Chapter 29
Projects

Tips on Talking about Mathematics

It's not easy to talk about mathematics to other people. In this section, we present some tips that we find helpful when we present a talk to undergraduates.

Let's say someone has just asked you to give a talk about mathematics to undergraduates. Here's what you need to do:

- Thank them, and say you'd love to. Then do the rest of the things below.
- Find out who the audience is and what they know.
- Pick an interesting topic. Find out about the history of the topic, the main players in the field, and the main results.
- Now that you have your topic, you need to write the talk. Start with something everyone is interested in. This could be the history of what you plan to talk about, or it could be an interesting related result. Then motivate the question you are interested in looking at, build up the talk, and remember to find a good conclusion for it.
- As you write your talk, keep the level of the audience in mind. Do not use terms that your audience will not understand. If they haven't heard certain words you will have to define them, which brings us to our next point: the more terms you have to define, the more people you will lose. Pick a topic that doesn't require a lot of introduction.
- You need to decide whether you will use transparencies, the computer, or the blackboard. Each has its advantages and disadvantages. We'll run through each below.

    1. *Blackboard.* If you use the blackboard, you'll most likely move at the right speed for the audience. It's also livelier than the other methods. On the other hand, you should absolutely not rely on your notes. Therefore, if you give a talk using the blackboard, you'll need to know what you are going to say and when you are going to say it. You'll need to watch where you write things, and you shouldn't erase something you want the audience to look at. Make

U. Daepp and P. Gorkin, *Reading, Writing, and Proving: A Closer Look at Mathematics*, Undergraduate Texts in Mathematics, DOI 10.1007/978-1-4419-9479-0_29,

sure that you move away from the board so that everyone can see what you wrote. If your handwriting is illegible, think about using transparencies or the computer.

2. *Transparencies.* Unless you are very careful, you will probably move too quickly for the audience. You'll probably also stand in front of the transparency from time to time, blocking the audience's view. If you are aware of these potential problems, you can correct them. For example, you can use two overheads. You should not write too much on one transparency, and you should always be aware of where you are standing. Find out how big the room is, and make sure that someone in the back of the room will be able to see what you have written. The advantage of transparencies or the computer is that you'll have all your diagrams and pictures in place, and you'll have an outline of your talk with you. So the main disadvantages are that your talk may become monotonous and that it's possible to move so quickly that your audience won't be listening. These are pretty big disadvantages.
3. *Computer.* In many ways, using the computer to give your talk is similar to using transparencies. Many of the advantages and disadvantages are the same. Still, there are a few things that we should mention. For mathematics, many people use Beamer from LaTex. (A tutorial can be found at [9].) As we mentioned, some things are the same as for transparencies. The basic rule is: Don't overdo it. Don't use too many fonts, too many pictures, too many colors, and don't put too much on one screen. However, the computer presents new challenges: If you use a computer, you cannot correct things in front of an audience. You'll need to proofread your slides very very carefully. It's also possible to use a tool that allows you to stand in exactly one position, moving only your thumb. If you do this for your entire talk, it's fairly likely that your talk—no matter how well you prepare it—will be dull. Move! Even if you don't have to, it's important to move around. If you must use a laser pointer, use it sparingly. It's distracting to see a red beam moving rapidly around as you try to read a slide. You can liven up the talk by adding relevant photographs of places, manuscripts, or people. You might even add a video clip. Just make sure that these "attention getters" are relevant and well incorporated.
4. *Blackboard, Transparencies, and Computer.* One thing you can do is combine two or three of these methods of presentation. In a talk for undergraduates, it's nice for them to have something to look at from time to time, other than the speaker.

Pick the method you are most comfortable with and that you like the best. Then work around the disadvantages.

- So now you have your topic, your talk, and a method of presentation. You're done, right? Um ... no. You still have to present the talk. Surprisingly, the hardest part of the talk is timing. We've alluded to this already in our discussion on transparencies, but there's more to be said.

- Find out how long the talk is. If it's twenty minutes, talk for twenty minutes. (No one will complain if it's eighteen minutes, and everyone will complain if it's thirty.) There is only one way to know how long your talk is: practice it.
- The best way to practice a talk is to give it to yourself once. Fix the things you realize need fixing. Then try to find an audience of two people, one who knows what you are talking about and one who does not. Ask them if you can present the talk to them. Listen to their comments and use them to improve your talk.
- Write an interesting, but truthful abstract. The abstract should indicate the level of the talk.
- Before you give your talk, ask if you can see the room that you will speak in. Check that everything you need is there.
- Make sure that everyone in the room can hear you when you speak. When you give the talk, look at the audience. They'll let you know how you are doing.

There are other articles on how to talk about mathematics ([68], [43]), but these are primarily aimed at graduate students or professional mathematicians. Of course, many of the tips are the same, because many of the mistakes people make—whether talking to undergraduates, graduate students, or professors—are the same.

29.1 Picture Proofs

Introduction

You have probably heard the saying "a picture is worth a thousand words." The same is true in mathematics: a good picture can help a reader visualize what is happening, it can aid a mathematician in finding a solution, and it can shed light on other potential results. A bad picture, on the other hand, can be deceiving. Relying too much on what we see might lead us to incorrect proofs, which in turn can lead to false results. This project should help convince you of that.

One of the most influential theorems in mathematics is Pythagoras' theorem. It states that in a right triangle the lengths of the sides of the triangle satisfy $a^2 + b^2 = c^2$, where c denotes the length of the hypotenuse, and a and b denote the lengths of the other two sides of the triangle. There are many known proofs of this theorem, some of them based on clever figures. You will see two such proofs below.

Prerequisites

Basic geometry skills plus an understanding of what constitutes a rigorous argument are the necessary prerequisites for this project. We suggest that you read through Chapter 5 before attempting this project.

Guided Project

1. The diagram in Figure 29.1 suggests a proof of Pythagoras' theorem. To make this proof rigorous, however, you will need to do two things; you need to prove something about the diagram and you need to do an algebraic calculation. Do both.
2. Give a second proof of Pythagoras' theorem based on Figure 29.2. This one does not need algebraic calculations. It is all in the picture—or is it?
3. If you accepted the picture of Figure 29.2 as a complete proof of Pythagoras' theorem, then you are probably willing to believe that Figure 29.3 provides a proof that $168 = 169$. After all, both proofs require that we shift the pieces around to form another familiar object. What is wrong with this proof?
4. Find a picture to illustrate the statement

$$\sum_{k=1}^{\infty} \frac{1}{2^k} = 1.$$

   Does your picture amount to a rigorous proof? What are its strengths and what are its weaknesses?
5. Use the picture of Figure 29.4 to prove that

$$\int_0^1 \frac{dx}{1+x^2} = \frac{\pi}{4}.$$

   (This problem was proposed by Michael Vowe in [105]. Figure 29.4 is part of the solution given by Gerhard Wanner in [106].)

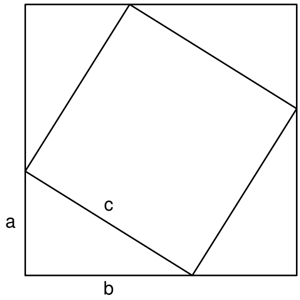

Fig. 29.1 $a^2 + b^2 = c^2$

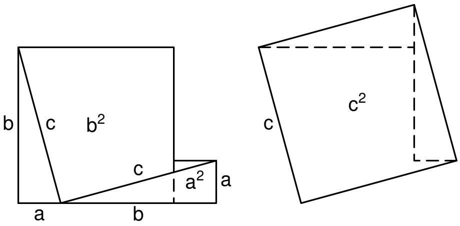

Fig. 29.2 $a^2 + b^2 = c^2$

Open-Ended Project

Try to find some other picture proofs. (We suggest you think back to your geometry course.) Can you also come up with a (somewhat) convincing picture proof of a false statement?

Notes and Sources

We first learned of the false proof presented in part 3 from our colleague, G. Adams. For a connection between this problem and Fibonacci sequences see the article [54], where the author indicates that this “not a picture proof” can be traced back to the year 1868. There are two excellent books on picture proofs by R. B. Nelsen, [75] and [76]. The website by A. Bogomolny [13] contains 84 proofs of Pythagoras’ theorem, many of them with pictures, and some of them with applets.

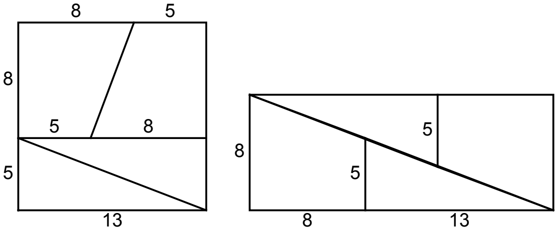

Fig. 29.3 $169 = 13^2 = (8+13)\cdot 8 = 168$

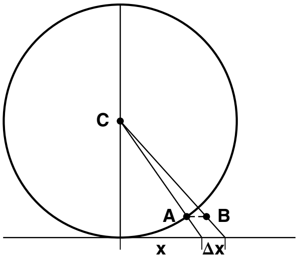

Fig. 29.4 $\int_0^1 \frac{dx}{1+x^2} = \frac{\pi}{4}$

29.2 The Best Number of All (and Some Other Pretty Good Ones)

Introduction

We know that positive integers can be even or odd, they can be prime or composite, and they can be triangular or square. (Each of these terms, with the exception of "square," appears either below or in the index of this book, if you have forgotten the definition.) In this project we'll look at some more things that they may be: the sum of their proper divisors, the product of their proper divisors, or both.

Prerequisites

This exercise requires an understanding of proof techniques (Chapter 5).

Guided Project

Recall that an integer greater than 1 is prime if its only positive divisors are 1 and itself. A positive integer greater than 1 that is not prime is called composite. By a proper divisor, we mean a positive divisor that is not equal to the integer itself. A positive integer is said to be **perfect** if it is the sum of its proper divisors.

1. Show that 6 is a perfect number.
2. Show that 6 is the only perfect number less than 10.
3. Find another perfect number that is less than 30.

By now you should have found the first two perfect numbers. The next is 496.

4. Check that 496 is a perfect number.

5. Find five positive integers, each one being the product of all of its proper divisors.
6. Characterize all positive integers that are the product of their proper divisors.

Now you are almost ready to prove the main theorem in this project. Steps 7–9 below will lead you through the proof.

Theorem 29.1. *There is only one positive integer that is both the product and sum of all its proper positive divisors, and that number is* 6*.*

7. Let p be a prime. Prove that p^3 is not perfect.
8. Prove as many of the following as you need to, until you see the proof of the theorem.
    (a) Prove that the only even number that is both the product and sum of all its proper positive divisors is 6.
    (b) Prove that the only multiple of 3 that is both the product and sum of all its proper positive divisors is 6.
    (c) Prove that there is no multiple of 5 with this property.
    (d) Prove that there is no multiple of 7 with this property.
9. Prove the theorem.

The goal of the next part of this project is to solve the following:

Problem. Let n be an odd positive integer. Find all perfect numbers of the form n^n+1.

It is also possible to find all perfect numbers of the form n^n+1 when n is an even integer—but this is more difficult. The case n odd is already quite difficult, so we will help you by outlining steps you may follow to solve the problem. We also suggest that you use the following theorem, which is due to Euler. (See, for example, [22, pp. 10–11] for a proof of this theorem.)

Theorem 29.2 (Euler). *If N is an even perfect number, then $N = 2^{k-1}(2^k-1)$, where 2^k-1 is prime.*

10. Find an integer a such that $n^n+1=(n+1)a$. (The integer a will be a sum and an expression that involves n.)
11. Prove that $n+1$ and a have no positive common divisor other than 1. (We say that $n+1$ and a are relatively prime.)
12. Assuming that n is odd and n^n+1 is perfect, use Euler's theorem to show that $n+1=2^{k-1}$ for some integer k.
13. Solve the problem.

This was posed as a problem in the *American Mathematical Monthly* [72].

Open-Ended Project

Let p be a polynomial over $\mathbb{Z}$ or $\mathbb{R}$ (see Problem 10.13). What might it mean to say that a polynomial is prime? composite? perfect? square? triangular? While some of these might make sense, others may not. Once you have defined the terms that make sense, are there some interesting theorems you can prove about them?

Notes and Sources

Euclid, in his *Elements*, IX.36, gave the result that if $p = 2^k - 1$ is a prime, then $2^{k-1}p$ is perfect. For $k = 2, 3, 5$, and 7 we note that $2^k - 1$ is prime. Thus we get four perfect numbers, 6, 28, 496, and 8128. The eighth perfect number is already quite large: 2,305,843,008,139,952,128. A good source to begin learning more about numbers is the book [20]. The problem we discussed in the guided portion of this project appears in [15], which we recommend to those wanting to know more about number theory.

29.3 Set Constructions

Introduction

It is amazing how much one is able to build out of almost nothing—and by almost nothing here we mean the empty set. The guided project will lead you through a construction of the natural numbers.

Prerequisites

While the set theory introduced in Chapters 6–9 is sufficient, you may find it helpful to have an understanding of mathematical induction (Chapter 18), which is also introduced in this project.

Guided Project

Let x be a set. Define the successor of x to be the set $x^+ = x \cup \{x\}$.

1. Determine the successors and the successors of the successors of the sets $\emptyset, \{\emptyset\}$, and $\{a, b, c\}$.

We now introduce the following notation. Let $0 = \emptyset$, $1 = 0^+$, $2 = 1^+$, and so on.

2. Write down $0, 1, 2, 3$, and 4 as sets in two different ways; first using the definitions made above, and then using only the symbol $\emptyset$, set brackets, and appropriate set notation.

It may seem intuitively obvious that if we "do this forever," then we will have defined the natural numbers. However, as simple and as attractive as this approach may be, it is not what we call mathematically rigorous. What we need is a statement that explains that we can do this forever. We will take this statement as an axiom, and thus it will not be proved.

Axiom 29.3 (Axiom of infinity). There exists a set containing 0 and containing the successor of each of its elements.

3. Let I be a nonempty set and $\{A_k : k \in I\}$ be an indexed collection of sets. Suppose that for each $k \in I$, the set A_k has the two properties (i) $0 \in A_k$ and (ii) if $x \in A_k$, then $x^+ \in A_k$. Show that the set $\bigcap_{k \in I} A_k$ also has these two properties. We will call a set with these two properties a successor set.
4. The axiom of infinity guarantees the existence of a successor set. So, let A be an arbitrary successor set. Define the set ω_A to be the intersection of all subsets of A that are also successor sets. In symbols we might write

$$\omega_A = \bigcap_{B \in I} B,$$

   where $I = \{B : B \subseteq A,$ and B is a successor set$\}$.
   By part 3, ω_A is a successor set. Show that $\omega_A = \omega_B$ for all successor sets A and B. Perhaps surprisingly, our definition does not depend on our initial choice of successor set, and therefore we will write ω rather than ω_A.
   We call ω the set of natural numbers. Thus far we know that ω is a successor set, and it is the only successor set that is contained in every other successor set.
5. Prove the following statement. Suppose $S \subseteq \omega$ satisfies the two properties

   (i) $0 \in S$, and
   (ii) if $x \in S$, then $x^+ \in S$.

   Show that $S = \omega$. (This is called the principle of mathematical induction and is discussed in Chapter 18.)

6. Prove that $x^+ \neq 0$ for all $x \in \omega$.
7. Consider the set $S = \{x \in \omega : \forall y \in \omega, \text{ if } y \in x, \text{ then } y \subseteq x\}$. Use part 5 to show that $S = \omega$. Conclude that for all u and v in ω, if $u \in v$, then $u \subseteq v$.
8. Use part 7 to prove that if x and y are in ω and $x^+ = y^+$, then $x = y$.

The two defining properties ((i) and (ii)) of a successor set, the principle of mathematical induction, and parts 6 and 8 of this project are known as the five Peano axioms. They are the pillars of the construction of the natural numbers.

Open-Ended Project

We have created new sets from old ones using element relations, union, intersection, power sets, and Cartesian products. Use some (or all) of these to create new sets from the empty set. Do your new sets have some interesting properties?

Notes and Sources

This project is guided by Chapters 11 and 12 of P. Halmos' *Naive Set Theory* [41]. For a brief presentation of the Peano axioms and some other attempts to give the natural numbers a solid foundation see [59, pp. 987–989].

29.4 Rational and Irrational Numbers

Introduction

We know that when we add two rational numbers, the result is a rational number. For this reason, we say that the rationals are *closed under addition*. Similarly, when we multiply two rational numbers, the result is rational. Thus, the rationals are also *closed under multiplication*. In this project, you will investigate the behavior of the rationals and irrationals under other operations.

Prerequisites

This project relies on proofs in cases (Chapter 5), as well as familiarity with rational and irrational numbers. In particular, you will need to use the fact that $\sqrt{2}$ is irrational.

Guided Project

Let a and b be two irrational numbers.

1. Give an example of two irrational numbers a and b such that $a+b$ is irrational.
2. Give an example of two irrational numbers a and b such that $a+b$ is rational.

So the irrational numbers are not closed under addition and certainly are less well behaved than the rational numbers. Now consider two real numbers, a and b.

3. Give an example of two rational numbers a and b such that a^b is rational.
4. Give an example of two rational numbers a and b such that a^b is irrational.

Here's a charming little proof, based entirely upon things that you have proved in this course, that an irrational number raised to an irrational power can be rational.

5. Consider the following.

   Theorem 29.4. *There exist irrational numbers a and b such that a^b is rational.*

   Complete the proof of this theorem, using appropriate choices for a and b and the two cases below:
   Case 1. $\sqrt{2}^{\sqrt{2}}$ is a rational number;
   Case 2. $\sqrt{2}^{\sqrt{2}}$ is an irrational number.

The interesting thing about your proof of Theorem 29.4 is that you don't need to know whether $\sqrt{2}^{\sqrt{2}}$ is rational or irrational!

6. There are many other examples of irrational powers of irrational numbers that are rationals, assuming you know lots of different ways to express irrational numbers. See if you can come up with another example based on the fact that the natural logarithm of 2, denoted $\ln 2$, is irrational. Can you find other examples?

Knowing that an irrational number to an irrational power may be rational raises the question of whether an irrational to an irrational can be irrational. Again, we are looking for a proof that does not use anything more than what we stated in the prerequisites. There are some nonelementary proofs of this, but an elementary proof exists as well [56].

7. Prove the following theorem.

   Theorem 29.5. *There exist irrational numbers a and b such that a^b is irrational.*

   We suggest that you consider using a proof in cases, with $\sqrt{2}^{\sqrt{2}}$ for one of your cases.

Open-Ended Project

Study the behavior of the rationals and irrationals under different operations. Your investigations might deal with specific numbers, or with the rationals and irrationals in general. For example, is $\sqrt{2}+\sqrt{3}$ irrational? In another direction, can you define an operation, $\odot$, such that $a \odot b$ is irrational for all irrational a and b? Think of other questions along these lines and try to answer them.

Notes and Sources

The connection of this problem to Hilbert's seventh problem is discussed in the Spotlight: Hilbert's Seventh Problem at the end of this chapter. The proof that an irrational number to an irrational power can be irrational appears in [56]. These authors attribute the proof of Theorem 29.4 to D. Jarden, [55]. This problem appears as a "fun fact" on the Web at [104].

29.5 Irrationality of e and π

Introduction

The problems in this project require knowledge of calculus. More specifically, you need to know what the number e is, what a geometric series is, and what the series expansion for e is. If you have seen all this, then you probably have also been told that e is an irrational number. The first task of this project is to work through Ivan Niven's proof of this fact. If you have never seen the proof, it's a nice application of series. Everything you need to prove that e is irrational is provided in this project.

The proof that π is irrational, outlined in this project, is also due to I. Niven. In his words, "In the June 1947 issue of the *Bulletin of the A. M. S.*, I gave a one page proof that π is irrational. I had worked on this problem for a specific reason: in the first edition (1938) of what is now a great classic, *Introduction to the Theory of Numbers*, by G. H. Hardy and E. M. Wright, the authors made the observation that 'There is no simple proof of the irrationality of π.' I wondered why this should be so." (See [3] for the full text of Niven's conversation.)

We have provided you with all the steps you need to re-create Niven's one-page proof.

Prerequisites

Since the proofs are by contradiction, you will need to have covered Chapter 5. This project also assumes that you have a basic understanding of infinite series.

For the proof that these numbers are irrational, you will need to recall three results from your calculus course. The first is that, for $-1 < r < 1$, the geometric series satisfies

$$\sum_{n=0}^{\infty} r^n = \frac{1}{1-r}.$$

The second fact is that the series expansion for e^x is

$$e^x = 1 + x/1! + x^2/2! + x^3/3! + \cdots + x^k/k! + \cdots .$$

The last result that you will need is the product rule for differentiation.

Guided Project

1. Prove the following theorem, using the steps outlined below.

   Theorem 29.6. *The number e is irrational.*

   Step 1. Let $k \in \mathbb{Z}^+$. Show that

   $$\frac{1}{(k+1)} + \frac{1}{(k+1)(k+2)} + \frac{1}{(k+1)(k+2)(k+3)} + \cdots \leq \frac{1}{(k+1)} + \frac{1}{(k+1)^2} + \frac{1}{(k+1)^3} + \cdots.$$

   Step 2. Prove that if k is an integer with $k \geq 2$, then

   $$\frac{1}{(k+1)} + \frac{1}{(k+1)(k+2)} + \frac{1}{(k+1)(k+2)(k+3)} + \cdots < 1.$$

   Step 3. Suppose to the contrary that e is rational. Prove that this implies there exists an integer k such that $k!e$ is an integer.
   Step 4. Using the series expansion for e, show that $k!e$ is never an integer. This step should complete the contradiction.
2. Prove the following theorem by contradiction, using the steps below.

   Theorem 29.7. *The number π is irrational.*

   Suppose to the contrary that there are positive integers a and b such that $\pi = a/b$. We will write $f^{(m)}$ for the mth derivative of f.
   For $n \in \mathbb{Z}^+$, define the two polynomials f_n and F_n by

   $$f_n(x) = \frac{x^n(a-bx)^n}{n!} \quad \text{and}$$

   $$F_n(x) = f_n(x) - f_n^{(2)}(x) + f_n^{(4)}(x) - \cdots + (-1)^n f_n^{(2n)}(x).$$

   We will determine a value for n in the fifth step below. Until then, assume that n is a positive integer.
   Step 1. Show that for every positive integer j, all of the following are integers: $f_n(0)$, $f_n(\pi) = f_n(a/b)$, $f_n^{(j)}(0)$, and $f_n^{(j)}(\pi) = f_n^{(j)}(a/b)$.
   Step 2. Prove that $f_n(x)\sin x = \frac{d}{dx}(F_n'(x)\sin x - F_n(x)\cos x)$.
   Step 3. Prove that $\int_0^\pi f_n(x)\sin x\,dx = F_n(\pi) + F_n(0)$.
   Step 4. Find the maximum of the function f_n on the interval $[0,\pi]$. (Note that the maximum depends on n.)
   Step 5. Prove that for n sufficiently large, $\int_0^\pi f_n(x)\sin x\,dx$ is not an integer. This step should complete the contradiction.

Open-Ended Project

Can you prove that e^2 is irrational? What else can you prove is irrational?

Notes and Sources

In 1737, Euler showed that e is irrational. Johann Heinrich Lambert showed, in 1761, that π is irrational. The number π has a very interesting history. For a brief history of π, see [26, p. 100]. For a fuller account, up to about 1971, see [11]. For more recent developments, see [7].

The one-page proof in the *Bulletin of the A.M.S.* that Niven refers to in the quote above can be found in [77]. The reference for Hardy and Wright's text is given in [46]. The conversation with Niven appears in [3].

29.6 A Complex Project

Introduction

In this project, we investigate the complex numbers. In order to say something interesting, we will need to assume several facts—some elementary and some not.

Prerequisites

You will need to use the material on relations in Chapter 10 and order in Chapters 12 and 13. In particular, you must be familiar with the order definitions: Definitions 13.1 and 13.2. We will introduce complex numbers here, and we will not assume that you have already seen them. This project also assumes a basic familiarity with series. If you have taken a calculus course that covered infinite series of functions including e^x, $\sin x$, and $\cos x$, you will have the necessary background in series.

Guided Project

Let's begin by recalling the complex numbers,

$$\mathbb{C} = \{z : z = a + b\mathrm{i}, \text{ where } a, b \in \mathbb{R} \text{ and } \mathrm{i}^2 = -1\}.$$

Complex numbers can be thought of in several ways. When considered as above, it's easy to see how to multiply and add them: For $z, w \in \mathbb{C}$ write $z = a + b\mathrm{i}$ and $w = c + d\mathrm{i}$, where $a, b, c, d \in \mathbb{R}$. Then

$$z + w = (a + b\mathrm{i}) + (c + d\mathrm{i}) = (a + c) + (b + d)\mathrm{i}$$

and

$$z \cdot w = (a + b\mathrm{i})(c + d\mathrm{i}) = (ac - bd) + (ad + bc)\mathrm{i}.$$

Using these definitions and the properties stated in the Appendix on page 363 (Algebraic Properties of $\mathbb{R}$), answer the following questions:

1. Which of the properties A1–A4, M1–M4, and D1 in the Appendix on page 363 apply to the complex numbers with multiplication and division defined as above?

There is another way to think about complex numbers that is quite helpful for computations. For this notation, you should think in polar coordinates. For $z = 0$, for example, we can write

$$0 = 0 + 0\mathrm{i} = 0(\cos\theta + \mathrm{i}\sin\theta),$$

for any choice of a real number θ. For $z \neq 0$, we may write

$$z = a + b\mathrm{i} = r(\cos\theta + \mathrm{i}\sin\theta) \qquad (29.1)$$

where, as you learned when you discussed polar coordinates, $\theta \in \mathbb{R}$ is the measure of the angle from the polar axis to the line joining the origin to the point (a, b). When $\theta > 0$, the measure is taken in the counterclockwise direction (as in Figure 29.5) and when $\theta < 0$ it is taken in the clockwise direction. The nonnegative real number $r = (a^2 + b^2)^{1/2}$ represents the distance of z to the origin. Of course, there are infinitely many choices for θ, for once one choice works $\theta + 2n\pi$ will work for every integer n.

If you haven't done this before, you should practice writing several numbers in both notations. You can check that you have the correct answer using a calculator or computer.

Euler's formula provides another way to write complex numbers. Euler's formula says that for any real number t,

$$e^{\mathrm{i}t} = \cos t + \mathrm{i}\sin t. \qquad (29.2)$$

As a consequence of equations 29.1 and 29.2, we can write every complex number in the form $re^{\mathrm{i}\theta}$, where θ and r are real numbers and $r \geq 0$.

We'll ask you to provide a justification for Euler's formula in a moment. Before proceeding, we provide two exercises to convince you that multiplication and raising complex numbers to high powers is much more pleasant if you use Euler's formula. What we mean is the following: Consider $z = re^{\mathrm{i}\alpha}$ and $w = se^{\mathrm{i}\beta}$. Then

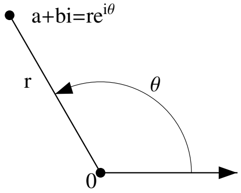

Fig. 29.5 The complex number $a+b\mathrm{i} = re^{\mathrm{i}\theta}$ with $\theta > 0$

$$zw = (re^{\mathrm{i}\alpha})(se^{\mathrm{i}\beta}) = rse^{\mathrm{i}(\alpha+\beta)}. \tag{29.3}$$

2. Multiply $e^{\mathrm{i}\pi/4}$ and $2e^{\mathrm{i}\pi/3}$ by writing the first as $a+b\mathrm{i}$, the second as $c+d\mathrm{i}$, and then performing the multiplication. Then multiply the two numbers using equation (29.3). Finally, show that the two answers are equal. (For the final part of this problem, you may want to use the formulas for $\sin(x+y)$ and $\cos(x+y)$.)
3. Compute $(1+\mathrm{i})^{10000}$ without a calculator. You should write the answer in the form $s^n(a+b\mathrm{i})$, where $s > 0$.

We are not interested in a rigorous proof of Euler's formula here, but we hope to convince you of its validity using facts about series from your calculus classes. So recall that for all real x the following series converge as indicated:

$$e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!}, \ \cos x = \sum_{n=0}^{\infty} \frac{(-1)^n x^{2n}}{(2n)!}, \text{ and } \sin x = \sum_{n=0}^{\infty} \frac{(-1)^n x^{2n+1}}{(2n+1)!}.$$

4. Ignoring issues of convergence in the proofs below, assuming that you may replace x by it in the equations above, and rearranging terms in the series if need be, show that you can obtain Euler's formula: $e^{\mathrm{i}t} = \cos t + \mathrm{i}\sin t$.
   In particular, when $t = \pi$ we have
   $$e^{\mathrm{i}\pi} = \cos\pi + \mathrm{i}\sin\pi,$$
   or
   $$e^{\mathrm{i}\pi} + 1 = 0,$$
   which is sometimes called Euler's equation.
5. Show that $e^{\mathrm{i}\pi/2} = \mathrm{i}$. Using this fact and assuming that exponentiation works as usual, show that i^{i} is real. Once you have completed this part of the project, please read the notes (under Notes and Sources) provided below.
6. Complex numbers are, actually, more complex than real numbers. Our brief discussion of exponentiation has already pointed out one potential problem. There are some very famous "false proofs" involving complex numbers. Here is a proof that $1 = -1$. See if you can figure out where the error is.

Not a proof. Since $(-1)/1 = 1/(-1)$ we may take square roots to obtain the equation $\sqrt{-1/1} = \sqrt{1/-1}$. Thus $\sqrt{-1}/\sqrt{1} = \sqrt{1}/\sqrt{-1}$. So $\mathrm{i} = 1/\mathrm{i}$ and multiplying the equation by i, we get $-1 = 1$. ⍰

We probably all can agree that something is wrong. Find the mistake and write a concise explanation of what the error is.

In the final part of this guided project, we discuss order on the complex numbers. In Chapter 12 we studied some properties of the ordered sets $\mathbb{R}$ and $\mathbb{N}$. For example, we introduced the well-ordering principle of $\mathbb{N}$. Sets, including $\mathbb{N}$ and $\mathbb{R}$, may be ordered in many ways. In this project, we will discuss a specific order on the complex numbers. At this point, you will need to recall Definitions 13.1 and 13.2.

We can define an order on the complex numbers as follows: If $z = a + b\mathrm{i}$ and $w = c + d\mathrm{i}$, we will say that

$$z \preceq w \text{ if } a < c \text{ or we have } a = c \text{ and } b \leq d.$$

Note that if the numbers z and w are real, then $z = a + 0\mathrm{i}$ and $w = c + 0\mathrm{i}$ and this order reduces to the usual one ($\leq$) on $\mathbb{R}$. This order is called the lexicographical order on $\mathbb{C}$ because the order is the same as the one used to order the words in a dictionary.

7. Show that the lexicographical order on $\mathbb{C}$ is a partial order.
8. Show that the lexicographical order on $\mathbb{C}$ is a total order.
9. One important property of $\mathbb{R}$ is the following: If a, b, and c are real numbers with $a \leq b$ and $0 < c$, then $ac \leq bc$. We now investigate this property in $\mathbb{C}$. We have seen that the lexicographical order on $\mathbb{C}$ reduces to the usual less than or equal to relation on $\mathbb{R}$. Writing $u \prec v$ for $u \preceq v$ and $u \neq v$, does the lexicographical order preserve the property above? That is, if $z \preceq w$ and $0 \prec u$, is it always the case that $zu \preceq wu$? Either prove this or give a counterexample.

Open-Ended Project

This part of the project is an exercise in searching journals and/or the Web. There are at least two other “proofs” of Euler’s formula. Do a search until you find the one you feel is simplest. You should have at least three proofs (including the one given here). Explain the one you have decided is simplest, providing as much detail as you can. Summarize the other two and explain why you believe the proof you chose is the “best.”

Notes and Sources

In your proof that i^{i} is real, we told you to use the fact that $e^{\mathrm{i}\pi/2} = \mathrm{i}$. It is also true that $e^{\mathrm{i}5\pi/2} = \mathrm{i}$ and had we suggested you use $e^{\mathrm{i}5\pi/2}$ instead, you would have obtained a different value of i^{i}. That's because exponentiation of complex numbers is more complicated than that of real numbers and it involves a discussion of "multivalued functions" that we will not address here. Instead, we recommend [95] and [74]. We do note, however, that this is like a complex version of Theorem 29.4, which showed that there exist irrational numbers a and b such that a^b is rational.

The equation $e^{\mathrm{i}\pi} + 1 = 0$ is considered one of the most beautiful equations of all time. One reason for this is that it provides a relationship between e, i, π, 1, and 0, which are considered five of the most important constants in mathematics. In fact, readers of *Physics World* were asked in 2004 to vote for their favorite equation and this one came in first, beating out other obvious contenders such as $E = mc^2$. (Admittedly, it tied with Maxwell's equations of electromagnetism.) Nahin, [73], wrote a whole book about what he called "Dr. Euler's Fabulous Formula."

You might wish to conduct a survey of your mathematical friends and teachers to see what they think is the most beautiful equation. It will almost certainly be Euler's equation!

29.7 When Does $f^{-1} = 1/f$?

Introduction

Students often confuse the inverse of f, denoted f^{-1}, with the multiplicative inverse of f, denoted $1/f$. When are these two equal? Surprisingly, although the mistake of assuming $f^{-1} = 1/f$ is common, functions that have this seemingly intuitive property are not common at all.

Prerequisites

This project requires an understanding of functions and their inverses, presented in Chapters 14–16.

Guided Project

In what follows, $f : X \to Y$ will always denote a bijective function between two subsets, X and Y, of $\mathbb{R}$ satisfying $f^{-1} = 1/f$.

1. What can you say about the domain and range of such a function?
2. Find an example of such a function, where the domain of f consists of a single point.
3. Find an example of such a function on a domain consisting of two points.
4. Can such a function f exist on the integers? Why or why not?
5. Show that $(f \circ f)(x) = 1/x$ and $f(1/f(x)) = x$ for all $x \in X$.
6. Show that $f(1/x) = 1/f(x)$ for all $x \in X$.
7. Define a function $g : (\mathbb{R} \setminus \{0\}) \to (\mathbb{R} \setminus \{0\})$ by

$$g(x) = \begin{cases} -x^3, & \text{if } x > 0 \\ -1/(x^{1/3}), & \text{if } x < 0. \end{cases}$$

   Show that g satisfies $g^{-1} = 1/g$ on its domain $\mathbb{R} \setminus \{0\}$.
8. Can you find other examples of such functions?

Open-Ended Project

We mention here some other common errors that occur with functions $f : X \to \mathbb{R}$, where $X \subseteq \mathbb{R}$. Students often confuse the composition $f \circ f$ with the product $f \cdot f$, where $(f \cdot f)(x) = f(x) \cdot f(x)$ for all $x \in X$. What can you say about a function f that satisfies $f \circ f = f \cdot f$?

Yet another problem arises with powers. Which functions $f : X \to \mathbb{R}$ have the property that $f(x^2) = (f(x))^2$ for all $x \in X$?

Notes and Sources

This project is based upon two interesting articles. The first article, [6], has several other interesting questions and problems for students. Some of them require knowledge of continuous functions. The second article, [18], is rather advanced, and it presents much more than we have here. It includes a look at complex-valued functions.

29.8 Pascal's Triangle

Introduction

In this project you will explore an arithmetical triangle that was the object of study by Blaise Pascal in a treatise he wrote in 1654 (though it was known to mathematicians before him). He used this triangle to solve a question posed to him about gambling. You can find out more about the history of this problem from the references at the end of the project.

Prerequisites

This project is appropriate after Chapter 18 on induction has been covered. You should read over Problem 18.25 before you begin.

Guided Project

Pascal's triangle is presented below. Each line has one more entry than the previous line. All entries along the left and right edges of the triangle are one. Every other entry in a line is the sum of the two numbers on the line above that lie to the immediate left and right. The triangle is unbounded below.

$$\begin{array}{ccccccccccccccc}
 & & & & & & & 1 & & & & & & & \\
 & & & & & & 1 & & 1 & & & & & & \\
 & & & & & 1 & & 2 & & 1 & & & & & \\
 & & & & 1 & & 3 & & 3 & & 1 & & & & \\
 & & & 1 & & 4 & & 6 & & 4 & & 1 & & & \\
 & & 1 & & 5 & & 10 & & 10 & & 5 & & 1 & & \\
 & \cdot & & \cdot & & \cdot & & \cdot & & \cdot & & \cdot & & \cdot & \\
\cdot & & \cdot & & \cdot & & \cdot & & \cdot & & \cdot & & \cdot & & \cdot
\end{array}$$

Recall that we defined n factorial and the binomial coefficient $\binom{n}{k}$ in the problems in Chapter 18.

The first few exercises should help familiarize you with Pascal's triangle.

1. Compute each of the following:

$$\binom{6}{0}, \binom{6}{1}, \binom{6}{2}, \binom{6}{3}, \binom{6}{4}, \binom{6}{5}, \text{ and } \binom{6}{6}.$$

2. Solve Problem 18.25 (c) if you haven't already. In other words, prove that for all $k, n \in \mathbb{N}$ with $1 \leq k \leq n$, we get

$$\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}.$$

3. Use the definition of Pascal's triangle given above to show that all entries in Pascal's triangle are binomial coefficients and find a familiar mathematical expression for the kth entry from the left in the nth row. (The first entry from

the left is entry 0 and the first row is row 0.) Use induction to prove that your familiar expression is correct.

4. For each $n \in \mathbb{N}$, consider the statement

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n.$$

   (a) Check this formula for a few small values of n.
   (b) Prove the statement. (You may use Theorem 18.10.)
   (c) Show how you can obtain this sum using Pascal's triangle.

5. For each $n \in \mathbb{Z}^+$, consider the statement

$$\sum_{k=1}^{n} \binom{k}{k-1} = \binom{n+1}{n-1}.$$

   (a) Do something clever for a few n (as you did in 4 (a)).
   (b) Prove the statement.
   (c) Show how you can obtain this sum using Pascal's triangle.

6. How does Pascal's triangle relate to the Binomial Theorem (Theorem 18.10)?

Now you are ready for the main task of this project. Work it carefully. Be as creative, imaginative, clever, and resourceful as possible.

Open-Ended Project

Find a pattern that appears in Pascal's triangle, but that does not already appear in the text. State your formula carefully, and then prove the result. There are many different patterns!

Notes and Sources

Pascal's original article, in Latin with a French translation, appears in [81]. A very readable comprehensive history of Pascal's triangle can be found in [23].

Fig. 29.6 First stage: E_1

Fig. 29.7 Second stage: E_2

29.9 The Cantor Set

Introduction

In this project, you'll learn about the Cantor set—a set that is in some ways very small, and in other ways very big.

Prerequisites

Proofs in this section are by induction. You will need the background provided by Chapter 18, and Chapters 21–23.

Guided Project

1. **(The Cantor Set)** To construct the Cantor set, let $I = [0,1]$.

   (a) (First stage.) We will remove the middle third of this set; that is, we remove the open interval $(1/3, 2/3)$ from $[0,1]$. So two intervals remain. (See Figure 29.6.) Let $E_1 = I \setminus (1/3, 2/3) = [0,1/3] \cup [2/3,1]$. If you were to assign a length to E_1, what length would you assign?

   (b) (Second stage.) Remove the middle open third from each of the two remaining intervals; that is, let $E_2 = E_1 \setminus ((1/9, 2/9) \cup (7/9, 8/9))$. So E_2 is a union of four closed intervals. (See Figure 29.7.) Write E_2 as this union of four closed intervals. If you were to assign a length to E_2, what length would you assign?

   (c) (Third stage.) Remove the middle open third from each of the remaining four intervals. Thus E_3 is a union of eight intervals. (See Figure 29.8.) Write E_3 as a union of these eight closed intervals. If you were to assign a length to E_3, what length would you assign?

   (d) (nth stage.) Now consider E_n, obtained from E_{n-1} by removing the open middle thirds of each of the intervals that compose E_{n-1}. If you

Fig. 29.8 Third stage: E_3

were to assign a length to E_n, what length would you assign? State your guess for the length of E_n in a complete, coherent sentence. Prove that your guess is correct.

The **Cantor set** is the set E defined by $E = \bigcap_{n=1}^{\infty} E_n$.

2. If you were to assign a length to E, what length would you assign? Why?
3. Give examples of numbers that you know are in the Cantor set; that is, give examples of numbers that are in E_n for every n.
4. *Another view of the Cantor set.* There are far more points in the Cantor set than you might think. To see this, it is best to revisit the Cantor set.

   Each point x in the interval $[0,1]$ has something called a ternary expansion. The first digit in the ternary expansion for x, denoted x_1, is found as follows: We divide the interval $[0,1]$ into thirds. If x lies in the first third, $[0,1/3]$, we assign x_1 the value 0. If x lies in the middle third, $[1/3,2/3]$, we assign x_1 the value 1, and if it lies in the last third, $[2/3,1]$, we assign x_1 the value 2. (We note that there is some ambiguity about what happens at the endpoints. When working with the Cantor set (as we discuss below), whenever we have a choice, we will choose either 0 or 2 and not the number 1.)

   We now proceed to the second digit, x_2, in the ternary expansion, which we find as follows: If $x_1 = 0$, then x lies in the interval $[0,1/3]$. Divide this interval into thirds. If x lies in the first third, $[0,1/9]$, we assign x_2 the value 0. If x lies in the middle third, $[1/9,2/9]$, we assign x_2 the value 1. And if x lies in the final third, $[2/9,3/9]$, we assign x_2 the value 2. Similarly, if $x_1 = 1$, then x lies in the interval $[1/3,2/3]$, and we assign x_2 a value of 0 if x lies in the interval $[3/9,4/9]$, a value of 1 if x lies in the interval $[4/9,5/9]$, and a value of 2 if x lies in the interval $[5/9,6/9]$. Finally, if $x_1 = 2$, then x lies in $[2/3,1]$, and we divide this interval into thirds, assigning x_2 the value of $0,1$, or 2.

   For x_3, we use x_1 and x_2 to tell us which interval to look at. We then divide that interval into thirds, and we assign a value of $0,1$, or 2 to x_3. It should be clear that all endpoints will have two possible representations, while all other points will have exactly one representation. Comparing the procedure defined in part 1 of this project, with the procedure we have outlined to find the ternary expansion of x, we see that the Cantor set consists of all points for which there exists a ternary expansion consisting of 0's and 2's. (That's why we never chose the number 1.) Without going into too many details, the ternary expansion really means that

$$x = \sum_{k=1}^{\infty} \frac{x_k}{3^k}, \text{ where } x_k = 0, 1, \text{or } 2.$$

(a) There are two ternary representations for the number $1/3$. What are they?
(b) There are two ternary representations for the number $2/3$. What are they?
(c) Find the first six terms of the sequence associated with $1/4$.
(d) Find the first six terms of the sequence associated with $1/8$.

5. If you have studied series, then you recall that for $-1 < r < 1$, we have the following formula for the sum of the geometric series: $\sum_{k=1}^{\infty} r^k = r/(1-r)$. Using the first six terms of the ternary expansion for $1/4$ that you determined above, guess all the other digits in the expansion. Then sum the series $\sum_{k=1}^{\infty} x_k/3^k$ to show that you have found the representation for $1/4$. Does $1/4$ lie in the Cantor set? What about $1/8$?
6. We have presented the outline of a proof that there is a one-to-one correspondence between points in the Cantor set and sequences of 0's and 2's. Fill in the details, and use this to prove the theorem below.

Theorem 29.8. *The Cantor set is uncountable.*

So the Cantor set has "length" zero, but is an uncountable set. You can learn more about the Cantor set (much more) and the idea of length in the reference given below.

Open-Ended Project

What happens if instead of removing the middle third of the set, you remove the middle fifth? Think about other sets you can create in this way, and say as much as you are able to about them.

Notes and Sources

This topic is discussed in many textbooks. In particular, a summary of many of the interesting properties of this set can be found in [8, pp. 352–354]. For a short article (with a card trick) relating the Cantor set to fractals, see [12, pp. 114–121].

29.10 The Cauchy–Bunyakovsky–Schwarz Inequality

Introduction

In this project you'll prove two inequalities. The second of the two is the triangle inequality in $\mathbb{R}^n$, and the first is used to prove the second.

Prerequisites

What you need for this project depends upon how you prove it. You may need little to no background, other than an understanding of what $\mathbb{R}^n$ is and how you add and subtract in that space.

Guided Project

Consider two points, $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n)$, in $\mathbb{R}^n$. Recall that $x + y = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n)$ and $x \cdot y = x_1y_1 + x_2y_2 + \cdots + x_ny_n$. We'll introduce some notation that will make things neater. We'll write $x \cdot y = \sum_{j=1}^{n} x_jy_j$ and $\|x\| = \sqrt{x_1^2 + x_2^2 + \cdots + x_n^2}$. For $\lambda \in \mathbb{R}$, we write $\lambda x = (\lambda x_1, \lambda x_2, \ldots, \lambda x_n)$.

1. Get used to this notation: Let $x = (0,1,2)$ and $y = (-1,2,3)$ in $\mathbb{R}^3$. What is $x \cdot y$? What is $\|x\|$? $\|y\|$? $x - y$? $x + y$? Make up some examples in $\mathbb{R}^2$ and $\mathbb{R}^4$.
2. Keep getting used to this notation: What is the set $\{x \in \mathbb{R}^2 : \|x\| = 1\}$? What is $\{x \in \mathbb{R}^3 : \|x\| = 1\}$? If you fix $x \in \mathbb{R}^3$, what is $\{y \in \mathbb{R}^3 : \|x - y\| \leq 2\}$?
3. Let $x \in \mathbb{R}^n$ and $\lambda \in \mathbb{R}$. Prove that $\|\lambda x\| = |\lambda|\|x\|$.
4. Let $x, y \in \mathbb{R}^n$. Prove that $(x + y) \cdot (x + y) = \|x + y\|^2$.
5. Let $x, y \in \mathbb{R}^n$. Prove that $(x - y) \cdot (x - y) = \|x\|^2 - 2(x \cdot y) + \|y\|^2$.
6. Let $x, y \in \mathbb{R}^n$. Find a similar formula for $(x + y) \cdot (x + y)$.
7. Suppose x and y are two points in $\mathbb{R}^n$ such that $\|x\| = 1$ and $\|y\| = 1$. Prove that $|x \cdot y| \leq 1$. (Problem 5 above together with the fact that $z \cdot z \geq 0$ for all $z \in \mathbb{R}^n$, should help to point you in the right direction.)
8. Let $x \in \mathbb{R}^n$. Prove that if $x \neq (0,0,\ldots,0)$, then $\|x/\|x\|\| = 1$.
9. Let x and y be two points in $\mathbb{R}^n$. Prove that $|x \cdot y| \leq \|x\| \, \|y\|$. (Problems 7 and 8 should be helpful here.) In many textbooks, this inequality is referred to as the Cauchy–Schwarz inequality; others call it the Cauchy–Bunyakovsky–Schwarz inequality.
10. Use Problems 4 and 9 to prove that for x and y in $\mathbb{R}^n$, the triangle inequality holds; that is, $\|x + y\| \leq \|x\| + \|y\|$.
11. The Cauchy–Bunyakovsky–Schwarz inequality can be used to prove interesting inequalities about real numbers. Use it to prove the following: Let

$a_1, a_2, \dots, a_n$ be real numbers. Then

$$\sum_{j=1}^{n} a_j^2 \geq (\sum_{j=1}^{n} a_j)^2/n.$$

12. Bunyakovsky, Cauchy, and Schwarz all have their names attached to this theorem. Who proved what, and when did they prove it?

Open-Ended Project

For two points x and y in $\mathbb{R}^n$, the **line segment** joining x and y is defined by the set $\{z \in \mathbb{R}^n : z = \lambda x + (1-\lambda)y,$ where $\lambda \in \mathbb{R}$ and $0 \leq \lambda \leq 1\}$. For example, in $\mathbb{R}^2$ choose two points, say $(1,2)$ and $(2,4)$. Then the line segment joining these two points is the set

$$\{(\lambda + 2(1-\lambda), 2\lambda + 4(1-\lambda)), 0 \leq \lambda \leq 1\} = \{(2-\lambda, 4-2\lambda) : 0 \leq \lambda \leq 1\},$$

which is indeed the line segment joining the two points $(1,2)$ and $(2,4)$. Try this out on other points, and in $\mathbb{R}^3$, and then move on to the next definition:

A nonempty set $S \subseteq \mathbb{R}^n$ is said to be **convex** if whenever $x, y \in S$, then the line segment joining x and y is in S. Investigate this definition, considering the following in your investigation. (You'll find the triangle inequality, as well as many of the exercises above, quite handy.)

1. Show that $\{x \in \mathbb{R}^n : \|x\| \leq 1\}$ is convex.
2. Give other examples of convex sets.
3. Is the union of two convex sets convex?
4. Is the intersection of two convex sets convex?
5. Now return to part 2 and see if you can come up with other interesting examples.
6. What are some other interesting questions (and answers) about convex sets?

Notes and Sources

For more information on the Cauchy–Bunyakovsky–Schwarz inequality, see the article by P. Schreiber [96]. There are also other (more clever, less intuitive) ways of proving this inequality.

29.11 Algebraic Numbers

Introduction

A real number is **algebraic** if it is the root of a polynomial

$$p(x) = a_n x^n + \cdots + a_1 x + a_0,$$

where n is a positive integer, $a_0, a_1, \ldots, a_n \in \mathbb{Z}$, and $a_n \neq 0$. A real number is **transcendental** if it is not algebraic.

It's easy to think of examples of algebraic numbers: 0 is algebraic, because it is a (the) root of the polynomial $p(x) = x$; the number $1/2$ is algebraic, because it is a root of the polynomial $q(x) = 2x^2 - x$. It's much more difficult to think of a number that is not algebraic. Why? Well, suppose you have a guess that a certain real number a is transcendental. Then to prove your guess, you must show that for *every* polynomial p with integer coefficients, $p(a) \neq 0$. Before reading on, try to guess whether there are more transcendental numbers or more algebraic numbers.

In an 1874 paper Georg Cantor proved:

Theorem 29.9 (Cantor). *There are countably many algebraic numbers.*

In this project, you will prove this theorem.

Prerequisites

This project requires material up to and including Chapter 23. We mention one additional theorem that you will need and that we have not covered yet, namely Theorem 29.15 stated below. If you work Project 29.12, you will also have a proof of this theorem. For this project, however, you may assume the validity of Theorem 29.15 and apply it to complete the work required here.

Theorem 29.15. *If for each $j \in \mathbb{Z}^+$ the set A_j is countable, then $\bigcup_{j \in \mathbb{Z}^+} A_j$ is countable.*

Guided Project

1. Familiarize yourself with the definition of an algebraic number by answering the next few questions. As you do so, you should also get an idea of what transcendental numbers are like, and you will begin to suspect some of your old numerical friends of being transcendentals.
   Come up with examples of algebraic real numbers that have not been presented in this project. Are some rational numbers algebraic? are all rational numbers algebraic? What about the irrational numbers? How would you

prove that a particular number is algebraic or transcendental? Try to guess which of the following are transcendental numbers: $\sqrt{2}, 5/7, \pi$, and e. (If you think one of these numbers is algebraic, prove it. It's beyond our capabilities, at this time, to prove that the other numbers are transcendental.)

Now you should be ready for the proof of Cantor's theorem. The proof is outlined below.

2. How might you attack the proof of Cantor's theorem? Does it remind you of anything we have done before? What?
3. Solve Problem 5.22, if you haven't already done so.
4. Solve Problem 23.10, if you haven't already done so.
5. Recall that for sets $A_1, A_2, \ldots, A_n$, the Cartesian product of these n sets is

$$A_1 \times A_2 \times \cdots \times A_n = \{(x_1, x_2, \ldots, x_n) : x_j \in A_j\}.$$

Prove the following generalization of Corollary 23.10.

Theorem 29.10. *Let $n \in \mathbb{Z}^+$. If A_i is countable for all $i = 1, 2, \ldots, n$, then $A_1 \times A_2 \times \cdots \times A_n$ is countable.*

6. Let $n \in \mathbb{Z}^+$. Show that the set of polynomials of degree n with integer coefficients is countable.
7. Prove that the set of all polynomials with integer coefficients is countable.
8. Prove that the set of algebraic numbers is countable.
9. Show that there exist transcendental numbers. (Suggestion: Don't try to actually find such a number; just try to show that they exist.)
10. Are the transcendental numbers countable or uncountable? Prove your answer.

You have now seen how the partition of the reals into the algebraic numbers and the transcendental numbers works. It is time to try something on your own.

Open-Ended Project

Define a property $\mathscr{P}$ of real numbers that seems to be of value to you. Let A denote the set of all reals that have property $\mathscr{P}$, and let B denote the set of all reals that do not have property $\mathscr{P}$. Then decide for each of the two sets, A and B, whether the set is countable or not. Prove all your statements. The more creative you are in defining $\mathscr{P}$, the harder it will be to prove the countability or uncountability of your sets. Here's a chance to really show all your mathematical prowess!

Notes and Sources

There is a difference between proving the existence of transcendental numbers, and showing that a particular number is transcendental. As we mention in the Spotlight: Hilbert's Seventh Problem, proofs that the numbers π and e are transcendental were given around the time of Cantor's proof. The original paper by G. Cantor [16] is written in German. A brief summary of Cantor's proof can be found in M. Kline's book [59, pp. 996–997].

29.12 The Axiom of Choice

Introduction

Return, for the moment, to Hilbert's Hotel Infinity discussed in Chapter 21. Suppose that in each room there is exactly one pair of boots. Can you come up with a rule that chooses one boot from each room? To be mathematically precise, we'll introduce the following notation. The set B_j will contain the two boots, and only the two boots, in room j. Then $\mathscr{B} = \{B_j : j \in \mathbb{Z}^+\}$ is the collection of all these sets of boots. Can we find a function $f : \mathscr{B} \to \bigcup_{j \in \mathbb{Z}^+} B_j$ such that $f(B_j) \in B_j$? The answer, as you probably guessed, is "sure, we can do that." For instance, we can define $f(B_j)$ to be the left boot in B_j. The sentence "y is the left boot in the set B_j" is a statement. Thus the substitution axiom on page 365 allows us to obtain the desired function.

Suppose now that the hotel guests have gone out and taken their boots, but they have forgotten their socks. Assume that their socks are identical; that is, you cannot tell the right sock from the left sock. (This is true of most, but not all, socks!) Can we come up with a rule that chooses one sock from each room? We'll let S_j denote the set containing the two socks, and only the two socks, of room j. Then $\mathscr{S} = \{S_j : j \in \mathbb{Z}^+\}$ is the collection of all these sets of socks. The question is then, can we find a function $f : \mathscr{S} \to \bigcup_{j \in \mathbb{Z}^+} S_j$ such that $f(S_j) \in S_j$? This time it's difficult to come up with a solution to this problem; in fact, we don't have a rule available along the lines of the one we had for shoes. Nevertheless, intuitively speaking, it seems as though it should be possible to pick one sock from each pair—at least, most mathematicians think this is intuitive. We'll now introduce an axiom that will allow us to do exactly this.

Axiom 29.11 (Axiom of Choice). Given a nonempty collection $\mathscr{F}$ of nonempty sets, there is a function $f : \mathscr{F} \to \bigcup_{A \in \mathscr{F}} A$ such that $f(A) \in A$.

There are many statements that turn out to be equivalent to the axiom of choice. Some of these statements are major theorems, some are part of set theory, and some are theorems in other fields of mathematics. We'll just mention two of the most important ones in set theory. In order to understand the statements you will need to review Definitions 13.1 and 13.2.

We'll introduce a few more terms before we begin this project. You'll need a firm grasp on these definitions, so work through some examples and nonexamples of each. We start by generalizing Definition 19.3 to arbitrary partially ordered sets. Namely, if X is a set with a partial order $\preceq$ and A is a nonempty subset of X, then we call $a \in X$ an upper bound of A if $x \preceq a$ for all $x \in A$. A chain in a partially ordered set X is a subset C that is totally ordered when the order on X is restricted to C. A least element in a partially ordered set X is an element $m \in X$ such that $m \preceq x$ for all $x \in X$. A maximal element, $M \in X$, is an element with the property that for all $x \in X$, if $M \preceq x$, then $M = x$. Finally, a partially ordered set Y is well-ordered if every nonempty subset A of Y has a least element in A.

Theorem 29.12 (Well-ordering theorem). *Every set can be well-ordered.*

This theorem surely reminds you of the well-ordering principle of $\mathbb{N}$ in Chapter 12. In some ways it is a generalization, as the theorem above applies to any set—not just to the natural numbers. But be careful: the well-ordering theorem does not tell you about a particular order on a set; it just claims that there is an order under which the set is well-ordered. For instance, $\mathbb{R}$ with the usual order (less than or equal to) is not well-ordered. (Why not?) The theorem claims that there is an order under which $\mathbb{R}$ is well-ordered but, unfortunately, it does not give us any hints on how to construct such an order. Looking at it from this perspective, we see that the theorem stated above is not a generalization of the well-ordering principle of $\mathbb{N}$.

It turns out that the following form of the axiom of choice is particularly useful. It is due to Max Zorn, a much-loved mathematician as can be seen from testimonies of his family [114] and colleagues [40].

Lemma 29.13 (Zorn's lemma). *Let X be a partially ordered set such that every chain in X has an upper bound in X. Then X contains a maximal element.*

For a proof of the equivalence of Zorn's lemma, the axiom of choice, and the well-ordering theorem see [41]. A short proof that the axiom of choice implies Zorn's lemma is in [63]. Despite the fact that all three statements are equivalent, people have a better intuition for some of them than for others. The American mathematician Jerry Bona expressed this aptly: "The Axiom of Choice is obviously true, the well-ordering principle obviously false, and who can tell about Zorn's lemma?"

One of our goals in this project is to help you understand the axiom of choice; it will appear frequently in your future mathematics courses. But our main goal in the guided portion of this project is to show that we can find a total order that allows us to compare the cardinalities of every pair of sets from a collection of sets, $\mathscr{A}$.

Prerequisites

This project requires that you have a basic understanding of sets, relations, order, and functions as explained in Chapters 5 through 17. You also need to understand the theory of cardinality as developed in Chapters 22 through 24.

Guided Project

In the introduction to this project we presented you lots of definitions, some old and some new. We need to make sure that you fully understand them before proceeding to the project.

1. Solve (or re-solve) Problems 13.13–13.15.
2. Consider $\mathscr{P}(\mathbb{N})$ with the partial order $\subseteq$. Give an example of an interesting nonempty finite subset of $\mathscr{P}(\mathbb{N})$ that is a chain and an interesting infinite subset of $\mathscr{P}(\mathbb{N})$ that is a chain. Then give an example of a nonempty finite subset of $\mathscr{P}(\mathbb{N})$ that is not a chain and an infinite subset of $\mathscr{P}(\mathbb{N})$ that is not a chain—both sets should be interesting! (We define "interesting" in this problem to mean that the sets are nontrivial, and that the answers to part 3 below are as varied as possible.)
3. Write down the definitions of greatest element and minimal element. Explain the difference between greatest element and maximal element as well as the difference between least element and minimal element. For each of your four sets in part 2, decide whether it has a minimal, maximal, greatest, and least element.

Let $\mathscr{A}$ be a nonempty collection of sets and denote by $E(\mathscr{A})$ the set of all equivalence classes of the relation $\approx$ on $\mathscr{A}$ as defined in Definition 21.1 (and shown to be an equivalence relation in Theorem 21.1). Thus if $E_A \in E(\mathscr{A})$, then two sets A_1 and A_2 in $\mathscr{A}$ are in E_A if and only if there is a bijection between the two sets A_1 and A_2.

For $E_A, E_B \in E(\mathscr{A})$, we will let A' denote a set in E_A and B' denote a set in E_B. We define the relation $\preceq$ on $E(\mathscr{A})$ by $E_A \preceq E_B$ if $|A'| \leq |B'|$ (that is, there is an injective function $f : A' \to B'$).

We aim to establish the theorem below, using the terminology introduced above. This theorem tells us that we can compare the cardinality of any two sets and that this comparison obeys the usual rules of a total order.

Theorem 29.14. *For a nonempty collection $\mathscr{A}$ of sets, the relation $\preceq$ is a total order on $E(\mathscr{A})$.*

4. If you have not yet done so, work Problem 24.4.
5. Prove that the relation $\preceq$ on $E(\mathscr{A})$, as defined above, is well-defined. That is, show that given $E_A, E_B \in E(\mathscr{A})$ we can always find $A' \in E_A$ and $B' \in E_B$ and that the definition of $\preceq$ does not depend on the particular choice of A' and B'.
6. Using the result of part 4, show that $\preceq$ is a partial order on $E(\mathscr{A})$.
7. For two sets A and B we say that f is a partial function from A to B if $f : A' \to B$ for some $A' \subseteq A$. Let $\mathscr{F}$ be the set of all injective partial functions from A to B. We define a relation $\vdash$ on $\mathscr{F}$ as follows: For $f_1 : A_1 \to B$ and $f_2 : A_2 \to B$, partial functions in $\mathscr{F}$,

$$f_1 \vdash f_2 \text{ if } A_1 = \operatorname{dom}(f_1) \subseteq \operatorname{dom}(f_2) = A_2 \text{ and}$$
$$f_1 \text{ is the restriction of } f_2 \text{ to } A_1.$$

Prove that $\vdash$ is a partial order on $\mathscr{F}$.

8. Let A and B be two sets such that $|A| \not\geq |B|$. Prove that $|A| \leq |B|$ using the construction from part 7 of this project and Zorn's lemma.
9. Prove Theorem 29.14.

Now we turn our attention to the following theorem, which is a generalization of Corollary 23.7.

Theorem 29.15. *If for each $j \in \mathbb{Z}^+$ the set A_j is countable, then $\bigcup_{j\in\mathbb{Z}^+} A_j$ is countable.*

10. Prove Theorem 29.15. Note that induction will not work here. We suggest that you adapt the ideas of the alternate proof of Theorem 23.11 outlined in Problem 23.12.
11. Say, explicitly, where you used the axiom of choice in the above proof.

Open-Ended Project

This part is an exercise in the history of mathematics. We will ask you to find resources, summarize your findings, and present them in a coherent and interesting way: Research the history of the axiom of choice. Find variations and give an overview of equivalent forms of the axiom of choice. What does mathematical constructivism think of the axiom of choice? (To answer the last question you will need to find out what mathematical constructivism is!)

Notes and Sources

There are many books that explore the history of the axiom of choice, its implications, and its equivalent forms. Two of them are [48] and [91]. The first part of the guided project is based on [28]. Finally, we note that there are many jokes based on Zorn's lemma and the axiom of choice. Every budding mathematician should know the following, "What is yellow, sour, and equivalent to the axiom of choice?" Answer: "Zorn's lemon."

Mathematicians are funny.

29.13 The RSA Code

Introduction

Though coding theory has always been important, a giant leap forward occurred in the second half of the twentieth century, with the invention of public key cryptography. The main idea (due to W. Diffie and M. Hellman) is the concept of a trapdoor function—a function that has an inverse, but the inverse is very difficult to find. In fact, it should require so long for someone who did not invent the original function to find the inverse that, for all practical purposes, the inverse does not exist. In 1976, R. L. Rivest, A. Shamir, and L. M. Adleman succeeded in finding such a class of functions, and their idea is based upon one of the most elementary ideas in mathematics—multiplication of two numbers. (See the Spotlight: Public and Secret Research in Chapter 28.)

It turns out that if you take two very large numbers and multiply them together, a machine can quickly compute the answer. But, if you give the machine the answer and ask for two factors, the factorization will not appear in a useful amount of time. The public key system, built upon these ideas, is now known as RSA-key (after the three men who created the system). It was described in Chapter 28, but in this project you will learn the details.

Prerequisites

We assume that you worked Chapters 27 and 28 on modular arithmetic and Euler's theorem. In particular, we will refer to the description of the public code that was given at the end of Chapter 28. The notation was introduced in the chapter. You will also need a good calculator; one that is able to determine whether a number is prime, can factor an integer, and can do modular arithmetic. For some parts of this project, you will need to use Mathematica. (If you don't have access to Mathematica, you can skip the parts that require it.)

Guided Project

1. Reread the paragraphs of Chapter 28 following the proof of Euler's theorem.
2. Let's start with a small example to make sure we understand the basics of the code: We choose $p = 13$ and $q = 17$ (so that $n = pq = 13 \cdot 17 = 221$). For the encoding exponent we choose $e = 11$. Verify that $e = 11$ is a feasible choice for the encoding exponent. Use the public key (n, e) to calculate the "secret" value of d. Encode the following three plaintexts:

   (a) $m = 157$;

(b) $m = 97216$;
(c) $m = 91$.

Decode them again to convince yourself that the method works.

3. Note that $\gcd(91, 13 \cdot 17) = 13 \neq 1$, so the hypothesis of Example 28.8 is not satisfied. It turns out that the method still works, even in this case. Let's try to see why it still works—what could go wrong? In this code, we always assume that n is the product of two primes: $n = pq$, where p and q are primes. Thus, the $\gcd(m,n)$ is p, q, or 1. If $\gcd(m,n) = 1$, then Example 28.8 applies. Prove that even if $\gcd(m,n) = p$ (or q), the decoding with exponent d still works:

   Lemma 29.16. *Let $m,n \in \mathbb{Z}$ with $0 < m < n$, $\gcd(m,n) = p$, and $n = pq$ for primes p and q with $p \neq q$. Further, let $e,d \in \mathbb{Z}$ with $ed \equiv 1 \pmod{\phi(n)}$. Then $m^{ed} \equiv m \pmod{n}$.*

   You will need Theorem 28.10 (appearing in the problem section) and Theorem 28.7 for this proof.

4. In practice, n must be chosen to be quite large—certainly larger than 10. Nevertheless, it may still be the case that the plaintext m may satisfy $m \geq n$. Recall that if $m \geq n$, then we have to break the integer m into parts. Here's how to do this: Choose positive integers $m_1, m_2, \ldots, m_k$ such that $m_i < n$ for $1 \leq i \leq k$ and $m = m_1|m_2|\ldots|m_k$, where the last expression denotes simple lining up of the integers in the decimal notation for m. (For example, if $m = 15208$ and $n = 77$, we can take $m_1 = 15$, $m_2 = 20$, and $m_3 = 8$. Then $m = 15|20|8$.) We will then denote the (chopped up) plaintext as $(m_1, m_2, \ldots, m_k)$ and the ciphertext as $(m_1^e \pmod{n}, m_2^e \pmod{n}, \ldots, m_k^e \pmod{n})$.
   Now you are ready for the problem: Suppose you are given the public key, $n = 2881$ and $e = 47$. The intercepted message contains the criminal's hair color. However, the message is encoded according to the rules we described in the previous paragraph. The ciphertext reads $(2574, 1120, 166, 742)$ (all integers $\pmod{2881}$). The translation from letters to integers is done by converting $a \to 01, b \to 02, \ldots, z \to 26$. Crack the code to find out the criminal's hair color.

5. If you cracked the message in the previous part, then it is obvious that this encryption is not safe. That's because the function we used in that part of the problem is not really a trapdoor function. However, it will become one if we choose our primes large enough. The bigger the primes, the harder it is to factor n (a task believed to be necessary to break the code). To get a feeling for the unequal amount of time it takes to find primes and multiply versus factoring, do the following on your calculator.

   (a) By trial and error using the calculator's prime check, find two primes of ten digits each. (Primality testing is also an interesting and important subject. Your calculator uses sophisticated algorithms to check whether an integer is prime.)
   (b) Multiply the two integers together. (Notice how quickly your calculator can do that!)

(c) Now use the factor command to factor the number you obtained into its two primes. How long did it take?

6. To do safe encoding with the RSA method you need huge primes. Currently the recommendation is to use primes of 300 decimal digits each. If you have access to Mathematica, download the notebook RSA-Notebook.nb from the site given below. Explore this package and use it to communicate with a classmate, creating public keys and sending messages to each other.
http://library.wolfram.com/infocenter/MathSource/1966/

Open-Ended Project

Either create a code of your own, or find a code from another book. Try your code out on a partner, compare it to RSA, and discuss the strengths and weaknesses of your code.

Notes and Sources

The original paper by R.L. Rivest, A. Shamir, and L.M. Adleman appears in [88]. A more detailed treatment can be found in the general number theory text book by K. H. Rosen [89, Chapter 8]. See [90] for the commercial site of RSA Security Inc., a company founded by Rivest, Shamir, and Adleman.

To learn about primality testing, you can start with the *Mathematics Magazine* article [70] that gives a historical treatment of the subject up to the use of computers. A comprehensive treatment at the undergraduate level is contained in the text by Bressoud [14]. Also, a recent breakthrough is presented in the more advanced paper [1].

Spotlight: Hilbert's Seventh Problem

In 1900, David Hilbert presented a speech in Paris entitled "Mathematische Probleme" to the International Congress of Mathematicians. His aim was to look at the future of mathematics. His speech began with a description of what makes a problem significant. This introduction is followed by the statement and discussion of 23 problems. His speech appeared in 1900 in the *Nachrichten* of the Göttingen Scientific Society (more precisely, in *Nachrichten von der Königlichen Gesellschaft der Wissenschaften zu Göttingen)*. It was translated into English, and published in 1902 in the *Bulletin of the American Mathematical Society.*

Information about the time leading up to and following the presentation can be found in C. Reid's biography *Hilbert* [86]. We present the English translation of the seventh problem below. Even today, it's exciting to hold a copy of this speech in your hands.

(You can find a definition of algebraic and transcendental numbers in Project 29.11.)

> Hermite's arithmetical theorems on the exponential function and their extension by Lindemann are certain of the admiration of all generations of mathematicians. Thus the task at once presents itself to penetrate further along the path here entered, as A. Hurwitz has already done in two interesting papers,[1] "Ueber arithmetische Eigenschaften gewisser transzendenter Funktionen." I should like, therefore, to sketch a class of problems which, in my opinion, should be attacked as here next in order. That certain special transcendental functions, important in analysis, take algebraic values for certain algebraic arguments, seems to us particularly remarkable and worthy of thorough investigation. Indeed, we expect transcendental functions to assume, in general, transcendental values for even algebraic arguments; and, although it is well known that there exist integral transcendental functions which even have rational values for all algebraic arguments, we shall still consider it highly probable that the exponential function $e^{\mathrm{i}\pi z}$, for example, which evidently has algebraic values for all rational arguments z, will on the other hand always take transcendental values for irrational algebraic values of the argument z. We can also give this statement a geometrical form, as follows:
>
> *If, in an isosceles triangle, the ratio of the base angle to the angle at the vertex be algebraic but not rational, the ratio between base and side is always transcendental.*
>
> In spite of the simplicity of this statement and of its similarity to the problems solved by Hermite and Lindemann, I consider the proof of this theorem very difficult; as also the proof that
>
> *The expression α^{β}, for an algebraic base α and an irrational algebraic exponent β, e. g., the number $2^{\sqrt{2}}$ or $e^{\pi} = \mathrm{i}^{-2\mathrm{i}}$, always represents a transcendental or at least an irrational number.*
>
> It is certain that the solution of these and similar problems must lead us to entirely new methods and to a new insight into the nature of special irrational and transcendental numbers. [51, pp. 455–456].

Hilbert mentions Charles Hermite, who proved in 1873 that e is transcendental, and Ferdinand Lindemann, who proved in 1882 that π is transcendental [26, p. 466]. The answer to Hilbert's question was published in 1934 by Aleksandr O. Gelfond, and (independently) by Theodor Schneider in 1935. It follows from the Gelfond–Schneider theorem that $\sqrt{2}^{\sqrt{2}}$ is irrational (see Project 29.4), but there's an easier example. You can find this easier solution at [104].

Hilbert's original address can be found in [50]. The full text of the English translation is available on the Web, [51]. See also [59, Chapter 25, sec. 1] and [59, p. 980]. For another view of Hilbert's problems read [36], and for a recent book on this topic see [37].

In honor of the 100-year anniversary of Hilbert's Paris address, the new century, and the new millenium, several mathematicians were asked to pose problems for the next century. Steve Smale proposed 18 problems for your century that you can

[1] *Math. Ann.*, vols. 22, 32 (1883, 1888).

find in [100]. The article [39] by Phillip Griffiths also contains a look at challenges for the future. The Clay Mathematics Institute of Cambridge, Massachusetts (CMI) selected seven problems for the new millenium. They also offer a reward of one million dollars per problem, and consequently have received a fair amount of publicity. More information about the Institute and the problems can be found on their website, [19], as well as in [21].