathbf{C}$. We'll show that α is a limit point of $D(0,1)$ if and only if $|\alpha| \leq 1$.

Proof that (α is a limit point of $D(0,1)$) $\implies |\alpha| \leq 1$.
Suppose α is a limit point of $D(0,1)$. Then there is a sequence $\{a_n\}$ in $D(0,1) \setminus \{\alpha\}$ such that $\{a_n\} \to \alpha$. Since the absolute value function is continuous, it follows that $\{|a_n|\} \to |\alpha|$. Since $a_n \in D(0,1)$ we know that $|a_n| < 1$ (and hence $|a_n| \leq 1$.) for all $n \in \mathbf{N}$. By the inequality theorem for limits of sequences, $\lim\{|a_n|\} \leq 1$, i.e. $|\alpha| \leq 1$.

Proof that $(|\alpha| \leq 1) \implies \alpha$ is a limit point of $D(0,1)$.

Case 1: Suppose $0 < |\alpha| \leq 1$. Let $f_\alpha(n) = \dfrac{n}{n+1}\alpha$ for all $n \in \mathbf{Z}_{\geq 1}$. Then

$$|f_\alpha(n)| = \frac{n}{n+1}|\alpha| \leq \frac{n}{n+1} < 1 \text{ so } f_\alpha(n) \in D(0,1), \text{ and clearly } f_\alpha(n) \neq \alpha.$$

Now $\{f_\alpha(n)\}_{n\geq 1} = \left\{\dfrac{1}{1+\frac{1}{n}} \cdot \alpha\right\}_{n\geq 1} \to \alpha$, so α is a limit point of $D(0,1)$.

Case 2: $\alpha = 0$. This case is left to you.

8.22 Exercise. Supply the proof for Case 2 of example 8.21; i.e., show that 0 is a limit point of $D(0,1)$.

8.23 Example. The set $\mathbf{Z}$ has no limit points. Suppose $\alpha \in \mathbf{C}$, and there is a sequence f in $\mathbf{Z}\backslash\{\alpha\}$ such that $f \to \alpha$. Let $g(n) = f(n) - f(n+1)$ for all $n \in \mathbf{N}$. By the translation thoerem $g \to \alpha - \alpha = 0$; i.e., g is a null sequence. Let N_g be a precision function for g. Then for all $n \in \mathbf{N}$,

$$\begin{aligned} n \geq N_g\left(\frac{1}{2}\right) &\implies |g(n)| < \frac{1}{2} \\ &\implies |f(n) - f(n+1)| < \frac{1}{2}. \end{aligned}$$

Now $|f(n) - f(n+1)| \in \mathbf{N}$, so it follows that

$$n \geq N_g\left(\frac{1}{2}\right) \implies |f(n) - f(n+1)| = 0 \implies f(n) = f(n+1)$$

and hence

$$\alpha = \lim f = f\left(N_g\left(\frac{1}{2}\right)\right).$$

This contradicts the fact that $f(n) \in \mathbf{Z}\backslash\{\alpha\}$ for all $n \in \mathbf{N}$. $\|$

8.24 Definition (Limit of a function.) Let f be a complex function, and let a be a limit point of $\mathrm{dom}(f)$. We say that f *has a limit at* a or that $\lim_a f$ *exists* if there exists a function F with $\mathrm{dom}(F) = \mathrm{dom}(f) \cup \{a\}$ such that $F(z) = f(z)$ for all $z \in \mathrm{dom}(f)\backslash\{a\}$, and F is continuous at a. In this case we denote the value of $F(a)$ by $\lim_a f$ or $\lim_{z\to a} f(z)$. Theorem 8.30 shows that this definition makes sense. We will give some examples before proving that theorem.

8.25 Warning. Notice that $\lim_a f$ is defined only when a is a limit point of $\mathrm{dom}(f)$. For each complex number β, define a function $F_\beta : \mathbf{N} \cup \{\frac{1}{2}\} \to \mathbf{C}$ by

$$F_\beta(n) = \begin{cases} n! & \text{if } n \in \mathbf{N}, \\ \beta & \text{if } n = \frac{1}{2}, \end{cases}$$

Then F_β is continuous, and $F(n) = n!$ for all $n \in \mathbf{N}$. If I did not put the requirement that a be a limit point of $\mathrm{dom}(f)$ in the above definition, I'd have

$$\lim_{n\to\frac{1}{2}} n! = F_\beta(\frac{1}{2}) = \beta \text{ for all } \beta \in \mathbf{C}.$$

I certainly do not want this to be the case.

8.26 Example. Let $f(z) = \dfrac{z^2-1}{z-1}$ for all $z \in \mathbf{C}\backslash\{1\}$ and let $F(z) = z+1$ for all $z \in \mathbf{C}$. Then $f(z) = F(z)$ on $\mathbf{C}\backslash\{1\}$ and F is continuous at 1. Hence $\lim\limits_{1} f = F(1) = 2$.

8.27 Example. If $f(z) = \begin{cases} z & \text{for} \neq 1 \\ 3 & \text{for } z = 1 \end{cases}$, then $\lim\limits_{1} f = 1$, since the function $F : z \mapsto z$ agrees with f on $\mathbf{C}\backslash\{1\}$ and is continuous at 1.

8.28 Example. If f is continuous at a, and a is a limit point of domain f, then f has a limit at a, and

$$\lim_{a} f = f(a).$$

8.29 Example. Let $f(z) = \dfrac{z^*}{z}$ for all $z \in \mathbf{C}\setminus\{0\}$. Then f has no limit at 0.

Proof: Suppose there were a continuous function F on $\mathbf{C}$ such that $F(z) = f(z)$ on $\mathbf{C}\backslash\{0\}$. Let $\{a_n\} = \left\{\dfrac{i}{n+1}\right\}$ and $\{b_n\} = \left\{\dfrac{1}{n+1}\right\}$. Then $\{a_n\} \to 0$ and $\{b_n\} \to 0$ and so

$$F(0) = \lim\{F(a_n)\} = \lim\left\{\frac{\frac{-i}{n+1}}{\frac{i}{n+1}}\right\} = \lim\{-1\} = -1$$

and also

$$F(0) = \lim\{F(b_n)\} = \lim\left\{\frac{\frac{1}{n+1}}{\frac{1}{n+1}}\right\} = \lim\{1\} = 1.$$

Hence we get the contradiction $-1 = 1$. |||

8.30 Theorem (Uniqueness of limits.) *Let f be a complex function, and let a be a limit point of* $\operatorname{dom}(f)$. *Suppose F, G are two functions each having domain* $\operatorname{dom}(f) \cup \{a\}$, *and each continuous at a, and satisfying $f(z) = F(z)$ $= G(z)$ for all $z \in \operatorname{dom}(f)\backslash\{a\}$. Then $F(a) = G(a)$.*

Proof: $F - G$ is continuous at a, and $F - G = 0$ on $\operatorname{dom}(f)\backslash\{a\}$. Let $\{a_n\}$ be a sequence in $\operatorname{dom}(f)\backslash\{a\}$ such that $\{a_n\} \to a$. Since $F - G$ is continuous at a, we have

$$\{(F-G)(a_n)\} \to (F-G)(a);$$

i.e.,

$$\{0\} \to F(a) - G(a),$$

so $F(a) - G(a) = 0$; i.e., $F(a) = G(a)$. ‖

8.31 Exercise. Investigate the following limits. (Give detailed reasons for your answers). In this exercise you should not conclude from the fact that I've written $\lim_{w \to b} f(w)$ that the implied limit exists.

a) $\lim_{t \to 4} t^{\frac{1}{2}}$.

b) $\lim_{n \to 2} n!$.

c) $\lim_{z \to 0} |z|^2 \left(\frac{1}{z} - \frac{1}{z^*} \right)$.

d) $\lim_{z \to a} \frac{\frac{1}{z} - \frac{1}{a}}{z - a}$. (Here $a \in \mathbf{C} \setminus \{0\}$).

e) $\lim_{t \to 0} \frac{\sqrt{t+4} - 2}{t}$.

8.32 Theorem. *Let f be a complex function and let a be a limit point of $\text{dom}(f)$. Then f has a limit at a if and only if there exists a number L in $\mathbf{C}$ such that for every sequence y in $\text{dom}(f) \backslash \{a\}$*

$$y \to a \implies f \circ y \to L. \tag{8.33}$$

In this case, $L = \lim_a f$.

Proof: Suppose f has a limit at a, and let F be a continuous function with $\text{dom}(F) = \text{dom}(f) \cup \{a\}$, and $F(z) = f(z)$ for all $z \in \text{dom}(f) \backslash \{a\}$. Let y be a sequence in $\text{dom}(f) \backslash \{a\}$ such that $\{y_n\} \to a$. Then y is a sequence in $\text{dom}(F)$, so by continuity of F,

$$\{f(y_n)\} = \{F(y_n)\} \to F(a).$$

Hence, condition (8.33) holds with $L = F(a)$.

Conversely, suppose there is a number L such that

$$\text{for every sequence } y \text{ in } \text{dom}(f) \backslash \{a\}, \ (y \to a \implies f \circ y \to L.). \tag{8.34}$$

Define $F\colon \mathrm{dom}(f) \cup \{a\} \to \mathbf{C}$ by

$$F(z) = \begin{cases} f(z) & \text{if } z \in \mathrm{dom}(f)\backslash\{a\} \\ L & \text{if } z = a. \end{cases}$$

I need to show that F is continuous at a. Let z be a sequence in $\mathrm{dom}(F)$ such that $z \to a$. I want to show that $F \circ z \to L$.

Let w be a sequence in $\mathrm{dom}(f) \setminus \{a\}$ such that $w \to a$. (Such a sequence exists because a is a limit point of $\mathrm{dom}(f)$). Define a sequence y in $\mathrm{dom}(f)\backslash\{a\}$ by

$$y(n) = \begin{cases} z(n) & \text{if } z(n) \neq a \\ w(n) & \text{if } z(n) = a. \end{cases}$$

Let $N_{z-\tilde{a}}$ and $N_{w-\tilde{a}}$ be precision functions for $z - \tilde{a}$ and $w - \tilde{a}$ respectively. Let

$$M(\varepsilon) = \max(N_{z-\tilde{a}}(\varepsilon), N_{w-\tilde{a}}(\varepsilon)) \text{ for all } \varepsilon \in \mathbf{R}^+.$$

Then M is a precision function for $y - \tilde{a}$, since for all $\varepsilon \in \mathbf{R}^+$ and all $n \in \mathbf{N}$,

$$\begin{aligned} &n \geq M(\varepsilon) \\ &\implies \begin{cases} n \geq N_{z-\tilde{a}}(\varepsilon) \implies |z(n) - a| < \varepsilon \implies |y(n) - a| < \varepsilon & \text{if } z(n) \neq a \\ n \geq N_{w-\tilde{a}}(\varepsilon) \implies |w(n) - a| < \varepsilon \implies |y(n) - a| < \varepsilon & \text{if } z(n) = a. \end{cases} \end{aligned}$$

Hence $y \to a$, and by assumption (8.34), it follows that $f \circ y \to L$. I now claim that $F \circ z \to L$, and in fact any precision function P for $f \circ y - \tilde{L}$ is a precision function for $F \circ z - \tilde{L}$. For all $\varepsilon \in \mathbf{R}^+$ and all $n \in \mathbf{N}$,

$$\begin{aligned} n \geq P(\varepsilon) &\implies |f(y(n)) - L| < \varepsilon \\ &\implies \begin{cases} |F(z(n)) - L| = |f(y(n)) - L| < \varepsilon & \text{if } z(n) \neq a \\ |F(z(n)) - L| = |F(a) - L| = 0 < \varepsilon & \text{if } z(n) = a. \end{cases} \end{aligned}$$

This completes the proof. |||

8.35 Example. Let

$$f(z) = f(x + iy) = f((x, y)) = \frac{xy|x|}{x^4 + y^2} + iy \text{ for all } z \in \mathbf{C}\backslash\{0\}.$$

I want to determine whether f has a limit at 0, i.e., I want to know whether there is a number L such that for every sequence z in $\mathbf{C}\backslash\{0\}$

$$z \to 0 \implies f(z) \to L.$$

If $x \in \mathbf{R}^+$ and $\gamma \in \mathbf{Q}^+$ then

$$f((x,x^\gamma)) = \frac{x \cdot x \cdot x^\gamma}{x^4 + x^{2\gamma}} + ix^\gamma = \begin{cases} \dfrac{x^{\gamma+2}}{x^4(1+x^{2(\gamma-2)})} + ix^\gamma = \dfrac{x^{\gamma-2}}{1+x^{2(\gamma-2)}} + ix^\gamma \\ \dfrac{x^{\gamma+2}}{x^{2\gamma}(x^{2(2-\gamma)}+1)} + ix^\gamma = \dfrac{x^{2-\gamma}}{x^{2(2-\gamma)}+1} + ix^\gamma \end{cases}$$

Since $|2-\gamma|$ is either $2-\gamma$ or $\gamma-2$, we have

$$f((x,x^\gamma)) = \frac{x^{|2-\gamma|}}{1+x^{2|2-\gamma|}} + ix^\gamma.$$

For each $\gamma \in \mathbf{Q}^+$, define a sequence z_γ by

$$z_\gamma : n \mapsto \left(\frac{1}{n}, \frac{1}{n^\gamma}\right) \text{ for all } n \in \mathbf{Z}^+.$$

Then $z_\gamma \to 0$, and

$$f(z_\gamma(n)) = \frac{\frac{1}{n^{|2-\gamma|}}}{1+\frac{1}{n^{2|2-\gamma|}}} + \frac{i}{n^\gamma}.$$

Hence

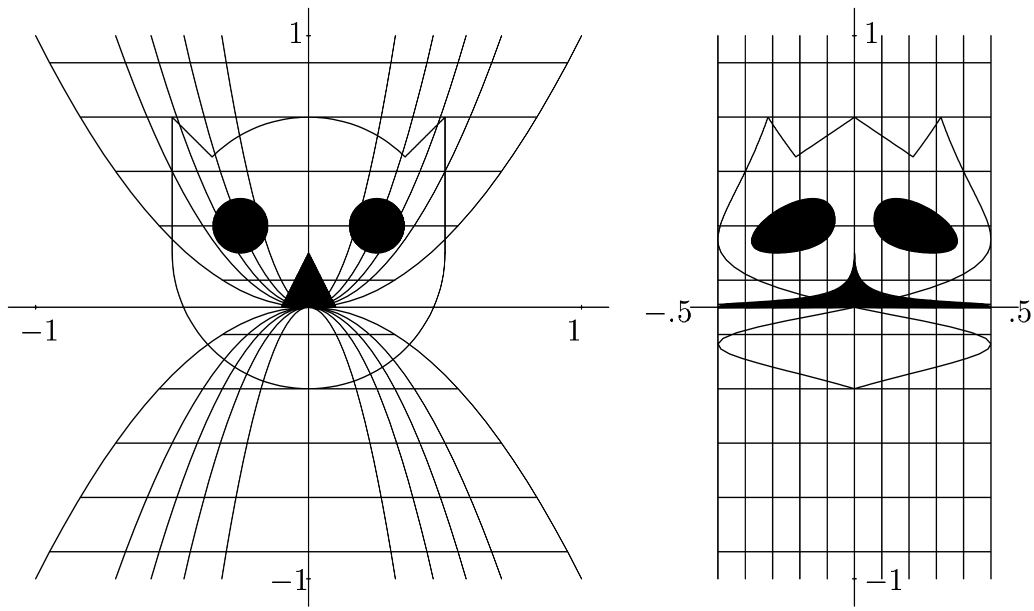
$$\begin{aligned} f \circ z_\gamma &\to 0 \quad \text{if} \quad \gamma \neq 2 \\ f \circ z_\gamma &\to \frac{1}{2} \quad \text{if} \quad \gamma = 2. \end{aligned}$$

It follows that f has no limit at 0.

Let $y_0 \in \mathbf{R}$. It is clear that f maps points on the horizontal line $y = y_0$ to other points on the line $y = y_0$. I'll now look at the image of the parabola $y = cx^2$ under f.

$$f(x+icx^2) = \frac{xcx^2|x|}{x^4+c^2x^4} + icx^2 = \frac{|x|}{x}\left(\frac{c}{1+c^2}\right) + icx^2 \text{ for } x \neq 0.$$

So f maps the right half of the parabola $y = cx^2$ into the vertical line $x = \dfrac{c}{1+c^2}$, and f maps the left half of the parabola to the line $x = \dfrac{-c}{1+c^2}$. Parabolas with $c > 0$ get mapped to the upper half plane, and parabolas with $c < 0$ get mapped to the lower half plane. The figure below shows some parabolas and horizontal lines and their images under f.



Discontinuous Image of a Cat

8.36 Entertainment. Explain how the cat's nose in the above picture gets stretched, while its cheeks get pinched to a point. (Hint: The figure shows the images of some parabolas $y = cx^2$ where $|c| \geq 1$. What do the images of the parabolas $y = cx^2$ look like when $|c| < 1$?)

8.37 Example. It isn't quite true that "the limit of the sum is the sum of the limits." Let

$$\begin{aligned} f(x) &= \sqrt{x} \text{ for } x \in [0, \infty) \\ g(x) &= \sqrt{-x} \text{ for } x \in (-\infty, 0]. \end{aligned}$$

Then from the continuity of the square root function and the composition theorem,

$$\lim_0 f = 0 = \lim_0 g.$$

But $\lim_0 (f+g)$ does not exist, since $\text{dom}(f+g) = \{0\}$ and 0 is not a limit point of $\text{dom}(f+g)$.

8.38 Theorem (Sum and product theorem.) *Let f, g be complex functions and let a be a limit point of* $\text{dom}(f) \cap \text{dom}(g)$. *If* $\lim_a f$ *and* $\lim_a g$ *exist,* *then* $\lim_a(f+g)$, $\lim_a(f-g)$ *and* $\lim_a(f\cdot g)$ *all exist and*

$$\begin{aligned}\lim_a(f+g) &= \lim_a f + \lim_a g,\\ \lim_a(f-g) &= \lim_a f - \lim_a g,\\ \lim_a(f\cdot g) &= \lim_a f\cdot\lim_a g.\end{aligned}$$

If a *is a limit point of* $\operatorname{dom}\left(\dfrac{f}{g}\right)$ *and* $\lim_a g \neq 0$ *then* $\lim_a \dfrac{f}{g}$ *exists and* $\lim_a\left(\dfrac{f}{g}\right) = \dfrac{\lim_a f}{\lim_a g}$.

Proof: Suppose that $\lim_a f$ and $\lim_a g$ exist. Let x be any sequence in $\operatorname{dom}(f+g)\backslash\{a\}$ such that $x \to a$. Then x is a sequence in both $\operatorname{dom}(f)$ and $\operatorname{dom}(g)$, so

$$\lim\{f(x_n)\} = \lim_a f \text{ and } \lim\{g(x_n)\} = \lim_a g.$$

By the sum theorem for limits of sequences,

$$\lim\{(f+g)(x_n)\} = \lim\{f(x_n)\} + \lim\{g(x_n)\} = \lim_a f + \lim_a g.$$

Hence $f+g$ has a limit at a, and $\lim_a(f+g) = \lim_a f + \lim_a g$.

The other parts of the theorem are proved similarly, and the proofs are left to you. |||

8.39 Exercise. Prove the product theorem for limits; i.e., show that if f, g are complex functions such that f and g have limits at $a \in \mathbf{C}$, and if a is a limit point of $\operatorname{dom}(f)\cap\operatorname{dom}(g)$, then $f\cdot g$ has a limit at a and

$$\lim_a(f\cdot g) = \lim_a f\cdot\lim_a g.$$

8.40 Definition (Bounded set and function.) A subset S of $\mathbf{C}$ is *bounded* if S is contained in some disc $\bar{D}(0,B)$; i.e., if there is a number B in $\mathbf{R}^+$ such that $|s| \leq B$ for all $s \in S$. We call such a number B a *bound* for S.

Now suppose $f: U \to \mathbf{C}$ is a functiom from some set U to $\mathbf{C}$ and A is a subset of U. We say *f is bounded on A* if $f(A)$ is a bounded set, and any bound for $f(A)$ is called a *bound for f on A*. Thus a number $B \in \mathbf{R}^+$ is a bound for f on A if and only if

$$|f(a)| \leq B \text{ for all } a \in A.$$

We say *f is bounded* if f is bounded on $\text{dom}(f)$. If f is not bounded on A, we say *f is unbounded on A*.

8.41 Examples. The definition of bounded sequence given in 7.41 is a special case of the definition just given for bounded function.

Let $f(z) = \dfrac{1}{1+z^2}$ for all $z \in \mathbf{C}\backslash\{\pm i\}$. Then f is bounded on $\mathbf{R}$ since

$$|f(z)| \leq \frac{1}{1+z^2} \leq 1 \text{ for all } z \in \mathbf{R}.$$

However, f is not a bounded function, since

$$\begin{aligned} \left| f\left(i + \frac{1}{n}\right) \right| &= \left| \frac{1}{1 + \left(-1 + \frac{2i}{n} + \frac{1}{n^2}\right)} \right| = \left| \frac{n}{2i + \frac{1}{n}} \right| \\ &= \frac{n}{\sqrt{4 + \frac{1}{n^2}}} \geq \frac{n}{\sqrt{5}} \end{aligned}$$

for all $n \in \mathbf{Z}_{\geq 1}$.

Let

$$F(z) = \begin{cases} \dfrac{xy|x|}{x^4 + y^2} & \text{for } z \in \mathbf{C}\backslash\{0\} \\ 0 & \text{for } z = 0. \end{cases}$$

(F is the real part of the discontinuous function from example 8.35.)

I claim F is bounded by 1. For all $a, b \in \mathbf{R}$,

$$|a|\ |b| \leq \max(|a|, |b|)^2 \leq a^2 + b^2.$$

(NOTE: $\max(|a|, |b|)^2$ is either a^2 or b^2.) Hence if $(a, b) \neq (0, 0)$, then

$$\left| \frac{ab}{a^2 + b^2} \right| \leq 1.$$

To prove my claim, apply this result with $a = x|x|$ and $b = y$.

8.42 Exercise. Show that

$$\left|\frac{ab}{a^2+b^2}\right| \le \frac{1}{2}$$

for all $(a,b) \in \mathbf{R}\times\mathbf{R}\backslash\{(0,0)\}$, and that equality holds if and only if $|a| = |b|$. (This shows that $\frac{1}{2}$ is a bound for the function F in the previous example.) HINT: Consider $(|a| - |b|)^2$.

8.43 Exercise. For each of the functions f below:

1) Decide whether f is bounded, and if it is, find a bound for f.

2) Decide whether f is bounded on $\text{dom}(f) \cap D(0,1)$, and if it is, find a bound for f on $\text{dom}(f) \cap D(0,1)$.

3) Decide whether f has a limit at 0, and if it does, find $\lim\limits_{0} f$.

Here $z = (x,y) = x + iy$.

a) $f(z) = \dfrac{x^2}{x^2+y^2}$ for all $z \in \mathbf{C}\backslash\{0\}$.

b) $f(z) = \dfrac{x^2 y}{x^2+y^2}$ for all $z \in \mathbf{C}\backslash\{0\}$.

c) $f(z) = \dfrac{(z^*)^2}{z^2}$ for all $z \in \mathbf{C}\backslash\{0\}$.

d) $f(x) = \dfrac{x^2+x^6}{x^2+x^4}$ for all $x \in \mathbf{R}\backslash\{0\}$.

e) $f(x) = \dfrac{\sqrt{x+1}-1}{x}$ for all $x \in [-1,\infty)\backslash\{0\}$.

Chapter 9

Properties of Continuous Functions

9.1 Extreme Values

9.1 Definition (Maximum, Minimum.) Let $f: S \to \mathbf{R}$ be a function from a set S to $\mathbf{R}$, and let $a \in S$. We say that f *has a maximum at* a if $f(a) \geq f(x)$ for all $x \in S$, and we say f *has a minimum at* a if $f(a) \leq f(x)$ for all $x \in S$.

9.2 Definition (Maximizing set.) Let $f: S \to \mathbf{R}$ be a function and let M be a subset of S. We say M is a *maximizing set* for f on S if for each $x \in S$ there is a point $m \in M$ such that $f(m) \geq f(x)$.

9.3 Examples. If f has a maximum at a then $\{a\}$ is a maximizing set for f on S.

If M is a maximizing set for f on S, and $M \subset B \subset S$, then B is also a maximizing set for f on S.

If $f: S \to \mathbf{R}$ is any function (with $S \neq \emptyset$), then S is a maximizing set for f on S, so every function with non-empty domain has a maximizing set.

Let

$$f(z) = \begin{cases} \frac{1}{|z|} & \text{for } z \neq 0 \\ 0 & \text{for } z = 0. \end{cases}$$

Then every disc $D(0,\varepsilon)$ is a maximizing set for f, since if $z \in \mathbf{C}\backslash\{0\}$ we can find $n \in \mathbf{N}$ with $n > \max\left(\frac{1}{\varepsilon}, \frac{1}{|z|}\right)$; then $n > \frac{1}{\varepsilon}$, so $\frac{1}{n} < \varepsilon$, so $\frac{1}{n} \in D(0,\varepsilon)$ and $f\left(\frac{1}{n}\right) = n > \frac{1}{|z|} = f(z)$. This argument shows that $\left\{\frac{1}{n+1} : n \in \mathbf{N}\right\}$ is also a maximizing set for f.

9.4 Remark. Let S be a set, and let $f: S \to \mathbf{R}$, and let M be a subset of S. If M is *not* a maximizing set for f on S, then there is some point $x \in S$ such that $f(x) > f(m)$ for all $m \in M$.

9.5 Lemma. *Let S be a set, let $f: S \to \mathbf{R}$ be a function, and let M be a maximizing set for f on S. If $M = A \cup B$, then at least one of A, B is a maximizing set for f on S.*

Proof: Suppose $A \cup B$ is a maximizing set for f on S, but A is not a maximizing set for f on S. Then there is some $s \in S$ such that for all $a \in A$, $f(s) > f(a)$. Since $A \cup B$ is a maximizing set for f on S, there is an element t in $A \cup B$ such that $f(t) \geq f(s)$, so $f(t) > f(a)$ for all $a \in A$, so $t \notin A$, so $t \in B$. Now, for every $x \in S$ there is an element c in $A \cup B$ with $f(c) \geq f(x)$. If $c \in A$, then the element $t \in B$ satisfies $f(t) > f(c) \geq f(x)$ so there is some element $u \in B$ with $f(u) \geq f(x)$ (if $c \in A$, take $u = t$; if $c \in B$, take $u = c$.) Hence B is a maximizing set for f on S. |||

9.6 Theorem (Extreme value theorem.) *Let $a, b \in \mathbf{R}$ with $a < b$ and let $f: [a,b] \to \mathbf{R}$ be a continuous function. Then f has a maximum and a minimum on $[a,b]$.*

Proof: We will construct a binary search sequence $\{[a_n, b_n]\}$ with $[a_0, b_0] = [a,b]$ such that each interval $[a_n, b_n]$ is a maximizing set for f on $[a,b]$. We put

$$\begin{aligned} [a_0, b_0] &= [a,b] \\ [a_{n+1}, b_{n+1}] &= \begin{cases} \left[a_n, \frac{a_n+b_n}{2}\right] & \text{if } \left[a_n, \frac{a_n+b_n}{2}\right] \text{ is a maximizing set for } f \\ \left[\frac{a_n+b_n}{2}, b_n\right] & \text{otherwise.} \end{cases} \end{aligned}$$

By the preceding lemma (and induction), we see that each interval $[a_n, b_n]$ is a maximizing set for f on $[a,b]$. Let c be the number such that $\{[a_n, b_n]\} \to c$

and let $s \in [a,b]$. Since $[a_n,b_n]$ is a maximizing set for f on $[a,b]$, there is a number $s_n \in [a_n,b_n]$ with $f(s_n) \geq f(s)$. Since

$$a_n \leq c \leq b_n \text{ and } a_n \leq s_n \leq b_n,$$

we have $|s_n - c| \leq |b_n - a_n| = \dfrac{(b-a)}{2^n}$, so $\{s_n\} \to c$. By continuity of f, $\{f(s_n)\} \to f(c)$. Since $f(s_n) \geq f(s)$, it follows by the inequality theorem for limits that

$$f(c) = \lim\{f(s_n)\} \geq f(s).$$

Hence c is a maximum point for f on $[a,b]$. This shows that f has a maximum. Since $-f$ is also a continuous function on $[a,b]$, $-f$ has a maximum on $[a,b]$; i.e., there is a point $p \in [a,b]$ such that $-f(p) \geq -f(x)$ for all $x \in [a,b]$. Then $f(p) \leq f(x)$ for all $x \in [a,b]$, so f has a minimum at p. |||

9.7 Definition (Upper bound.) Let S be a subset of $\mathbf{R}$, let $b, B \in \mathbf{R}$. We say B is an *upper bound* for S if $x \leq B$ for all $x \in S$, and we say b is a *lower bound* for S if $b \leq x$ for all $x \in S$.

9.8 Remark. If S is a bounded subset of R and B is a bound for S, then B is an upper bound for S and $-B$ is a lower bound for S, since

$$|x| \leq B \implies -B \leq x \leq B.$$

Conversely, if a subset S of $\mathbf{R}$ has an upper bound B and a lower bound b,then S is bounded, and $\max(|b|,|B|)$ is a bound for S, since

$$b \leq x \leq B \implies -\max(|b|,|B|) \leq -|b| \leq b \leq x \leq B \leq |B| \leq \max(|b|,|B|).$$

9.9 Theorem (Boundedness theorem.) *Let $a, b \in \mathbf{R}$ with $a < b$ and let $f\colon [a,b] \to \mathbf{R}$ be a continuous function. Then f is bounded on $[a,b]$.*

Proof: By the extreme value theorem, there are points $p, q \in [a,b]$ such that

$$f(p) \leq f(x) \leq f(q) \text{ for all } x \in [a,b].$$

Hence $f([a,b])$ has an upper bound and a lower bound, so $f([a,b])$ is bounded. |||

9.10 Exercise. Give examples of the functions described below, or explain why no such function exists. Describe your functions by formulas if you can, but pictures of graphs will do if a formula seems too complicated.

a) $f\colon [0,1] \to \mathbf{R}$, f is not bounded.

b) $g\colon (0,1) \to \mathbf{R}$, g is continuous, g is not bounded.

c) $h\colon [0,\infty) \to \mathbf{R}$, h is continuous, h is not bounded.

d) $k\colon [0,\infty) \to \mathbf{R}$, k is strictly increasing, k is continuous, k is bounded.

e) $l\colon [0,1] \to \mathbf{R}$, l is continuous, l is not bounded.

9.2 Intermediate Value Theorem

9.11 Theorem (Intermediate Value Theorem.) *Let $a, b \in \mathbf{R}$ with $a < b$, and let $f\colon [a,b] \to \mathbf{R}$ be a continuous function. Suppose $f(a) < 0 < f(b)$. Then there is some point $c \in (a,b)$ with $f(c) = 0$.*

Proof: We will construct a binary search sequence $[a_n, b_n]$ with $[a_0, b_0] = [a, b]$ such that

$$f(a_n) \leq 0 \leq f(b_n) \text{ for all } n. \tag{9.12}$$

Let

$$\begin{aligned} [a_0, b_0] &= [a, b] \\ [a_{n+1}, b_{n+1}] &= \begin{cases} \left[a_n, \frac{a_n+b_n}{2}\right] & \text{if } f\left(\frac{a_n+b_n}{2}\right) \geq 0 \\ \left[\frac{a_n+b_n}{2}, b_n\right] & \text{if } f\left(\frac{a_n+b_n}{2}\right) < 0. \end{cases} \end{aligned}$$

This is a binary search sequence satisfying condition (9.12).

Let c be the number such that $\{[a_n, b_n]\} \to c$. Then $\{a_n\} \to c$ and $\{b_n\} \to c$ (cf theorem 7.87), so by continuity of f, $\{f(a_n)\} \to f(c)$ and $\{f(b_n)\} \to f(c)$. Since $f(b_n) \geq 0$ for all n, it follows by the inequality theorem that $f(c) = \lim\{f(b_n)\} \geq 0$, and since $f(a_n) \leq 0$, we have $f(c) = \lim\{f(a_n)\} \leq 0$. Hence, $f(c) = 0$. |||

9.13 Exercise (Intermediate value theorem.) Let $a, b \in \mathbf{R}$ with $a < b$ and let $f : [a,b] \to \mathbf{R}$ be a continuous function with $f(a) < f(b)$. Let y be a number in the interval $(f(a), f(b))$. Show that there is some $c \in (a,b)$ with $f(c) = y$. (Use theorem 9.11. Do not reprove it.)

9.14 Notation (x is between a and b.) Let $a, b, x \in \mathbf{R}$. I say x is *between* a and b if either $a < x < b$ or $b < x < a$.

9.15 Corollary (Intermediate value theorem.) *Let $a, b \in \mathbf{R}$ with $a < b$. Let $f: [a, b] \to \mathbf{R}$ be a continuous function with $f(a) \neq f(b)$. If y is any number between $f(a)$ and $f(b)$, then there is some $c \in (a, b)$ such that $f(c) = y$. In particular, if $f(a)$ and $f(b)$ have opposite signs, there is a number $c \in (a, b)$ with $f(c) = 0$.*

Proof: By exercise 9.13, the result holds when $f(a) < f(b)$. If $f(a) > f(b)$, let $g = -f$. Then g is continuous on $[a, b]$ and $g(a) < g(b)$, so by exercise 9.13 there is a $c \in (a, b)$ with $g(c) = 0$, so $-f(c) = 0$ so $f(c) = 0$. ‖

9.16 Example. Let A, B, C, D be real numbers with $A \neq 0$, and let

$$f(x) = Ax^3 + Bx^2 + Cx + D.$$

We will show that there is a number $c \in \mathbf{R}$ such that $f(c) = 0$. Suppose, in order to get a contradiction, that no such number c exists, and let

$$g(x) = \frac{f(-x)}{f(x)} = \frac{-Ax^3 + Bx^2 - Cx + D}{Ax^3 + Bx^2 + C + D} \text{ for all } x \in \mathbf{R}.$$

(I use the fact that $f(x)$ has no zeros here.) Then

$$\begin{aligned} \lim\{g(n)\}_{n\geq 1} &= \lim\left\{\frac{-A + \frac{B}{n} - \frac{C}{n^2} + \frac{D}{n^3}}{A + \frac{B}{n} + \frac{C}{n^2} + \frac{D}{n^3}}\right\}_{n\geq 1} \\ &= \frac{-A + 0 + 0 + 0}{A + 0 + 0 + 0} = -1. \end{aligned}$$

It follows that $g(n) < 0$ for some n, so $f(-n)$ and $f(n)$ have opposite signs for some n, and g is continuous on $[-n, n]$, so by the intermediate value theorem, $g(c) = 0$ for some $c \in (-n, n)$, contradicting the assumption that g is never zero.

9.17 Exercise. Give examples of the requested functions, or explain why no such function exists. Describe your functions by formulas if you can, but pictures of graphs will do if a formula seems too complicated.

a) $f: [0, 1] \to \mathbf{R}$, f has no maximum.

b) $g: [0, \infty) \to \mathbf{R}$, g is continuous, g has no maximum.

c) $k: [0, \infty) \to \mathbf{R}$, k is continuous, k has no maximum or minimum.

d) $l\colon (0,1) \to \mathbf{R}$, l is bounded and continuous, l has no maximum.

9.18 Exercise. Let $f(x) = x^3 - 3x + 1$. Prove that the equation $f(x) = 0$ has at least three solutions in $\mathbf{R}$.

9.19 Exercise. Let F be a continuous function from $\mathbf{R}$ to $\mathbf{R}$ such that

a) For all $x \in \mathbf{R}$, $\big((F(x) = 0) \iff (x^2 = 1)\big)$.

b) $F(2) > 0$.

Prove that $F(4) > 0$.

9.20 Note. The intermediate value theorem was proved independently by Bernhard Bolzano in 1817 [42], and Augustin Cauchy in 1821[23, pp 167-168]. The proof we have given is almost identical with Cauchy's proof.

The extreme value theorem was proved by Karl Weierstrass circa 1861.

Chapter 10

The Derivative

10.1 Derivatives of Complex Functions

You are familiar with derivatives of functions from **R** to **R**, and with the motivation of the definition of derivative as the slope of the tangent to a curve. For complex functions, the geometrical motivation is missing, but the definition is formally the same as the definition for derivatives of real functions.

10.1 Definition (Derivative.) Let f be a complex valued function with $\text{dom}(f) \subset \mathbf{C}$, let a be a point such that $a \in \text{dom}(f)$, and a is a limit point of $\text{dom}(f)$. We say f is *differentiable at* a if the limit

$$\lim_{z \to a} \frac{f(z) - f(a)}{z - a}$$

exists. In this case, we denote this limit by $f'(a)$ and call $f'(a)$ the *derivative of* f *at* a.

By the definition of limit, we can say that f is differentiable at a if $a \in \text{dom}(f)$, and a is a limit point of $\text{dom}(f)$ and there exists a function $D_a f : \text{dom}(f) \to \mathbf{C}$ such that $D_a f$ is continuous at a, and such that

$$D_a f(z) = \frac{f(z) - f(a)}{z - a} \text{ for all } z \in \text{dom}(f) \backslash \{a\}, \tag{10.2}$$

and in this case $f'(a)$ is equal to $D_a f(a)$.

It is sometimes useful to rephrase condition (10.2) as follows: f is differentiable at a if $a \in \text{dom}(f)$, a is a limit point of $\text{dom}(f)$, and there is a function $D_a f \colon \text{dom} f \to \mathbf{C}$ such that $D_a f$ is continuous at a, and

$$f(z) = f(a) + (z-a)D_a f(z) \text{ for all } z \in \text{dom}(f). \tag{10.3}$$

In this case, $f'(a) = D_a f(a)$.

10.4 Remark. It follows immediately from (10.3) that if f is differentiable at a, then f is continuous at a.

10.5 Example. Let $f \colon \mathbf{C} \to \mathbf{C}$ be given by

$$f \colon z \mapsto z^2,$$

and let $a \in \mathbf{C}$. Then for all $z \neq a$,

$$\frac{f(z) - f(a)}{z - a} = \frac{z^2 - a^2}{z - a} = z + a.$$

If we define $D_a f \colon \mathbf{C} \to \mathbf{C}$ by

$$D_a f(z) = z + a \text{ for all } z \in \mathbf{C},$$

then $D_a f$ is continuous at a, so f is differentiable at a and

$$f'(a) = D_a f(a) = a + a = 2a \text{ for all } a \in \mathbf{C}.$$

We could also write this calculation as

$$\lim_{z \to a} \frac{f(z) - f(a)}{z - a} = \lim_{z \to a} \frac{z^2 - a^2}{z - a} = \lim_{z \to a} z + a = a + a = 2a.$$

Hence f is differentiable at a and $f'(a) = 2a$ for all $a \in \mathbf{C}$.

10.6 Example. Let $v(z) = \dfrac{1}{z}$ for $z \in \mathbf{C}\backslash\{0\}$ and let $a \in \mathbf{C}\backslash\{0\}$. Then for all $z \in \mathbf{C}\backslash\{a\}$

$$\frac{v(z) - v(a)}{z - a} = \frac{\frac{1}{z} - \frac{1}{a}}{z - a} = \frac{a - z}{za(z - a)} = -\frac{1}{za}.$$

Let $D_a v\colon \mathbf{C}\backslash\{0\} \to \mathbf{C}$ be defined by

$$D_a v(z) = -\frac{1}{za} \text{ for all } z \in \mathbf{C}\backslash\{0\}.$$

Then $D_a v$ is continuous at a, so v is differentiable at a, and

$$v'(a) = D_a v(a) = -\frac{1}{a^2}$$

for all $a \in \mathbf{C}\backslash\{0\}$.

10.7 Warning. The function $D_a f$ should not be confused with f'. In the example above

$$D_a v(z) = -\frac{1}{za}, \quad v'(z) = \frac{-1}{z^2}.$$

Also it is not good form to say

$$D_a f(z) = \frac{f(z) - f(a)}{z - a} \tag{10.8}$$

without specifying the condition "for $z \neq a$," since someone reading (10.8) would assume $D_a f$ is undefined at a.

10.9 Example. Let $f(z) = z^*$ for all $z \in \mathbf{C}$, and let $a \in \mathbf{C}$. Let

$$D_a f(z) = \frac{f(z) - f(a)}{z - a} = \frac{z^* - a^*}{z - a} \text{ for all } z \in \mathbf{C} \setminus \{a\}.$$

I claim that $D_a f$ does not have a limit at a, and hence f is a nowhere differentiable function.

Let

$$\{a_n\}_{n\geq 1} = \left\{a + \frac{1}{n}\right\}_{n\geq 1}, \{b_n\}_{n\geq 1} = \left\{a + \frac{i}{n}\right\}_{n\geq 1}.$$

Then $\{a_n\}_{n\geq 1}$ and $\{b_n\}_{n\geq 1}$ are sequences in $\mathrm{dom}(f)\backslash\{a\}$ both of which converge to a. For all $n \in \mathbf{Z}_{\geq 1}$,

$$\begin{aligned} D_a f(a_n) &= \frac{\left(a + \frac{1}{n}\right)^* - a^*}{a + \frac{1}{n} - a} = \frac{\frac{1}{n}}{\frac{1}{n}} = 1, \\ D_a f(b_n) &= \frac{\left(a + \frac{i}{n}\right)^* - a^*}{a + \frac{i}{n} - a} = \frac{\frac{-i}{n}}{\frac{i}{n}} = -1, \end{aligned}$$

so $\{D_a f(a_n)\}_{n\geq 1} \to 1$ and $\{D_a f(b_n)\}_{n\geq 1} \to -1$, and hence $D_a f$ does not have a limit at a.

10.10 Exercise. Investigate the following functions for differentiability at an arbitrary point $a \in \mathbf{C}$. Calculate the derivatives of any differentiable functions.

a) $f(z) = Az + B \qquad A, B$ are given complex numbers.

b) $g(z) = \dfrac{1}{(z+i)^2} \qquad z \in \mathbf{C}\backslash\{-i\}.$

c) $h(z) = \text{Re}(z)$, i.e. $h(x+iy) = x$.

10.11 Theorem (Sum theorem for differentiable functions.) *Let f, g be complex functions, and suppose f and g are differentiable at $a \in \mathbf{C}$. Suppose a is a limit point of* $\text{dom}(f) \cap \text{dom}(g)$. *Then $f+g$ is differentiable at a and $(f+g)'(a) = f'(a) + g'(a)$.*

Proof: Since f, g are differentiable at a, there are functions $D_af \colon \text{dom}(f) \to \mathbf{C}$, $D_ag \colon \text{dom}(g) \to g$ such that D_af, D_ag are continuous at a, and

$$\begin{aligned} f(z) &= f(a) + (z-a)D_af(z) \text{ for all } z \in \text{dom}(f) \\ g(z) &= g(a) + (z-a)D_ag(z) \text{ for all } z \in \text{dom}(g). \end{aligned}$$

It follows that

$$(f+g)(z) = (f+g)(a) + (z-a)[D_af(z) + D_ag(z)] \text{ for all } z \in \text{dom}(f+g)$$

and $D_af + D_ag$ is continuous at a.

We can let $D_a(f+g) = D_af + D_ag$ and we see $f+g$ is differentiable at a and

$$(f+g)'(a) = (D_af + D_ag)(a) = D_af(a) + D_ag(a) = f'(a) + g'(a). \ \|$$

10.12 Theorem. *Let f be a complex function and let $c \in \mathbf{C}$. If f is differentiable at a, then cf is differentiable at a and $(cf)'(a) = c \cdot f'(a)$.*

Proof: The proof is left to you. |||

10.13 Theorem (Chain Rule.) *Let f, g be complex functions, and let $a \in \mathbf{C}$. Suppose f is differentiable at a, and g is differentiable at $f(a)$, and that a is a limit point of* $\text{dom}(g \circ f)$. *Then the composition $(g \circ f)$ is differentiable at a, and*

$$(g \circ f)'(a) = g'(f(a)) \cdot f'(a).$$

Proof: From our hypotheses, there exist functions

$$D_a f\colon \mathrm{dom}(f) \to \mathbf{C}, \qquad D_{f(a)} g\colon \mathrm{dom}(g) \to \mathbf{C}$$

such that $D_a f$ is continuous at a, $D_{f(a)}g$ is continuous at $f(a)$ and

$$\begin{aligned} f(z) &= f(a) + (z-a)D_a f(z) \text{ for all } z \in \mathrm{dom}(f) && (10.14)\\ g(z) &= g\left(f(a)\right) + \left(z - f(a)\right) D_{f(a)} g(z) \text{ for all } z \in \mathrm{dom}(g). && (10.15) \end{aligned}$$

If $z \in \mathrm{dom}(g \circ f)$, then $f(z) \in \mathrm{dom}(g)$, so we can replace z in (10.15) by $f(z)$ to get

$$g\left(f(z)\right) = g\left(f(a)\right) + \left(f(z) - f(a)\right) D_{f(a)} g\left(f(z)\right) \text{ for all } z \in \mathrm{dom}(g \circ f).$$

Using (10.14) to rewrite $f(z) - f(a)$, we get

$$(g \circ f)(z) = (g \circ f)(a) + (z-a)D_a f(z)(D_{f(a)} g \circ f)(z) \text{ for all } z \in \mathrm{dom}(g \circ f).$$

Hence we have

$$D_a(g \circ f) = D_a f \cdot \Big((D_{f(a)} g) \circ f\Big)$$

and $D_a(g \circ f)$ is continuous at a. Hence $g \circ f$ is differentiable at a and

$$\begin{aligned} (g \circ f)'(a) &= D_a(g \circ f)(a) = D_a f(a) D_{f(a)} g\left(f(a)\right) \\ &= f'(a) \cdot g'\left(f(a)\right). \ \| \end{aligned}$$

10.16 Theorem (Reciprocal rule.) *Let f be a complex function, and let $a \in \mathrm{dom}(f)$. If f is differentiable at a and $f(a) \neq 0$, then $\frac{1}{f}$ is differentiable at a and* $\left(\dfrac{1}{f}\right)'(a) = \dfrac{-f'(a)}{\left(f(a)\right)^2}$.

Proof: If $v(z) = \dfrac{1}{z}$ for all $z \in \mathbf{C}\backslash\{0\}$, we saw above that v is differentiable and $v'(z) = -\dfrac{1}{z^2}$. Let f be a complex function, and let $a \in \mathbf{C}$. Suppose f is differentiable at a, and $f(a) \neq 0$. Then $(v \circ f)(z) = \dfrac{1}{f(z)}$. By the chain rule $v \circ f$ is differentiable at a, and

$$(v \circ f)'(a) = v'\left(f(a)\right) \cdot f'(a) = -\frac{1}{f(a)^2} f'(a). \ \|$$

10.17 Exercise (Product rule.) Let f, g be complex functions. Suppose f and g are both differentiable at a, and that a is a limit point of $\operatorname{dom}(f) \cap \operatorname{dom}(g)$. Show that fg is differentiable at a, and that

$$(fg)'(a) = f'(a)g(a) + f(a)g'(a).$$

10.18 Exercise (Power rule.) Let f be a complex function, and suppose that f is differentiable at $a \in \mathbf{C}$. Show that f^n is differentiable at a for all $n \in \mathbf{Z}_{\geq 1}$ and

$$(f^n)'(a) = n\,(f(a))^{n-1}\, f'(a).$$

(Use induction.)

10.19 Exercise (Power rule.) Let f be a complex function. suppose that f is differentiable at $a \in \mathbf{C}$, and $f(a) \neq 0$. Show that f^n is differentiable at a for all $n \in \mathbf{Z}^-$, and that

$$(f^n)'(a) = n\,(f(a))^{n-1}\, f'(a).$$

for all $n \in \mathbf{Z}^-$.

10.20 Exercise (Quotient rule.) Let f, g be complex functions and let $a \in \mathbf{C}$. Suppose f and g are differentiable at a and $g(a) \neq 0$, and a is a limit point of $\operatorname{dom}\left(\frac{f}{g}\right)$. Show that $\frac{f}{g}$ is differentiable at a and

$$\left(\frac{f}{g}\right)'(a) = \frac{g(a)f'(a) - f(a)g'(a)}{g(a)^2}.$$

10.2 Differentiable Functions on R

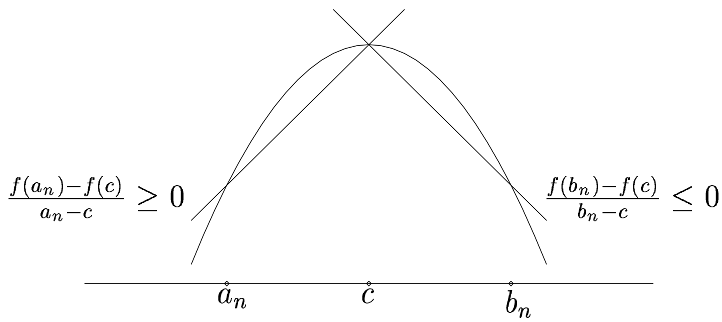
10.21 Warning. By the definition of differentiablity given in Math 111, the domain of a function was required to contain some interval $(a-\varepsilon, a+\varepsilon)$ in order for the function be differentiable at a. In definition 10.1 this condition has been replaced by requiring a to be a limit point of the domain of the function. Now a function whose domain is a closed interval $[a, b]$ may be differentiable at a and/or b.

10.22 Definition (Critical point.) Let f be a complex function, and let $a \in \mathbf{C}$. If f is differentiable at a and $f'(a) = 0$, we call a a *critical point* for f.

10.23 Theorem (Critical Point Theorem.) *Let $f\colon \text{dom}(f) \to \mathbf{R}$ be a function. Suppose f has a maximum at some point $c \in \text{dom}(f)$, and that $\text{dom}(f)$ contains an interval $(c-\varepsilon, c+\varepsilon)$ where $\varepsilon \in \mathbf{R}^+$. If f is differentiable at c, then $f'(c) = 0$. The theorem also holds if we replace "maximum" by "minimum."*

Proof: Suppose f has a maximum at c,

$$f'(c) = \lim_{x \to c} \frac{f(x) - f(c)}{x - c}.$$



Define two sequences $\{a_n\}$, $\{b_n\}$ in $(c-\varepsilon, c+\varepsilon)$ by

$$\begin{aligned} a_n &= c - \frac{\varepsilon}{(n+2)} \text{ for all } n \in \mathbf{N} \\ b_n &= c + \frac{\varepsilon}{(n+2)} \text{ for all } n \in \mathbf{N}. \end{aligned}$$

Clearly $\{a_n\} \to c$ and $\{b_n\} \to c$, and $f(a_n) \leq f(c)$ and $f(b_n) \leq f(c)$ for all $n \in \mathbf{N}$. We have

$$\frac{f(a_n) - f(c)}{a_n - c} = \frac{f(a_n) - f(c)}{-\left(\frac{\varepsilon}{n+2}\right)} \geq 0.$$

By the inequality theorem,

$$f'(c) = \lim \left\{ \frac{f(a_n) - f(c)}{a_n - c} \right\} \geq 0.$$

Also,

$$\frac{f(b_n) - f(c)}{b_n - c} = \frac{f(b_n) - f(c)}{\left(\frac{\varepsilon}{n+2}\right)} \leq 0,$$

so

$$f'(c) = \lim \left\{ \frac{f(b_n) - f(c)}{b_n - c} \right\} \leq 0.$$

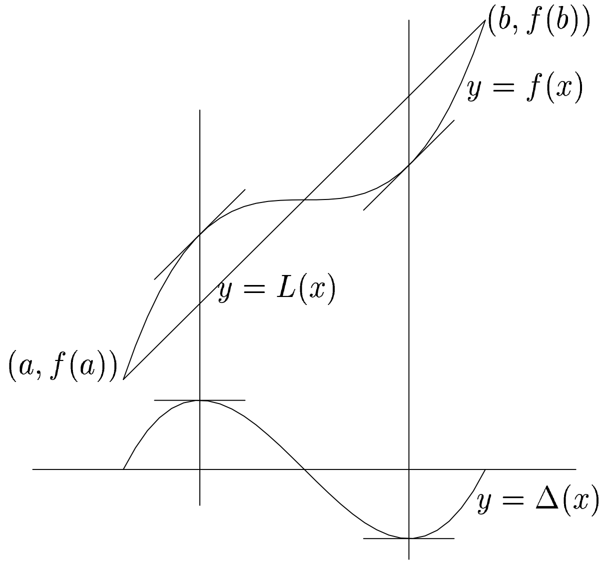
Since $0 \leq f'(c) \leq 0$, we conclude that $f'(c) = 0$. The proof for minimum points is left to you. ‖

10.24 Theorem (Rolle's Theorem.) *Let $a, b \in \mathbf{R}$ with $a < b$ and let $f: [a, b] \to \mathbf{R}$ be a function that is continuous on $[a, b]$ and differentiable on (a, b). Suppose that $f(a) = f(b)$. Then there is a number $c \in (a, b)$ such that $f'(c) = 0$.*

Proof: We know from the extreme value theorem that f has a maximum at some point $p \in [a, b]$. If $p \in (a, b)$, then the critical point theorem says $f'(p) = 0$, and we are finished. Suppose $p \in \{a, b\}$. We know there is a point $q \in [a, b]$ such that f has a minimum at q. If $q \in (a, b)$ we get $f'(q) = 0$ by the critical point theorem, so suppose $q \in \{a, b\}$. Then since $f(a) = f(b)$ and $p \in \{a, b\}, q \in \{a, b\}$, we have $f(p) = f(q)$, and it follows that f is a constant function on $[a, b]$, and in this case $f'(c) = 0$ for all $c \in (a, b)$. ‖

10.25 Theorem (Mean Value Theorem.) *Let $a, b \in \mathbf{R}$ with $a < b$, and let f be a function from $[a, b]$ to $\mathbf{R}$ such that f is continuous on $[a, b]$ and differentiable on (a, b). Then there is a point $c \in (a, b)$ such that*

$$f'(c) = \frac{f(b) - f(a)}{b - a}.$$



This theorem says that the tangent to the graph of f at some point $(c, f(c))$ is parallel to the chord joining $(a, f(a))$ to $(b, f(b))$.
Proof: Let

$$L(x) = f(a) + \frac{f(b) - f(a)}{b - a}(x - a) \text{ for all } x \in \mathbf{R},$$

so the equation of the line joining $(a, f(a))$ to $(b, f(b))$ is $y = L(x)$, and

$$L'(x) = \frac{f(b) - f(a)}{b - a} \text{ for all } x \in \mathbf{R}.$$

Let

$$\Delta(x) = f(x) - L(x) \text{ for all } x \in [a, b].$$

Then

$$\begin{aligned} \Delta(a) &= f(a) - L(a) = f(a) - f(a) = 0, \\ \Delta(b) &= f(b) - L(b) = f(b) - f(b) = 0, \end{aligned}$$

and Δ is continuous on $[a, b]$ and differentiable on (a, b). By Rolle's theorem, there is some $c \in (a, b)$ such that $\Delta'(c) = 0$; i.e., $f'(c) - L'(c) = 0$; i.e.,

$$f'(c) = L'(c) = \frac{f(b) - f(a)}{b - a}. \ \|\!|$$

10.26 Remark. The mean value theorem does not hold for complex valued functions. Let

$$F(t) = (1 + it)^4 \text{ for all } t \in [-1, 1].$$

Then

$$F(\pm 1) = (1 \pm i)^4 = (\pm 2i)^2 = -4,$$

so

$$\frac{F(1) - F(-1)}{1 - (-1)} = 0.$$

But

$$F'(t) = 4i(1 + it)^3,$$

so $F'(t) = 0 \iff t = -i$, and there is no point in $t \in (-1, 1)$ with $F'(t) = 0$.

10.27 Definition (Interior point.) Let J be an interval in $\mathbf{R}$. A number $a \in J$ is an *interior point* of J if and only if a is not an end point of J. The set of all interior points of J is called the *interior* of J and is denoted by $\text{int}(J)$.

10.28 Examples. If $a < b$, then

$$\begin{aligned} \operatorname{int}([a,b)) = \operatorname{int}([a,b]) = \operatorname{int}((a,b)) &= (a,b), \\ \operatorname{int}([a,\infty)) = \operatorname{int}((a,\infty)) &= (a,\infty). \end{aligned}$$

If J is an interval, and s, t are points in J with $s < t$, then every point in (s,t) is in the interior of J.

10.29 Theorem. *Let J be an interval in $\mathbf{R}$, and let $f \colon J \to \mathbf{R}$ be a continuous function on J. Then:*

a) If $f'(x) \geq 0$ for all $x \in \operatorname{int}(J)$, then f is increasing on J.

b) If $f'(x) > 0$ for all $x \in \operatorname{int}(J)$, then f is strictly increasing on J.

c) If $f'(x) \leq 0$ for all $x \in \operatorname{int}(J)$, then f is decreasing on J.

d) If $f'(x) < 0$ for all $x \in \operatorname{int}(J)$, then f is strictly decreasing on J.

e) If $f'(x) = 0$ for all $x \in \operatorname{int}(J)$, then f is constant on J.

Proof: All five statements have similar proofs. I'll prove only part a).

Suppose $f'(x) \geq 0$ for all $x \in \operatorname{int}(J)$. Then for all $s, t \in J$ with $s < t$ we have f is continuous on $[s,t]$ and differentiable on (s,t), so by the mean value theorem

$$\begin{aligned} s < t \implies & \frac{f(t) - f(s)}{t - s} = f'(c) \text{ for some } c \in (s,t) \subset \operatorname{int}(J) \\ \implies & \frac{f(t) - f(s)}{t - s} \geq 0 \text{ and } t - s > 0 \\ \implies & f(t) - f(s) \geq 0 \\ \implies & f(t) \geq f(s). \end{aligned}$$

Hence, f is increasing on J.

10.30 Exercise. Prove part e) of the previous theorem; i.e., show that if J is an interval in $\mathbf{R}$ and $f \colon J \to \mathbf{R}$ is continuous and satisfies $f'(t) = 0$ for all $t \in \operatorname{int}(J)$, then f is constant on J. [It is sufficient to show that $f(s) = f(t)$ for all $s, t \in J$.]

10.31 Exercise. For each assertion below, either prove that the assertion is true for all functions f, or give a function f for which the assertion is false. (A proof may consist of quoting a theorem.)

a) If f is differentiable on $(-1,1)$ and f is strictly increasing on $(-1,1)$, then $f'(t) > 0$ for all $t \in (-1,1)$.

b) If f is differentiable on $[-1,1]$, and f has a maximum at $t_0 \in [-1,1]$, then $f'(t_0) = 0$.

c) If f is continuous on $[-1,1]$ and f is differentiable on $(-1,1)$, and $f'(t) > 0$ for all $t \in (-1,1)$, then f is strictly increasing on $[-1,1]$.

10.32 Theorem (Restriction theorem) *Let S be a subset of $\mathbf{C}$, let $f : S \to \mathbf{C}$, and let $a \in S$ be a point such that f is differentiable at a. Let T be a subset of S containing a, and let $f|_T : T \to \mathbf{C}$ be the restriction of f to T, i.e.*

$$f|_T(z) = f(z) \text{ for all } z \in T.$$

If a is a limit point of T, then $f|_T$ is differentiable at a, and

$$f|_T'(a) = f'(a).$$

Proof: Let $\{z_n\}$ be any sequence in $T \setminus \{a\}$ such that $\{z_n\} \to a$. Then $\{z_n\}$ is a sequence in $S \setminus \{a\}$, and hence

$$\left\{\frac{f(z_n) - f(a)}{z_n - a}\right\} \to f'(a).$$

It follows that

$$\left\{\frac{f|_T(z_n) - f|_T(a)}{z_n - a}\right\} = \left\{\frac{f(z_n) - f(a)}{z_n - a}\right\} \to f'(a).$$

I've shown that

$$\lim_{z \to a} \frac{f|_T(z) - f|_T(a)}{z - a} = f'(a). \ \|$$

10.33 Definition (Path, line segment.) If $a, b \in \mathbf{C}$, then the *path joining a to b* is the function $\lambda_{ab}\colon [0,1] \to \mathbf{C}$

$$\lambda_{ab}\colon t \mapsto a + t(b-a) \text{ for all } t \in [0,1]$$

and the set

$$\Lambda_{ab} = \lambda_{ab}([0,1]) = \{a + t(b-a)\colon 0 \le t \le 1\}$$

is called the *line segment* joining a to b.

10.34 Example. We showed in example 10.9 that the function conj : $z \mapsto z^*$ is a nowhere differentiable function on $\mathbf{C}$. I will show that for all a, b in $\mathbf{C}$ with $a \neq b$, the restriction $\text{conj}|_{\Lambda_{ab}}$ of conj to the line segment Λ_{ab} is differentiable, and

$$\text{conj}|_{\Lambda_{ab}}{}'(z) = \frac{b^* - a^*}{b - a} \text{ for all } z \in \Lambda_{ab}.$$

Note that all points of Λ_{ab} are limit points of Λ_{ab}. If $z \in \Lambda_{ab}$, then for some real number t

$$z = a + t(b - a) \tag{10.35}$$

and

$$z^* = a^* + t(b^* - a^*). \tag{10.36}$$

If we solve equation (10.35) for t we get

$$t = \frac{z - a}{b - a}.$$

By using this value for t in equation (10.36) we get

$$z^* = a^* + \frac{b^* - a^*}{b - a}(z - a) \text{ for all } z \in \Lambda_{ab}.$$

Let $H_{ab} : \mathbf{C} \to \mathbf{C}$ be defined by

$$H_{ab}(z) = a^* + \frac{b^* - a^*}{b - a}(z - a) \text{ for all } z \in \mathbf{C}.$$

Then H_{ab} is differentiable, and $H'(z) = \dfrac{b^* - a^*}{b - a}$ for all $z \in \mathbf{C}$. We have

$$H_{ab}|_{\Lambda_{ab}} = \text{conj}|_{\Lambda_{ab}},$$

so by the restriction theorem

$$\text{conj}|_{\Lambda_{ab}}{}'(z) = H|_{\Lambda_{ab}}{}'(z) = \frac{b^* - a^*}{b - a} \text{ for all } z \in \Lambda_{ab}.$$

10.37 Exercise. Let $C(0,1)$ denote the unit circle in $\mathbf{C}$. Show that $\text{conj}|_{C(0,1)}$ is differentiable, and that

$$\text{conj}_{C(0,1)}{}'(z) = -(z^*)^2 \text{ for all } z \in C(0,1).$$

In general, the real and imaginary parts of a differentiable function are not differentiable.

10.38 Example. If $f(z) = z$ for all $z \in \mathbf{C}$, then f is differentiable and $f'(z) = 1$. However, $\text{Re}f$ is nowhere differentiable. In fact, if $a \in \mathbf{C}$, $\dfrac{\text{Re}(z) - \text{Re}(z)}{z - a}$ has no limit at a. To see this, let $a_n = a + \dfrac{1}{n}$, $b_n = a + \dfrac{i}{n}$ for all $n \in \mathbf{Z}_{\geq 1}$. Then $\{a_n\} \to a$, $\{b_n\} \to a$, and

$$\frac{\text{Re}(a_n) - \text{Re}(a)}{a_n - a} = \frac{\text{Re}(a + \frac{1}{n}) - \text{Re}(a)}{a + \frac{1}{n} - a} = 1$$

and

$$\frac{\text{Re}(b_n) - \text{Re}(a)}{b_n - a} = \frac{\text{Re}(a) - \text{Re}(a)}{a + \frac{i}{n} - a} = 0.$$

Hence, the sequences $\left\{\dfrac{\text{Re}(a_n) - \text{Re}(a)}{a_n - a}\right\}_{n\geq 1}$ and $\left\{\dfrac{\text{Re}(b_n) - \text{Re}(a)}{b_n - a}\right\}_{n\geq 1}$ have different limits, so $\lim\limits_{z\to a} \dfrac{\text{Re}(z) - \text{Re}(a)}{z - a}$ does not exist.

However, we do have the following theorem.

10.39 Theorem. *Let J be an interval in $\mathbf{R}$ and let $f\colon J \to \mathbf{C}$ be a function differentiable at a point $a \in J$. Write $f(t) = u(t) + iv(t)$ where u, v are real valued. Then u and v are differentiable at a, and $f'(a) = u'(a) + iv'(a)$.*

Proof: Since f is differentiable at a there is a function $D_a f$ on J such that $D_a f$ is continuous at a and

$$f(t) = f(a) + (t - a)D_a f(t) \text{ for all } t \in J.$$

If $r \in \mathbf{R}$ and $c \in \mathbf{C}$, then $\text{Re}(rc) = r\text{Re}(c)$ and $\text{Im}(rc) = r\text{Im}(c)$, so

$$(\text{Re}(f))(t) = (\text{Re}(f))(a) + (t - a)(\text{Re}(D_a f))(t) \text{ for all } t \in J \tag{10.40}$$

and

$$(\text{Im}(f))(t) = (\text{Im}(f))(a) + (t - a)(\text{Im}(D_a f))(t) \text{ for all } t \in J. \tag{10.41}$$

Since $D_a f$ is continuous at a, $\text{Re}(D_a f)$ and $\text{Im}(D_a f)$ are continuous at a, so equations (10.40) and (10.41) show that $\text{Re}f$ and $\text{Im}f$ are differentiable and

$$\begin{aligned} (\text{Re}f)'(a) &= (\text{Re}(D_a f(a)) = \text{Re}(f'(a)) \\ (\text{Im}f)'(a) &= (\text{Im}\,(D_a f(a))) = \text{Im}(f'(a)). \ \| \end{aligned}$$

10.42 Example. Let $a \in \mathbf{R}$, and let $f(t) = (2t + ia)^3$ for all $t \in \mathbf{R}$. Then f is differentiable and (by the chain rule),

$$\begin{aligned} f'(t) &= 3(2t + ia)^2 \cdot 2 \\ &= 6[(4t^2 - a^2) + 4iat] \\ &= (24t^2 - 6a^2) + 24iat. \end{aligned}$$

We have by direct calculation,

$$\begin{aligned} f(t) &= 8t^3 + 12iat^2 - 6ta^2 - ia^3 \\ &= (8t^3 - 6ta^2) + (12at^2 - a^3)i, \end{aligned}$$

so

$$f'(t) = (24t^2 - 6a^2) + (24at)i.$$

(This example just illustrates that the theorem is true in a special case.)

10.43 Theorem. *Let f be a complex function and let $a, b \in \mathbf{C}$, and suppose* $\mathrm{dom}(f)$ *contains the line segment Λ_{ab}, and that $f'(z) = 0$ for all $z \in \Lambda_{ab}$. Then f is constant on Λ_{ab}; i.e., $f(z) = f(a)$ for all $z \in \Lambda_{ab}$.*

Proof: Define a function $F\colon [0,1] \to \mathbf{C}$ by

$$F(t) = f\left(\lambda_{ab}(t)\right) = f\left(a + t(b - a)\right).$$

By the chain rule, F is differentiable on $[0,1]$ and $F'(t) = f'\left(a + t(b-a)\right)\cdot(b-a)$. Since $f'(z) = 0$ for all $z \in \Lambda_{ab}([0,1])$, we have $F'(t) = 0$ for all $t \in [0,1]$. Hence

$$(\mathrm{Re}(F))'(t) = 0 \text{ and } (\mathrm{Im}(F))'(t) = 0 \text{ for all } t \in [0,1]$$

and hence

$$\mathrm{Re}(F) \text{ and } \mathrm{Im}(F) \text{ are constant on } [0,1].$$

If $\mathrm{Re}(F) = p$ and $\mathrm{Im}(F) = q$, then $F(t) = p + iq$ for all $t \in [0,1]$. |||

10.44 Exercise. Let $D(a,\varepsilon)$ be a disc in $\mathbf{C}$.

a) Show that if $b \in D(a,\varepsilon)$ then the segment Λ_{ab} is a subset of $D(a,\varepsilon)$.

b) Let $f\colon D(a,\varepsilon) \to \mathbf{C}$ be a function such that $f'(z) = 0$ for all $z \in D(a,\varepsilon)$. Show that f is constant on $D(a,\varepsilon)$.

10.3 Trigonometric Functions

10.45 Example. Suppose that there are real valued functions S, C on $\mathbf{R}$ such that

$$\begin{array}{ll} S' = C, & S(0) = 0, \\ C' = -S, & C(0) = 1. \end{array}$$

You have seen such functions in your previous calculus course. Let $H = S^2 + C^2$. Then

$$H' = 2SS' + 2CC' = 2SC - 2CS = 0.$$

Hence, H is constant on $\mathbf{R}$, and since $H(0) = S^2(0) + C^2(0) = 0 + 1$, we have

$$S^2 + C^2 = \tilde{1} \text{ on } \mathbf{R}.$$

In particular,

$$|S(t)| \leq 1 \text{ and } |C(t)| \leq 1 \text{ for all } t \in \mathbf{R}.$$

Let $K(t) = (S(t) + S(-t))^2 + (C(t) - C(-t))^2$. By the power rule and chain rule,

$$\begin{aligned} &K'(t) \\ &= 2(S(t) + S(-t))(S'(t) - S'(-t)) + 2(C(t) - C(-t))(C'(t) + C'(-t)) \\ &= 2(S(t) + S(-t))(C(t) - C(-t)) + 2(C(t) - C(-t))(-S(t) - S(-t)) \\ &= 0. \end{aligned}$$

Hence K is constant and since $K(0) = 0$, we conclude that $K(t) = 0$ for all t. Since a sum of squares in $\mathbf{R}$ is zero only when each summand is zero, we conclude that

$$\begin{aligned} S(-t) &= -S(t) \text{ for all } t \in \mathbf{R}, \\ C(-t) &= C(t) \text{ for all } t \in \mathbf{R}. \end{aligned}$$

Let

$$F_0(t) = -C(t) + 1 \text{ for all } t \in \mathbf{R}.$$

Then $F_0(t) \geq 0$ for all $t \in \mathbf{R}$ and $F_0(0) = 0$. I will now construct a sequence $\{F_n\}$ of functions on $\mathbf{R}$ such that $F_n(0) = 0$ for all $n \in \mathbf{N}$, and $F'_{n+1}(t) = F_n(t)$

for all $t \in \mathbf{R}$. I have

$$\begin{aligned} F_1(t) &= -S(t) + t, \\ F_2(t) &= C(t) + \frac{t^2}{2!} - 1, \\ F_3(t) &= S(t) + \frac{t^3}{3!} - \frac{t}{1!}, \\ F_4(t) &= -C(t) + \frac{t^4}{4!} - \frac{t^2}{2!} + 1, \\ F_5(t) &= -S(t) + \frac{t^5}{5!} - \frac{t^3}{3!} + t. \end{aligned}$$

It should be clear how this pattern continues. Since $F_1'(t) = F_0(t) \geq 0$, F_1 is increasing on $[0, \infty)$ and since $F_1(0) = 0$, $F_1(t) \geq 0$ for $t \in [0, \infty)$. Since $F_2'(t) = F_1(t) \geq 0$ on $[0, \infty)$, F_2 is increasing on $[0, \infty)$ and since $F_2(0) = 0$, $F_2(t) \geq 0$ for $t \in [0, \infty)$.

This argument continues (I'll omit the inductions), and I conclude that $F_n(t) \geq 0$ for all $t \in [0, \infty)$ and all $n \in \mathbf{N}$. Now

$$\begin{aligned} F_0(t) \geq 0 \text{ and } F_2(t) \geq 0 &\implies \frac{-t^2}{2!} \leq C(t) - 1 \leq 0, \\ F_1(t) \geq 0 \text{ and } F_3(t) \geq 0 &\implies \frac{-t^3}{3!} \leq S(t) - t \leq 0, \\ F_2(t) \geq 0 \text{ and } F_4(t) \geq 0 &\implies 0 \leq C(t) - 1 + \frac{t^2}{2!} \leq \frac{t^4}{4!}, \\ F_3(t) \geq 0 \text{ and } F_5(t) \geq 0 &\implies 0 \leq S(t) - t + \frac{t^3}{3!} \leq \frac{t^5}{5!}, \\ F_4(t) \geq 0 \text{ and } F_6(t) \geq 0 &\implies \frac{-t^6}{6!} \leq C(t) - 1 + \frac{t^2}{2!} - \frac{t^4}{4!} \leq 0. \end{aligned}$$

For each $n \in \mathbf{N}$, $t \in \mathbf{C}$, define

$$\begin{aligned} c_n(t) &= \frac{(-1)^n t^{2n}}{(2n)!}, \\ s_n(t) &= \frac{(-1)^n t^{2n+1}}{(2n+1)!}, \\ C_n(t) &= \sum_{j=0}^{n} c_j(t) = \sum_{j=0}^{n} \frac{(-1)^j t^{2j}}{(2j)!}, \\ S_n(t) &= \sum_{j=0}^{n} s_j(t) = \sum_{j=0}^{n} \frac{(-1) t^{2j+1}}{(2j+1)!}. \end{aligned}$$

The equations above suggest that for all $n \in \mathbf{N}$, $t \in [0, \infty)$,

$$|C(t) - C_n(t)| \leq |c_{n+1}(t)| \tag{10.46}$$

and

$$|S(t) - S_n(t)| \leq |s_{n+1}(t)| \tag{10.47}$$

I will not write down the induction proof for this because I believe that it is clear from the examples how the proof goes, but the notation becomes complicated.

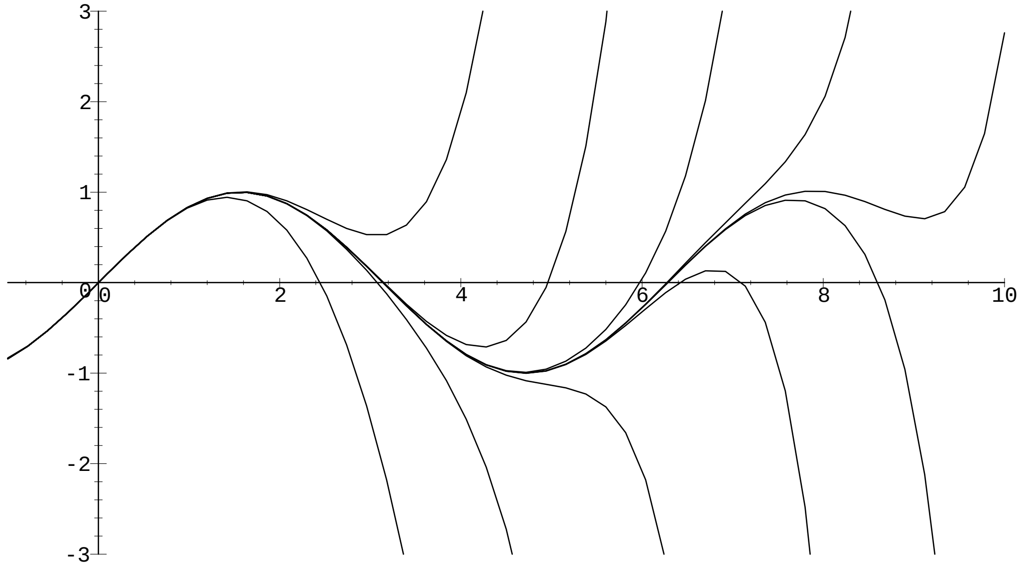
Since $C(t) = C(-t)$, $C_n(t) = C_n(-t)$ and $c_n(t) = c_n(-t)$, the relation (10.46) actually holds for all $t \in \mathbf{R}$ (not just for $t \in [0, \infty)$) and similarly relation (10.47) holds for all $t \in \mathbf{R}$. From (10.46) and (10.47), we see that if $\{c_n(t)\}$ is a null sequence, then the sequence $\{C_n(t)\}$ converges to $C(t)$, and if $\{s_n(t)\}$ is a null sequence, then $\{S_n(t)\}$ converges to $S(t)$.

We will show later that both sequences $\{C_n(z)\}$ and $\{S_n(z)\}$ converge for all *complex* numbers z, and we will define

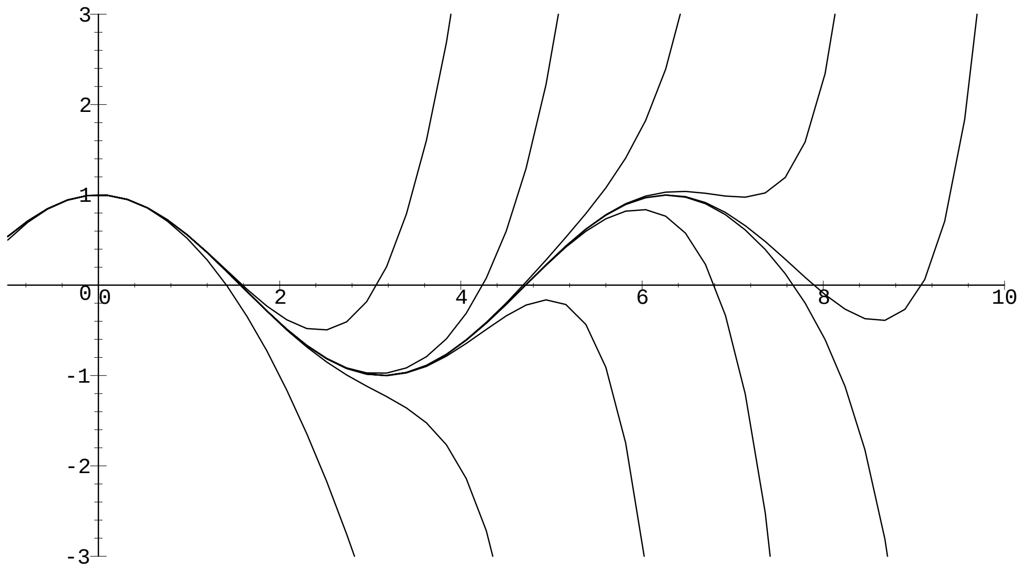
$$\cos(z) = \lim\{C_n(z)\} = \lim\left\{\sum_{j=0}^{n} \frac{(-1)^j z^{2j}}{(2j)!}\right\} \tag{10.48}$$

$$\sin(z) = \lim\{S_n(z)\} = \lim\left\{\sum_{j=0}^{n} \frac{(-1)^j z^{2j+1}}{(2j+1)!}\right\} \tag{10.49}$$

for all $z \in \mathbf{C}$. The discussion above is supposed to convince you that for real z this definition agrees with whatever definition of sine and cosine you are familiar with. The figures show graphs of C_n and S_n for small n.



Graphs of the polynomials S_n for $1 \le n \le 10$

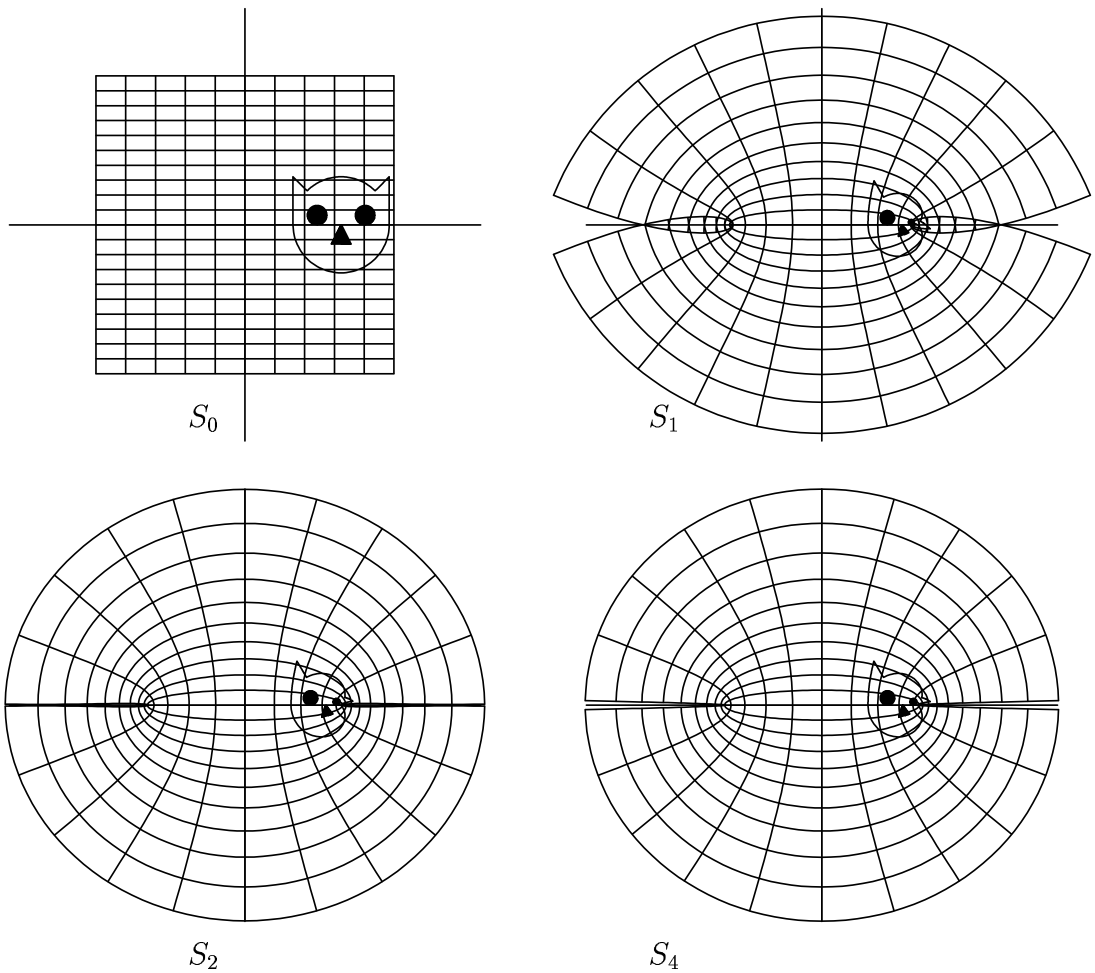


Graphs of the polynomials C_n for $1 \le n \le 10$

10.50 Exercise. Show that $\{c_n(t)\}$ and $\{s_n(t)\}$ are null sequences for all complex t with $|t| \le 1$.

10.51 Exercise. a) Using calculator arithmetic, calculate the limits of $\left\{C_n\left(\frac{1}{10}\right)\right\}$ and $\left\{S_n\left(\frac{1}{10}\right)\right\}$ accurate to 8 decimals. Compare your results with your calculator's value of $\sin\left(\frac{1}{10}\right)$ and $\cos\left(\frac{1}{10}\right)$. [Be sure to use radian mode.]

b) Calculate $\cos(i)$ to 3 or 4 decimals accuracy. Note that $\cos(i)$ is real.



Polynomial Approximations to sine Function
$-1.55 \leq x \leq 1.55, \quad -1.55 \leq y \leq 1.55$

The figure shows graphical representations for S_0, S_1, S_2, and S_4. Note that S_0 is the identity function.

10.52 Entertainment. Show that for all $a, x \in \mathbf{R}$

$$C(a+x) = C(a)C(x) - S(a)S(x)$$

and

$$S(a+x) = S(a)C(x) + C(a)S(x).$$

Use a trick similar to the trick used to show that $S(-x) = -S(x)$ and $C(-x) = C(x)$.

10.53 Entertainment. By using the definitions (10.48) and (10.49), show that

a) For all $a \in \mathbf{R}$, $\cos(ia)$ is real, and $\cos(ia) \geq 1$.

b) For all $a \in \mathbf{R}$, $\sin(ia)$ is pure imaginary, and $\sin(ia) = 0$ if and only if $a = 0$.

c) Assuming that the identity

$$\sin(z+w) = \sin(z)\cos(w) + \cos(z)\sin(w)$$

is valid for all complex numbers z and w, show that if $a \in \mathbf{R} \setminus \{0\}$ then sin maps the horizontal line $y = a$ to the ellipse having the equation

$$\frac{x^2}{|\cos(ia)|^2} + \frac{y^2}{|\sin(ia)|^2} = 1.$$

d) Describe where sin maps vertical lines. (Assume that the identity $\sin^2(z) + \cos^2(z) = 1$ holds for all $z \in \mathbf{C}$.)

10.54 Note. Rolle's theorem is named after Michel Rolle (1652–1719). An English translation of Rolle's original statement and proof can be found in [46, pages 253–260]. It takes a considerable effort to see any relation between what Rolle says, and what our form of his theorem says.

The series representations for sine and cosine (10.48) and (10.49) are usually credited to Newton, who discovered them some time around 1669. However, they were known in India centuries before this. Several sixteenth century Indian writers quote the formulas and attribute them to Madhava of Sangamagramma (c. 1340-1425)[30, p 294].

The method used for finding the series for sine and cosine appears in the 1941 book *What is Mathematics"* by Courant and Robbins[17, page 474]. I expect that the method was well known at that time.

Chapter 11

Infinite Series

11.1 Infinite Series

11.1 Definition (Series operator.) If f is a complex sequence, we define a new sequence $\sum f$ by

$$(\sum f)(n) = \sum_{j=0}^{n} f(j) \text{ for all } n \in \mathbf{N}$$

or

$$\sum\{f(n)\} = \{\sum_{j=0}^{n} f(j)\} \text{ for all } n \in \mathbf{N}.$$

We use variations, such as

$$\sum\{f(n)\}_{n\geq 1} = \{\sum_{j=1}^{n} f(j)\}_{n\geq 1}.$$

$\sum$ is actually a function that maps complex sequences to complex sequences. We call $\sum f$ the *series* corresponding to f.

11.2 Remark. If f, g are complex sequences and $c \in \mathbf{C}$, then

$$\sum(f+g) = \sum f + \sum g$$

and

$$\sum(cf) = c(\sum f),$$

since for all $n \in \mathbf{N}$,

$$\begin{aligned}\left(\sum(f+g)\right)(n) &= \sum_{j=0}^{n}(f+g)(j) = \sum_{j=0}^{n} f(j)+g(j) \\ &= \sum_{j=0}^{n} f(j) + \sum_{j=0}^{n} g(j) = (\sum f)(n) + (\sum g)(n) \\ &= (\sum f + \sum g)(n)\end{aligned}$$

and

$$\begin{aligned}\left(\sum(cf)\right)(n) &= \sum_{j=0}^{n}(cf)(j) = \sum_{j=0}^{n} c\cdot f(j) = c\sum_{j=0}^{n} f(j) \\ &= c\cdot\left((\sum f)(n)\right) = (c\cdot\sum f)(n).\end{aligned}$$

11.3 Examples. If $\{r^n\}$ is a geometric sequence, then $\sum\{r^n\} = \{\sum_{j=0}^{n} r^j\}$ is a sequence we have been calling a geometric series. If $\{c_n(t)\} = \left\{\dfrac{t^{2n}(-1)^n}{(2n)!}\right\}$, then $\sum\{c_n(t)\} = \{C_n(t)\}$ is the sequence for $\cos(t)$ that we studied in the last chapter.

11.4 Definition (Summable sequence.) A complex sequence $\{a_n\}$ is *summable* if and only if the series $\sum\{a_n\}$ is convergent. If $\{a_n\}$ is summable, we denote $\lim(\sum\{a_n\})$ by $\sum\limits_{n=0}^{\infty} a_n$. We call $\sum\limits_{n=0}^{\infty} a_n$ the *sum* of the series $\sum\{a_n\}$.

11.5 Example. If $r \in \mathbf{C}$ and $|r| < 1$, then $\sum\limits_{n=0}^{\infty} r^n = \lim\{\sum\limits_{j=0}^{n} r^j\} = \dfrac{1}{1-r}$.

11.6 Example (Harmonic series.) The series

$$\sum\left\{\frac{1}{n}\right\}_{n\geq 1} = \left\{\sum_{j=1}^{n}\frac{1}{j}\right\}_{n\geq 1}$$

is called the *harmonic series*, and is denoted by $\{H_n\}_{n\geq 1}$. Thus

$$H_n = \sum_{j=1}^{n}\frac{1}{j}.$$

We will show that $\{H_n\}_{n\geq 1}$ diverges; i.e., the sequence $\left\{\frac{1}{n}\right\}_{n\geq 1}$ is not summable. For all $n \geq 1$, we have

$$\begin{aligned}
H_{2n} &= 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \cdots + \frac{1}{2n-1} + \frac{1}{2n} \\
&\geq \left(\frac{1}{2} + \frac{1}{2}\right) + \frac{1}{2} + \frac{1}{4} + \frac{1}{4} + \frac{1}{6} + \frac{1}{6} + \cdots + \frac{1}{2n} + \frac{1}{2n} \\
&= \frac{1}{2} + \frac{2}{2} + \frac{2}{4} + \frac{2}{6} + \cdots + \frac{2}{2n} \\
&= \frac{1}{2} + \left(1 + \frac{1}{2} + \cdots + \frac{1}{n}\right) \\
&= \frac{1}{2} + H_n.
\end{aligned}$$

From the relation $H_{2n} \geq \frac{1}{2} + H_n$, we have

$$\begin{aligned}
H_2 &\geq \frac{1}{2} + H_1 = \frac{1}{2} + 1 \\
H_4 &\geq \frac{1}{2} + H_2 \geq \frac{2}{2} + 1 \\
H_8 &\geq \frac{1}{2} + H_4 \geq \frac{3}{2} + 1
\end{aligned}$$

and (by induction),

$$H_{2^n} \geq \frac{n}{2} + 1 \text{ for all } n \in \mathbf{Z}_{\geq 1}.$$

Hence, $\{H_n\}_{n\geq 1}$ is not bounded, and thus $\{H_n\}$ diverges; i.e., $\left\{\frac{1}{n}\right\}_{n\geq 1}$ is not summable.

11.7 Theorem (Sum theorem for series.) *Let f, g be summable sequences and let $c \in \mathbf{C}$. Then $f + g$ and cf are summable, and*

$$\begin{aligned}
\sum_{n=0}^{\infty} (f+g)(n) &= \sum_{n=0}^{\infty} f(n) + \sum_{n=0}^{\infty} g(n) \\
\sum_{n=0}^{\infty} cf(n) &= c\sum_{n=0}^{\infty} f(n).
\end{aligned}$$

If f is not summable, and $c \neq 0$, then cf is not summable.

Proof: The proof is left to you.

11.8 Exercise. Let f, g be summable sequences. Show that $f+g$ is summable and that

$$\sum_{j=0}^{\infty}(f+g)(j)=\sum_{j=0}^{\infty}f(j)+\sum_{j=0}^{\infty}g(j).$$

11.9 Example. The product of two summable sequences is not necessarily summable. If

$$f=\left\{1,-1,\sqrt{\frac{1}{2}},-\sqrt{\frac{1}{2}},\sqrt{\frac{1}{3}},-\sqrt{\frac{1}{3}},\sqrt{\frac{1}{4}},-\sqrt{\frac{1}{4}},\cdots\right\}_{n\geq 1}$$

then

$$\sum f=\left\{1,0,\sqrt{\frac{1}{2}},0,\sqrt{\frac{1}{3}},0,\sqrt{\frac{1}{4}},0,\cdots\right\}_{n\geq 1}.$$

This is a null sequence, so f is summable and $\sum_{n=1}^{\infty}f(n)=0$. However,

$$f^2=\left\{1,1,\frac{1}{2},\frac{1}{2},\frac{1}{3},\frac{1}{3},\frac{1}{4},\frac{1}{4},\cdots\right\}_{n\geq 1},$$

so $\left(\sum(f^2)\right)(2n)=2\sum_{j=1}^{n}\frac{1}{j}=2H_n$. Thus $\sum(f^2)$ is unbounded and hence f^2 is not summable.

11.10 Theorem. *Every summable sequence is a null sequence. [The converse is not true. The harmonic series provides a counterexample.]*

Proof: Let f be a summable sequence. Then $\{\sum_{j=0}^{n}f(j)\}$ converges to a limit L, and by the translation theorem $\{\sum_{j=0}^{n+1}f(j)\}\to L$ also. Hence

$$\{\sum_{j=0}^{n+1}f(j)\}-\{\sum_{j=0}^{n}f(j)\}\to L-L=0;$$

i.e.,

$$\{f(n+1)\}\to 0$$

and it follows that f is a null sequence. ‖

11.2 Convergence Tests

In this section we prove a number of theorems about convergence of series of real numbers. Later we will show how to use these results to study convergence of complex sequences.

11.11 Theorem (Comparison test for series.) *Let f, g be two sequences of non-negative numbers. Suppose that there is a number $N \in \mathbf{N}$ such that*

$$f(n) \leq g(n) \text{ for all } n \in \mathbf{Z}_{\geq N}.$$

Then

if g is summable, then f is summable,

and

if f is not summable, then g is not summable.

Proof: Note that the two statements in the conclusion are equivalent, so it is sufficient to prove the first.

Suppose that g is summable. Then $\sum g$ converges, so $\sum g$ is bounded — say $(\sum g)(n) \leq B$ for all $n \in \mathbf{N}$. Then for all $n \geq N+1$,

$$\begin{aligned} \sum_{j=0}^{n} f(j) &= \sum_{j=0}^{N} f(j) + \sum_{j=N+1}^{n} f(j) \leq \sum_{j=0}^{N} f(j) + \sum_{j=N+1}^{n} g(j) \\ &\leq \sum_{j=0}^{N} f(j) + \sum_{j=0}^{n} g(j) \leq \sum_{j=0}^{N} f(j) + B. \end{aligned}$$

Since for $n \leq N$ we have

$$\sum_{j=0}^{n} f(j) \leq \sum_{j=0}^{N} f(j) \leq \sum_{j=0}^{N} f(j) + B,$$

we see that $\sum f$ is bounded by $\sum_{j=0}^{N} f(j) + B$. Also $\sum f$ is increasing, since $(\sum f)(n+1) = (\sum f)(n) + f(n+1) \geq \sum f(n)$. Hence $\sum f$ is bounded and increasing, and hence $\sum f$ converges; i.e., f is summable. |||

11.12 Examples. Since

$$\frac{1}{\sqrt{n}} \geq \frac{1}{n} > 0 \text{ for all } n \in \mathbf{Z}_{\geq 1}$$

and $\sum \left\{\frac{1}{n}\right\}_{n\geq 1}$ diverges, it follows that $\sum \left\{\frac{1}{\sqrt{n}}\right\}_{n\geq 1}$ also diverges. Since $\sum\{t^n\}$ converges for $0 \leq t < 1$, $\sum \left\{\frac{t^n}{n!}\right\}$ also converges for $0 \leq t < 1$.

In order to use the comparison test, we need to have some standard series to compare other series with. The next theorem will provide a large family of standard series.

11.13 Theorem. *Let $p \in \mathbf{Q}$. Then $\left\{\frac{1}{n^p}\right\}_{n\geq 1}$ is summable if $p > 1$, and is not summable if $p \leq 1$.*

Proof: Let $f_p(n) = \frac{1}{n^p}$ for $n \in \mathbf{Z}_{\geq 1}$. Then for all $n \in \mathbf{Z}_{\geq 1}$ and all $p \geq 0$,

$$\begin{aligned}
(\textstyle\sum f_p)(n) &\leq (\textstyle\sum f_p)(2n+1) \\
&= \frac{1}{1^p} + \frac{1}{2^p} + \frac{1}{3^p} + \frac{1}{4^p} + \frac{1}{5^p} + \cdots + \frac{1}{(2n)^p} + \frac{1}{(2n+1)^p} \\
&\leq 1 + \frac{1}{2^p} + \frac{1}{2^p} + \frac{1}{4^p} + \frac{1}{4^p} + \cdots + \frac{1}{(2n)^p} + \frac{1}{(2n)^p} \\
&= 1 + 2\left(\frac{1}{2^p} + \frac{1}{4^p} + \cdots + \frac{1}{(2n)^p}\right) \\
&= 1 + \frac{2}{2^p}\left(\frac{1}{1^p} + \frac{1}{2^p} + \cdots + \frac{1}{n^p}\right) \\
&= 1 + 2^{1-p}(\textstyle\sum f_p)(n).
\end{aligned}$$

Hence,

$$(1 - 2^{1-p})\left((\textstyle\sum f_p)(n)\right) \leq 1.$$

If $p > 1$, then $1 - p < 0$, so $2^{1-p} < 1$ and $1 - 2^{1-p}$ is positive. Hence $(\sum f_p)(n) \leq \frac{1}{1 - 2^{1-p}}$; i.e., the sequence $\sum f_p$ is bounded. It is also increasing, so it converges.

If $p < 1$, then $\frac{1}{n^p} \geq \frac{1}{n}$, so by using the comparison test with the harmonic series, f_p is not summable. ‖

11.14 Remark. For $p > 1$, the proof of the previous theorem shows that

$$\sum_{j=1}^{\infty} \frac{1}{n^p} = \lim \sum f_p \leq \frac{1}{1 - 2^{1-p}}.$$

Hence, we get

$$\sum_{n=1}^{\infty} \frac{1}{n^2} \leq \frac{1}{1 - 2^{-1}} = 2,$$

and

$$\sum_{n=1}^{\infty} \frac{1}{n^4} \leq \frac{1}{1 - 2^{-3}} = \frac{8}{7} = 1.1428\cdots.$$

The exact values of the series (found by Euler) are

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6} = 1.6449\cdots$$

and

$$\sum_{n=1}^{\infty} \frac{1}{n^4} = \frac{\pi^4}{90} = 1.0823\cdots.$$

11.15 Examples. $\left\{\frac{1}{n^2 + n^{1/2}}\right\}_{\geq 1}$ is summable, since

$$0 \leq \frac{1}{n^2 + n^{1/2}} \leq \frac{1}{n^2} \text{ for all } n \in \mathbf{Z}_{\geq 1}$$

and $\left\{\frac{1}{n^2}\right\}$ is summable.

$\left\{\frac{1}{1 + n^{1/2}}\right\}_{n \geq 1}$ is not summable since

$$\frac{1}{1 + n^{1/2}} \geq \frac{1}{n^{1/2} + n^{1/2}} = \frac{1}{2} \cdot \frac{1}{n^{1/2}} \text{ for all } n \in \mathbf{Z}_{\geq 1}$$

and $\left\{\frac{1}{n^{1/2}}\right\}_{n \geq 1}$ is not summable.

11.16 Example. Let $w = \frac{3}{5} + \frac{4}{5}i$, and let $z \in D(0, 1)$. Then $\left\{\frac{1}{n^2 |z - w^n|}\right\}_{\geq 1}$ is summable.

Proof: By the reverse triangle inequality, we have for all $n \in \mathbf{Z}_{\geq 1}$

$$|z - w^n| \geq |w^n| - |z| = 1 - |z| > 0$$

so

$$0 \leq \frac{1}{n^2|z - w^n|} \leq \frac{1}{n^2(1 - |z|)} \text{ for all } n \in \mathbf{Z}_{\geq 1}.$$

Since $\left\{c \cdot \dfrac{1}{n^2}\right\}_{n \geq 1}$ is a summable sequence for all $c \in \mathbf{C}$, it follows from the comparison test that $\left\{\dfrac{1}{n^2|z - w^n|}\right\}_{n \geq 1}$ is summable. ∥

11.17 Example. Let $f(n) = \dfrac{(99.99)^n}{n!}$ for all $n \in \mathbf{N}$. Then

$$f(n+1) = \frac{(99.99)^{n+1}}{(n+1)!} = \frac{(99.99) \cdot (99.99)^n}{(n+1)n!} = \frac{99.99}{n+1} \cdot f(n).$$

If $n \geq 100$, then $n + 1 \geq 101$, so

$$f(n+1) = \frac{99.99}{n+1} \cdot f(n) \leq \frac{99.99}{101} f(n).$$

Hence,

$$\begin{aligned}
f(101) &\leq \left(\frac{99.99}{101}\right) f(100) \\
f(102) &\leq \left(\frac{99.99}{101}\right) \cdot f(101) \leq \left(\frac{99.99}{100}\right)^2 f(100) \\
f(103) &\leq \left(\frac{99.99}{101}\right) \cdot f(102) \leq \left(\frac{99.99}{100}\right)^3 f(100).
\end{aligned}$$

Hence, (by induction)

$$\begin{aligned}
f(100+n) &\leq \left(\frac{99.99}{101}\right)^n f(100) \\
&= \left(\frac{99.99}{101}\right)^{n+100} \left[\left(\frac{101}{99.99}\right)^{100} f(100)\right] \\
&= C\left(\frac{99.99}{101}\right)^{100+n}
\end{aligned}$$

where $C = \left(\frac{101}{99.99}\right)^{100} f(100)$; i.e., $f(j) \le C\left(\frac{99.99}{101}\right)^j$ for all $j > 100$. Since the geometric series $\left\{\sum_{j=0}^{n}\left(\frac{99.99}{101}\right)^j\right\}$ converges, it follows from the comparison test that $\left\{\sum_{j=0}^{n}\frac{(99.99)^j}{j!}\right\}$ converges also.

11.18 Exercise. Determine whether or not the sequences below are summable:

(a) $\{(-1)^n\}$

(b) $\{(-1)^n + (-1)^{n+1}\}$

(c) $\{(-1)^n\} + \{(-1)^{n+1}\}$

(d) $\left\{\frac{n^2}{n^4+1}\right\}_{n\ge 1}$

(e) $\left\{1 - \frac{n}{n+1}\right\}_{n\ge 1}$

(f) $\left\{\frac{1}{n^3+\sqrt{n}}\right\}_{n\ge 1}$

(g) $\left\{\frac{n^2+n}{n^4+1}\right\}_{n\ge 1}$

(h) $\left\{\frac{3^n}{n!}\right\}$

11.19 Exercise. Give examples of the following, or explain why no such examples exist.

a) Two real sequences f and g such that f and g are not summable, but $f+g$ is summable.

b) Two real sequences f and g such that f and g are summable, but $f+g$ is not summable.

c) Two real sequences f and g such that $f(n) < g(n)$ for all $n \in \mathbf{N}$, and g is summable but f is not summable.

11.20 Theorem (Limit comparison test.) *Let f, g be sequences of positive numbers. Suppose that $\dfrac{f}{g}$ converges to a non-zero limit L. Then f is summable if and only if g is summable.*

Proof: We know that $L > 0$. Let $N = N_{\frac{f}{g}-\tilde{L}}$ be a precision function for $\dfrac{f}{g} - \tilde{L}$. Then

$$\left|\frac{f(n)}{g(n)} - L\right| \leq \frac{L}{2} \text{ for all } n \geq N\left(\frac{L}{2}\right);$$

i.e.,

$$\frac{L}{2} \leq \frac{f(n)}{g(n)} \leq \frac{3L}{2} \text{ for all } n \geq N\left(\frac{L}{2}\right).$$

If g is summable, then $\dfrac{3L}{2}g$ is summable, and since $f(n) \leq \dfrac{3L}{2}g(n)$ for all $n \geq N\left(\dfrac{L}{2}\right)$, it follows from the comparison test that f is summable. If g is not summable, then since $g(n) \leq \frac{2}{L}f(n)$ for all $n \geq N(\frac{l}{2})$ it follows that $\dfrac{2}{L}f$ is not summable, and hence f is not summable. |||

11.21 Example. Is $\left\{\dfrac{n^2+5n+1}{6n^3+3n-2}\right\}_{n\geq 1}$ summable? Let $a_n = \dfrac{n^2+5n+1}{6n^3+3n-2}$. Note that $a_n > 0$ for all $n \in \mathbf{Z}_{\geq 1}$. For large n, a_n is "like" $\dfrac{n^2}{6n^3} = \dfrac{1}{6n}$, so I'll compare this series with $\left\{\dfrac{1}{n}\right\}_{n\geq 1}$. Let $b_n = \dfrac{1}{n}$ for all $n \in \mathbf{Z}_{\geq 1}$. Then

$$\frac{a_n}{b_n} = \frac{n^3+5n^2+n}{6n^3+3n-2} = \frac{1+\frac{5}{n}+\frac{1}{n^3}}{6+\frac{3}{n^2}-\frac{2}{n^3}},$$

so

$$\left\{\frac{a_n}{b_n}\right\}_{n\geq 1} = \left\{\frac{1+\frac{5}{n}+\frac{1}{n^3}}{6+\frac{3}{n^2}-\frac{2}{n^3}}\right\}_{n\geq 1} \to \frac{1+0+0}{6+0+0} = \frac{1}{6} \neq 0.$$

Since $\{b_n\}_{n\geq 1} = \left\{\dfrac{1}{n}\right\}_{n\geq 1}$ is not summable, $\left\{\dfrac{n^2+5n+1}{6n^3+3n-2}\right\}_{n\geq 1}$ is also not summable.

11.22 Exercise. Determine whether or not the sequences below are summable.

a) $\left\{\dfrac{n^2+3n+2}{n^4+n+1}\right\}_{n\geq 1}$.

b) $\left\{\dfrac{n+n^2}{n^3+n+1}\right\}_{n\geq 1}$.

11.23 Theorem (Ratio test.) *Let $\{a_n\}$ be a sequence of positive numbers. Suppose the $\left\{\dfrac{a_{n+1}}{a_n}\right\}$ converges, and $\lim\left\{\dfrac{a_{n+1}}{a_n}\right\} = R$. Then, if $R < 1$, $\{a_n\}$ is summable. If $R > 1$, $\{a_n\}$ is not summable. (If $R = 1$, the theorem makes no assertion.)*

Proof: Suppose $\left\{\dfrac{a_{n+1}}{a_n}\right\} \to R$.

Case 1: $R < 1$. Let N be a precision function for $\left\{\dfrac{a_{n+1}}{a_n} - R\right\}$. Then for all $n \in \mathbf{N}$,

$$\begin{aligned} n \geq N\left(\frac{1-R}{2}\right) &\implies \left|\frac{a_{n+1}}{a_n} - R\right| < \frac{1-R}{2} \\ &\implies \frac{a_{n+1}}{a_n} < R + \frac{1-R}{2} = \frac{R+1}{2}. \end{aligned}$$

Write $M = N\left(\dfrac{1-R}{2}\right)$ and $S = \dfrac{1+R}{2}$, so $(0 < S < 1)$. Then

$$n \geq M \implies a_{n+1} \leq S \cdot a_n,$$

so

$$\begin{aligned} a_M &\leq S^0 a_M \\ a_{M+1} &\leq S a_M \\ a_{M+2} &\leq S \cdot a_{M+1} \leq S^2 a_M \\ a_{M+3} &\leq S \cdot a_{M+2} \leq S^3 a_M, \end{aligned}$$

and (by an induction argument which I omit)

$$a_{M+k} \leq S^k a_M \text{ for all } k \in \mathbf{N},$$

or

$$a_{M+k} \le S^{M+k}(a_M S^{-M}) \text{ for all } k \in \mathbf{N},$$

or

$$a_n \le S^n(a_M S^{-M}) \text{ for all } n \in \mathbf{Z}_{\ge M}.$$

Since $\{S^n\}$ is a summable geometric series, it follows from the comparison test that $\{a_n\}$ is also summable.

Case 2: $(R > 1)$. As before, let N be a precision function for $\left\{\dfrac{a_{n+1}}{a_n} - R\right\}$. Then for all $n \in \mathbf{N}$,

$$\begin{aligned} n \ge N\left(\frac{R-1}{2}\right) &\implies \left|\frac{a_{n+1}}{a_n} - R\right| < \frac{R-1}{2} \\ &\implies \frac{a_{n+1}}{a_n} > R - \left(\frac{R-1}{2}\right) = \frac{R+1}{2} > 1 \\ &\implies a_{n+1} > a_n. \end{aligned}$$

Hence $\{a_n\}$ is not a null sequence. So $\{a_n\}$ is not summable. |||

11.24 Warning. The ratio test does not say that if $\dfrac{a_{n+1}}{a_n} < 1$ for all n, then $\{a_n\}$ is summable. If $a_n = \dfrac{1}{n}$ for $n \in \mathbf{Z}_{\ge 1}$, then $\dfrac{a_{n+1}}{a_n} = \dfrac{n}{n+1} < 1$ for all n but $\{a_n\}$ is not summable. (In this case, $\lim\left\{\dfrac{a_{n+1}}{a_n}\right\} = 1$, and the ratio test does not apply.)

If $b_n = \dfrac{1}{n^2}$ for all $n \in \mathbf{Z}_{\ge 1}$, then $\dfrac{b_{n+1}}{b_n} = \left(\dfrac{n^2}{(n+1)^2}\right)$ for all n and hence $\lim\left\{\dfrac{b_{n+1}}{b_n}\right\} = 1$, and $\{b_n\}$ is summable. These examples show that when $\lim\left\{\dfrac{a_{n+1}}{a_n}\right\} = 1$ the ratio test gives no useful information.

11.25 Remark. If, in applying the ratio test, you find that $\dfrac{a_{n+1}}{a_n} \ge 1$ for all large n, you can conclude that $\sum\{a_n\}$ diverges (even if $\lim\left\{\dfrac{a_{n+1}}{a_n}\right\}$ does not exist), since this condition shows that $\{a_n\}$ is not a null sequence.

11.26 Example. Let t be a positive number and let $a_n = \dfrac{(3n)!t^n}{(n!)^3}$. We apply the ratio test to the series $\sum\{a_n\}$.

$$\frac{a_{n+1}}{a_n} = \frac{(3(n+1))!t^{n+1}(n!)^3}{[(n+1)!]^3(3n)!t^n}.$$

Note that

$$\begin{aligned}(3(n+1))! &= (3n+3)! = (3n+3)(3n+2)! = (3n+3)(3n+2)(3n+1)! \\ &= (3n+3)(3n+2)(3n+1)(3n)!.\end{aligned}$$

Hence

$$\begin{aligned}\frac{a_{n+1}}{a_n} &= \frac{(3n)!t\cdot(3n+3)(3n+2)(3n+1)}{(3n)!}\left(\frac{n!}{(n+1)!}\right)^3 \\ &= t\left(\frac{3n+3}{n+1}\right)\left(\frac{3n+2}{n+1}\right)\left(\frac{3n+1}{n+1}\right) \\ &= t\cdot 3\cdot\left(\frac{3+\frac{2}{n}}{1+\frac{1}{n}}\right)\left(\frac{3+\frac{1}{n}}{1+\frac{1}{n}}\right).\end{aligned}$$

From this we see that $\left\{\dfrac{a_{n+1}}{a_n}\right\} \to 27t$. The ratio test says that if $27t < 1$ (i.e., if $t < \frac{1}{27}$), then $\left\{\dfrac{(3n)!t^n}{(n!)^3}\right\}$ is summable, and if $t > \frac{1}{27}$, then the sequence is not summable.

Can we figure out what happens in the case $t = \dfrac{1}{27}$? For $t = \dfrac{1}{27}$, our formula above gives us

$$\frac{a_{n+1}}{a_n} = \frac{\left(1+\frac{2}{3n}\right)\left(1+\frac{1}{3n}\right)}{\left(1+\frac{1}{n}\right)\left(1+\frac{1}{n}\right)} = \frac{1+\frac{1}{n}+\frac{2}{9n^2}}{\left(1+\frac{1}{n}\right)^2} > \frac{\left(1+\frac{1}{n}\right)}{\left(1+\frac{1}{n}\right)^2} = \frac{n}{n+1};$$

i.e., $a_{n+1} > \dfrac{n}{n+1}a_n$ for $n \geq 1$. Thus,

$$\begin{aligned}a_2 &\geq \frac{1}{2}\cdot a_1 \\ a_3 &\geq \frac{2}{3}a_2 \geq \frac{2}{3}\cdot\frac{1}{2}a_1 = \frac{1}{3}a_1 \\ a_4 &\geq \frac{3}{4}a_3 \geq \frac{3}{4}\cdot\frac{1}{3}a_1 = \frac{1}{4}a_1 \\ a_5 &\geq \frac{4}{5}a_4 \geq \frac{4}{5}\cdot\frac{1}{4}a_1 = \frac{1}{5}a_1\end{aligned}$$

and (by induction),

$$a_n \geq \frac{1}{n} a_1 \text{ for } n \geq 1.$$

Since $\left\{\frac{a_1}{n}\right\}_{n\geq 1}$ is not summable, it follows that $\{a_n\}$ is not summable for $t = \frac{1}{27}$.

11.27 Example. Let $b_n = \frac{(n!)^2 4^n}{(2n)!}$ for all $n \in \mathbf{N}$. I'll apply ratio test to $\sum\{b_n\}$. For all $n \in \mathbf{N}$,

$$\begin{aligned} \frac{b_{n+1}}{b_n} &= \frac{(n+1)!^2 4^{n+1}}{(2n+2)!} \cdot \frac{(2n)!}{(n!)^2 4^n} \\ &= \frac{(n+1)^2 \cdot 4}{(2n+1)(2n+2)} = \frac{2n+2}{2n+1} = \frac{1+\frac{1}{n}}{1+\frac{1}{2n}} \end{aligned}$$

Hence $\left\{\frac{b_{n+1}}{b_n}\right\} \to 1$ and the ratio test does not apply. But since $\frac{2n+2}{2n+1} > 1$ for all n, I conclude that $\{b_n\}$ is an increasing sequence and hence $\sum\{b_n\}$ diverges.

11.28 Exercise. For each of the series below, determine for which $x \in [0, \infty)$ the series converges.

a) $\sum\left\{\frac{x^n}{n!}\right\}$

b) $\sum\left\{\frac{x^{2n}}{(2n)!}\right\}$

c) $\sum\left\{\frac{3^n x^n}{n^2}\right\}_{n\geq 1}$

d) $\sum\left\{\frac{x^n}{2^n\sqrt{n}}\right\}_{n\geq 1}$

e) $\sum\{nx^n\}_{n\geq 1}$

f) $\sum\{n!x^n\}$

g) $\sum\left\{\frac{(n!)^2 x^n}{(2n)!}\right\}$ [For this series, there is one $x \in [0, \infty)$ for which you don't need to answer the question.]

11.3 Alternating Series

11.29 Definition (Alternating series.) Series of the form $\sum\{(-1)^n a_n\}$ or $\sum\{(-1)^{n+1} a_n\}$ where $a_j \geq 0$ for all j are called *alternating series.*

11.30 Theorem (Alternating series test.) *Let f be a decreasing sequence of positive numbers such that $\{f(n)\} \to 0$. Then $\{(-1)^n f(n)\}$ is summable. Moreover,*

$$\sum_{j=0}^{2m+1} (-1)^j f(j) \leq \sum_{j=0}^{\infty} (-1)^j f(j) \leq \sum_{j=0}^{2n} (-1)^j f(j)$$

and

$$\left|\sum_{j=0}^{n} (-1)^j f(j) - \sum_{j=0}^{\infty} (-1)^j f(j)\right| \leq f(n+1)$$

for all $m, n \in \mathbf{N}$.

Proof: Let $S_n = \sum_{j=0}^{n} (-1)^j f(j)$. For all $n \in \mathbf{N}$,

$$S_{2(n+1)} = S_{2n+2} = S_{2n} - f(2n+1) + f(2n+2) \leq S_{2n}$$

and

$$S_{2(n+1)+1} = S_{2n+1} + f(2n+2) - f(2n+3) \geq S_{2n+1}.$$

Thus $\{S_{2n}\}$ is decreasing and $\{S_{2n+1}\}$ is increasing. Also, for all $n \in \mathbf{N}$,

$$S_1 \leq S_{2n+1} = S_{2n} - f(2n+1) \leq S_{2n}$$

so $\{S_{2n}\}$ is bounded below by S_1, and

$$S_{2n+1} = S_{2n} - f(2n+1) \leq S_{2n} \leq S_0$$

so $\{S_{2n+1}\}$ is bounded above by S_0.

It follows that there exist real numbers L and M such that

$$\{S_{2n}\} \to L \text{ and } S_{2n} \geq L \text{ for all } n \in \mathbf{N}$$
$$\{S_{2n+1}\} \to M \text{ and } S_{2n+1} \leq M \text{ for all } n \in \mathbf{N}.$$

Now

$$\begin{aligned} L - M &= \lim\{S_{2n}\} - \lim\{S_{2n+1}\} = \lim\{S_{2n} - S_{2n+1}\} \\ &= \lim\{f(2n+1)\} = 0, \end{aligned}$$

so $L = M$.

It follows from the next lemma that $\{S_n\} \to L$; i.e.,

$$M = L = \lim S_n = \sum_{n=0}^{\infty} (-1)^n f(n).$$

Since for all $n \in \mathbf{N}$

$$S_{2n+1} \leq L \leq S_{2n},$$

we have

$$|L - S_{2n}| \leq S_{2n} - S_{2n+1} = f(2n+1)$$

and since

$$\begin{aligned} S_{2n+1} \leq L &\leq S_{2n+2} \\ |L - S_{2n+1}| &\leq S_{2n+2} - S_{2n+1} = f(2n+2). \end{aligned}$$

Thus, in all cases, $|L - S_n| < f(n+1)$; i.e., $\sum_{j=0}^{n} (-1)^j f(j)$ approximates $\sum_{j=0}^{\infty} (-1)^j f(j)$ with an error of no more than $f(n+1)$. ‖

11.31 Lemma. *Let $\{a_n\}$ be a real sequence and let $L \in \mathbf{R}$. Suppose $\{a_{2n}\} \to L$ and $\{a_{2n+1}\} \to L$. Then $\{a_n\} \to L$.*

Proof: Let N be a precision function for $\{a_{2n} - L\}$ and let M be a precision function for $\{a_{2n+1} - L\}$. For all $\varepsilon \in \mathbf{R}^+$, define

$$N_{a-\tilde{L}}(\varepsilon) = \max\left(2N(\varepsilon), 2M(\varepsilon) + 1\right).$$

I claim $N_{a-\tilde{L}}$ is a precision function for $a - \tilde{L}$, and hence $a \to L$. Let $n \in \mathbf{N}$.

Case 1: n is even. Suppose n is even. Say $n = 2k$ where $k \in \mathbf{N}$. Then

$$\begin{aligned} (n \geq N_{a-\tilde{L}}(\varepsilon) &\implies 2k \geq N_{a-\tilde{L}}(\varepsilon) \geq 2N(\varepsilon) \\ &\implies k > N(\varepsilon) \implies |a_{2k} - L| < \varepsilon \\ &\implies |a_n - L| < \varepsilon, \end{aligned}$$

Case 2: n is odd. Suppose n is odd. Say $n = 2k+1$ where $k \in \mathbf{N}$. Then

$$\begin{aligned} (n \geq N_{a-\tilde{L}}(\varepsilon) &\implies 2k+1 \geq N_{a-\tilde{L}}(\varepsilon) \geq 2M(\varepsilon) + 1 \\ &\implies k \geq M(\varepsilon) \implies |a_{2k+1} - L| < \varepsilon \\ &\implies |a_n - L| < \varepsilon. \end{aligned}$$

Hence, in all cases,

$$n \geq N_{a-\tilde{L}}(\varepsilon) \implies |a_n - L| < \varepsilon. \ \|$$

11.32 Remark. The alternating series test has obvious generalizations for series such as

$$\sum\{(-1)^{j+1} f(j)\} \text{ or } \sum\{(-1)^j f(j)\}_{j\geq k},$$

and we will use these generalizations.

11.33 Example. If $0 \leq t \leq 1$, then

$$\left\{\frac{t^{2n}}{(2n)!}\right\} \text{ and } \left\{\frac{t^{2n+1}}{(2n+1)!}\right\}$$

are decreasing positive null sequences, so

$$\left\{\frac{(-1)^n t^{2n}}{(2n)!}\right\} \text{ and } \left\{\frac{(-1)^n t^{2n+1}}{(2n+1)!}\right\}$$

are summable; i.e.,

$$\left\{\sum_{j=0}^{n} \frac{(-1)^j t^{2j}}{(2j)!}\right\} \text{ and } \left\{\sum_{j=0}^{n} \frac{(-1)^j t^{2j+1}}{(2j+1)!}\right\} \text{ converge.}$$

(These are the sequences we called $\{C_n(t)\}$ and $\{S_n(t)\}$ in example 10.45.)

Also, $\displaystyle\sum_{j=0}^{\infty} \frac{(-1)^j \left(\frac{1}{10}\right)^{2j}}{(2j)!} = 1 - \frac{1}{200} + \frac{1}{240000}$, with an error smaller than $\dfrac{1}{720000000}$. My calculator says

$$\cos(.1) = 0.995004165$$

and

$$1 - \frac{1}{200} + \frac{1}{240000} = 0.995004166.$$

11.34 Entertainment. Since $\left\{\dfrac{t^n}{n}\right\}_{n\geq 1}$ is a decreasing positive null sequence for $0 \leq t \leq 1$, it follows that $\displaystyle\sum\left\{\frac{(-1)^{n-1} t^n}{n}\right\}_{n\geq 1}$ converges for

$0 \le t \le 1$. We will now explicitly calculate the limit of this series using a few ideas that are not justified by results proved in this course. We know that for all $x \in \mathbf{R} \setminus \{-1\}$, and all $n \in \mathbf{N}$,

$$1 - x + x^2 - x^3 + \cdots + (-x)^{n-1} = \frac{1-(-x)^n}{1-(-x)} = \frac{1}{1+x} + (-1)^{n+1}\frac{x^n}{1+x}.$$

Hence, for all $t > -1$,

$$\int_0^t 1 - x + x^2 + \cdots + (-x)^{n-1}dx = \int_0^t \frac{1}{1+x}dx + (-1)^{n+1}\int_0^t \frac{x^n}{1+x}dx;$$

i.e.,

$$x - \frac{x^2}{2} + \frac{x^3}{3} + \cdots + \frac{(-1)^{n-1}x^n}{n}\Big|_0^t = \ln(1+x)\Big|_0^t + (-1)^{n+1}\int_0^t \frac{x^n}{1+x}dx.$$

Thus

$$t - \frac{t^2}{2} + \frac{t^3}{3} + \cdots + \frac{(-1)^{n-1}t^n}{n} = \ln(1+t) + (-1)^{n+1}\int_0^t \frac{x^n}{1+x}dx.$$

Hence

$$\left|t - \frac{t^2}{2} + \frac{t^3}{3} + \cdots + \frac{(-1)^{n-1}t^n}{n} - \ln(1+t)\right| = \left|\int_0^t \frac{x^n}{1+x}dx\right|$$

for all $t > -1$.

If we can show that $\left\{\int_0^t \frac{x^n}{1+x}dx\right\}$ is a null sequence, it follows that

$$\left\{t - \frac{t^2}{2} + \frac{t^3}{3} + \cdots + \frac{(-1)^{n-1}t^n}{n}\right\} \to \ln(1+t),$$

or in other words,

$$\ln(1+t) = \sum_{j=1}^{\infty} \frac{(-1)^{j+1}t^j}{j}. \qquad (11.35)$$

I claim $\left\{\int_0^t \frac{x^n}{1+x}dx\right\}$ is a null sequence for $-1 < t \le 1$ and hence (11.35) holds for $-1 < t \le 1$. In particular,

$$\ln(2) = 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \frac{1}{5} - \frac{1}{6} + \cdots.$$

First suppose $t \geq 0$, then $\dfrac{1}{1+x}x^n \leq x^n$ for $0 \leq x \leq t$, so

$$0 = \int_0^t \frac{1}{1+x} \cdot x^n dx \leq \int_0^t x^n dx = \left.\frac{x^{n+1}}{n+1}\right|_0^t = \frac{t^{n+1}}{n+1}.$$

Since $\left\{\dfrac{t^{n+1}}{n+1}\right\}$ is a null sequence for $0 \leq t \leq 1$, it follows from the comparison test that $\left\{\displaystyle\int_0^t \frac{x^n}{1+x}dx\right\}$ is a null sequence for $0 \leq t \leq 1$. Now suppose $-1 < t < 0$. Then

$$\frac{1}{1+x} \leq \frac{1}{1+t} \text{ for } t \leq x \leq 0,$$

so $\dfrac{|x|^n}{1+x} \leq \dfrac{|x|^n}{1+t}$ and

$$\begin{aligned}
\left|\int_0^t \frac{x^n}{1+x}dx\right| &= \int_t^0 \frac{|x|^n}{1+x}dx \leq \int_t^0 \frac{|x|^n}{1+t}dx \\
&= \frac{1}{1+t}\int_t^0 |x|^n dx = \frac{1}{1+t}\int_0^{|t|} x^n dx \\
&= \frac{1}{1+t} \cdot \frac{|t|^{n+1}}{n+1}.
\end{aligned}$$

If $-1 < t < 0$, then $\left\{\dfrac{1}{1+t} \cdot \dfrac{|t|^{n+1}}{n+1}\right\}$ is a null sequence, so $\left\{\displaystyle\int_0^t \frac{x^n}{1+x}dx\right\}$ is a null sequence. ‖

11.36 Entertainment. By starting with the formula

$$1 - x^2 + x^4 - x^6 + \cdots + (-x^2)^{n-1} = \frac{1-(-x^2)^n}{1-(-x^2)}$$

for all $x \in \mathbf{R}$ and using the ideas from the last example, show that

$$\sum_{j=0}^{\infty} \frac{(-1)^j x^{2j+1}}{(2j+1)} = \arctan(x) \text{ for all } x \in [-1,1]. \tag{11.37}$$

Conclude that

$$\frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \frac{1}{11} + \cdots$$

11.38 Exercise. Determine whether or not the following series converge.

a) $\sum\left\{(-1)^n\frac{n+1}{n^2}\right\}_{n\geq 1}$

b) $\sum\left\{(-1)^n\frac{n+1}{n}\right\}_{n\geq 1}$

c) $\sum\left\{\frac{(-1)^n t^{2n}}{(2n)!}\right\}$ (assume here $-1\leq t\leq 1$).

11.4 Absolute Convergence

11.39 Definition (Absolute Convergence.) Let f be a complex sequence. We say that f is *absolutely summable* if and only if $|f|$ is summable; i.e., if and only if $\{\sum_{j=0}^{n}|f(j)|\}$ converges. In this case, we also say that the series $\sum f$ is *absolutely convergent.*

11.40 Example. $\sum\left\{\frac{(-1)^n}{n}\right\}_{n\geq 1}$ is convergent, but is not absolutely convergent.

11.41 Theorem. *Let f be a complex sequence. If $\sum f$ is absolutely convergent, then $\sum f$ is convergent.*

Proof:

Case 1: Suppose $f(n)$ is real for all $n\in\mathbf{N}$, and that $\sum|f|$ converges. Then

$$0\leq f(n)+|f(n)|\leq|f(n)|+|f(n)|=2|f(n)|$$

for all $n\in\mathbf{N}$, so by the comparison test, $\sum(f+|f|)$ converges. Then $\sum(f+|f|)-\sum|f|$, being the difference of two convergent sequences, is convergent; i.e., $\sum f$ converges.

Case 2: Suppose f is an arbitrary absolutely convergent complex series. We know that for all $n\in\mathbf{N}$,

$$0\leq|\text{Re}(f)(n)|\leq|f(n)|$$

and

$$0 \leq |\text{Im}(f)(n)| \leq |f(n)|,$$

so by the comparison test, $\sum|\text{Re}(f)|$ and $\sum|\text{Im}(f)|$ are convergent, and by Case 1, $\sum(\text{Re}(f))$ and $\sum(\text{Im}(f))$ are convergent. It follows that $\sum(\text{Re}(f)) + i\sum(\text{Im}(f)) = \sum f$ is convergent. $\|$

11.42 Example. Let z be a non-zero complex number. Let

$$\{C_n(z)\} = \sum\{c_n(z)\} = \left\{\sum_{j=0}^{n} \frac{z^{2j}(-1)^j}{(2j)!}\right\}.$$

I claim $\sum\{c_n\}$ is absolutely convergent (and hence convergent). We have

$$|c_n(z)| = \frac{|z|^{2n}}{(2n)!}.$$

We have

$$\left\{\frac{|c_{n+1}(z)|}{|c_n(z)|}\right\} = \left\{\frac{|z|^{2n+2}}{(2n+2)!}\frac{(2n)!}{|z|^{2n}}\right\} = \left\{\frac{|z|^2}{(2n+1)(2n+2)}\right\} \to 0 < 1$$

so by the ratio test, $\sum\{|c_n(z)|\}$ converges. Hence $\sum\{c_n(z)\}$ is absolutely convergent, and hence it is convergent. Clearly $\{C_n(0)\} \to 1$, so $\{C_n(z)\}$ converges for all $z \in \mathbf{C}$. In the exercises you will show that $\sum\left\{\frac{(-1)^j z^{2j+1}}{(2j+1)!}\right\}$ is also convergent for all $z \in \mathbf{C}$.

Motivated by the results of section 10.3, we make the following definitions:

11.43 Definition (sin **and** cos.) For all $z \in \mathbf{C}$, we define

$$\begin{aligned} \cos(z) &= \sum_{j=0}^{\infty} \frac{(-1)^j z^{2j}}{(2j)!}. \\ \sin(z) &= \sum_{j=0}^{\infty} \frac{(-1)^j z^{2j+1}}{(2j+1)!}. \end{aligned}$$

11.44 Remark. It is clear from the definition that

$\sin(0) = 0$ and $\cos(0) = 1$.

$\sin(-z) = -\sin(z)$ for all $z \in \mathbf{C}$.

$\cos(-z) = \cos(z)$ for all $z \in \mathbf{C}$.

For all $n \in \mathbf{N}$, $z \in \mathbf{C}$, let

$$\begin{aligned} C_n(z) &= \sum_{j=0}^{n} \frac{(-1)^j z^{2j}}{(2j)!}, \\ S_n(z) &= \sum_{j=0}^{n} \frac{(-1)^j z^{2j+1}}{(2j+1)!}. \end{aligned}$$

Then

$$\begin{aligned} S_n'(z) &= \sum_{j=0}^{n} \frac{(-1)^j (2j+1) z^{2j}}{(2j+1)!} \\ &= \sum_{j=0}^{n} \frac{(-1)^j z^{2j}}{(2j)!} = C_n(z). \end{aligned}$$

I would now like to be able to say that for all $z \in \mathbf{C}$,

$$\begin{aligned} \{S_n(z)\} \to S(z) &\implies \{S_n'(z)\} \to S'(z) \\ &\implies \{C_n(z)\} \to S'(z) \\ &\implies S'(z) = C(z) \text{ (since } \{C_n\} \to C); \end{aligned}$$

i.e., I would like to have a theorem that says

$$\{f_n(z)\} \to f(z) \implies \{f_n'(z)\} \to f'(z).$$

However, the next example shows that this hoped for theorem is not true.

11.45 Example. Let $f_n(z) = \dfrac{z}{1+nz^2}$ for all $z \in \mathbf{C}$, $n \in \mathbf{Z}_{\geq 1}$. Then for all $z \in \mathbf{C} \setminus \{0\}$,

$$\{f_n(z)\} = \frac{z}{n} \frac{1}{\left(\frac{1}{n} + z^2\right)} \to 0 \cdot \frac{1}{0 + z^2} = 0,$$

and

$$\{f_n(0)\} = \{0\} \to 0,$$

so

$$f_n(z) \to \tilde{0}(z) \text{ for all } z \in \mathbf{C}.$$

Now $f_n'(z) = \dfrac{(1+nz^2) - 2nz^2}{(1+nz^2)^2} = \dfrac{1-nz^2}{(1+nz^2)^2}$. So $f_n'(0) = 1$ for all n, and thus $\{f_n'(0)\} \to 1 \neq \tilde{0}'(0)$. Eventually we will show that $\sin' = \cos$ and $\cos' = -\sin$, but it will require some work.

11.46 Warning. Defining sine and cosine in terms of infinite series can be dangerous to the well being of the definer. In 1933 Edmund Landau was forced to resign from his position at the University of Göttingen as a result of a Nazi-organized boycott of his lectures. Among other things, it was claimed that Landau's definitions of sine and cosine in terms of power series was "un-German", and that the definitions lacked "sense and meaning" [33, pp 226–227].

11.47 Exercise. Show that $\sum\left\{\dfrac{(-1)^n z^{2n+1}}{(2n+1)!}\right\}$ converges for all $z \in \mathbf{C}$.

11.48 Exercise.

a) Does the series $\sum\left\{\dfrac{\left(\frac{3}{5}+\frac{4i}{5}\right)^n}{n^2}\right\}_{n\geq 1}$ converge?

b) Does the sequence $\left\{\displaystyle\sum_{j=1}^{4n}\frac{i^j}{j}\right\}_{n\geq 1}$ converge?

11.49 Exercise.

a) For what complex numbers z does $\sum\{nz^n\}$ converge?

b) For what complex numbers z does $\sum\{z^{(n^2)}\}$ converge?

11.50 Note. The harmonic series was shown to be unbounded by Nicole Oresme c. 1360 [31, p437]. However, many 17th and 18th century mathematicians believed that (in our terminology) every null sequence is summable. Jacob Bernoulli rediscovered Oresme's result in 1687, and reported that it contradicted his earlier belief that an infinite series whose last term vanishes must be finite[31, p 437]. As late as 1770, Lagrange said that a series represents a number if its nth term approaches 0 [31, p 464].

The ratio test was stated by Jean D'Alembert in 1768, and by Edward Waring in 1776[31, p 465]. D'Alembert knew that the ratio test guaranteed absolute convergence.

The alternating series test appears in a letter from Leibniz to Jacob Bernoulli written in 1713[31, p461].

The series (11.35) for $\ln(1+t)$ is called *Mercator's formula* after Nicolaus Mercator who published it in 1668. It was discovered earlier by Newton in 1664 when he was an undergraduate at Cambridge. After Newton read Mercator's book, he quickly wrote down some of his own ideas (which were much more general than Mercator's) and allowed his notes to be circulated, but not published. Newton used the logarithm formula to calculate $\ln(1.1)$ to 68 decimals (of which the 28th and 43rd were wrong), but a few years later, he redid the calculation and corrected the errors.

See [22, chapter 2] for a discussion of Newton's work on series.

The series representation for arctan (11.37) is called *Gregory's formula* after John Gregory (1638-1675) or *Leibniz's formula* after Gottfried Leibniz (1646-1716). However, it was known to sixteenth century Indian mathematicians who credited it to Madhava (c. 1340-1425). The Indian version was

$$\theta = \frac{\sin\theta}{\cos\theta} - \frac{1}{3}\frac{\sin^3\theta}{\cos^3\theta} + \frac{1}{5}\frac{\sin^5\theta}{\cos^5\theta}\cdots.$$

(See[30, p292].)

Chapter 12

Power Series

12.1 Definition and Examples

12.1 Definition (Power Series.) Let $\{a_n\}$ be a sequence of complex numbers. A series of the form $\sum\{a_n z^n\}$ is called a *power series.*

We think of a power series as a sequence of polynomials

$$\{a_0, a_0 + a_1 z, a_0 + a_1 z + a_2 z^2, a_0 + a_1 z + a_2 z^2 + a_3 z^3, \cdots\}.$$

In general, this sequence will converge for certain complex numbers, and diverge for other numbers. A power series $\sum\{a_n z^n\}$ determines a function whose domain is the set of all $z \in \mathbf{C}$ such that $\sum\{a_n z^n\}$ converges.

12.2 Examples. The geometric series $\sum\{z^n\}$ is a power series that converges to $\dfrac{1}{1-z}$ for $|z| < 1$ and diverges for $|z| \geq 1$.

The series $C = \sum \left\{ \dfrac{(-1)^n z^{2n}}{(2n)!} \right\}$ and $S = \sum \left\{ \dfrac{(-1)^n z^{2n+1}}{(2n+1)!} \right\}$ are power series that converge for all $z \in \mathbf{C}$. C corresponds to the sequence

$$\{a_n\} = \left\{1, 0, -\frac{1}{2}, 0, \frac{1}{24}, \cdots\right\}$$

and S corresponds to

$$\{a_n\} = \left\{0, 1, 0, -\frac{1}{6}, 0, \frac{1}{120}, \cdots\right\}.$$

The limits are $\cos z$ and $\sin z$, respectively (by definition 11.43.)

Every power series $\sum\{a_n z^n\}$ converges at $z = 0$. (The limit is a_0.)

The series $\sum\{n!z^n\}$ converges only when $z = 0$ (see exercise 12.5).

12.3 Notation (a^{b^c}) The expression a^{b^c} is ambiguous. Since

$$2^{(2^3)} = 2^8 = 256,$$

and

$$(2^2)^3 = 4^3 = 64,$$

we see that in general $a^{(b^c)} \neq (a^b)^c$. We make the convention that

$$a^{b^c} \text{ means } a^{(b^c)}.$$

The expression $(a^b)^c$ is usually simplified and written without parentheses by use of theorem 3.64:

$$(a^b)^c = a^{(bc)} = a^{bc}.$$

12.4 Example. I would like to consider the series $\sum\left\{\frac{z^{n^2}}{n^2}\right\}_{n\geq 1}$ to be a power series. This series corresponds to $\sum\{c_n z^n\}$ where

$$\begin{aligned}\{c_n\} &= \{0, 1, 0, 0, \frac{1}{4}, 0, 0, 0, 0, \frac{1}{9}, \cdots\} \\ \sum\{c_n z^n\} &= \{0, z, z, z, z + \frac{z^4}{4}, z + \frac{z^4}{4}, \cdots\},\end{aligned}$$

which is not identical with

$$\sum\left\{\frac{z^{n^2}}{n^2}\right\}_{n\geq 1} = \left\{z, z + \frac{z^4}{4}, z + \frac{z^4}{4} + \frac{z^9}{9}, \cdots\right\},$$

but you should be able to see that one series converges if and only if the other does, and that they have the same limits. In the future I will sometimes blur the distinctions between two series like this.

For $z \neq 0$, let $a_n = \dfrac{z^{n^2}}{n^2}$. Then

$$\frac{|a_{n+1}|}{|a_n|} = \left|\frac{z^{n^2+2n+1}}{(n+1)^2}\right|\left|\frac{n^2}{z^{n^2}}\right| = |z|^{2n+1}\left(\frac{n}{n+1}\right)^2.$$

If $|z| < 1$, then $|z|^{2n+1}\left(\dfrac{n}{n+1}\right)^2 \leq |z|^{2n+1}$ and $\lim\left\{\dfrac{|a_{n+1}|}{|a_n|}\right\}_{n\geq 1} = 0 < 1$, so by the ratio test, $\sum\left\{\dfrac{z^{n^2}}{n^2}\right\}_{n\geq 1}$ converges absolutely for $|z| < 1$.

If $|z| > 1$ and $n \geq 1$, then

$$\left\{\left|\frac{a_{n+1}}{a_n}\right|\right\} = |z|^{2n+1}\left(1 - \frac{1}{(n+1)}\right)^2 \geq |z|^{2n+1}\cdot\frac{1}{4},$$

so $\dfrac{|a_{n+1}|}{|a_n|} > 1$ for large n, and the series diverges. If $|z| = 1$, then $|a_n| = \dfrac{1}{n^2}$, so $\sum\{|a_n|\}$ converges by the comparison test, and $\sum\left\{\dfrac{z^{n^2}}{n^2}\right\}_{n\geq 1}$ converges absolutely. This shows that the function

$$f(z) = \sum_{n=1}^{\infty}\frac{z^{n^2}}{n^2}$$

is defined for all $z \in \bar{D}(0,1)$, and determines a function from $\bar{D}(0,1)$ into $\mathbf{C}$. The figure on page 229 shows the images under f of circles of radius $\dfrac{j}{10}$ for $1 \leq j \leq 10$ and of rays that divide the disc into twelve equal parts. The images of the interior circles are nice differentiable curves. The image of the boundary circle seems to have interesting properties that I do not know how to demonstrate.

12.5 Exercise.

a) Show that $\sum\{n!z^n\}$ converges only for $z = 0$.

b) Show that $\sum\left\{\dfrac{z^{2^n}}{2^n}\right\}$ converges if and only if $|z| \leq 1$. ‖

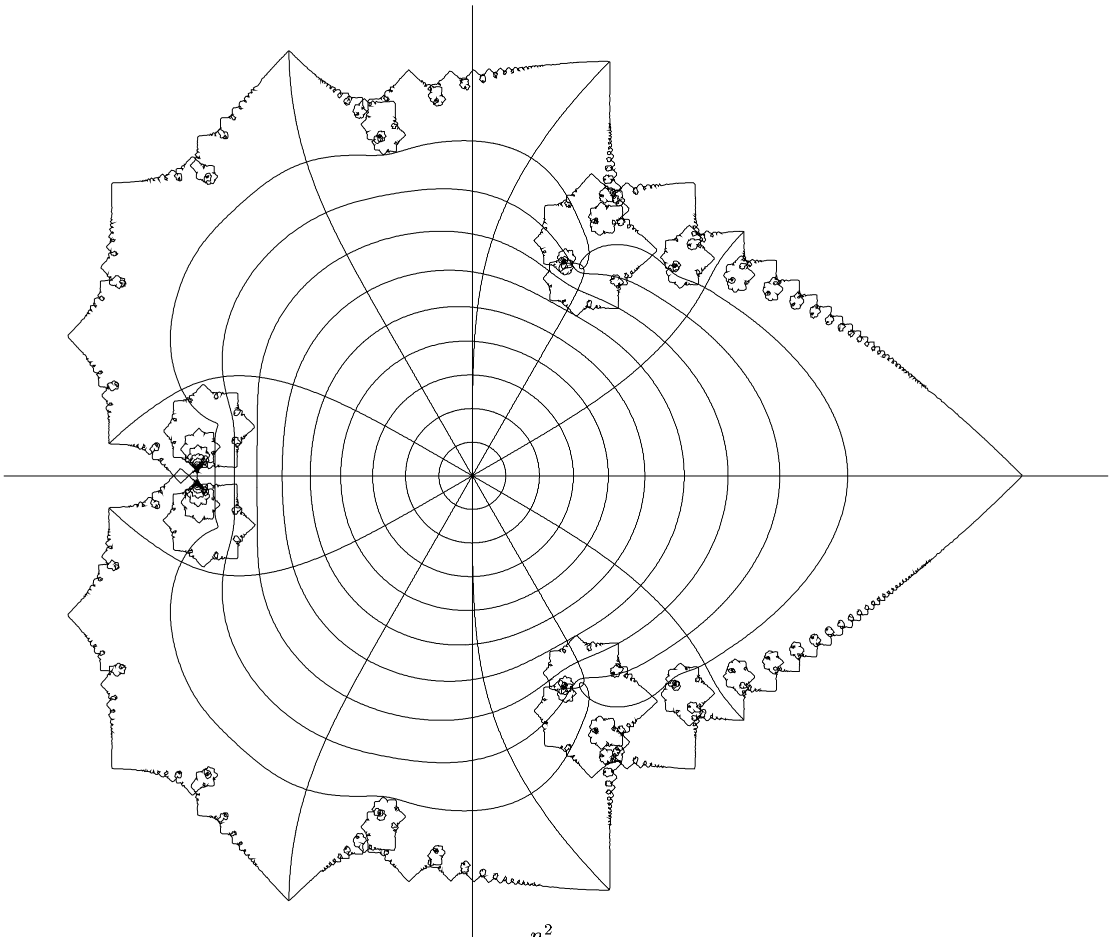


Image of $\sum \left\{ \frac{z^{n^2}}{n^2} \right\}_{n \geq 1}$

Let $g(z) = \sum_{n=0}^{\infty} \frac{z^{2^n}}{2^n}$ for $|z| \leq 1$.

The figure on page 230 shows the images under g of circles of radius $\frac{j}{10}$ for $1 \leq j \leq 10$, and of rays that divide the disc into 12 equal parts.

12.6 Exercise. Let $g(z) = \sum_{n=0}^{\infty} \frac{z^{2^n}}{2^n}$ for $|z| \leq 1$. It appears from figure on page 230 that $g(-1) = 0$, and $g(i)$ is pure imaginary. Show that this is the case.

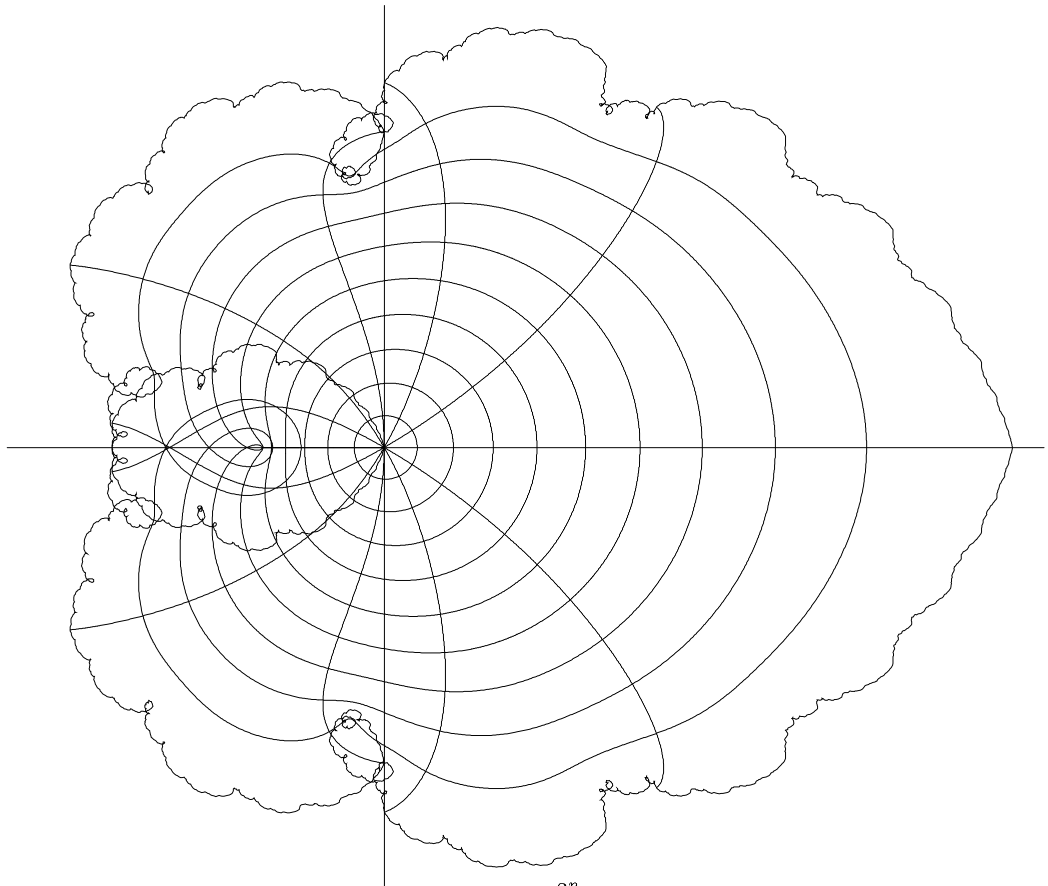


Image of $\sum\left\{\frac{z^{2^n}}{2^n}\right\}$

12.7 Entertainment. It appears from the image of $g(z)=\sum_{n=0}^{\infty}\frac{z^{2^n}}{2^n}$ that if $w=\frac{1}{2}+i\frac{\sqrt{3}}{2}$ (a cube root of -1), then $g(w)$ is pure imaginary, and has length a little larger than the length of $g(i)$. Show that this is the case. (From the fact that $w^3=-1$, notice that

$$\{w^1,w^2,w^4,w^8,w^{16},w^{32},w^{64},\cdots\}=\{w,w^2,-w,w^2,-w,w^2,-w,\cdots\}.)$$

12.2 Radius of Convergence

12.8 Theorem. *Let $\sum\{a_n z^n\}$ be a power series. Suppose $\sum\{a_n w^n\}$ converges for some $w \in \mathbf{C}\backslash\{0\}$. Then $\sum\{a_n z^n\}$ converges absolutely for all $z \in D(0, |w|)$.*

Proof: Since $\sum\{a_n w^n\}$ converges, $\{a_n w^n\}$ is a null sequence, and hence is bounded. Say $|a_n w^n| \leq M$ for all $n \in \mathbf{N}$. Let $z \in D(0, |w|)$, so $|z| < |w|$, and let $R = \dfrac{|z|}{|w|} < 1$. Then for all $n \in \mathbf{N}$

$$|a_n z^n| = |a_n w^n| \left|\frac{z}{w}\right|^n \leq MR^n.$$

Now $\sum\{MR^n\}$ is a convergent geometric series, so by the comparison test, $\sum\{|a_n z^n|\}$ converges; i.e., $\sum\{a_n z^n\}$ is absolutely convergent. ∥

12.9 Corollary. *Let $\sum\{a_n z^n\}$ be a power series. Suppose $\sum\{a_n w^n\}$ diverges for some $w \in \mathbf{C}$. Then $\sum\{a_n z^n\}$ diverges for all $z \in \mathbf{C}$ with $|z| > |w|$.*

Proof: Suppose $|z| > |w|$. If $\sum\{a_n z^n\}$ converges, then by the theorem, $\sum\{a_n w^n\}$ would also converge, contrary to our assumption. ∥

12.10 Theorem. *Let $\sum\{c_n z^n\}$ be a power series. Then one of the following three conditions holds:*

a) $\sum\{c_n z^n\}$ converges only when $z = 0$.

b) $\sum\{c_n z^n\}$ converges for all $z \in \mathbf{C}$.

c) There is a number $R \in \mathbf{R}^+$ such that $\sum\{c_n z^n\}$ converges absolutely for $|z| < R$ and diverges for $|z| > R$.

Proof: Suppose that neither a) nor b) is true. Then there are numbers $w, v \in \mathbf{C}\backslash\{0\}$ such that $\sum\{c_n w^n\}$ converges and $\sum\{c_n v^n\}$ diverges. If $a = \dfrac{|w|}{2}$, and $b = 2|v|$, it follows that $\sum\{c_n a^n\}$ converges and $\sum\{c_n b^n\}$ diverges. By a familiar procedure, build a binary search sequence $\{[a_k, b_k]\}$ such that $[a_0, b_0] = [a, b]$, and for all $k \in \mathbf{N}$, $\sum\{c_n a_k^n\}$ converges and $\sum\{c_k b_k^n\}$ diverges. Let R be the number such that $\{[a_k, b_k]\} \to R$. Then $a_k \leq R \leq b_k$ for all $k \in \mathbf{N}$ and

$\lim\{a_k\} = \lim\{b_k\} = R$.
If $|z| < R$, then for some $k \in \mathbf{N}$ we have $|a_k - R| < R - |z|$, and

$$\begin{aligned} |a_k - R| < R - |z| &\implies a_k > R - (R - |z|) = |z| \\ &\implies \sum\{c_n z^k\} \text{ converges.} \end{aligned}$$

If $|z| > R$, then for some $k \in \mathbf{N}$ we have $|b_k - R| < |z| - R$, and

$$\begin{aligned} |b_k - R| < |z| - R &\implies b_k < R + (|z| - R) = |z| \\ &\implies \sum\{c_n z^n\} \text{ diverges.} \quad \| \end{aligned}$$

12.11 Definition (Radius of convergence.) Let $\{\sum c_n z^n\}$ be a power series. If there is a number $R \in \mathbf{R}^+$ such that $\sum\{c_n z^n\}$ converges for $|z| < R$, and diverges for $|z| > R$, we call R the *radius of convergence* of $\sum\{c_n z^n\}$. If $\sum\{c_n z^n\}$ converges only for $z = 0$, we say $\sum\{c_n z^n\}$ has radius of convergence 0. If $\sum\{c_n z^n\}$ converges for all $z \in \mathbf{C}$, we say $\sum\{c_n z^n\}$ has radius of convergence ∞.

If a power series has radius of convergence $R \in \mathbf{R}^+$, I call $D(0, R)$ the *disc of convergence* for the series, and I call $C(0, R)$ the *circle of convergence* for the series. If $R = \infty$, I call $\mathbf{C}$ the disc of convergence of the series (even though $\mathbf{C}$ is not a disc).

12.12 Example. I will find the radius of convergence for $\sum \left\{ \dfrac{(3n)! z^n}{n!(2n)!} \right\}$. I will apply the ratio test. Since the ratio test applies to positive sequences, I will consider absolute convergence. Let $a_n = \dfrac{(3n)! z^n}{n!(2n)!}$ for all $n \in \mathbf{N}$. Then for all $z \in \mathbf{C} \setminus \{0\}$,

$$\begin{aligned} \frac{|a_{n+1}|}{|a_n|} &= \frac{(3(n+1))!|z|^{n+1}}{(n+1)!(2(n+1))!} \cdot \frac{n!(2n)!}{(3n)!|z|^n} = \frac{(3n+1)(3n+2)(3n+3)}{(n+1)(2n+1)(2n+2)}|z| \\ &= \frac{(3+\frac{1}{n})(3+\frac{2}{n})(3+\frac{3}{n})}{(1+\frac{1}{n})(2+\frac{1}{n})(2+\frac{2}{n})}|z|. \end{aligned}$$

Hence

$$\left\{ \frac{|a_{n+1}|}{|a_n|} \right\} \to \frac{3 \cdot 3 \cdot 3}{1 \cdot 2 \cdot 2}|z| = \frac{27|z|}{4}.$$

By the ratio test, $\sum\{a_n\}$ is absolutely convergent if $|z| < \frac{4}{27}$, and is divergent if $|z| > \frac{4}{27}$. It follows that the radius of convergence for our series is $\frac{4}{27}$.

12.13 Exercise. Find the radius of convergence for the following power series:

a) $\sum\{3^n\sqrt{n}z^n\}_{n\geq 1}$.

b) $\sum\left\{\dfrac{z^n}{n^n}\right\}_{n\geq 1}$.

12.14 Exercise. Let r be a positive real number.

a) Find a power series whose radius of convergence is equal to r.

b) Find a power series whose radius of convergence is ∞.

c) Find a power series whose radius of convergence is 0.

12.3 Differentiation of Power Series

If $\sum\{c_nz^n\} = \{c_0, c_0 + c_1z, c_0 + c_1z + c_2z^2, \cdots\}$ is a power series, then the series obtained by differentiating the terms of $\sum\{c_nz^n\}$ is

$$\sum\{c_nnz^{n-1}\} = \{0, c_1, c_1 + 2c_2z, c_1 + 2c_2z + 3c_3z^2, \cdots\}.$$

This is not a power series, but its translate

$$\sum\{c_{n+1}(n+1)z^n\} = \{c_1, c_1 + 2c_2z, c_1 + 2c_2z + 3c_3z^2, \cdots\}$$

is.

12.15 Definition (Formal derivative.) If $\sum\{c_nz^n\}$ is a power series, then the *formal derivative of* $\sum\{c_nz^n\}$ is

$$D(\sum\{c_nz^n\}) = \sum\{c_{n+1}(n+1)z^n\}.$$

I will sometimes write $D(\sum\{c_nz^n\}) = \sum\{c_nnz^{n-1}\}$ when I think this will cause no confusion.

12.16 Examples.

$$\begin{aligned} D(\sum\{z^n\}) &= \sum\{nz^{n-1}\} = \sum\{(n+1)z^n\} \\ &= \{1, 1 + 2z, 1 + 2z + 3z^2, \cdots\}. \end{aligned}$$

$$
\begin{aligned}
D(S) &= D\left(\sum\left\{\frac{(-1)^n z^{2n+1}}{(2n+1)!}\right\}\right)\\
&= D\left(\left\{0, z, z, z-\frac{z^3}{3!}, z-\frac{z^3}{3!}, z-\frac{z^3}{3!}+\frac{z^5}{5!}, \cdots\right\}\right)\\
&= \left\{\ 1, 1, 1-\frac{z^2}{2!}, 1-\frac{z^2}{2!}, 1-\frac{z^2}{2!}+\frac{z^4}{4!}, \cdots\right\}\\
&= \sum\left\{\frac{(-1)^n z^{2n}}{(2n)!}\right\} = C
\end{aligned}
$$

or

$$
D\left(\sum\left\{\frac{(-1)^n z^{2n+1}}{(2n+1)!}\right\}\right) = \sum\left\{\frac{(2n+1)(-1)^n z^{2n}}{(2n+1)!}\right\} = \sum\left\{\frac{(-1)^n z^{2n}}{(2n)!}\right\} = C.
$$

Our fundamental theorem on power series is:

12.17 Theorem (Differentiation theorem.) *Let $\sum\{a_n z^n\}$ be a power series. Then $D(\sum\{a_n z^n\})$ and $(\sum\{a_n z^n\})$ have the same radius of convergence. The function f associated with $\sum\{a_n z^n\}$ is differentiable in the disc of convergence, and the function represented by $D(\sum\{a_n z^n\})$ agrees with f' on the disc of convergence.*

The proof is rather technical, and I will postpone it until section 12.8. I will derive some consequences of it before proving it (to convince you that it is worth proving).

12.18 Example. We know that the geometric series $\sum\{z^n\}$ has radius of convergence 1 and $f(z) = \sum_{n=0}^{\infty} z^n = \frac{1}{1-z}$ for $|z| < 1$. The differentiation theorem says $D(\sum\{z^n\}) = \sum\{nz^{n-1}\}$ also has radius of convergence 1, and

$$
f'(z) = \sum_{n=0}^{\infty} nz^{n-1} = \sum_{n=0}^{\infty}(n+1)z^n \text{ for } |z| < 1;
$$

i.e.,

$$
\sum_{n=0}^{\infty}(n+1)z^n = \frac{1}{(1-z)^2} \text{ for } |z| < 1.
$$

We can apply the theorem again and get

$$\sum_{n=0}^{\infty}(n+1)(n)z^{n-1} = \frac{2}{(1-z)^3} \text{ for } |z| < 1,$$

or

$$\sum_{n=0}^{\infty}\frac{(n+1)(n+2)}{2}z^n = \frac{1}{(1-z)^3} \text{ for } |z| < 1.$$

Another differentiation gives us

$$\sum_{n=0}^{\infty}\frac{n(n+1)(n+2)z^{n-1}}{2} = \frac{3}{(1-z)^4} \text{ for } |z| < 1,$$

or

$$\sum_{n=0}^{\infty}\frac{(n+1)(n+2)(n+3)}{3!}z^n = \frac{1}{(1-z)^4} \text{ for } |z| < 1.$$

The pattern is clear, and I omit the induction proof that for all $k \in \mathbf{N}$

$$\begin{aligned}\frac{1}{(1-z)^{k+1}} &= \sum_{n=0}^{\infty}\frac{(n+1)(n+2)(n+3)\cdots(n+k)}{k!}z^n \\ &= \sum_{n=0}^{\infty}\frac{(n+k)!}{n!k!}z^n \text{ for } |z| < 1.\end{aligned}$$

12.19 Exercise. By assuming the differentiation theorem, we've shown that the series $\sum\left\{\left(\frac{(n+k)!}{n!k!}\right)z^n\right\}$ has radius of convergence 1 for all $k \in \mathbf{N}$. Verify this directly.

12.20 Exercise. Find formulas for $\sum_{n=0}^{\infty} nz^n$ and $\sum_{n=0}^{\infty} n^2z^n$ that are valid for $|z| < 1$. (You may assume the differentiation theorem.)

12.21 Example. By the differentiation theorem, if

$$C(z) = \sum_{n=0}^{\infty}\frac{(-1)^n z^{2n}}{(2n)!} \text{ and } S(z) = \sum_{j=0}^{\infty}\frac{(-1)^n z^{2n+1}}{(2n+1)!},$$

then C and S are differentiable on $\mathbf{C}$ and $C'(z) = -S(z)$, and $S'(z) = C(z)$. (We saw in earlier examples that both series have radius of convergence ∞, and that the formal derivatives satisfy $DS = C$ and $DC = -S$.) Also, clearly $C(z)$ and $S(z)$ are real when z is real. The discussion in example 10.45 then shows that for real z, C and S agree with the cosine and sine functions you discussed in your previous calculus course, and in particular that

$$\sin^2 z + \cos^2 z = 1 \text{ for all } z \in \mathbf{R}.$$

12.4 The Exponential Function

12.22 Example. Suppose we had a complex function E such that E is everywhere differentable and

$$E' = E, \text{ and } E(0) = 1. \tag{12.23}$$

Let $H(z) = E(z)E(-z)$ for all $z \in \mathbf{C}$. By the chain and product rules,

$$H'(z) = E'(z)E(-z) + E(z)[-E'(-z)] = E(z)E(-z) - E(z)E(-z) = 0$$

on $\mathbf{C}$, so H' is constant. Since $H(0) = E(0)E(0) = 1$, we conclude

$$E(z)E(-z) = 1 \text{ for all } z \in \mathbf{C}. \tag{12.24}$$

In particular $E(z)$ is never 0, and

$$E(-z) = (E(z))^{-1} \text{ for all } z \in \mathbf{C}.$$

Now let $a \in \mathbf{C}$ and define a function $H_a\colon \mathbf{C} \to \mathbf{C}$ by

$$H_a(z) = E(z + a)E(-z).$$

We have

$$\begin{aligned} H_a'(z) &= E'(z+a)E(-z) + E(z+a)[-E'(-z)] \\ &= E(z+a)E(-z) - E(z+a)E(-z) = 0 \end{aligned}$$

for all $z \in \mathbf{C}$, so H_a is constant, and $H_a(0) = E(a)E(0) = E(a)$. Thus

$$E(z+a)E(-z) = E(a) \text{ for all } z \in \mathbf{C},\ a \in \mathbf{C},$$

and by (12.24),

$$E(z+a) = E(a)E(z) \text{ for all } z \in \mathbf{C},\ a \in \mathbf{C}. \tag{12.25}$$

Next suppose you know some function $e\colon \mathbf{R} \to \mathbf{R}$ such that $e'(t) = e(t)$ for all $t \in \mathbf{R}$ and $e(0) = 1$. (You do know such a function from your previous calculus course.) Let

$$K(t) = E(-t)e(t) \text{ for all } t \in \mathbf{R}.$$

Then by the product and chain rules,

$$K'(t) = [-E(-t)]e(t) + E(-t)e(t) = 0 \text{ for all } t \in \mathbf{R},$$

so K is constant on $\mathbf{R}$, and since $K(0) = E(0)e(0) = 1$, we have $E(-t)e(t) = 1$. By (12.24),

$$e(t) = E(t) \text{ for all } t \in \mathbf{R}.$$

Now I will try to construct a function E satisfying the differential equation (12.23) by hoping that E is given by a power series. Suppose

$$\begin{aligned} E(z) &= a_0 + a_1 z + a_2 z^2 + a_3 z^3 + a_4 z^4 \cdots \text{ for all } z \in \mathbf{C}. \\ E(0) &= a_0 + 0 + 0 + \cdots. \end{aligned}$$

Since $E(0) = 1$, we must have $a_0 = 1$, and

$$E(z) = 1 + a_1 z + a_2 z^2 + a_3 z^3 + a_4 z^4 + \cdots.$$

By the differentiation theorem,

$$E'(z) = a_1 + 2a_2 z + 3a_3 z^2 + 4a_4 z^3 + \cdots,$$

and

$$a_1 = E'(0) = E(0) = 1.$$

By the differentiation theorem again,

$$E'(z) = 2 \cdot 1 a_2 + 3 \cdot 2 a_3 z + 4 \cdot 3 a_4 z^2 + \cdots,$$

so

$$2 \cdot 1 a_2 = E'(0) = E(0) = 1 \text{ and } a_2 = \frac{1}{2 \cdot 1}.$$

Hence

$$E(z) = E'(z) = 1 + 3 \cdot 2 a_3 z + 4 \cdot 3 a_4 z^2 + \cdots.$$

Repeating the process, we get

$$E'(z) = 3 \cdot 2 \cdot 1 a_3 + 4 \cdot 3 \cdot 2 a_4 z + \cdots,$$

so

$$3 \cdot 2 \cdot 1 a_3 = E'(0) = E(0) = 1 \text{ and } a_3 = \frac{1}{3 \cdot 2 \cdot 1}.$$

I see a pattern here: $a_n = \dfrac{1}{n!}$.

12.26 Definition (Exponential function.) Let E denote the power series $\sum\left\{\frac{z^n}{n!}\right\} = \left\{1 + z + \frac{z^2}{2!} + \cdots + \frac{z^n}{n!}\right\}$. We will show in exercise 12.31 that E has infinite radius of convergence. We write

$$E(z) = \exp(z) = \sum_{n=0}^{\infty} \frac{z^n}{n!} \text{ for all } z \in \mathbf{C}.$$

12.27 Theorem. $\exp' = \exp$ *and* $\exp(0) = 1$.

Proof: It is clear that $\exp(0) = 1$. The formal derivative of E is

$$DE = \sum\left\{\frac{nz^{n-1}}{n!}\right\} = \sum\left\{\frac{(n+1)z^n}{(n+1)!}\right\} = \sum\left\{\frac{z^n}{n!}\right\} = E,$$

so the [still unproved] differentiation theorem says that $\exp' = \exp$. It follows from our discussion above that $\exp(z)$ is never 0,

$$\exp(-z) = (\exp(z))^{-1} \text{ for all } z \in \mathbf{C}, \tag{12.28}$$

and

$$\exp(a + z) = \exp(a)\exp(z) \text{ for all } z \in \mathbf{C}. \tag{12.29}$$

It is clear that $\exp(z)$ is real for all $z \in \mathbf{R}$. In fact, we must have $\exp(z) \in \mathbf{R}^+$ for all $z \in \mathbf{R}$, since exp is continuous (differentiable functions are continuous) and if $\exp(t) < 0$ for some z, the intermediate value theorem would say $\exp(y) = 0$ for some y between 0 and t. Since $\exp'(t) = \exp(t) > 0$ on $\mathbf{R}$, exp is strictly increasing on $\mathbf{R}$. ‖

12.30 Definition (e.) We define e to be the number $\exp(1)$; i.e., $e = \sum_{n=0}^{\infty} \frac{1}{n!}$.

12.31 Exercise. Show that $\sum\left\{\frac{z^n}{n!}\right\}$ has infinite radius of convergence.

12.32 Exercise. Use the definition of e to show that $e > 2.718$.

12.33 Exercise.

a) Show that $\exp(nz) = (\exp(z))^n$ for all $n \in \mathbf{N}$, $z \in \mathbf{C}$.

b) Show that $\exp(nz) = (\exp(z))^n$ for all $n \in \mathbf{Z}$, $z \in \mathbf{C}$.

12.34 Exercise. From the previous exercise, it follows that

$$\exp(nz) = (\exp(z))^n \text{ for all } z \in \mathbf{C},\ n \in \mathbf{Z}.$$

Use this to prove that

$$\exp\left(\frac{p}{q}t\right) = (\exp(t))^{\frac{p}{q}} \text{ for all } t \in \mathbf{R},\ p \in \mathbf{Z},\ q \in \mathbf{Z}^+;$$

i.e.,

$$\exp(rt) = (\exp(t))^r \text{ for all } t \in \mathbf{R},\ r \in \mathbf{Q}.$$

(Note that for $t = 1$, this says

$$\exp(r) = (\exp(1))^r = e^r.$$

12.35 Notation (e^z.) Another notation for $\exp(z)$ is e^z. This notation is motivated by the previous exercise. With this notation, we have

$$\begin{aligned} e^{z+a} &= e^z e^a \text{ for all } z, a \in \mathbf{C}. \\ (e^z)^{-1} &= e^{-z} \text{ for all } z \in \mathbf{C}. \\ (e^t)^r &= e^{(tr)} \text{ for all } t \in \mathbf{R},\ r \in \mathbf{Q}. \end{aligned}$$

12.36 Theorem. *Every number $t \in \mathbf{R}^+$ can be written as $t = \exp(s)$ for a unique $s \in \mathbf{R}$.*

Proof: The uniqueness of s follows from the fact that exp is strictly increasing on $\mathbf{R}$. Let $t \in (1, \infty)$. From the expansion $\exp(t) = 1 + t + \frac{t^2}{2!} + \cdots$, we see that $\exp(t) > t$. Since exp is continuous, we can apply the intermediate value theorem to exp on $[0, t]$ to conclude $t = \exp(s)$ for some $s \in (0, t)$. If $t \in (0, 1)$, then $\frac{1}{t} \in (1, \infty)$, so $\frac{1}{t} = e^s$ for some $s \in (0, \infty)$, and $t = e^{-s}$ where $-s \in (-\infty, 0)$. Since $1 = e^0$, the theorem has been proved in all cases. ‖

12.5 Logarithms

12.37 Definition (Logarithm.) Let $t \in \mathbf{R}^+$. The *logarithm of* t is the unique number $s \in \mathbf{R}$ such that $e^s = t$. We denote the logarithm of t by $\ln(t)$, Hence

$$e^{\ln(t)} = t \text{ for all } t \in \mathbf{R}^+. \tag{12.38}$$

12.39 Remark. Since $\ln(e^r)$ is the unique number s such that $e^s = e^r$, it follows that

$$\ln(e^r) = r \text{ for all } r \in \mathbf{R}. \tag{12.40}$$

12.41 Theorem. *For all* $a, b \in \mathbf{R}^+$,

$$\ln(ab) = \ln a + \ln b.$$

Proof:

$$\begin{aligned} \ln(ab) &= \ln(e^{\ln a} \cdot e^{\ln b}) \quad \text{(by (12.38))} \\ &= \ln(e^{(\ln a + \ln b)}) \\ &= \ln a + \ln b \quad \text{(by (12.40))}. \ \| \end{aligned}$$

12.42 Exercise. Show that

a) $\ln(a^{-1}) = -\ln(a)$ for all $a \in \mathbf{R}^+$.

b) $\ln(a^r) = r\ln(a)$ for all $a \in \mathbf{R}^+$, $r \in \mathbf{Q}$.

c) $\ln\left(\frac{a}{b}\right) = \ln a - \ln b$ for all $a, b \in \mathbf{R}^+$.

12.43 Remark. It follows from the fact that exp is strictly increasing on $\mathbf{R}$ that ln is strictly increasing on $\mathbf{R}^+$: if $0 < t < s$, then both of the statements $\ln(t) = \ln(s)$ and $\ln(t) > \ln(s)$ lead to contradictions.

12.44 Theorem (Continuity of ln.) ln *is a continuous function on* $\mathbf{R}^+$.

Proof: Let $a \in \mathbf{R}^+$, and let f be a sequence in $\mathbf{R}^+$ such that $f \to a$. I want to show that $\ln \circ f \to \ln(a)$. Let $N_{f-\tilde{a}}$ be a precision function for $f - \tilde{a}$. I want to construct a precision function M for $\ln \circ f - \widetilde{\ln(a)}$.

Scratchwork: For all $\varepsilon \in \mathbf{R}^+$, and all $n \in \mathbf{N}$,

$$\begin{aligned} |\ln(f(n)) - \ln(a)| < \varepsilon &\iff \ln(a) - \varepsilon < \ln(f(n)) < \ln(a) + \varepsilon \\ &\iff e^{\ln(a)-\varepsilon} < f(n) < e^{\ln(a)+\varepsilon} \\ &\iff e^{\ln(a)-\varepsilon} - a < f(n) - a < e^{\ln(a)+\varepsilon} - a \end{aligned}$$

Note that since ln is strictly increasing, $e^{\ln(a)+\varepsilon} - a$ and $a - e^{\ln(a)-\varepsilon}$ are both positive. This calculation motivates the following definition:

For all $\varepsilon \in \mathbf{R}^+$, let

$$M(\varepsilon) = \max(N_{f-\tilde{a}}(e^{\ln(a)+\varepsilon} - a), N_{f-\tilde{a}}(a - e^{\ln(a)-\varepsilon})).$$

Then for all $n \in \mathbf{N}$, $\varepsilon \in \mathbf{R}^+$,

$$\begin{aligned} n \geq M(\varepsilon) &\implies \begin{cases} f(n) - a \leq |f(n) - a| \leq e^{\ln(a)+\varepsilon} - a \\ a - f(n) \leq |f(n) - a| \leq a - e^{\ln(a)-\varepsilon} \end{cases} \\ &\implies e^{\ln(a)-\varepsilon} < f(n) < e^{\ln(a)+\varepsilon} \\ &\implies \ln(a) - \varepsilon < \ln(f(n)) < \ln(a) + \varepsilon \\ &\implies |\ln(f(n)) - \ln(a)| < \varepsilon \end{aligned}$$

Hence M is a precision function for $\ln \circ f - \widetilde{\ln(a)}$. ‖

12.45 Theorem (Differentiability of ln.) *The function* ln *is differentiable on* $\mathbf{R}^+$ *and*

$$\ln'(x) = \frac{1}{x} \text{ for all } x \in \mathbf{R}^+.$$

Proof: Let $a \in \mathbf{R}^+$ and let $\{x_n\}$ be a sequence in $\mathbf{R}^+ \backslash \{a\}$. Then

$$\frac{\ln(x_n) - \ln(a)}{x_n - a} = \frac{\ln(x_n) - \ln(a)}{e^{\ln(x_n)} - e^{\ln(a)}} = \frac{1}{\left(\frac{e^{\ln(x_n)} - e^{\ln(a)}}{\ln(x_n) - \ln(a)}\right)}.$$

(Note, I have not divided by 0.) Since ln is continuous, I know $\{\ln(x_n)\} \to \ln(a)$, and hence

$$\left\{\frac{e^{\ln(x_n)} - e^{\ln(a)}}{\ln(x_n) - \ln(a)}\right\} \to \exp'(\ln(a)) = e^{\ln(a)} = a.$$

Hence,

$$\lim \left\{\frac{\ln(x_n) - \ln(a)}{x_n - a}\right\} = \frac{1}{a};$$

i.e.,

$$\lim_{x \to a} \frac{\ln(x) - \ln(a)}{x - a} = \frac{1}{a}.$$

This shows that $\ln'(a) = \dfrac{1}{a}$.

12.6 Trigonometric Functions

Next we calculate $\exp(it)$ for $t \in \mathbf{R}$.

$$\exp(it) = \sum_{j=0}^{\infty} \frac{(it)^j}{j!}, \quad t \in \mathbf{R}.$$

Now $\{i^n\} = \{1, i, -1, -i, 1, i, -1, -i, \cdots\}$ and it is clear that $(i)^{2n} = (-1)^n \in \mathbf{R}$, $(i)^{2n+1} = i(-1)^n$ is pure imaginary. Hence,

$$\begin{aligned} \mathrm{Re}\,(\exp(it)) &= \sum_{j=0}^{\infty} \frac{(-1)^j t^{2j}}{(2j)!} = \cos t \\ \mathrm{Im}\,(\exp(it)) &= \sum_{j=0}^{\infty} \frac{(-1)^j t^{2j+1}}{(2j+1)!} = \sin t; \end{aligned}$$

i.e.,

$$\exp(it) = \cos t + i \sin t \text{ for all } t \in \mathbf{R}. \tag{12.46}$$

For any complex number $(x, y) = x + iy$, we have

$$\begin{aligned} \exp(x + iy) &= \exp(x)\exp(iy) = \exp(x)[\cos(y) + i\sin(y)] \\ &= \exp(x)\cos(y) + i\exp(x)\sin(y). \end{aligned}$$

Since your calculator has buttons that calculate approximations to exp, sin and cos, you can approximately calculate the exponential of any complex number with a few key strokes.

The relation (12.46)

$$\exp(it) = \cos t + i \sin t$$

actually holds for all $t \in \mathbf{C}$, since

$$\begin{aligned} \sum_{j=0}^{n} \frac{(-1)^j z^{2j}}{(2j)!} + i \sum_{j=0}^{n} \frac{(-1)^j z^{2j+1}}{(2j+1)!} &= \sum_{j=0}^{n} \frac{(iz)^{2j}}{(2j)!} + \sum_{j=0}^{n} \frac{(i)^{2j+1} z^{2j+1}}{(2j+1)!} \\ &= \sum_{j=0}^{2n+1} \frac{(iz)^j}{j!}. \end{aligned}$$

Hence
$$e^{iz} = \cos z + i \sin z \text{ for all } z \in \mathbf{C}, \tag{12.47}$$
so
$$e^{-iz} = \cos z - i \sin z \text{ for all } z \in \mathbf{C}. \tag{12.48}$$
We can solve (12.47) and (12.48) for $\sin(z)$ and $\cos(z)$ to obtain
$$\cos(z) = \frac{e^{iz} + e^{-iz}}{2} \text{ for all } z \in \mathbf{C}. \tag{12.49}$$
$$\sin(z) = \frac{e^{iz} - e^{-iz}}{2i} \text{ for all } z \in \mathbf{C}. \tag{12.50}$$
From (12.47) it follows that
$$|e^{it}| = 1 \text{ for all } t \in \mathbf{R},$$
i.e., e^{it} is in the unit circle for all $t \in \mathbf{R}$.

12.51 Exercise (Addition laws for sin **and** cos.**)** Prove that
$$\begin{aligned} \cos(z+a) &= \cos(z)\cos(a) - \sin(z)\sin(a) \\ \sin(z+a) &= \sin(z)\cos(a) + \cos(z)\sin(a) \end{aligned}$$
for all $z, a \in \mathbf{C}$.

By the addition laws, we have (for all $x, y \in \mathbf{C}$),
$$\cos(x+iy) = \cos(x)\cos(iy) - \sin(x)\sin(iy) \tag{12.52}$$
$$\sin(x+iy) = \sin x \cos(iy) + \cos x \sin(iy). \tag{12.53}$$
By (12.49) and (12.50)
$$\cos(iy) = \frac{e^{i(iy)} + e^{-i(iy)}}{2} = \frac{e^{y} + e^{-y}}{2}$$
and
$$\sin(iy) = \frac{e^{i(iy)} - e^{-i(iy)}}{2i} = \frac{e^{-y} - e^{y}}{2i} = i\left(\frac{e^{y} - e^{-y}}{2}\right).$$

12.54 Definition (Hyperbolic functions.) For all $z \in \mathbf{C}$, we define the *hyperbolic sine* and *hyperbolic cosine* of z by

$$\begin{aligned}\sinh(z) &= \frac{e^z - e^{-z}}{2}\\ \cosh(z) &= \frac{e^z + e^{-z}}{2}.\end{aligned}$$

Note that if z is real, $\sinh(z)$ and $\cosh(z)$ are real. Most calculators have buttons that calculate cosh and sinh. We can now rewrite (12.52) and (12.53) as

$$\begin{aligned}\cos(x+iy) &= \cos(x)\cosh(y) - i\sin(x)\sinh(y)\\ \sin(x+iy) &= \sin(x)\cosh(y) + i\cos(x)\sinh(y).\end{aligned}$$

These formulas hold true for all complex x and y.

Since

$$\sin' = \cos, \qquad \cos' = -\sin, \quad \sin(0) = 0 \qquad \text{and } \cos(0) = 1,$$

it follows from our discussion in example 10.45 that

$$\sin(x) \geq x - \frac{x^3}{6} \text{ and } \cos x \leq 1 - \frac{x^2}{2} + \frac{x^4}{24}$$

for all $x > 0$. In particular

$$\sin(x) \geq x\left(1 - \frac{x^2}{6}\right) > 0 \text{ for } 0 < x < \sqrt{6}$$

and

$$\cos(2) < 1 - \frac{4}{2} + \frac{16}{24} < 0.$$

Hence $\cos' = -\sin < 0$ on $(0,2)$, so cos is strictly decreasing on $[0,2]$. Moreover cos is continuous (since it is differentiable) so by the intermediate value theorem there is a number c in $(0,2)$ such that $\cos(c) = 0$. Since cos is strictly decreasing on $(0,2)$ this number c is unique. (Cf. exercise 5.48.)

12.55 Definition (π.) We define the real number π by the condition $\frac{\pi}{2}$ is the unique number in $(0,2)$ satisfying $\cos\left(\frac{\pi}{2}\right) = 0$.

12.56 Theorem. exp *is periodic of period* $2\pi i$*; i.e.,*

$$\exp(z + 2\pi i) = \exp(z) \text{ for all } z \in \mathbf{C}.$$

Proof: Since $\sin^2 t + \cos^2 t = 1$ for all $t \in \mathbf{C}$, we have $\sin^2\left(\frac{\pi}{2}\right) = 1$, so $\sin\left(\frac{\pi}{2}\right) = \pm 1$. We have noted that $\sin t > 0$ on $(0, 2)$ so $\sin\left(\frac{\pi}{2}\right) = 1$. Hence

$$e^{\frac{i\pi}{2}} = \cos\left(\frac{\pi}{2}\right) + i \sin\left(\frac{\pi}{2}\right) = i,$$

and

$$e^{2i\pi} = \left(e^{\frac{i\pi}{2}}\right)^4 = i^4 = 1. \tag{12.57}$$

It follows that $e^{2\pi i + z} = e^{2\pi i} e^z = 1e^z = e^z$ for all $z \in \mathbf{C}$. ∥

12.58 Entertainment. If Maple or Mathematica are asked for the numerical values of $(-1)^{3.14}$ and i^i, they agree that

$$(-1)^{3.14} = -.9048 \cdots - i \cdot .4257 \cdots$$

and

$$i^i = .2078 \cdots.$$

Can you propose a reasonable definition for $(-1)^z$ and i^z when z is an arbitrary complex number, that is consistent with these results? To be reasonable you would require that when $z \in \mathbf{Z}$, $(-1)^z$ and i^z give the expected values, and

$$\begin{aligned} (-1)^{z+w} &= (-1)^z (-1)^w \text{ for all } z, w \in \mathbf{C}, \\ (i)^{z+w} &= i^z i^w \text{ for all } z, w \in \mathbf{C}. \end{aligned}$$

12.59 Exercise. Prove that:

a) $\cos \pi = -1$, and $\sin \pi = 0$.

b) $\cos \frac{3\pi}{2} = 0$, and $\sin \frac{3\pi}{2} = -1$.

c) $\cos 2\pi = 1$, and $\sin 2\pi = 0$.

d) $\sin(2\pi - t) = -\sin t$ for all $t \in \mathbf{C}$.

e) $\cos(2\pi - t) = \cos t$ for all $t \in \mathbf{C}$.

f) $\sin(\pi - t) = \sin t$ for all $t \in \mathbf{C}$.

g) $\cos(\pi - t) = -\cos t$ for all $t \in \mathbf{C}$.

h) $\sin(2\pi + t) = \sin t$ for all $t \in \mathbf{C}$.

i) $\cos(2\pi + t) = \cos t$ for all $t \in \mathbf{C}$.

12.60 Theorem. $\cos(2\pi) = 1$ *and* $\cos t < 1$ *for* $0 < t < 2\pi$.

Proof: From the previous exercise, $\cos(2\pi) = \cos(0) = 1$. We've noted that $\sin t > 0$ for $t \in \left(0, \frac{\pi}{2}\right]$,

$$\begin{aligned} t \in \left(\tfrac{\pi}{2}, \pi\right) &\implies \frac{\pi}{2} < t < \pi \implies 0 < \pi - t < \frac{\pi}{2} \\ &\implies \sin(\pi - t) > 0 \\ &\implies \sin(t) > 0. \end{aligned}$$

Hence $\sin(t) > 0$ for $t \in (0, \pi)$. Hence $\cos'(t) = -\sin(t) < 0$ for $t \in (0, \pi)$. Hence cos is strictly decreasing on $(0, \pi)$. Hence $\cos(x) < \cos(0) = 1$ for all $x \in (0, \pi)$.

Now

$$\begin{aligned} t \in (\pi, 2\pi) &\implies \pi < t < 2\pi \implies 0 < 2\pi - t < \pi \\ &\implies \cos(2\pi - t) < 1 \\ &\implies \cos t < 1, \end{aligned}$$

and since $\cos(\pi) = -1 < 1$, we've shown that $\cos t < 1$ for all $t \in (0, 2\pi)$. ‖

12.61 Theorem. *Every point* (x, y) *in the unit circle can be written as* $(x, y) = e^{it}$ *for a unique* $t \in [0, 2\pi)$.

Proof: We first show uniqueness.

Suppose $(x, y) = x + iy = e^{it} = e^{is}$ where $s, t \in [0, 2\pi)$. Without loss of generality, say $s \le t$. Then

$$1 = \frac{e^{it}}{e^{is}} = e^{i(t-s)} = \cos(t - s) + i \sin(t - s),$$

and $t - s \in [0, 2\pi)$. By the previous theorem, 0 is the only number in $[0, 2\pi)$ whose cosine is 1, so $t - s = 0$, and hence $t = s$.

Let (x, y) be a point in the unit circle, so $x^2+y^2 = 1$, and hence $-1 \leq x \leq 1$. Since $\cos(0) = 1$ and $\cos(\pi) = -1$, it follows from the intermediate value theorem that $x = \cos t$ for some $t \in [0, \pi]$. Then

$$y^2 = 1 - x^2 = 1 - \cos^2(t) = \sin^2(t),$$

so $y = \pm\sin(t)$.

$$\begin{aligned} y = \sin t &\implies (x, y) = (\cos t, \sin t) = e^{it} \\ y = -\sin t &\implies (x, y) = (\cos t, -\sin t) = (\cos(2\pi - t), \sin(2\pi - t)) = e^{i(2\pi - t)} \end{aligned}$$

and since $t \in [0, \pi]$, we have $2\pi - t \in [\pi, 2\pi]$. $\|$

12.62 Lemma. *The set of all complex solutions to* $e^z = 1$ *is* $\{2\pi in : n \in \mathbf{Z}\}$.

Proof: By exercise 12.59

$$e^{2\pi i} = \cos 2\pi + i \sin 2\pi = 1 + i0 = 1,$$

so

$$e^{2\pi in} = \left(e^{2\pi i}\right)^n = 1^n = 1.$$

Let $w = (a, b) = a + ib$ be any solution to $e^z = 1$; i.e.,

$$1 = e^{a+bi} = e^a e^{ib}.$$

By uniqueness of polar decomposition,

$$e^a = 1 \text{ and } e^{ib} = 1,$$

so $a = 0$ (since for real a, $e^a = 1 \iff a = 0$). We can write $\dfrac{b}{2\pi} = n + \varepsilon$ where $n \in \mathbf{Z}$ and $\varepsilon \in [0, 1)$ by theorem 5.30, so $b = 2\pi n + 2\pi\varepsilon$ where $2\pi\varepsilon \in [0, 2\pi)$. Now

$$1 = e^{ib} = e^{2\pi in + i2\pi\varepsilon} = e^{2\pi i\varepsilon}.$$

By theorem 12.61, $2\pi i\varepsilon = 0$, so $\varepsilon = 0$, and $b = 2\pi n$; i.e., $w = 2\pi in$. $\|$

12.63 Definition (Argument.) Let $a \in \mathbf{C}\backslash\{0\}$ and write a in its polar decomposition $a = |a|u$, where $|u| = 1$. We know $u = e^{iA}$ for a unique $A \in [0, 2\pi)$. I will call A the *argument* of a and write $A = \text{Arg}(a)$. Hence

$$a = |a|e^{i\text{Arg}(a)} \quad A \in [0, 2\pi).$$

12.64 Remark. Our definition of Arg is rather arbitrary. Other natural definitions are

$$\text{Arg}_1(z) \text{ is the unique number } a \text{ in } [-\pi,\pi) \text{ such that } z = |z|e^{ia},$$

or

$$\text{Arg}_2(z) \text{ is the unique number } b \text{ in } (-\pi,\pi] \text{ such that } z = |z|e^{ib}.$$

None of these argument functions is continuous; e.g.,

$$\left\{e^{\frac{-i\pi}{n}}\right\}_{n\geq 1} \to 1.$$

But

$$\left\{\text{Arg}\left(e^{\frac{-i\pi}{n}}\right)\right\}_{n\geq 1} = \left\{\left(2\pi - \frac{\pi}{n}\right)\right\}_{n\geq 1} \to 2\pi \neq \text{Arg}(1).$$

12.65 Theorem. *Let $a \in \mathbf{C}\backslash\{0\}$. Then the complex solutions to the equation $e^z = a$ are exactly the numbers of the form*

$$z = \ln|a| + i\text{Arg}(a) + 2\pi i n \textit{ where } n \in \mathbf{Z}.$$

In particular, every non-zero $a \in \mathbf{C}$ is the exponential of some $z \in \mathbf{C}$.

Proof: Since

$$\begin{aligned} e^{(\ln|a|+i\text{Arg}(a)+2\pi i n)} &= e^{\ln|a|}e^{i\text{Arg}(a)}e^{2\pi i n} \\ &= |a|e^{i\text{Arg}(a)} = a, \end{aligned}$$

the numbers given are solutions to $e^z = a$. Let w be any solution to $e^w = a$. Then $e^{w-\ln|a|-i\text{Arg}(a)} = \frac{a}{a} = 1$. Hence, by the lemma 12.62,

$$w - \ln|a| + i\text{Arg}(w) = 2\pi i n \text{ for some } n \in \mathbf{Z}. \ \|$$

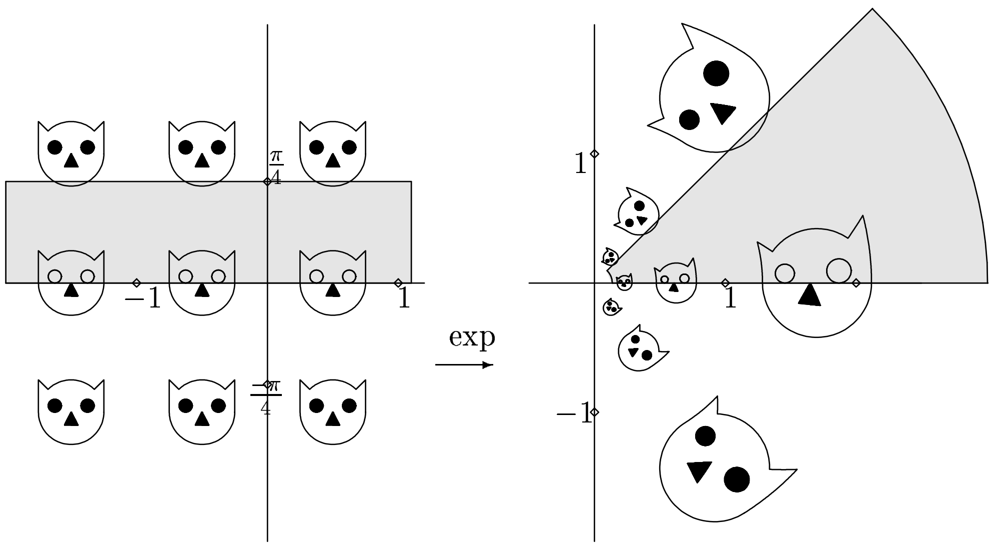
We will now look at exp geometrically as a function from $\mathbf{C}$ to $\mathbf{C}$.
Claim: exp maps the vertical line $x = x_0$ into the circle $C(0, e^{x_0})$.
Proof: If $z = x_0 + iy$, then

$$|e^z| = |e^{x_0+iy}| = |e^{x_0}e^{iy}| = |e^{x_0}||e^{iy}| = e^{x_0}.$$

Claim: exp maps the horizontal line $y = y_0$ into the ray through 0 with direction e^{iy_0}.
Proof: If $z = x + iy_0$, then

$$e^z = e^{x+iy_0} = e^x \cdot e^{iy_0} \text{ and } e^x > 0.$$

Since exp is periodic of period $2\pi i$, exp maps an infinite horizontal strip of width w into an infinite circular segment making "angle w" at the origin.



The Exponentials of Some Cats

exp maps every strip $\{(x,y): y_0 \le y < y_0 + 2\pi\}$ onto all of $\mathbf{C}\backslash\{0\}$.

12.66 Theorem (Roots of complex numbers.) *Let $a \in \mathbf{C}\backslash\{0\}$ and let $n \in \mathbf{Z}^+$. Then the solutions to $z^n = a$ in $\mathbf{C}$ are exactly the numbers*

$$z = |a|^{\frac{1}{n}} e^{i\left(\frac{\text{Arg}(a)+2\pi k}{n}\right)} \text{ where } k \in \mathbf{Z} \text{ and } 0 \le k < n.$$

(These numbers are distinct.)

Proof: These numbers are clearly solutions to $z^n = a$. Let $w = |w|e^{i\text{Arg}(w)}$ be any solution to $z^n = a$. Then

$$|w|^n e^{in\text{Arg}(w)} = w^n = a = |a|e^{i\text{Arg}(a)}.$$

By uniqueness of polar decomposition,

$$|w|^n = |a| \text{ and } e^{in\text{Arg}(w)} = e^{i\text{Arg}(a)},$$

i.e., $|w| = |a|^{1/n}$ and $e^{i[n\text{Arg}(w) - \text{Arg}(a)]} = 1$. Hence, $n\text{Arg}(w) - \text{Arg}(a) = 2\pi k$ for some $k \in \mathbf{N}$ and

$$\text{Arg}(w) = \frac{\text{Arg}(a) + 2\pi k}{n} \text{ for some } k \in \mathbf{N}.$$

Thus

$$e^{i\mathrm{Arg} w} = e^{i\left(\frac{\mathrm{Arg}(a)+2\pi k}{n}\right)} \text{ for some } k \in \mathbf{N}.$$

For each $k \in \mathbf{Z}$, the number

$$w_k = |w|^{\frac{1}{n}} e^{\frac{i\mathrm{Arg}(a)}{n}} \cdot e^{\frac{2\pi i k}{n}}$$

is a solution to $w^n = a$. For $0 \leq k < n$, the numbers $\dfrac{2\pi i k}{n}$ are distinct numbers in $[0, 2\pi)$, so the numbers $e^{\frac{2\pi i k}{n}}$ are distinct. For every $K \in \mathbf{Z}$, $\dfrac{K}{n} = M + \varepsilon$ where $M \in \mathbf{Z}$ and $\varepsilon \in [0,1)$, so $K = nM + \varepsilon n$ where $\varepsilon n \in [0, n)$ and $\varepsilon n = K - nM \in \mathbf{Z}$; i.e.,

$$K = nM + k \text{ where } k \in \mathbf{Z} \text{ and } 0 \leq k < n.$$

Then $\frac{K}{n} = M + \frac{k}{n}$, so

$$e^{2\pi i \frac{K}{n}} = e^{2\pi i M} e^{\frac{2\pi i k}{n}} = e^{\frac{2\pi i k}{n}} \text{ where } k \in \mathbf{Z} \text{ and } 0 \leq k < n. \ \|$$

12.7 Special Values of Trigonometric Functions

We have

$$\cos\left(\frac{\pi}{4}\right) = \cos\left(\frac{\pi}{2} - \frac{\pi}{4}\right) = \cos\frac{\pi}{2}\cos\frac{\pi}{4} + \sin\frac{\pi}{2}\sin\frac{\pi}{4} = \sin\frac{\pi}{4}.$$

Hence $1 = \cos^2\left(\frac{\pi}{4}\right) + \sin^2\left(\frac{\pi}{4}\right) = 2\sin^2\left(\frac{\pi}{4}\right)$, and hence $\left(\cos\frac{\pi}{4}\right) = \sin\left(\frac{\pi}{4}\right) = \pm\sqrt{\frac{1}{2}} = \pm\frac{\sqrt{2}}{2}$. Since we know sin is positive on $(0, \pi)$, we conclude that

$$\cos\left(\frac{\pi}{4}\right) = \sin\left(\frac{\pi}{4}\right) = \frac{\sqrt{2}}{2}.$$

Observe that if $t \in \mathbf{R}$, then the problem of calculating $\cos(t)$ and $\sin(t)$ is the same as the problem of calculating e^{it}. Let $n \in \mathbf{Z}^+$. We know that the complex solutions of $z^n - 1 = 0$ are

$$\left\{e^{\frac{2\pi i k}{n}} : 0 \leq k < n,\ k \in \mathbf{Z}\right\},$$

so if we can express the solutions to $z^n - 1 = 0$ in algebraic terms, then we can express $\sin\left(\frac{2\pi k}{n}\right)$ and $\cos\left(\frac{2\pi k}{n}\right)$ in algebraic terms. We have

$$z^6-1=0 \iff (z^3-1)(z^3+1)=0 \iff (z-1)(z^2+z+1)(z+1)(z^2-z+1)=0.$$

Here $z = 1$ and $z = -1$ are obvious sixth roots of 1, and the other four roots are the solutions of the quadratic equations

$$z^2 + z + 1 = 0 \text{ and } z^2 - z + 1 = 0.$$

12.67 Exercise. Find the solutions to $z^2 + z + 1 = 0$ and $z^2 - z + 1 = 0$ in terms of square roots of rational numbers. These solutions are

$$\left\{e^{\frac{\pi i}{3}}, e^{\frac{2\pi i}{3}}, e^{\frac{4\pi i}{3}}, e^{\frac{5\pi i}{3}}\right\}.$$

Identify each solution with one of these exponentials. Find $\cos\left(\frac{\pi}{3}\right)$ and $\sin\left(\frac{\pi}{3}\right)$.

12.68 Exercise. Use the fact that

$$e^{\frac{\pi i}{6}} = e^{\frac{\pi i}{2}} \cdot e^{-\frac{\pi i}{3}}$$

to find $\cos\frac{\pi}{6}$ and $\sin\frac{\pi}{6}$. ‖

The numbers $\cos\left(\frac{2\pi}{5}\right)$ and $\sin\left(\frac{2\pi}{5}\right)$ can also be expressed algebraically. If $z = e^{\frac{2\pi i}{5}}$, then $z^5 - 1 = 0$, so

$$(z-1)(z^4 + z^3 + z^2 + z + 1) = 0$$

and since $z \neq 1$,

$$(z^4 + z^3 + z^2 + z + 1) = 0.$$

The fact that $z^5 = 1$ says $z^{-1} = z^4$ and $z^{-2} = z^3$, so

$$1 + z + z^{-1} + z^2 + z^{-2} = 0;$$

i.e.,

$$1+e^{\frac{2\pi i}{5}}+e^{\frac{-2\pi i}{5}}+e^{\frac{4\pi i}{5}}+e^{\frac{-4\pi i}{5}}=0,$$

or

$$1+2\cos\left(\frac{2\pi}{5}\right)+2\cos\left(\frac{4\pi}{5}\right)=0.$$

Now for all $z \in \mathbf{C}$,

$$\cos(2z)=\cos(z+z)=\cos^2(z)-\sin^2(z)=\cos^2(z)-\Big(1-\cos^2(z)\Big)=2\cos^2(z)-1,$$

so

$$1+2\cos\left(\frac{2\pi}{5}\right)+2\left(2\cos^2\left(\frac{2\pi}{5}\right)-1\right)=0. \qquad (12.69)$$

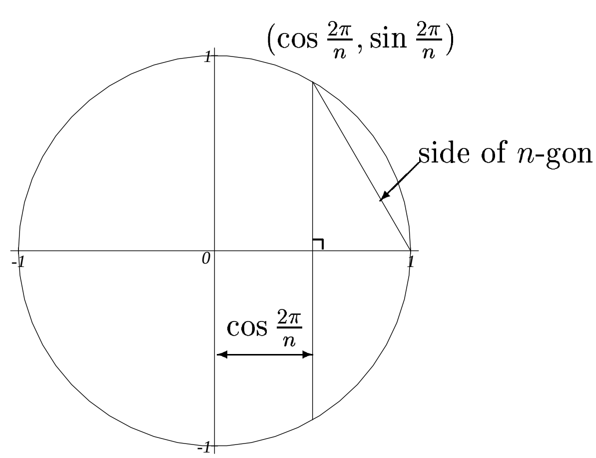
Hence $\cos\left(\frac{2\pi}{5}\right)$ satisfies a quadratic equation.

12.70 Exercise.

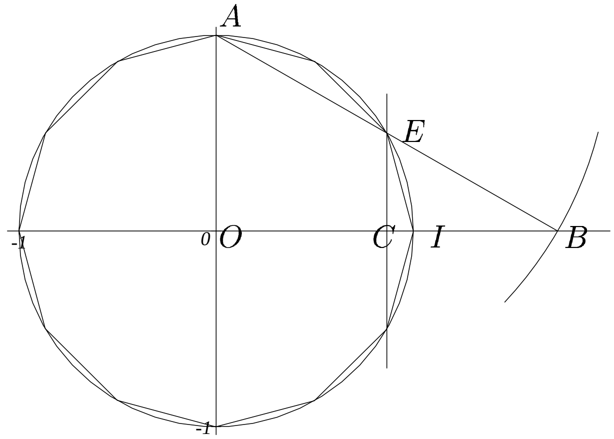
a) Solve (12.69), and determine $\cos\left(\frac{2\pi}{5}\right)$ and $\sin\left(\frac{2\pi}{5}\right)$ in algebraic terms.

b) The quadratic equation has two solutions, one of which is $\cos\left(\frac{2\pi}{5}\right)$. What is the geometrical significance of the other solution?

12.71 Entertainment. The algebraic representation for $\cos\left(\frac{2\pi}{5}\right)$ shows that a regular pentagon can be inscribed in a given circle. Let a circle be given, and call its radius 1. If you can construct $\cos\left(\frac{2\pi}{n}\right)$ with compass and straightedge (see the figure), then you can construct a side of a regular n-gon inscribed in the circle (and hence you can construct the n-gon).



For example, since $\cos\left(\frac{2\pi}{12}\right) = \frac{\sqrt{3}}{2}$, we can construct a dodecagon as follows:



Construction of a Dodecagon

In the figure, make an arc of radius 2 with center at A, intersecting the x-axis at B. Then $OB = \sqrt{3}$, so if C bisects OB, then $OC = \cos\left(\frac{2\pi}{12}\right)$, and the vertical line through C intersects the circle at E where IE is a side of the 12-gon.

Use the formula for $\cos\left(\frac{2\pi}{5}\right)$ to inscribe a regular pentagon in a circle.

12.72 Entertainment. (This problem entertained Gauss. It will probably not really entertain you, unless you are another Gauss.) Show that a regular 17-gon can be inscribed in a circle using compasses and straightedge.

Gauss discovered this result in 1796 [31, p 754] when he was a nineteen year old student at Göttingen. The result is [21, p 458]

$$\begin{aligned}\cos\left(\frac{2\pi}{17}\right) &= -\frac{1}{16} + \frac{1}{16}\sqrt{17} + \frac{1}{16}\sqrt{34 - 2\sqrt{17}} \\ &\quad + \frac{1}{8}\sqrt{17 + 3\sqrt{17} - \sqrt{(34 - 2\sqrt{17})} - 2\sqrt{34 + 2\sqrt{17}}}.\end{aligned}$$

12.8 Proof of the Differentiation Theorem

12.73 Lemma. *The power series* $\sum\{nz^n\}$ *has radius of convergence equal to* 1.

12.74 Exercise. Prove lemma 12.73. (We proved this lemma earlier using the differentiation theorem. Since we need this result to prove the differentiation theorem, we now want a proof that does *not* use the differentiation theorem.)

12.75 Lemma. *Let $\sum\{a_n z^n\}$ be a power series. Then the two series $\sum\{a_n z^n\}$ and $\sum\{na_n z^{n-1}\}$ have the same radius of convergence.*

Proof: I'll show that for all $w, v \in \mathbf{C}\backslash\{0\}$.

a) If $\sum\{|na_n w^{n-1}|\}$ converges, then $\{\sum |a_n w^n|\}$ converges.

b) If $\sum\{|a_n w^n|\}$ converges and $|v| < |w|$, then $\sum\{|na_n v^{n-1}|\}$ converges.

a) follows from the comparison test, since

$$|a_n w^n| \leq |na_n w^{n-1}| \cdot |w| \text{ for all } n \in \mathbf{Z}^+.$$

To prove b), suppose $\sum\{|a_n w^n|\}$ converges and $|v| < |w|$. By lemma 12.73, $\sum\left\{n\left|\frac{v}{w}\right|^n\right\}$ converges, and hence $\left\{n\left|\frac{v}{w}\right|^n\right\}$ is bounded. Choose $M \in \mathbf{R}^+$ such that

$$n\left|\frac{v}{w}\right|^n \leq M \text{ for all } n \in \mathbf{N}.$$

Then $n|v|^n < M|w^n|$, and

$$\left|a_n n|v|^{n-1}\right| \leq |a_n w^n| \cdot \frac{M}{|v|} \text{ for all } n \in \mathbf{N}.$$

By the comparison test, $\sum\{|a_n n v^{n-1}|\}$ converges. |||

12.76 Corollary. *$\sum\{a_n z^n\}$ and $\sum\{a_n n(n-1)z^{n-2}\}$ have the same radius of convergence.*

Proof: Use the lemma twice. |||

12.77 Theorem. *Let $\sum\{c_n z^n\}$ be a power series with positive radius of convergence. Let $f(z) = \sum_{n=0}^{\infty} c_n z^n$ for all z in the disc of convergence for f and let $Df(z) = \sum_{n=1}^{\infty} nc_n z^{n-1}$ be the function corresponding to the formal derivative of $\sum\{c_n z^n\}$. Then f is differentiable on its disc of convergence, and $f'(a) = Df(a)$ for all a in the disc of convergence.*

Proof: Let a be a point in the disc of convergence, and let z be a different point in the disc. Then

$$\begin{aligned} f(z)-f(a) &= \sum_{n=0}^{\infty} c_n z^n - \sum_{n=0}^{\infty} c_n a^n \\ &= \sum_{n=1}^{\infty} c_n (z^n - a^n) \qquad \text{(since } z^0 = a^0\text{)} \\ &= \sum_{n=1}^{\infty} c_n (z-a) \sum_{j=0}^{n-1} z^{n-1-j} a^j \\ &= (z-a) \sum_{n=1}^{\infty} c_n \sum_{j=0}^{n-1} z^{n-1-j} a^j. \end{aligned}$$

Let

$$D_a f(z) = \sum_{n=1}^{\infty} c_n \sum_{j=0}^{n-1} z^{n-1-j} a^j.$$

Then

$$f(z) - f(a) = (z-a) D_a f(z),$$

and since

$$D_a f(a) = \sum_{n=1}^{\infty} c_n \sum_{j=0}^{n-1} a^{n-1} = \sum_{j=1}^{\infty} c_n n a^{n-1} = Df(a),$$

the theorem will follow if we can show that $D_a f$ is continuous at a.

In the calculation below, I quietly use the following facts:

a) When $n = 1$, $\sum_{j=0}^{n-1} z^{n-1-j} a^j - \sum_{j=0}^{n-1} a^{n-1-j} a^j = 0$.

b) When $j = n-1$, $z^{n-1-j} - a^{n-1-j} = 0$.

$$\begin{aligned} D_a f(z) - D_a f(a) &= \sum_{n=1}^{\infty} c_n \sum_{j=0}^{n-1} z^{n-1-j} a^j - \sum_{n=1}^{\infty} c_n \sum_{j=0}^{n-1} a^{n-1-j} a^j \\ &= \sum_{n=2}^{\infty} c_n \sum_{j=0}^{n-1} a^j (z^{n-1-j} - a^{n-1-j}) \\ &= \sum_{n=2}^{\infty} c_n \sum_{j=0}^{n-2} a^j (z-a) \sum_{k=0}^{n-2-j} z^{n-2-j-k} a^k \\ &= (z-a) \sum_{n=2}^{\infty} c_n \sum_{j=0}^{n-2} \sum_{k=0}^{n-2-j} z^{n-2-j-k} a^{j+k}. \qquad (12.78) \end{aligned}$$

Let the radius of convergence of our power series be R, and let $\varepsilon = \dfrac{R - |a|}{2}$. Then

$$\begin{aligned} |z-a| < \varepsilon \implies & |z| - |a| \le |z-a| < \varepsilon \\ \implies & |z| < |a| + \varepsilon = |a| + \frac{R-|a|}{2} = \frac{R+|a|}{2}. \end{aligned}$$

Let $S = \dfrac{R + |a|}{2} < R$. Then $|a| < S$, and

$$\begin{aligned} |z-a| < \varepsilon \implies & |z| < S \\ \implies & \left| \sum_{j=0}^{n-2} \sum_{k=0}^{n-2-j} z^{n-2-j-k} a^{j+k} \right| \le \sum_{j=0}^{n-2} \sum_{k=0}^{n-2-j} |z|^{n-2-j-k} |a|^{j+k} \\ \le & \sum_{j=0}^{n-2} \sum_{k=0}^{n-2-j} S^{n-2} = S^{n-2} \sum_{j=0}^{n-2} (n-1-j) \\ \le & S^{n-2} \sum_{j=0}^{n-2} n \le S^{n-2} \sum_{j=0}^{n-1} n \\ = & S^{n-2} \cdot \frac{n(n-1)}{2} \le S^{n-2} \cdot n(n-1). \end{aligned}$$

(Here I've used the fact that $n - 1 - j \le n$ for $0 \le j \le n - 2$.) Thus

$$|z-a| < \varepsilon \implies \sum_{n=2}^{\infty} \left| c_n \sum_{j=0}^{n-2} \sum_{k=0}^{n-2-j} z^{n-2-j-k} a^{j+k} \right| \le \sum_{n=2}^{\infty} |c_n| S^{n-2} \cdot n(n-1).$$

We noticed in the corollary to lemma 12.75 that the series $\sum\{n(n-1)c_n z^{n-2}\}$ has radius of convergence R, and hence $\sum\{|c_n| S^{n-2} n(n-1)\}_{n \ge 2}$ converges to a limit M, and by (12.78),

$$|D_a f(z) - D_a f(a)| \le |z - a| \cdot M \text{ whenever } |z - a| < \varepsilon.$$

If $\{w_n\}$ is a sequence in $\operatorname{dom}(D_a f)$ such that $\{w_n\} \to a$, then

$$|D_a f(w_n) - D_a f(a)| \le |w_n - a| \cdot M$$

for all large n, and by the null-times bounded theorem and comparison theorem for null sequences, $\{D_a f(w_n)\} \to D_a f(a)$. Hence, $D_a f$ is continuous at a. ‖

12.9 Some XVIII-th Century Calculations

The following proofs that

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = 1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \&c = \frac{\pi^2}{6}$$

and

$$\sum_{n=0}^{\infty} \frac{1}{(2n+1)^2} = 1 + \frac{1}{3^2} + \frac{1}{5^2} + \frac{1}{7^2} + \&c = \frac{\pi^2}{8}$$

use XVIII-th century standards or rigor. You should decide what parts are justified. I denote $f'(\theta)$ by $\dfrac{df}{d\theta}$ below. By the geometric series formula,

$$\sum_{n=0}^{\infty} z^n = \frac{1}{1-z}.$$

If $z = re^{i\theta}$ where $r > 0$, $\theta \in \mathbf{R}$, then

$$\sum_{n=0}^{\infty} r^n e^{in\theta} = \frac{1}{1 - re^{i\theta}} \cdot \frac{1 - re^{-i\theta}}{1 - re^{-i\theta}}$$

so

$$\sum_{n=0}^{\infty} (r^n \cos(n\theta) + ir^n \sin(n\theta)) = \frac{1 - re^{-i\theta}}{1 - r(e^{i\theta} + e^{-i\theta}) + r^2} = \frac{(1 - r\cos\theta) + ir\sin\theta}{1 + r^2 - 2r\cos\theta}.$$

By equating the real and imaginary parts, we get

$$\sum_{n=0}^{\infty} r^n \cos n\theta = \frac{1 - r\cos\theta}{1 + r^2 - 2r\cos\theta}, \quad \sum_{n=0}^{\infty} r^n \sin n\theta = \frac{r\sin\theta}{1 + r^2 - 2r\cos\theta}.$$

For $r = 1$, this yields

$$\sum_{n=0}^{\infty} \cos n\theta = \frac{1 - \cos\theta}{2 - 2\cos\theta} = \frac{1}{2}.$$

Thus, $1 + \sum_{n=1}^{\infty} \cos n\theta = \frac{1}{2}$, so

$$\sum_{n=1}^{\infty} \cos n\theta = -\frac{1}{2}.$$

Hence,

$$\frac{d}{d\theta}\left(\sum_{n=1}^{\infty}\frac{\sin n\theta}{n}\right)=\frac{d}{d\theta}\left(-\frac{1}{2}\theta\right).$$

Since two antiderivatives of a function differ by a constant

$$\sum_{n=1}^{\infty}\frac{\sin n\theta}{n}=-\frac{1}{2}\theta+C$$

for some constant C. When $\theta=\pi$, we get

$$0=\sum_{n=1}^{\infty}\frac{\sin n\pi}{n}=-\frac{1}{2}\pi+C$$

so $C=\frac{1}{2}\pi$ and thus

$$\sum_{n=1}^{\infty}\frac{\sin n\theta}{n}=\frac{1}{2}(\pi-\theta). \tag{12.79}$$

For $\theta=\frac{\pi}{2}$, this gives us

$$\frac{1}{1}-\frac{1}{3}+\frac{1}{5}-\frac{1}{7}+\frac{1}{9}+\&c=\frac{1}{2}\left(\pi-\frac{\pi}{2}\right)=\frac{\pi}{4}$$

(which is the Gregory-Leibniz-Madhava formula). We can rewrite (12.79) as

$$\frac{d}{d\theta}\sum_{n=1}^{\infty}-\frac{\cos n\theta}{n^2}=\frac{d}{d\theta}\left(-\frac{(\pi-\theta)^2}{4}\right).$$

Again, since two antiderivatives of a function differ by a constant, there is a constant C_1 such that

$$\sum_{n=1}^{\infty}\frac{\cos n\theta}{n^2}=\frac{(\pi-\theta)^2}{4}+C_1.$$

For $\theta=0$, this says

$$\sum_{n=1}^{\infty}\frac{1}{n^2}=\frac{\pi^2}{4}+C_1,$$

and for $\theta=\pi$, this says

$$\sum_{n=1}^{\infty}\frac{(-1)^n}{n^2}=C_1.$$

Subtract the second equation from the first to get

$$\sum_{n=1}^{\infty} \frac{1-(-1)^n}{n^2} = \frac{\pi^2}{4};$$

i.e.,

$$2 + \frac{2}{3^2} + \frac{2}{5^2} + \frac{2}{7^2} + \&c = \frac{\pi^2}{4},$$

and thus

$$1 + \frac{1}{3^2} + \frac{1}{5^2} + \frac{1}{7^2} + \&c = \frac{\pi^2}{8}. \tag{12.80}$$

Let $S = 1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \frac{1}{5^2} + \&c$. Subtract (12.80) from this to get

$$\begin{aligned} S - \frac{\pi^2}{8} &= \frac{1}{2^2} + \frac{1}{4^2} + \frac{1}{6^2} + \&c = \frac{1}{4\cdot 1} + \frac{1}{4\cdot 2^2} + \frac{1}{4\cdot 3^2} + \&c \\ &= \frac{1}{4}\left[1 + \frac{1}{2^2} + \frac{1}{3^2} + \&c\right] = \frac{1}{4}S. \end{aligned}$$

Hence, $\frac{3}{4}S = \frac{\pi^2}{8}$, and then $S = \frac{\pi^2}{6}$. |||

An argument similar to the following was given by Jacob Bernoulli in 1689 [31, p 443]. Let

$$N = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \&c.$$

Then

$$N - 1 = \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \&c.$$

Subtract the second series from the first to get

$$\begin{aligned} 1 &= \left(1 - \frac{1}{2}\right) + \left(\frac{1}{2} - \frac{1}{3}\right) + \left(\frac{1}{3} - \frac{1}{4}\right) + \left(\frac{1}{4} - \frac{1}{5}\right) + \&c \\ &= \frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4} + \frac{1}{4\cdot 5} + \&c. \end{aligned}$$

Therefore,

$$1 = \frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4} + \frac{1}{4\cdot 5} + \&c.$$

12.81 Exercise.

a) Explain why Bernoulli's argument is not valid.

b) Give a valid argument proving that

$$\sum_{n=1}^{\infty} \frac{1}{n(n+1)} = 1.$$

12.82 Note. The notation π was introduced by William Jones in 1706 to represent the ratio of the circumference to the diameter of a circle[15, vol2, p9]. Both Maple and Mathematica designate π by `Pi` .

The notation e was introduced by Euler in 1727 or 1728 to denote the base of natural logarithms[15, vol 2, p 13]. In Mathematica e is denoted by `E` . In the current version of Maple there is no special name for e; it is denoted by `exp(1)` .

Bibliography

[1] Tom M. Apostol. *Calculus*, volume I. John Wiley & Sons, Inc., second edition, 1967. QA300 .A5726 1967 v.1.

[2] Archimedes. *The Works of Archimedes Edited in Modern Notation with Introductory Chapters by T. L. Heath*. Dover Publications, 195? QA31 .A692.

[3] V. I. Arnold and A. Avez. *Ergodic Problems of Classical Mechanics*. Benjamin, 1968. QA845 .A713.

[4] Aristotle. *The Works of Aristotle Translated into English under the Editorship of W. D. Ross: Analytica Priora*. Oxford University Press, 1952. B407.R83 1952 v1.

[5] Aristotle. *Aristotle's Metaphysics Translated with Commentaries and Glossary by Hippocrates G. Apostle*. Indiana University Press, 1966. B434 A5A6.

[6] Emil Artin and Otto Schreier. Algebraische konstruction reeler Körper. In *Collected Papers of Emil Artin*, pages 258–272. Springer-Verlag, 1982. QA7 .A68 1982.

[7] Paul Bencerraf and Hilary Putnam, editors. *Philosophy of Mathematics*. Cambridge University Press, 1983. QA8.4 .P48 1983.

[8] Jacob Bernoulli. *Die Werke Von Jacob Bernoulli*, volume 3. Birkäuser Verlag Basel, 1975. QA3 B52 1969 v.3.

[9] Evert Willem Beth. *The foundations of mathematics; a study in the philosophy of science*. North-Holland Pub.Co, 1959. QA9 .B5153.

[10] Errett Bishop. Schizophrenia in contemporary mathematics. In Murray Rosenblatt, editor, *Errett Bishop: Reflections on Him and His Research*, pages 1–32. American Mathematical Society, 1985. QA326 .E75 1985.

[11] George Boole. *An investigaton of the Laws of Thought on which are founded the mathematical theories of logic and probabilities.* Dover Publications, 1951. BC135 B6 1951.

[12] R. Creighton Buck. *Advanced Calculus.* McGraw Hill, third edition, 1978. QA303 .B917 1978.

[13] Joe Buhler. Real and complex numbers, series, and functions. Technical report, Reed College Mathematics Department, 1998.

[14] Florian Cajori. *A History of Mathematics.* Macmillan, 1913. QA21 .C13.

[15] Florian Cajori. *A History of Mathematical Notations(Two volumes bound as one).* Dover Publications, 1993. QA41 .C32 1993.

[16] Girolamo Cardano. *Ars Magna or The Rules of Algebra Translated and Edited by T. Richard Witmer.* Dover Publications, 1993. QA154.8.C3713 1993.

[17] Richard Courant and Herbert Robbins. *What is Mathematics? An elementary approach to ideas and methods.* Oxford University Press, 1941. QA37 .C675 1941.

[18] Leonard Eugene Dickson. Definition of a group and a field by independent postulates. *Transactions of the American Mathematical Society*, 6:198–204, 1905.

[19] Euclid. *Euclid's Elements Translated with Introduction and Commentary by Sir Thomas L. Heath (3 volumes).* Dover Publications, 1956. QA31 .E875 1956.

[20] Leonard Euler. *Elements of Algebra Translated by Rev. John Hewlett, B.D. F.A.S. &c.* Springer–Verlag, 1984. QA154.E813 1984.

[21] Carl Friedrich Gauss. *Disquisitiones Arithmeticae - English Translation by Arthur A Clarke.* Yale University Press, 1966. QA241 .G2613.

[22] Herman H. Goldstine. *A History of Numerical Analysis from the 16th through the 19th Century.* Springer-Verlag, 1977. QA297 .G64.

[23] Judith V. Grabiner. *The Origins of Cauchy's Rigorous Calculus.* MIT Press, 1981.

[24] William Rowen Hamilton. On a new species of imaginary quantities connected with the theory of quaternions. In *The Mathematical Papers of Sir William Rowan Hamilton*, volume III, pages 111–116. Cambridge University Press, 1967. QA3 .H269 v.3.

[25] William Rowen Hamilton. Theory of conjugate functions or algebraic couples; with a preliminary and elementary essay on algebra as the science of pure time. In *The Mathematical Papers of Sir William Rowan Hamilton*, volume III, pages 3–96. Cambridge University Press, 1967. QA3 .H269 v.3.

[26] Sir Thomas Heath. *Mathematics in Aristotle.* Oxford University Press, 1949. QA31 A95H4.

[27] Leon Henkin. On mathematical induction. *American Mathematical Monthly*, 67:323–338, 1960.

[28] Edward V. Huntington. Complete sets of postulates for the theory of real quantities. *Transactions of the American Mathematical Society*, 4:358–370, 1903.

[29] Edward V. Huntington. Definitions of a field by sets of independent postulates. *Transactions of the American Mathematical Society*, 4:31–37, 1903.

[30] George Gheverghese Joseph. *The Crest of the Peacock : Non-European Roots of Mathematics.* I.B. Tauris, 1991. QA21 .G53 1991.

[31] Morris Kline. *Mathematical Thought from Ancient to Modern Times.* Oxford University Press, 1972. QA21 .53.

[32] Helge von Koch. Une méthod géometrique Élémentaire pour l'Étude de certaines questiones de la théorie des courbes planes. *Acta Mathematica*, 30:145–174, 1906.

[33] Herbert Mehrtens. Ludwig Bieberbach and "deutsche mathematik". In Esther Phillips, editor, *Studies in the History of Mathematics*, pages 195–241. Mathematical Association of America, 1987. QA21.S92 1987

[34] Jan Mycielski. How to teach limits and continuity. Letters to the Editor, Notices of the American Mathematical Society, page 569, May 1998.

[35] John M. H. Olmsted. *The Real Number System.* Appleton-Century-Crofts, 1962. QA255 .O43.

[36] Blaise Pascal. Treatise on the arithmetic triangle. In *A Source Book in Mathematics*, pages 67–79. Dover Publications, 1969. QA3.S66 1959.

[37] Giuseppe Peano. The principles of arithmetic presented by a new method. In *From Frege to Godel; a source book in mathematical logic, 1879–1931*, pages 83–97. Harvard Unibersity Press, 1967. QA9 .V3.

[38] Plato. *Great Dialogues of Plato, Translated by W. D. Rouse, edited by Eric H. Warmington and Philip G. Rouse.* New American Library, 1956.

[39] Plato. *The Laws: Translated with an Introduction by Trevor J. Saunders.* Penguin Books, 1970. B358 .R6.

[40] Helena M. Pycior. *Symbols, Impossible Numbers, and Geometric Entanglements.* Cambridge University Press, 1997. QA151.P94 1997.

[41] Alain Robert. *Nonstandard Analysis.* John Wiley & Sons, Inc, 1988. QA299.82 .R5813 1988.

[42] S. B. Russ. A translation of Bolzano's paper on the intermediate value theorem. *Historia Mathematica*, 7:156–185, 1980.

[43] Bertrand Russell. *Principles of mathematics.* W. W. Norton & Company, second edition, 1943. QA9 .R88 1943.

[44] David Singmaster. An elementary evaluation of the Catalan numbers. *American Mathematical Monthly*, 85:366–368, 1978.

[45] David Eugene Smith. *History of Mathematics*, volume II. Dover Publications, 1958. QA21 .S62 1958 v.2.

[46] David Eugene Smith, editor. *A Source Book in Mathematics.* Dover Publications, 1959. QA3 .S66 1959.

[47] Michael Spivak. *Calculus.* Publish or Perish, Inc., third edition, 1994. QA303 .S761c, 1994.

[48] H. Weber. Die allgemeinen Grundlagen der Galois'schen Gleicheungstheorie. *Mathematische Annalen*, 43:521–549, 1893.

Appendix A

Associativity and Distributivity of Operations in $\mathbf{Z}_n$

Let $n \in \mathbf{Z}$ satisfy $n \geq 2$. Let $\mathbf{Z}_n = \{x \in \mathbf{N}: x < n\}$. Let $\oplus_n$ and $\odot_n$ be the binary operations on $\mathbf{Z}_n$ defined by

$$\begin{aligned} a \oplus_n b &= \text{remainder when } a+b \text{ is divided by } n, \\ a \odot_n b &= \text{remainder when } ab \text{ is divided by } n. \end{aligned}$$

Thus for all $a, b \in \mathbf{Z}_n$,

$$a + b = r \cdot n + (a \oplus_n b) \text{ for some } r \in \mathbf{N}. \tag{A.1}$$

$$a \cdot b = s \cdot n + (a \odot_n b) \text{ for some } s \in \mathbf{N}. \tag{A.2}$$

We will show that $\oplus_n$ and $\odot_n$ are associative by using the usual properties of addition and multiplication on $\mathbf{Z}$.

A.3 Lemma. *Let $x, y \in \mathbf{Z}_n$, $q, r \in \mathbf{Z}$. If $nq + x = nr + y$, then $x = y$ and $q = r$.*

Proof:

Case 1. Suppose $y \leq x$. Then by our assumptions,

$$x - y = n(r - q)$$

and

$$0 \leq x - y \leq x < n \cdot 1.$$

So

$$0 \leq n(r-q) < n \cdot 1.$$

Since $n > 0$, it follows that $0 \leq r - q < 1$ and since $r - q$ is an integer $r - q = 0$, so $r = q$. Then $x - y = 0$, so $x = y$.

Case 2. If $y > x$, use Case 1 with y and x interchanged. ‖

A.4 Theorem. *$\oplus_n$ is associative on $\mathbf{Z}_n$.*

Proof: Let $a, b, c \in \mathbf{Z}_n$. Then

$$a + b = n \cdot t + (a \oplus_n b) \text{ for some } t \in \mathbf{Z}. \tag{A.5}$$

$$b + c = n \cdot r + (b \oplus_n c) \text{ for some } r \in \mathbf{Z}. \tag{A.6}$$

$$(a \oplus_n b) + c = n \cdot s + ((a \oplus_n b) \oplus_n c) \text{ for some } s \in \mathbf{Z}. \tag{A.7}$$

$$a + (b \oplus_n c) = n \cdot w + (a \oplus_n (b \oplus_n c)) \text{ for some } w \in \mathbf{Z}. \tag{A.8}$$

By adding c to both sides of (A.5), we get

$$(a + b) + c = nt + ((a \oplus_n b) + c)\,, \tag{A.9}$$

and by adding a to both sides of (A.6), we get

$$a + (b + c) = nr + (a + (b \oplus_n c))\,. \tag{A.10}$$

Replace $(a \oplus_n b) + c$ in (A.9) by its value from (A.7) to get

$$(a + b) + c = n(s + t) + ((a \oplus_n b) \oplus_n c) \tag{A.11}$$

and replace $a + (b \oplus_n c)$ in (A.10) by its value from (A.8) to get

$$a + (b + c) = n(r + w) + (a \oplus_n (b \oplus_n c)) \tag{A.12}$$

By (A.11) and (A.12) and the associative law in $\mathbf{Z}$,

$$n(s + t) + ((a \oplus_n b) \oplus_n c) = n(r + w) + (a \oplus_n (b \oplus_n c))\,.$$

the associativity of $\oplus_n$ follows from lemma (A.3). ‖

A.13 Theorem. *$\odot_n$ is associative on $\mathbf{Z}_n$.*

Proof: The proof is nearly identical with the proof that $\oplus_n$ is associative.

A.14 Theorem. *The distributive law holds in $\mathbf{Z}_n$; i.e., for all $a, b, c \in \mathbf{Z}_n$,*

$$a \odot_n (b \oplus_n c) = (a \odot_n b) \oplus_n (a \odot_n c).$$

Proof: We have

$$b + c = n \cdot t + (b \oplus_n c) \text{ for some } t \in \mathbf{Z}. \tag{A.15}$$

$$a \cdot (b \oplus_n c) = n \cdot s + (a \odot_n (b \oplus_n c)) \text{ for some } s \in \mathbf{Z}. \tag{A.16}$$

$$a \cdot b = n \cdot u + (a \odot_n b) \text{ for some } u \in \mathbf{Z}. \tag{A.17}$$

$$a \cdot c = n \cdot v + (a \odot_n c) \text{ for some } v \in \mathbf{Z}. \tag{A.18}$$

Multiply both sides of (A.15) by a to get

$$a \cdot (b + c) = n \cdot at + a \cdot (b \oplus_n c). \tag{A.19}$$

Replace $a \cdot (b \oplus_n c)$ in (A.19) by its value from (A.16) to get

$$a \cdot (b + c) = n(at + s) + (a \odot_n (b \oplus_n c)). \tag{A.20}$$

Now add equations (A.17) and (A.18) to get

$$a \cdot b + a \cdot c = n \cdot (u + v) + ((a \odot_n b) + (a \odot_n c)). \tag{A.21}$$

We know that for some $w \in \mathbf{Z}$,

$$(a \odot_n b) + (a \odot_n c) = n \cdot w + ((a \odot_n b) \oplus_n (a \odot_n c)),$$

and if we substitute this into (A.21), we obtain

$$a \cdot b + a \cdot c = n(u + v + w) + ((a \odot_n b) \oplus_n (a \odot_n c)). \tag{A.22}$$

From (A.20) and (A.22) and the distributive law in $\mathbf{Z}$, we conclude

$$n(at + s) + (a \odot_n (b \oplus_n c)) = n(u + v + w) + ((a \odot_n b) \oplus_n (a \odot_n c)).$$

The distributive law follows from lemma A.3. ‖

Appendix B

Hints and Answers

Exercise 2.11: In each case there is only one invertible element.

Exercise 2.40: Note that the calculator sum of a very small number and a very large number is the large number. Note that the calculator product of two small positive numbers is 0.

Exercise 2.55: The system $(\mathbf{Q}, \oplus, \odot)$ fails two axioms. The other three each fail one axiom.

Exercise 2.78: Use (2.75).

Exercise 2.90: For part (b), use (2.74).

Exercise 2.93: Part e) can be done quickly by using parts a), b) and d).

Exercise 2.123: One of the conditions is that a and b have the same sign.

Exercise 2.135: There are nine cases to consider (three for a and three for y). They can be reduced to five cases, one of which is $((x = 0$ or $y = 0)$.

Exercise 2.144: There is a *very* short proof for a).

Exercise 2.145: Apply the product formula for absolute values to $|a \cdot a^{-1}|$.

Exercise 2.154: Use (2.138).

Exercise 3.24: You can take $S = F^+$.

Exercise 3.32: Suppose n is both even and odd, and derive a contradiction by using theorems 3.15 and 3.19.

Exercise 3.43: For part b) use part a) together with exercise 3.32

Exercise 3.57: You can let $P(n) =$"for all $m \in \mathbf{N}((a^n)^m = a^{(nm)})$" or $P(m) =$"for all $n \in \mathbf{N}((a^n)^m = a^{(nm)})$".

Exercise 3.82: f) Note that $x^6 + a^6 = (x^2)^3 - (-a^2)^3$.

Exercise 3.85: $S_n = \frac{n}{n+1}$.

Exercise 3.87: $T_n = n^2$.

Exercise 4.19: a) Note that $\frac{1}{z} = z^{-1}$. b) The solutions are i and $\frac{2}{5} - \frac{1}{5}i$.

Exercise 4.23: For part c), write $z = w \cdot \frac{z}{w}$ and use part b). Remark 4.22 is used for part f).

Exercise 4.25: a) 1. b) 32i.

Exercise 5.15: I let $P(n) =$"$2^n \geq n$ and $2^n \geq 1$" and I used the fact that $2^{n+1} = 2^n + 2^n$. (It would be reasonable to assume $2^n \geq 1$ for all n, but I proved it).

Exercise 5.48: Suppose $f(x) = a = f(t)$, and use trichotomy to show that $x = t$.

Exercise 5.51: a) If $x^q = y^q$, then $x = y$. b) If $x^{qr} = y^{rq}$, then $x = y$. (We know the laws of exponents for integer exponents.)

Exercise 5.54: Raise both sides of the equation to the same integer power, and use laws of exponents for integer powers.

Exercise 6.5: e) Notice that $x^2 \leq x^2 + y^2$, and use theorem 2.128.

Exercise 6.26: The roots are $\pm\left(\frac{5}{\sqrt{2}} + \frac{i}{\sqrt{2}}\right)$.

Exercise 7.21: I showed $|(\frac{2+i}{3})|^2 < .7$, so that $|(\frac{2+i}{3})| < \sqrt{.7}$. Then I used the fact that $\{.7^n\}$ is known to be a null sequence, and used the root theorem and the comparison theorem.

Exercise 7.22: All three sequences are null sequences. For the last sequence, I showed $\frac{n^2+6}{n^2+3} \leq 2$ for all $n \geq 1$. For the first sequence $\{a_n\}$, I showed $|a_n| \leq \frac{10000}{\sqrt{n}}$ for all $n \geq 1$.

Exercise 7.24: The set of all complex sequences does not form a field. All of the field axioms except one hold.

Exercise 7.28: $N_{fg}(\epsilon) = \max(N_f(\epsilon), N_g(1))$ works.

Exercise 7.44: You can take $N_{fg}(\epsilon) = N_f(\frac{\epsilon}{M})$, where $|g(n)| \leq M$ for all $n \in \mathbf{N}$.

Exercise 7.49: Note that $g = (f+g) - f$, and show that the assumption $f+g$ converges is contradictory.

Exercise 7.50: Note that if $c \neq 0$, then $f = \frac{1}{c} \cdot cf$.

Exercise 7.56: Multiply numerator and denominator of $\sqrt{f(n)} - \sqrt{L}$ by $\sqrt{f(n)} + \sqrt{L}$.

Exercise 7.57: All of the sequences converge. $h \to \frac{-4i}{3}$ and $l \to \frac{1}{2}$.

Exercise 7.58: If B_1 is a bound for f, and B_2 is a bound for g, then $B_1 + B_2$ is a bound for $f+g$.

Exercise 7.60: A convergent sequence is the sum of a null sequence and a constant sequence. Now use exercise 7.58.

Exercise 7.69: $\{a_n\} \to \frac{37}{55}$.

Exercise 7.70: One of the sequences diverges. One of the limits is $\frac{255}{82} + \frac{20}{41}i$.

Exercise 7.74: Apply theorem 7.73 to $g - f$.

Exercise 7.75: The statement is false.

Exercise 7.86: The sequence converges to $\frac{A}{a}$ or to $\frac{B}{b}$ or else it diverges. (You should find exact conditions on a, b, A, and B corresponding to each case.)

Exercise 7.94: If $L \leq a_n \leq U$ for all $n \in \mathbf{N}$, then either $|L| + |U|$ or $\max(|L|, |U|)$ will be a bound for $\{a_n\}$

Exercise 7.100: Use corollary 7.96 to show that the sequence converges. Note $a_{n+1} = a_n \cdot \frac{60}{n+1}$. Use the translation theorem to show that the limit is 0.

Exercise 8.4: I used the polar decomposition for α.

Exercise 8.19: Yes. In fact every function from $\mathbf{N}$ to $\mathbf{C}$ is continuous. The only integer p that satisfies $|p| < \frac{1}{2}$ is zero.

Exercise 8.43: a) Limit does not exist. b) Let $\{z_n = x_n + iy_n\}$ be a sequence converging to 0. Apply null-times-bounded theorem to $\{f(z_n)\}$. c) I looked at sequences $\{\frac{\omega}{n}\}$, where ω is a direction.

Exercise 9.10: Four of the requested five functions exist. The other one doesn't.

Exercise 9.13: Apply theorem 9.11 to g, where $g(x) = f(x) - y$

Exercise 9.17: All four functions exist. I described k by drawing its graph.

Exercise 9.19: Assume $F(4) < 0$ and derive a contradiction from the intermediate value theorem.

Exercise 10.10: h is nowhere differentiable. The same sequences that show complex conjugation is nowhere differentiable show that h is also.

Exercise 10.17: $D_a(fg)(z) = f(a)D_ag(z) + g(a)D_af(z) + (z-a)D_af(z)D_ag(z)$.

Exercise 10.19: Write $f^n = \frac{1}{f^{-n}}$, and use the reciprocal rule and exercise 10.18.

Exercise 10.20: Use the product rule and the reciprocal rule.

Exercise 10.31: Only one of the three statements is true.

Exercise 10.37: Use the result of exercise 6.36

Exercise 10.50: For both parts, compare with $\{\frac{1}{n}\}_{n\geq 1}$

Exercise 10.51: The exact value of $\cos(i)$ is $\frac{1}{2}(e + \frac{1}{e})$. You can't prove this (because we have not yet defined e), but you can check your answer using this.

Exercise 11.19: c) Note that the comparison test holds only for sequences of non-negative numbers.

Exercise 11.28: In most cases there is one value for which the ratio test gives no information. However the exceptional values are usually standard test series. For part g) the exceptional value was considered in example 11.27.

Exercise 11.48: b) Show that the real and imaginary parts of the series both converge.

Exercise 11.49: Both series converge absolutely for $|z| < 1$ and diverge for $|z| \geq 1$. (I used the ratio test.)

Exercise 12.6: a) If $z = -1$ then $z^{2^n} = 1$ for all $n \geq 1$, and if $z = i$, then $z^{z^n} = 1$ for all $n \geq 2$. Except for the first few terms, both series are geometric series,

Exercise 12.14: a) Consider geometric series of the form $\sum\{c^n z^n\}$. c) Cf exercise 12.5.a

Exercise 12.20: The sums are $\frac{z}{(1-z)^2}$ and $\frac{z+z^2}{(1-z)^3}$ Get the second by differentiating the first.

Exercise 12.33: a) Use induction and (12.29). b) Use part a) and (12.28).

Exercise 12.34: Calculate $\exp(p \cdot t) = \exp(q \cdot (\frac{p}{q} \cdot t))$ using exercise 12.33

Exercise 12.42: a) Write $a = \exp(\ln(a))$ and use (12.28). b) Write $a = \exp(\ln(a))$ and use exercise 12.34.

Exercise 12.51: Write the trig functions in terms of exponentials, and use $e^a e^b = e^{a+b}$ several times.

Exercise 12.59: Everything follows from $e^{\frac{i\pi}{2}} = i$ and $e^{it} = \cos(t) + i\sin(t)$ and $e^a e^b = e^{a+b}$.

Exercise 12.70: $\cos(\frac{2\pi}{5}) = \frac{\sqrt{5}-1}{4}$.

Appendix C

List of Symbols

$\mathbf{N}$	natural numbers, 6, 69
$\mathbf{Z}$	integers, 6, 69
$\mathbf{Q}$	rational numbers, 6, 69
$\emptyset$	empty set, 6
$\mathbf{Q}^+$	positive rationals, 6
$a \in A$	a is in A, 6
$a \notin A$	a is not in A, 6
$A \subset B$	subset, 7
$\subset$	subset, 7
$A = B$	set equality, 7
$a \neq b$	a is not equal to b., 9
$P \implies Q$	P implies Q, 9
$P \implies Q \implies R \implies S$	11
$P \iff Q$	11
$x = y$	12
$a = b = c = d$	13
$P(x)$, proposition form	14
$\{x \in A : P(x)\}$	the set of all x in A such that $P(x)$ is true, 14
$R \cap T$	intersection of sets, 15
$R \cup T$	union of sets, 15
$R \setminus T$	set difference, 15

Index