Undergraduate Texts in Mathematics
Readings in Mathematics

UTM

Kenneth Ireland
Al Cuoco

Excursions in Number Theory, Algebra, and Analysis

Springer

Undergraduate Texts in Mathematics

Undergraduate Texts in Mathematics

Readings in Mathematics

Undergraduate Texts in Mathematics are generally aimed at third- and fourth-year undergraduate mathematics students at North American universities. These texts strive to provide students and teachers with new perspectives and novel approaches. The books include motivation that guides the reader to an appreciation of interrelations among different aspects of the subject. They feature examples that illustrate key concepts as well as exercises that strengthen understanding.

Kenneth Ireland · Al Cuoco

Excursions in Number Theory, Algebra, and Analysis

Springer

Kenneth Ireland
(deceased)
Fredericton, NB, Canada

Al Cuoco
Education Development Center
Waltham, MA, USA

ISSN 0172-6056 ISSN 2197-5604 (electronic)
Undergraduate Texts in Mathematics
ISSN 2945-5839 ISSN 2945-5847 (electronic)
Readings in Mathematics
ISBN 978-3-031-13016-8 ISBN 978-3-031-13017-5 (eBook)
https://doi.org/10.1007/978-3-031-13017-5

Mathematics Subject Classification: 11Axx, 11Dxx, 11Mxx, 11Nxx, 26Axx, 26Bxx, 26Cxx, 12Fxx, 00Axx, 01Axx, 11Cxx, 11Jxx, 11Lxx, 20Bxx, 20Dxx, 30xx

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Micky: Ancora una volta, tutto quello che faccio, lo faccio per te.

Preface

History

In 1972, I took a summer course from the late Ken Ireland at Bowdoin College. I was a new high-school teacher attending a four-summer NSF institute leading to a master's degree. For close to fifty years, I had wanted to create a book for mathematics majors based on Ken's course, his typed notes, and the accompanying experience of learning from his lectures and discussions during his office hours. Now I have done so, and you are holding it in your hands or reading it on a computer monitor. I had three reasons for writing this book:

(i) As a capstone course for majors, it ties together much of undergraduate mathematics in ways that situate topics in the history of the subject and that make connections to major themes in the discipline. It is not that the mathematical topics have direct connections to the content of any particular course (although many do); rather, they provide valuable background that can be used to place that content in the broad landscape of mathematics as a scientific discipline. One of Ken's premises was that there are dozens of famous mathematical results that are part of the "folklore" of many of the courses that undergraduates take. Some of those results go back to the Greeks. Some come from arithmetic, number theory, and analysis, and some involve classical algebra. His course developed the mathematics needed to prove a large collection of these results.

For example, the fact that π is irrational is part of the folklore of precollege mathematics—often stated but never proved. So too with the fundamental theorem of algebra.

(ii) Most "content courses" for undergraduates use a classical structure and pedagogy; general results are developed with proofs, and then the results are applied to several concrete situations. This is a wonderfully efficient and elegant structure for presenting established results, but it misses some of the messiness and false starts that are so typical of doing (as opposed to learning) mathematics. Ken's style was much less formal; it was based much more on filling in details and background for problem sets that provide practice with technique, to be sure, but also preview ideas that might not get nailed down until later in one's mathematical career. This kind of immersion in doing mathematics has been one of the inspirations for my teaching and for the approach that my colleagues and I take to professional development for practicing teachers. The other is my collaboration with Glenn Stevens in Boston University's PROMYS for teachers, also organized around experience before formality. I have seen how an immersion experience in mathematics is a jump start for many people, helping them develop the

disposition and habits needed to make sense both of more traditionally organized courses and of mathematics in practice.

(iii) In addition to a dive into classical content, this book gives students a real sense of mathematical culture—its history, its norms, and even its humor. The book is full of anecdotes about mathematicians, examples of milestones in the history of mathematics, and stories about life as a mathematician. Ken was a master at this, a consummate mathematician who loved to tell stories and make jokes. "Problem 17 is left out due to lack of space." "Hint for Problem 23: See Problem 17." My experience is that this kind of playfulness draws people into the culture. It certainly had that effect on me.

Some will look at the book and say that it has holes. And indeed it does, but that, too, is on purpose. It makes assumptions about what the reader knows (a little field theory, for example). Although I have triaged some of these, I think leaving things to the reader is important, because having to act on insufficient information reflects reality. We routinely face problems that arrive without having asked us what chapter we just read. I have included citations that help students look up material for themselves.

The book is aimed at students who have the equivalent of the first two or three years of undergraduate mathematics, but it would work for students with less background if they have the disposition and drive to fill in some gaps. Instructors may need to (re)introduce some common notation—$\mathbb{Z}$, $\mathbb{Q}$, and so on.

The Ireland course had a huge influence on my teaching and career, and this book is my attempt to preserve his work and share it with others. I hope that it will help students and readers bind together undergraduate studies and give them a big-picture view of the landscape they want to tour with their own students or in their future mathematical work.

—Al Cuoco

From Ken's Original Preface

These notes represent a series of thirty lectures delivered to an enthusiastic and capable audience of sixty-four secondary school teachers. The purpose of the course was to acquaint the student with several mathematical structures, their interrelationship and fundamental properties. At the same time, technique was developed through exercises. As the lectures proceeded, two hundred exercises were distributed so that the students could acquire manipulative skills and encounter the limitations in actual practice of general theory. The exercises cover special cases of Galois theory, Fourier series, field theory, symmetric functions, modular arithmetic, and so forth. Discussion resulting from the problems generated supplements, expanded chapters, and a deeper study of certain concepts.

The fundamental theorem of algebra was examined from several points of view, and its algebraic-analytic aspect thoroughly discussed. An interest in

numbers not algebraic over the rationals led to a chapter on irrational and transcendental numbers.

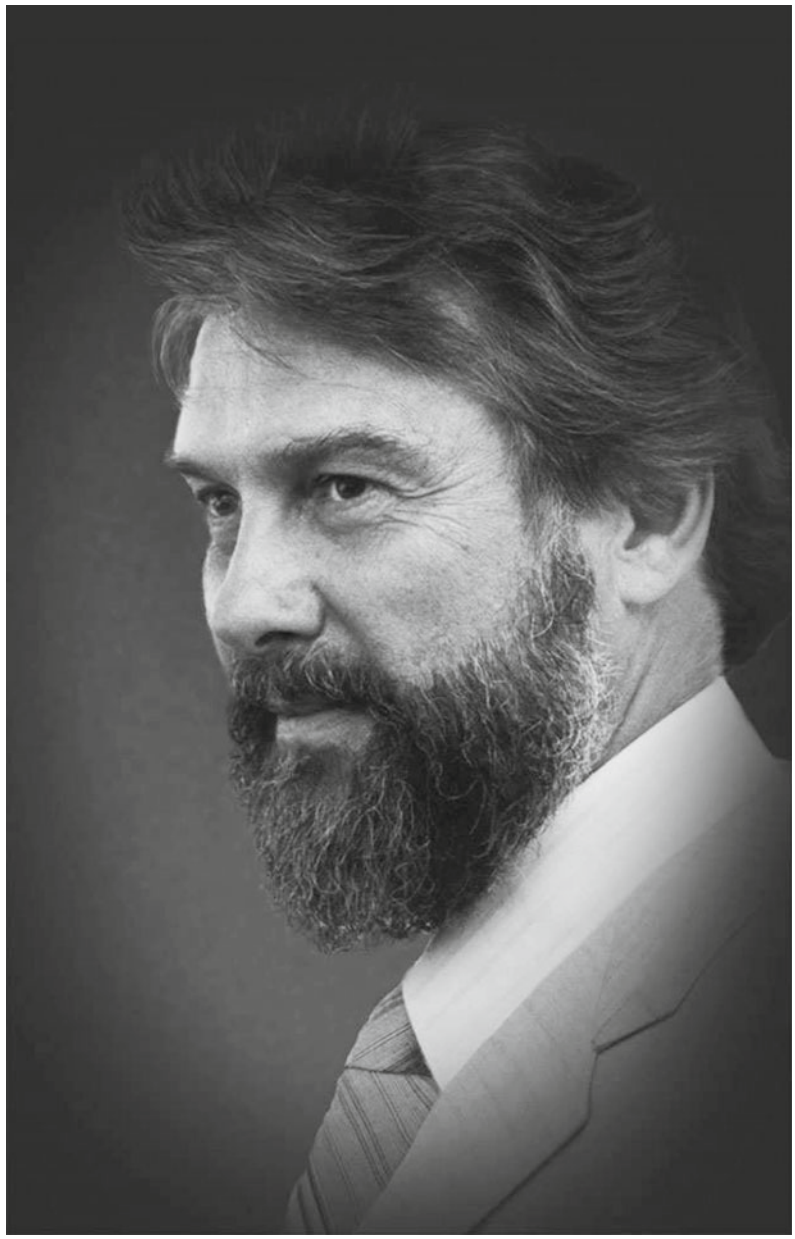
The use of orbits in elementary group theory shows, beyond a doubt, that reasonably sophisticated results can be obtained with very little effort. The Sylow theorem on existence of subgroups in a group, while appearing here at the end of Chapter 2, was proved toward the end of the course, as a result of interest generated by the problems. The underlying theme of Galois theory sprinkled through the lectures and exercises would have led to a proof of the fundamental theorem, had time permitted.

The analytic portion of the lectures entered with the fundamental theorem of algebra and continued with an elementary treatment of classical Fourier series. After a tedious proof of the transcendence of π, it was refreshing to find simple regular expressions for this number arising from trigonometric expansions of simple functions. A sophisticated link with Chapter 2, on pentagons and modular arithmetic, is achieved by the evaluation of the classical Gauss sum, a sum of roots of unity appearing in the construction of regular polygons. The central result in the Fourier series chapter is the simple proof of convergence due to Dirichlet. The simplicity of this result is often obscured in texts that develop the theory more extensively or are primarily concerned with physical applications.

The constant interplay between basic concepts and the frequent capturing of substantial results, along with the wonderful cooperation and enthusiasm of the members, of course, made the adventure a great pleasure for me.

I wish to thank Bowdoin College and NSF for giving me the opportunity to work with the participants of the program. Special thanks also to Nancy MacDonald, who did a fantastic job of keeping abreast of the daily ream of lecture notes.

—Kenneth Ireland
August, 1972



Ken Ireland, 1937–1991

Using This Book

For Readers

This is not your grandmother's mathematics book. Rather than a "dogmatic exposition of an established theory" [9], think of this book as a guided tour of some major themes in modern mathematics. It is based on a course given by Ken Ireland in 1972, so a great deal has happened since then. Most notably, the celebrated Fermat conjecture (that there are no triples (a, b, c) of positive integers such that $a^n + b^n = c^n$ for $n > 2$ is now a theorem, established in the 1990s. And the use of computational technology (including computer algebra), now a mainstay of mathematics research, was in its infancy in the 1970s. So I have added sections that address these and other advancements, but I have tried to stay faithful to the playful and parsimonious style of Ken's original notes—typescript and handwritten notes that I have hung onto all these years.

The book begins with a chapter called "Dialing In Problems." It contains eight problem sets, each designed to help you "dial in" to several mathematical structures and theories. I can't stress the following enough:

> *These problems make up the heart of what you'll learn from this book.*
> *The chapters exist to support your work on the Dialing In problems.*

The sets are split into smaller numbered sections, each one prefaced with a note about the main themes developed in that set. Each set also contains problems that deepen earlier results and methods and preview upcoming ideas, often with special cases of theorems that will be proved later in more generality. The purpose of this setup is to develop interconnections—for example, connections between algebra and geometry or between analysis and arithmetic.

If you are using the book as a text for a course, your instructor will have more to say about how the Dialing In problems are be assigned and used. Here's my advice (from someone who has lived with these problems and used them with students for decades) about how they can be most useful:

> Look over each set before you dig in. Look for problems that look familiar and try them. And make a mental or real list of the problems that make no sense (because of either vocabulary or notation). If a problem makes you wonder or scratch your head, that's good. The Dialing Ins are meant to be tried and tried again. Feel free to skip around and to revisit a problem after you have given it some time to percolate.

While each section contains a mix of problems, each of them can be supported by chapters in the book:

- Set 1 is a tour of some ideas that are developed in Chapter 2, a chapter that introduces some of the main structures and themes developed in the book—complex numbers, finite fields, group theory, and number theory.

- Set 2 is supported by the ideas in Chapter 3, a chapter that develops unique factorization in $\mathbb{Z}$ and introduces formal Dirichlet series as a tool to investigate questions in arithmetic.
- Set 3 deepens some of the ideas and methods in Chapter 3 and develops some concrete experience with the algebraic tools that are used in Chapter 4. If you like to calculate in old-fashioned algebra (as I do), this set is for you.
- Set 4 offers more classical algebra, including a heavy dose of what was once called the theory of equations—expressing the roots of a polynomial equation as expressions in its coefficients. Chapter 4 provides support.
- Set 5 revisits and deepens some algebraic and arithmetic ideas and results from the previous chapters—field theory, group theory, polynomial algebra, and arithmetic. It previews some ideas that will come up in Chapter 5 around irrational real numbers.
- Set 6 introduces in earnest the analytic themes of the book (there are previews before this). Use Chapter 5 as a resource. In this chapter, you will study the proofs of the irrationality and transcendence of some classical constants that show up in precollege mathematics (such as π and e). In this set, you will see some of the ideas that motivate the proofs in Chapter 5, but you will also revisit some old friends from the previous chapters.
- Sets 7 and 8, the last two Dialing Ins, cover a wide swath of beautiful mathematics, folding Fourier series into the mix of algebra, number theory, and analysis, with lots of trigonometry and beautiful series calculations for added measure. Use the last two chapters of the book as a resource.

After you have worked through a chapter or two, look back at the Dialing Ins. Just think about what you have learned. It will make you smile.

There are also exercises at the end of most sections. These are closely tied to the sections themselves, and they provide practice and extensions of some of the ideas introduced in the section. Some of them are previewed in the Dialing In sets.

In addition to the Supplement sections that Ken mentions in his introduction, there are also sections labeled Lookout Point and Take It Further. These are digressions into related topics or deeper dives into the ideas presented in the chapter. Many of them are accompanied by citations to other works. They can often be skipped, but doing so would be a shame.

Of course, you can use, this material in any way you like, but the preferred sequence is *try, study, try again*.

The main point I want to make is that this book is an invitation to *do* mathematics. Yes, you'll learn about many results and develop many techniques, all curated by a brilliant mathematician (Ken, not me) and teacher. But what is more important is that you will experience the thrill of your own mathematical thinking.

About prerequisites: I want to say that there are none, except for the drive and stamina needed to work on hard problems and ideas. More realistically, the formal prerequisites for this book are standard courses in abstract algebra and real analysis. However, readers without these courses, do not despair!

The process of learning mathematics need not always be linear; with a spirit of inquiry and some extra reading, the background material can be acquired as you go along. If you come across a term or result that you haven't encountered before (or perhaps you have, but it didn't stick), *look it up*. Internet searches of the kind we have now didn't exist when I started teaching, but now they are ubiquitous. (*Warning*: The quality of search results varies wildly.) Keith Conrad's website [12] is a wonderful resource, beautifully written and thorough. There are others, and if you are using this for a text or resource in a course, your instructor will surely have a stash of good references. As for published books, most of what is needed here is developed in [19, 41, 53, 70].

And by the way, many of the citations used in the chapters refer to other books, some very old. If you don't have ready access to some of these, you can use the good old internet.

And finally, spending as much time as you can working on the Dialing In problems, looking up terms or results when they do not make sense, will enhance your enjoyment and understanding of the expository parts of the text.

The Epilogue (which follows Chapter 6) will say more about this interplay between "doing and studying."

I'll bet that a great deal of this preface makes little sense right now. Think of it as a kind of Dialing In. After you have worked through a couple of chapters, come back and try again.

For Instructors

The advice in the section above was for readers of the book. But for instructors who are thinking about using it as a text or resource for a course, a piece of that advice still holds: this is not your grandmother's mathematics text.

A note on notation: to avoid a digression into the meaning of $\mathbb{Z}/p\mathbb{Z}$, $\mathbb{Z}_p$ stands for the field with a prime number, p, of elements, identified as the field of integers modulo p, even though it often stands for the p-adic integers. I hope this doesn't irritate anyone.

A central feature of the design is the Dialing In problem sets. They are based on problem sets that were handed out in waves during the original course, roughly one set (15–20 problems) each day or two. They contained reviews, previews, and études. Like the celebrated Ross–PROMYS [81] and PCMI [82] problem sets, students should not (and will not) be able to complete all of the problems when they are first introduced. So to distinguish them from the section-specific Exercises, I have numbered them consecutively, 1–200, and placed them in the first chapter, sectioned off, with advice about how to use them. Each Dialing In problem is a kind of open invitation to explore an idea or a connection among ideas. Students will get the most out of the book if they spend most of their time Dialing In before ideas are elaborated in lecture, and of course afterward as well. Indeed, in the original course, lectures were often inspired by ideas that arose from students' attempts to approach this or that problem. It would be fun for you and your students to build an occasional lecture that is a riff on what students have done in the Dialing In sets.

Dialing In supports an approach to learning mathematics that my colleagues and I call *experience before formality*. In the last decade, this design principle has gained traction among instructors at all levels. It goes by several names these days, each a variation on the theme of active learning, inquiry-based learning, exposure before closure, and many others. Teachers at all levels who have taught in this way cite many benefits; one of the most

Even the "flipped classroom" model can be made to fit into this genre.

salient is that students retain what they learn and use it in ways that are faithful to how mathematics is done.

The Ireland course was decades ahead of its time in this regard, and I still remember how unsettling it was for many teachers in the class ("why doesn't he just tell us how to do it?"). Working intensely on problems in tandem with learning from lectures and explanations has had a profound effect on my own approach to teaching and learning. And I am convinced that before grad school, all of the mathematics I really understood (rather than simply learned) had its roots in the experience before formality structure of Ken's course.

If cuts have to be made, consider the fact that although algebra, analysis, and number theory rear their heads throughout, the front half of the book is more algebra than analysis, and then things switch in Chapter 4.

This book is based on an intense residential course for practicing high-school teachers that ran for six weeks, two hours a day, five days a week. That model is perfect for this material, but what about the more realistic situations faced by most faculty? Here are some thoughts, gathered from my experience and that of colleagues.

(i) Many states now require that teachers enroll in a content-based master's program early in their careers. The NSF teacher institutes in the 1960s and 70s were also aimed at early-career teachers. This material would fit perfectly with such programs, as a full course or as selections curated from the text (see item iv below for examples of curations).

Many of the alumni of those NSF institutes (including the Bowdoin program) contributed to the directions that high-school mathematics took throughout the last century.

(ii) For all the reasons listed in the preface, this material would make a great capstone course for mathematics majors. But don't be fooled by the fact that this is a thin book. It covers a wide swath of modern mathematics, and it treats it in depth with a minimum of pedantry. If students really dig into the problems as they learn the material, the book can easily fill a semester. For example, a semester course that meets twice a week for 80-minute sessions might go like this:

- Weekend homework is the Dialing In for the upcoming week.
- Tuesday: class begins with table/small group discussions of Dialing In problems (15–20 minutes). Then
  - 20–25 minutes of lecture
  - 30 minutes of work on the Exercises specific to that section
  - 10 minutes of reflection and presenting
- Homework for Thursday: work on the remaining Exercises and Dialing In problems.
- Repeat

For 50-minute classes, some days could be mostly student work and some could be mostly lecture.

This structure can be easily adapted to a flipped classroom by switching out the lecture for a preclass video.

(iii) Selections from the book are ideal fodder for seminars for advanced students. A good example is Chapter 4, which offers different takes on the fundamental theorem of algebra. Especially for preservice teachers, this is a valuable piece of background for talking about historical developments and different approaches. The fundamental theorem of algebra lives in the folklore of high school, and without an

Chapter 5 is another good choice for this audience, but it may be a little steep for students without solid algebra and analysis backgrounds.

understanding of the essential "analytic step," it is all too easy (as some books do) to fall into the trap of Exercise 4.12.

(iv) Sections of the book could enhance a number of standard undergraduate courses:

- Sections 2.1–2.3 and 3.1–3.4 fit nicely into an elementary number theory course.
- Sections 2.3–2.6 and 3.1–3.3 make ideal units for a first abstract algebra course.
- Sections 5.1–5.5 make a good basis for an extended project in an analysis course.

These are just examples of how the book can be used as a flexible resource for many undergraduate courses. My hope is that however you use these materials, you will find in them ways to fuel your imagination and that of your students.

And the Dialing In sets are a well-crafted store of problems that will fit in a wide variety of settings.

Acknowledgments

Early on, Michael Rosen (of Ireland–Rosen fame [41]) encouraged me to take on this project, which had been percolating in my head for over four decades, and he put me in touch with Ken's widow, Noel, and daughter Linda. This turned out to be a joyous bonus to all the joy I had experienced while writing this book. I learned so much about the Ireland family from them—stories that gave me deeper insight and appreciation for Ken, his mathematics, his teaching, and his approach to life. I looked forward to our phone calls and emails and always felt energized after we talked.

I keep lobbying the Irelands to publish some of their stories in some way. They would be a real inspiration to the next generation of mathematics teachers at all levels.

Jim Newton was in Ireland's course with me in 1972. Jim and I were novice high-school teachers, each with a couple years' experience under our belts. We spent many afternoons and nights puzzling over the "exercises" from the course. What's more important is that our two families became close friends, attending each other's children's weddings and getting together a couple of times a year in Baltimore or Boston or Maine. Jim has been a source of constant encouragement during the writing of this book, even when he was reminded of the nervousness he felt as an undergraduate when he had to present the proof that e is transcendental to his algebra class at Towson.

Our daughter Alicia was less than a year old when we packed up our 1970 VW and headed for Bowdoin.

My family—Micky, Alicia, Scott, and Atticus—have been cheerleading this effort all the way. Every family dinner would start out with one of them asking, "How's the book coming?" (I think they were skeptical that I could pull it off.) My wife, Micky, and I relived so many stories about the Bowdoin experience—hot dogs (and demonstrations) on the common, high chairs in the cafeteria, Jon Lubin's lessons on how to eat a lobster, life in the dorm, and our parents driving up for a cookout behind Coleman hall.

Loretta Bartolini is so much more than the editor for this project. She helped shape the essence of this book with what I consider brilliant ideas about communication, design, and content. Designing the structure of the book was a heavy lift—it's not a typical mathematics text—and I can't thank

The Lookout Point design element (see page 17 for the first of these) was Loretta's idea.

Loretta enough for her insight into how we could make this usable while preserving its core organizing principle that asks students to try things before they are formally introduced.

Loretta introduced me to David Kramer, and this was another source of unexpected good luck for me as the project came to a close. David is one of those people who do not fit into any of the standard categories. He is, at once, a mathematician (number theory, of course), a talented writer (with a wonderful sense of style), a proofreader (with an amazing eye for detail), an editor (with an ear for clarity and precision), a translator (see, for example, [6]), and so much more. If you could compare my penultimate draft of this book with what it became after David did his work, you would see what I mean.

Paul and I talk at least once a week, and he's been the perfect sounding board for many of the ideas in the book.

My colleagues and friends Paul Goldenberg and Sarah Sword were always there with just the right suggestions and comments. Examples: Sarah suggested the sample semester schedule on page xviii; Paul showed me ways to make some of the Dialing In problems less intimidating, and he was the main source of expertise when it came to revising the graphics, some of which were hand drawn in Ken's original notes. Throughout, they read drafts and made everything they touched much better.

John Ewing read the entire set of typescript notes that Ken produced for the course. John saw what I saw and almost insisted that I get this project underway. John knows exactly the kinds of teachers that this material will excite.

The team at SPi Global created the TEX source from the original typewritten notes created by Nancy MacDonald in 1972. The folks at SPi were extremely patient with me. And Yongyuan Huang, a brilliant undergraduate at Boston University, helped me navigate the vagaries and potholes involved in BIBTEX.

And as always, none of this work would have been possible without the love and support of my dear Micky.

Kenneth Ireland
Al Cuoco

Recollections from Colleagues and Friends

From Michael Rosen

I began my career as an instructor of mathematics at Brown University in September 1962. Ken came to Brown as an assistant professor a few years later. Soon after his arrival on campus, we became friends, partly because we had many interests in common, e.g., number theory, algebraic geometry, literature, poetry, and classical music.

For a while we shared an office. I soon discovered that Ken was a fascinating individual with a keen intellect, a wonderful dry sense of humor, and a zest for life. I found Ken to be one of the most engaging and interesting people I would ever know.

He came to Brown after receiving his Ph.D. degree from Johns Hopkins University under the direction of Bernard Dwork. He spent a year or two at Brandeis University before coming to Brown. As it happened, I received my BA degree from Brandeis in 1959. Our paths were destined to cross early and often.

At first, Ken and I shared an office on the first floor of Howell House, a rickety old building that housed the Mathematics Department. Ken immediately noticed that our office could easily accommodate a ping-pong table. We rented and installed such a table and soon became very popular with our colleagues, who would show up often for "a game or two." This was great fun, but not at all conducive to serious work. We soon abandoned both our office and the ping-pong table for two small individual offices on the third floor. Our productivity immediately increased.

Ken brought to my attention a short, but very influential, paper by the world-famous mathematician André Weil. The title of Weil's paper was "Number of Solutions of Equations in a Finite Field." Toward the end of this paper, Weil formulated three conjectures that became the focus of research in arithmetic-algebraic geometry for many years. The first conjecture was proved by Ken's thesis advisor, Bernard Dwork. The second was proved primarily by Alexander Grothendiek, and the third, the Riemann hypothesis for varieties over finite fields, was proved by Pierre Deligne. Weil's paper gave evidence for his conjectures by showing that they were true in special cases. All these conjectures were proved with the use of new and very difficult theorems in algebraic geometry. These were far from being accessible to beginners. However, we noted that the results in Weil's paper were relatively elementary and could be made understandable to advanced undergraduates and beginning graduate students in mathematics. Thus was born our project of writing a number theory book with the goal of presenting all the background needed to be able to read and understand Weil's paper discussed above. Our first book in this direction was *Elements of Number Theory: Including an Introduction to Equations over Finite Fields.* It was published by Bogden and Quigley in 1972. Subsequently, Bogden and Quigley went out of business. However, Springer-Verlag agreed to publish a greatly expanded version of our book with the title *A Classical Introduction*

to Modern Number Theory [41]. This was published in 1982. A second edition appeared in 1990. Unfortunately, before the second edition appeared, Ken Ireland passed away, suddenly, and prematurely, in 1991.

The University of New Brunswick, where Ken taught from 1971 to 1991, established an annual lecture series in his honor entitled "The Ken Ireland Memorial Lecture." I was very pleased to have been asked to give the first lecture in this series, on November 2, 1992. The title of my talk was "Niels Henrik Abel and Equations of the Fifth Degree."

I have many fond memories of our relationship. When we were both at Brown, I would occasionally visit the Math Department after dinner to work in my office. On entering the building I would often find Ken, alone in the Common Room, playing classical music on his flute. The beautiful music would follow me up the stairs. He was a truly unique and memorable individual. To this day, I still miss him.

—Michael Rosen, Professor Emeritus, Brown University

From Ken Ribet

When I arrived at Brown University in 1965, I thought that I would major in mathematics but had no sense of what a mathematics student might study in college. I was turned on to abstract mathematics by my first professors—Frank M. Stewart and Allan H. Clark. As Clark's course on abstract algebra was coming to a close, I met Ken Ireland by chance in the Brown math building (Howell House). After I told Ireland what I was studying, he challenged me to cite examples of abelian Galois extensions. I replied immediately that extensions of finite fields were cyclic. Ireland agreed that this was the case but then asked me about number fields. Cyclotomic extensions were on his mind. At the end of our discussion, Ireland suggested that I read an article about roots of unity. He handed me André Weil's celebrated 1949 article "Numbers of Solutions of Equations in Finite Fields." This was the article that corresponds to the Weil conjectures about the cohomology of algebraic varieties over finite fields. The article is totally elementary (and very clearly written); I could follow every word. I returned to see Ireland not long after our initial encounter and reported that I had finished Weil's paper. "Great! Now read this one." Ireland was asking me to study Weil's "Jacobi Sums as 'Grössencharaktere,"' which I was able to do, more or less. (I had no sense that Weil was computing the Hasse–Weil zeta function in special cases.)

As a result of the apparent success of my independent study, Ireland offered to direct the senior thesis, which I wrote during my last year at Brown. He was not shy about making recommendations: he told me what literature to read, where to apply to graduate school, and who my advisor should be at Harvard—the school that he recommended for my graduate study.

Although Ken Ireland seemed to have a mental block against doing research on his own, he devoured preprints on all sorts of topics and organized research-level seminars for discussion of the most interesting papers. He was a marvelous classroom teacher, and he had a great sense of humor.

He began the graduate algebra course that I attended with the statement that the definition of a group would be left as an exercise. While visiting a middle-school class, he asked the children in front of him to define a point in mathematics. A kid walked up to the front of the room and drew a dot on the blackboard. Ireland squinted at the dot and proclaimed, "That's no point. It looks like a pile of chalk."

—Kenneth A. Ribet, University of California, Berkeley

From the University of New Brunswick

Ken Ireland joined the Department of Mathematics and Statistics at the University of New Brunswick, Fredericton, in 1971. He immediately became one of its most prominent members in scholarship, teaching, and collegial decision-making, remaining a leading light throughout his two decades with us. A colleague recalls that "Ken was a penetrating thinker who could go to the heart of a problem and solve it with elegant style and transparent rigor." His command of mathematics was exceptionally broad and deep, enabling him to assist colleagues in diverse fields and facilitate their research work, while keeping abreast of developments well beyond his own immediate fields of number theory, algebra, algebraic geometry, and analysis. A colleague working in analysis recalls, "Ken's example motivated me ... to improve." An applied mathematician recalls successful collaborations with Ken on projects in computational number theory.

He was an outstanding, truly gifted teacher. He inspired the students in his classes and was exceptionally generous with his time assisting students, not only those enrolled in his own courses but any students who approached him for help in mathematics. Many students in mathematics courses are apprehensive and lack confidence in their own abilities. A colleague recalls how Ken helped them overcome these issues by "offering respect to them and receiving it back," and by breaking tension with the use of humour that helped such students to relax and focus on course topics. Another recalled that he also was a generous mathematical mentor to talented undergraduate and graduate students.

A superb expositor in general and frequent contributor of talks in the department's weekly research seminar series, he inspired others by his example. These talents were brought to international audiences in the widely acclaimed book *A Classical Introduction to Modern Number Theory*, coauthored with his long-time collaborator and friend Michael Rosen of Brown University. This text appeared in two editions, 1982 and 1990, the latter with additional chapters discussing research advances by prominent number theorists during the intervening decade. Both written during his time at UNB, they made accessible to graduate students some of the most significant results of mid-twentieth-century research in the field.

Ken actively engaged in recruitment of new faculty, insisting on excellent research and teaching, while also promoting equity and diversity. He was a leader in successful efforts to recruit the department's first two women in

full-time faculty positions, making this a priority. He helped encourage both these highly qualified candidates to accept UNB's offers by being knowledgeable about their specialties. One recalls, "Ken knew all about my thesis."

His interest in improving mathematical education in schools and experience in summer NSF programs for school teachers in the United States led to securing a joint appointment between our department and UNB's Faculty of Education. His knowledge and active engagement at UNB in this area, along with personal persuasiveness, were key factors in the two relevant deans and the vice-president agreeing to authorize the joint position. Both women that Ken helped recruit were granted tenure and made many significant contributions during their careers at UNB.

Ken also was an inspiration in cultural and intellectual matters, encouraging others to broaden their horizons. A dedicated amateur flautist, he occasionally gave public recitals, both solo and accompanied by other musicians. He preferred challenging scores, with J. S. Bach his favourite composer. He had wide literary interests, including novels and poems by Russian, German, and Austrian writers, which he read in the original languages. His profound understanding of the history of mathematics shone in the course he regularly taught, which always attracted substantial enrollments of students in diverse degree programs. At the time of his death, Ken was well advanced in a manuscript on the history of reciprocity laws in number theory. It extended from the conjecture by Euler and first proofs by Gauss through the many generalizations and applications by others during subsequent centuries.

Ken's life and work are honoured by the Ken Ireland Memorial Scholarship (two are awarded annually to UNB undergraduates) and the annual Kenneth Ireland Memorial Lecture series delivered at UNB by distinguished mathematicians. Topics in the lectures have represented a wide range of mathematical fields, as may be illustrated by a partial list of speakers from the three decades of the series: Michael Rosen (Brown University—the first in the series), Yuri Bahturin (Lomonosov Moscow State University), Gilbert Strang (Massachusetts Institute of Technology), Nigel Higson (Pennsylvania State University), Kenneth Ribet (University of California, Berkeley), Kumar Murty (University of Toronto, the most recent in the series).

—Bruce Lund, Gordon Mason, Barry Monson, Nora NiChuiv,
Donald Small, and Jon Thompson.

Contents

Notation

Symbol	Page	Definition
$\mathbb{R}$	16	the field of real numbers
$\mathbb{C}$	16	the field of complex numbers
$N(z)$	17	the norm of the complex number z
S'	18	the unit circle
ζ_n	20	$\cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$
$\mathbb{Q}$	27	the field of rational numbers
$F[x]$	28	the ring of polynomials in x with coefficients in a field F
$F[\alpha]$	31	the field obtained by adjoining the number α to F
$\mathbb{Z}$	28	the ring of integers
ϕ	34	Euler's phi function
$\mathbb{Z}_p$	32	the field of integers modulo a prime p
$\Psi_n(x)$	34	the minimal polynomial for $\cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$
$[K : F]$	35	the degree of a field extension
$a \equiv b \bmod m$	24	a is congruent to b modulo m
$\left(\frac{a}{p}\right)$	43	Legendre symbol
$\left(\mathbb{Z}_p^*\right)^2$	44	squares in $\mathbb{Z}_p$
$h\|n$	48	h is a factor of n
$[G : G_1]$	54	the number of left cosets of a subgroup G_1 in G
$\|G(s)\|$	54	the number of elements in $G(S)$
$v_p(r)$	56	the highest power of p that divides r
$(a_1, \ldots, a_m)$	61	$a_1\mathbb{Z} + a_2\mathbb{Z} + \cdots + a_n\mathbb{Z}$
$\gcd(a, b)$	62	the greatest common divisor of integers a and b
$\deg(f)$	65	the degree of polynomial f
$\zeta(s)$	81	formal Riemann zeta function
$\mathbb{Q}_p$	91	the field of p-adic numbers
$\|\|z\|\|$	93	distance from the complex number z to 0

1 Dialing In Problems

In case you forgot or didn't read (ahem) the purpose of the Dialing In problem sets in the preface, these are problems for you to try before (or in tandem with) your formal instruction or reading. They cover a wide range of topics. Some of them will not be familiar to you. But try them now, look things up (in this book, for example), and come back to them as you proceed through the text.

1.1 Dialing In Set 1

1. Find the solutions in $\mathbb{C}$ to $x^4 + 1 = 0$.
2. Find all primitives in $\mathbb{Z}_{17}$.
3. Show that
$$\cos 4x = \cos^4 x - 6\cos^2 x \sin^2 x + \sin^4 x.$$
4. Show that there are infinitely many primes $p \equiv 3 \pmod 4$.
5. Find a group of order 16 such that every element different from the identity has order 2.
6. Find the subgroup of order 4 in $\mathbb{Z}_{13}^*$.
7. Calculate the subgroup of cubes in $\mathbb{Z}_{19}^*$ and $\mathbb{Z}_{37}^*$.
8. Find all groups of order 4.
9. Let $E \supset F \supset K$ be three fields. Suppose that E is a vector space of dimension n over F, while F is a vector space of dimension m over K. Show that E is a vector space of dimension nm over K.
10. Find an irreducible polynomial with rational coefficients that has $\sqrt{2}+\sqrt{3}$ for a root.
11. Show that if G is a cyclic group of order n, then there is exactly one subgroup of order m for each $m \mid n$.
12. Show that if p is prime, then there is a polynomial in $\mathbb{Z}_p[x]$ with no root.
13. Find an irreducible polynomial in $\mathbb{Z}_2[x]$ of degree 4.
14. Show that -3 is a square in $\mathbb{Z}_p$ if and only if $p \equiv 1 \pmod 3$. Give examples.

In this book, $\mathbb{Z}_p$ stands for the ring of integers modulo p, while $\mathbb{Z}_p^*$ stands for the nonzero elements of $\mathbb{Z}_p$. See Section 2.2.4 for the meaning of *primitive*.

For inspiration, how about a group of order 4 in which every nontrivial element has order 2?

What does it mean for a vector space to have dimension n over F?

K. Ireland and A. Cuoco, *Excursions in Number Theory, Algebra, and Analysis*, Readings in Mathematics, https://doi.org/10.1007/978-3-031-13017-5_1

1.2 Dialing In Set 2

The intriguing question of representation by sums of squares is taken up in Section 3.4. Let us see what we can work out for ourselves with the tools we already have.

Welcome to a new installment of Dialing In. As usual, it contains some looking back and some previews of coming attractions. The previews include a visit with the following intriguing question: given an integer, in how many ways can it be expressed as the sum of two perfect squares? Try a few examples and see what you can see. Looking back, we revisit some group and field theory. There's plenty here to appeal to a wide variety of interests. So pick and choose and have fun.

15. Factor $8+7i$, $4+5i$, $11+12i$ into irreducibles in $\mathbb{Z}[i]$.

16 Show that

$$1 + x + x^2 + x^3 + x^4 + x^5 + x^6$$

is irreducible in $\mathbb{Q}[x]$.

Why *a* greatest common divisor and not *the* greatest? Stay tuned.

17. Find a greatest common divisor of $3+5i$ and $1+3i$.

18. Define $\chi(n) = 0$ if n is even, $\chi(n) = -1$ if $n \equiv -1 \pmod 4$, and $\chi(n) = +1$ if $n \equiv 1 \pmod 4$. Show that $\chi(ab) = \chi(a)\chi(b)$.

19. Show that if γ is irreducible in $\mathbb{Z}[i]$, then so is $\overline{\gamma}$.

20. Apply the Euclidean algorithm in $\mathbb{Z}[i]$ to

    (a) $\alpha = 1+i$, $\beta = 6+5i$,

    (b) $\alpha = 4+3i$, $\beta = -1+7i$.

21. A subset $\sigma \subseteq \mathbb{Z}[i]$ is called an *ideal* if

    (a) $\alpha, \beta \in \sigma \Rightarrow \alpha + \beta \in \sigma$ and

    (b) $\alpha \in \sigma$, $\gamma \in \mathbb{Z}[i] \Rightarrow \alpha\gamma \in \sigma$.

    Show that every ideal in $\mathbb{Z}[i]$ is of the form $\delta \cdot \mathbb{Z}[i]$.

See [19, Chapter 8] for more about $\mathbb{Z}[\rho]$.

22. Develop the arithmetic of $\mathbb{Z}[\rho] = \{\, a+b\rho \mid a, b \in \mathbb{Z} \,\}$, where $1+\rho+\rho^2 = 0$.

23. Show that if γ is irreducible in $\mathbb{Z}[i]$, than either

    (a) $\gamma\overline{\gamma} = p$ for a prime $p \equiv 1 \pmod 4$, or

    (b) $\gamma = u\,q$ for a prime $q \equiv 3 \pmod 4$ and a unit $u \in \mathbb{Z}[i]$, or

    (c) $\gamma = u(1-i)$ for some unit $u \in \mathbb{Z}[i]$.

"Formal Dirichlet series"?

24. Define $\mu(1) = 1$, $\mu(n) = 0$ if $p^2 \mid n$ for some prime p, and $\mu(p_1 \cdots p_s) = (-1)^s$ if $p_1, \ldots, p_s$ are distinct primes. Show that $\sum_{d|n} \mu(d) = 0$ if $n > 1$, and conclude that

$$\left(\sum_{n=1}^{\infty} \frac{1}{n^s}\right)\left(\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}\right) = 1$$

as formal Dirichlet series.

The representation function $r(n)$ is defined in Section 3.4.

25. If $(a,b) = 1$, $a, b \in \mathbb{Z}$, $a, b > 0$, show that $4r(ab) = 4r(a)r(b)$.

26. Let $f(n)$ be a real-valued function on $1, 2, 3, \ldots$ with $f(ab) = f(a)f(b)$ when $(a, b) = 1$. Show that as a formal Dirichlet series,

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^2} = \prod_p \left(\frac{1}{1 - f(p)/p^2} \right).$$

27. Consider 10 as an element of $\mathbb{Z}_p$. For example, $10 = 1$ in $\mathbb{Z}_3$, $10 = 3$ in $\mathbb{Z}_7$, $10 = 10$ in $\mathbb{Z}_{11}, \ldots$. Show that for $p \neq 2, 5$, the order of 10 as an element of $\mathbb{Z}_p^*$ is the length of the period in the repeating decimal expansion of $1/p$.

It isn't known whether there are infinitely many p for which the order of 10 is maximal, i.e., $p - 1$.

28. Show that $x^4 + 7$ is irreducible in $\mathbb{Q}[x]$. Is it irreducible in $\mathbb{Z}_5[x]$? in $\mathbb{Z}_{11}[x]$?

29. Show that the only automorphisms of $\mathbb{Q}(i)$ leaving $\mathbb{Q}$ pointwise fixed are the identity map and $\sigma : a + bi \to a - bi$.

30. Show that the only automorphisms of $\mathbb{Q}\left(\sqrt{2}\right)$ are the identity and $\sigma : a + b\sqrt{1} \to a - b\sqrt{2}$.

31. Compute the Galois group of $\mathbb{Q}\left(\zeta + \zeta^{-1}\right)$, where $\zeta^7 = 1$, $\zeta \neq 1$.

32. (a) If G and H are groups with operations $*$ and $\odot$ respectively, then $G \oplus H$ is the set of pairs (g, h), $g \in G$, $h \in H$, with the operation $(g, h) \cdot (g', h') = (g * g', h \odot h')$. Show that $G \oplus H$ is a group.

    (b) Show that an abelian group of order 8 must be isomorphic to $G_2 \oplus G_2 \oplus G_2$ or $G_4 \oplus G_2$ or G_8, where G_n denotes the cyclic group with n elements.

33. Find an irreducible polynomial of degree 3 over $\mathbb{Z}_{11}$.

34. Write $x_1^4 + x_2^4 + x_3^4$ as a polynomial in the elementary symmetric functions $\sigma_1 = x_1 + x_2 + x_3$, $\sigma_2 = x_1x_2 + x_1x_3 + x_2x_3$, $\sigma_3 = x_1x_2x_3$ with coefficients in $\mathbb{Q}$.

35. What is the highest power of p dividing $\binom{n}{p^s}$ for a prime p?

36. Look up a primitive in $\mathbb{Z}_{41}$. Use it to solve the equations $x^5 = 1$ and $x^8 = 1$ in $\mathbb{Z}_{41}$.

37. Is the product of the first n primes plus 1 always prime?

38. Show that there are infinitely many primes $\equiv 5 \pmod 6$.

39. Use the fundamental theorem of arithmetic to show that $\sqrt[5]{31}$ is not rational.

1.3 Dialing In Set 3

This Dialing In set is mainly an algebraic excursion (although some analysis sneaks in). The algebra involves formal polynomial identities (arithmetic in $\mathbb{Z}[x]$, for example) and the connections to polynomial functions and equations. Many of these problems look at results from high-school algebra in more general settings. Relax and have fun. And remember: you can pick and choose and then revisit (over and over).

40. How many subgroups does $\mathbb{Z}_{397}^*$ have? Write 397 as the sum of two squares. Did you know that 5 is the smallest primitive in $\mathbb{Z}_{397}$?

It is not known whether there are infinitely many primes p for which 2 is a primitive in $\mathbb{Z}_p$. This is Emil Artin's conjecture.

41. The largest prime less than 4000 is 3989. Show that 2 is a primitive in $\mathbb{Z}_{3989}$.[1]

42. Carry out the proof of the symmetric function theorem (Theorem 4.10) for the case of two variables. Does the proof significantly simplify?

43. Consider the ring $\mathbb{R}[x]$. Call two polynomials f and g equivalent if x^2+1 divides $f-g$. We write $f \equiv g \pmod{(x^2+1)}$. Define multiplication and addition of equivalence classes (after you have shown that the relation between polynomials is an equivalence relation) and show that the resulting ring is a field isomorphic to $\mathbb{C}$.

This problem asks you to consider (once again) Exercise 3.8 in Section 3.1.

44. Consider a fixed E with $\mathbb{C} \supset E \supset \mathbb{Q}$. If $\dim_{\mathbb{Q}} E = 2$, show that $E = \mathbb{Q}(\sqrt{\alpha}) = \{ a + b\sqrt{\alpha} \mid a, b \in \mathbb{Q} \}$ for some integer α.

Hint: Observe that $x-\alpha$ divides $x^n - \alpha^n$ (proof?). Then write $f(x) = f(x) - f(\alpha) = \cdots$.

45. Let R be a commutative ring with identity. If $f \in R[x]$ and $f(\alpha) = 0$ for some $\alpha \in R$, show that $f(x) = (x-\alpha)h(x)$ for some $h(x) \in R[x]$. (Note: You don't have a division algorithm in general.)

46. Show that the matrices of the form $\left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right)$ for a, b real form a subfield of the ring of all 2×2 matrices and that this subfield is isomorphic to $\mathbb{C}$ via the mapping

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \longleftrightarrow a + bi\,.$$

What does the norm in $\mathbb{Z}[i]$ correspond to?

47. Use the existence of a primitive to prove Wilson's theorem: $(p-1)! = -1$ in $\mathbb{Z}_p$.

48. Suppose that f and g are polynomials of degree n in $\mathbb{Q}[x]$. Show that if f and g agree on $n+1$ values, then they are equal as functions on $\mathbb{Q}$.

49. Construct a field E with p^2 elements that contains $\mathbb{Z}_p$ for $p \equiv 3 \pmod 4$ by imitating the construction of $\mathbb{C}$ from $\mathbb{R}$. Determine the automorphisms of E that leave $\mathbb{Z}_p$ fixed. What group do you get?

50. Show that if π is irreducible in $\mathbb{Z}[i]$, then $N(\pi)$ is either prime or the square of a prime.

51. Let $f(x)$ be an irreducible polynomial in $\mathbb{Q}[x]$. If α and β are roots of f, show that the field $\mathbb{Q}(\alpha)$ is isomorphic to $\mathbb{Q}(\beta)$ by an isomorphism that takes α to β.

In fact, you will show in Chapter 6 that $\cos nx \in \mathbb{Z}[\cos x]$ (see Exercise 6.1, part ii). Or show it now—give it a try.

52. Use de Moivre's theorem to show that for each positive integer n, one has

$$\sin nx \in \mathbb{Z}[\sin x, \cos x]\,,$$
$$\cos nx \in \mathbb{Z}[\sin x, \cos x]\,,$$

where as usual, $\mathbb{Z}[\alpha, \beta]$ means polynomials in α and β.

[1] Don't do this problem. [When Ken wrote this footnote, pocket calculators, let alone computers, were not widely available. Go ahead and solve the problem!]

53. Let S be a set and G a group. Suppose each $g \in G$ is also a map from S to S and denote the image of $s \in S$ under g by $g(s)$. Suppose $e(s) = s$ for the identity e and $g_1 \cdot g_2(s) = g_1(g_2(s))$ for each s, g_1, g_2. Put $G(s) = \{ g(s) \mid g \in G \}$. Show that either $G(s) = G(s')$ or $G(s) \cap G(s') = \varnothing$ for two elements s and s' from S.
54. Consider the cubic polynomial $x^3 + x + 1$. Find a polynomial in $\mathbb{Q}[x]$ whose roots are the squares of the roots of the above polynomial.
55. Consider $x^3 + 4x^2 + 2x + 1$ $\mathbb{Z}_5[x]$. Find the polynomial whose roots are $\alpha_1 + \alpha_2$, $\alpha_1 + \alpha_3$, and $\alpha_2 + \alpha_3$, where α_1, α_2, α_3 are the roots of the above polynomial in some extension field E of $\mathbb{Z}_5$.
56. Write $(x_1 - x_2)^2(x_1 - x_3)^2(x_2 - x_3)^2$ as a polynomial in $\mathbb{Z}[\sigma_1, \sigma_2, \sigma_3]$, where in σ_1, σ_2, σ_3 are the three elementary symmetric functions in x_1, x_2, x_3.
57. Consider $\zeta_{12} = \cos \frac{2\pi}{12} + i \sin \frac{2\pi}{12}$. Show that $\zeta_{12} + \zeta_{12}^{-1}$ is not a rational number.
58. Find the polynomial $f \in \mathbb{Q}[x]$ of lowest degree such that $f(\zeta_{12} + \zeta_{12}^{-1}) = 0$.
59. Is $x^4 + x^2 + 1$ irreducible in $\mathbb{Q}[x]$?

Well, $x^2 + x + 1$ is irreducible in $\mathbb{Q}[x]$, right?

60. Consider $x^3 + ax^2 + bx + c = (x - \alpha)(x - \beta)(x - \gamma)$. Find the cubic polynomial with roots $\alpha + \beta$, $\alpha + \gamma$, $\beta + \gamma$. Here a, b, c, α, β, γ belong to a field.
61. Calculate, up to isomorphism, all groups with eight elements.
62. Use the proof of the theorem on the primitive element to construct a primitive in $\mathbb{Z}_{13}$.

Exercises like 60 and 63 give a taste of the symmetric function theorem, which is coming up.

63. Consider $f(x) = x^3 + ax^2 + bx + c = (x - \alpha)(x - \beta)(x - \gamma)$. Find the polynomial with roots $\alpha + \beta + \alpha\beta$, $\alpha + \gamma + \alpha\gamma$, and $\beta + \gamma + \beta\gamma$.
64. Consider the additive groups in $\mathbb{Z}_5$ and $\mathbb{Z}_3$. Show that $\mathbb{Z}_5 \oplus \mathbb{Z}_3$ is isomorphic to $\mathbb{Z}_{15}$.
65. (For those who need to review analysis.) Let $E \subset \mathbb{R} \times \mathbb{R}$ with E compact. Show that if $E \subset \bigcup_\alpha V_\alpha$, where V_α is open and α an arbitrary index set, then there exist $\alpha_1, \ldots, \alpha_n$ such that $E \subset V_{\alpha_1} \cup V_{\alpha_2} \cup \cdots \cup V_{\alpha_n}$.

Our definition of compact is in Section 4.2.

66. Show that the map $x \mapsto |x|$ of $\mathbb{C}$ to $\mathbb{R}$ is continuous.

1.4 Dialing In Set 4

This set develops some of the algebraic background that will be useful in our algebraic approach to the fundamental theorem of algebra. And as usual, it revisits some earlier results and previews some of what is coming up later in the book. And as usual, pick and choose and come back often.

One way to state the theorem is that every polynomial with real coefficients has a root in the complex numbers. More is true, as you will see.

67. If $E \supset \mathbb{Q}$, where E is a field of vector space dimension 3 over $\mathbb{Q}$, show that $E = \mathbb{Q}(\theta)$, where θ is a root of an irreducible cubic in $\mathbb{Q}[x]$.

68. Show that $\log_{10} 7$ is irrational.

69. Show that $\sqrt{2} + \sqrt{3}$ is irrational.

70. Calculate the minimal polynomial for $\sqrt{a} + \sqrt{b}$, where a and b are square-free integers.

71. Let A be an integral domain. If $\alpha \in A$, call α irreducible if $\alpha = \beta\delta$ implies that either β or δ is a unit in A. Show that if Ψ is an automorphism of A, then $\Psi(\alpha)$ is irreducible if and only if α is irreducible.

72. One of the other problems is a special case of problem 71. Which one is it?

73. Show that 1, $\sqrt[3]{2}$, $\sqrt[3]{4}$ form a vector space basis for the field obtained by adjoining to $\mathbb{Q}$ the real root of $x^3 - 2$.

74. Find a *reducible* polynomial over $\mathbb{Q}$ with *all* roots nonreal.

75. Check out Wilson's theorem explicitly for $\mathbb{Z}_5, \mathbb{Z}_{11}, \mathbb{Z}_{13}, \mathbb{Z}_{17}, \mathbb{Z}_{19}$. Do not cheat.

76. This problem is omitted for lack of space.

77. Consider $\mathbb{Z}_p[x_1, \ldots, x_n]$. Notice that $x_1^p + x_2^p + \cdots + x_n^p$ is symmetric. According to the symmetric function theorem, it must be in $\mathbb{Z}_p[\sigma_1, \ldots, \sigma_n]$. Which element is it?

78. True or False: problem 77 is a trick. The answer is immediate.

79. Let Ψ be an automorphism of a ring R. Define Ψ^* on $R[x]$ by

$$\Psi^*\left(a_0 + a_1 x + \cdots + a_n x^n\right) = \Psi(a_0) + \Psi(a_1)x + \cdots + \Psi(a_n)x^n\,.$$

If f and g are in $R[x]$, show that $\Psi^*(f \cdot g) = \Psi^*(f) \cdot \Psi^*(g)$.

80. Let $\alpha_1, \ldots, \alpha_n$ be indeterminates. Consider the polynomial

$$\prod_{i<j} \left(z - (\alpha_i + \alpha_j + \alpha_i\alpha_j)\right) = H(z)\,.$$

Show that the coefficients of $H(z)$ are symmetric in $\alpha_1, \ldots, \alpha_n$.

81. Let

$$\begin{aligned} f(x) &= x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Q}[x] \\ &= (x - \theta_1)(x - \theta_2)\cdots(x - \theta_n)\,. \end{aligned}$$

If $g(x) \in \mathbb{Q}[x]$, show that $\prod_{i=1}^{n}(x - g(\theta_i))$ is in $\mathbb{Q}[x]$.

82. Factor $x^p + y^p$ in $\mathbb{Z}_p[x, y]$.

83. Show that if $0 < m < n$, then $\frac{n(n-1)\cdots(n-m+1)}{m!} \in \mathbb{Z}$.

84. Show that $x^4 + 6x^2 + 1$ is irreducible over $\mathbb{Q}$ but reducible mod p for all primes p.

85. Show that if f is irreducible in $\mathbb{Q}[x]$, then in $\mathbb{C}[x]$ one has

$$f(x) = (x - \alpha_1)\cdots(x - \alpha_n),$$

where $\alpha_i \neq \alpha_j$ for $i \neq j$.

Hint: Consider the derivative $f'(x)$.

86. Consider $F(\alpha)/F$, where α is algebraic over F. Let $g(\alpha) \in F(\alpha)$. Show that $g(\alpha)$ is algebraic and the minimal polynomial of $g(\alpha)$ has degree dividing the degree of the minimal polynomial of α.

Hint: Study "Some properties of algebraic extensions of fields" in Section 2.2.

87. Calculate the irreducible monic polynomial in $\mathbb{Q}[x]$ that has $\sqrt{-1}+\sqrt{-2}$ as a root.

88. Find four real roots of $x^8 - 47x^4 + 1$.

89. Consider $x^3 + ax + b = (x - \alpha)(x - \beta)(x - \delta)$. Express $\frac{1}{\alpha^2} + \frac{1}{\beta^2} + \frac{1}{\delta^2}$ in terms of a and b.

90. Show that for every real number $N > 0$, there exist consecutive primes p and q such that $q - p > N$.

91. Find an algebraic number α such that $\alpha^n \notin \mathbb{Q}$ for all $n > 0$.

1.5 Dialing In Set 5

To finish up this algebraic tour, here is a collage of problems that revisits and extends some of the algebra we have used from group theory, ring theory, and polynomial algebra. It also previews some themes about irrationality in Chapter 5. Enjoy.

92. Consider $\mathbb{Z}[i]$. Show that if $N(\alpha) = p$, where p is prime, then α is irreducible.

93. Show that the reflections and rotations of an equilateral triangle form a group of order 6 that is not abelian.

94. Classify, up to isomorphism, all groups of order 6.

95. Calculate the order of $10 \mod p$ for the primes $7, 11, 13, 17, 19$ and show that in each case, it is the length of the period in the repeating decimal expansion of $1/p$.

96. Consider the quartic $x^4+x+1 \mod 2$. Find the polynomial $\mathbb{Z}_2[x]$ whose roots are the squares of the roots of $x^4 + x + 1$ (those latter roots being in some larger field containing $\mathbb{Z}_2$).

97. Calculate the number of irreducibles mod p of degree 3 for low p. Any conjectures as to a general formula?

98. Although there is space for problem 98, that space has been used by the present sentence (problems 99 to ∞ to follow).

99. If K is a field, show that $K[x]$ has unique factorization.

100. Show that there are infinitely many nonisomorphic cyclic groups each having no proper subgroup other than the identity subgroup.

101. Show that there are infinitely many primes by considering $n! + 1$.
102. Write out the proof of the symmetric function theorem (Theorem 4.7) for the special case of three variables.
103. Find the minimal polynomial for $\sqrt{2} + \sqrt[3]{2}$.
104. Show that $\sqrt{2} + \sqrt[3]{2}$ is irrational.
105. Write out carefully a proof that the set of algebraic numbers is countable.
106. Construct a field with eight elements.
107. Give an example of a nonabelian group with $2n$ elements for each positive integer n.
108. Show that if G is a group with an even number of elements, then there is an element of order 2 in G.
109. Show that if 3 divides the order of a finite group G, then there is an element of order 3. Don't use any general theorems that automatically give the result (like Cauchy or Sylow).
110. Show that $x^5 + 6x^4 + 18x^3 + 463104x + 1155$ is irreducible in $\mathbb{Q}[x]$.

1.6 Dialing In Set 6

Finally, we get to some analysis. Some of the problems ask you to fill in details in the proofs in Chapter 5. These proofs all use the same basic method (proof by contradiction) to show that a cleverly constructed function cannot exist. The purpose of many of the problems in this set is to show that the "cleverness" of these functions is no mystery—they are defined as a result of looking at concrete examples and abstracting off the properties needed to obtain a contradiction. There is algebra in here, too, just to mix things up. And some problems belong to more than one mathematical field.

111. Show that every rational number has a repeating decimal expansion.
112. Show that every repeating decimal is a rational number.

For problems 113 and 114, consult the proofs of Theorems 5.4 and 5.5.

113. The irrationality of e^n follows the same pattern of proof as that of π. Can you use a similar method to show that π^n is irrational? How about π^2 for context.
114. In the proof of the irrationality of π, why won't $x(1-x)/n!$ work in place of $x^n(1-x)^n/n!$?
115. Let $f(x) \in \mathbb{Z}[x]$ and consider $h(x) = x^n f(x)/n!$. Show that the $h^{(j)}(0)$ are always integers. Prove also that $n+1$ divides $h^{(j)}(0)$ for $j \neq n$. What happens at $j = n$?

And for 116, check out the proof of Theorem 5.8.

116. In the proof of the transcendence of e why can't

$$\frac{x^{p-1}[(x-1)\cdots(x-n)]^p}{(p-1)!}$$

be replaced simply by

$$\frac{[x(x-1)\cdots(x-n)]^p}{(p-1)!}\,?$$

117. Let $\zeta_9 = \cos\frac{2\pi}{9} + i\sin\frac{2\pi}{9}$. Compute the minimal polynomial for $\zeta + \zeta^{-1}$.
118. Show that $a + bi$ is algebraic over $\mathbb{Q}$ if and only if a and b are algebraic over $\mathbb{Q}$.
119. Find the number of representations of 119 as the sum of two squares.
120. Using the theorem of Weierstrass–Lindemann (Theorem 5.2), show that $\log\alpha$ is transcendental for α a nonzero real algebraic number, $\alpha \neq 1$.
121. Show that under the assumptions of problem 120, $\sin\alpha$ is transcendental for α nonzero real algebraic.

The restriction to "real" is inessential in problems 120 and 121.

122. Show that if α is transcendental, then so is α^r for $r \neq 0$ and rational.
123. Show that the set of all algebraic numbers in $\mathbb{C}$ is an algebraically closed field.
124. Find the minimal polynomial for $\sqrt{7} + \sqrt{11}$ in $\mathbb{Z}[x]$.
125. Use the proof of the transcendence of e (Theorem 5.5) to show that e does not satisfy a relation of the type $ae^2 + be + c = 0$ with a, b, c rational.
126. Show that if f and g are n-times differentiable real-valued functions, then

$$(fg)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} f^{(n-k)} g^{(k)},$$

where $f^{(m)}$ denotes the mth derivative of f.

127. Prove that $f^{(j)}(s)$ is always an integer for $s = 1, 2, \ldots, n$, where

$$f(x) = \frac{x^{p-1}[(x-1)(x-2)\cdots(x-n)]^p}{(p-1)!}.$$

128. Show that if $E \supset F$ are fields and E is a one-dimensional vector space over F, then $E = F$.
129. Use the method of proof for the irrationality of e to exhibit other irrational numbers.
130. Can you use the method of proof for the irrationality of e to show that

$$1 + \frac{1}{2} + \frac{1}{(2\cdot 3)^2} + \frac{1}{(2\cdot 3\cdot 5)^3} + \cdots + \frac{1}{(2\cdot 3\cdot p_n)^n} + \cdots$$

is irrational, where p_n is the nth prime?

131. By considering $\int_0^{\pi/4} \tan^n x\,dx$, show that

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

132. Reduce the proof of the transcendence of e to the case $n = 1$. This gives a proof of the irrationality of e that does not depend on the series for e.

133. Suppose a finite group satisfies the condition that $x^d = 1$ has exactly d solutions for every $d \mid n$. Show that the group is cyclic.

134. Use the pentagon game of Section 2.2 to find a fifth root of unity in $\mathbb{Z}_{41}$.

135. Show that π does not satisfy a quadratic equation with rational coefficients.

136. (For those who have done Dialing In problem 53, a really important problem.) Let G be a finite group and let p divide $|G|$, p prime. Put

$$S = \left\{ \left(a_1, \ldots, a_p\right) \mid a_1 \cdot a_2 \cdots a_p = e, a_i \in G \right\}$$

and let $Z_p = \{ 1, \sigma, \ldots, \sigma^{p-1} \}$ be a cyclic group of order p that operates on G by $\sigma\left(a_1, \ldots, a_p\right) = \left(a_p, a_1, a_2, \ldots, a_{p-1}\right)$. Show that this is a good action on S, and by counting orbits, show that there is an element of order p in G (Cauchy's theorem).

This proof is due to McKay [55].

137. Let $p \equiv 3 \pmod 4$ and consider $\mathbb{Z}_p\left(\sqrt{-1}\right)$. Show that conjugation is the pth-power map.

Liouville's theorem: Theorem 5.1.

138. Using the mean value theorem, get an explicit estimate for the constant in Liouville's theorem on approximation of algebraic numbers.

139. Can you get an explicit proof of Liouville for $\sqrt[3]{2}$?

140. (For those who have done Dialing In problem 53, still a really important problem.) Let G operate as a transformation group on a set S. If $s \in S$, let I_s be the subgroup of all $g \in G$ such that $g(s) = s$. Show that the number of cosets of I_s is equal to the number of distinct elements in the orbit $G(s)$ of s.

141. Let F be a field and $\alpha, \beta, \gamma \in F$. Suppose that $\alpha + \beta + \gamma = 0$. Show that $\alpha^3 + \beta^3 + \gamma^3 = 3\alpha\beta\gamma$.

142. Let n be a positive integer. Consider

$$\Psi_n(x) = \prod_{\substack{(j,n)=1 \\ 1 \le j \le n}} (x - \zeta^j),$$

where $\zeta = e^{2\pi i/n} = \cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n}$. Show that $\Psi_n(x) \in \mathbb{Z}[x]$.

143. A subgroup H of a group G is called normal if $aH = Ha$ for all $a \in G$. Let G be a group of order p^n and H a subgroup of order p^{n-1}. Using orbits and counting, find a result concerning the normality of H.

144. Compute $\begin{vmatrix} 1 & x & y & z \\ 1 & x^2 & y^2 & z^2 \\ 1 & x^3 & y^3 & z^3 \\ 1 & x^4 & y^4 & z^4 \end{vmatrix}$.

145. Consider $\zeta_{11} = \cos\frac{2\pi}{11} + i \sin\frac{2\pi}{11}$. Find the minimal polynomial for $\zeta_{11} + \zeta_{11}^{-1}$.

146. Show that if $m > 1$, m an integer, then $|\Psi_n(m)| > (m-1)^s$, where s is the number of positive integers less than n and relatively prime to n.

Ψ_n is defined above in problem 142.

147. Fill in the blanks: The _____ of ___ is _____ or _____

1.7 Dialing In Set 7

Fourier series are added to the mix of Dialing Ins from the first five chapters. The formula in problem 151 might seem quite mysterious, but the mystery will be solved in Chapter 6. The result of problem 158 might seem obvious, but how can you *prove* it?

148. Show that the Galois group of $\mathbb{Q}(\zeta_p)$ over $\mathbb{Q}$ is a cyclic group of order $p-1$. Here p is a prime larger than 2.

149. Calculate the Fourier series for $f(x) = x^2$ on $[-\pi, \pi]$.

Calculating Fourier series for specific functions builds algebraic muscle.

150. Calculate the Fourier series for $f(x) = \cos\frac{x}{2}$ on $[-\pi, \pi]$.

151. Find a Fourier series proof of $\frac{\pi^2}{6} = 1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots$.

152. Find the Fourier series for $\cos x$ if cos is rendered an odd function on $[-\pi, +\pi]$ by defining

$$f(x) = \begin{cases} \cos x, & 0 < x < \pi, \\ -\cos x, & -\pi < x < 0. \end{cases}$$

153. (For those who have done Dialing In 53 and related problems.) If G is a group, then the center of G is the set of all x such that $xy = yx$ for all $y \in G$. Show that the center $Z(G)$ is a subgroup and that if G is a p-group (that is, $|G| = p^n$ for a prime p), then $Z(G) \neq \{e\}$.

154. Let p and q be distinct primes. What can you say about $\mathbb{Q}(\zeta_p, \zeta_q)$? Can you find ξ such that $\mathbb{Q}(\zeta_p, \zeta_q) = \mathbb{Q}(\xi)$? If not, why not? If so, why?

155. Calculate the Fourier series for $f(x) = |x^3|$, $-\pi \le x \le \pi$.

156. Let F be a field with p^n elements, p prime. Show that $\sigma : F \to F$ defined by $\sigma(x) = x^p$ is an automorphism. Show also that the fixed field of σ is (isomorphic to) $\mathbb{Z}_p$.

157. Show that $\int_0^\infty x^{n-1}e^{-x}\,dx = (n-1)!$ for n an integer, $n \ge 1$.

158. Prove that there is no integer x such that $0 < x < 1$.

159. Write out a careful proof that the Fourier series averages at jump discontinuities with finite left slope and right slope.

160. Compute $\int_\Gamma e^z\,dz$, where Γ is the unit circle traversed counterclockwise. Compute also $\int_\Gamma z^n\,dz$, $n \ge 1$. Finally, be sure to calculate $\int_\Gamma \frac{1}{z}\,dz$.

161. Consider the curve defined by $y = \sqrt{|x|}$ on $[-\pi, \pi]$. The left and right derivatives at 0 are ∞. Show that nevertheless, Dirichlet's argument can be modified to give the Fourier series at 0.

Hint: Sketch a graph.

162. Using

$$1 + e^{ix} + e^{2ix} + \cdots + e^{nix} = \frac{e^{i(n+1)x} - 1}{e^{ix} - 1},$$

show that

$$\frac{1}{2} + \cos x + \cos 2x + \cdots + \cos nx = \frac{\sin(n + \frac{1}{2})x}{2 \sin \frac{x}{2}}.$$

Show other things too.

163. Show that $\int_0^1 x^x \, dx = 1 + \frac{1}{2^2} + \frac{1}{3^3} + \frac{1}{4^4} + \frac{1}{5^5} + \cdots$. *Hint*: See problem 157.

164. Omitted.

165. Show that $x^2 + y^2 = -1$ always has a solution for x, y in $\mathbb{Z}_p$. *Hint*: See problem 164.

But $f \neq g$ in $\mathbb{Z}[x]$. How can this happen?

166. Let $f(x) = x^5 + x^2 + 2x$ and $g(x) = x^2 + 3x$. Show that $f(a) = g(a)$ for all a in $\mathbb{Z}_5$.

167. Show that $(x + y)^{p^n} = x^{p^n} + y^{p^n}$ in $\mathbb{Z}_p[x, y]$.

1.8 Dialing In Set 8

This last set contains more variations on the recurring themes that run through the book, developing some especially nice identities. The one in problem 172 shows up in many texts (precollege and undergraduate) without proof, joining the long list of identities that are part of the folklore of mathematics. So too with problems 181 and 194. Chapter 6, with its results and methods of Fourier series, will give you the tools to prove identities like this and more exotic ones like the stunning formula in problem 180.

168. Write down a group of order 6561 every nonidentity element of which has order 3.

169. Left out due to lack of ideas.

170. Let $E \supset \mathbb{Z}_p$ be fields and assume that E is finite-dimensional over $\mathbb{Z}_p$. Consider the mapping from E into E defined by $\varphi(x) = x^p$. Show that φ is onto E.

171. Show that for $x \in [0, \pi]$,

$$\frac{\pi^2}{8} - \frac{\pi x}{4} = \cos x + \frac{\cos 3x}{3^2} + \frac{\cos 5x}{5^2} + \cdots.$$

172. Prove that

$$\frac{\pi}{3} = 1 + \frac{1}{5} - \frac{1}{7} - \frac{1}{11} + \frac{1}{13} + \frac{1}{17} - \frac{1}{19} - \frac{1}{23} + \cdots.$$

173. Calculate the units in the ring $\mathbb{Z}\left[\sqrt{-5}\right]$, which comprises all $a + b\sqrt{-5}$, $a, b \in \mathbb{Z}$.

174. Show that Lemma 3.11 in Section 3.2 breaks down for $\mathbb{Z}\left[\sqrt{-5}\right]$ and find a counterexample to Lemma 3.16 for $\mathbb{Z}\left[\sqrt{-5}\right]$.

175. Let p and q be distinct primes. When is $\zeta_p \notin \mathbb{Q}(\zeta_q)$? Here, of course, $p \neq 2$.

176. Find the minimal polynomial for ζ_{p^2} for an arbitrary prime p.

177. Find the nonprime that differs by 2 from the 41st prime.

178. In $\mathbb{Z}[x]$, let

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0,$$
$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_0.$$

Suppose that $a_n, a_{n-1}, \ldots, a_0$ have no common factors except ± 1, and $b_n, b_{n-1}, \ldots, b_0$, have no common factors except ± 1. Show that the same is true of the coefficients of $f(x) \cdot g(x)$.

179. **Take It Further.** Consider the ring $\mathbb{Z}[x]$. Show that the polynomial $z^n + x^2 z^{n-1} + x^3 z^{n-2} + \cdots + x^{n+1}z + x$ is irreducible in $(\mathbb{Z}[x])[z]$.

180. **Take It Further.** Show that for $x \in (-\pi, \pi)$, one has

$$x^3 = 2\pi^2 \sum_{n=1}^{\infty} (-1)^{n+1} \frac{\sin nx}{n} + 12 \sum_{n=1}^{\infty} (-1)^n \frac{\sin nx}{n^3}.$$

Conclude that $\sin x - \frac{\sin 2x}{2^3} + \frac{\sin 3x}{3^3} - \cdots$ is (on $(-\pi, \pi)$) a polynomial in x of degree 3 in $\mathbb{R}[x]$.

181. Prove (at least formally) that

$$\sin^{-1} x = x + \frac{1}{2} \cdot \frac{x^3}{3} + \frac{1 \cdot 3}{2 \cdot 4} + \frac{x^5}{5} + \frac{1 \cdot 3 \cdot 5}{2 \cdot 4 \cdot 6} \cdot \frac{x^7}{7} + \cdots.$$

Letting $x = 1$, we have

$$\frac{\pi}{2} = 1 + \frac{1}{2 \cdot 3} + \frac{1 \cdot 3}{2 \cdot 4} \cdot \frac{1}{5} + \frac{1 \cdot 3 \cdot 5}{2 \cdot 4 \cdot 6} \cdot \frac{1}{7} + \cdots,$$

a positive series for π.

182. Making cos odd on $(-\pi, \pi)$ by defining

$$f(x) = \begin{cases} \cos x, & 0 < x < \pi, \\ -\cos x, & -\pi < x < 0, \end{cases}$$

show that

$$\cos x = \frac{8}{\pi} \sum_{n=1}^{\infty} \frac{n \sin 2nx}{4n^2 - 1}$$

for $x \in (0, \pi)$.

183. Show that every group of order p^2, where p is prime, is abelian.

184. Let $f(x)$ be irreducible of degree n in $\mathbb{Z}_p[x]$. Suppose $f(x) = (x-\alpha_1)\cdots(x-\alpha_n)$, where $\alpha_i \in E \supset \mathbb{Z}_p$. Find the polynomial whose roots are the pth powers of the roots $\alpha_1, \ldots, \alpha_n$.

185. Consider $E \supset F$, where E, F are fields. If $\alpha \in E$ is algebraic over F and σ is an automorphism of E leaving F elementwise fixed, then show that α and $\sigma(\alpha)$ have the same minimal polynomial.

186. Relate problem 185 to problem 184.

For this reason, $\mathbb{Z}_p$ is called *perfect*. It truly *is* perfect.

187. Let $f(x)$ be irreducible in $\mathbb{Z}_p[x]$. Show that $f(x)$ cannot have a repeated root in any extension field of $\mathbb{Z}_p$.

188. Find the Fourier series for $\sin^5(x)$.

189. Calculate $\lim_{x\to 0}\left(\frac{\cos x}{x^4} + \frac{x^2}{6!} - \frac{1}{4!} + \frac{1}{2x^2} - \frac{1}{x^4}\right)$ if the limit exists.

190. Calculate $\lim_{x\to 0}\left(\frac{1}{x^2} - \frac{1}{2\sin\frac{x^2}{2}}\right)$.

191. Evaluate $\int_0^\infty \frac{\sin x}{x}\cdot\cos x\,dx$. *Hint*: The answer is $\pi/2$.

192. Let G be a group of order $2p$, where p is prime. Is G abelian? How many nonisomorphic groups are there of order $2p$?

193. Calculate the Fourier series on $[-\pi, \pi]$ for e^x.

194. Show that $\frac{\pi^4}{90} = 1 + \frac{1}{2^4} + \frac{1}{3^4} + \frac{1}{4^4} + \cdots$.

195. Establish the following trig identities:

$$\cos 2\theta = 2\cos^2\theta - 1,$$
$$\cos 3\theta = 4\cos^3\theta - 3\cos\theta,$$
$$\cos 4\theta = 8\cos^4\theta - 8\cos^2\theta + 1.$$

196. Prove that if $x \notin \pi\cdot\mathbb{Z}$, then

$$\sin x + \sin 3x + \cdots + \sin(2n-1)x = \frac{\sin^2 nx}{\sin x}.$$

197. Using problem 196, show that $\int_0^{\frac{\pi}{2}} \frac{\sin^2 nt}{\sin^2 t}\,dt = \frac{\pi n}{2}$.

198. Show that $\frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots + \frac{1}{n}$ is never an integer.

199. Consider $F = \mathbb{Q}(\sqrt[4]{2}, i) = \mathbb{Q}(\sqrt[4]{2})(i)$. Calculate the Galois group of $F/\mathbb{Q}$.

200. Let G be a finite group of order $n = pm$, $p \nmid m$. Show that if H_1 and H_2 are subgroups of order p, then there is an element $\alpha \in G$ such that $\alpha H_1 \alpha^{-1} = H_2$.

2 Polygons and Modular Arithmetic

There are connections between algebra and geometry that go well beyond the function–graph–analytic-geometry connections studied in high school.

Those high-school connections are important too.

We will use the field of complex numbers to tie together the geometry of regular polygons and the algebra of polynomials. As a bonus, we will meet some number theory and a little group theory, all bound up in a delightful package. Here we go ...

2.1 The Complex Numbers

One of the richest mathematical structures is the field of complex numbers. With its wonderful balance of algebraic, analytic, and topological properties, it has played a major role in the development of classical and modern mathematics.

But as late as the nineteenth century, the existential status of this field was unclear, resulting in the unfortunate but colorful adjective "imaginary." One reason for this is that unlike the folklore prevalent in most school algebra texts, complex numbers originally appeared not as attempts to adjoin $\sqrt{-1}$ to the real numbers, but as devices that were used in algorithms that produced solutions to cubic equations with real coefficients and real solutions. These "imaginaries" occurred in the algorithms at certain points but canceled out in the end.

It took more than two centuries before the reification of complex numbers as pairs of real numbers came into common usage. This topological visualization as the Cartesian plane by Carl Friedrich Gauss (1777–1855) and Jean-Robert Argand (1768–1822) already suggested a rigorous definition, and the realization that the correspondence $a + bi \leftrightarrow (a, b)$ admitted both algebraic and geometric interpretation was a breakthrough in mathematics. The floodgates surrounding the idea soon broke open.

In 1797, Caspar Wessel presented a paper to the Royal Danish Academy of Sciences entitled "On the Analytic Representation of Direction: An Attempt." Largely unnoticed, it contained the essence of the geometric correspondence.

But in point of fact, simply the consideration of expressions like $a + bi$, where $i^2 = -1$, gives a perfectly valid algebraic construction. This point of view was generally accepted by Leopold Kronecker's (1823–1896) time. The definition of the field of complex numbers as ordered pairs with the desired multiplicative and additive structure had already appeared in Heinrich Weber's *Lehrbuch der Algebra*. James Pierpont, who reviewed the first edition, commented:

K. Ireland and A. Cuoco, *Excursions in Number Theory, Algebra, and Analysis*,
Readings in Mathematics, https://doi.org/10.1007/978-3-031-13017-5_2

> In so small a space as this, the complex numbers and the four arithmetical operations upon it are defined. Of the mystery that once surrounded this number, not an atom is left by such a treatment; fractions and irrational numbers, negative and complex numbers, all stand on the same footing; all are equally real or unreal.

Leopold Kronecker gave a procedure for constructing a general field that contains all the roots of a polynomial with coefficients in that field, a construction that applies to $\mathbb{C}$. More about this in Chapter 4.

Thus the romance of the imaginary was replaced by the romance of abstract construction.

Throughout this book, we will denote by $\mathbb{R}$ the field of real numbers, and we will assume that you are familiar with their structure. For a quick and elegant review, consult the first several chapters of Jean Dieudonné's *Foundations of Modern Analysis* [22].

Section 2.3 develops another way to think about $\mathbb{C}$ using modular arithmetic for polynomials, very much in the spirit of Kronecker's formulation.

By $\mathbb{C}$ we will denote the field of complex numbers. Recall that this field is conveniently defined as the set $\mathbb{R} \times \mathbb{R}$ with the following addition and multiplication:

$$(a, b) + (c\ d) = (a + c, b + d),$$
$$(a\ b) \cdot (c, d) = (ac - bd, bc + ad).$$

You should quickly verify that these definitions indeed impose the structure of a field (a general set with two operations satisfying all the ordinary high-school rules of associativity and commutativity for both operations, inverses for the nonzero elements, and the distributive laws) on $\mathbb{R} \times \mathbb{R}$, where the additive identity is $(0, 0)$ and the multiplicative identity is $(1, 0)$. If we identify $(a, 0)$ with the number $a \in \mathbb{R}$, then $\mathbb{R}$ becomes a subfield of $\mathbb{C}$. Now by definition,

$$(0, 1) \cdot (0, 1) = (-1, 0).$$

So on putting $(0, 1) = i$, we have, using the above identification, $i^2 = -1$, which was what we wanted in the first place. Furthermore, every element of $\mathbb{C}$ is uniquely represented in the form $a + bi$, where a and b are in $\mathbb{R}$, which is rephrased by saying that $\mathbb{C}$ is a two-dimensional vector space over $\mathbb{R}$ with basis 1 and i.

We can therefore represent the set of complex numbers $\mathbb{C}$ in Cartesian coordinates, where the horizontal axis represents the real numbers a, the vertical axis represents the complex numbers bi for real b, and the point (a, b) represents the number $a + bi$. We can now say that a complex number *lies in the complex plane*.

Observe that the multiplicative inverse of $a + bi \neq 0$ is

$$\frac{a - bi}{a^2 + b^2},$$

the existence of which is ensured by the fact that $a^2 + b^2 = 0$ if and only if $a = b = 0$. This is equivalent to the fact that -1 is not a square in $\mathbb{R}$, which was the original observation of the subject.

Not only is -1 not a square, it is not even the sum of squares in $\mathbb{R}$. A great deal of interesting mathematics has arisen out of generalizing this notion to a general field.

Lookout Point 2.1. A field F is called *formally real* if -1 is not the sum of squares. If it is the sum of squares, then we call the minimum positive integer $s(F)$ for which -1 is the sum of $s(F)$ squares the *level* of the field. We shall see later in connection with our study of modular arithmetic that the integers modulo p have level one if 4 divides $p-1$. A very beautiful result was proved by Albrecht Pfister in 1965 [62]. He showed that the level of a field is always a power of 2. And furthermore, given any power of 2, say 2^n, there is a field with that level. Pfister has proved many other exciting results in the modern theory of quadratic forms and questions related to Hilbert's 17th problem.

See Section 3.5 for more on Hilbert's 17th problem.

Returning to the complex numbers $\mathbb{C}$, there is a very important operation largely responsible for much of $\mathbb{C}$'s success. It is called *conjugation* and is defined by $\overline{z} = a - bi$, where $z = a + bi$. Geometrically, conjugation is a reflection in the x-axis, and algebraically, it is an automorphism over $\mathbb{R}$ of order 2. These statements are codified in a theorem:

Theorem 2.1. *If z and w are complex numbers, then the following relations hold:*

(i) $\overline{z+w} = \overline{z} + \overline{w}$,

(ii) $\overline{zw} = \overline{z}\,\overline{w}$,

(iii) $\overline{z} = z$ *if and only if* $z \in \mathbb{R}$,

(iv) $z\overline{z} \in \mathbb{R}$,

(v) $\overline{\overline{z}} = z$.

Property (iii) is really important—it characterizes $\mathbb{R}$ as a subfield of $\mathbb{C}$. We will use it often.

It follows that the map $z \mapsto \overline{z}$ is one-to-one and onto.

See Exercise 2.2 for the meanings of "one-to-one" and "onto."

The real number $z\overline{z}$ is called the *norm* of z and is denoted by $N(z)$. If $z = a+bi$, then $N(z) = z\overline{z} = a^2+b^2$, and since $\sqrt{(a^2+b^2)}$ is the distance from the origin to the point z in the complex plane, we call $\sqrt{N(z)}$ the *absolute value* or *modulus* of z and denote it by $|z|$. The norm inherits most of its properties from the above theorem. One that will be very important in what follows is that the norm function is *multiplicative*.

Corollary 2.2. *If z and w are complex numbers, then*

$$N(zw) = N(z)\,N(w)$$

In particular, $N\left(z^2\right) = (N(z))^2$.

If $z = a + bi$, then $N(z) = a^2 + b^2$. Pythagoras, anyone?

Lookout Point 2.2. If $z = (a + bi)$ and $w = (c + di)$, the result of Corollary 2.2, when written out in all its glory, becomes

$$\left(a^2+b^2\right)\left(c^2+d^2\right) = (ac-bd)^2 + (bc+ad)^2\,.$$

Establishing this identity shows up in some high-school texts as an exercise (try it). The multiplicativity of the norm shows where it comes from. Algebraically, we see that the product of the two "quadratic forms" on the left is a sum of two squares of bilinear forms in all the variables.

In general, Adolf Hurwitz [40] showed that the identity

$$\left(x_1^2 + \cdots + x_n^2\right)\left(y_1^2 + \cdots + y_n^2\right) = z_1^2 + \cdots + z_n^2,$$

where the z_i are bilinear expressions in the x's and y's, has a solution only for $n = 1, 2, 4, 8$.

The set of complex numbers with norm 1 is called the unit circle. We denote it by S^1. Hence

$$S^1 = \left\{ z \mid N(z) = 1 \right\} = \left\{ z \mid z = x + iy,\ x^2 + y^2 = 1 \right\}.$$

The 3-sphere is the set of all (a, b, c, d) with $a^2 + b^2 + c^2 + d^2 = 1$.

Topologists call this a 1-sphere. (What is the common name for a 2-sphere?)

Notice that S^1 is a multiplicative group. It has lots of points with rational coordinates. In fact, the points

$$\frac{2t}{1+t^2} + \left(\frac{1-t^2}{1+t^2}\right) i$$

are on S^1 for every real t (check this). Notice that we are doing number theory again, because the homogenized identity of this reads

$$(2xy)^2 + \left(x^2 - y^2\right)^2 = \left(x^2 + y^2\right)^2,$$

...another old chestnut from high school.

and that says that there are infinitely many (primitive) Pythagorean triples, i.e., triples (a, b, c) of coprime integers with $a^2 + b^2 = c^2$.

For a basic and complete development of elementary trigonometry, see the notes written by the late Dick Askey at http://go.edc.org/askey-trig-2021.

In what follows, we will need the existence and basic properties of the trigonometric functions. It would be a long analytic digression, equivalent roughly to one semester of elementary analysis, to develop them thoroughly. Let us stabilize the situation by defining them and listing the properties we need using algebra. Note carefully the way in which π sneaks into the act, because later, when we prove that π is irrational, the definition chosen here will be important.

We define $\sin x$ and $\cos x$ as two functions of a *real* variable x given by the following formulas:

In addition to expediency and elegance, this development inverts the usual path (the usual path: from geometry of the unit circle to the algebra of power series). It is probably not a good way to introduce trig, but it is a very elegant example of the power of old-fashioned algebra.

$$\begin{aligned} \sin x &= x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^3}{3!} - \frac{x^7}{7!} + \cdots, \\ \cos x &= 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \frac{x^6}{6!} - \frac{x^8}{8!} + \cdots. \end{aligned} \tag{2.1}$$

The geometric motivation for this definition comes from the desire to find functions satisfying the differential equation $y'' = -y$. Check that using these definitions, if $y = \sin x$, then $y'' = -y$. Is the same true for $y = \cos x$?

You can show (try it) that sine and cosine defined in this way satisfy the following functional equations:

$$\begin{aligned} \sin(x+y) &= \sin x \cos y + \sin y \cos x, \\ \cos(x+y) &= \cos x \cos y - \sin x \sin y. \end{aligned} \tag{2.2}$$

It follows (with some work) that

$$\sin^2 x + \cos^2 x = 1\,,$$

The work is yours in Exercise 2.9

showing that these two functions are bounded in absolute value by 1. The cosine function is positive at $x = 0$, since $\cos 0 = 1$. If the cosine were positive everywhere, then its second derivative, $-\cos x$, would be negative everywhere. But that is incompatible with a bounded continuous function. It follows that the cosine function must have zeros, and it must have them at positive and negative values of x (why?). Let η denote the first positive number such that $\cos \eta = 0$. That is,

$$\cos x > 0 \text{ on } [0, \eta) \quad \text{and} \quad \cos \eta = 0\,.$$

From this, using equations (2.2), one derives the periodicity of the sine and cosine:

$$\sin(x + 4\eta) = \sin x, \quad \cos(x + 4\eta) = \cos x\,.$$

We see that as t goes from 0 to 4η, the complex number $\cos t + i \sin t$ traverses the unit circle S^1 starting at $(1, 0)$ in the Cartesian plane, in a counterclockwise manner, exactly once.

Putting $x = \cos t$ and $y = \sin t$ and using the formula for arc length, we see that the arc on S^1 from $(1, 0)$ to $(\cos t, \sin t)$ in the counterclockwise sense has length t for $0 \le t \le 4\eta$, as illustrated in Figure 2.1.

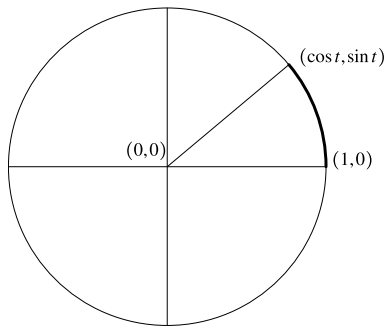


Figure 2.1. The arc defined by $(\cos t, \sin t)$.

The unit circle, of course, has length 2π, so $2\pi = 4\eta$, whence $\eta = \pi/2$, the period of the sine and cosine functions is 2π, $\cos\left(\frac{\pi}{2} + \pi n\right) = 0$ for all integers n, and everyone is happy.

One of the most important results in mathematics is the famous theorem of Abraham de Moivre (1667–1754), who is now well recognized as an unrecognized genius. He knew Isaac Newton and Alexander Pope. The result is simply this.

Theorem 2.3 (De Moivre). *For every integer n,*

$$(\cos x + i \sin x)^n = \cos nx + i \sin nx.$$

Proof. First, we can assume n to be positive. (Why?) The base case: if $n = 1$, we are through. (Why?) The inductive step is just the addition formulas: Assume that the theorem is true for $n - 1$. Then

$$(\cos x + i \sin x)^n = (\cos x + i \sin x)(\cos x + i \sin x)^{n-1},$$

which by the induction hypothesis equals

$$\begin{aligned}
&(\cos x + i \sin x)\big(\cos(n-1)x + i \sin(n-1)x\big) \\
&\quad = \cos x \cos(n-1)x - \sin x \sin(n-1)x \\
&\qquad + i\big(\sin x \cos(n-1)x + \cos x \sin(n-1)x\big) \\
&\quad = \cos nx + i \sin nx. \quad \text{So there.}
\end{aligned}$$

■

This result is really useful, for it enables us to solve lots of important equations. The most important equation for us is

$$x^n = 1\,. \tag{2.3}$$

It is not a priori clear at all that this has any roots besides $x = 1$. However, consider the complex number

$$\zeta_n = \cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n}\,.$$

Then

$$\zeta_n^n = \left(\cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n}\right)^n = \cos 2\pi + i \sin 2\pi = 1. \tag{2.4}$$

Hence ζ_n is a root of (2.3). You can also see this by noting, as you will see in Lookout Point 2.4, that to multiply two complex numbers, just add their angles and multiply their absolute values.

It follows that

$$1,\ \zeta_n,\ \zeta_n^2,\ \zeta_n^3,\ \ldots,\ \zeta_n^{n-1}$$

are the n distinct roots of (2.3), and they give the vertices of a regular polygon with n sides, as shown in Figure 2.2.

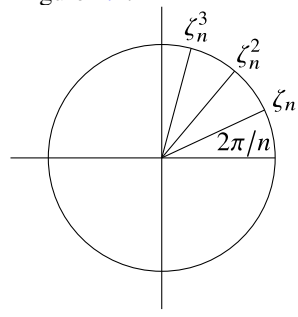


Figure 2.2. The powers of ζ_n.

This is a remarkable fact. Let us restate it as follows.

Theorem 2.4. *The solutions to the equation $x^n = 1$ form a multiplicative cyclic group of order n.*

These terms are all defined in Section 2.5.

Lookout Point 2.3. Here is an interesting fact. Are there any other finite multiplicative subgroups of the complex numbers? Suppose G is a subgroup of $\mathbb{C}^* = \mathbb{C} - \{0\}$ with n elements. Since G is a group, we see that $x^n = 1$ for each $x \in G$, by elementary group theory. In this situation, trigonometry plays the role of establishing an existence theorem. Later, we shall see that if a field K has a finite multiplicative subgroup G, then that group G must necessarily be cyclic; that is, there is an element $\rho \in K$ such that $G = \left\{ e, \rho, \rho^2, \ldots, \rho^{n-1} \right\}$. Hence G is an n-sided regular polygon. This observation plays an important role in establishing arithmetic analogues of some ruler-and-compass constructions in plane geometry (stay tuned).

See Sections 2.5 and 2.6 for more detail. And Joseph Rotman's *An Introduction to the Theory of Groups* [70] is a good reference for group theory.

What are the finite multiplicative subgroups of the field of real numbers?

Now, since $1, \zeta_n, \zeta_n^2, \zeta_n^3, \ldots, \zeta_n^{n-1}$ are n roots of $x^n - 1$, and since $x^n - 1$ can have at most n roots, we have by elementary algebra (writing ζ for ζ_n),

$$x^n - 1 = (x-1)(x-\zeta)\left(x-\zeta^2\right)\cdots\left(x-\zeta^{n-1}\right).$$

However, it is straightforward to see (in several different ways) that

$$\frac{x^n - 1}{x - 1} = 1 + x + x^2 + \cdots + x^{n-1}, \tag{2.5}$$

This formula implies the formula for the sum of a geometric series. This is Exercise 2.10.

so that

$$1 + x + x^2 + \cdots + x^{n-1} = (x-\zeta)\left(x-\zeta^2\right)\cdots\left(x-\zeta^{n-1}\right).$$

This is a very nice formula, and we will have an opportunity to refer to it again.

Putting $x = 1$, we have

$$n = (1-\zeta)\left(1-\zeta^2\right)\cdots\left(1-\zeta^{n-1}\right),$$

which decomposes n into the product of $n - 1$ complex numbers.

Now

$$\zeta = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n},$$

so

$$\zeta^{-1} = \cos\frac{2\pi}{n} - i\sin\frac{2\pi}{n}.$$

Hence

$$\zeta + \zeta^{-1} = 2\cos\frac{2\pi}{n}. \tag{2.6}$$

This will be useful when we look at constructibility of regular polygons in Section 2.2.

One more thing: notice that

$$\zeta_2 = \cos\frac{2\pi}{2} + i\sin\frac{2\pi}{2} = -1$$

and

$$\zeta_4 = \cos\frac{2\pi}{4} + i\sin\frac{2\pi}{4} = i\,.$$

Lookout Point 2.4. When we derived equation (2.4) in Section 2.1, we noted that to multiply two complex numbers, you just add their angles and multiply their absolute values. The typical way to develop the "add their angles" piece of this is to wait for the addition formulas for sine and cosine (equations (2.1) in Section 2.1). Which is why many texts punt when they get to "multiply the lengths and add the angles" in classes before trig, usually appealing to experiments or other kinds of motivation. But teachers at the Park City Teacher Leadership Program [82] (re)discovered a proof that uses nothing more than similar triangles. A detailed development of this proof can be found in [19, Chapter 3].

This may seem like small potatoes to many ("who cares what comes before what?"), but it has curricular implications:

- Students can understand the addition formulas *before* any advanced trig.
- More importantly, one can use the geometry of multiplication to *prove* the addition formulas. This saves a great deal of class time and simplifies the whole arc of results.

And it allows one to use complex numbers to derive trig identities (something that used to be considered circular reasoning).

For example, to get a formula for $\cos\left(\frac{\pi}{4}+\theta\right)$, calculate like this:

$$\begin{aligned}\cos\left(\frac{\pi}{4}+\theta\right) + i\sin\left(\frac{\pi}{4}+\theta\right) &= \left(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}\right)(\cos\theta + i\sin\theta)\\ &= \frac{1}{\sqrt{2}}(1+i)\,(\cos\theta + i\sin\theta) = \frac{1}{\sqrt{2}}\big((\cos\theta - \sin\theta) + i(\cos\theta + \sin\theta)\big)\,.\end{aligned}$$

Hence

$$\cos\left(\frac{\pi}{4}+\theta\right) = \frac{1}{\sqrt{2}}(\cos\theta - \sin\theta)\,,$$

and as a bonus,

$$\sin\left(\frac{\pi}{4}+\theta\right) = \frac{1}{\sqrt{2}}(\cos\theta + \sin\theta).$$

Exercises

2.1 Prove Theorem 2.1.

2.2 Show that the map $z \mapsto \overline{z}$ satisfies two properties:

(i) it is one to one: if $\overline{z} = \overline{w}$, then $z = w$;

(ii) if $z \in \mathbb{C}$, then $z = \overline{w}$ for some $w \in \mathbb{C}$.

2.3 Show that the norm function is multiplicative.

2.4 **Take It Further.** If f is a polynomial with complex coefficients, define $\overline{f}$ to be the polynomial you get by replacing each coefficient in f by its conjugate. Show that

(i) $\overline{f+g} = \overline{f} + \overline{g}$.

(ii) $\overline{fg} = \overline{f}\,\overline{g}$.

(iii) $\overline{f} = f$ if and only if $f(x)$ has real coefficients.

(iv) $f\overline{f}$ has real coefficients.

(v) If $z \in \mathbb{C}$, then $\overline{f(z)} = \overline{f}(\overline{z})$.

2.5 Let f be a polynomial with coefficients in $\mathbb{C}$. If a complex number z is a root of f, show that $\overline{z}$ is a root of $\overline{f}$.

2.6 Suppose f is a polynomial with coefficients in $\mathbb{C}$. Let $g = f\overline{f}$. Show that if $g(z) = 0$, then either $f(z) = 0$ or $f(\overline{z}) = 0$.

2.7 Show that S^1 has the structure of a multiplicative group.

Recall that S^1 is the set of complex numbers of norm 1.

2.8 Let ℓ be a line in the plane that passes through $-1 + 0i$ with rational slope t.

(i) If ℓ intersects S^1 in another point, show that this point's coordinates are rational.

(ii) In fact, find an expression in terms of t for the second intersection point.

2.9 Using our definitions of sine and cosine, show that

"Our definitions" are equations (2.1).

$$\sin^2 x + \cos^2 x = 1\,.$$

2.10

(i) Establish the algebraic identity

$$\frac{x^n - 1}{x - 1} = 1 + x + x^2 + \cdots + x^{n-1}\,.$$

(ii) Use it to derive the formula for the sum of a geometric series.

2.11 Generalize the "very nice formula" (2.5) to show that if n is a nonnegative integer and $\zeta = \zeta_n$, then the following hold:

(i) If x and y are integers, then

$$x^n - y^n = (x-y)(x-\zeta y)\left(x-\zeta^2 y\right)\cdots\left(x-\zeta^{n-1}y\right)\,.$$

(ii) If x and y are integers and n is odd, then

$$x^n + y^n = (x+y)(x+\zeta y)\left(x+\zeta^2 y\right)\cdots\left(x+\zeta^{n-1}y\right).$$

2.12 Take It Further. Using the power series definitions of sine and cosine, prove all the statements made in this section. Prove other things too.

2.2 The Pentagon, Gauss, and Kronecker

"Ruler" here refers to a straightedge—a ruler with no markings.

The pentagon is the first really interesting polygon. We will see how the use of complex numbers leads to a proof that the pentagon can be constructed by ruler and compass. An examination of the proof also leads to some interesting arithmetic questions that will enable us to explore a little modular arithmetic.

Consider the five-sided regular polygon inscribed in the unit circle in the complex plane, as illustrated in Figure 2.3:

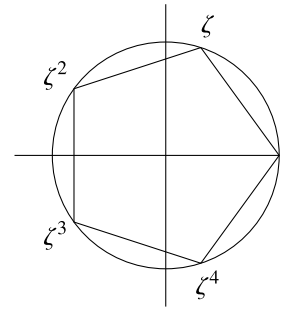


Figure 2.3. The regular unit pentagon.

This follows from de Moivre's theorem.

Here, $\zeta = \cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5}$ and $\zeta^5 = 1$. It follows that

$$\zeta^4 = \zeta^{-1}, \quad \zeta^3 = \zeta^{-2}, \quad \zeta^2 = \zeta^{-3}, \quad \zeta = \zeta^{-4}.$$

Two whole numbers a and b are said to be "equal modulo m" or "congruent modulo m" if m divides $a-b$, in which case a and b are the same up to (modulo) a multiple of m. One writes, with Gauss, $a \equiv b \mod m$ or simply $a \equiv b(m)$.

Already we see the modular arithmetic that we will further develop in Section 2.3, because the exponents are always "congruent modulo 5." Thus $\zeta^{21} = \zeta$ and $\zeta^{-7} = \zeta^{13}$. For example,

$$\zeta^{21} = \zeta^{1+5\cdot4} = \zeta^1 \cdot \zeta^{5\cdot4} = \zeta\cdot(\zeta^5)^4 = \zeta.$$

Notice that

$$\zeta + \zeta^{-1} = 2\cos\frac{2\pi}{5}, \tag{2.7}$$

which is twice the real part of the first vertex, as previewed in equation (2.6) in Section 2.1. So to get the value of the side length of our pentagon, we must first find a nice expression for $\zeta + \zeta^{-1}$.

For that, we use the great idea of squaring $\zeta + \zeta^{-1}$, which gives

$$\left(\zeta + \zeta^{-1}\right)^2 = \zeta^2 + 2 + \zeta^{-2}.$$

Now, ζ is a solution to

$$\frac{x^5 - 1}{x - 1} = 0,$$

but by Exercise 2.10, we have

$$\frac{x^5 - 1}{x - 1} = 1 + x + x^2 + x^3 + x^4, \tag{2.8}$$

so we have

$$1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4 = 0. \tag{2.9}$$

Rewrite this as

$$1 + \zeta + \zeta^2 + \zeta^{-2} + \zeta^{-1} = 0,$$

To see this, use the fact that $\left(\zeta + \zeta^{-1}\right)^2 = \zeta^2 + 2 + \zeta^{-2}$.

or

$$\zeta^2 + \zeta^{-2} = -1 - \zeta^{-1} - \zeta,$$

or

$$\left(\zeta + \zeta^{-1}\right)^2 = 1 - \left(\zeta + \zeta^{-1}\right),$$

or

$$\left(\zeta + \zeta^{-1}\right)^2 + \left(\zeta + \zeta^{-1}\right) - 1 = 0.$$

Well, this is wonderful! We have a quadratic equation in $\zeta + \zeta^{-1}$.

Solving this equation gives

$$\zeta + \zeta^{-1} = \frac{-1 + \sqrt{5}}{2},$$

The rest of the story is taken up in the exercises.

and there we are: we have an expression for $\cos \frac{2\pi}{5}$ that involves only rational numbers and $\sqrt{5}$.

We can play with this. Here we have also found the golden mean. Consider the segment of length 1, divided into two parts. Find x such that the length of the larger segment is the geometric mean of the length of the whole (that is, 1) and the length of the smaller segment, that is, such that

$$\frac{1 - x}{x} = \frac{x}{1}.$$

See Figure 2.4.

Figure 2.4. Find the point x such that $\frac{1-x}{x} = \frac{x}{1}$.

This becomes

$$x^2 = 1 - x,$$

or

$$x^2 + x - 1 = 0,$$

so that

$$x = \frac{-1+\sqrt{5}}{2} \quad \text{(our old friend).}$$

And there's more: from

$$x^2 + x - 1 = 0,$$

we see that

$$x(1+x) = 1,$$

or

As Van Morrison said so well [56], "Too late to stop now."

$$x = \frac{1}{1+x} = \frac{1}{1+\frac{1}{1+x}} = \frac{1}{1+\frac{1}{1+\frac{1}{1+x}}} = \cdots.$$

This gives rise to the continued fraction

$$1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1+\cdots}}},$$

whose partial sums are the ratios of consecutive Fibonacci numbers! So it's a small world.

There are a few other observations to make about the above argument. We have seen that

$$\zeta + \zeta^{-1} = \frac{-1+\sqrt{5}}{2},$$

or

$\zeta^9 = \zeta^4$, and ...

$$\sqrt{5} = 1 + 2\left(\zeta + \zeta^{-1}\right) = 1 + \zeta + \zeta^4 + \zeta^9 + \zeta^{16}.$$

In other words, $\sqrt{5}$ is the sum of *square* powers of a fifth root of unity. This remarkable fact was generalized by Gauss. He took an arbitrary prime number p and considered ζ_p, the first vertex of a p-sided polygon. Then he showed that if $4 \mid (p-1)$, then

$$\sqrt{p} = 1 + \zeta + \zeta^4 + \zeta^9 + \zeta^{16} + \cdots + \zeta^{(p-1)^2}. \tag{2.10}$$

This is not an elementary fact, and it took Gauss at least a year of work to prove it. We shall prove it in Chapter 6.

The right-hand side is called a Gauss sum. It lies at the base of his proof that a regular polygon with a prime number p of sides can be constructed if p is of the form $2^t + 1$ for some t. Such primes are called *Fermat primes*. This result is the very first entry of Gauss's diary for March 30, 1796, and he was quite proud of it, for it represented the first progress in the constructibility of regular polygons since classical antiquity. Although Gauss stated as well that for a regular polygon with a prime number of sides to be constructible, the prime had to be a Fermat prime, he did not provide a proof. A proof was given in 1837 by Pierre Wantzel (1814–1848). The next two primes to which his result applies are 17 and 257.

2.2.1 A Theorem of Kronecker

Another observation on the above results has to do with a deep result due to Kronecker. Since $\sqrt{5} = 1 + 2(\zeta_5 + \zeta_5^4)$, we see that the field $\mathbb{Q}[\sqrt{5}]$ of all expressions $a + b\sqrt{5}$, where a and b are rational numbers, lies in the field $\mathbb{Q}[\zeta_5]$ of all expressions $a_0 + a_1\zeta_5 + a_2\zeta_5^2 + a_3\zeta_5^3$, where a_0, a_1, a_2, a_3 are rational. More generally, it is true that $\mathbb{Q}[\sqrt{d}]$ lies in some $\mathbb{Q}[\zeta_n]$ for some n ($4d$ will do it). The fields $\mathbb{Q}[\sqrt{d}]$ are special cases of what are known as *abelian extensions* of the rationals. The word "abelian" here refers to the fact that the set of automorphisms of $\mathbb{Q}[\sqrt{d}]$ forms an abelian group under the composition of mappings. Indeed, the only automorphisms of $\mathbb{Q}[\sqrt{d}]$ are the identity and the mapping that sends $a + b\sqrt{d}$ to $a - b\sqrt{d}$, and these two operations form a group of order 2, which is, of course, abelian. You should verify this.

$\mathbb{Q}$ denotes the field of rational numbers. Think "$\mathbb{Q}$ for quotient."

The *fields* $\mathbb{Q}[\sqrt{d}]$ and $\mathbb{Q}(\zeta_5)$? Stay tuned.

Even *more* generally, let F be any subfield of the complex numbers that has a finite basis as a vector space over $\mathbb{Q}$. Every element α of F must satisfy a polynomial equation with coefficients in $\mathbb{Q}$, because

Such fields are called *algebraic number fields*.

$$1,\ \alpha,\ \alpha^2,\ \alpha^3,\ \ldots,\ \alpha^n$$

must be $\mathbb{Q}$-linearly dependent for some n. If every isomorphism of F into $\mathbb{C}$ sends F back to F (as in the above examples), then we say that F is a *Galois extension* of $\mathbb{Q}$ or simply that F is Galois.

Now given a Galois extension F, one can attach to it a very important finite group G called its Galois group. This group reflects in its structure much of the interaction between F and $\mathbb{Q}$ and is the object of many interesting investigations in algebra. It is quite simple to define: it is the set of all automorphisms of F, and the group operation is composition of functions. That is, an element of G is a mapping from F to F that is onto, one-to-one, and preserves all the algebraic operations. If such a mapping is denoted by σ, then the structure-preserving requirement means that

For example, the Galois group of $\mathbb{Q}[\sqrt{d}]$ consists of the two automorphisms described above: the identity map and the map that sends $a + b\sqrt{d}$ to $a - b\sqrt{d}$.

$$\sigma(a + b) = \sigma(a) + \sigma(b)$$

and

$$\sigma(ab) = \sigma(a)\sigma(b)\,.$$

We say that the field F is *abelian* if the Galois group of F is abelian (that is, commutative). Now at last we can state Kronecker's big result. Here it is:

Every abelian extension field F of $\mathbb{Q}$ sits inside $\mathbb{Q}[\zeta_n]$ for some n.

Kronecker's theorem is also known as the Kronecker–Weber theorem. Note that n depends on F.

This result is quite deep, and its generalizations form the object of much research.

Another example: Consider ζ_8, the first vertex of the regular octagon situated in the complex plane. Then $\zeta_8^4 = -1$, and so (putting $\zeta_8 = \zeta$), we have

$$\left(\zeta + \zeta^{-1}\right)^2 = \zeta^2 + 2 + \zeta^{-2} = 2 + \frac{\zeta^4 + 1}{2} = 2\,.$$

Another simple example: $i = \zeta_4$, so trivially, $\mathbb{Q}[i] \subset \mathbb{Q}[\zeta_4]$, because $\mathbb{Q}[i] = \mathbb{Q}[\zeta_4]$.

Hence $\zeta + \zeta^{-1} = \sqrt{2}$, and therefore, $\mathbb{Q}[\sqrt{2}] \subset \mathbb{Q}[\zeta_8]$. Again we have a special case of Kronecker–Weber.

Notice that in our examples, all the fields $\mathbb{Q}[\sqrt{-1}]$, $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{5}]$ are two-dimensional over $\mathbb{Q}$. Later, we will encounter a field F of dimension 3 over $\mathbb{Q}$, and again, as a byproduct of a deeper investigation on roots of unity, we will have another instance of Kronecker's theorem.

2.2.2 Some Properties of Algebraic Extensions of Fields

Unnoticed, had it not been for the sidenote on that page.

In Section 2.2.1, we slipped in a comment that may have gone unnoticed—we referred to $\mathbb{Q}[\zeta_5]$, the set of rational linear combinations powers of ζ_5, as a *field*. Recall that this means that in $\mathbb{Q}[\zeta_5]$, addition and multiplication are commutative and that all the usual rules of high-school algebra hold. It *also* means that the reciprocal of every nonzero element of $\mathbb{Q}[\zeta_5]$ sits in $\mathbb{Q}[\zeta_5]$. Other familiar fields are $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$. But $\mathbb{Z}$ is not a field, because, for example, $\frac{1}{5}$ is not in $\mathbb{Z}$.

$\mathbb{Z}$ (zahlen) denotes the ring of ordinary integers.

In this section, we will prove that $\mathbb{Q}[\zeta_5]$ is a field, and along the way, we will show that $\mathbb{Q}[\zeta_5]$ is a vector space over $\mathbb{Q}$ with basis $\left\{1, \zeta, \zeta^2, \zeta^3\right\}$. In the following paragraphs, we shall develop a few facts from field theory that cover these statements.

And there will be nothing special about 5 in the development.

A Little Field Theory

We have been a little relaxed until now about distinctions that we should make explicit. If F is a field, we let $F[x]$ denote the system of polynomials in x with coefficients in F together with the usual operations of high school—addition and multiplication. But $F[x]$ is not a field, because the reciprocal of a polynomial is not, in general, another polynomial. In fact, $F[x]$ is a ring, the ring of polynomials with coefficients in F

Are there any polynomials in $\mathbb{Q}[x]$ that have reciprocals in $\mathbb{Q}[x]$?

Polynomials are formal objects, and as such, you can do arithmetic with them. You can also evaluate polynomials at real or complex numbers, so that each formal polynomial defines a polynomial *function*. This interplay between formal polynomials and polynomial functions—form and function—is a cornerstone of modern algebra. For example, you can factor $x^5 - 1$ using equation (2.8):

This arithmetic is very similar to ordinary arithmetic with integers (this similarity is described in detail in [19, Chapter 6]).

$$x^5 - 1 = (x - 1)\left(x^4 + x^3 + x^2 + x + 1\right).$$

This is a formal identity in $\mathbb{Q}[x]$. It is a statement about polynomials, not numbers, and you could prove it by, for example, multiplying out the right-hand side and watching all but two terms disappear. Because this is a formal identity, you can replace x by any number, and you will get a true statement about numbers (why?). So for example, on replacing x by 2, we get

The motto is "formal polynomial identities are true under any substitution."

$$31 = 16 + 8 + 4 + 2 + 1.$$

And putting $x = \zeta_5$, we get

$$0 = (\zeta_5 - 1)\left(\zeta_5^4 + \zeta_5^3 + \zeta_5^2 + \zeta_5 + 1\right),$$

providing another look at equation (2.9) from Section 2.2.

Lookout Point 2.5. Suppose again that F is a field. If you take all the polynomials in $F[x]$ and replace x by some number, say ζ_5, you get a new system (this time consisting exclusively of numbers), which we can suggestively denote by $F[\zeta]$. So elements of $F[\zeta]$ are "polynomials in ζ." Note, though, that two polynomials in $F[x]$ can produce the same number in $F[\zeta]$. For example, $x^5 - x + 1$ and $2 - x$ both produce $2 - \zeta$ when x is replaced by ζ (check this). While $F[x]$ does not contain the reciprocals of all of its nonzero elements, we will prove next that $F[\zeta]$ does! It is not at all obvious that the reciprocal of a linear combination of powers of ζ with coefficients in F is also a linear combination of powers of ζ. But it is true. For example, in $\mathbb{Q}[\zeta]$, we have

Let's use just plain ζ for ζ_5.

$$\frac{1}{\zeta^3 - \zeta^2 + 2\zeta} = -\frac{1}{11}\left(7\zeta^3 + 9\zeta^2 + 8\zeta + 3\right).$$

Checking that

$$\left(\zeta^3 - \zeta^2 + 2\zeta\right)\left(7\zeta^3 + 9\zeta^2 + 8\zeta + 3\right) = -11$$

makes for a delightful calculation—try it! (This calculation didn't drop out of the sky. You will see later that there is a general method that allows one to calculate reciprocals in $\mathbb{Q}[\zeta_n]$ using little more than high-school algebra and some arithmetic. We will take this up in the coming chapters.)

Meanwhile, back at the ranch ... If E and F are fields and $E \supset F$, we say that E is an *extension field* of F, and we make a "tower diagram" like this:

If you don't get "Meanwhile, back at the ranch...," check out the Wikipedia article on the subject.

$$\begin{array}{c} E \\ | \\ F \end{array}$$

An element $\alpha \in E$ is said to be *algebraic* over F if there exists a nonzero polynomial f in $F[x]$ for which $f(\alpha) = 0$. For example, i, viewed as an element of $\mathbb{C}$ or $\mathbb{Q}(i)$, is algebraic over $\mathbb{Q}$, since it satisfies the equation $x^2+1 = 0$. Similarly, ζ_n is algebraic over $\mathbb{Q}$, since $\zeta_n^n - 1 = 0$. If $\alpha \in E$ is algebraic over F, we can construct $F[\alpha]$ in the same way that we built $F[\zeta]$ in the Lookout Point above: $F[\alpha]$ is the set of linear combinations of powers of α with coefficients in F.

In Chapter 5, we will prove that π is *not* algebraic over $\mathbb{Q}$.

It is natural to seek, among all polynomials f in $F[x]$ that admit α as a root, polynomials of lowest degree. The next result shows that such a polynomial is essentially unique and that it is irreducible.

A polynomial is *irreducible* in $F[x]$ if it doesn't factor into polynomials of lower positive degree. And a polynomial with leading coefficient 1 is a *monic* polynomial.

Theorem 2.5. *Let α be algebraic over a field F, and let $f(x)$ be a polynomial in $F[x]$ of minimal degree with $f(\alpha) = 0$, normalized so that its leading coefficient is* 1. *Then:*

(i) $f(x)$ *is the* only *monic polynomial with this property.*

(ii) $f(x)$ *is irreducible.*

Proof. (i) Suppose there were two monic polynomials of smallest degree that send α to 0. Their difference would also vanish at α, and the difference would have lower degree. This contradicts the minimality of degree of the original polynomial.

(ii) If $f(x) = g(x)h(x)$, $f(\alpha) = 0$, and both $g(x)$ and $h(x)$ are of positive degree, then we must have either $g(\alpha) = 0$ or $h(\alpha) = 0$. But the (alleged) g and h would then have degree less than that of f. ∎

Corollary 2.6. *Let $f(x)$ be the monic polynomial in $F[x]$ of minimal degree with $f(\alpha) = 0$. If $g(x) \in F[x]$ and $g(\alpha) = 0$, then $f(x)$ divides $g(x)$.*

This is the division algorithm for polynomials. See [41] or [19].

Proof. Write

$$g(x) = f(x)h(x) + r(x) \text{ with } 0 \le \deg r(x) < \deg f(x)\,.$$

Then

$$0 = g(\alpha) = f(\alpha)h(\alpha) + r(\alpha) = r(\alpha)\,.$$

By the minimality of the degree, we must have $r(x) = 0$. ∎

It follows that the monic polynomial $f \in F[x]$ of minimal degree satisfying $f(\alpha) = 0$ is uniquely determined by α and F. It is called the *minimal polynomial* for α. Theorem 2.5 shows that the minimal polynomial is nothing more than the unique monic irreducible polynomial in $F[x]$ that has α as a root.

2.2.3 Now We Can Show That $\mathbb{Q}[\zeta_n]$ Is a Field

Up until now, $\mathbb{Q}[\zeta_n]$ has meant the set of rational linear combinations of ζ_n. We will now show that $\mathbb{Q}[\zeta_n]$ contains the reciprocals of all its nonzero elements.

Theorem 2.7. *Let α be algebraic over a field F, and let f be the minimal polynomial for α in $F[x]$.*

(i) *If $g(x)$ is a nonzero polynomial in $F[x]$ and $g(\alpha) \neq 0$, then $\frac{1}{g(\alpha)}$ is in $F[\alpha]$.*

(ii) *If f is the minimal polynomial for α, then $F[\alpha]$ is a vector space over F of dimension equal to the degree n of f with basis $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$.*

For more on the Euclidean algorithm in $F[x]$ (and in $\mathbb{Z}$), see Chapter 3, [19, Chapter 6], or [41, Chapter 1].

Proof. (i) Note that $f(x)$ does not divide $g(x)$ (for $g(\alpha) \neq 0$). Since $f(x)$ is irreducible, it follows that $f(x)$ and $g(x)$ are relatively prime. Now, just as in the case of $\mathbb{Z}$, one can use the Euclidean algorithm in $F[x]$ to show that the greatest common divisor of two polynomials is an $F[x]$-linear combination of the two polynomials. In other words, one can find $s(x)$ and $t(x)$ in $F[x]$ such

that $s(x)f(x)+t(x)g(x)=1$. On substituting $x=\alpha$, we see that $t(\alpha)g(\alpha)=1$. So $1/g(\alpha)=t(\alpha)$.

(ii) Write

$$f(x)=x^n+a_{n-1}x^{n-1}+a_{n-2}x^{n-2}+\cdots+a_1x+a_0\,.$$

Since $f(\alpha)=0$, we have

$$\alpha^n=-a_{n-1}\alpha^{n-1}-a_{n-2}\alpha^{n-2}-\cdots-a_1\alpha-a_0\,.$$

Thus every linear combination of powers of α may be written (by repeated substitution) in the form

$$c_0+c_1\alpha+c_2\alpha^2+\cdots+c_{n-1}\alpha^{n-1}\,.$$

It remains to show that $1,\alpha,\alpha^2,\ldots,\alpha^{n-1}$ are linearly independent over F. Suppose to the contrary that

$$b_0+b_1\alpha+b_2\alpha^2+\cdots+b_{n-1}\alpha^{n-1}=0\,,$$

with not all the b_i zero. Then by Corollary 2.6, $f(x)$ must divide the polynomial

$$b_0+b_1x+b_2x^2+\cdots+b_{n-1}x^{n-1}\,.$$

However, that is absurd, since $f(x)$ has degree n and $b_0+b_1x+b_2x^2+\cdots+b_{n-1}x^{n-1}$ has degree less than n. Hence we have established all assertions. ■

Corollary 2.8. *Let α be algebraic over a field F. Then $F[\alpha]$ is a field. That is,*

$$F[\alpha]=\left\{\frac{h(\alpha)}{g(\alpha)}\,\middle|\,h,g\in F[x],\ g(\alpha)\neq 0\right\}\,.$$

$$\begin{array}{c}F[\alpha]=F(\alpha)\\ \vert\\ F\end{array}$$

When a ring $F[a]$ turns out to be a field, we usually indicate this by employing the notation $F(a)$.

Corollary 2.9.

$\mathbb{Q}(\zeta_n)$ is a field; it contains the reciprocals of its nonzero elements. We may therefore write $\mathbb{Q}[\zeta_n]$ as $\mathbb{Q}(\zeta_n)$, the field of linear combinations of powers of ζ_n.

2.2.4 A Criterion for Irreducibility

This is just the beginning. One can go on and on, developing the entire theory of algebraic extensions. One of the early payoffs in such a program is Galois theory. However, let us limit ourselves to a clarification of the cyclotomic situation discussed earlier in Section 2.1.

In general, it is difficult to establish the irreducibility of a given polynomial in $\mathbb{Z}[x]$. One very useful criterion is due to Gotthold Eisenstein (1823–1852). It is based on a bit of modular arithmetic, which we will take up in more detail in Section 2.3. For now, here are some basic facts.

"cyclotomic" = "circle dividing."

There is a story that may be true. On being asked who he believed were the three greatest mathematicians of all time, Gauss answered, "Archimedes, Newton, and Eisenstein." The correct answer is, of course, Archimedes, Newton, and Gauss.

Preview: A Little Modular Arithmetic

Before we develop modular arithmetic systematically, let us look at a special case. Consider the prime number 7 and denote by $\mathbb{Z}_7$ the set of seven symbols $\{0, 1, 2, 3, 4, 5, 6\}$. These symbols are already familiar to you, but we can introduce new operations on them, new addition and new multiplication, so that we remain in $\mathbb{Z}_7$. For that, we use the following rule: multiply or add as like in the old days, but throw away sevens until you get back to $\mathbb{Z}_7$. For example, $5 \times 6 = 2$ (because $30 - 4 \times 7 = 2$), and $5 + 6 = 4$. The complete addition and multiplication tables are given in Figure 2.5.

You may have met these operations before. Sometimes, they are called the operations of "clock arithmetic." Why?

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

×	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Figure 2.5. Addition and multiplication tables for $\mathbb{Z}_7$.

An examination of the tables shows that $\mathbb{Z}_7$ is a field—in particular, every nonzero element has a multiplicative inverse. There are other properties that are not so evident. Take 2, for example, and begin raising it to various powers, $1, 2, 2^2, 2^3, \ldots$. One obtains $1, 2, 4, 1, 2, 4, 1, 2, 4, \ldots$, showing that $\{ 1, 2, 4 \}$ is a (cyclic) subgroup of three elements. On the other hand, beginning with 3, we have $\{ 1, 3, 3^2, 3^3, 3^4, 3^5 \} = \{ 1, 3, 2, 6, 4, 5 \}$, which is the whole set of nonzero elements in $\mathbb{Z}_7$. Because the number 3 generates the entire multiplicative subgroup of $\mathbb{Z}_7$, it is called a *primitive element*, or simply a *primitive*, modulo 7. Are there any other primitives modulo 7?

Just as with any field, we can consider the set $\mathbb{Z}_7[x]$ of formal polynomials in one variable with coefficients in $\mathbb{Z}_7$. And just as with polynomials in $\mathbb{Q}[x]$ or $\mathbb{C}[x]$, we can do arithmetic with elements of $\mathbb{Z}_7[x]$. This arithmetic supports addition and multiplication, and all the usual rules of algebra apply. In particular, it so happens that every polynomial in $\mathbb{Z}_7[x]$ can be factored into irreducible polynomials in essentially one way. It takes a little time to get used to algebra in $\mathbb{Z}_7[x]$, but you will get used to it with a little practice. For example, $x^2 - 1 = (x - 1)(x + 1)$, as always. But $x^2 - 1 = (x + 6)(x + 1)$, too. (Why is this the same factorization?) Another example: $x^2 - 2 = (x+4)(x+3)$.

The shorthand for this is that $\mathbb{Z}_7[x]$ is a *unique factorization domain*.

One of the most useful properties of this setup is in the interaction between $\mathbb{Z}_7[x]$ and $\mathbb{Z}[x]$. If f is any polynomial in $\mathbb{Z}[x]$, you can get a corresponding polynomial $\overline{f}$ by "reducing the coefficients of f modulo 7." This means replacing each coefficient in f with the remainder when that coefficient is divided by 7. So for example:

7 is just a placeholder here for any prime.

(i) $\overline{x^3 + 14x^2 + 8x + 9} = x^3 + x + 2$;

(ii) $\overline{x^3 - 12x^2 + 21x - 10} = x^3 + 2x^2 + 4$;
(iii) $\overline{x^3 - 49x^2 + 21x - 7} = x^3$;
(iv) $\overline{x^3 - 14x^2 + 28x - 7} = x^3$;
(v) $\overline{x^{100} - 14x^2 + 28x - 7} = x^{100}$;
(vi) $\overline{(x^{40} - 14x^2 + 28x - 7)(x^{60} - 42x^2 + 28x - 14)} = x^{100}$.

If you work it out, you will see that

$$\overline{(x^{40} - 14x^2 + 28x - 7)} \cdot \overline{(x^{60} - 42x^2 + 28x - 14)}$$

is also x^{100}. And it works with addition, too. Details are in the exercises.

Meanwhile, back at the ranch ... We want a test for irreducibility. As usual, we begin with an example. Consider the polynomial $x^4 + 2$ in $\mathbb{Z}[x]$. How do you know that this polynomial is irreducible? You should check that there is no linear factor. To eliminate the possibility of quadratic factors, however, requires a bit of calculation, which, although far from insurmountable, is doomed to limitation. Suppose, for example, we asked about the irreducibility of $x^{100} + 2$. Eisenstein simply viewed the equation modulo 2. In $\mathbb{Z}_2[x]$, the polynomial becomes x^{100}. If $x^{100} + 2$ were reducible, then one could write $x^{100} + 2 = f(x)g(x)$ in $\mathbb{Z}[x]$, each having positive degree less than 100 and monic. On reducing modulo 2, in $\mathbb{Z}_2[x]$ we would have

$$\overline{x^{100} + 2} = \overline{f(x)g(x)},$$

or

$$\overline{x^{100}} = \overline{f(x)}\,\overline{g(x)},$$

and since factorization is unique, we must have, *in* $\mathbb{Z}_2[x]$,

$$\overline{f(x)} = x^m \quad \text{and} \quad \overline{g(x)} = x^n, \quad 0 < m, n < 100\,.$$

Gauss showed that if a polynomial is irreducible in $\mathbb{Z}[x]$, then it is also irreducible in $\mathbb{Q}[x]$.

Lifting these equations back to $\mathbb{Z}[x]$, we see that $f(x)$ must look like $x^m + a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \cdots + a_0$, with 2 dividing all the a_i, and $g(x)$ must look like $x^n + b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \cdots + b_0$, with 2 dividing all the b_i. Thus 4 must divide $a_0 b_0$, which is impossible, because $f(x)g(x) = x^{100} + 2$.

The argument is identical if we consider $x^{100} + 2x^{47} + 12x^5 + 2$ or $x^{100} + 16x + 2$, because we only picked on a_0 and b_0 and required that the polynomial become x^{100} in $\mathbb{Z}_2[x]$. You see how powerful the criterion is. It was crucial that the constant term was 2 and not 2^2. On the other hand, it could have been 6 or $2s$ for s odd. These observations lead to the following theorem due to Eisenstein. The proof is just as simple as the example, and we leave it to you as an exercise.

Theorem 2.10 (Eisenstein's criterion). *Suppose that* $f(x) = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_0$ *is a polynomial in* $\mathbb{Z}[x]$ *and that* p *is a prime number that divides each of the* a_i *but* p^2 *does not divide* a_0. *Then* f *is irreducible in* $\mathbb{Q}[x]$.

Proof. This is Exercise 2.30. Have fun. ■

Lookout Point 2.6. Here is a famous example of how Eisenstein's criterion is applied: when p is a prime, $f(x) = x^{p-1} + x^{p-2} + \cdots + 1$ is irreducible in $\mathbb{Q}[x]$.

But there aren't any primes dividing the coefficients! A clever substitution comes to the rescue: It is enough to show that $f(x+1)$ is irreducible (as you will show in Exercise 2.31). We have seen this before for $p = 5$, but it works in general. Namely, $f(x) = \frac{x^p-1}{x-1}$. So

You will show this in Exercise 2.15.

$$f(x+1) = \frac{(x+1)^p - 1}{x} = x^{p-1} + px^{p-2} + \binom{p}{2}x^{p-3} + \cdots + p\,.$$

Each of the binomial coefficients is of the form

$$\binom{p}{j} = \frac{p(p-1)(p-2)\cdots(p-j+1)}{j!}\,,$$

where $j < p$. Look at the fraction on the right-hand side: p is a factor of the numerator, but p doesn't divide the denominator. Hence p is a factor of $\binom{p}{j}$. And p^2 is not a factor of the constant term (it is just p). So Eisenstein applies, and $f(x)$ is irreducible.

A couple of facts follow from this:

Theorem 2.11.

(i) *The minimal polynomial for ζ_p in $\mathbb{Q}[x]$ is $1 + x + x^2 + \cdots + x^{p-1}$.*

(ii) *If p is a prime, then $\mathbb{Q}[\zeta_p]$ (=$\mathbb{Q}(\zeta_p)$) is the set of all linear combinations*

$$a_0 + a_1\zeta + a_1\zeta^2 + \cdots + a_{p-1}\zeta^{p-2}$$

with coefficients a_i in $\mathbb{Q}$.

(iii) *To close a loop that we opened earlier in this section, when $p = 5$, $\mathbb{Q}(\zeta_5)$ is a vector space over $\mathbb{Q}$ with basis $1, \zeta_5, \zeta_5^2, \zeta_5^3$.*

What about a method for producing the minimal polynomial for ζ_n for any positive integer n, a polynomial that we will denote by $\Psi_n(x)$? Instead of considering all powers of ζ_n, just consider the powers ζ_n^j, where $(j,n) = 1$, that is, where j and n are relatively prime. The number of such integers is denoted by $\phi(n)$. The function ϕ ("Euler's phi function") shows up all over mathematics and has some beautiful properties. One of them is that $\phi(n) = n\prod_{p|n}\left(1 - \frac{1}{p}\right)$, where the product is over all primes dividing n. The minimal polynomial for ζ_n turns out to be

$$\Psi_n(x) = \prod_{(j,n)=1}\left(x - \zeta_n^j\right)\,.$$

Take heart. We'll prove both of these statements in the Supplement to Chapter 4.

It is not obvious that this polynomial is in $\mathbb{Z}[x]$, but it is. Even less obvious is that it is irreducible in $\mathbb{Z}[x]$. But it is.

Lookout Point 2.7. You should notice that $1 + x + x^2 + \cdots + x^n$ is not irreducible for general n. It is irreducible when $n = p - 1$ for a prime p, as we have just seen. But consider

This is a beautiful example, one that can be mined to illustrate the power of unique factorization in $\mathbb{Q}[x]$.

$$1 + x + x^2 + x^3 + x^4 + x^5 = \frac{x^6 - 1}{x - 1}.$$

You can factor $x^6 - 1$ in two ways: as a difference of squares or a difference of cubes:

$$x^6 - 1 = \left(x^3\right)^2 = \left(x^3 - 1\right)\left(x^3 + 1\right) = (x - 1)(x^2 + x + 1)(x + 1)(x^2 - x + 1),$$
$$x^6 - 1 = \left(x^2\right)^3 = \left(x^2 - 1\right)\left(x^4 + x^2 + 1\right) = (x - 1)(x + 1)\left(x^4 + x^2 + 1\right).$$

Either way, $1 + x + x^2 + x^3 + x^4 + x^5$ is not irreducible. And there's more: Comparing the two factorizations and invoking unique factorization, we must have

$$\left(x^4 + x^2 + 1\right) = \left(x^2 + x + 1\right)\left(x^2 - x + 1\right).$$

This could be computed directly by expanding the right-hand side and watching things fall away. Or you can recognize that the left-hand side is a "difference of squares in disguise":

$$x^4 + x^2 + 1 = \left(x^4 + 2x^2 + 1\right) - x^2.$$

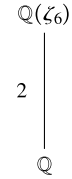
One moral of the story: It may seem natural to assume that $x^4 + x^2 + 1$ must be irreducible because $h(x) = x^2 + x + 1$ is, and the quartic is just $h(x^2)$. But the implication goes only one way: if $p(x)$ is a *reducible* polynomial in $\mathbb{Q}[x]$, then so is $p(x^n)$ for every positive integer n, as can be seen by a substitution. But if $p(x)$ is *irreducible*, then all bets are off regarding $p(x^n)$. It may or may not factor.

Meanwhile, back at the ranch ... Because ζ_6 satisfies

$$(x + 1)\left(x^2 + x + 1\right)\left(x^2 - x + 1\right) = 0,$$

we see that $[\mathbb{Q}[\zeta_6] : \mathbb{Q}] < 5$. In fact, thanks to de Moivre, $\zeta_6 = \frac{1}{2} + i\frac{\sqrt{3}}{2}$, so ζ_6 and its conjugate are roots of $x^2 - x + 1 = 0$ (check this), and the minimal polynomial for ζ_6 over $\mathbb{Q}$ is thus $x^2 - x + 1$.

The dimension of $\mathbb{Q}[\zeta_6]$ as a vector space over $\mathbb{Q}$ is called the *degree* of the extension. We denote this degree by $[\mathbb{Q}[\zeta_6] : \mathbb{Q}]$ and decorate the field tower diagram like this:



As a final example, let us consider the problem of constructing a regular 7-gon with ruler and compass. As we did with the pentagon, let $\zeta = \cos\frac{2\pi}{7} + i\sin\frac{2\pi}{7}$, so that the regular unit heptagon inscribed in the unit circle in the complex plane looks like Figure 2.6.

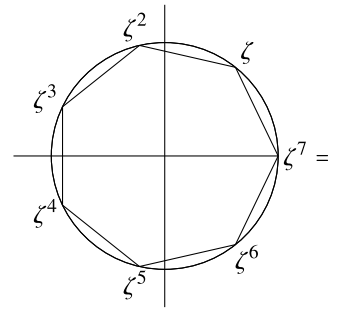


Figure 2.6. The regular unit heptagon.

Just as we did in equation (2.7), let us look for the numerical value of the real part of ζ; that is, look at $\zeta + \zeta^{-1} = 2\cos\frac{2\pi}{7}$. It's the same drill: Start with our favorite relation

$$1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4 + \zeta^5 + \zeta^6 = 0\,.$$

On dividing through by ζ^3, we obtain

$$\zeta^{-3} + \zeta^{-2} + \zeta^{-1} + 1 + \zeta + \zeta^2 + \zeta^3 = 0,$$

or

$$\zeta^3 + \zeta^{-3} + \zeta^2 + \zeta^{-2} + \zeta + \zeta^{-1} + 1 = 0\,.$$

It begins to look suspiciously as though $\zeta + \zeta^{-1}$ satisfies a cubic polynomial. In fact,

$$\left(\zeta + \zeta^{-1}\right)^3 = \zeta^3 + \zeta^{-3} + 3\left(\zeta + \zeta^{-1}\right)$$

and

$$\left(\zeta + \zeta^{-1}\right)^2 = \zeta^2 + \zeta^{-2} + 2,$$

and solving these two equations for $\zeta^3 + \zeta^{-3}$ and $\zeta^2 + \zeta^{-2}$ respectively and substituting in the above gives

$$\left(\zeta + \zeta^{-1}\right)^3 - 3\left(\zeta + \zeta^{-1}\right) + \left(\zeta + \zeta^{-1}\right)^2 - 2 + 1 = 0,$$

or

$$\left(\zeta + \zeta^{-1}\right)^3 + \left(\zeta + \zeta^{-1}\right)^2 - 2\left(\zeta + \zeta^{-1}\right) - 1 = 0\,.$$

Hence $\zeta + \zeta^{-1}$ is a root of the cubic

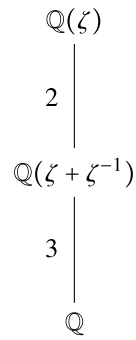
$$x^3 + x^2 - 2x - 1\,.$$

Hint: Do you recall the rational root theorem from high-school algebra?

You can show that this cubic is irreducible.

Thus $\mathbb{Q}\left(\zeta + \zeta^{-1}\right)$ is a vector space of dimension 3 over $\mathbb{Q}$. Since $\mathbb{Q}(\zeta)$ is of dimension 6 over $\mathbb{Q}$ (because $1 + x + x^2 + \cdots + x^6$ is irreducible), the rest of the extension, that is, $\mathbb{Q}(\zeta)$ over $\mathbb{Q}(\zeta + \zeta^{-1})$, must be quadratic (see Exercise 2.38).

So, we have a field tower



Now for the punchline. Exercise 2.13 implies that a segment whose length is a quadratic irrationality (resulting in an extension of degree 2) can be constructed with ruler and compass. A succession of such constructions always results in a field of degree 2^n over $\mathbb{Q}$. And it can be shown (see [19, Chapter 7], for example) that this is the whole story: a length can be constructed with ruler and compass if and only if it lies in an extension of degree 2^n for some integer n. The side length of a regular heptagon results in an extension of degree 3. Hence the heptagon cannot be constructed with ruler and compass.

Many details are missing here, but this is the basic idea.

Incidentally, the other roots of $x^3+x^2-2x-1=0$ are $\zeta^3+\zeta^{-3}$ and $\zeta^2+\zeta^{-2}$ (check this). Thus we have constructed a cubic polynomial that is irreducible and has three real roots. Can you think of an easier way to find an irreducible cubic with three real roots?

Lookout Point 2.8. When Gauss was seventeen years old, he showed that it is possible to construct a regular 17-gon with ruler and compass; in fact, he outlined a method for carrying out the construction. A wonderful video shows David Eisenbud actually carrying out the steps.[1]

Later, Gauss showed that a regular polygon with p sides is constructible if p is a so-called *Fermat prime*—a prime of the form 2^n+1 (such as 5 and 17).

More details are in [19, Chapter 7].

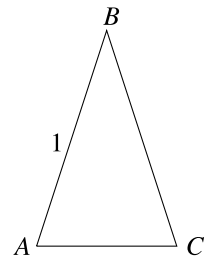
We met Fermat primes before in the discussion after equation (2.10).

Exercises

2.13 If n is a positive integer, show how to construct a segment of length $\sqrt{n}$ with ruler and compass.

2.14 In the figure below, $\triangle ABC$, $AB = BC = 1$, and the measure of $\angle B$ is $36°$. Find AC.

[1] Available at https://youtube.com/watch?v=87uo2TPrsl8.



2.15 Show that if n is a positive integer, then $\frac{x^n-1}{x-1} = 1 + x + x^2 + \cdots + x^{n-1}$ in $\mathbb{Q}[x]$.

Hint: Use the result of Exercise 2.15.

2.16 Find the value of

$$\sum_{k=0}^{20} 3^k .$$

2.17 Let $f(n) = a + ar + ar^2 + \cdots + ar^n$, where n is a positive integer and a and r are real numbers. Use the result of Exercise 2.15 to find a closed-form formula for $f(n)$.

2.18 What is the side length of a unit regular pentagon. How would you construct it?

2.19 Find the length of a side of a regular decagon inscribed in the unit circle.

2.20 Show that the only automorphisms of $\mathbb{Q}(\sqrt{d})$ are the identity and the mapping that sends $a + b\sqrt{d}$ to $a - b\sqrt{d}$, and these two mappings form an abelian group of order 2.

2.21 Show that partial sums of

$$1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cdots}}}$$

It's a small world after all.

are the ratios of consecutive Fibonacci numbers.

2.22 In Section 2.2.1, we stated that in $\mathbb{Q}(\zeta_5)$, addition and multiplication are commutative and that all the usual rules of high-school algebra hold. Prove this.

2.23 Establish the formal identity

$$\left(x^2 + y^2\right)^2 = \left(x^2 - y^2\right)^2 + (2xy)^2 .$$

Replace x and y by some integers and describe what you get.

2.24 Show that

$$\left(\zeta_5^3 - \zeta_5^2 + 2\zeta_5\right)\left(7\zeta_5^3 + 9\zeta_5^2 + 8\zeta_5 + 3\right) = -1 .$$

2.25 Are there any polynomials in $\mathbb{Q}[x]$ that have reciprocals in $\mathbb{Q}[x]$?

2.26 Using polynomial arithmetic, characterize the set of polynomials in $\mathbb{Q}[x]$ that produce the same complex number when x is replaced by ζ_5.

2.27 Let $\alpha = \zeta_5^4 + \zeta_5$. Express $1/\alpha$ as a polynomial in ζ_5.

2.28 Find the minimal polynomial for ζ_8 in $\mathbb{Q}[x]$. How about ζ_9? How about $\sqrt{2}$? Oh, and don't forget $\sqrt{2}+\sqrt{3}$. Try some other interesting algebraic numbers.

2.29 Suppose p is a prime and f and g are polynomials in $\mathbb{Z}[x]$ Let $\bar{f}$ be the polynomial in $\mathbb{Z}_p[x]$ that you get when you reduce all the coefficients of f modulo p. Show that

(i) $\overline{f+g} = \bar{f} + \bar{g}$

(ii) $\overline{fg} = \bar{f} \cdot \bar{g}$

2.30 Prove Eisenstein's criterion (Theorem 2.10).

2.31 Show that a polynomial $f(x) \in \mathbb{Z}[x]$ is irreducible if and only if $f(x+1)$ is irreducible.

2.32 Show that

$$\frac{(x+1)^p - 1}{x} = x^{p-1} + px^{p-2} + \binom{p}{2}x^{p-3} + \cdots + p\,.$$

2.33 Let $\zeta = \zeta_5$. Express each of these numbers in $\mathbb{Q}(\zeta)$ as a linear combination of the basis $\{1, \zeta, \zeta^2, \zeta^3\}$:

(i) ζ^4

(ii) ζ^{-4}

(iii) ζ^{58}

(iv) $2\zeta^7$

(v) $2\zeta^7 + \zeta^{58} + \frac{1}{\zeta^{58}}$

(vi) more like these ...

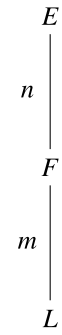
2.34 Give an example of a polynomial $p(x)$ in $\mathbb{Q}[x]$ with the property that $p(x)$ and $p(x^2)$ are both irreducible.

2.35 Calculate $\phi(n)$ for $n = 1, \ldots, 50$. Or go higher, just for fun. Conjecture some properties of ϕ. Prove some of them.

2.36 Can you show that $1 - x^2 + x^4$ is irreducible directly without using the fact that it is the minimal polynomial for ζ_{12}? Go ahead.

2.37 Show that $x^3 + x^2 - 2x - 1$ is irreducible in $\mathbb{Q}[x]$.

2.38 Show that in a field tower with degrees like this:



the degree of E over L is mn.

2.39 Show that it is impossible to construct (with ruler and compass) a cube with twice the volume of a given cube.

2.40 **Take It Further.** If n is a nonnegative integer, how many irreducible factors in $\mathbb{Z}[x]$ does $x^n - 1$ have? (Fill in the table below to gather some data.)

n	Number of Irreducible Factors of $x^n - 1$
1	1
2	2
3	2
4	
5	2
6	
7	
8	
9	
10	
11	
12	

2.3 Modular Arithmetic

A complete development of quadratic reciprocity can be found in [41, Chapter 5]. It requires some background from the earlier parts of that book.

Caution: The standard notation for the finite field of integers modulo p is $\mathbb{Z}/p\mathbb{Z}$. It would make a long digression to describe the motivation for this, so we have adopted the nonstandard $\mathbb{Z}_p$. See [19, Chapter 7] for details.

In this section we'll show how the algebra of the last section can be extended to mod p considerations and give special cases of a famous result due to Gauss called the law of quadratic reciprocity. We won't be able to prove this result, but you will acquire some experimental familiarity with it.

You met the finite fields $\mathbb{Z}_p$ in Section 2.2.4. We used $p = 7$, but any prime will do. Carrying on with the questions asked there, another important question to ask is this: what are the squares in $\mathbb{Z}_7$? On squaring everything nonzero, we get $\{1, 4, 2\}$, and so these are the three squares.

Note that 2, which isn't a square in $\mathbb{Z}$, is a square in $\mathbb{Z}_7$. However, in $\mathbb{Z}_5$, the squares are $\{1, 4\}$, and 2 is not a square. How can one tell when 2 is a square in $\mathbb{Z}_p$? How about the set of all primes p for which 2 is a square in $\mathbb{Z}_p$? Is it infinite? Do they have a pattern? For the answers to these and many other really interesting questions, continue reading.

The more general issue concerning "reciprocity" is simply the following. If p and q are distinct primes, is there any relationship between p being a

square in $\mathbb{Z}_q$ and q being a square in $\mathbb{Z}_p$?

Back up a bit and fix a prime p. How does one know that $\mathbb{Z}_p$ is a field? If $a \in \mathbb{Z}_p$ is not 0, we must show that there is an element b in $\mathbb{Z}_p$ such that $ab = 1$ (recall that = means equality in $\mathbb{Z}_p$). But if $a \neq 0$, then (since $1 \leq a \leq p-1$) a and p have no common factor. According to a basic result due to Euclid that we will prove in Chapter 3, there exist integers x and y such that

You can check that $\mathbb{Z}_7$ is a field just by looking at its tables for addition and multiplication. But you wouldn't want to use that method for $\mathbb{Z}_{101}$.

$$ax + py = 1\,.$$

But that just means that $ax = 1$ in $\mathbb{Z}_p$ (if x happens to be outside the range $1, \ldots, p-1$, just take x mod p).

This argument proves that $\mathbb{Z}_p$ is a field, and that deserves to be celebrated in a theorem.

Theorem 2.12. *If p is a prime, then $\mathbb{Z}_p$ is a field—every nonzero element of $\mathbb{Z}_p$ has a multiplicative inverse in $\mathbb{Z}_p$.*

Next, string out the elements of

$$\mathbb{Z}_p - \{0\} = \{\, 1, 2, 3, \ldots, p-1 \,\}$$

and consider $\{\, a, 2a, 3a, \ldots, a(p-1) \,\}$, $a \neq 0$ in $\mathbb{Z}_p$. The second sequence is the same as the first! Hence

Prove that the two sequences are the same using the fact that $\mathbb{Z}_p$ is a field.

$$1 \cdot 2 \cdot 3 \cdot 4 \cdots (p-1) = a \cdot 2a \cdot 3a \cdot a(p-1) = a^{p-1}\big(1 \cdot 2 \cdot 3 \cdots (p-1)\big)\,.$$

Canceling gives the basic result of modular arithmetic, due to Pierre de Fermat (1607?–1665), as stated in the following theorem.

Theorem 2.13 (Fermat's little theorem). *If $a \neq 0$ in $\mathbb{Z}_p$, then $a^{p-1} = 1$ in $\mathbb{Z}_p$. Equivalently, if $a \in \mathbb{Z}$, $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$. In other words, p divides $a^{p-1} - 1$.*

There's another very famous theorem associated with Fermat: *Fermat's last theorem*. That wasn't proved until the 1990s (not by Fermat, of course). See [19] for some of the history.

Using group theory, a bit of which we shall review later in this chapter, we could have proved Theorem 2.13 more compactly as follows: Since $\mathbb{Z}_p$ is a field, $\mathbb{Z}_p - \{0\}$ is a multiplicative group of order $p-1$. By Lemma 2.25, $a^{p-1} = 1$ for all $a \in \mathbb{Z}_p - \{0\}$.

Sometimes the theorem is stated in the form "if $a \in \mathbb{Z}_p$, then $a^p = a$ in $\mathbb{Z}_p$." Or equivalently, "if $a \in \mathbb{Z}$, then $a^p \equiv a \pmod{p}$." And another formulation is worthy of statement as a corollary:

Corollary 2.14. *If p is prime, then in $\mathbb{Z}_p[x]$,*

$$x^{p-1} - 1 = (x-1)(x-2)\cdots(x-(p-1))\,.$$

The next, equally important, result is called the theorem on the primitive element. It was conjectured by Euler and used in his investigations, but although it isn't very hard, the proof had to wait until Gauss came along. It

is the generalization of the fact that $\mathbb{Z}_7 = \{3, 3^2, \ldots, 3^6\}$. Namely, there is an element $\rho \in \mathbb{Z}_p$ such that

$$\mathbb{Z}_p^* = \{1, \rho, \rho^2, \ldots, \rho^{p-2}\}.$$

Recall that $\mathbb{Z}_p^* = \mathbb{Z}_p - \{0\}$.

Let us assume this result for a while, as Euler did, and using arguments like those in the previous section, derive some interesting results. A proof will show up soon, in Section 2.5.

The following observation is basic: Suppose n divides $p-1$. Since $\mathbb{Z}_p^*$ is cyclic, we can find a generator ρ as above. Then $\rho^{(p-1)/n} = \xi$ is an element of $\mathbb{Z}_p^*$ that generates a cyclic subgroup of order n, namely

$$\{1, \xi, \xi^2, \ldots, \xi^{n-1}\}.$$

For example, $3^{\frac{7-1}{3}} = 3^2 = 2$ should generate a subgroup with three elements. And it does: $\{1, 2, 4\}$.

Let's return to the argument we used to construct the regular pentagon and see how one adapts this to $\mathbb{Z}_p$. Suppose that 5 divides $p-1$. Then one can find an element in $\mathbb{Z}_p$, call it ζ, such that $\zeta^5 = 1$ and $\zeta \neq 1$. Then $\mathbb{Z}_p$ has the five *distinct* elements $1, \zeta, \zeta^2, \zeta^3, \zeta^4$. It follows that

$$\zeta^{-1} = \zeta^4, \quad \zeta^{-2} = \zeta^3, \quad \zeta^{-3} = \zeta^2,$$

Caution: This is not a rerun of what we did earlier—this all happens in $\mathbb{Z}_p$.

where ζ^{-1}, ζ^{-2}, and ζ^{-3} make perfectly good sense, since $\mathbb{Z}_p$ is a field. Then just as before (equation (2.9) in Section 2.2), because

$$\zeta^5 - 1 = (\zeta - 1)\left(1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4\right) = 0,$$

we have

$$1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4 = 0$$

and

$$\left(\zeta + \zeta^{-1}\right)^2 = \zeta^2 + \zeta^{-2} + 2 = 1 - \left(\zeta + \zeta^{-1}\right).$$

Hence

$$\left(\zeta + \zeta^{-1}\right)^2 + \left(\zeta + \zeta^{-1}\right) - 1 = 0.$$

Hence $\zeta + \zeta^{-1}$ satisfies the quadratic equation

$$x^2 + x - 1 = 0.$$

Now the question is this: can we solve this quadratic equation in $\mathbb{Z}_p$? Sure, because $p \neq 2$ implies that 2 has an inverse mod p. Call it $\frac{1}{2}$. Then

But notice that in $\mathbb{Z}_7$, $\frac{1}{2}$ is 4, and in $\mathbb{Z}_{11}$, $\frac{1}{2}$ is 6.

$$x^2 + x - 1 = \left(x + \frac{1}{2}\right)^2 - \frac{5}{4}.$$

Hence in $\mathbb{Z}_p$, we have

$$x = -\frac{1}{2} \pm \frac{\sqrt{5}}{2}.$$

In any event, $\sqrt{5}$ is in $\mathbb{Z}_p$(!) That means that 5 is a square in $\mathbb{Z}_p$. The condition on p was that $p \equiv 1 \bmod 5$.

Legendre introduced the following notation for this kind of statement. If $a \neq 0$ and a is a square in $\mathbb{Z}_p$, then one writes $\left(\frac{a}{p}\right) = +1$. If a is not a square modulo p, one writes $\left(\frac{a}{p}\right) = -1$. Using this *Legendre symbol*, we can phrase the above statement as the following theorem.

Theorem 2.15. *If* $p \equiv 1 \bmod 5$, *then* $\left(\frac{5}{p}\right) = +1$.

Lookout Point 2.9. Theorem 2.15 can be stated in a slightly different way. The statement amounts to $p - 1 = 5t$, or $p = 5t + 1$. In other words, the primes congruent to 1 modulo 5 are just the primes in the arithmetic progression $\{5t + 1 \mid t \in \mathbb{Z}\}$, which consists of the integers $1, 6, 11, 16, 21, 26, 31, \ldots$. Our result says that 5 is a square modulo each prime p in that sequence (check this out for a few primes).

Results of this type were arrived at experimentally by Fermat already in the early 1640s.

An interesting question: How many prime numbers are there in the progression $1, 6, 11, 16, 21, \ldots$? If there were infinitely many primes, then 5 would be a square in $\mathbb{Z}_p$ for infinitely many p. See Section 2.4 for more on the story.

Another slight variation points to another interesting question: to say that 5 is not a square in $\mathbb{Z}_p$ is simply to say that $x^2 - 5$ is irreducible in $\mathbb{Z}_p[x]$. For example, $x^2 - 5$ is irreducible in $\mathbb{Z}_7[x]$; that is, it cannot be factored into linear polynomials in $\mathbb{Z}_7[x]$. On the other hand, $x^2 - 5$ is reducible in $\mathbb{Z}_{11}[x]$. In fact, $x^2 - 5 = (x - 4)(x - 7)$. Indeed, 4 and 7 are the two square roots of 5 in $\mathbb{Z}_{11}$. In general, it is very difficult to know when a polynomial with integer coefficients is reducible modulo p for a prime p.

Notice that $7 + 4 = 0$ in $\mathbb{Z}_{11}$. What is the sum of the roots of $x^2 - 5$ in $\mathbb{Z}_p[x]$ for any prime p?

2.3.1 Quadratic Reciprocity

We showed above that if $p \equiv 1(5)$, then 5 is a square mod p. When is p a square mod 5? The squares in $\mathbb{Z}_5$ are 1 and -1, so if p is a square mod 5, then we must have $p \equiv \pm 1(5)$. Is there a reciprocity here? That is, if $p \equiv -1(5)$, is 5 also a square mod p? More generally, if p and q are primes, what the relationship between $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$?

The condition $p \equiv \pm 1(5)$ is that p be of the form $5k + 1$ or $5k + 4$.

The answer, the *law of quadratic reciprocity*, is one of the most beautiful results in arithmetic. It has several parts, so we state them one at a time:

Theorem 2.16 (Odd primes). *Let* p *and* q *be distinct* odd *primes. If* p *or* q *is congruent to* 1 *modulo* 4, *then* p *is a square modulo* q *exactly when* q *is a square modulo* p. *If both are congruent to* 3 *modulo* 4, *then* p *is a square in* $\mathbb{Z}_q$ *if and only if* q *is not a square in* $\mathbb{Z}_p$.

Why does 4 play such an important role? That's connected to arithmetic in the "Gaussian integers," which we take up in Chapter 3.

You should test some cases and show that the above statement can be written in the nicely symmetric form

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}.$$

$(\mathbb{Z}_p^*)^2$ means (as the notation suggests) the set of squares in $\mathbb{Z}_p^*$.

Lookout Point 2.10. Here is one way to think about this. Say that two odd primes p and q have "positive reciprocity" if

$$p \in \left(\mathbb{Z}_q^*\right)^2 \iff q \in \left(\mathbb{Z}_p^*\right)^2 .$$

"Negative reciprocity" means (no surprise)

$$p \in \left(\mathbb{Z}_q^*\right)^2 \iff q \notin \left(\mathbb{Z}_p^*\right)^2 .$$

Then quadratic reciprocity for odd primes can be summarized in a table:

Prime type	$4n+1$	$4n+3$
$4n+1$	+	+
$4n+3$	+	−

Theorem 2.16 was first proved by Gauss (of course) in his masterwork *Disquisitiones Arithmeticae* [29], a book that laid the foundation for modern number theory. He loved the result so much that he gave eight proofs over his career, including one that uses geometry. A complete proof can be found in [41].

See Chapter 7 of [15] for a geometric proof, essentially due to Eisenstein.

Theorem 2.16 answers the question for p and q both odd. What happens if one of the primes is 2? The question as to when 2 is a square in $\mathbb{Z}_p$ can be partially answered by appealing to the octagon.

Suppose that 8 divides $p-1$. By the theorem on the primitive element, there is an element ζ in $\mathbb{Z}_p$ such that $\zeta^8 = 1$ and no lower positive power is 1. Then $(\zeta^4)^2 = 1$, so $\zeta^4 = \pm 1$. Since $\zeta^4 = 1$ is excluded, we conclude that $\zeta^4 = -1$. Then just as before,

$$\left(\zeta + \zeta^{-1}\right)^2 = \zeta^2 + \zeta^{-2} + 2 = 2 . \tag{2.11}$$

(This is Exercise 2.47.) Hence $\zeta + \zeta^{-1}$ is an element of $\mathbb{Z}_p$ whose square is 2. What have we shown?

Lemma 2.17. *If* $p \equiv 1(8)$, *then* $\left(\frac{2}{p}\right) = +1$.

For example, take $p = 17$. Then $17 \equiv 1(8)$, so $\left(\frac{2}{17}\right) = +1$. Indeed, $6^2 = 36 \equiv 2(17)$. A good exercise is to find a primitive ζ modulo 17 and show that $\zeta + \zeta^{-1}$ must be either 6 or 11. (This is Exercise 2.46.)

Again, the details are in [41].

The complete answer about the nature of 2 is given by the following theorem.

Theorem 2.18 (The quadratic character of 2). 2 *is a square in* $\mathbb{Z}_p^*$ *if and only if* $p \equiv \pm 1(8)$.

Another useful part of the story concerns the quadratic nature of -1. For which primes p is -1 a square in $\mathbb{Z}_p$?

Suppose that p is a prime and that for some integer a, $-1 = a^2$ in $\mathbb{Z}_p$. A clever idea: raise both sides to the $\frac{p-1}{2}$ power and use Theorem 2.13:

$$(-1)^{\frac{p-1}{2}} = (a^2)^{\frac{p-1}{2}} = a^{p-1} = 1 .$$

This is an equation in $\mathbb{Z}_p$.

Now, in $\mathbb{Z}$, we know that $(-1)^{\frac{p-1}{2}} = \pm 1$. And as long as $p \neq 2$, we have $-1 \neq 1$ in $\mathbb{Z}_p$, so in $\mathbb{Z}$, we must have

-1 is already a square in $\mathbb{Z}_2$, so we can assume that $p \neq 2$.

$$(-1)^{\frac{p-1}{2}} = 1\,.$$

This implies that $\frac{p-1}{2}$ is even, and this implies that $p \equiv 1(4)$ (why?), from which the next lemma follows.

Lemma 2.19.

$$\left(\frac{-1}{p}\right) = 1 \implies p \equiv 1(4)\,.$$

And conversely, -1 is a square for *all* primes that are congruent to 1 mod 4. One way to see this is to use Corollary 2.14. A numerical example gives the basic idea. Suppose, for example, that $p = 29$. Then in $\mathbb{Z}_{29}[x]$, we have

$$\begin{aligned} x^{28} - 1 &= \left((x^4)^7 - 1\right) \\ &= (x^4 - 1)\left((x^4)^6 + (x^4)^5 + (x^4)^4 + (x^4)^3 + (x^4)^2 + x^4 + 1\right) \\ &= (x^2 - 1)(x^2 + 1)\left((x^4)^6 + \cdots + 1\right)\,. \end{aligned}$$

And by Corollary 2.14, the distinct roots of $x^{28} - 1 = 0$ are the nonzero elements of $\mathbb{Z}_{29}$, namely $1, 2, 3, \ldots, 28$. Hence one (in fact two) of these elements must satisfy $x^2 + 1 = 0$.

What makes this work is that $x^2 + 1$ is a factor of $x^{28} - 1$. That depends on the fact that $29 - 1$ is divisible by 4. So we have the converse of lemma 2.19:

Lemma 2.20.

$$p \equiv 1(4) \implies \left(\frac{-1}{p}\right) = 1\,.$$

Putting the lemmas together, we have a pretty result:

Theorem 2.21 (The quadratic character of -1).

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}\,.$$

Theorems 2.16, 2.18, and 2.21 combine to the give several parts of the law of quadratic reciprocity:

Theorem 2.22 (The Law of Quadratic Reciprocity).

(i) *If p and q are odd primes, then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}\,.$$

(ii) *If p is an odd prime, then* $\left(\frac{2}{p}\right) = 1 \iff p \equiv \pm 1(8)$.

(iii) *If p is an odd prime, then* $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

(iv) $\left(\frac{-1}{2}\right) = 1$.

Exercises

2.41 Find a generator for $\mathbb{Z}_p^*$ if

(i) $p = 11$
(ii) $p = 17$
(iii) $p = 37$
(iv) $p = 101$
(v) $p = 109$
(vi) $p = 1009$

2.42 Find $\sqrt{5}$ in $\mathbb{Z}_{11}$ and in $\mathbb{Z}_{101}$.

2.43 **Take It Further.** Find $\sqrt{5}$ in $\mathbb{Z}_{1011}$.

2.44 Using the notation from Section 2.2.4, show that if a monic polynomial f is reducible in $\mathbb{Z}[x]$, then $\overline{f}$ is reducible in $\mathbb{Z}_p[x]$ for every prime p.

2.45 Show that if p is a prime and $p \equiv 1(8)$, then there is an element ζ in $\mathbb{Z}_p$ such that $\zeta^8 = 1$.

2.46 Find a primitive ζ in $\mathbb{Z}_{17}$ and show that $\zeta + \zeta^{-1}$ is either 6 or 11.

2.47 Using the notation of equation (2.11), show that

$$\left(\zeta + \zeta^{-1}\right)^2 = \zeta^2 + \zeta^{-2} + 2 = 2\,.$$

2.48 Prove Corollary 2.14.

2.49 Prove Lemma 2.20.

2.50 Let p be prime.

(i) Show that the product of two nonsquares in $\mathbb{Z}_p^*$ is a square in $\mathbb{Z}_p^*$.
(ii) (Euler) If u and v are nonzero integers, show that

$$\left(\frac{u}{p}\right)\left(\frac{v}{p}\right) = \left(\frac{uv}{p}\right).$$

2.51 (Euler) Suppose p is an odd prime and $p \nmid a$. Show that in $\mathbb{Z}_p$,

$$\left(\frac{a}{p}\right) = -1^{\left(\frac{p-1}{2}\right)}.$$

2.52 Prove Wilson's theorem: If p is a prime, then

$$(p-1)! \equiv -1(p)\,.$$

2.4 Supplement: Dirichlet's Theorem on Primes in Arithmetic Progression

In Lookout Point 2.9, we asked about the number of primes in the sequence

$$1,\ 6,\ 11,\ 16,\ 21,\ 26,\ 31,\ \ldots\,.$$

An examination of a large portion of this progression might suggest to the optimist that there are infinitely many such primes. This is indeed the case, but the proof is far from trivial. More generally, consider an arbitrary arithmetic progression a, $a+b$, $a+2b, \ldots$, where a and b have no common factor. Peter Gustav Lejeune Dirichlet (1805–1859) proved in the 1830s that such an arithmetic progression contains infinitely many primes. His proof was a great triumph of complex analytic machinery, and it established Dirichlet as the leading mathematician in the world. He assumed Gauss's chair at the time of the latter's death in 1855. While Dirichlet's proof is well beyond the scope of this book, it will come as a pleasant surprise that we can, with the aid of our results on the "modular" fifth roots of unity and a simple fact from group theory, establish the result for the $5n+1$ sequence $1, 6, 11, 16, 21, \ldots$.

A complete proof of Dirichlet's theorem can be found in [41].

In order to motivate the proof, recall the famous Euclidean argument for the existence of infinitely many primes. If $p_1, \ldots, p_s$ are distinct primes, consider their product increased by 1: $p_1 \cdots p_s + 1$. By the fundamental theorem of arithmetic, this integer has a prime divisor, say p. Then p must be distinct from $p_1, \ldots, p_s$. (Why?) This gives a new prime.

See Exercise 2.53.

In order to generalize this argument to our situation, we step back a bit and look at Euclid's argument from a higher vantage point. Euclid asserts that the progression $1, 3, 5, 7, 11, \ldots$ of all odd numbers contains infinitely many primes. The number that makes the argument work, $p_1 \cdots p_s + 1$, is the value of $p_1 \cdots p_s$ when it is substituted into the polynomial $x+1$. Thinking of cyclotomic integers and polynomials (a bit of a stretch), note that

$$x + 1 = \frac{x^2 - 1}{x - 1}\,.$$

For the $5n+1$ sequence $1, 6, 11, 16, 21, \ldots$, we use a similar argument, this time with the polynomial

$$\frac{x^5 - 1}{x - 1} = 1 + x + x^2 + x^3 + x^4\,.$$

Now begin as above. Suppose $p_1, \ldots, p_s$ are s distinct primes all of the form $5n+1$. Our goal is to find another prime, distinct from $p_1, \ldots, p_s$, of the form $5n+1$.

To that end, we form the product

You will see in a minute why we need to toss in 5.

$$\alpha = 5p_1 p_2 \cdots p_s$$

and let $\xi = 1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4$. This is a big integer, and so it of course has at least one prime divisor; call it p. We are going to show that p is the desired new prime.

First, we will show that p is of the form $5n+1$. Since p divides $1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4$, it follows that in $\mathbb{Z}_p$,

$$1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4 = 0\,.$$

Therefore, α is a root in $\mathbb{Z}_p$ of $x^5 - 1 = (x-1)\left(1 + x + x^2 + x^3 + x^4\right)$.

We must show that $\alpha \neq 1$ in $\mathbb{Z}_p$. If such were the case, we would have $1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4 = 1 + 1 + 1 + 1 + 1 = 0$, which holds in $\mathbb{Z}_p$ only for $p = 5$.

But by the construction of α, we have $\xi \equiv 1 \pmod 5$, so $5 \nmid \xi$, whence $p \neq 5$, and so $\alpha \neq 1$ in $\mathbb{Z}_p$.

It follows that α is one of the other roots, and so $1, \alpha, \alpha^2, \alpha^3, \alpha^4$ are distinct elements of $\mathbb{Z}_p^*$, forming a subgroup of five elements. Now recall that if H is a subgroup of order h in a group G of order n, then h is a factor of n. This too is proved in Section 2.5.

It follows that 5 divides $p-1$, which is precisely the condition for p to be a member of the progression $1, 6, 11, 16, \ldots$.

And p is surely distinct from $p_1, \ldots, p_s$, since otherwise, it would divide α and hence divide $1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4 - \left(\alpha + \alpha^2 + \alpha^3 + \alpha^4\right)$, which is equal to 1. Thus the proof of Dirichlet's theorem is a rather nice application of roots of unity and modular arithmetic.

You should test your understanding of the argument by showing that the sequence $1, 4, 7, 10, 13, \ldots$ contains infinitely many primes. In this case, use $1 + x + x^2$.

Exercises

2.53 True or false: If $p_1, p_2, \ldots, p_n$ is the set of the first n primes, then

$$p_1 p_2 \cdots p_n + 1$$

is prime.

2.54 Show that the sequence

$$1, 4, 7, 10, 13, \ldots$$

contains infinitely many primes.

2.55 Show that there are infinitely many primes in the sequence defined by $4n + 1$:

$$1, 5, 9, 13, 17, \ldots .$$

Perhaps use the polynomial $x^2 + 1$.

2.5 A Little Group Theory

In the past several sections, we have used the language of groups. Here, we review the most elementary properties of finite groups and prove the important result on the primitive element that formed the basis of our arithmetic considerations.

It is a good idea to ameliorate the austerity with some concrete examples of your own. See [70] for inspiration.

Lookout Point 2.11. The arguments in this section are intentionally austere. We shall develop a few results in the theory of finite groups with no examples and no historical motivation. However, the arguments, as you will see, involve many of the same ideas from the first several sections.

Recall that a group is a set G equipped with a binary operation, denoted here by $\cdot$, satisfying the following axioms:

(i) $x \cdot (y \cdot z) = (x \cdot y) \cdot z$.

(ii) There is an element $e \in G$ such that $x \cdot e = e \cdot x = x$ for all x.

(iii) For every $x \in G$, there is an element $y \in G$ such that $xy = e = yx$.

Note that the operation $\cdot$ need not be commutative.

You should show that there is only one e in a group and that the element y of item (iii), which is generally denoted by x^{-1}, is also unique. Exercise 2.56 asks you to show that $xy = xw$ implies $y = w$, so that cancellation is possible.

Lemma 2.23. *Let a be an element of a finite group G. Then there is a smallest positive integer n such that $a^n = e$. If $a^m = e$ for a positive integer m, then $n \mid m$.*

Proof. Start raising a to various powers: $a, a^2, a^3, \ldots$. Since G is finite, it follows that $a^s = a^t$ for some $s \neq t$, $0 < s < t$. Hence $a^{t-s} = e$. So a to some power is e. Let n be the smallest positive power such that $a^n = e$. If $a^m = e$, then $m \geq n$. Divide n by m and use the division algorithm to write the result as $m = n\delta + \rho$, where $0 \leq \rho < n$.

The division algorithm codifies "division with remainder" for integers. Its proof can be found in Chapter 3 (Lemma 3.3).

Then $e = a^m = a^{n\delta} \cdot a^\rho$. Since $a^n = e$, this becomes $a^\rho = e$. But $0 \leq \rho < n$, so the minimality of n forces $\rho = 0$. Thus $m = n\delta$ and $n \mid m$. ∎

The n of Lemma 2.23 is called the *order* of a.

A subset H of G is called a *subgroup* if H is a group with the same operation. Let $|H|$ denote the number of elements of H. It is called the *order* of H. If a has order n, then $\{e, a, \ldots, a^{n-1}\}$ is a subgroup of G, called a *cyclic* subgroup. It has order n. (Thus the order of an element is the order of the cyclic subgroup that it generates.)

Note the overloading of the notation $|\cdot|$. We have seen it used to denote absolute value, and here it is being used both for the number of elements of a group and the minimal positive power of a group element equal to the identity.

Lemma 2.24. *If H is a subgroup of a finite group G, then the order of H divides the order of G.*

Proof. If $H = G$, we are through. Otherwise, let $a \in G$, $a \notin H$. Consider aH, the set of all ah, $h \in H$. These elements are distinct from one another, and $aH \cap H = \varnothing$, since $ah_1 = h_2$ would give $a = h_2 {h_1}^{-1} \in H$. If $aH \cup H = G$, then stop. Otherwise, let $b \in G$, $b \notin aH$, $b \notin H$, and consider bH. Then $bH \cap (aH \cup H) = \varnothing$, and bH has $|H|$ distinct elements. Keep going until you have exhausted the group. Each time, we have added $|H|$ new elements. So $|G|$ is an integer multiple of $|H|$. ∎

The sets aH are called *left cosets* of H.

Lemma 2.25. *If $a \in G$ and G is a finite group, then the order of a divides the order of G.*

Proof. $H = \{e, \ldots, a^{n-1}\}$ is a subgroup of G, so apply the preceding lemma. ∎

Earlier in this section, we stated and used the result due to Gauss that $\mathbb{Z}_p^*$ $(= \mathbb{Z}_p - \{0\})$, viewed as a finite multiplicative group, is cyclic. We also noticed that every finite subgroup of $\mathbb{C}^* = \mathbb{C} - \{0\}$ is also cyclic, and its elements form a regular polygon when plotted in the complex plane. That was proved with the help of de Moivre and Lemma 2.25. However, as mentioned in Section 2.1, one can establish a general result about finite subgroups of any field whatsoever: *they are always cyclic.*

To prove this, we first need a lemma on abelian groups, that is, groups in which multiplication is commutative: $xy = yx$ for all $x, y \in G$.

Lemma 2.26. *Let G be a finite abelian group and a and b two elements of orders s and t respectively. Suppose that s and t are relatively prime. Then the order of ab is $s \cdot t$.*

That $m = s_1 t_1$ follows, for example, from the fundamental theorem of arithmetic, which we will prove in Chapter 3.

Proof. Since $a^s = e$, $b^t = e$, and G is abelian, it follows that $(ab)^{st} = e$. Now let the order of ab be m. Then by Lemma 2.23, we know that $m \mid st$. Since s and t have no common factor, it follows that $m = s_1 t_1$, where $s_1 \mid s$ and $t_1 \mid t$, so that $e = (ab)^m = (ab)^{s_1 t_1}$. Then using a little fancy footwork, we have

$$e = e^{s/s_1} = \left((ab)^{s_1 t_1}\right)^{s/s_1} = (ab)^{st_1} = a^{st_1} b^{st_1} = b^{st_1}.$$

Therefore, again by Lemma 2.23, we find that $t \mid st_1$. Hence $t \mid t_1$, since s and t have no common factor. Since $t_1 \mid t$, we see that $t = t_1$. Similarly, $s = s_1$. ■

We are now ready to prove the basic result. Suppose F is a field and G a finite multiplicative subgroup of $F^* = F - \{0\}$. If n denotes the order of G, write $n = {p_1}^{\alpha_1} {p_2}^{\alpha_2} \cdots {p_m}^{\alpha_m}$, where $p_1, \ldots, p_m$ are distinct primes. Since G has order n, it follows that $\alpha^n = 1$ for each $\alpha \in G$.

By basic algebra, $x^n - 1 = \prod_{\alpha \in G} (x - \alpha)$ is in $F[x]$. If $c \mid n$, then $x^c - 1$ divides $x^n - 1$. It follows that $x^c - 1$ has c distinct roots in G. Hence for each i from 1 to m, $x^{{p_i}^{\alpha_i}} - 1$ has ${p_i}^{\alpha_i}$ roots in G. Let β_i be a root of $x^{{p_i}^{\alpha_i}} - 1$ that is not a root of $x^{{p_i}^{\alpha_i - 1}} - 1$. Then since $\beta_i^{{p_i}^{\alpha_i}} = 1$, the *order* of β_i must be a power of p_i. But that power cannot be less than α_i, or else one would get $\beta_i^{{p_i}^{\alpha_i - 1}} = 1$. Hence the order of β_i is ${p_i}^{\alpha_i}$. But ${p_1}^{\alpha_1}, \ldots, {p_m}^{\alpha_m}$ are mutually relatively prime. Hence by an inductive generalization of Lemma 2.26, we conclude that $\beta_1 \cdot \beta_2 \cdots \beta_m$ has order ${p_1}^{\alpha_1} \cdot {p_2}^{\alpha_2} \cdots {p_m}^{\alpha_m} = n$. This means that G is cyclic! This deserves to be celebrated as a theorem.

The relationship between factors and roots of polynomials shows up in high-school algebra in $\mathbb{R}[x]$, in Corollary 2.14 in $\mathbb{Z}_p[x]$, and here in $F[x]$. What makes it work in all these systems?

Theorem 2.27. *If F is a field, then every finite subgroup of F^* is cyclic.*

As a special case, we finally state the theorem that was so essential to our investigation of cyclotomy.

Theorem 2.28 (Theorem of the primitive element). *The multiplicative group of a finite field is cyclic. In particular, if p is a prime, there exists an element $\rho \in \mathbb{Z}_p$ such that*

$$\mathbb{Z}_p^* = \left\{ \rho, \rho^2, \ldots, \rho^{p-2} \right\}.$$

The first complete proof of Theorem 2.28 was given by Gauss (of course) in [29].

Incidentally, we have retrieved the existence of polygons without trigonometry. By the fundamental theorem of algebra, we know that $x^n = 1$ has n roots in $\mathbb{C}$. They form a group, so the group is cyclic. Let ζ_1 be a generator, so the group's elements are $\zeta_i = \zeta_1^i$, $i = 1, \ldots, n$. Since $\zeta_i^n = 1$, we have $|\zeta_i| = 1$ for all i, and so these n elements sit on the unit circle. Finally, $|\zeta_i - \zeta_{i+1}| = \left|{\zeta_1}^i - {\zeta_1}^{i+1}\right| = \left|{\zeta_1}^i\right||1 - \zeta_1| = |1 - \zeta_1|$, and so the ζ_i are all the same distance apart!

Recall that $|\zeta|$ denotes the absolute value of ζ.

Exercises

2.56 Show that in a group G, cancellation is possible; that is, if $xy = xw$, then $y = w$.

2.57 **True or False:** If G is a group and $x, y \in G$, then one always has $(xy)^{-1} = x^{-1} \cdot y^{-1}$. If it is true, prove it. If it is not, salvage it with a fix.

2.58 Suppose that F is a field and c, n are nonnegative integers.

(i) Show that $(x^c - 1) \mid (x^n - 1)$ in $F[x]$.

(ii) Is the converse true?

2.59 Prove all the assertions made in the proof of Lemma 2.24.

2.60 The proof of Theorem 2.27 makes several assertions. Prove them all.

2.6 Orbits and Elementary Group Theory

In 1959, Helmut Wielandt (1910–2001) published a very simple proof of a general theorem in group theory due to the Norwegian mathematician Peter Ludwig Mejdell Sylow (1832–1918) [88]. The theorem states that if n is the order of G and $p^s \mid n$ for a prime p and positive integer s, then there is a subgroup H of order p^s. The standard proofs prior to Wielandt's were considered somewhat difficult for beginners. Many textbooks on algebra and elementary group theory now contain an exposition of Wielandt's proof. In this section, we develop this point of view and prove a number of results about finite groups.

The basic notion is that of a group G *operating on a set* S. In other words, if $g \in G$ and $s \in S$, then $g(s)$ denotes an element of S. Picture it like Figure 2.7.

The group structure of G is involved in two axioms that we shall impose on the action of G on S:

The action of G on S equips G with additional structure: elements of G become *functions* with domain S and image in S.

1. In the first place, we want the identity e of G to operate on S like an identity: $e(s) = s$ for all $s \in S$.
2. Our second condition states that multiplying in G corresponds to composition of the action on S. In symbols, this is the requirement that for $g_1, g_2 \in G$, we should have

$$(g_1 \cdot g_2)(s) = g_1(g_2(s)).$$

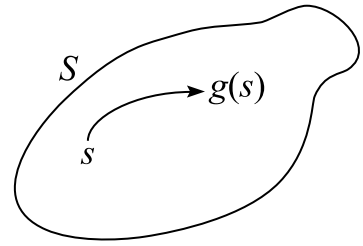


Figure 2.7. Every element $g \in G$ sends $s \in S$ to $g(s) \in S$.

We then say that G *operates* on S and that the action of G on S is *good*.

Let us give a few examples.

Example 1. Fix a set H. Let S be the set whose elements are pairs (a, b) with $a, b \in H$. For the group G we take a cyclic group with two elements, say $\{e, \sigma\}$, $\sigma^2 = e$. We shall let G operate on S according to the prescription

$$\begin{aligned} e(a,b) &= (a,b), \\ \sigma(a,b) &= (b,a). \end{aligned}$$

You should also check that $\sigma(e(a,b)) = \sigma \cdot e(ab)$, and so on.

To check that G really *operates* on S we need, by axiom 2, to see that

$$\sigma(\sigma(a,b)) = \sigma^2(a,b),$$

which is immediate, since $\sigma^2 = e$ and $\sigma(\sigma(a,b)) = \sigma(b,a) = (a,b)$.

Example 2. Do the same as above, but put

$$S = \underbrace{H \times H \times \cdots \times H}_{n},$$

and let G be a cyclic group with n elements, $G = \left\{ e, \sigma, \sigma^2, \ldots, \sigma^{n-1} \right\}$, $\sigma^n = e$. How shall G operate on S? Define

$$\begin{aligned} e(a_1, a_2, \ldots, a_n) &= (a_1, a_2, \ldots, a_n), \\ \sigma(a_1, a_2, \ldots, a_n) &= (a_n, a_1, a_2, \ldots, a_{n-1}), \\ \sigma^2(a_1, a_2, \ldots, a_n) &= (a_{n-1}, a_n, a_1, a_2, \ldots, a_{n-2}), \\ &\vdots \\ \sigma^{n-1}(a_1, a_2, \ldots, a_n) &= (a_2, a_3, a_4, \ldots, a_n, a_1). \end{aligned}$$

G cyclically permutes the elements of S.

Check that G operates on S. We shall see a little later how this simple action gives a swift proof that when p divides the order of a group G, for a prime p, then there is an element of order p in G.

Example 3. Suppose G already operates on a set T. Let S be the *set of all subsets* of T. If $A \in S$, then define $g(A) = \{ g(t) \mid t \in A \}$. Then $g(A) \in S$ and G operates on S (check this).

Example 4. This time, let G be a group and let the set that we usually call S be G as well. That is, we are going to let G operate on itself. If $g \in G$, then define $g(s) = g \cdot s \cdot g^{-1}$ for all $s \in G$. Then $e(s) = ese^{-1} = s$ for all s, and we have

$$\begin{aligned}(g_1 \cdot g_2)(s) &= (g_1 g_2)s(g_1 g_2)^{-1} = g_1 g_2 s g_2^{-1} g_1^{-1} \\ &= g_1(g_2 s g_2^{-1}) g_1^{-1} = g_1(g_2(s))\,.\end{aligned}$$

We say that G operates on G by inner automorphisms.

Example 5. Let G be any group and H a subgroup of G. We let S be the *set* of left cosets $aH = \{\, ah \mid h \in H \,\}$. The action of G on S is given by

$$g(aH) = gaH \in S\,.$$

$(g_1 \cdot g_2)(aH)$
$= g_1 \cdot (g_2 \cdot aH)$
$= g_1(g_2(aH))$.

Example 6. This is the one used in proving Sylow's theorem. Here G is a fixed group, s is a fixed positive integer, and S is the set whose *elements* are subsets consisting of p^s elements of G. If $A \in S$, then define the action by $g(A) = \{\, ga \mid a \in A \,\}$. You can show that $g(A) \in S$ and G operates on S. Try it.

Each of the above examples will be used in later applications.

If G operates on a set S, then we define the *orbit* $G(s)$ of an element $s \in S$ by $G(s) = \{\, g(s) \mid g \in G \,\}$. In Example 4, the orbit of an element a is called the *conjugacy class* of a. A basic result is the following lemma.

Lemma 2.29. *Two orbits are either identical or disjoint.*

Proof. It is enough to show that if two orbits $G(s)$ and $G(s')$ have a common element, then $G(s) = G(s')$. But if $g(s) = g'(s')$, then by definition of G operating on S, we have $s = e(s) = g^{-1}g(s) = g^{-1}g'(s')$. Hence $s \in G(s')$, and it follows that $G(s) \subset G(s')$. By symmetry, $G(s') \subset G(s)$. ∎

It follows that the action of G on S *breaks S up into disjoint orbits*. For applications, it is important to have some way of obtaining information on the number of elements in a given orbit. For example:

(i) If $g(s) = s$ for *all* $g \in G$, then $G(s) = \{\, s \,\}$, and the orbit has just one element.

(ii) In Example 2 above, take $H \times H \times H$. Then (a, a, a) has an orbit of one element, while (a, b, b) has an orbit of three elements: (b, a, b), (b, b, a), and (a, b, b).

Another example: If we let a cyclic group of order 6 operate on $H \times H \times H \times H \times H \times H$ as in Example 2, then (a, b, a, b, a, b), $a \neq b$, has an orbit of two elements. Which elements of $G = \{\, e, \sigma, \sigma^2, \sigma^3, \sigma^4, \sigma^5 \,\}$ leave (a, b, a, b, a, b) fixed? Answer: $\{\, e, \sigma^2, \sigma^4 \,\}$, which is the subgroup of G of order 3. We call $\{\, e, \sigma^2, \sigma^4 \,\}$ the *stabilizer* (or the isotropy group) of (a, b, a, b, a, b).

What is the stabilizer of (a, b, c, a, b, c) if a, b, c are distinct elements of H?

Let G operate on a set S. The *stabilizer*, or the *isotropy group*, of an element $s \in S$ is the set $I_s = \{ g \in G \mid g(s) = s \}$. The set I_s is a subgroup of G. Thus the stabilizer of an element s of S is the *subgroup of* G of elements that don't move s, i.e., that leave s fixed.

In the above examples, notice that the *number of elements in the orbit of an element of a group G multiplied by the number of elements in the stabilizer of that element is equal to the order of* G.

If G_1 is a subgroup of a finite group, then the *index* of G_1 in G, denoted from now on by $[G : G_1]$, is, by definition, the number of left cosets of G_1. Lemma 2.24 tells us that if the order of G_1 is m and the order of G is n, then m divides n. Thus $[G : G_1] = n/m$.

In the above examples, we can use this vocabulary to rephrase "the number of elements in the orbit of an element multiplied by the number of elements in the stabilizer of that element is equal to the order of G" as "the number of elements in the orbit of $s \in S$ is equal to the index of its stabilizer." This is true quite generally.

Lookout Point 2.12. There is a way in which the above statement makes some intuitive sense: The real action of G on an element s happens outside the action of the stabilizer of s—the stabilizer just leaves s alone. In a sense, to see what really happens to s under G's action, you can "mod out" by I_s. This is the same principle as viewing $\mathbb{Z}_7$ as $\mathbb{Z}$, ignoring multiples of 7.

More precisely:

Lemma 2.30. *If I_s is the stabilizer of an element $s \in S$, then the number of elements in the orbit $G(s)$ of s is equal to the index of I_s in G. In symbols,*

$|G(s)|$ denotes the number of elements in $G(s)$.

$$|G(s)| = [G : I_s], \quad \text{or} \quad |G(s)| \cdot |I_s| = |G| .$$

Proof. Write a left coset decomposition of I_s in G:

$$G = g_1 I_s \cup g_2 I_s \cup \cdots \cup g_m I_s .$$

Then m is the index of I_s in G, by definition. To prove the lemma, it is enough to show that the set $\{ g_1(s), g_2(s), \ldots, g_m(s) \}$ comprises precisely the distinct elements in the orbit $G(s)$. And indeed it does. Here is why.

First, the elements are distinct, for $g_i(s) = g_j(s)$ implies $g_j^{-1} g_i(s) = s$ implies $g_j^{-1} g_i \in I_s$ implies $g_i \in g_j I_s$, which is impossible. (Why?)

Next let $g(s) \in G(s)$. Then using the above decomposition, you can say that $g = g_i h$ for some i and $h \in I_s$. Then $g(s) = g_i h(s) = g_i(s)$, an element of our alleged orbit $\{ g_1(s), g_2(s), \ldots, g_m(s) \}$. Done. ∎

Corollary 2.31. *With notation as in the lemma, both $|G(s)|$ and $|I_s|$ divide $|G|$.*

Let us put Lemmas 2.29 and 2.30 to work.

Application 1. Let H be a finite group and let p be a prime dividing the order of H, which we denote by n. A theorem due to Cauchy states that there is an element of order p in H. The following "orbit" proof is due to James McKay [55].

Consider the set S of all p-tuples $(a_1, a_2, \ldots, a_p)$ with $a_1, \ldots, a_p \in H$ and $a_1 \cdot a_2 \cdots a_p = e$. As in Example 2, define a cyclic permutation σ of the elements of S by

$$\sigma(a_1, a_2, \ldots, a_p) = (a_p, a_1, a_2, \ldots, a_{p-1}) .$$

Let G_p denote the cyclic group $\left\{ e, \sigma, \sigma^2, \ldots, \sigma^{p-1} \right\}$ of order p. Then G_p operates on S.

We must check, of course, that G_p is a good action. In Example 2, you saw that the action satisfies the two properties from Section 2.6. We also need to check that $(a_p, a_1, \ldots, a_{p-1}) \in S$. But $a_1 \cdot a_2 \cdots a_p = e$, so $a_1 \cdots a_{p-1}$ is the inverse of a_p. It follows that $a_p a_1 a_2 \cdots a_{p-1} = e$.

Now let us look at orbits. If the orbit of $(a_1, \ldots, a_p)$ has only *one* element, then $a_1 = a_2 = \cdots = a_p$, so that $a_1{}^p = e$ and a_1 is an element of order p. If $s \in S$ has an orbit with *more* than one element, then I_s is a *proper* subgroup of G_p, and that forces $I_s = \{ e \}$, since p is prime. This means that $G(s)$ has p elements.

Much of this argument uses Lemma 2.24.

Hence either the orbit has one element or p elements. Now use Lemma 2.29. The set S is partitioned into disjoint orbits. If there are k elements with orbit just a single element, then the number of elements of S is $k + pt$ for some whole number t. But for each choice of $a_1, \ldots, a_{p-1}$, there is a *unique* a_p such that $a_1 a_2, \ldots, a_p = e$. Thus the number of elements in S is n^{p-1}. Hence $n^{p-1} = k + pt$, from which it follows that $p \mid k$, since $p \mid n$. Hence $k > 1$, and there is an element of orbit a single point besides $(e, e, e, \ldots, e)$. That gives an element of order p.

Lookout Point 2.13. This argument is a direct generalization of the argument that shows that a group with an even number of elements has an element of order 2: Each element a that is not of order 2 can be paired with its inverse $a^{-1} \neq a$. Thus there is an even number of such elements. What remains are the identity and the elements of order 2. Since the group has an even number of elements altogether, it must have an odd number of elements of order 2, hence at least one such element.

Application 2. Let G be a group. If $a \in G$ and $ag = ga$ for *all* $g \in G$, then we say that a belongs to the *center* of G. The center of G is denoted by $Z(G)$, and you can see that $Z(G)$ forms a subgroup. Here is another way to describe $Z(G)$. Put $S = G$ and let G operate on G by inner automorphisms (Example 4). Thus $g(s) = gsg^{-1}$. What is the isotropy group I_s? By definition,

Thus the center of G is all of G if and only if G is abelian.

Z is for the German word *Zentrum* = center.

$$I_s = \left\{ g \mid gsg^{-1} = s \right\} = \left\{ g \mid gs = sg \right\} .$$

Thus I_s is the subgroup of all elements in G that commute with s. If $I_s = G$, then every element commutes with s, and we have $s \in Z(G)$. In other

words, $Z(G)$ is the set of single-element orbits. When does $Z(G)$ contain more elements than just e? A partial answer is given in the following lemma.

Lemma 2.32. *If the order of G is p^n, for a prime p, then $Z(G) \neq \{ e \}$.*

Proof. It suffices to show that the number of single-element orbits is greater than 1. To that end, we decompose G under the above action into disjoint orbits. Each orbit $G(s)$ contains either one element (an element of $Z(G)$) or p^j elements for some j (Corollary 2.31). Counting, we have

$$p^n = |G| = k + pt,$$

where $k \geq 1$ is the number of single-element orbits. We then have $p \mid k$, whence $k \geq p$, and therefore $Z(G) \neq \{ e \}$. ■

Application 3. Sylow's theorem. Let G be a group with n elements and suppose that $p^s \mid n$, where p is a prime. We will locate a subgroup of order p^s. To do this, we let S be the set whose elements are subsets of G with p^s elements. The number of elements in S is

$$\binom{n}{p^s} = \frac{n(n-1)\cdots(n-p^s+1)}{(p^s)!}.$$

We need to know the highest power of p dividing $\binom{n}{p^s}$. The answer: Put $n = p^t m$ with $p \nmid m$. Then the highest power is p^{t-s}. This is seen by matching:

$$\left(\frac{p^t m}{p^s}\right)\frac{(p^t m-1)}{(p^s-1)}\cdots\frac{(p^t m-p)}{(p^s-p)}\cdots\frac{(p^t m-(p^s-1))}{p^s-(p^s-1)}.$$

You can show (Exercise 2.63) that each fraction except the first has the same power of p in the numerator and denominator. Thus the answer is $t-s$.

Now let G operate on S as in Example 6, namely, for $A \in S$ and $gA = \{ ga \mid a \in A \}$. Check that gA also has p^s elements and that G is a good action on S.

Since p^{t-s} is the *highest* power of p dividing the number of elements of S, and since, by Lemma 2.29, the orbits disjointly partition S, it follows that there must exist at least one orbit whose number of elements is not divisible by p^{t-s+1}.

Denote this distinguished orbit by $G(\alpha)$, where α is a fixed element of S. The main point of the construction is this: the stabilizer I_α of α in G is a subgroup with p^s elements. Let us prove this. By Lemma 2.30, we have

$$|G(\alpha)| \cdot |I_\alpha| = |G|.$$

For example, $\nu_5(2625) = 3$.

Also, if r is a positive integer, let $\nu_p(r)$ denote the highest power of p dividing r. Then

$$\nu_p|G(\alpha)| + \nu_p|I_\alpha| = \nu_p|G|.$$

By definition of $G(\alpha)$, we know that

$$v_p|G(\alpha)| \leq t - s\,.$$

Hence since $v_p|G| = t$, we see that

$$t - s + v_p|I_\alpha| \geq t\,,$$

Recall that $n = p^t m$ with $p \nmid m$.

or

$$v_p|I_\alpha| \geq s\,.$$

Thus $|I_\alpha| \geqq p^s$.

In order to show that $|I_\alpha| \leq p^s$, we make the following observation. Write

$$\alpha = \{\, g_1, g_2, \ldots, g_{p^s} \,\}\,.$$

If g is an arbitrary element of I_α, we know by the definition of I_α that $g\alpha = \alpha$. In other words,

$$\{\, g_1, g_2, \ldots, g_{p^s} \,\} = \{\, gg_1, gg_2, \ldots, gg_{p^s} \,\}$$

(as sets!). Hence $gg_1 = g_j$ for some j, with $1 \leq j \leq p^s$. But then $g = g_j g_1^{-1}$, which shows that there are only p^s choices for g. Hence $|I_\alpha| \leq p^s$. We conclude finally that $|I_\alpha| = p^s$, which proves Sylow's theorem.

Theorem 2.33 (Sylow's theorem). *Let G be a group with n elements and suppose that $p^s \mid n$, where p is a prime. Then G has a subgroup of order p^s.*

Exercises

2.61 Fill in the details for the claim in the proof of Sylow's theorem that

$$v_p\binom{p^t m}{p^s} = t - s\,.$$

2.62 If p is a prime and a and b are positive integers, show that

$$v_p(ab) = v_p(a) + v_p(b)\,.$$

2.63 Referring to the proof of Sylow's theorem, show that each fraction except for the first has the same power of p in the numerator and denominator.

3 The Fundamental Theorem of Arithmetic

In Chapter 2, we made extensive use of the fact that every positive integer can be written in one and only one way as a product of powers of distinct primes. This property of $\mathbb{Z}$ is basic to mathematics. It is *so* basic that many people don't even think to question it. This is especially true in school, where students spend much of elementary school working with integers, using this *unique factorization* property as if it were a law of nature. For example, young children build "factor trees" for whole numbers, and it is usually taken for granted that two different trees, like those in Figure 3.1, end up with the same set of prime factors.

And later in school, it is usually taken for granted that two different factorizations in $\mathbb{Z}[x]$ produce the same irreducible factors.

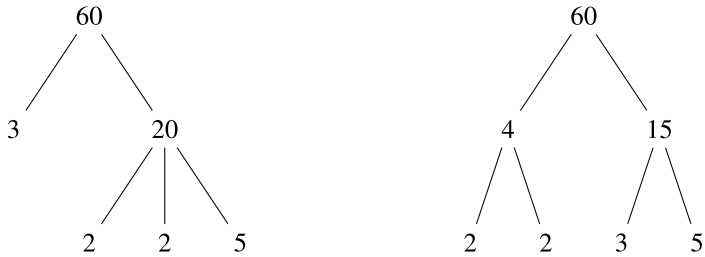


Figure 3.1. Two factor trees for 60.

Assuming unique factorization isn't the sole province of beginners. As we shall see in Section 3.2, accomplished mathematicians assumed that rings of cyclotomic integers enjoyed unique factorization and ended up with flawed proofs of a longstanding conjecture, the famous "Fermat conjecture" (read on). And attempts to fix the flaws contributed to the creation of modern algebraic number theory.

But happily, our old friend $\mathbb{Z}$ enjoys unique factorization, and that is what we take up in this chapter.

K. Ireland and A. Cuoco, *Excursions in Number Theory, Algebra, and Analysis*, Readings in Mathematics, https://doi.org/10.1007/978-3-031-13017-5_3

3.1 Getting Started

We never defined the word *prime* in Chapter 2 (whoops). To set things right, a positive integer distinct from 1 is said to be *prime* if it has only 1 and itself as positive divisors. From this definition it is not immediately clear that every positive integer different from 1 has a prime divisor. But it's true:

Insisting that primes be positive eliminates the need for some fussiness.

Lemma 3.1. *Let $n > 1$, $n \in \mathbb{Z}$. Then there exists a prime p such that $p \mid n$.*

Proof. The integer n has divisors bigger than 1 (itself, for example). Let m be minimal in the set of divisors of n larger than 1. If m were not prime, then we could write $m = ab$, $1 < a < m$ ($a \in \mathbb{Z}$). But then we would have $a \mid m$ and $m \mid n$, from which we conclude that $a \mid n$, which contradicts the minimality of m. ∎

Lemma 3.2. *Let $n > 1$, $n \in \mathbb{Z}$. Then n can be written in the form*

$$n = p_1 p_2 \cdots p_s, \quad \text{for primes } p_1, \ldots, p_s .$$

Proof. We proceed by strong induction. Check the first few cases, say $n = 2, 3, 4, 5, 6$. If n is prime, we are done. So assume that n is composite. Choose $p_1 \mid n$ by Lemma 3.1. Then $1 < n/p_1 < n$, so by induction, there are primes $p_2, \ldots, p_s$ such that

$$\frac{n}{p_1} = p_2 \cdots p_s .$$

But then

$$n = p_1 p_2 \cdots p_s .$$

∎

It is a great experiment to ask a youngster whether 13 divides $2 \times 3 \times 5 \times 7 \times 11$. Many kids will perform the multiplication, divide by 13 and (hopefully) obtain a nonzero remainder.

On grouping the distinct primes, we see that one may write $n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ for distinct primes $p_1, \ldots, p_s$. But here is the catch. Suppose $p \mid n$ for a prime p. How do you know that $p = p_i$ for some i? The proof is by no means trivial—it requires a chain of lemmas, each of which is important in itself and which, taken together, determine the algebraic structure of $\mathbb{Z}$. Here we go.

Lookout Point 3.1. Before we carry on, let us tie up another loose end from Chapter 2, one that is essential to what follows.

Lemma 3.3 (The division algorithm). *If a is an integer and b is a positive integer, then $a = bq + r$, where q and r are integers with $0 \le r < b$.*

The existence of a minimal element among the $a - bq$ follows from the "well-ordering property of $\mathbb{Z}$," discussed in [19, Chapter 1].

Proof. Consider the set of all $a - bj$, where j ranges over $\mathbb{Z}$. This set has nonnegative members (right?). Let q be such that $a - bq \ge 0$ and $a - bq$ is minimal among the nonnegative members. Put $a - bq = r$. Claim: $r < b$. Suppose to the contrary that $r \ge b$. This would imply that $a - bq \ge b$. Then $a - (q+1)b \ge 0$. But $a - (q+1)b < a - qb$, since $b > 0$. This contradicts the minimality of $a - bq$, so $r < b$ after all, and that establishes the lemma. ∎

Another way to think about this is to consider the rational number a/b. It gets caught between two consecutive integers, q and $q+1$, say. Put $\frac{a}{b} - q = w$. This makes $|w| < 1$ (why?), and it is rigged to make

$$a = bq + bw\,.$$

But

$$|bw| = |b|\,|w| < |b|\,.$$

So we take r to be bw.

The fact that every real number is caught between two consecutive integers is called the *Archimedean property* of $\mathbb{R}$. It implies that there exist real numbers arbitrarily large in absolute value. Young children get used to this when they play with the "number line." Not every useful field is Archimedean [45].

Back at the ranch, consider two positive integers a and b. They have a common divisor, namely 1. And since every divisor of a and b must be less than $\max\{a, b\}$, one can consider their *largest* (aka *greatest*) common divisor. Call it d. Our first goal is to show that if m is a common divisor of a and b, then m divides d. To do this, we show that d has an amazing property: it turns out that the set of $\mathbb{Z}$-linear combinations of a and b coincides with the set of multiples of d. We capture the greatest common divisor "linearly" by the following fundamental lemma.

Lemma 3.4. *Let a and b be integers. Let*

$$a\mathbb{Z} + b\mathbb{Z} = \{\, ax + by \mid x, y \in \mathbb{Z} \,\}\,.$$

Then:

(i) There is a unique nonnegative integer d satisfying

$$a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}.$$

(ii) If $m \mid a$ and $m \mid b$, then $m \mid d$. Hence d is the greatest common divisor of a and b.

Proof. (i) If $a = b = 0$, let $d = 0$. Otherwise, $a\mathbb{Z} + b\mathbb{Z}$ has positive elements. Let d be positive and minimal in $a\mathbb{Z} + b\mathbb{Z}$. Then $d\mathbb{Z} \subseteq a\mathbb{Z} + b\mathbb{Z}$. To get the reverse inclusion, suppose that $m \in a\mathbb{Z} + b\mathbb{Z}$. Write $m = ds + r$, where $0 \le r < d$. Then one sees that $m - ds \in a\mathbb{Z} + b\mathbb{Z}$ (because $a\mathbb{Z} + b\mathbb{Z}$ is closed under addition and subtraction). Hence $r \in a\mathbb{Z} + b\mathbb{Z}$, which forces r to be zero (why?). Therefore, $d \mid m$. Hence m is a multiple of d, and we have established the reverse inclusion:

$$a\mathbb{Z} + b\mathbb{Z} \subseteq d\mathbb{Z}.$$

(ii) Since $a \in a\mathbb{Z} + b\mathbb{Z}$, we have $a \in d\mathbb{Z}$, which means that $d \mid a$. Similarly, $d \mid b$. If $m \mid a$ and $m \mid b$, then m divides every member of $a\mathbb{Z}+b\mathbb{Z}$. In particular, it divides d, since $d \in a\mathbb{Z} + b\mathbb{Z}$. ∎

Lookout Point 3.2. Lemma 3.4 is responsible for a very suggestive piece of notation: if $a_1, \ldots, a_m$ are integers, we let $(a_1, \ldots, a_m)$ denote the set

$$a_1\mathbb{Z} + a_2\mathbb{Z} + \cdots + a_m\mathbb{Z}\,.$$

Using this convention, the lemma says that if d is the greatest common divisor of a and b, then

$$(a, b) = (d) .$$

Yes, $(a_1, \ldots, a_m)$ often denotes an n-tuple. Context matters.

This is an equality of sets. If we want to refer to integers rather than sets, the convention is to write

$$d = \gcd(a, b) .$$

But (again, context matters), we will sometimes refer to (a, b) as the greatest common divisor of a and b. There is more to the story behind all this (see [41]).

We are now in a position to establish the result that if a prime p divides a product, then it divides one of the factors.

If 6 divides a product ab, must it divide a or b?

Theorem 3.5 (Euclid's lemma). *Let p be prime. If $p \mid ab$ for integers a and b, then p divides at least one of a and b.*

Proof. Suppose that $p \nmid a$. Since p is prime, p and a have greatest common divisor 1. By Lemma 3.4, we have $ax + py = 1$ for suitable integers x and y. Multiply by b to get ab into the act. This gives

$$abx + pby = b . \tag{3.1}$$

But $p \mid ab$ and $p \mid p$. Therefore, p divides the left-hand side of equation (3.1), so it also divides the right-hand side: $p \mid b$. Done. ∎

We conclude immediately the following:

Lemma 3.6. *If $n > 1$ is written $n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$, where $p_1, \ldots, p_s$ are distinct primes, and if a prime p divides n, then $p = p_i$ for some $i = 1, \ldots, s$.*

Proof. Write $n = p_1 \cdot \left(p_1^{\alpha_1 - 1} \cdots p_s^{\alpha_s}\right)$. Then either $p \mid p_1$, in which case $p = p_1$, or else $p \mid p_1^{\alpha_1 - 1} \cdots p_s^{\alpha_s}$. Continue in this way. ∎

The fundamental theorem of arithmetic follows in the same spirit:

"Essentially one way" means that the list of prime powers in such a factorization is unique up to the order in which they are listed.

Theorem 3.7 (The fundamental theorem of arithmetic for $\mathbb{Z}$). *Every integer can be written as a product of primes in essentially one way.*

Proof. The existence of such a factorization is the content of Lemma 3.2. On to uniqueness: Suppose that $p_1^{\alpha_1} \cdots p_s^{\alpha_s} = q_1^{\beta_1} \cdots q_t^{\beta_t}$, where the p_i and q_i are primes, $p_i \neq p_j$ for $i \neq j$, and $q_i \neq q_j$ for $i \neq j$. We claim that $s = t$, $\{ p_1, \ldots, p_s \} = \{ q_i, \ldots, q_t \}$, and if $p_i = q_j$, then $\alpha_i = \beta_j$.

Well, Lemma 3.6 implies that the sets $\{ p_1, \ldots, p_s \}$ and $\{ q_1, \ldots, q_t \}$ are the same. Hence $s = t$. After relabeling, we have

$$p_1^{\alpha_1} \cdots p_s^{\alpha_s} = p_1^{\beta_1} \cdots p_s^{\beta_t} .$$

Suppose, however, that $\alpha_i \neq \beta_i$ for some i. If, say, $\alpha_i < \beta_i$, then cancellation shows that p_i divides the product $p_1^{\alpha_1} \cdots p_{i-1}^{\alpha_{i-1}} p_{i+1}^{\alpha_{i+1}} \cdots p_s^{\alpha_s}$. This contradicts the previous lemma. ■

There are various ways to organize the above steps depending on how you like to write out formal inductions. The real point is Theorem 3.5.

This completes the basic result. By restricting ourselves to *positive* primes and positive integers, we have avoided the harassment of the unit -1. In more general rings, however, you have to live with the units. The integers ± 1 are the only integers whose inverse in $\mathbb{Q}$ is actually in $\mathbb{Z}$. They form a subgroup of order 2. In more general rings, however, where arithmetic still plays an important role, there may be many units. For example, in $\mathbb{Z}[\zeta_6]$, there are six units:

The complex roots of unity were defined in the previous chapter.

$$1,\ \zeta_6,\ \zeta_6^2,\ \zeta_6^3,\ \zeta_6^4,\ \zeta_6^5\ .$$

And it gets worse (or better, depending on your tastes). Consider the ring $\mathbb{Z}[\sqrt{2}]$. Its elements look like $a + b\sqrt{2}$, where a and b are in $\mathbb{Z}$. In $\mathbb{Z}[\sqrt{2}]$, $1 + \sqrt{2}$ has inverse $-1 + \sqrt{2}$, which is in $\mathbb{Z}[\sqrt{2}]$. So $(1 + \sqrt{2})^n$, where n is a positive integer, will have inverse $(-1+\sqrt{2})^n$. Since $1+\sqrt{2} \neq 1$, the sequence $\left\{\left(1 + \sqrt{2}\right)\right\}^n$, $-\infty < n < \infty$, will give an infinite cyclic group of units!

Lemma 3.4 is often sufficient to prove results that also follow from the fundamental theorem. Here is an example.

Lemma 3.8. *If $a \mid st$ and a and t have no common factor bigger than 1, then $a \mid s$.*

Proof. Since a and t are relatively prime, one can find x and y such that $ax + ty = 1$. Multiply by s to get $asx + sty = s$. Then $a \mid a$ and $a \mid st$, so $a \mid s$. ■

Can you show that $a \mid cd$, where $(c, d) = 1$, implies $a = \mu\nu$, where $\mu \mid c$ and $\nu \mid d$, using only Lemma 3.4 and not the uniqueness argument of Theorem 3.7?

3.1.1 Computing Greatest Common Divisors

Lemma 3.3 is the basis of an algorithm for calculating the greatest common divisor of two integers, an algorithm that is simple (and enjoyable) to carry out by hand and is easily programmed in any programming language that supports recursion.

For example, see [18].

Greek mathematicians used a process called *antanairesis*, a free translation of which is "back and forth subtraction," when they realized that one consequence of the arithmetic structure of the integers is that

$$\text{if } a < b, \text{ then } \gcd(a, b) = \gcd(b - a, a)\ .$$

In repeated applications of this process, we can replace subtraction by division with remainder.

Lemma 3.9 (Euclid's algorithm). *If a and b are positive integers with $a < b$, and*

$$b = aq + r, \quad 0 \le r < a,$$

then

$$\gcd(a, b) = \gcd(r, b).$$

The proof is up to you (Exercise 3.1).

Repeated applications produce a wonderful rhythm. As an example, we illustrate one way to organize the steps that has been effective with students. Arrange the steps in computing $\gcd(124, 1028)$ as on the left:

$$\begin{array}{r} 8 \\ 124\overline{)\,1028} \\ \underline{992} \\ 36\overline{)\,124} \\ \underline{108} \\ 16\overline{)\,36} \\ \underline{32} \\ 4\overline{)\,16} \\ \underline{16} \\ 0 \end{array} \qquad \begin{array}{l} \mathbf{4} = 36 - 2 \cdot \mathbf{16} \\ \qquad\quad \searrow \\ = 36 - 2 \cdot (124 - 3 \cdot 36) \\ = -2 \cdot 124 + 7 \cdot \mathbf{36} \\ \qquad\qquad\quad \searrow \\ = -2 \cdot 124 + 7 \cdot (1028 - 8 \cdot 124) \\ = 7 \cdot 1028 - 58 \cdot 124 \end{array}$$

The last nonzero remainder is the greatest common divisor, so we have $\gcd(124, 1028) = 4$. This arrangement can be used (on the right) to read off the coefficients s and t, so that we have $4 = 124s + 1028t$. Start at the next-to-last division and solve for each remainder.

Lookout Point 3.3. In fact, you can check that the two recursively defined functions

$$s(a, b) = \begin{cases} 0 & \text{if } a = 0, \\ t(r, a) - qs(r, a) & \text{otherwise,} \end{cases}$$

and

$$t(a, b) = \begin{cases} 1 & \text{if } a = 0, \\ s(r, a) & \text{otherwise,} \end{cases}$$

where $b = aq + r$ is as in Lemma 3.9, calculate two integers such that

$$s(a, b)a + t(a, b)b = \gcd(a, b).$$

Model them in your favorite programming language and check them out. Then figure out how they mimic the "start at the next-to-last division and solve for each remainder" algorithm stated above.

3.1.2 Modular Arithmetic with Polynomials

There is a deep structural similarity between the rings $\mathbb{Z}$ and $\mathbb{R}[x]$. The key lever in this similarity is that there is a division algorithm—given two polynomials g and f in $\mathbb{R}[x]$, you can divide g by f and get a smaller remainder. The measure for "smaller" is now the *degree*, so that the division algorithm becomes the following lemma.

The degree of a polynomial f is denoted by $\deg(f)$. For a complete development of arithmetic with polynomials with coefficients in arbitrary fields, see [19, Chapter 6].

Lemma 3.10. *Let $f(x), g(x) \in \mathbb{R}[x]$. Then there exist $q(x), r(x) \in \mathbb{R}[x]$ with*

$$g = qf + r,$$

$\deg(r) < \deg(f)$.

It is most likely that you practiced the execution of this algorithm in high school. Just for old times' sake, finish off the rest of this calculation:

$$\begin{array}{r|l} & 4x^3 - 14x^2 \\ \hline x^2 + 3x - 2 & 4x^5 - 2x^4 + x^3 \\ & \underline{4x^5 + 12x^4 - 8x^3} \\ & -14x^4 + 9x^3 \\ & \vdots \end{array}$$

The results about $\mathbb{Z}$ in this section carry over with only slight modification to $\mathbb{R}[x]$. For example, every polynomial can be factored into irreducibles, and the factorization is essentially unique up to order and unit factors. Oh, and what are the units in $\mathbb{R}[x]$? You can check that if g and f are in $\mathbb{R}[x]$, then

$$\deg fg = \deg f + \deg g\,.$$

This answers the question raised in a sidenote in Section 2.2. One significant difference between $\mathbb{Z}$ and $\mathbb{R}[x]$: $\mathbb{Z}$ has two units and $\mathbb{R}[x]$ has infinitely many.

This implies that the only polynomials in $\mathbb{R}[x]$ that have reciprocals in $\mathbb{R}[x]$ are the nonzero constants—polynomials of degree 0.

And there's more: Euclid's lemma, properly formulated, holds in $\mathbb{R}[x]$: there is a greatest common divisor for two polynomials (unique up to a unit), and this greatest common divisor is a linear combination of the two polynomials.

This implies that you can compute the greatest common divisor of two polynomials with the same routine that you used in $\mathbb{Z}$. For example:

$$\begin{array}{r|l} & 3 \\ \hline 2x^2 - x - 1 & 6x^2 + x - 1 \\ & \underline{6x^2 - 3x - 3} \\ & 4x + 2 \end{array} \qquad \begin{array}{r|l} & \frac{1}{2}x - \frac{1}{2} \\ \hline 4x + 2 & 2x^2 - x - 1 \\ & \underline{2x^2 - x - 1} \\ & 0 \end{array}$$

This says that

$$\gcd\left(2x^2 - x - 1, 6x^2 + x - 1\right) = 4x + 2\,.$$

Hmm.... The high-school way to do this is to factor each polynomial into irreducibles and take the common factors:

$$\begin{aligned} 2x^2 - x - 1 &= (2x+1)(x-1)\,, \\ 6x^2 + x - 1 &= (2x+1)(3x-1)\,, \end{aligned}$$

so the gcd is $2x + 1$, not $4x + 2$. But recall that gcd is unique only up to unit factors, and $4x + 2 = 2(2x + 1)$.

This peskiness goes away if we use the "linear combination" way to characterize gcd that we saw in Lemma 3.4, because

$$\begin{aligned} &(2x^2 - x - 1)\mathbb{R}[x] + (6x^2 + x - 1)\mathbb{R}[x] \\ &\quad = (4x + 2)\mathbb{R}[x] = (2x + 1)\mathbb{R}[x]\,, \end{aligned}$$

as you can (and should) check.

And there's more.... The two functions defined in Lookout Point 3.3 work for polynomials! That is, if $f, g \in \mathbb{R}[x]$ and $q(x)$ and $r(x)$ are the (quotient and remainder) polynomials guaranteed by Lemma 3.10, define two functions s and t on $\mathbb{R}[x]$ by

$$s(f,g) = \begin{cases} 0 & \text{if } f = 0, \\ t(r,f) - q\, s(r,f) & \text{otherwise,} \end{cases} \tag{3.2}$$

and

$$t(f,g) = \begin{cases} 1 & \text{if } f = 0, \\ s(r,f) & \text{otherwise.} \end{cases} \tag{3.3}$$

Then

$$\left(s(f,g) \cdot f\right) \mathbb{R}[x] + \left(t(f,g) \cdot g\right) \mathbb{R}[x] = \gcd(f,g)\, \mathbb{R}[x]\,.$$

Indeed,

$$\left(s(f,g) \cdot f\right) + \left(t(f,g) \cdot g\right)$$

is the output of Euclid's algorithm applied to the pair (f, g) (Exercise 3.6).

Lookout Point 3.4. By now, you are probably itching to implement the calculations and algorithms described in this chapter on a computer, and it is a worthwhile and satisfying adventure to build computational models of all this. If you are inclined to do it, one piece of advice: build your models in an environment that has formal expressions (polynomials, for example) as first-class objects. There are many such computer algebra systems, such as Mathematica and Wolfram alpha; some even exist on handheld calculators

(like the TI family). A detailed account of what we do in this section, complete with Mathematica code, can be found in [16].

Just as an example, you can use these algorithms to compute (by hand, even) the output of Euclid's algorithm on the pair

$$f(x) = x^4 - x^3 - 5x^2 + 8x - 4, \quad g(x) = 3x^3 - 6x^2 + x - 2\,.$$

You will get (we hope)

$$\frac{7}{4}x - \frac{7}{2}\,.$$

The high-school method (looking for common factors) produces $x - 2$, right?

Next, compute $s(f,g)$ and $t(f,g)$:

$$s(f,g) = \frac{9}{10}x + \frac{9}{20},$$
$$t(f,g) = -\frac{3}{10}x^2 - \frac{9}{20}x + \frac{17}{20}\,.$$

And (applause) finally:

$$\left(\frac{9}{10}x + \frac{9}{20}\right)\left(x^4 - x^3 - 5x^2 + 8x - 4\right) + \left(-\frac{3}{10}x^2 - \frac{9}{20}x + \frac{17}{20}\right)\left(3x^3 - 6x^2 + x - 2\right) = \frac{7}{4}x - \frac{7}{2}\,.$$

Don't take our word for it; dig in and calculate or write the program.

There is an important application of these ideas, one that goes back to when $\mathbb{C}$ first reared its head in mathematics. The approach to complex numbers taken by many Renaissance mathematicians (and the same approach taken by many high-school students) is, essentially, to consider complex numbers as polynomials in i, where calculations are carried out as usual with the extra simplification rule $i^2 = -1$. This amounts to looking at polynomials in i and setting $i^2 + 1 = 0$.

This approach is sometimes frowned upon by educators, but it contains the germ of a brilliant insight.

This setting of something equal to 0 should look familiar. In constructing $\mathbb{Z}_p$ from $\mathbb{Z}$, we threw away multiples of p (that is, we set them equal to 0), and we saw that this idea is compatible with addition and multiplication. The ring $\mathbb{Z}_p$ turned out to be a field, thanks in large part to Theorem 2.12.

For more on Renaissance approaches to $\mathbb{C}$, check out [19, Chapter 3].

We can transport this idea to $\mathbb{R}[x]$ by exploiting its structural similarities with $\mathbb{Z}$. More precisely, $x^2 + 1$ is irreducible in $\mathbb{R}[x]$, so it could play the role of the prime p in $\mathbb{Z}_p$. And it turns out that "reducing mod $x^2 + 1$" produces a field, *a field that is abstractly identical to* $\mathbb{C}$ (Exericse 3.8).

And this is exactly what our teenagers and Renaissance ancestors wanted.

And there is more: later, we will see that this construction (reducing modulo an irreducible polynomial) is much more general, and we shall apply it to fields other than $\mathbb{R}$.

Exercises

3.1 Prove Lemma 3.9.

3.2 Write $\gcd(216, 3162)$ as a linear combination of 216 and 3162.

3.3 Find the remainder when each polynomial is divided by $x^2 + 1$:

(i) $5x^3 - 3x^2 + 2x + 1$
(ii) $x^4 - 3x^3 + 2x - 4$
(iii) $5x^3 - 3x^2 + 2x + 1 + x^4 - 3x^3 + 2x - 4$
(iv) $(5x^3 - 3x^2 + 2x + 1)(x^4 - 3x^3 + 2x - 4)$
(v) $(5x^3 - 3x^2 + 2x + 1)^2 + (x^2 + 1)(x^4 - 3x^3 + 2x - 4)$

3.4 Find the greatest common divisor of each pair (f, g) in $\mathbb{R}[x]$ and write it as a linear combination of f and g:

(i) $(x^3 - x^2 - x - 2, x^3 - 3x^2 + 3x - 2)$
(ii) $(x^6 - 1, x^5 - 1)$
(iii) $(x^3 - x^2 - x - 2, 2x^3 - 4x^2 + 2x - 4)$
(iv) $(x^6 - 1, x^6 + x^5 - 2)$
(v) $\big((2x + 1)(x^6 - 1), (2x + 1)(x^5 - 1)\big)$
(vi) $(3x^6 - 3, 2x^5 - 2)$

3.5 Show that $x^m - 1$ divides $x^n - 1$ in $\mathbb{R}[x]$ if and only if $m \mid n$.

3.6 Consider the functions (3.2) and (3.3) defined above. Show that

$$(s(f, g) \cdot f) + (t(f, g) \cdot g)$$

is the output of Euclid's algorithm applied to the pair (f, g).

3.7 Prove Lemma 3.10.

3.8 **Take It Further.** Develop the theory of polynomials modulo $x^2 + 1$ and show that the resulting ring is a field that is structurally identical to $\mathbb{C}$. Show that every polynomial is congruent (modulo $x^2 + 1$) to a linear polynomial $a + bx$ for $a, b \in \mathbb{R}$. Make sure to show that nonzero elements have reciprocals, and while you're at it, find a formula for the reciprocal of $a + bx$.

For inspiration, you can consult [16], but don't do that until you have played with this exercise for yourself.

3.2 The Gaussian Integers

An *integral domain* is a commutative ring in which every product of nonzero elements is nonzero. What are some examples besides the Gaussian integers? Nonexamples?

Gauss developed the arithmetic of the integral domain of complex numbers of the form $a + bi$, where a and b are ordinary integers, in his memoir of 1828 on biquadratic residues. He was interested in problems concerning the subgroup of fourth powers in $\mathbb{Z}_p$, the field of integers modulo p, and was able to establish the remarkable fact that 2 is a fourth power in $\mathbb{Z}_p$ for $p \equiv 1(4)$ if and only if $p = a^2 + 64b^2$. His treatment of the elementary properties of the above integral domain, now known as the *Gaussian integers* and denoted by $\mathbb{Z}[i]$, represents an important step in the early development of algebraic number theory. Although we won't prove the result about 2, we will, with the aid of the simplest considerations in $\mathbb{Z}[i]$, be able to show that every prime p that exceeds by 1 a multiple of 4 is the sum of two squares. Thus we generalize the observations $13 = 9 + 4$, $41 = 25 + 16$, and $2232037 = 1^2 + 1494^2$.

Furthermore, if such a representation is unique, then the number is prime! In this way, the representation of 2232037 can be used to prove that it is prime (Euler). The result on two squares goes back to Fermat. In fact, we find a letter of June 15, 1641, from Fermat to Bernard Frénicle de Bessy (c. 1604–1674) beginning, "La proposition fondamentale des triangles rectangles est que tout nombre premier, qui surpasse de l'unité un multiple de 4, est composé de deux quarrés" [27, p. 221].[1] It was later discovered by Lagrange that every integer is the sum of four squares. The two-square result depends on the fact that -1 is a square in $\mathbb{Z}_p$ only when $p \equiv 1 \pmod 4$, while the four-square result depends on the fact that -1 is *always* the sum of *two* squares in $\mathbb{Z}_p$. Let us therefore begin with the arithmetic in $\mathbb{Z}[i]$.

If $\alpha \in \mathbb{Z}[i]$, recall that $\overline{\alpha}$ denotes the complex conjugate of α. The complex conjugate of an element of $\mathbb{Z}[i]$ is also in $\mathbb{Z}[i]$, and moreover, $\alpha\overline{\alpha}$ is an ordinary integer in $\mathbb{Z}$, called the *norm* of α and denoted by $N(\alpha)$.

We observe that $N(\alpha) \geq 0$, and $N(\alpha) = 0$ if and only if $\alpha = 0$. Furthermore, as we saw in Chapter 2, the norm mapping is multiplicative:

$$N(\alpha)N(\beta) = N(\alpha\beta)\,.$$

An element $u \in \mathbb{Z}[i]$ is called a *unit* if $ut = 1$ for some $t \in \mathbb{Z}[i]$, that is, if u has an inverse in $\mathbb{Z}[i]$. In other words, the units in a ring are the ring's *invertible elements*. If u is a unit, then $N(u)N(t) = N(ut) = N(1) = 1$. Since $N(u)$ is a positive integer, we have $N(u) = 1$. If we put $u = x + iy$, then $N(u) = 1$ says that $x^2 + y^2 = 1$. The integer solutions to this equation are $x = 0$, $y = \pm 1$, and $x = \pm 1$, $y = 0$, giving the four elements $\pm i$, ± 1. So the units form the vertices of a square in the complex plane and coincide with the cyclic group of fourth roots of unity. We see also that the units are precisely the elements of $\mathbb{Z}[i]$ of norm 1. Two Gaussian integers are said to be *associates* if one is a unit times the other.

What are all the associates of $3 + 2i$?

The really nice thing about the ring $\mathbb{Z}[i]$ is that one can prove a division algorithm. It goes as follows:

In much of the following, we are harassed by units dangling in front of our elements. Learn to deal with it.

Lemma 3.11 (Division algorithm in the Gaussian integers). *Let $\alpha, \beta \in \mathbb{Z}[i]$, $\beta \neq 0$. Then there exist $\gamma, \delta \in \mathbb{Z}[i]$ such that $\alpha = \beta\gamma + \delta$, where $0 \leq N(\delta) < N(\beta)$.*

Proof. If we write α/β as the complex number $a + bi$, then it is easily seen that a and b are rational numbers, but they won't be integers in general. But we *can* find integers x and y such that $|x - a| \leq 1/2$ and $|y - b| \leq 1/2$. Form the element $x + iy$ of $\mathbb{Z}[i]$ and try it as a candidate for γ. That is, form $\frac{\alpha}{\beta} - \gamma$. And then put $\delta = \alpha - \beta\gamma$. So we have

Where is $x + yi$ in relation to $a + bi$ in the complex plane? That is Exercise 3.11.

$$\alpha = \beta\gamma + \delta\,.$$

So far, all we have done is rig things so that this equation is true. Now we would like to show that $0 \leq N(\delta) < N(\beta)$.

To this end, we would like

$$N\left(\frac{\alpha}{\beta} - \gamma\right) < 1\,,$$

[1] The fundamental proposition on right triangles is that every prime number that exceeds by one a multiple of 4 is composed of two squares.

for then

$$N(\alpha - \beta\gamma) = N(\delta) < N(\beta)\,.$$

But

$$N\left(\frac{\alpha}{\beta} - \gamma\right) = N(a + bi - (x + iy)) = N(a - x + i(b - y))$$
$$= (a - x)^2 + (b - y)^2 \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2} < 1.$$

■

So $\mathbb{Z}[i]$ has a division algorithm. We should put it to work for us and derive a fundamental theorem of arithmetic for $\mathbb{Z}[i]$. Instead of using the word *prime* again, let's introduce the somewhat more general concept of *irreducible* to describe an element whose only divisors are itself and a unit times itself. Thus an irreducible element in $\mathbb{Z}[i]$ is an element α whose only divisors are units and units times α. For example, since the only divisors of $2 + 3i$ are 1, i, $-i$, -1, $2i - 3$, $2 + 3i$, $-2i + 3$, and $-2 - 3i$ (Check this!), it follows that $2 + 3i$ is irreducible.

In general, suppose $a + bi$ has norm p a prime. Then $a + bi$ is irreducible. Because if $a + bi = \alpha\beta$, where α and β are nonunits, then $N(\alpha) > 1$ and $N(\beta) > 1$. But $N(a + bi) = p = N(\alpha)N(\beta)$, so that is impossible. But an irreducible need not have a prime norm. For example, you can check that 7 is irreducible in $\mathbb{Z}[i]$ (try it). But $N(7) = 49$. We will show later that the norm of an irreducible in $\mathbb{Z}[i]$ is either prime or the square of a prime.

Lemma 3.12. *If α is a nonunit in $\mathbb{Z}[i]$, then there exists an irreducible element $\pi \in \mathbb{Z}[i]$ such that $\pi \mid \alpha$.*

Proof. We know that α has nonunit divisors (α, for example). Let π be a nonunit divisor of *smallest norm*. If π were not irreducible, then π could be written as a product, $\pi = \pi_1\pi_2$, with $N(\pi_1) > 1$ and $N(\pi_2) > 1$ (because π_1, π_2 are nonunits). This would imply that $N(\pi_1) < N(\pi)$. But $\pi_1 \mid \alpha$. ■

Similarly, we have a result analogous to Lemma 3.2 in Section 3.1.

Lemma 3.13. *If α is a nonunit in $\mathbb{Z}[i]$, then $\alpha = \pi_1\pi_2\pi_3\cdots\pi_s$, where the π_i, $i = 1, \ldots, s$, are irreducible.*

Proof. The lemma is true for all elements of $\mathbb{Z}[i]$ of norm 2 (in fact, it is true for all elements whose norm is prime, as we showed above). If α is irreducible, then it is the product of one irreducible, and we are done. Suppose, then, that α is not irreducible and has norm n, and assume for the induction hypothesis that the lemma holds for all elements of norm at least 2 and less

This proof should feel familiar.

than n. Choose $\pi_1 \mid \alpha$, where π_1 is irreducible, and write $\alpha = \pi_1\beta$, and so $N(\alpha) = N(\pi_1\beta) = N(\pi_1)N(\beta)$, whence $2 \le N(\beta) = N(\alpha)/N(\pi_1) < N(\alpha)$, the first inequality holding because β is not a unit. By the induction hypothesis, $\beta = \pi_2 \cdots \pi_s$, and so $\alpha = \pi_1\pi_2\pi_3\cdots\pi_s$, as desired. ∎

Lemma 3.14. *If α is a nonunit, then $\alpha = u \cdot \pi_1^{\alpha_1}\cdots\pi_s^{\pi_s}$, where $\pi_1, \ldots, \pi_s$ are irreducibles no two of which differ by a unit (i.e., $\pi_i \ne u \cdot \pi_j$ for a unit u).*

Proof. Write $\alpha = \pi_1 \cdots \pi_t$ and collect terms. ∎

Many of the results in Section 3.1 generalize to $\mathbb{Z}[i]$. One important example is that there is an analogue of the greatest common divisor, inspired by Lemma 3.4, not as a Gaussian integer (units get in the way), but as a linear combination. That is, if α and β are in $\mathbb{Z}[i]$, we put

$$(\alpha, \beta) = \alpha\mathbb{Z}[i] + \beta\mathbb{Z}[i] \quad (= \{\alpha x + \beta y \mid x, y \in \mathbb{Z}[i]\}),$$

and we use this as our gcd.

Lemma 3.15. *If α and β are in $\mathbb{Z}[i]$, then there is $\delta \in \mathbb{Z}[i]$ such that*

$$\alpha\mathbb{Z}[i] + \beta\mathbb{Z}[i] = \delta\mathbb{Z}[i].$$

Furthermore, δ has the following properties:

(i) *$\delta \mid \alpha$ and $\delta \mid \beta$.*

(ii) *If $\mu \mid \alpha$ and $\mu \mid \beta$, then $\mu \mid \delta$.*

Proof. If $\alpha = \beta = 0$, then put $\delta = 0$. Otherwise, consider the set of all $\alpha x + \beta y$, x and y ranging over $\mathbb{Z}[i]$. Choose δ in that set with smallest positive norm. If μ is in the set, then by the division algorithm, we have

$$\mu = s\delta + r, \quad \text{where } 0 \le N(r) < N(\delta).$$

However, $\mu - s\delta$ is of the form $\alpha x' + \beta y'$. So r is in $\alpha\mathbb{Z}[i] + \beta\,\mathbb{Z}[i]$, which forces $N(r) = 0$. Therefore, $r = 0$. Thus

$$\delta\mathbb{Z}[i] \supset \alpha\mathbb{Z}[i] + \beta\mathbb{Z}[i].$$

You can establish the reverse inclusion (try it).

Finally, α and β are in $\delta\mathbb{Z}[i]$, so $\delta \mid \alpha$ and $\delta \mid \beta$. If $\mu \mid \alpha$ and $\mu \mid \beta$, then μ divides every $\alpha x + \beta y$. In particular, $\mu \mid \delta$. ∎

Note that if $\delta\mathbb{Z}[i] = \delta'\mathbb{Z}[i]$, then $\delta \mid \delta'$ and $\delta' \mid \delta$. Thus δ and $\delta'$are associates, that is, $\delta = u\delta'$, with u a unit.

The basic result corresponding to Euclid's lemma (Theorem 3.5) is as follows.

Theorem 3.16 (Euclid's lemma in the Gaussian integers). *If π is irreducible and $\pi \mid \alpha\beta$, then $\pi \mid \alpha$ or $\pi \mid \beta$.*

Proof. If $\pi \nmid \alpha$, then π and α have only units as common factors. By Lemma 3.15, therefore,

$$\pi\,\mathbb{Z}[i] + \alpha\,\mathbb{Z}[i] = u\,\mathbb{Z}[i],$$

where u is a unit. Now, $u\mathbb{Z}[i] = \mathbb{Z}[i]$. Hence $1 = \pi s + \alpha t$ for s and t from $\mathbb{Z}[i]$. Multiplying by β gives $\beta = \pi\beta s + \alpha\beta t$. Thus $\pi \mid \pi$ and $\pi \mid \alpha\beta$ implies $\pi \mid \beta$. ∎

The fundamental theorem is next, and the proof is up to you (Exercise 3.12):

Theorem 3.17 (The fundamental theorem of arithmetic for Gaussian integers). *Every Gaussian integer can be written as a product of irreducibles in essentially one way.*

If you get stuck, see [19, Chapter 8]. The ring $\mathbb{Z}[\rho]$ is often called the ring of *Eisenstein integers*.

A very nice way to spend (at least) a half hour is to carry through the results of this section for the integral domain $\mathbb{Z}[\rho]$, where $\rho = \left(-1 + i\sqrt{3}\right)/2$ is one of the two complex cube roots of unity satisfying $1+\rho+\rho^2 = 0$. Eisenstein did this and was led to cubic reciprocity. For these results and others, he received the praise of Gauss.

Exercises

3.9 Show that the distance between two complex numbers z and w in the complex plane is $\sqrt{N(z-w)}$.

3.10 The division algorithm locates a quotient and remainder. Are they unique

(i) in $\mathbb{Z}$?

(ii) in $\mathbb{Z}[i]$?

3.11 Using the notation of Lemma 3.11, where is $x + yi$ in relation to $a + bi$ in the complex plane?

3.12 Prove Theorem 3.17.

3.3 The Two Square Theorem

In Section 3.2, you checked that 7 is an ordinary prime that is also an irreducible in $\mathbb{Z}[i]$, while $13 = (2+3i)(2-3i)$ is not. We say that 7 is *inert*, while 13 is said to *split*. Can one describe the set of all primes that are inert? When does a prime split?

In order to answer these questions, we need a lemma from modular arithmetic.

Lemma 3.18. *If* $p \equiv 1 \pmod 4$, *then* -1 *is a square in* $\mathbb{Z}_p$.

Proof. We did this already! Remember Theorem 2.21 (or more precisely, Lemma 2.20) in Section 2.3? But if something is worth proving once, it is worth proving twice. Here is a proof that has a bonus:

By Fermat's little theorem, $a^{p-1} - 1 = 0$ for $a = 1, 2, \ldots, p-1$. Hence

$$x^{p-1} - 1 = (x-1)(x-2)\cdots(x-(p-1)) \text{ in } \mathbb{Z}_p\,.$$

Put $x = 0$ to obtain

$$-1 = (-1)(-2)\cdots(-(p-1)) = (p-1)! \quad \text{(Wilson's theorem!)}$$

You met Wilson's theorem in Exercise 2.52 in Section 2.3.

But

$$\begin{aligned} -1 &= p-1\,,\\ -2 &= p-2\,,\\ &\vdots\\ -\frac{(p-1)}{2} &= \frac{p+1}{2}\,. \end{aligned}$$

Some people think that Wilson's theorem is named after the rock 'n' roll legend Jackie Wilson.

Hence

$$-1 = \left(\left(\frac{p-1}{2}\right)!\right)^2 \cdot (-1)^{\frac{p-1}{2}} = \left(\left(\frac{p-1}{2}\right)!\right)^2\,.$$

■

Lookout Point 3.5. And if that's not enough, here is another variation on a proof: Since $4 \mid p-1$, the theorem of the primitive element gives an element α of order 4. Thus $\alpha^4 = 1$, or $\left(\alpha^2 - 1\right)\left(\alpha^2 + 1\right) = 0$. Since $\alpha^2 \neq 1$, we conclude that $\alpha^2 = -1$, showing that -1 is a square.

On which proof is this a variation?

Now we can prove the famous two square theorem.

Theorem 3.19. *If $p \equiv 1 \bmod 4$, then*

$$p = \pi\overline{\pi}\,,$$

In fancy language, if $p \equiv 1 \bmod 4$, then p splits in $\mathbb{Z}[i]$.

where π is irreducible in $\mathbb{Z}[i]$.

Proof. Since -1 is a square modulo p, we see that $a^2 = -1$ in $\mathbb{Z}_p$ for an ordinary integer a. Thus $p \mid \left(a^2 + 1\right)$ in $\mathbb{Z}$. So $p \mid (a+i)(a-i)$ in $\mathbb{Z}[i]$. It follows that p is not irreducible in $\mathbb{Z}[i]$. For otherwise, by Euclid's lemma (Lemma 3.16), we would have $p \mid (a-i)$ or $p \mid (a+i)$. That would say that

$$\frac{a}{p} - \frac{1}{p}i \quad \text{or} \quad \frac{a}{p} + \frac{1}{p}i$$

is in $\mathbb{Z}[i]$, which is absurd. So write $p = \alpha\beta$ with $N(\alpha) > 1$, $N(\beta) > 1$. On taking norms, we obtain

$$p^2 = N(\alpha)N(\beta).$$

Hence by unique factorization in $\mathbb{Z}$, we have $p = N(\alpha) = \alpha\overline{\alpha}$. Since $N(\alpha)$ is prime, α is irreducible. ■

As a corollary we have the lovely result that every prime in the sequence $\{1, 5, 9, 13, 17, 21, 25, \dots\}$ is expressible as the sum of two squares.

Corollary 3.20. *If $p \equiv 1 \bmod 4$ is prime, then $p = a^2 + b^2$ for integers a and b in $\mathbb{Z}$.*

Proof. Write $\pi = a + bi$ in Theorem 3.19. ∎

Using unique factorization in $\mathbb{Z}[i]$, you can show that the above representation is unique up to order and the signs of a and b (try it).

It would be good also to know whether $p \equiv 3 \bmod 4$ implies that p is *inert* (does not split) in $\mathbb{Z}[i]$, in other words, that p is not the sum of two squares. Indeed, if $p = a^2 + b^2$, then exactly one of a^2 and b^2 would be even. Say a^2 is even and b^2 is odd. That implies that 4 divides a^2 and b^2 is congruent to 1 modulo 4. Thus $a^2 + b^2$ is congruent to 1 mod 4. Thus the inertial primes are precisely the primes congruent to 3 modulo 4.

There is one remaining prime that we haven't discussed. The even prime 2 can be written as

$$2 = -i(1 + i)^2.$$

The number $1 + i$ is irreducible, since it has norm 2, and $-i$ is a unit. Hence $2 = u \cdot \pi^2$. In algebraic number theory, 2 is called a *ramified* prime.

To summarize all this:

Theorem 3.21 (Law of decomposition in the Gaussian integers). *Every rational prime p decomposes in $\mathbb{Z}[i]$ in one of three ways:*

(i) *p splits into two conjugate prime factors if $p \equiv 1 \bmod 4$.*

(ii) *p is inert if $p \equiv 3 \bmod 4$.*

(iii) *$p = 2$ ramifies: $2 = -i(1 + i)^2$.*

Theorem 3.21 tells us how primes in $\mathbb{Z}$ behave when they are viewed as elements of $\mathbb{Z}[i]$. And you can show that every irreducible in $\mathbb{Z}[i]$ divides a prime in $\mathbb{Z}$, because every irreducible π divides its norm, $\pi\overline{\pi}$. Using this, you can establish how primes in $\mathbb{Z}[i]$ behave.

Corollary 3.22 (Classification of Gaussian irreducibles). *The irreducibles π in $\mathbb{Z}[i]$ are of three types:*

We say that π *lies over* p.

(i) *$\pi = a + bi$, and π divides a prime $p \in \mathbb{Z}$ such that $p \equiv 1 \bmod 4$. In this case, $N(\pi) = a^2 + b^2$.*

The proof is up to you (Exercise 3.13).

(ii) *$\pi = p$, where p is a prime in $\mathbb{Z}$ such that $p \equiv 3 \bmod 4$. In this case, $N(p) = p^2$.*

(iii) *$\pi = 1 + i$ and its associates. In this case, $N(1 + i) = 2$.*

Figure 3.2 shows one way to visualize the story.

One can consider integral domains other than $\mathbb{Z}[\sqrt{-1}]$, for example, the domain $\mathbb{Z}[\sqrt{-d}]$ for a fixed positive square-free integer. If $d \equiv -1 \bmod 4$, you

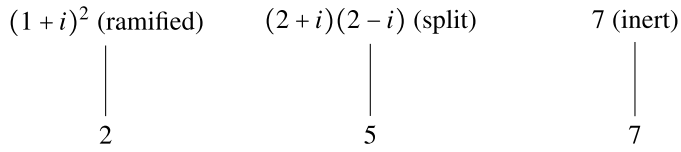
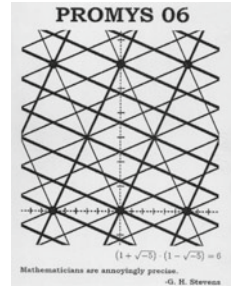


Figure 3.2. Primes upstairs in $\mathbb{Z}[i]$ and primes downstairs in $\mathbb{Z}$.

need a slightly larger ring that allows 2 in the denominator. It turns out that the only such rings that have a Euclidean algorithm are those for $d = 1, 2, 3, 7, 11$. That the fundamental theorem of arithmetic fails for certain rings can be seen by considering the decomposition of 6 in the ring of integers $\mathbb{Z}\left[\sqrt{-5}\right]$. Then $6 = 3 \cdot 2 = \left(1+\sqrt{5}\right)\left(1-\sqrt{-5}\right)$, and one proves quickly that $2, 3, 1+\sqrt{-5}$, and $1-\sqrt{5}$ are all irreducible in $\mathbb{Z}\left[\sqrt{-5}\right]$ and that they do not differ by a unit factor. Similarly, $9 = 3 \cdot 3 = \left(1+\sqrt{10}\right)\left(-1+\sqrt{10}\right)$ in $\mathbb{Z}\left[\sqrt{10}\right]$.



A T-shirt that celebrates nonunique factorization.

3.3.1 Fermat's Last Theorem

Surely, one of the oldest and best-known problems in number theory involves the search for Pythagorean triples—triples of positive integers (a, b, c) that are side lengths of a right triangle, so that

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

Diophantus of Alexandria developed, around 250 CE, a geometric method for generating such triples. Stated in modern language, he realized that a rational point on the unit circle (the graph of $x^2 + y^2 = 1$), when written in the form $\left(\frac{a}{c}, \frac{b}{c}\right)$, produces a Pythagorean triple:

$$\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1 \quad \Longrightarrow \quad a^2 + b^2 = c^2 .$$

One can get such a rational point by forming a line with positive rational slope through the point $P = (-1, 0)$ and intersecting the line with the circle. The second intersection point will then be rational (check this). Hence, it was known early on that there are infinitely many Pythagorean triples (details are in [19]).

There are several algebraic methods for generating Pythagorean triples. One method builds on an old party trick: Ask each person at a party to pick a favorite Gaussian integer $r + si$ (make $r > s > 0$) and *square it*. Watch eyes light up:

$$\begin{aligned}(2+i)^2 &= 3+4i,\\ (3+2i)^2 &= 5+12i,\\ (5+2i)^2 &= 21+20i,\\ (5+4i)^2 &= 9+40i\,.\end{aligned}$$

Compute the norms of each of these Gaussian integers for another nice punchline.

The punchline: the square of a Gaussian integer seems to be of the form $x+yi$,

where x and y are the legs of a Pythagorean triple. You should prove this using only high-school algebra.

This is more than a party game, though. It expresses a property of Gaussian integers that you may have noticed: if $z \in \mathbb{Z}[i]$, then the norm $N(z)$ is a sum of the squares of two integers. So if we can find z such that $N(z)$ is a perfect square, then you have a Pythagorean triple, right?

Corollary 2.2 from Chapter 2 comes to the rescue: for every Gaussian integer z, we have

$$N(z^2) = (N(z))^2 \ .$$

The right-hand side is the square of an integer, and the left-hand side (because it is a norm) is the sum of two squares of integers. Bingo.

For example, suppose that $z = 3 + 2i$. Then $N(z) = 13$ and $z^2 = 5 + 12i$. So

$$(N(z))^2 = 13^2 \quad \text{and} \quad N(z^2) = 5^2 + 12^2 \ .$$

This gives an easily programmable method for generating all the Pythagorean triples you will ever need. Try it. Table 3.1 gives just a small sample of the treasures that await:

Table 3.1. $(r + si)^2$ and the square of the resulting norm.

	$s = 1$	$s = 2$	$s = 3$	$s = 4$
$r = 2$	$3 + 4i$, 5			
$r = 3$	$8 + 6i$, 10	$5 + 12i$, 13		
$r = 4$	$15 + 8i$, 17	$12 + 16i$, 20	$7 + 24i$, 25	
$r = 5$	$24 + 10i$, 26	$21 + 20i$, 29	$16 + 30i$, 34	$9 + 40i$, 41
$r = 6$	$35 + 12i$, 37	$32 + 24i$, 40	$27 + 36i$, 45	$20 + 48i$, 52
$r = 7$	$48 + 14i$, 50	$45 + 28i$, 53	$40 + 42i$, 58	$33 + 56i$, 65
$r = 8$	$63 + 16i$, 65	$60 + 32i$, 68	$55 + 48i$, 73	$48 + 64i$, 80

We can see the same thing in a less fancy way: if you want integers a and b such that $a^2 + b^2$ is a perfect square, you might write the sum of those two squares as

$$a^2 + b^2 = (a + bi)(a - bi)$$

and try to make each factor on the right-hand side the square of a Gaussian integer. And it is within the scope of high-school mathematics to show that if $a + bi = (r + si)^2$, then $a - bi = (r - si)^2$. You can finish the argument.

About fourteen centuries after Diophantus, Fermat (1607?–1665) proved that there are no positive integers a, b, c such that $a^4 + b^4 = c^4$. He was studying his copy of Diophantus's *Arithmetica*, published in 1621, and he wrote in its margin:

> It is impossible for a cube to be written as a sum of two cubes or a fourth power to be written as a sum of two fourth powers or, in general, for any number that is a power greater than the second to be written as a sum of two like powers. I have discovered a truly marvelous demonstration of this proposition which this margin is too narrow to contain.

Fermat was not the first mathematician to write a marginal note in a copy of Diophantus. Next to the same problem, the Byzantine mathematician Maximus Planudes wrote, "Thy soul, Diophantus, be with Satan because of the difficulty of your theorems."

Fermat never returned to this problem (at least not publicly) except for his proof of the case $n = 4$. The statement that if $n > 2$, there are no positive integers a, b, c such that $a^n + b^n = c^n$ is called *Fermat's last theorem*. The original text in which Fermat wrote his famous marginal note is lost today. Fermat's son edited an edition of Diophantus, published in 1670, containing his father's annotations, including his famous "last theorem." It contained other unproved assertions as well, most true, some not. By the early 1800s, only Fermat's conjecture about sums of powers remained undecided, whence the name "last theorem." It became a famous problem, resisting the attempts of mathematicians of the highest order for 300 years. Most mathematicians believe that Fermat did not have a correct proof. The quest for a proof of Fermat's last theorem generated much beautiful mathematics. In particular, it led to an understanding of complex numbers, factorization, and polynomials.

One of the basic strategies for trying to prove Fermat's last theorem in the seventeenth, eighteenth, and nineteenth centuries was the method we used for $n = 2$: show that $a^n + b^n$ factors in $\mathbb{Z}[\zeta_n]$, but this time, show that the factors cannot combine to produce a perfect nth power in that system. It is worth looking at the basic idea, because it shows the importance of unique factorization.

If the equation $x^n + y^n = z^n$ has a solution in $\mathbb{Z}$, then it has a solution for every prime factor of n, because if $n = pq$, then

$$a^n + b^n = c^n \Longrightarrow (a^q)^p + (b^q)^p = (c^q)^p \ . \tag{3.4}$$

Because Fermat proved the theorem for $n = 4$, equation (3.4) implies that it has no solution for $n = 2^r$ for every integer $r \geq 2$. So using equation (3.4) again, it follows that it is enough to show that there are no integer solutions to $x^n + y^n = z^n$ for odd prime exponents.

Suppose, then, that p is an odd prime number. The goal is to show that there are no positive integer solutions to

$$a^p + b^p = c^p \,, \tag{3.5}$$

and again, the idea is to factor $a^p + b^p$ in $\mathbb{Z}[\zeta_p]$ and show that the factorization cannot contain the pth power of some prime.

Using Exercise 2.11 in Section 2.1, we have

$$a^p + b^p = (a+b)(a+\zeta b)\left(a+\zeta^2 b\right)\cdots\left(a+\zeta^{n-1} b\right) \ .$$

With excruciatingly technical calculations and arguments, mathematicians (Lamé may have been the first, around 1847) showed that it was impossible for at least one prime factor of $a^p + b^p$ to show up at least p times on the right-hand side of this equation. It seemed as if the "Fermat conjecture" was settled.

But there was a basic flaw in these arguments, a flaw that has its roots in school mathematics. As we said in the introduction to this chapter, elementary-school students build "factor trees " for whole numbers, and it is more or less assumed that if two different children build two different trees by starting from, say, 4×3 and 6×2, they will end up with the same prime factors. This

In high school, we also assume the same property for $\mathbb{C}[x]$.

unique factorization property is never questioned (and hardly ever comes up) in school mathematics.

And the argument outlined above for $a^p + b^p$ also assumes that elements in $\mathbb{Z}[\zeta_p]$ can (just as in $\mathbb{Z}$) be factored into primes in only one way. For some values of p, this is true, and for such primes, $\mathbb{Z}[\zeta_p]$ has the unique factorization property mentioned above. The arguments that use Gaussian integers are solid, because $\mathbb{Z}[i]$ has unique factorization. The first case in which the property fails is $\mathbb{Z}[\zeta_{23}]$ [66, p. 7], a fact established by Ernst Eduard Kummer while he was researching a different but related question. It was eventually shown that unique factorization fails in infinitely many cases.

It was natural to think that just as in $\mathbb{Z}$ or in the polynomials of high school, the rings $\mathbb{Z}[\zeta_p]$ would have unique factorization, as evidenced by the number of mathematicians in the seventeenth, eighteenth, and nineteenth centuries who assumed it. How could so many not have known, for example, that unique factorization failed in $\mathbb{Z}[\zeta_{23}]$? It may seem that 23 is not all that large, but the calculations in $\mathbb{Z}[\zeta_{23}]$ are hefty, even with computers. Imagine the stamina required to calculate by hand in this ring (some of Kummer's tour-de-force calculations are recounted in [24, Chapter 4]). So the assumption that $\mathbb{Z}[\zeta_p]$ is a unique factorization domain was widespread, and once it occurred to Kummer and others that this might not hold for every p, the proof that unique factorization fails in $\mathbb{Z}[\zeta_{23}]$ was, quite simply, very hard (again, see [24, Chapter 4]).

We shall leave the story here, only to note that Kummer went on to prove Fermat's last theorem in the case that $\mathbb{Z}[\zeta_p]$ has unique factorization. And using an idea that is already present when children argue that the prime factorization of 4×3 is the same as that of 6×2—there are primes "behind" each of the composite factors that are recombined in different ways—Kummer also developed a theory that would restore a kind of unique factorization, proving the theorem for a much wider class of primes [19]. But a complete proof had to wait until the mid-1990s, when Andrew Wiles, using sophisticated methods developed in the twentieth century, was finally able to prove Fermat's last theorem in full generality.

Exercises

3.13 Prove Corollary 3.22.

3.14 Show that there are no integers x, y, z with $3 \nmid xyz$ such that $x^3 + y^3 = z^3 \bmod 9$.

3.15 Show that there are no integers x, y, z with $5 \nmid xyz$ such that $x^5 + y^5 = z^5 \bmod 25$. This exercise implies Fermat's last theorem for exponent 5 in the case that $5 \nmid xyz$.

3.16 Are there any integers x, y, z with $7 \nmid xyz$ such that $x^7 + y^7 = z^7 \bmod 49$?

3.17 (i) Sketch the graph of $x^3 + y^3 = 1$.

(ii) Show that the only rational points on the graph are $(1, 0)$ and $(0, 1)$.

3.18 Take It Further. Let G be the graph of $x^3 + y^3 = 9$.

(i) Sketch G.

(ii) Find the equation of the line ℓ tangent to G at $(2, 1)$.

(iii) Find the intersection of ℓ and G.

(iv) Show that there are infinitely many triples of integers (x, y, z) such that

$$x^3 + y^3 = 9z^3.$$

3.4 Formal Dirichlet Series and the Number of Representations of an Integer as the Sum of Two Squares

We saw in the previous section that every prime congruent to 1 modulo 4 is the sum of two squares. In fact, if $p \equiv 1 \bmod 4$, then $p = \pi\overline{\pi}$ for $\pi \in \mathbb{Z}[i]$. Furthermore, since π is irreducible $(N(\pi) = p)$, it follows that if $\pi = a + bi$, then $p = a^2 + b^2$ is the only representation up to plus or minus signs and permuting a and b. For π irreducible means that the only factorizations of p in $\mathbb{Z}[i]$ are $p = (\pi u)(\overline{\pi}u')$, where u and u' are units. But the only units in $\mathbb{Z}[i]$ are $1, -1, i, -i$, which leads to the representations

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

Four other trivial changes (interchanging a and b) arise from $\overline{\pi}$ and its associates. We say that p has eight representations as a sum of two squares.

If we consider an integer that is not prime, then the situation is quite different. For example,

$$65 = 49 + 16 = 1 + 64\,.$$

The different possibilities come from

$$65 = 5 \cdot 13 = (2 + i)(2 - i)(2 + 3i)(2 - 3i)\,.$$

One grouping gives $(7 + 4i)(7 - 4i)$, and another gives $(1 + 8i)(1 - 8i)$, as illustrated in Figure 3.3.

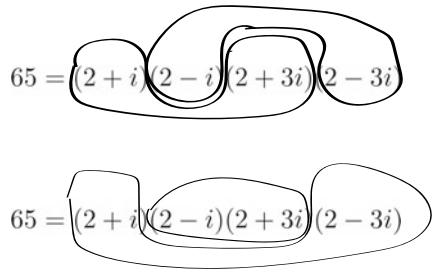


Figure 3.3. 65 obtained in two different ways as the sum of two squares.

For a general integer n, the various regroupings into conjugate pairs of terms of the complete factorization of n in $\mathbb{Z}[i]$ lead to a messy counting argument. However, the final result is hardly wanting in mathematical elegance:

Theorem 3.23. *The number of representations of a positive integer n as the sum of two squares in $\mathbb{Z}$ is four times the excess of the number of divisors of the form $4t+1$ over those of the form $4t-1$.*

Let's consider an example. Take $n = 18$. Its divisors are $1, 2, 3, 6, 9, 18$. Two of these are congruent to 1 modulo 4 (1 and 9). There is one, namely 3, that is congruent to -1 modulo 4. Thus the excess is 1, and so there are four representations. They are $(\pm 3)^2 + (\pm 3)^2$. On the other hand, take $n = 12$. Its divisors are $1, 2, 3, 4, 6, 12$. The only one congruent to 1 mod 4 is 1, while 3 is the only divisor congruent to -1 modulo 4. The excess is 0, so there are no representations of 12 as the sum of two squares, a fact that is quickly checked. It seems remarkable that the number of divisors of the form $4t-1$ should never exceed the number of the form $4t+1$. Can you prove this without knowing that it is the number of representations of n as a sum of two squares?

Yes, there are computer algebra systems that will do this for you, but (as Glenn Stevens always says), don't let the computer have all the fun.

It is worth spending a half hour to compute more examples and to tabulate the results for n between, say, 1 and 50. You could also check, just for fun, that 15625 can be written as a sum of two squares in 28 ways, and 815730721 can be so written in a whopping 36 ways.

This result can be formulated nicely by introducing the function χ. We define $\chi(n) = 0$ if n is even. If $n = 4k+1$, put $\chi(n) = 1$, and if $n = 4k-1$, put $\chi(n) = -1$. If you think about it, the sum

$$\sum_{d>0,\, d|n} \chi(d)$$

measures the difference between the number of positive divisors of n of the form $4k+1$ and those of form $4k-1$, right?

So, letting $r(n)$ be the *total* number of representations of n as a sum of two squares, our result can be stated in the following theorem.

Theorem 3.24. *The number of representations of a positive integer n as a sum of two squares is given by*

$$r(n) = 4\Big(\sum_{d|n} \chi(d)\Big),$$

where the sum is over the positive divisors of n.

There are several ways to prove this. One of the prettiest uses a piece of equipment that finds applications all over number theory. Here we go....

3.4.1 Formal Dirichlet Series

There is a formalism going back to Euler that makes it possible to prove Theorem 3.24 in a particularly elegant manner. A formal *Dirichlet series* is a creature of the form

$$\sum_{n=1}^{\infty} \frac{a(n)}{n^s} = a(1) + \frac{a(2)}{2^s} + \frac{a(3)}{3^s} + \cdots,$$

where the $a(n)$ are complex numbers.

The word "formal" is important here—we think of these series as bookkeeping devices keeping track of combinatorial or numerical data. We don't worry about questions of convergence; we think of s simply as an *indeterminate* rather than as a variable that can be replaced by a real or complex number. This misses many of the wonderful analytic applications of such series, but it turns out that their formal algebraic properties are all we need for this discussion.

Dirichlet series are added and multiplied formally. Addition is done term by term:

$$\sum_{n=1}^{\infty} \frac{a(n)}{n^s} + \sum_{n=1}^{\infty} \frac{b(n)}{n^s} = \sum_{n=1}^{\infty} \frac{a(n)+b(n)}{n^s}\,.$$

Multiplication is also done term by term, but then one gathers up all terms with the same denominator. For example, if we are looking for $c(12)/12^s$ in

$$\sum_{n=1}^{\infty} \frac{a(n)}{n^s} \sum_{n=1}^{\infty} \frac{b(n)}{n^s} = \sum_{n=1}^{\infty} \frac{c(n)}{n^s},$$

then a denominator of 12^s could come only from the products

$$\frac{a(1)}{1^s}\cdot\frac{b(12)}{12^s},\quad \frac{a(2)}{2^s}\cdot\frac{b(6)}{6^s},\quad \frac{a(3)}{3^s}\cdot\frac{b(4)}{4^s},$$
$$\frac{a(4)}{4^s}\cdot\frac{b(3)}{3^s},\quad \frac{a(6)}{6^s}\cdot\frac{b(2)}{2^s},\quad \frac{a(12)}{12^s}\cdot\frac{b(1)}{1^s}.$$

In general, the coefficient $c(n)$ above is given by

$$c(n) = \sum_{d|n} a(d)\cdot b\left(\frac{n}{d}\right),$$

where again, $\sum_{d|n}$ means that the sum is over the positive divisors of n.

The simplest Dirichlet series is the *Riemann zeta function*:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Actually, the *zeta function* usually means the function of a complex variable s (introduced by Riemann) that analytically continues this infinite series. It is the object of much current research. Google, for example, the *Riemann hypothesis*.

Then the above expression for $c(n)$ implies that if

$$\zeta(s)\sum_{n=1}^{\infty} \frac{a(n)}{n^s} = \sum_{n=1}^{\infty} \frac{c(n)}{n^s},$$

then

$$c(n) = \sum_{d|n} a(d)\,.$$

Let us state this as a theorem.

Theorem 3.25.

$$\zeta(s)\sum_{n=1}^{\infty} \frac{a(n)}{n^s} = \sum_{n=1}^{\infty} \frac{c(n)}{n^s},$$

where $c(n) = \sum_{d|n} a(d)$.

Theorem 3.25 gives us a key corollary that we will need very soon:

Corollary 3.26. *If $\alpha(n)$ is defined by*

$$\sum_{n=1}^{\infty} \frac{\alpha(n)}{n^s} = \zeta(s) \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s},$$

then

$$\alpha(n) = \sum_{d|n} \chi(d).$$

So, $\alpha(n)$ is the excess of the number of positive divisors of n of the form $4k+1$ over the number of divisors of n of the form $4k-1$. Bingo: this is exactly the function that is the heart of Theorem 3.24. The idea, then, is to form the Dirichlet series with coefficients $r(n)$ and show that

$$\sum_{n=1}^{\infty} \frac{r(n)}{n^s} = 4\,\zeta(s) \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}.$$

The 4 out front is there because we want to include the different ways to write a^2+b^2 (switching a and b and sign changes). To keep things simple, let us use the function r_1 instead, where $r_1(n)$ is the number of representations $x^2+y^2=n$, $x \geq 0$, $y > 0$. When we are done, we will simply multiply by 4.

Our (new) goal, then, is to show that

$$\sum_{n=1}^{\infty} \frac{r_1(n)}{n^s} = \zeta(s) \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}.$$

To do this, we will convert each of the sums to a product. For that, we need a (yet another) new idea: a function a defined on nonnegative integers is *strongly multiplicative* if for all nonnegative integers m, n, we have

$$a(mn) = a(m)a(n).$$

A function is said to be multiplicative if $a(mn) = a(m)a(n)$ whenever $\gcd(m,n) = 1$.

Examples of strongly multiplicative functions include the constant function that assigns 1 to every number and (check this) our function χ. Can you think of some others?

When a is strongly multiplicative, the Dirichlet series with coefficients $a(n)$ has an alternative form that shows its connection with arithmetic.

Theorem 3.27. *If a is a strongly multiplicative function, then*

$$\sum_{n=1}^{\infty} \frac{a(n)}{n^s} = \prod_{p} \left(\frac{1}{1 - a(p)/p^s} \right),$$

where the product is over all prime numbers p.

Lookout Point 3.6. Wait! What does "product is over all prime numbers" mean? Here is what we need: Consider the formal product

$$\prod_{p} \left(\frac{1}{1 - a(p)/p^s} \right).$$

To write this as a Dirichlet series $\sum_{n=1}^{\infty} \frac{b(n)}{n^s}$, fix n and factor n into prime powers:

$$p_1{}^{\alpha_1} \cdots p_t{}^{\alpha_t} = n\,.$$

Next, look at the finite product

$$\prod_{i=1}^{t} \left(\frac{1}{1 - a(p_i)/p_i^s} \right).$$

Each factor can be expanded as a geometric series:

$$\begin{aligned} \frac{1}{1 - a(p_i)/p_i^s} &= 1 + \left(\frac{a(p_i)}{p_i^s} \right) + \left(\frac{a(p_i)}{p_i^s} \right)^2 + \left(\frac{a(p_i)}{p_i^s} \right)^3 + \cdots \\ &= 1 + \left(\frac{a(p_i)}{p_i^s} \right) + \left(\frac{a(p_i^2)}{p_i^{2s}} \right) + \left(\frac{a(p_i^3)}{p_i^{3s}} \right) + \cdots. \end{aligned}$$

Then look at the coefficients of

$$\frac{a(p_1^s)}{p_1^{\alpha_1 s}}, \quad \frac{a(p_2^s)}{p_2^{\alpha_2 s}}, \quad \ldots, \quad \frac{a(p_t^s)}{p_t^{\alpha_t s}},$$

and multiply them together. That's $b(n)$.

Back at the ranch, we want to show that

$$\sum_{n=1}^{\infty} \frac{a(n)}{n^s} = \prod_{p} \left(\frac{1}{1 - a(p)/p^s} \right),$$

where a is our strongly multiplicative function.

Proof. As above, each factor on the right-hand side is a geometric series:

$$\begin{aligned} \frac{1}{1 - a(p)/p^s} &= 1 + \left(\frac{a(p)}{p^s} \right) + \left(\frac{a(p)}{p^s} \right)^2 + \left(\frac{a(p)}{p^s} \right)^3 + \cdots \\ &= 1 + \left(\frac{a(p)}{p^s} \right) + \left(\frac{a(p^2)}{p^{2s}} \right) + \left(\frac{a(p^3)}{p^{3s}} \right) + \cdots. \end{aligned}$$

Now multiply the expressions for $\frac{1}{1-a(p_i)/p^s}$ together (one for each prime). You get the sum of every possible expression of the form

$$\frac{a(p_1^{e_1})a(p_2^{e_2}) \cdots a(p_r^{e_r})}{p_1^{e_1 s} p_2^{e_2 s} \cdots p_r^{e_r s}} = \frac{a(p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r})}{\left(p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}\right)^s}\,.$$

Since every $n \in \mathbb{Z}$ can be written in one and only one way as a product of powers of primes (the fundamental theorem of arithmetic again), this is the same as the sum

$$\sum_{n=1}^{\infty} \frac{a(n)}{n^s}\,.$$

■

We shall use two applications of Theorem 3.27:

(i) The constant function $a(n) = 1$ is strongly multiplicative, so the Riemann zeta function has a product expansion

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \frac{1}{1 - 1/p^s} . \tag{3.6}$$

(ii) Our favorite function χ is also strongly multiplicative, so

$$\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_p \left(\frac{1}{1 - \chi(p)/p^s} \right) .$$

At last, we are ready to derive a formula for $r_1(n)$, the number of representations of n in the form $x^2 + y^2$, where $x > 0$, $y \geq 0$. Consider the formal Dirichlet series

$$\sum_{n=1}^{\infty} \frac{r_1(n)}{n^s} .$$

Here's the clever idea: each term in the sum is itself a sum of fractions with numerator 1, and the number of such fractions is the number of Gaussian integers with given norm. For example, $r_1(25) = 3$, because 25 can be written as a sum of squares in $Q_1 := \{ x + yi \mid x, y \in \mathbb{Z},\ x > 0,\ y \geq 0 \}$ in three ways,

Where does Q_1 sit in the complex plane?

$$3^2 + 4^2, \quad 4^2 + 3^2, \quad 5^2 + 0^2 ,$$

so $3/25^s$ comes from

$$\frac{1}{N(3+4i)} + \frac{1}{N(4+3i)} + \frac{1}{N(5+0i)} .$$

Using this idea of representing a sum of two squares as a norm from $\mathbb{Z}[i]$, using the multiplicativity of N, and letting Q_1 denote the first quadrant as we have defined it, we get a product formula for the left-hand side:

$$\begin{aligned} \sum_{n=1}^{\infty} \frac{r_1(n)}{n^s} &= \sum_{\alpha \in Q_1} \frac{1}{(N(\alpha))^s} \\ &= \prod_{\pi \in Q_1} \sum_{k=0}^{\infty} \frac{1}{\left((N(\pi))^k \right)^s} \quad \text{(use the fundamental theorem in } \mathbb{Z}[i]) \\ &= \prod_{\pi \in Q_1} \frac{1}{1 - 1/N(\pi)^s} \quad \text{(sum a geometric series)} . \end{aligned}$$

This is best understood by calculating a few coefficients by hand.

Here the product is over all Gaussian irreducibles in the first quadrant.

Now, for convenience, let us use P as a shorthand for $\sum_{n=1}^{\infty} r_1(n)/n^s$, so that

$$P = \prod_{\pi \in Q_1} \frac{1}{1 - 1/N(\pi)^s} .$$

We will now pick P apart, looking at the each factor. Here we go....

If π is an irreducible in $\mathbb{Z}[i]$, then $N(\pi) = p$ for some prime p in $\mathbb{Z}$. And by the law of decomposition in $\mathbb{Z}[i]$ (Theorem 3.21), there are three kinds of primes p:

(i) If $p \equiv 1 \bmod 4$, then p splits into two conjugate prime factors: $p = \pi\overline{\pi}$ for an irreducible π. This contributes two identical terms to P:

$$\frac{1}{1-1/N(\pi)^s} \quad \text{and} \quad \frac{1}{1-1/N(\overline{\pi})^s},$$

both equal to $\frac{1}{1-1/p^s}$, and hence P contains a term

$$\left(\frac{1}{1-1/p^s}\right)^2,$$

one for each prime $p\,\mathbb{Z}$, $p \equiv 1 \bmod 4$.

(ii) If $p \equiv 3 \bmod 4$, then p is inert, so it is irreducible in $\mathbb{Z}[i]$ and we can move p upstairs to $\mathbb{Z}[i]$ as itself. Hence $\overline{p} = p$ and $N(p) = p^2$. So P contains a term

$$\frac{1}{1-1/p^{2s}},$$

one for each prime p in $\mathbb{Z}$, $p \equiv 3 \bmod 4$.

(iii) If $p = 2$, it ramifies: $-i(1+i)^2$, and $N(p) = 2$. Hence P contains exactly *one* term for the prime $p = 2$:

$$\frac{1}{1-1/2^s}.$$

And now, put it all together into one lovely algebraic calculation. Enjoy:

It is a very good idea to give reasons for each step in this calculation.

$$\sum_{n=1}^{\infty}\frac{r_1(n)}{n^s} = \prod_{\pi\in Q_1} 1/\left(1-\frac{1}{N(\pi)^s}\right)$$

$$= \frac{1}{1-1/2^s}\left(\prod_{p\equiv 1 \bmod 4}\frac{1}{1-1/p^s}\right)^2\left(\prod_{p\equiv 3 \bmod 4}\frac{1}{1-1/p^{2s}}\right)$$

$$= \frac{1}{1-1/2^s}\left(\prod_{p\equiv 1 \bmod 4}\frac{1}{1-1/p^s}\right)^2\left(\prod_{p\equiv 3 \bmod 4}\frac{1}{1-1/p^s}\right)\left(\prod_{p\equiv 3 \bmod 4}\frac{1}{1+1/p^s}\right)$$

$$= \frac{1}{1-1/2^s}\left(\prod_{p \text{ odd}}\frac{1}{1-1/p^s}\right)\left(\prod_{p\equiv 1 \bmod 4}\frac{1}{1-1/p^s}\right)\left(\prod_{p\equiv 3 \bmod 4}\frac{1}{1+1/p^s}\right)$$

$$= \zeta(s)\left(\prod_{p\equiv 1 \bmod 4}\frac{1}{1-\chi(p)/p^s}\right)\left(\prod_{p\equiv 3 \bmod 4}\frac{1}{1-\chi(p)/p^s}\right)$$

$$= \zeta(s)\left(\prod_{p \text{ odd}}\frac{1}{1-\chi(p)/p^s}\right)$$

$$= \zeta(s)\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}.$$

And finally, invoking Corollary 3.26, we have

$$r_1(n) = \sum_{d|n} \chi(d)\,.$$

That's the punchline (applause)—we have proved Theorem 3.24, which gives the number of representations of an integer as a sum of two squares.

We have seen that the classification of the irreducible elements in $\mathbb{Z}[i]$ using Dirichlet series gives a remarkably simple proof of the representation formula of an integer as the sum of two squares. For a proof not using Dirichlet series, see, for example, Hardy and Wright [35] or Niven and Zuckerman [61]. Both texts are excellent introductions to elementary number theory.

Exercises

3.19 If α and β are two strongly multiplicative functions, show that the function γ defined by

$$\gamma(n) = \sum_{d|n} \alpha(d)\,\beta\frac{n}{d}$$

is also strongly multiplicative.

3.5 Supplement: Hilbert's 17th Problem

At the International Congress of Mathematicians held in Paris in 1900, Professor David Hilbert delivered an address entitled "Mathematical Problems." Here is the opening statement of his address:

> Wer von uns würde nicht gern den Schleier lüften, unter dem die Zukunft verborgen liegt, um einen Blick zu werfern auf die bevorstehenden Fortschritte unserer Wissenschaft und in die Geheimnisse ihrer Entwicklung während der künftigen Jahrhunderte!

And here is a translation:

> Who among us would not gladly lift the veil behind which the future lies hidden to cast a glance at the coming advances of our science and the secrets of its development in future centuries?

Hilbert, then still in his thirties and recognized by many as the greatest living mathematician, then proceeded to discuss twenty-three problems that he considered the most pressing at that time. The problems range over analysis, geometry, topology, number theory, and algebra. The seventeenth problem is easy to state.

Consider the rational numbers $\mathbb{Q}$ and the field of rational functions

$$\mathbb{Q}(x_1, \ldots, x_n)$$

in n variables. Recall that this means that an element of $\mathbb{Q}(x_1, \ldots, x_n)$ looks like

$$\frac{f(x_1, \ldots, x_n)}{g(x_1, \ldots, x_n)},$$

where f and g are polynomials in $x_1, \ldots, x_n$ with coefficients in $\mathbb{Q}$. Call such a rational function *definite* if

$$\frac{f(\alpha_1, \ldots, \alpha_n)}{g(\alpha_1, \ldots, \alpha_n)} \geq 0$$

whenever $\alpha_1, \ldots, \alpha_n$ are n rational numbers such that $g(\alpha_1, \ldots, \alpha_n) \neq 0$. Hilbert asked whether every definite element in $Q(x_1, \ldots, x_n)$ can be represented as the sum of a finite number of squares of rational functions. This seemingly simple question had to wait until 1926 for a solution, when Emil Artin answered the question in the affirmative. His solution follows from his work with Otto Schreier on formally real fields. Hilbert himself had already shown that every definite polynomial in two variables can be represented as the sum of four squares. The question of how many squares would be needed for n variables remained unsettled. Then in 1966, James Ax conjectured that 2^n squares should do it, and his conjecture was proved by Albrecht Pfister in 1967.

Lookout Point 3.7. One can seek, however, more quantitative information by asking, for a given field F, the smallest number $t(F)$ such that if $\alpha \in F$ can be represented as a sum of squares, then it can be done with $t(F)$ squares. Pfister's theorem implies that $t(\mathbb{R}) \leq 2^n$. It is also known that $t(\mathbb{R}) \geq n + 1$, because J. W. S. Cassells proved in 1964 that $1 + x_1^2 + \cdots + x_n^2$ cannot be written as a sum of n squares in $\mathbb{R}(x_1, \ldots, x_n)$. Hence

$$n + 1 \leq t(\mathbb{R}) \leq 2^n.$$

But nobody knows what the actual value of $t(\mathbb{R})$ is! Cassels, William Ellison, and Pfister showed in 1971 that in the case of two variables, the answer is 4. In other words, every rational function that is a sum of squares can be expressed as the sum of at most four squares, and furthermore, three won't do for at least one definite function. Indeed, they exhibited the function

$$f(x, y) = 1 + x^2 \left(x^2 - 3\right) y^2 + x^2 y^4$$

and showed that although f is definite, it is not the sum of three squares of rational functions in $\mathbb{R}(x, y)$. Their proof is very difficult and uses a lot of fancy algebraic geometry.

As you can see, the problem is still very much alive. The solution to Hilbert's original question only led to more problems. Such is the nature of mathematics. As Hilbert said, "Moreover, a mathematical problem should be difficult in order to entice us, yet not completely inaccessible, lest it mock our efforts." And in another place, Hilbert reminds us, "As long as a branch of science

offers an abundance of problems, so long is it alive; a lack of problems foreshadows extinction or the cessation of independent development."

In 1930, Hilbert wrote a paper, "Naturerkennen und Logik," which he delivered at the Kongress der Gesellschaft Deutscher Naturforscher und Ärtze, which ends with these words:

> Wir müssen wissen.
> Wir werden wissen.[2]

[2] Naturerkennen und Logik = logic and the understanding of nature; Kongress der Gesellschaft Deutscher Naturforscher und Ärtze = conference of the Association of German Naturalists and Physicians; Wir müssen wissen, Wir werden wissen = we must know; we shall know.

4 The Fundamental Theorem of Algebra

The field $\mathbb{C}$ of complex numbers has the remarkable property that every non-constant polynomial with coefficients in that field has a root in that field. An arbitrary field F with this property is said to be *algebraically closed*.

That $\mathbb{C}$ is algebraically closed is not an obvious fact, and there are numerous proofs from various points of view. The proofs are roughly grouped into those that exploit the algebraic aspect of the theorem and those that use mainly topology and analysis.

The fundamental theorem guarantees the *existence* of roots of polynomial equations, but it doesn't provide methods for *finding* roots—that is another whole can of worms. There are classes of equations, such as quadratic equations and cyclotomic equations, for which solution algorithms exist, but there are no general methods that apply to all polynomial equations. In this chapter, we will be (very) happy just establishing the existence of solutions.

See [19, Chapter 3] for more on algorithms for solving equations.

4.1 Getting Started

First, note that it is enough to establish the fundamental theorem of algebra for polynomials with *real* coefficients. For if f has complex coefficients, then $f\bar{f}$ has real coefficients, where $\bar{f}$ is the polynomial obtained from f by replacing each coefficient by its complex conjugate (this is Exercise 4.1). Then a root α of $f(x)\bar{f}(x)$ will satisfy either $f(\alpha) = 0$ or $\bar{f}(\alpha) = 0$. In the latter case, taking conjugates gives $f(\bar{\alpha}) = 0$.

The theorem then says that the field obtained from $\mathbb{R}$ by adjoining a root of $x^2 + 1 = 0$ is algebraically closed. It seems rather amazing, viewed abstractly, that one can arrive at an algebraically closed field from a given field by adjoining a root of a single polynomial. A beautiful theorem of Emil Artin and Otto Schreier states that if $E \supset F$, where E is any algebraically closed field that is a finite-dimensional vector space over F, then if $F \neq E$, one can conclude that $E = F(i)$, where i satisfies $x^2 + 1 = 0$.

It is easy to find fields that are not algebraically closed:

(i) No subfield of $\mathbb{R}$ ($\mathbb{Q}$, for example) is algebraically closed (why?).

(ii) Consider the simplest field $\mathbb{Z}_2$, of two elements. Then $x^2 + x + 1$ has no root in $\mathbb{Z}_2$.

(iii) If $\mathbb{Z}_p$ is the field with p elements, where p is prime, then $x^p - x + 1$ has no root in $\mathbb{Z}_p$ by Fermat's little theorem.

K. Ireland and A. Cuoco, *Excursions in Number Theory, Algebra, and Analysis*, Readings in Mathematics, https://doi.org/10.1007/978-3-031-13017-5_4

(iv) A formally real field—a field in which -1 is not the sum of squares, will not be algebraically closed.

It is even easier than that. If the elements of F are $a_1, \ldots, a_n$, then $(x - a_1)(x-a_2)\cdots(x-a_n)+1$ has no root.

(v) In the same way, no finite field can be algebraically closed. For let F be finite. Then F^* is a finite group with, say, $n-1$ elements. By elementary group theory, $x^{n-1} = 1$ for all $x \neq 0$. Hence $x^n - x + 1$ has no root in F.

(vi) More generally, if F is an ordered field such that $\alpha^2 > 0$ for $\alpha \neq 0$, then F will not be algebraically closed.

Don't get the impression that $\mathbb{C}$ is the end of the road. For let t be an indeterminate and consider the field $\mathbb{C}(t)$ of rational functions in t with complex coefficients. Since $x^2 - t$ has no root in $\mathbb{C}(t)$, we see that $\mathbb{C}(t)$ is not algebraically closed. You should write out a proof of this.

We will need a more abstract (and hence more general) description of the real numbers. The set of real numbers $\mathbb{R}$ can be described axiomatically as a *complete Archimedean ordered field*. It is constructed from $\mathbb{Q}$ by a completion process: First, one puts the usual absolute value $|r|$ on $\mathbb{Q}$ by means of the *order* relation in $\mathbb{Q}$, namely, $|r| = r$ if $r > 0$ and $|r| = -r$ if $r \leq 0$. Using this absolute value, one defines *Cauchy sequences*. Two Cauchy sequences $\{a_n\}$ and $\{b_n\}$ are called *equivalent* if $a_n - b_n$ has limit zero as $n \to \infty$. Then equivalence classes of Cauchy sequences form a field that contains an isomorphic (structurally identical) copy of $\mathbb{Q}$ and is complete (Cauchy sequences converge to a limit in the field), ordered, and Archimedean (if $\alpha > 0$, then $\alpha + \alpha + \cdots$ gets as big as you like). The order relation plays a very important role in this construction. The complete Archimedean order on $\mathbb{R}$ already gives substantial information about the roots of polynomials.

See Section 3.1 of Chapter 3 for what we mean by *Archimedean*.

"*This*" absolute value? Yes, there are others. Read on.

A Cauchy sequence (a_n) is one whose terms can be made as close together as you like by taking n large enough.

For example, one of the main theorems in elementary analysis is the intermediate value theorem, a result first proved by Bernard Bolzano in 1817. It implies that if a continuous real-valued function defined on $[a, b]$ (the closed interval from a to b) satisfies the conditions $f(a) < 0$ and $f(b) > 0$, then there is a real number ξ with $f(\xi) = 0$. In particular, if f is a monic polynomial in $\mathbb{R}[x]$ of odd degree, convince yourself that $f(x) < 0$ for x very negative and $f(x) > 0$ for x very positive. It follows that $f(x)$ has a real root. Hence to prove the fundamental theorem of algebra, which is the historical name for the fact that $\mathbb{C}$ is algebraically closed, one has "only" to deal with polynomials of even degree.

Lookout Point 4.1. Another way of stating the result about polynomials of odd degree goes like this: *there is no field E containing the field of real numbers $\mathbb{R}$ such that E is a finite-dimensional vector space over $\mathbb{R}$ of odd degree greater than* 1.

To see this, suppose that E is a finite-dimensional vector space of odd degree over $\mathbb{R}$. Take an element $\alpha \in E$. Since E is finite-dimensional over $\mathbb{R}$, we see that for some n, the powers $1, \alpha, \alpha^2, \ldots, \alpha^n$ are $\mathbb{R}$-linearly dependent. Thus α is the root of a polynomial. Let f be the monic polynomial of minimal degree m that has α as a root. By Theorem 2.7 in Section 2.2, we see that $\mathbb{R}(\alpha)$ is a field that is a vector space of dimension m over $\mathbb{R}$. Thus we have a tower:

$$\begin{array}{c} E \\ | \\ \mathbb{R}(\alpha) \\ m \,| \\ \mathbb{R} \end{array}$$

Then by Exercise 2.38 in the same section, it follows that m divides the degree of E over $\mathbb{R}$, which forces m to be odd. But the intermediate value theorem then shows that $f(x)$ has a root in $\mathbb{R}$, which shows that $f(x)$, an *irreducible* polynomial, must be $x - \alpha$. Thus $\alpha \in \mathbb{R}$. Since α was arbitrary, we conclude that $E \subset \mathbb{R}$, and so $E = \mathbb{R}$. This observation will be useful to us later, when we see how the fundamental theorem of Galois theory gives a very short proof that $\mathbb{C}$ is algebraically closed.

Incidentally, there are other ways to put an absolute value on $\mathbb{Q}$. First we must decide what an "absolute value" is. It is a real-valued function $|\cdot|$ on $\mathbb{Q}$ such that

$$\begin{aligned} |x| \geq 0, \text{ and } |x| = 0 \text{ if and only if } x = 0, \\ |xy| = |x|\,|y|, \\ |x + y| \leq |x| + |y|. \end{aligned}$$

To find other absolute values on $\mathbb{Q}$, fix a prime p. If $n \in \mathbb{Z}$, $n \neq 0$, write $n = p^a m$, $p \nmid m$. Define $|n|_p = p^{-a}$. Thus n is "small" if a high power of p divides it. If $a/b \in \mathbb{Q}$, $b \neq 0$, put

$$\left|\frac{a}{b}\right|_p = \frac{|a|_p}{|b|_p}.$$

Show that this doesn't depend on the way $\frac{a}{b}$ is written (Euclid!), and check that $|\alpha + \beta|_p \leq |\alpha|_p + |\beta|_p$. This is enough to put the Cauchy machine into action: you can now form sequences and equivalence classes and finally arrive at a field, denoted by $\mathbb{Q}_p$, that contains $\mathbb{Q}$ and is complete; but it is not Archimedean, because $|n|_p \leq 1$ for all integers n! (that is an exclamation point, not a factorial symbol).

Lookout Point 4.2. Thus one can construct infinitely many new fields $\mathbb{Q}_2, \mathbb{Q}_3, \mathbb{Q}_5, \mathbb{Q}_7, \mathbb{Q}_{11}, \ldots$, arising from different absolute values on $\mathbb{Q}$. The number-theoretic mystique requires that one write $\mathbb{Q}_\infty$ in place of $\mathbb{R}$. From this point of view, $\mathbb{Q}_\infty$ occupies a very special position, for unlike $\mathbb{Q}_\infty$, the field $\mathbb{Q}_p$ for $p \neq \infty$ *never* has the property that $\mathbb{Q}_p(s)$, where s is a symbol satisfying $s^2 = -1$, is algebraically closed! In fact, one can show that if $p \equiv 1 \bmod 4$, then -1 is actually a square in $\mathbb{Q}_p$. Furthermore, there are irreducible polynomials of arbitrarily high degree over $\mathbb{Q}_p$. For example $x^3 + p$ has no root in $\mathbb{Q}_p$, in contrast to the case for $\mathbb{Q}_\infty$. These observations are not deep, but they require a little better understanding of $\mathbb{Q}_p$ than is offered here.

Very readable introductions to this "p-adic" land include [3, 33, 45].

Thus it is a remarkable fact of nature that one can get from $\mathbb{R}$ to an algebraically closed field with so little effort. In general, one has to be content

with an abstract construction. Indeed, there is a basic result established in every commutative algebra course that asserts that for every field F, one can construct a field E that contains F and is algebraically closed. Furthermore, every element in E is algebraic over F. This last condition does not follow from the fact that E is algebraically closed. For example, we shall see in Chapter 6 that π is not algebraic over $\mathbb{Q}$. The field of all complex numbers that are *algebraic* over $\mathbb{Q}$ is algebraically closed. Can you prove this, assuming that $\mathbb{C}$ is algebraically closed? It is a good exercise (and it is Exercise 4.4).

Gauss found a proof that $\mathbb{C}$ is algebraically closed in 1797 and published it as his PhD thesis in 1799. During his lifetime, Gauss discovered a number of proofs of the theorem and published four in all. They appeared in 1799, 1816 (two proofs), and 1850. In the following, we will give a number of proofs. After giving a particularly simple proof that relies on a few basic facts from elementary analysis, we examine other proofs that involve more background. One is based on an idea of Gauss and uses the theorem on symmetric functions. Except for the existence of an abstract field containing the roots of a polynomial over a given field, this proof is completely elementary. On the other hand, we will show how a very simple proof (Artin, 1926) can be derived from the basic result of Galois theory. The field $\mathbb{C}$ is a very special field, and it is perfectly reasonable to ask whether one can verify that it is algebraically closed by applying general algebraic theorems. But algebra alone will not do. We will discuss this later in this chapter after we work through several proofs of the theorem.

Of course, we shall not prove the fundamental theorem of Galois theory but just content ourselves with giving a clear statement.

Take It Further

On the other hand, anyone who has had a basic course in complex analysis is familiar with proofs using complex integration theory. Polynomials are entire functions (holomorphic in the whole complex plane), and if a polynomial f has no zeros, then it is bounded away from zero, and therefore $1/f$ is a bounded entire function. Hence by Liouville's theorem, it is constant. Another complex-analytic proof that exploits the topological character of the mapping $f(x)$ is the following. A basic result in complex analysis is that holomorphic functions (analytic, regular) are open. That is, they map open sets onto open sets. For polynomials, this turns out to be equivalent to the fact that $\mathbb{C}$ is algebraically closed.

The definition of *holomorphic function* is in Section 4.7.

In the next section, we will begin a completely rigorous proof of the theorem. But first, some exercises:

Exercises

4.1 Show that if $f \in \mathbb{C}[x]$, then $f\bar{f}$ has real coefficients, where $\bar{f}$ is the polynomial obtained from f by replacing each coefficient by its complex conjugate

4.2 Prove the claim made in this section that the equivalence classes of Cauchy sequences form a field that contains an isomorphic copy of $\mathbb{Q}$.

4.3 Referring to the definition of $|\cdot|_p$ in this section, prove a strong triangle inequality: If α and β are integers, then

$$|\alpha+\beta|_p \le \max\left\{|\alpha|_p, |\beta|_p\right\} .$$

Also, show that equality holds if $|\alpha|_p \neq |\beta|_p$.

4.4 Take It Further. Assuming that $\mathbb{C}$ is algebraically closed, show that the field of all complex numbers that are *algebraic* over $\mathbb{Q}$ is algebraically closed.

4.5 Prove Corollary 4.3.

4.2 Background from Elementary Analysis

Consider $\mathbb{R}\times\mathbb{R}$ as the Euclidean plane with its usual metric. The distance function allows one to introduce the notions of boundedness and closedness for subsets. We need to use the fact that $\mathbb{R}\times\mathbb{R}$ is complete as a metric space. In other words, if $\xi_1, \xi_2, \ldots$ are in $\mathbb{R}\times\mathbb{R}$ and if $\|\xi_i - \xi_j\| \to 0$ as $i, j \to \infty$ (more precisely, if given $\epsilon > 0$, there exists an integer N such that $\|\xi_i - \xi_j\| < \epsilon$ for $i, j > N$), then there is a point $\xi \in \mathbb{R}\times\mathbb{R}$ such that $\|\xi - \xi_i\| \to 0$. A set $A \subset \mathbb{R}\times\mathbb{R}$ is said to be *closed* if A contains all its limit points. In other words, if $\xi_i \to \xi$, $\xi_i \in A$, then $\xi \in A$. If A is closed and bounded, then we say that A is *compact*.

Here $\|z\|$ denotes the distance from z to the origin.

Lemma 4.1. *Let f be a real-valued continuous mapping defined on a compact set A in $\mathbb{R}\times\mathbb{R}$. Then f is bounded on A. That is, there exists N such that $|f(x)| < N$ for all $x \in A$.*

Proof. Since A is compact, put a big square S around it. Divide the square into four congruent squares. If f is unbounded on A, then it is unbounded on a part of A inside one of the smaller squares. Pick one of those squares and call it S_1. Take $\xi_1 \in S_1 \cap A$ with $|f(\xi_1)| > 2$. Divide S_1 into four squares. Since $f(x)$ is unbounded in S_1, it is unbounded in one of the new smaller squares, say S_2. Take $\xi_2 \in S_2 \cap A$ with $|f(\xi_2)| > 4$. Continuing in this way, we get a sequence $\{\xi_i\}$ in which $f(\xi_i) > 2^i$ for each i.

Consider $\bigcap_{i=1}^{\infty} S_i = \{\xi\}$, which must be a single point. Since A is closed, we have $\xi \in A$. Now, $\xi_i \in S_i \cap A$ implies that $\xi_i \to \xi$. Furthermore, since f is continuous, it follows that $f(\xi_i) \to f(\xi)$. But then for every positive integer i, we must have

$$2^i < |f(\xi_i)| \le |f(\xi) - f(\xi_i)| + |f(\xi)| .$$

Since $|f(\xi) - f(\xi_i)|$ goes to zero, we have a ridiculous situation. Since mathematics is not ridiculous, we have proved the lemma. ∎

Lemma 4.2. *Let f be a real-valued continuous function defined on a compact set A in $\mathbb{R}\times\mathbb{R}$. Then there exists $\xi \in A$ such that $f(x) \le f(\xi)$ for all $x \in A$.*

Proof. By the preceding lemma, the set of real numbers $f(A)$ is a bounded set. By a fundamental property of $\mathbb{R}$, there is a least upper bound ("maxi-

mum") τ to $f(A)$. Recall that this τ is characterized by the following properties:

(i) $\tau \geq \alpha$ for $\alpha \in f(A)$.

(ii) Given $\epsilon > 0$, there exists $\beta \in f(A)$ such that $\beta > \tau - \epsilon$.

Choose $\alpha, \tau_i \in f(A)$ such that $\alpha \geq \tau_i > \tau - 1/2^i$. Then $\tau_i = f(\xi_i)$ for some ξ_i, and $\tau_i \to \tau$. Now, $\{\xi_i\}$ is a bounded sequence of points in A, and a bisection argument shows that $\{\xi_i\}$ has a convergent subsequence. Call this subsequence ξ_{ρ_i}. Then $\xi_{\rho_i} \to \mu$, and since A is closed, we see that $\mu \in A$. Since f is continuous, we conclude that $f(\xi_{\rho_i}) \to f(\mu)$. But $f(\xi_{\rho_i}) \to \tau$, and so $f(\mu) \to \tau$. Thus τ, the least upper bound of $f(A)$, is attained by an element of A. This finishes the proof. ∎

Corollary 4.3. *Given f and A as above, there is an element $b \in A$ such that $f(x) \geq f(b)$ for all $x \in A$.*

Proof. Exercise 4.5. ∎

This completes the analytic preliminaries, with the exception of one more comment. The equation $x^n = \alpha$ for $\alpha \in \mathbb{C}$ always has a root in $\mathbb{C}$. First of all, if $r > 0$, then $\sqrt[n]{r}$ exists as a real number. Then de Moivre gives

$$\sqrt[n]{r}\left(\cos\frac{\theta}{n} + i\sin\frac{\theta}{n}\right)$$

as a root, where $\alpha = r(\cos\theta + i\sin\theta)$. Thus the proof of the fundamental theorem of algebra that follows also uses the existence of $\sin x$ and $\cos x$. Can you show that $x^n = \alpha$ has a root without trigonometry (and of course, without already knowing that $\mathbb{C}$ is algebraically closed)?

4.3 First Proof of the Fundamental Theorem of Algebra: An Analytic Approach

This proof is adapted from the classic calculus text by Edmund Landau [46]. The only facts we need from analysis are the theorem that continuous functions on compact sets attain their maxima and minima and de Moivre's theorem.

The fact that $\mathbb{C}$ is algebraically closed will follow immediately from the following two lemmas.

Convince yourself that together, these two lemmas imply that $\mathbb{C}$ is algebraically closed.

Lemma 4.4. *Given a polynomial $f(x) \in \mathbb{C}[x]$, there is a complex number α such that $|f(x)| \geq |f(\alpha)|$ for* all *$x \in \mathbb{C}$.*

Lemma 4.5. *If f is a nonconstant polynomial in $\mathbb{C}[x]$, then given $\alpha \in \mathbb{C}$ for which $f(\alpha) \neq 0$, there exists $\beta \in \mathbb{C}$ such that $|f(\beta)| < |f(\alpha)|$.*

Lemma 4.4 is not immediate. We cannot apply Lemma 4.2, for although $f(x)$ is a continuous real-valued function, the domain $\mathbb{C}$ is not compact (it is closed but not bounded). However, it is the easier of the two lemmas:

Proof of Lemma 4.4. We shall use the following fact: for complex numbers α and β, one has $|\alpha+\beta| \geq |\alpha| - |\beta|$. This follows from the triangle inequality $|a+b| \leq |a| + |b|$ by replacing a by $\alpha+\beta$ and b by $-\beta$.

Consider a polynomial $f(x)$, which we may normalize to the form

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0.$$

Then by the above, we see that

$$\begin{aligned} |f(x)| &\geq |x|^n - |a_{n-1}x^{n-1} + \cdots + a_0| \\ &\geq |x|^n \left(1 - \left|\frac{a_{n-1}}{x} + \frac{a_{n-2}}{x^2} + \cdots + \frac{a_0}{x^n}\right|\right). \end{aligned}$$

If $|x|$ is sufficiently large, then $\left|\frac{a_{n-1}}{x} + \cdots + \frac{a_0}{x^n}\right| < \frac{1}{2}$, say. Thus for $|x| > R$, we have $|f(x)| \geq |x|^n/2$.

Now choose $|x|$ larger (if necessary) so that $|x|^n/2 > |a_0| = |f(0)|$. With this adjustment, we now see that outside some big disk ($|x| > R_1$), we have

$$|f(x)| > |f(0)| \quad \text{for } x > R_1\,.$$

Inside the closed disk defined by $|x| \leq R_1$ (which is compact!), there exists α such that by the corollary to Lemma 4.2 applied to the continuous function $|f(x)|$ on a compact set (the closed disk of radius R_1), we have

$$|f(x)| \geq |f(\alpha)| \quad \text{for } |x| \leq R_1\,.$$

Oh, and note that $|f(0)| \geq |f(\alpha)|$ too, because 0 is in the disk! So, even outside the disk ($|x| > R_1$), we have

$$|f(x)| > |f(0)| \geq |f(\alpha)|\,.$$

This shows that for every $x \in \mathbb{C}$, we have

$$|f(x)| \geq |f(\alpha)|,$$

which finishes the proof of Lemma 4.4. ∎

The proof of Lemma 4.5 is a little more subtle. We will start with a particular form for $f(x)$ and then show how to reduce f to this special form. And so … we need (yet) another lemma:

Lemma 4.6. *Suppose $n \geq m$ and f has the following special form:*

That is, $f(0) = 1$ and the lowest-degree term besides the constant term has coefficient -1.

$$f(x) = 1 - x^m + a_{m+1}x^{m+1} + \cdots + a_n x^n\,.$$

Then there is a real number ξ, $0 < \xi < 1$, such that $|f(\xi)| < 1$.

Proof. To see this, apply the (generalized) triangle inequality: for every $x \in \mathbb{C}$, we have

$$|f(x)| \leq |1 - x^m| + \left|a_{m+1}x^{m+1}\right| + \cdots + |a_n x^n|\,.$$

If we restrict x to $0 < x < 1$, then $1 - x^m > 0$ and $\left|a_{m+i}x^{m+i}\right| = |a_{m+i}|\,x^{m+i}$, so we can make this inequality even stronger:

$$|f(x)| \le 1 - x^m + |a_{m+1}|x^{m+1} + |a_{m+2}|x^{m+2} + \cdots + |a_n|x^n\,.$$

Factor out x^m:

$$\begin{aligned}|f(x)| &\le 1 - x^m\left[1 - \left(|a_{m+1}|x^1 + |a_{m+2}|x^2 + \cdots + |a_n|x^{n-m}\right)\right]\\ &:= 1 - x^m[1 - B(x)]\,.\end{aligned}$$

We can now choose x close enough to zero to make $0 < B(x) < 1$, and so we have $0 < 1 - x^m[1 - B(x)] < 1$. Done. ∎

And now ... on to Lemma 4.5. It has been a while, so recall what we want to prove:

> If f is a nonconstant polynomial in $\mathbb{C}[x]$ and α is a complex number for which $f(\alpha) \neq 0$, we want to show that there exists $\beta \in \mathbb{C}$ such that $|f(\beta)| < |f(\alpha)|$.

Here we go ...

Proof of Lemma 4.5. Suppose now that

$$f(x) = a_0 + a_m x^m + \cdots + a_n x^n\,.$$

We can assume that $a_0 \neq 0$ (otherwise, we would be wasting our time).

Let

$$g(x) = \frac{f(x)}{a_0} = 1 + \frac{a_m}{a_0}x^m + \cdots + \frac{a_n}{a_0}x^n\,.$$

Now, to make this look like the special case, we construct

$$g\left(\sqrt[m]{-\frac{a_0}{a_m}}\,x\right) = 1 - x^m + \text{ terms of higher degree}\,,$$

where $\sqrt[m]{-\frac{a_0}{a_m}}$ is any one of the roots of $x^m - \frac{a_0}{a_m} = 0$ in $\mathbb{C}$ (de Moivre!). So, by our special case, there is a real number ξ such that

$$\left|g\left(\sqrt[m]{-\frac{a_0}{a_m}}\,\xi\right)\right| < 1\,,$$

or since $g = \frac{f}{a_0}$,

$$\left|f\left(\sqrt[m]{-\frac{a_0}{a_m}}\,\xi\right)\right| < a_0 = f(0)\,.$$

So there exists τ such that

$$|f(\tau)| < f(0)\,.$$

Almost there. One more clever transformation: Suppose $f(\alpha) \neq 0$. Consider the polynomial in $\mathbb{C}[x]$ defined by $h(x) = f(\alpha + x)$. Then by Lemma 4.6 applied to h, there exists τ' such that

$$f(\alpha + \tau') = h(\tau') < h(0) = f(\alpha)\,.$$

Bingo: We have built a β that the lemma promised. ∎

This completes the proof of Lemma 4.5 and our first proof of the fundamental theorem of algebra. Notice that besides using the existence of minima for continuous functions on compact sets in $\mathbb{R} \times \mathbb{R}$, we have used de Moivre's theorem to find mth roots of $-a_0/a_m$. In later, more algebraic, proofs we still need to use properties of continuous functions on compact sets, but we will need to assume only that if $\alpha \in \mathbb{C}$, then there exists $\beta \in \mathbb{C}$ with $\beta^2 = \alpha$. This can be shown without de Moivre. Nevertheless, the above proof is extremely elegant and is just about the simplest we know.

4.4 Background from the Theory of Equations

The proof of the algebraic closure of $\mathbb{C}$ presented in Section 4.3 leaned heavily on classical analysis and the order relation in $\mathbb{R}$. Furthermore, we used the extension of the absolute value to $\mathbb{C}$ and the triangle inequality in $\mathbb{C}$. The only analytic fact used in the proof developed in this section is that every polynomial of odd degree in $\mathbb{R}[x]$ has a real root. All the rest of the argument is algebraic.

A very old result from algebra is the theorem on symmetric functions. It played an important role in the classical development of the theory of equations and Galois theory. We shall develop the result in a little more generality than we need.

Consider an integral domain D and n indeterminates $x_1, \ldots, x_n$. As usual, $D[x_1, \ldots, x_n]$ denotes the ring of all polynomials in $x_1, \ldots, x_n$ with coefficients in D. We are interested in the following special polynomials:

$$\begin{aligned}
\sigma_1 &= x_1 + x_2 + \cdots + x_n\,,\\
\sigma_2 &= x_1x_2 + x_1x_3 + \cdots + x_1x_n + x_2x_3 + x_2x_4 + \cdots = \sum_{i<j} x_ix_j\,,\\
\sigma_3 &= \sum_{i<j<k} x_ix_jx_k\,,\\
&\vdots\\
\sigma_n &= x_1x_2\cdots x_n\,.
\end{aligned}$$

These are called the *elementary symmetric functions*. For example, consider $D[x_1, x_2, x_3, x_4]$. Then

$$\begin{aligned}
\sigma_1 &= x_1 + x_2 + x_3 + x_4 \ \text{(the sum)},\\
\sigma_2 &= x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4 \ \text{(the sum two at a time)},\\
\sigma_3 &= x_1x_2x_3 + x_1x_3x_4 + x_2x_3x_4 \ \text{(the sum three at a time)},\\
\sigma_4 &= x_1x_2x_3x_4 \ \text{(the "sum" four at a time)}.
\end{aligned}$$

The polynomials $\sigma_1, \ldots, \sigma_n$ all satisfy the important property that each remains the same when the variables are permuted in any of the $n!$ different ways (recall that a permutation of $\{1, 2, \ldots, n\} = T$ is a one-to-one mapping of T onto itself). In fancy language, they are invariant under the action of

the symmetric group S_n on n letters. However, there are other polynomials invariant under S_n as well. For example, $x_1^2 + x_2^2 + \cdots + x_n^2$ is invariant. Such polynomials that are invariant under the action of S_n are called called symmetric. But

$$(x_1 + \cdots + x_n)^2 = x_1^2 + \cdots + x_n^2 + 2\sum_{i<j} x_i x_j\,,$$

and so $x_1^2 + \cdots + x_n^2 = \sigma_1^2 - 2\sigma_2$, and we see that $x_1^2 + \cdots + x_n^2$ belongs to the ring $D[\sigma_1, \sigma_2, \ldots, \sigma_n]$ of all polynomials in $\sigma_1, \sigma_2, \ldots, \sigma_n$. The theorem on symmetric functions states that this is always the case, namely that every symmetric polynomial can be written as a polynomial in the *elementary* symmetric polynomials.

Theorem 4.7. *Let $f(x_1, \ldots, x_n) \in D[x_1 \cdots x_n]$, and suppose that*

$$f(x_1, \ldots, x_n) = f(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)})$$

for every permutation σ of the integers $1, \ldots, n$. Then

$$f(x_1 \cdots x_n) \in D[\sigma_1, \sigma_2, \ldots, \sigma_n].$$

For a refresher on determinants, see [20, Chapter 9].

There are a number of proofs of this result. We give a proof that supplies a little more information. First of all, we need to calculate the famous Vandermonde determinant.

Lemma 4.8.

$$\begin{vmatrix} 1 & x_1 & \cdots & x_1^{n-1} \\ 1 & x_2 & \cdots & x_2^{n-1} \\ \vdots & \vdots & \cdots & \vdots \\ 1 & x_n & \cdots & x_n^{n-1} \end{vmatrix} = \prod_{i>j} (x_i - x_j)\,.$$

Proof. By replacing the ith row by itself minus the jth row and noticing that $x_i - x_j$ divides $x_i^s - x_j^s$, we see that $x_i - x_j$ divides the left-hand side. But the various $x_i - x_j$ for different pairs (i, j), $i > j$, are relatively prime. Hence the right-hand side divides the left-hand side (here we used the fact that $D[x_1, \ldots, x_n]$ is a unique factorization domain). But the left-hand side has degree $n(n-1)/2$, since $1 + 2 + 3 + \cdots + n - 1 = n(n-1)/2$, and so does the right-hand side, since $\binom{n}{2} = n(n-1)/2$. Therefore, they differ by a constant. As an exercise, show that the constant is 1.

Another proof, perhaps simpler, is to continue to operate on the rows and columns. We proceed by induction on n. Check the lemma for $n = 1$ and 2. Then if we subtract from each column, beginning with the second, x_1 times the column preceding it on the left, we obtain

$$\begin{vmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & x_2 - x_1 & x_2^2 - x_1 x_2 & \cdots & x_2^{n-1} - x_1 x_2^{n-2} \\ \vdots & \vdots & \cdots & \vdots & \\ 1 & x_n - x_1 & x_n^2 - x_1 x_n & \cdots & x_n^{n-1} - x_1 x_n^{n-2} \end{vmatrix}.$$

But now we can kill all the ones in the first column except the top one by subtracting the first row from each of the other rows. Then you see that the resulting rows have $x_2 - x_1$, $x_3 - x_1, \ldots, x_n - x_1$ as a common factor, and so we have the whole determinant equal to

$$(x_2 - x_1)(x_3 - x_1)\cdots(x_n - x_1) \begin{vmatrix} 1 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 1 & x_2 & x_2^2 & \cdots & x_2^{n-2} \\ \vdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 1 & x_n & x_n^2 & \cdots & x_n^{n-2} \end{vmatrix}$$

$$= (x_2 - x_1)\cdots(x_n - x_1) \prod_{\substack{i>j \\ i,j\neq 1}} (x_i - x_j)$$

by the inductive hypothesis. But this is simply

$$\prod_{\substack{i>j \\ i,j\leq n}} (x_i - x_j),$$

and that finishes the proof. ∎

Now consider the integral domain $D[x_1, \ldots, x_n]$, which contains the integral domain $D[\sigma_1, \ldots, \sigma_n]$ as a subdomain:

$$\begin{array}{c} D[x_1, \ldots, x_n] \\ | \\ D[\sigma_1, \ldots, \sigma_n]. \end{array}$$

Build the polynomial in a new indeterminate z given by

$$(z - x_1)(z - x_2)\cdots(z - x_n).$$

This polynomial is simply

$$z^n - \sigma_1 z^{n-1} + \sigma_2 z^{n-2} - \cdots + (-1)^n \sigma_n$$

(verify this). It follows that each x_i satisfies the relation

$$x_i^n - \sigma_1 x_i^{n-1} + \sigma_2 x_i^{n-2} - \cdots + (-1)^n \sigma_n = 0\,.$$

This shows that x_i is algebraic over the ring $D[\sigma_1, \ldots, \sigma_n]$.

The following lemma shows that the above polynomial is the minimal polynomial of each x_i as an algebraic quantity over the field of symmetric functions. We state it only for x_1, but the proof is general in principle. Let S denote the subring of $D[x_1, \ldots, x_n]$ consisting of all symmetric polynomials in $x_1, \ldots, x_n$.

In other words, $1, x, x^2, \ldots, x^{n-1}$ are linearly independent over S.

Lemma 4.9. *If*

$$a_{n-1} x_1^{n-1} + a_{n-2} x_1^{n-2} + \cdots + a_0 = 0$$

for $a_0, a_1, \ldots, a_{n-1} \in S$, *then* $a_0 = a_1 = \cdots = a_{n-1} = 0$.

Proof. Since 0 is symmetric, the right-hand side is symmetric. Any permutation that sends x_1 to x_i for $i = 1, \ldots, n$ leaves $a_0, \ldots, a_{n-1}$ fixed by the definition of S. Hence for $i = 1, \ldots, n$, we have

$$a_{n-1}{x_i}^{n-1} + a_{n-2}{x_i}^{n-2} + \cdots + a_0 = 0\,.$$

Hence $(a_{n-1}, a_{n-2}, \ldots, a_0)$ is a solution vector to the homogeneous system of *linear* equations whose coefficient matrix has determinant

$$\begin{vmatrix} {x_1}^{n-1} & {x_1}^{n-2} & \cdots & 1 \\ \vdots & \vdots & \cdots & \\ x_n^{n-1} & {x_n}^{n-2} & \cdots & 1 \end{vmatrix}.$$

But Vandermonde tells us that this determinant is $\prod_{i>j}(x_i - x_j)$, which is nonzero. Hence this matrix is *nonsingular*, and $(a_{n-1}, a_{n-2}, \ldots, a_0)$ must be (identically) the zero vector. This finishes the proof. ∎

Now we can prove the symmetric function theorem (Theorem 4.7), restated more simply as follows.

Theorem 4.10 (Symmetric function theorem). *Let D be an integral domain and S the ring of all symmetric polynomials in $D[x_1, \ldots, x_n]$. Then S is equal to $D[\sigma_1, \ldots, \sigma_n]$, the ring of polynomials in the first n elementary symmetric polynomials.*

Proof. Check that the right-hand side is contained in the left-hand side. In the other direction, let $f(x_1, \ldots, x_n) \in S$. View $f(x_1, \ldots, x_n)$ as a polynomial in $x_2, \ldots, x_n$ with coefficients in $D[x_1]$. We prove the theorem by induction on n. In particular, we shall prove that a symmetric polynomial in n variables over *any* integral domain is a polynomial in $\sigma_1, \ldots, \sigma_n$.

The case $n = 1$ is self-evident: every symmetric polynomial in $D[x]$ is a polynomial in the symmetric polynomial x.

Now assume the result for $n - 1$. Then $f(x_1, \ldots, x_n)$ is certainly symmetric in $x_2, \ldots, x_n$ (we ignore x_1). Hence $f(x_1, \ldots, x_n) = g(x_1, \sigma_1', \ldots, \sigma_{n-1}')$, where $g(X_1, X_2, \ldots, X_n)$ is a polynomial with coefficients in D, and where, of course,

$$\begin{aligned} \sigma_1' &= x_2 + x_3 + \cdots + x_n\,, \\ \sigma_2' &= \sum_{\substack{i<j \\ i,j\geq 2}} x_i x_j\,, \\ &\vdots \\ \sigma_{n-1}' &= x_2 \cdots x_n. \end{aligned}$$

However, there are simple relations between $\sigma_1, \ldots, \sigma_n$ and $\sigma_1', \ldots, \sigma_{n-1}'$.

In fact,

$$\begin{aligned}\sigma_1 &= x_1 + \sigma_1',\\ \sigma_2 &= x_1\sigma_1' + \sigma_2',\\ &\vdots\\ \sigma_{n-1} &= x_1\sigma_{n-2}' + \sigma_{n-1}',\\ \sigma_n &= x_1\sigma_{n-1}'.\end{aligned}$$

Thus each $\sigma_1', \sigma_2', \ldots, \sigma_{n-1}'$ is seen to be a polynomial in $x_1, \sigma_1, \ldots, \sigma_n$ by successive substitution. Hence by substitution, $g(x_1, \sigma_1', \ldots, \sigma_{n-1}')$ becomes a polynomial $h(x_1, \sigma_1, \ldots, \sigma_n)$. Now recall that x_1 satisfies a relation

$$x_1^n - \sigma_1 {x_1}^{n-1} + \cdots + (-1)^n\sigma_n = 0,$$

and therefore, solving for x_1^n and repeatedly substituting, we may lower the degree of $h(x_1, \sigma_1, \ldots, \sigma_n)$ until it has degree less than n in x_1. Write the resulting polynomial as

$$a_0 x_1^{n-1} + a_1 x_1^{n-2} + \cdots + a_{n-1},$$

where $a_0, \ldots, a_{n-1}$ are in $D[\sigma_1, \ldots, \sigma_n]$. Recall that this polynomial is still $g(x_1, \ldots, x_n)$, which is in S. Hence

$$a_0 x_1^{n-1} + a_1 x^{n-2} + \cdots + (a_{n-1} - g) = 0$$

is a polynomial in x_1 with coefficients that are symmetric. According to Lemma 4.9, every coefficient is identically zero. In particular, $a_{n-1} - g = 0$, or $g = a_{n-1}$. Thus $g \in D[\sigma_1, \ldots, \sigma_n]$. This completes the proof. ■

From the point of view of Galois theory we have done the following. The symmetric group on n letters S_n is a group of automorphisms of the ring $R = D[x_1, \ldots, x_n]$. The subring of symmetric polynomials is simply the *fixed ring* of the group S_n. Denote that fixed ring by R_{S_n}. Then Theorem 4.10 above states that $R_{S_n} = D[\sigma_1, \sigma_2, \ldots, \sigma_n]$. The general procedure of descending from a ring with a group operating on it to the fixed ring and investigating the relationship between the group and the rings in between the top one and the fixed one is an extremely important source of information. It is the basic idea behind Galois theory.

4.5 Second Proof of the Fundamental Theorem of Algebra: All Algebra (Almost)

With the aid of the symmetric function theorem we will give another proof that $\mathbb{C}$ is algebraically closed. However, we need one more construction from abstract algebra. In this proof, we need to know that there exist roots somewhere. In other words, we need the fact that if F is a field and $f \in F[x]$, then one can construct a field E in which $f(x)$ has all its roots. Although

the construction of such a field is not particularly difficult, we will assume its existence and include a sketch of the proof in the next subsection. For now, we assume the following result.

Theorem 4.11. *Let F be a field and $f(x)$ a polynomial with coefficients in F. Then there is a field E such that $E \supset F$ and $f(x) = (x-\alpha_1)\cdots(x-\alpha_n)$ with $\alpha_1, \ldots, \alpha_n \in E$.*

Now we prove our main result.

Theorem 4.12. *The field of complex numbers $\mathbb{C}$ is algebraically closed.*

Proof. We will show that every polynomial with *real* coefficients has a complex root. As we mentioned earlier, in Section 4.1, this is sufficient. The proof goes by induction on m, where $\deg f = 2^m n$ and n is odd. If $m = 0$, the result follows from the intermediate value theorem.

So, take a polynomial $f \in \mathbb{R}[x]$ of degree $2^m n$, where $m > 0$. We want to show that $f(x)$ has a complex root. Consider $f(x)$ as a polynomial in $\mathbb{C}[x]$ and let E be a field containing $\mathbb{C}$ that contains all the roots of f.

Let $s = 2^m n$ and $f(x) = \prod_{i=1}^{s}(x-\alpha_i)$, where the α_i are the roots of f. Fix a positive integer h and form the polynomial whose roots are $\alpha_i + \alpha_j + h\alpha_i\alpha_j$ for $i < j$. Namely,

$$g(x) = \prod_{i<j}\big(x - (\alpha_i + \alpha_j + h\alpha_i\alpha_j)\big).$$

The coefficients of g are symmetric in $\alpha_1, \ldots, \alpha_n$. Hence by the symmetric function theorem, they are polynomials (with coefficients in $\mathbb{R}$) in the elementary symmetric functions of $\alpha_1, \ldots, \alpha_n$. But these elementary symmetric functions are the coefficients (up to ± 1) of $f(x)$. Hence $g(x) \in \mathbb{R}[x]$. Now, $\deg g(x) = \binom{s}{2} = s(s-1)/2 = 2^{m-1}n'$, where n' is odd. Hence the power of 2 dividing $\deg g(x) = \binom{s}{2}$ is less than m. By the induction hypothesis, $g(x)$ has a root in $\mathbb{C}$.

The idea is to *vary* the integer h. The induction hypothesis implies that for each h, at least one of the $\alpha_1 + \alpha_j + h\alpha_i\alpha_j$ is in $\mathbb{C}$. So if we let h take on more than $\binom{s}{2}$ integral values, there must be two of the $\alpha_i + \alpha_j + h\alpha_i\alpha_j$ that are in $\mathbb{C}$ with the same i, j. Thus there are distinct integers h_1 and h_2 such that $\alpha_i + \alpha_j + h_1\alpha_i\alpha_j \in \mathbb{C}$ and $\alpha_i + \alpha_j + h_2\alpha_i\alpha_j \in \mathbb{C}$ for some pair (i, j). By subtraction, we obtain $(h_1 - h_2)\alpha_i\alpha_j \in \mathbb{C}$, and so $\alpha_i\alpha_j \in \mathbb{C}$. This implies $\alpha_i + \alpha_j \in \mathbb{C}$. Then

$$(\alpha_i - \alpha_j)^2 = {\alpha_i}^2 + {\alpha_j}^2 - 2\alpha_i\alpha_j = (\alpha_i + \alpha_j)^2 - 4\alpha_i\alpha_j \in \mathbb{C},$$

whence $\alpha_i - \alpha_j \in \mathbb{C}$, since $\mathbb{C}$ certainly contains all its square roots (Exercise 4.6). But then $\alpha_i + \alpha_j \in \mathbb{C}$ implies that $\alpha_i \in \mathbb{C}$. This completes the proof. ∎

Let's review the ingredients of this proof. We needed the intermediate value theorem to get the induction going, the symmetric function theorem to build the polynomial g, and a general lemma from field theory that ensures

the existence of an abstract extension field that houses all the roots of f. All the analysis is tucked away in the statement that polynomials of odd degree with real coefficients have at least one real root.

4.5.1 The Idea behind the Proof of Theorem 4.11: More Modular Arithmetic with Polynomials

We have used the fact that if F is a field and $f \in F[x]$, then one can construct a field E that contains F in which $f(x)$ has all its roots. The fact that there is such a field somewhere up in the sky is due to Kronecker, and it deserves to be celebrated as a theorem:

Theorem 4.13 (Kronecker). *Let F be a field and let $f \in F[x]$ be a non-constant polynomial. Then there exist a field extension E/F and an element $u \in E$ such that $f(u) = 0$.*

A complete proof is in [19, Chapter 7]. But the idea is the same one that we used in the discussion of modular arithmetic with polynomials in Section 3.1. More precisely, we can assume that f is irreducible (and monic) of degree n, and then construct the ring E obtained by reducing elements of $F[x]$ modulo f. The construction is a little intricate, but (to oversimplify) the steps involved include showing the following:

(i) The ring E obtained by replacing each element of $F[x]$ by its remainder on division by f is given a ring structure (exactly as we built $\mathbb{Z}_p$ from $\mathbb{Z}$).

(ii) That makes E into a *field* that contains (an isomorphic copy of) F.

(iii) The image of x in E is a root of f in E (think of the image of x when polynomials in $\mathbb{R}[x]$ are reduced modulo $x^2 + 1$).

(iv) If $g(x) \in F[x]$ and z is a root of g in E, then $f \mid g$ in $F[x]$.

(v) E is a vector space over F, the set $\{1, x, x^2, \ldots, x^{n-1}\}$ is a basis, and

$$\dim_F E = n.$$

A main message here is that the same ideas that lead from $\mathbb{Z}$ to $\mathbb{Z}_p$ can be used as a method that guarantees roots of equations. That's quite wonderful.

As an example, in Lookout Point 2.5, we did a little arithmetic in $\mathbb{Q}[\zeta_5]$, and you checked that

$$\frac{1}{\zeta^3 - \zeta^2 + 2\zeta} = -\frac{1}{11}\left(7\zeta^3 + 9\zeta^2 + 8\zeta + 3\right).$$

As we said there, this value of $\left(\zeta^3 - \zeta^2 + 2\zeta\right)^{-1}$ didn't drop out of the sky. Here's the secret to the story:

The minimal polynomial for ζ_5 is

$$\Phi(x) = x^4 + x^3 + x^2 + x + 1\,.$$

Hence, the Kronecker construction of the field that houses a root of Φ is obtained by reducing polynomials in $\mathbb{Q}[x]$ modulo Φ. So use Euclid's algorithm in $\mathbb{Q}[x]$ to compute

$$\gcd\left(x^3 - x^2 + 2x, \Phi\right).$$

You will get $11/49$, a unit in $\mathbb{Q}[x]$ (try it). Using the functions s and t defined in Lookout Point 3.3, find that

$$\left(\frac{x^3}{7} - \frac{9x^2}{49} - \frac{8x}{49} - \frac{3}{49}\right)\left(x^3 - x^2 + 2x\right) + \left(\frac{x^2}{7} - \frac{5x}{49} + \frac{11}{49}\right)\Phi(x) = \frac{11}{49}\,.$$

So

$$\left(\frac{x^3}{7} - \frac{9x^2}{49} - \frac{8x}{49} - \frac{3}{49}\right)\left(x^3 - x^2 + 2x\right) \equiv \frac{11}{49} \mod \Phi\,.$$

Multiply both sides by $49/11$, and the secret is out.

Exercises

4.6 (i) Without using de Moivre, show that every nonzero complex number $a + bi$ has two square roots in $\mathbb{C}$.

(ii) Use the identity

$$(\alpha_i - \alpha_j)^2 = {\alpha_i}^2 + {\alpha_j}^2 - 2\alpha_i\alpha_j = (\alpha_i + \alpha_j)^2 - 4\alpha_i\alpha_j$$

to derive the quadratic formula without "completing the square."

4.7 Let $\Psi(x) = x^2 + 1$. Reduce each polynomial mod Ψ:

(i) $3 + 2x$ (ii) $3 + 2x + x^2$
(iii) $3 + 2x + x^2 + x^3$ (iv) $3 + 2x + x^2 + x^3$
(v) x^3 (vi) x^4
(vii) x^{18} (viii) x^{101}

4.8 Find the multiplicative inverse of each polynomial modulo $x^2 + 1$:

(i) $3 + 2x$ (ii) $3 + 2x + x^2$
(iii) $3 + 2x + x^2 + x^3$ (iv) $3 + 2x + x^2 + x^3 + x^4$
(v) x^3 (vi) x^4
(vii) x^{54} (viii) $a + bx$

4.9 Let $\rho(x) = x^2 + x + 1$. Reduce each polynomial mod ρ:

(i) $3 + 2x$ (ii) $3 + 2x + x^2$
(iii) $3 + 2x + x^2 + x^3$ (iv) $3 + 2x + x^2 + x^3 + x^4$
(v) x^3 (vi) x^4
(vii) x^{18} (viii) x^{101}

4.10 Find the multiplicative inverse of each polynomial modulo $x^2 + x + 1$.

(i) $3 + 2x$ (ii) $3 + 2x + x^2$
(iii) $3 + 2x + x^2 + x^3$ (iv) $3 + 2x + x^2 + x^3 + x^4$
(v) x^3 (vi) x^4
(vii) x^{101} (viii) $a + bx$

4.11 In $\mathbb{Q}[\zeta_5]$, express

$$\frac{1}{3 + 7\zeta_5 + 2\zeta_5^2}$$

as a linear combination of powers of ζ_5 with coefficients in $\mathbb{Q}$.

4.6 Galois Theory and the Fundamental Theorem of Algebra

It is possible, as Emil Artin has shown, to develop Galois theory without the symmetric function theorem.

The fundamental theorem of algebra follows quickly from the fundamental theorem of Galois theory and a few elementary facts about groups. While this may seem a little heavy-handed, it is nevertheless instructive to obtain special facts such as $\mathbb{C}$ being algebraically closed from more general ones. The following proof that $\mathbb{C}$ is algebraically closed is taken from Artin's paper of 1926 with Otto Schreier [2]. The fundamental theorem of Galois theory as stated in modern language leaves little trace of its origins in the theory of equations. It goes as follows:

Let F be a field that contains $\mathbb{Q}$ and let $E \supset F$ be a field containing F such that E is a finite-dimensional vector space over F. If $\alpha \in E$, let $f(x)$ be the minimal polynomial for α. Recall that this is the unique monic irreducible polynomial that has α as a root. If for each $\alpha \in E$, $f(x)$ has *all* its roots in E, i.e., $f(x)$ splits into linear factors, we say that E is a Galois extension of F. The Galois group of E over F is the *group of all automorphisms of E that leave each element of F fixed*. Denote this group by $G(E/F) = G$. It can be shown that G is a finite group of order equal to $\dim_F E$. The fundamental theorem of Galois theory states that there is a one-to-one correspondence between *subgroups* of G and *subfields* of E containing F. The correspondence is quite explicit. If $E \supset E_1 \supset F$, where E_1 is a field, then the corresponding subgroup of G is $G(E/E_1)$, the automorphisms of E that leave E_1 fixed. The inverse correspondence associates to each subgroup $H \subset G$ the field E_H of all α in E with $h(\alpha) = \alpha$ for all $h \in H$. The field E_H is called the *fixed field* of H. One can see that $G(E/E_H) = H$. Finally, H is a *normal* subgroup of G if and only if E_H is a Galois extension of F. (A subgroup $H \subset G$ is a *normal subgroup* if $ghg^{-1} \in H$ for each $h \in H$ and $g \in G$; see Example 4 in Section 2.6.)

In order to obtain the fact that $\mathbb{C}$ is algebraically closed, consider a polynomial $f(x) \in \mathbb{R}[x]$. Then let $E \supset \mathbb{C}$ be a Galois extension of $\mathbb{R}$ in which $f(x)$ has all its roots. That such a field exists follows from Kronecker's theorem (Theorem 4.13). We want to show that $E = \mathbb{C}$. If G is the Galois group of $E/\mathbb{R}$, suppose that G has order $n = 2^t m$ with m odd. By Sylow's theorem (Theorem 2.33 in Section 2.6), there exists a subgroup H of G of order 2^t. If E_H is the fixed field, we have the diagram in Figure 4.1.

Since the fundamental theorem of Galois theory implies that the dimension of E over E_H is 2^t, we see that E_H is an extension of $\mathbb{R}$ of odd degree. By Section 4.1 of this chapter, $E_H = \mathbb{R}$. Thus $E/\mathbb{R}$ has degree 2^t, and $m = 1$. Hence the Galois group of $E/\mathbb{C}$ is of order 2^{t-1}. If $E \neq \mathbb{C}$, then there would be a subgroup J in $G(E/\mathbb{C})$ of order 2^{t-2}, again by Sylow. Then the fixed

Where is the "analytic step" in this proof?

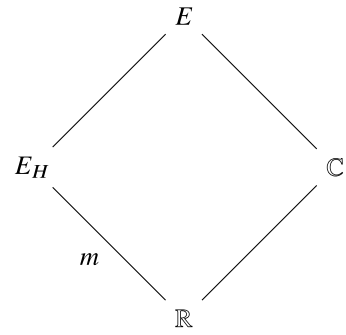


Figure 4.1. The "hypothetical" extension $E/\mathbb{C}$.

field E_J is a quadratic extension, i.e., an extension of degree 2, of $\mathbb{C}$ (again by Galois theory). That is impossible, since all quadratic equations over $\mathbb{C}$ have their roots in $\mathbb{C}$. This finishes the proof (applause).

The use of Galois and Sylow enabled us to collapse the "hypothetical" extension E to $\mathbb{C}$. Again, the analytic part of the proof is contained in the statement that $\mathbb{R}$ has no field extensions of odd degree greater than one.

You should by this time be drooling to read a good account of Galois theory. There are quite a few excellent books. Especially recommended:

(i) Lisl Gaal's *Classical Galois Theory* [28].

(ii) Pierre Samuel's beautiful introduction to algebraic number theory, *Theorie Algébrique des Nombres*, translated into English by Allan Silberger [76].

(iii) Joseph Rotman's *Galois Theory* [69].

(iv) Jörg Bewersdorff's *Galois Theory for Beginners: A Historical Perspective*, translated into English by David Kramer [6].

(v) And the best simple introduction to Galois theory is still Artin's *Galois Theory* [1].

4.7 The Topological Point of View

In this section, we examine the fact that $\mathbb{C}$ is algebraically closed from the point of view of topology. Thus we view $\mathbb{C}$ as the metric space $\mathbb{R} \times \mathbb{R}$ with its Euclidean topology. We know, for example, that $\mathbb{R}\times\mathbb{R}$ is connected, complete, and locally connected. A polynomial $f(x)$ can be viewed as a mapping from $\mathbb{C}$ to $\mathbb{C}$. The fundamental theorem of algebra then states that for every nonconstant polynomial $f(x)$, zero is in the image $f(\mathbb{C})$. But this is equivalent to the assertion that f is an *onto* mapping, i.e., $f(\mathbb{C}) = \mathbb{C}$. For suppose we know that $\mathbb{C}$ is algebraically closed. Let $a \in \mathbb{C}$ and consider $f(x) - a = g(x)$. Then $g(\alpha) = 0$ for some $\alpha \in \mathbb{C}$, and so $f(\alpha) = a$. Conversely, if $f(\mathbb{C}) = \mathbb{C}$, then $f(\alpha) = 0$ for some α. Hence the fact that $f(x)$ is onto implies that $\mathbb{C}$ is algebraically closed.

We will use some vocabulary and basic results from topology. A good introduction is the book by Steenrod and Chinn [4].

An important class of functions studied in complex function theory is the class of functions *holomorphic* on an open set $U \subset \mathbb{C}$. These functions are characterized by the property of having, near each $\alpha \in U$, a representation as a convergent power series, or equivalently, of having a complex derivative at each point. A basic result in the subject states that a holomorphic function is an *open* map. This means that if $V \subset U$, V open, then $f(V)$ is open in $\mathbb{C}$. Since a polynomial is a convergent power series defined everywhere on $\mathbb{C}$, it follows that $f(\mathbb{C})$ is open.

A polynomial is a "short" power series.

And $f(\mathbb{C})$ is also a closed set. For let $f(\xi_i) \to \alpha$ for some $\alpha \in f(\mathbb{C})$. Then $\{\xi_i\}$ is a bounded sequence, since we saw that $|f(x)|$ is arbitrarily large outside arbitrarily large disks (see Section 4.2). If ξ_{τ_i} is a convergent subsequence, then $f(\xi_{\tau_i}) \to \alpha$ and $f(\xi_{\tau_i}) \to f(\mu)$, where $\xi_{\tau_i} \to \mu$. Hence $\alpha = f(\mu)$, and since $f(\mathbb{C})$ contains all its limit points, it is closed in $\mathbb{C}$.

We know that $\mathbb{C}$ is a connected space, which means that $\mathbb{C}$ cannot be written as $A \cup B$ where A and B are nonempty, disjoint, and open. Or equivalently, $\mathbb{C}$ has no nonempty proper subset that is at the same time open and closed. This may be derived by combining the facts that $\mathbb{R}$ is connected and the topological product of two connected spaces is connected. Since $f(\mathbb{C})$ is not empty, we must have $f(\mathbb{C}) = \mathbb{C}$, and that proves our theorem.

A slight variation on this argument goes as follows. We learned in Section 4.2 that $|f(x)|$ has an absolute minimum, say $|f(\alpha)|$. Suppose $|f(\alpha)| \neq 0$. Then since f is open, there is a little disk centered at $f(\alpha)$, not containing 0, that must be covered by f, i.e., every point in the little disk must be an image point of f. But there are points closer to 0 than $f(\alpha)$ is. This contradicts the minimality of $|f(\alpha)|$. Hence $f(\alpha) = 0$.

Take It Further

A very intuitive proof is possible if we consider the image under f of a closed curve Γ in $\mathbb{C}$, as pictured in Figure 4.2.

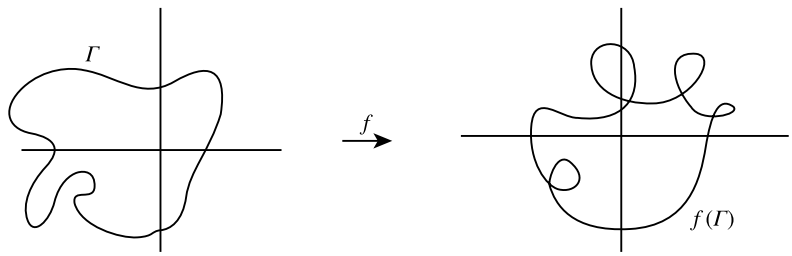


Figure 4.2. The image of Γ under the function f.

Consider a circle Γ_r of radius r in $\mathbb{C}$ and the simple polynomial z^n for $n \geq 1$. What is the image $f(\Gamma_r)$? It is just a circle of radius r^n. But since multiplication of complex numbers adds the angles, we see that the image circle is traversed n times as z goes around the circle of radius r once. We say

that n is the *winding number* of z^n.

Now, z^n is a particularly simple example, but it plays the leading role in this proof. Consider a polynomial $f(z)$ of degree n and view it as a mapping of circles of various radii in one plane to curves in another plane as illustrated in Figure 4.3.

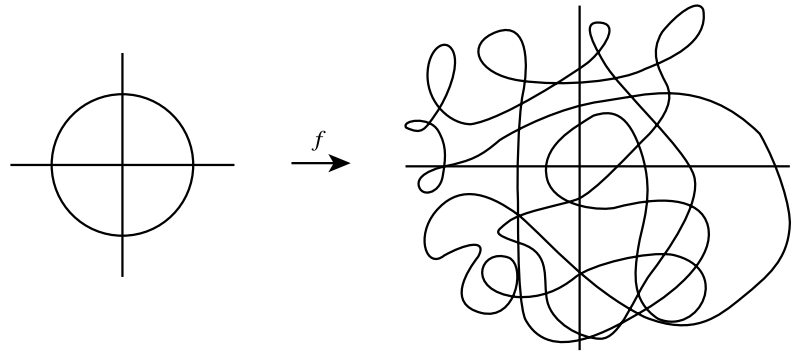


Figure 4.3. The image of a circle under the function f.

If $f(\Gamma_r)$ does not contain the origin, we may speak of the number of times the image goes around 0 as z traverses the circle Γ_r once in a counterclockwise manner. We count algebraically, so if the image point goes around clockwise, we subtract 1. Call this number $W_r(f)$. It is defined for every continuous function f. Although the picture is tempting, it isn't immediate how to define such a number rigorously. The idea is to vary the angle of $f(z)$ continuously and show that the total variation is an integral multiple of 2π. If you don't want to do that, then complex integration gives a good definition as

$$\frac{1}{2\pi i}\int_{\Gamma_r}\frac{f'}{f}.$$

However, let us proceed intuitively. If you think about it, you will see that the "winding" number varies *continuously* with r. What we shall do is to assume that $f(z)$ has no zero, so that $W_r(f)$ exists for all $r > 0$. Then we examine $W_r(f)$ for large r and see that it is n, and examine it for r small and see that it is zero. But $W_r(f)$ varies continuously with r, and since $\mathbb{R}$ is connected, it cannot jump from 0 to n. That is a contradiction, and so $f(z)$ must have a zero after all.

Now let us put in a few details. First consider $f(z)$ for large r. Since f has no zero, we must have $a_n \neq 0$. Write $f(z)$ as

$$f(z) = z^n + a_1 z^{n-1} + \cdots + a_n = z^n\left(1 + \frac{a_1}{z} + \cdots + \frac{a_n}{z^n}\right).$$

Since angles add, we see that

$$\begin{aligned} W_r(f) &= W_r(z^n) + W_r\left(1 + \frac{a_1}{z} + \cdots + \frac{a_n}{z^n}\right) \\ &= n + W_r\left(1 + \frac{a_1}{z} + \cdots + \frac{a_n}{z^n}\right). \end{aligned}$$

But when $|z|$ is very large, we have that

$$\left|\frac{a_1}{z} + \cdots + \frac{a_n}{z^n}\right|$$

is very small, and

$$1 + \frac{a_1}{z} + \cdots + \frac{a_n}{z^n}$$

just can't get around the origin. More precisely, if

$$\left|1 + \frac{a_1}{z} + \cdots + \frac{a_n}{z^n} - 1\right| < \frac{1}{2},$$

then

$$1 + \frac{a_1}{z} + \cdots + \frac{a_n}{z^n}$$

is confined to a disk of radius $1/2$ around 1. It follows that

$$W_r\left(1 + \frac{a_1}{z} + \cdots + \frac{a_n}{z^n}\right)$$

is zero for r large, and hence $W_r(f) = n$ for r large.

Now we look at $W_r(f)$ for r small. As z goes around a little circle of radius r, $1/z$ goes around a big circle of radius $1/r$ in the opposite direction. So let us just calculate the winding number of the composition of f with $1/z$. That is,

$$f\left(\frac{1}{z}\right) = \frac{1}{z^n} + \frac{a_1}{z^{n-1}} + \cdots + a_n = z^n\left(1 + \frac{a_1}{z} + \cdots + \frac{a_n}{z^n}\right).$$

As z goes around a little disk, $1/z$ goes around a big disk, and so

$$1 + \frac{a_1}{z} + \cdots + \frac{a_n}{z^n}$$

has winding number $-n$. However, z^n still has winding number n, so the total winding number is 0. Another way, perhaps simpler, of seeing this is to observe that

$$|z^n + a_1 z^{n-1} + \cdots + a_{n-1} z| < \frac{|a_n|}{2}$$

for $|z|$ small. Hence $|z^n + a_1 z^{n-1} + \cdots + a_{n-1} z + a_n|$ stays in a disk of radius $|a_n|/2$ about $a_n \neq 0$ for $|z| < \epsilon$. Hence the winding number is zero. And that does it!

The integer $W(f)$ is called the Brouwer degree of the mapping, and its general properties are developed in many texts on algebraic topology.

This concludes our excursion into the fundamental theorem of algebra. *But there's one more point that needs to be stressed:* As we have seen, the fundamental theorem is a basic fact about $\mathbb{C}$, and all proofs must involve in some way the fact that $\mathbb{R}$ is a complete Archimedean field. This so-called analytic step showed up in each of our proofs, and it can be shown that it needs to be there. Otherwise, we could have modified our proofs to show that $\mathbb{Q}[i]$ is algebraically closed, and that is just not true. The simplest invocation of analysis is in the algebraic proof, where it is used to ensure that polynomials of odd degree in $\mathbb{R}[x]$ have a root in $\mathbb{R}$.

Exercises

4.12 Show that if you assume the fundamental theorem of algebra, polynomials of odd degree have a real root. What is wrong with your proof?

4.8 Supplement: $x^n - 1$ and Its Factors

The polynomials $x^n - 1$ (n a positive integer) just might be the most important (read useful) class of polynomials in all of modern algebra. We have used these polynomials so far to investigate the geometry of regular polygons and the structure of Pythagorean triples. The roots of $x^n - 1$ (the "nth roots of unity") were an important part of the story when we looked at primes in an arithmetic progression, primitive elements, and Fermat's last theorem. They come up in field theory, group theory, analysis, and topology. Much of the success of $x^n - 1$ comes from the fact that its factors and roots have algebraic, geometric, and arithmetic interpretations. The irreducible factors of $x^n - 1$, the *cyclotomic polynomials*, have fascinated mathematicians ever since Gauss's *Disquitiones Arithmeticae* [29], and there is a vast literature that digs into their properties (see, for example, [12], or do a Google search).

And after working through some of the references, you might consult [86].

We will just scratch the surface here. More precisely, there are three purposes for this supplement.

(i) We will fulfill the promise made in Section 2.2: the polynomial Ψ_n defined by

$$\Psi_n(x) = \prod_{(j,n)=1} \left(x - \zeta_n^j\right) \tag{4.1}$$

Expression (4.1) describes a polynomial with complex coefficients. We want more: we will show that Ψ_n has *integer* coefficients.

has integer coefficients and is irreducible in $\mathbb{Z}[x]$. In fact, we shall prove the following theorem.

Theorem 4.14. *The polynomial $\Psi_n(x)$ is the minimal polynomial in $\mathbb{Z}[x]$ for*

$$\zeta_n = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}.$$

(ii) We shall also show that we have the factorization

$$x^n - 1 = \prod_{d|n} \Psi_d(x)$$

in $\mathbb{Z}[x]$, where the product is over the positive integer divisors of n.

(iii) And we shall investigate the structure of the various Ψ_n: their degrees and coefficients. This will make for some nice connections and (maybe) a surprise or two.

Let us break up our story into smaller pieces.

First: The Factorization of $\Psi_n(x)$ in $\mathbb{Z}[x]$

Every root of $x^n - 1$ has an order d that divides n. Conversely, if $d \mid n$, then a primitive dth root of unity satisfies $x^n - 1$. Since the $x - \zeta^j$ are relatively prime in $\mathbb{C}[x]$, we get the second claim in Theorem 4.14:

Lemma 4.15.

$$x^n - 1 = \prod_{d|n} \Psi_d(x). \tag{4.2}$$

Second: $\Psi_n(x) \in \mathbb{Z}[x]$

Equipped with the basics of group theory, we can restate some of the results from Chapter 2. The solutions to $x^n = 1$ in $\mathbb{C}$ form a cyclic group of order n with generator $\zeta = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$. The other generators are then ζ^j for $1 \le j < n$ with j relatively prime to n. These are the *primitive nth roots of unity*—the primitive elements in the group. Our polynomial Ψ_n is thus the monic polynomial whose roots are the primitive nth roots of 1.

The degree of $\Psi_n(x)$ is $\phi(n)$. If $n = p$, a prime, then $\Psi_n(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ (Theorem 2.11 in Section 2.2), so the coefficients are certainly integral. But in general, we don't have such an explicit expression (yet).

In Section 2.2, we denoted the number of integers j such that $(j, n) = 1$ by $\phi(n)$.

We will need Gauss's lemma.

Lemma 4.16 (Gauss). *Let*

$$f(x) = a_n x^n + \cdots + a_0, \quad a_i \in \mathbb{Z},$$
$$g(x) = b_m x^m + \cdots + b_0, \quad b_i \in \mathbb{Z},$$

be polynomials such that $a_n, \ldots, a_0$ have no common prime divisor, and similarly for $b_m, \ldots, b_0$. Then $f(x)g(x) = c_{n+m}x^{n+m} + \cdots + c_0$, where $c_{n+m}, \ldots, c_0$ have no common prime divisor.

Try working this out with two specific polynomials. It will feel very much like the argument we used for Eisenstein.

Proof. Suppose, to the contrary, that $f(x)g(x) = ph(x)$ for a prime p. Then reducing modulo p gives $\overline{f}(x)\overline{g}(x) = 0$ in $\mathbb{Z}_p$. Since $\mathbb{Z}_p[x]$ has no zero divisors (the whole point of the proof!), it follows that $\overline{f}(x) = 0$ or $\overline{g}(x) = 0$. If, say, $\overline{f}(x) = 0$, then p divides each of the coefficients of f, a contradiction. ■

As usual, $\overline{f}$ is the polynomial obtained by reducing the coefficients of f modulo p. It lives in $\mathbb{Z}_p[x]$.

A corollary of Gauss's lemma is sometimes more convenient to use.

Corollary 4.17. *A polynomial $f \in \mathbb{Z}[x]$ is irreducible in $\mathbb{Z}[x]$ if and only if f is irreducible in $\mathbb{Q}[x]$.*

Back at the ranch, we have a lemma to prove.

Lemma 4.18. $\Psi_n(x) \in \mathbb{Z}[x]$.

Proof. We use induction on n. When $n = 1$, we have $\Psi_1 = x - 1$, which is surely in $\mathbb{Z}[x]$. When $n > 1$, we write

$$x^n - 1 = \Psi_n(x) \prod_{\substack{d|n \\ d<n}} \Psi_d(x) =: \Psi_n(x) f(x) .$$

By the inductive hypothesis, $f(x)$ is in $\mathbb{Z}[x]$. But $x^n - 1$ is in $\mathbb{Z}[x]$ as well, and therefore, $\Psi_n(x)$, which by definition is a polynomial with complex coefficients, must in fact have real, indeed rational, coefficients. Clearing denominators, we can write $\Psi_n(x) = \frac{1}{b}\hat{\Psi}_n(x)$, where $b \in \mathbb{Z}$, $b \geq 1$, $\hat{\Psi}_n(x) \in \mathbb{Z}[x]$, and the coefficients of $\hat{\Psi}_n(x)$ have no common prime divisor. Since $f(x)$ is monic by construction, its coefficients also have no common prime divisor. Thus $f(x)$ and $\hat{\Psi}_n(x)$ satisfy the conditions of Lemma 4.16, so we may conclude that the coefficients of their product have no common prime divisor. But that means that the coefficients of $b(x^n - 1)$ have no common prime divisor. Hence $b = 1$, and we have $\Psi_n(x) \in \mathbb{Z}[x]$, as advertised. ∎

Third: $\Psi_n(x)$ Is Irreducible

Our proof will be the briefest of sketches, but you can fill in the details.

We can now finish the proof of the main result for this section, which is repeated here:

Theorem 4.14. The polynomial $\Psi_n(x)$ is the minimal polynomial in $\mathbb{Z}[x]$ for

$$\zeta_n = \cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n} .$$

Proof. We have established that $\Psi_n(x)$ has integer coefficients, and we know that ζ_n is a root. So "all" that is left is to establish the irreducibility of Ψ_n. We will do that now.

Thanks to Eisenstein, if p is prime, we already know that Ψ_p is irreducible.

Let $f(x)$ be the minimal polynomial for ζ_n; we claim that $\Psi_n = f$. Since f is irreducible, this will do the trick. To show this, it is enough to show that if p is a prime not dividing n, then $f(\zeta_n^p) = 0$. That last sentence requires an argument. ∎

Lemma 4.19. *Using the above notation, if p is a prime not dividing n implies that* $f(\zeta_n^p) = 0$*, then* $\Psi_n(x)$ *is the minimal polynomial in* $\mathbb{Z}[x]$ *for*

$$\zeta_n = \cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n} .$$

Proof. The roots of Ψ_n are the ζ_n^k, where $(k, n) = 1$. But such a k has a prime factorization involving only primes that don't divide n. So every root of Ψ_n is of the form $\left(\zeta_n^p\right)^{k'}$, where p does not divide n, and $(k', n) = 1$. But the hypothesis says that ζ_n^p is a root of both Ψ_n and f. Repeat the argument with $\zeta_n = \zeta_n^p$ and $k = k' \ldots$. This shows that f and Ψ_n have the same roots. Since both are monic, they are the same. ∎

Let us now prove our claim that $f(\zeta_n^p) = 0$. If $f \neq \Psi_n$, then $f \mid \Psi_n$, because the minimal polynomial for ζ_n is a factor of every polynomial in $\mathbb{Z}[x]$ that has ζ_n as a root. Assuming the worst, let us suppose that $fg = \Psi_n$. Then we know that

$$x^n - 1 = f(x)g(x)h(x), \tag{4.3}$$

where

$$h(x) = \prod_{\substack{d|n \\ 1 \le d < n}} \Psi_d(x).$$

If $f(\zeta_n^p) \neq 0$, then $g(\zeta_n^p) = 0$ (because all the other factors have roots that have orders less than n, and ζ_n^p has order n), so ζ_n is a root of $g(x^p)$. Hence there exists $j(x) \in \mathbb{Z}[x]$ such that $g(x^p) = f(x)j(x)$.

Now reduce mod p. By Fermat's little theorem, as a polynomial in $\mathbb{Z}_p[x]$, we have

$$g(x^p) = (g(x))^p,$$

so in $\mathbb{Z}_p[x]$, we have

$$(g(x))^p = f(x)j(x)$$

and $f \mid g^p$. Hence $f \mid g$. So from 4.3 above, we have

$$(f(x))^2 \mid x^n - 1.$$

Hence $x^n - 1$, as a polynomial in $\mathbb{Z}_p[x]$, has a multiple factor. So it and its derivative share a factor (mod p). But the derivative is nx^{n-1}, and since $(p, n) = 1$, its only factor in $\mathbb{Z}_p[x]$ is x, which is not a factor of $x^n - 1$.

The punchline is that $f(\zeta_n^p) = 0$. It follows that $f = \Psi_n$, and hence Ψ_n is irreducible. ■

Fourth: Calculating Ψ_n

We can rewrite equation (4.2) in a form that allows us to calculate the Ψ_n:

$$\Psi_n(x) = \frac{x^n - 1}{\prod_{\substack{d|n \\ d<n}} \Psi_d(x)}.$$

Using the fact that $\Psi_1(x) = x - 1$, we have a recursively defined formula for Ψ_n:

$$\Psi_n(x) = \begin{cases} x - 1 & \text{if } n = 1, \\ \dfrac{x^n - 1}{\prod_{\substack{d|n \\ d<n}} \Psi_d(x)} & \text{if } n > 1. \end{cases} \tag{4.4}$$

The recursive definition can be programmed into a computer algebra system. Doing this (or just doing it all by hand) gives, for example, the following table:

n	$\Psi_n(x)$
1	$x-1$
2	$x+1$
3	x^2+x+1
4	x^2+1
5	$x^4+x^3+x^2+1$
6	x^2-x+1
7	$x^6+x^5+x^4+x^3+x^2+1$
8	x^4+1
9	x^6+x^3+1
10	$x^4-x^3+x^2-x+1$
11	$x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+1$
12	x^4-x^2+1

You should verify that $x^{12}-1 = \prod_{d\in\{1,2,3,4,6,12\}} \Psi_d(x)$.

Some of these will look familiar to you—they are applications of Eisenstein. The table contains (especially if you extend it to more entries) a candy store of patterns. What do you see in it?

Look at one example: the minimal polynomial for ζ_{12}. Using the product $\prod_{(j,n)=1}\left(x-\zeta_n^j\right)$, we want

$$\left(x-\zeta_{12}\right)\left(x-\zeta_{12}^5\right)\left(x-\zeta_{12}^7\right)\left(x-\zeta_{12}^{11}\right).$$

The table says that this is equal to x^4-x^2+1. Why? Well,

$$x^{12}-1=\left(x-1\right)\left(x^2+x+1\right)\left(x+1\right)\left(x^2-x+1\right)\left(x^2+1\right)\left(x^4-x^2+1\right), \tag{4.5}$$

and we need something of degree four (why?). Hence the last factor is it. Can you show directly that x^4-x^2+1 is irreducible?

One more remark: each factor of (4.5) has, as its roots, powers of a primitive root $\zeta_{12}=\zeta$. It is a good exercise to check that they break up like this:

$$\begin{array}{cccccc}
(x-1) & (x+1) & \left(x^2+x+1\right) & \left(x^2+1\right) & \left(x^2-x+1\right) & \left(x^4-x^2+1\right) \\
\uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow \\
1 & -1 & -\frac{1}{2}\pm\frac{\sqrt{3}}{2}i & \pm i & \frac{1}{2}\pm\frac{\sqrt{3}}{2}i & \pm\frac{\sqrt{3}}{2}\pm\frac{1}{2}i \\
\uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow \\
\zeta^0 & \zeta^6 & \left\{\zeta^4,\zeta^8\right\} & \left\{\zeta^3,\zeta^9\right\} & \left\{\zeta^2,\zeta^{10}\right\} & \left\{\zeta,\zeta^5,\zeta^7,\zeta^{11}\right\}
\end{array}$$

Lookout Point 4.3. A delightful consequence of the fact that $\deg\Psi_n = \phi(n)$ uses Lemma 4.2 to obtain a result from elementary number theory that is often proved without mentioning cyclotomic polynomials, usually in much more complicated ways.

Corollary 4.20.

$$n=\sum_{d|n}\phi(d).$$

Convince yourself that this is true and verify it in some numerical cases. It's fun.

Fifth: The Coefficients of Ψ_n

Much has been written about the coefficients of Ψ_n. We include one example here: the sequence of cyclotomic polynomials gives rise to a wonderful "gotcha" example of misleading conclusions based on examining what seems to be a large data set.

Section 5 of Keith Conrad's expository paper [12] is a good place to see the lay of the land.

If you calculate (or look up, but calculate is better) Ψ_n for several dozen integers n using, say, formula (4.4), you might conclude that the coefficients are all 0, 1, or -1. Indeed, that is true for the first 104 values of n. But ψ_{105} contains -2 as the coefficient of x^7 and of x^{41}.

There are many other computable formulas for Ψ_n out there. Take your pick.

And it gets worse (or better, depending on your preference). Cleve Moler (Google him), founder of MathWorks [52] and the creator of MATLAB, wrote a MATLAB program to compute Ψ_n for some large values of n. He reported:

> For $n = 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 = 1062347$, the degree of $\Psi_n(x)$ is 760320. The coefficients range from -1749 to $+1694$. There are 11804 zero coefficients. The average coefficient magnitude is 409.9 ....
>
> $\Psi_n(x)$ is computed from the ratio of two polynomials, a numerator of degree 1105920 and a denominator of degree 345600. It takes about 6 minutes on my laptop to compute the numerator and denominator, and then about $2\frac{1}{2}$ hours to compute their ratio using only deconvolution.

This particular choice for n didn't come out of the blue. In [80], Jiro Suzuki proves the following result:

Theorem 4.21. *If k is odd and if $p_1 < p_2 < \cdots < p_k$ is a "front-loaded" sequence of primes—the sum of the first two in the sequence is greater than the last—and if n is the product of all the primes in the sequence, then $\psi_n(x)$ has $-k+1$ and $-k+2$ as coefficients.*

Since $105 = 3 \cdot 5 \cdot 7$, and $\{3, 5, 7\}$ is a front-loaded sequence of length 3, for $\psi_{105}(x)$ the theorem predicts the coefficient -2. And it is known that there exists a front-loaded sequence of length k for every odd $k \geq 3$.

Lookout Point 4.4. If you have access to a fairly powerful computational environment, take a look at the distribution of the coefficients of Ψ_n for some large values of n. Cleve Moler did it for Ψ_{760320} mentioned above. The distribution is given in Figure 4.4.

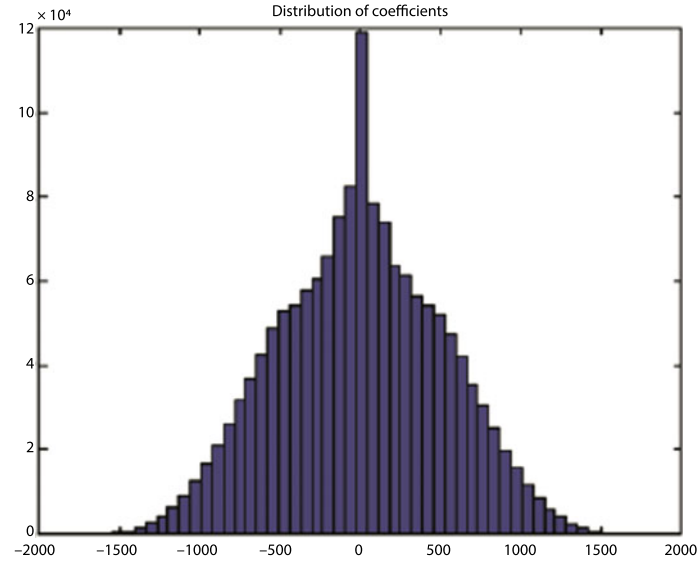


Figure 4.4. The distribution of coefficients of Ψ_n, based on a graphic by Cleve Moker, used with permission.

The moral of this story is that mathematical objects are *real*, and they exhibit all of the nuance found in physical phenomena.

Exercises

4.13 Develop a formula in terms of n for the number of irreducible factors in $\mathbb{Z}[x]$ of $x^n - 1$.

5 Irrational, Algebraic, and Transcendental Numbers

We have seen in the last chapter that the field of complex numbers admits no further algebraic extensions. Within the field of complex numbers, however, there are many numbers that are not algebraic over $\mathbb{Q}$. In fact, the algebraically closed field of all algebraic numbers in $\mathbb{C}$ is a countable set, for you can check that the algebraic numbers over $\mathbb{Q}$ that have a minimal polynomial of degree n are countable. Letting n vary gives a countable collection of countable sets, which is therefore countable. Let us agree to call a complex number that is not in $\mathbb{Q}$ an *irrational* number, so that an irrational number need not be real. For example, i is irrational. The irrational algebraic numbers are the algebraic numbers whose minimal polynomials have degree greater than one. Thus a real root of $x^5 + x + 1$ is a real irrational number. A real number is rational if and only if its decimal expansion is eventually periodic. Thus $101001000100001\ldots$, with an ever increasing number of 0's between the 1's, is irrational.

Many interesting numbers occur naturally in higher mathematics. They may arise as roots of polynomials, as in the case of algebraic numbers, or as values assumed by the various functions of classical analysis. Such numbers may be roughly called "classical" numbers (S. Lang, Ltd.).

Google Serge Lang. And see [49].

Several of the most important of these functions are

$$\cos x = 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \cdots,$$

$$\sin x = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \cdots,$$

$$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots,$$

$$J_0(x) = 1 - \frac{x^2}{2^2} + \frac{x^4}{x^4(2!)^2} - \frac{x^6}{2^6(3!)^2} + \cdots,$$

$$\zeta(x) = 1 + \frac{1}{2^x} + \frac{1}{3^x} + \cdots \quad (x > 1),$$

$$\ln(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \cdots,$$

$$\Gamma(x) = \int_0^\infty t^{x-1} e^{-t}\, dt\,.$$

A complex number is said to be *transcendental* if it is not algebraic over $\mathbb{Q}$.

K. Ireland and A. Cuoco, *Excursions in Number Theory, Algebra, and Analysis*,
Readings in Mathematics, https://doi.org/10.1007/978-3-031-13017-5_5

Thus α is transcendental if $f(\alpha) \neq 0$ for every nonzero polynomial $f(x)$ in $\mathbb{Q}[x]$. A general, and unsolved, problem in the theory of transcendental numbers is to construct an algorithm that will determine, for a given classical function $h(x)$, whether $h(\alpha)$ is transcendental on input an algebraic number α. Of course, one may compound classical functions and substitute algebraic numbers, pass to the algebraic closure of the field obtained by such procedures, and then begin all over again. For example, consider e^{α}, where α is a real root of $x^5 + J_0^2(1)x^4 - \zeta\left(e^{\sqrt{2}}\right)x + 1 = 0$. Needless to say, mathematics does not have a method to handle the question of transcendence of such numbers.

It isn't necessary to consider such complicated numbers to give examples of classical numbers whose irrationality or rationality is still open. For example, although it is known that $\zeta(2) = 1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots$ is equal to $\frac{\pi^2}{6}$, which is known to be transcendental, the number $\zeta(3) = 1 + \frac{1}{2^3} + \frac{1}{3^3} + \frac{1}{4^3} + \cdots$ has been studied without success. No one knows even whether it is irrational, much less transcendental.[1] The irrationality issue for $e + \pi$ has also not been settled. This whole area is full of unanswered questions.

We shall show that $\zeta(2) = \frac{\pi^2}{6}$ in Section 6.1.

Since "almost every" real number is transcendental, and since algebraic numbers arise in a very special way, most mathematicians would be shocked were it to turn out that numbers like $\zeta(3)$ and $e + \pi$ are not transcendental.

But take heart—we *will* get some important answers in this chapter.

(i) In Section 5.3, we will show that e is irrational.

(ii) In Section 5.4, we will show that e^n ($n \in \mathbb{Z}$) and π are irrational.

(iii) In Section 5.5, we will show that e is transcendental.

(iv) And the grand finale: in Section 5.6, we will show that π is transcendental.

To get going, we need some preliminary ideas, all useful in themselves. Here we go ...

5.1 Liouville's Observation

It isn't easy to give explicit examples of classical transcendental numbers. There is, however, a simple observation that was made by Joseph Liouville (1809–1882) that allows us to write down nonalgebraic numbers. Liouville's result has to do with the approximation of algebraic numbers by rational numbers. Here it is.

Theorem 5.1. *Let ξ be an algebraic number with minimal polynomial of degree $n \geq 2$. Then if $\frac{p}{q}$ is a rational number such that $\left|\frac{p}{q} - \xi\right| < 1$, then $\left|\frac{p}{q} - \xi\right| > \frac{c}{q^n}$, where c is a constant depending only on ξ.*

In other words you can't get too close to ξ with a rational number in the sense of the above inequality.

Proof. By clearing the denominators in the minimal polynomial, we have $f(\xi) = 0$, where $f(x)$ is an irreducible polynomial with *integer* coefficients:

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0.$$

[1] Such was the case in 1972 when I took Ken Ireland's summer course. But just six years later, completely out of the blue, the French mathematician Roger Apéry proved that $\zeta(3)$ is irrational.

Since f has degree $n > 1$, we see that $f\left(\frac{p}{q}\right) \neq 0$ for every rational number $\frac{p}{q}$ (why?). Hence on substituting, we have

$$\left| f\left(\frac{p}{q}\right) \right| = \left| \frac{a_n p^n + a_{n-1} p^{n-1} q + \cdots + a_0 q^n}{q^n} \right| \geq \frac{1}{q^n},$$

since the numerator is a *nonzero integer*.

Since ξ is a root of $f(x)$, we have

$$f(x) = (x - \xi) g(x),$$

where $g(x)$ is a polynomial with complex coefficients. Consider the closed interval $[\xi - 1, \xi + 1]$. Since a continuous function on a closed interval is bounded (Lemma 4.1), we may choose M such that $|g(x)| < M$ in that interval. Then for x in that interval, we have

$$|f(x)| = |x - \xi||g(x)| < |x - \xi| M.$$

Hence $|x - \xi| > \frac{|f(x)|}{M}$.

For rational $x = \frac{p}{q}$ in our interval, we have

$$\left| \frac{p}{q} - \xi \right| > \frac{\left| f\left(\frac{p}{q}\right) \right|}{M} \geq \frac{1}{M q^n}.$$

Putting $c = \frac{1}{M}$, we are through. ∎

As a corollary we produce a transcendental number. Consider the unclassical number

$$\alpha = \frac{1}{10^{1!}} + \frac{1}{10^{2!}} + \frac{1}{10^{3!}} + \cdots = 0.11000100000000000000000001\ldots.$$

Let us show that α is transcendental.

First of all, it isn't rational, because the decimal digits never repeat. And furthermore,

$$\alpha - \frac{1}{10} - \frac{1}{10^{2!}} - \cdots - \frac{1}{10^{m!}} = \frac{1}{10^{(m+1)!}} + \cdots,$$

so

$$\left| \alpha - \frac{p_m}{10^{m!}} \right| < \frac{2}{10^{(m+1)!}}, \tag{5.1}$$

where

$$\frac{p_m}{10^{m!}} = \frac{1}{10} + \frac{1}{10^{2!}} + \cdots + \frac{1}{10^{m!}}.$$

Now suppose α were an algebraic number of degree n for some $n \geq 2$. Then for sufficiently large m, the Liouville inequality would imply

$$\left| \alpha - \frac{p_m}{10^{m!}} \right| > \frac{c}{10^{nm!}}. \tag{5.2}$$

On combining inequality (5.2) with inequality (5.1), we get a sandwich,

$$\frac{2}{10^{(m+1)!}} > \left|\alpha - \frac{p_m}{10^{m!}}\right| > \frac{c}{10^{nm!}},$$

or

$$10^{(m+1)!-nm!} < \frac{c}{2},$$

which is false if m is big enough (recall that c and n are fixed!).

Hence we have shown that α is transcendental. There is an added bonus to this argument. Besides giving a simple *explicit* example of a transcendental number, we can even exhibit uncountably many transcendentals. Although we know that the transcendentals are uncountable by counting the algebraic numbers and knowing that the reals are uncountable, this argument is undeniably great.

The same argument also works for

$$\frac{\pm 1}{10^{1!}} + \frac{\pm 1}{10^{2!}} + \frac{\pm 1}{10^{3!}} + \cdots,$$

where the + and − signs are sprinkled arbitrarily. Each such number is created by taking a subset of the positive integers and putting minus signs at those terms and plus signs everywhere else. Thus the number of such reals is the cardinality of the set of all subsets of the positive integers, which is an uncountable set. This gives us an uncountable set of nonalgebraic numbers.

5.2 Gelfond–Schneider and Lindemann–Weierstrass

The transcendence of e was first proved by Charles Hermite in 1873, and it marks the beginning of the modern theory of transcendental numbers.

The problem of exhibiting a "classical" transcendental number requires methods more difficult than Liouville's observation. In Section 5.5, we prove that e is transcendental. In this section, in order to give a little more perspective as to what is known, we discuss two big theorems—without proof, of course.

There is no need to stop at e. A general result called the Lindemann–Weierstrass theorem (stated below) was proved in the early 1880s, and it implies that for every nonzero algebraic number α, the number e^α is transcendental. Its proof requires techniques more advanced than those used to prove the transcendence of e.

In order to state Lindemann–Weierstrass, we need a new piece of language. Notice first the relationship between transcendence and linear independence. The statement that α is transcendental is equivalent to the statement that for every n, the set of complex numbers $\{1, \alpha, \alpha^2, \ldots, \alpha^n\}$ is linearly independent over $\mathbb{Q}$. In this case, we say that the sequence $1, \alpha, \alpha^2, \alpha^3, \ldots$ is $\mathbb{Q}$-linearly independent. The transcendence of e^α then amounts to the requirement that

$$\{1, e^\alpha, e^{2\alpha}, e^{3\alpha}, \ldots\}$$

be $\mathbb{Q}$-linearly independent. The Lindemann–Weierstrass theorem replaces the exponents $0, \alpha, 2\alpha, 3\alpha, \ldots$ by an arbitrary sequence of distinct algebraic numbers and allows $\mathbb{Q}$ to be replaced by the field of all algebraic numbers. In other words, the theorem states the following.

Theorem 5.2 (Lindemann–Weierstrass). *Let F be the field of all algebraic numbers in $\mathbb{C}$. Let $\alpha_1, \alpha_2, \ldots$ be a sequence of distinct algebraic numbers. Then the sequence $e^{\alpha_1}, e^{\alpha_2}, e^{\alpha_3}, \ldots$ is F-linearly independent.*

We allow $\alpha_1 = 0$.

As a consequence, we see that π is transcendental. For we know by the above result that e^{α} is transcendental when α is nonzero and algebraic. So if π were algebraic, then $i\pi$ would be algebraic, and then $e^{i\pi} = -1$ would be transcendental, which is nonsense. But this is a tough way to show that π is transcendental. In Section 5.6, we will show that π isn't algebraic using a proof by Ivan Niven (1915–1999) inspired by an 1883 paper by Adolf Hurwitz (the same Hurwitz of the sums of squares theorems in Chapter 2).

A very clear proof of Theorem 5.2 can be found in Ivan Niven's delightful introduction *Irrational Numbers* [61]. This little book should be in your mathematical library.

Lookout Point 5.1. The seventh problem in Hilbert's 1900 Paris address is about this very circle of ideas. Here is the text from his address:

Irrationality and Transcendence of Certain Numbers.

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 Hurwitz has already done in two interesting papers, "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 $e^{i\pi z}$, 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:

Math. Annalen, vols. 22, 32 (1883, 1888).

Note that if α is algebraic, $\alpha \neq 0$, then, again using Lindemann–Weierstrass, we see that $e^{i\alpha}$ is transcendental. It follows that $\cos\alpha$ and $\sin\alpha$ are transcendental, as expected.

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.

See Exercise 5.1.

In spite of the simplicity of this statement and of its similarity to the problems solved by Hermite and Lindemann, we consider the proof of this theorem very difficult; as also the proof that

The expression a^{β}, for an algebraic base a and an irrational algebraic exponent β, e.g., the number $2^{\sqrt{2}}$ or $e^{\pi} = i^{-2i}$, 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.

Thirty-four years later, Alexander Osipovich Gelfond (1906–1968) solved the α^{β} conjecture, to be followed a year later by an independent proof by

Theodor Schneider (1911–1988).

In order to clarify the result, recall that if α and β are complex numbers, the number α^β, $\alpha \neq 0$, is defined by $e^{\beta \ln \alpha}$, where ln is the natural logarithm function. But the logarithm is not single-valued. For example, $e^{i\pi} = -1$ and $e^{3\pi i} = -1$, so $i\pi$ and $3\pi i$ are both values of $\ln(-1)$. Thus we speak of the *values* of α^β. Hence Gelfond–Schneider states the following.

Theorem 5.3 (Gelfond–Schneider). *If α and β are algebraic, $\alpha \neq 0$, and $\beta \notin \mathbb{Q}$, then every value of α^β is transcendental.*

Thus $3^{\sqrt{5}}$, $\sqrt{2}^{\sqrt{3}}$, 6^{ζ_5}, and 2^s, where s is a root of $x^5 + x + 1 = 0$, are all transcendental. But here is an added surprise. We can even catch e^π, which is a transcendental to a transcendental power. For consider the fun number i^i. By *definition*, this represents the various numbers $e^{i \ln i}$. One value of $\ln i$ is $\ln\left(-1^{1/2}\right) = \frac{1}{2}\ln(-1) = \frac{1}{2}\pi i$. Hence $e^{i \ln i} = e^{-\pi/2}$. Thus $e^{-\pi/2}$ is transcendental. From that you can quickly conclude that e^π is transcendental. This is hard to keep straight. The fact that $e^{i\pi} = -1$ with Lindemann gives the transcendence of π, while the fact that i^i has a value $e^{-\pi/2}$ proves the transcendence of e^π via Gelfond–Schneider. Got it?

The Gelfond–Schneider theorem is much deeper than the Lindemann–Weierstrass theorem. A very clear treatment by Einar Hille can be found in [38].

Another important naturally occurring real number is the Euler–Mascheroni constant γ, defined as the limit of the sequence $\{1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n}-\ln(n)\}$. It appears in the canonical decomposition of the gamma function $\Gamma(x)$ that exhibits its poles:

$$\Gamma(x)^{-1} = xe^{\gamma x}\prod_{n=1}^{\infty}\left(1+\frac{x}{n}\right)e^{-x/n}.$$

This constant "ought" to be transcendental, but in fact, it is unknown whether γ is even irrational.

Exercises

5.1 How is the assertion made in Lookout Point 5.1 connected to Hilbert's seventh problem?

The assertion: 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.

5.3 The Irrationality of e

Two classical constants that you probably encountered before you delved very deeply into mathematics are e, the base for the natural logarithm, and π. Let's discuss these constants more thoroughly. It turns out that e is the easier of the two to handle. This is due to the fact that e is nicely expressed as an infinite series with excellent denominators. More precisely,

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

we can use this to show that e is not a rational number. For suppose $e-1$ were rational and write $e - 1 = \frac{p}{q}$, where p and q are integers, $q \neq 0$. Then when n

is large (in fact $n \geq q$), the number $n!(e-1)$ is a positive integer. An estimate shows this to be impossible. Set $A = \sum_{j=1}^{n} \frac{1}{j!}$, the sum of the first n terms in the power series expansion of $e-1$. We note that $n!A$ is an integer, since every term in the sum when multiplied by $n!$ is an integer. Then we have

$$\begin{aligned} 0 &< n!(e-1) - n!A \\ &= n! \sum_{j=n+1}^{\infty} \frac{1}{j!} = n! \left(\frac{1}{(n+1)!} + \frac{1}{(n+2)!} + \cdots \right) \\ &= \frac{1}{(n+1)} + \frac{1}{(n+1)^2} + \frac{1}{(n+1)^3} + \cdots < \frac{1}{n} . \end{aligned}$$

Thus $n!(e-1) - n!A$ is a positive integer less than $\frac{1}{n}$, which is impossible. That was not too bad. For the record...

Be sure to verify each step in this calculation.

Theorem 5.4 (e is irrational).

$$e \notin \mathbb{Q} .$$

5.4 The Irrationality of π and e^c ($c \in \mathbb{Z}$)

In the case of π, an even more familiar constant to many, it is no longer a simple exercise to show that it is irrational. That it is irrational was first proved by Johann Heinrich Lambert (1728–1777) in 1761. Here is a very beautiful proof due to Ivan Niven (1946). The proof is related to an elegant treatment of the transcendence of e by Adolf Hurwitz in 1883. Hurwitz's paper, in turn, was a response to a paper by David Hilbert (1862–1943) in which the gamma function is used to establish the nonalgebraic character of e. In all these papers, the basic technique comes from an 1873 proof by Charles Hermite (1822–1901).

We'll work though Hurwitz's proof later.

Assume that π is rational and write $\pi = a/b$, where a and b are integers. Then construct (of course) the function f defined by

$$f(x) = \frac{x^n (a - bx)^n}{n!} . \tag{5.3}$$

Of course, the "(of course)" is facetious. Functions like this are created by studying many examples and looking for underlying structure. Also, we shall need to adjust n to suit our needs as that proof goes on.

We consider $f(x)$ on the interval $[0, \pi]$, and we observe that $f(x) = f(\pi - x)$. When n is large, the value of $f(x)$ is uniformly very small. Now form the alternating sum of the even derivatives of $f(x)$:

$$F(x) = f(x) - f^{(2)}(x) + f^{(4)}(x) - \cdots .$$

Since $f(x)$ has degree $2n$, this is a finite sum with n terms. Then on differentiating twice,

$$F''(x) = f^{(2)}(x) - f^{(4)}(x) + f^{(6)}(x) - \cdots ,$$

and adding, we see that

$$F(x) + F''(x) = f(x) .$$

Set $G(x) = F'(x)\sin x - F(x)\cos x$ and notice that its derivative is

$$F''(x)\sin x + F'(x)\cos x - F'(x)\cos x + F(x)\sin x,$$

which is $(F''(x) + F(x))\sin x$, which is $f(x)\sin x$.

By the mean value theorem, we have

$$G(\pi) - G(0) = \pi f(\xi)\sin\xi \tag{5.4}$$

for some $\xi \in (0,\pi)$. What we shall show is that the left-hand side of this equality is an integer, while the right-hand side is a positive real number that is less than 1.

Recall the definition of f:

$$f(x) = \frac{x^n(a-bx)^n}{n!}.$$

Returning to the definition of $f(x)$, we see that since the term of lowest degree is $a^n x^n/n!$, all the derivatives of order less than n vanish at $x = 0$, while all subsequent derivatives are integers at $x = 0$. But $f(x) = f(\pi - x)$, so $f^{(j)}(\pi)$ are also all integers. Using the fact that $\sin\pi = 0$, $\cos\pi = -1$, we conclude that the left-hand side of (5.4) is integral. As for the right-hand side, we notice that $1 > \sin x > 0$ on $(0,\pi)$, and for some constant M, we have $0 < f(x) < M^n/n!$, which approaches zero as n gets large. Hence for large n, $\pi f(\xi)\sin\xi$ is positive and less than 1. Since a positive integer cannot be less than 1, this proves the irrationality of π. Done. Let's celebrate this:

Theorem 5.5 (π **is irrational).**

$$\pi \notin \mathbb{Q}.$$

Exercise 5.2 asks you to fill in the details in the above argument. It's a good idea to do this now.

Notice that we have used only the facts that $\cos\pi = -1$, $\sin\pi = 0$, and $0 < \sin x < 1$ for $0 < x < \pi$. These facts follow quickly from the characterization of π as twice the first positive zero of $\cos x$. Furthermore, the only results from calculus used were the mean value theorem and the derivatives of $\sin x$ and $\cos x$. Hence the irrationality of π can be established quite early in the undergraduate program or even at the high-school calculus level. In view of the dominant role played by π in geometry and analysis, proving this result in beginning calculus seems like a good idea.

Lookout Point 5.2. The arguments for the irrationality and ultimately the transcendence of our classical constants will increase in complexity over the rest of this chapter, but the methods underneath them all will be quite similar to what we just did for the irrationality of π: assume that the numbers are rational (or, later, algebraic) and derive a contradiction by cooking up expressions (and this is the part that requires work, insight, and inspiration) that take on impossible values if our candidates are rational (or algebraic). For example, in the case of π above, the expression turned out to be integral and less than 1 at the hypothetical rational value, and that is a contradiction.

The "inspiration" that led to formula (5.3) was likely the result of a great deal of experiment and play.

Oh, and another device that will be useful in several places is a simple polynomial identity that should (and may be) part of every undergraduate

experience: Suppose that $f(x)$ is a polynomial with coefficients in a field and $F(x)$ is the (finite, really) sum of all the derivatives of f:

$$F(x) = \sum_{i=0}^{\infty} f^{(i)}(x)\,.$$

Then

$$F(x) - F'(x) = f(x)\,.$$

5.4.1 Next up: e^c

Using a very similar technique to the one used in establishing the irrationality of π, one can show in fact that e^c is irrational for every nonzero integer c. For the proof, we take our basic function to be

$$f(x) = \frac{x^n(1-x)^n}{n!}\,. \tag{5.5}$$

Form the alternating derived series with powers of c sprinkled about, this time using all derivatives. We have

$$F(x) = c^{2n} f(x) - c^{2n-1} f'(x) + \cdots + f^{(2n)}(x)\,.$$

Again we observe that since $f(x) = f(1-x)$, it follows that $f^{(j)}(0)$ and $f^{(j)}(1)$ are integers for all derivatives (check this).

Form $G(x) = e^{cx}F(x)$ and calculate its derivative

$$\begin{aligned} G'(x) &= e^{cx}F'(x) + ce^{cx}\,F(x) \\ &= e^{cx}(F'(x) + cF(x)) \\ &= e^{cx}\,c^{2n+1}f(x)\,. \end{aligned}$$

Now use the mean value theorem on $[0,1]$ applied to the function G to obtain

$$e^c F(1) - F(0) = e^{c\theta} c^{2n+1} f(\theta),$$

where $0 < \theta < 1$.

Up until now, we haven't assumed anything about our number e^c. We finish the proof by contradiction. If e^c were rational, we could write $e^c = A/B$ for integers A, B. Then

$$AF(1) - BF(0) = Be^{c\theta_n} c^{2n+1} f(\theta_n).$$

The left-hand side is a positive integer. As for the right-hand side, we see, by the definition of $f(x)$, that for $0 < x < 1$, we have

$$0 < f(x) < \frac{1}{n!}\,.$$

Hence

$$Be^{c\theta_n} c^{2n+1} f(\theta_n) < \frac{Be^c c^{2n+1}}{n!},$$

which goes to zero as $n \to \infty$. This proves the result.

Theorem 5.6 (Integer powers of e are irrational). *If $c \in \mathbb{Z}$, then*

$$e^c \notin \mathbb{Q}\,.$$

It follows that e^α is irrational for every rational nonzero α. And as a bonus, we can use Theorem 5.6 to show that the natural logarithm takes irrational values at integer arguments:

Corollary 5.7. *If $m \in \mathbb{Z}$, then*

$$\ln m \notin \mathbb{Q}\,.$$

The proof is up to you (Exercise 5.4). Of course, if we ask about the irrationality of $\log_{10} 2$, the answer is forthcoming if we suppose that $\log_{10} 2 = p/q$, which leads to an equality asserting that 2 to some integer power is equal to 5 to some integer power, which is impossible by the fundamental theorem of arithmetic. Fill in the details in Exercise 5.3.

Exercises

For example, "Using the fact that $\sin \pi = 0$, $\cos \pi = -1$, we conclude that the left-hand side of (5.4) is integral."

5.2 The proof of Theorem 5.5 makes quite a few claims. Write out a detailed proof of each one.

5.3 Prove that $\log_{10} 2$ is irrational.

5.4 Prove Corollary 5.7.

5.5 Show that for every real number r,

$$\lim_{n\to\infty} \frac{r^n}{n!} = 0\,.$$

5.5 The Transcendence of e

The fact that e^n is not rational is equivalent to the fact that e does not satisfy a polynomial equation of the form $x^n - r = 0$, where r is rational. Hence we have made some progress toward the transcendental character of e. It is a pleasant surprise that the same methods used to establish the irrationality of π and e^n generalize to prove that e is transcendental. Here are the details.

Suppose that e were algebraic. Write a polynomial relation for e with integer coefficients and nonvanishing constant term:

$$a_0 + a_1 e + a_2 e^2 + \cdots + a_n e^n = 0, \quad a_0 \neq 0.$$

In place of the little function $\frac{x^n(1-x)^n}{n!}$ used earlier, we consider a more complicated beast, the Hermite function

$$f(x) = \frac{x^{p-1}[(x-1)(x-2)\cdots(x-n)]^p}{(p-1)!}\,. \tag{5.6}$$

Keep in mind that throughout the proof, n is fixed, while we will choose p to be an appropriate large prime.

In fact, n is the alleged degree of the alleged polynomial satisfied by e, a polynomial that allegedly doesn't exist (we hope).

Again sum all the derivatives,

$$F(x) = \sum_{j=0}^{\infty} f^{(j)}(x) = f(x) + f^{(1)}(x) + f^{(2)}(x) + \cdots,$$

where the ∞ sign is phony, since $f(x)$ is a polynomial of degree $np + p - 1$, so that the sum is actually finite.

Again, we have $F'(x) - F(x) = -f(x)$, and therefore,

$$(e^{-x}F(x))' = e^{-x}F'(x) - e^{-x}F(x) = -e^{-x}f(x)\,.$$

Now consider the intervals $[0, 1], [0, 2], [0, 3], \ldots, [0, n]$ and apply the mean value theorem to the function $e^{-x}F(x)$ on each of these intervals. We have

$$\begin{aligned}
e^{-1}F(1) - F(0) &= -e^{-\theta_1}f(\theta_1), \quad 0 < \theta_1 < 1\,,\\
e^{-2}F(2) - F(0) &= -2e^{-\theta_2}f(\theta_2), \quad 0 < \theta_2 < 2\,,\\
&\vdots\\
e^{-n}F(n) - F(0) &= -ne^{-\theta_n}f(\theta_n), \quad 0 < \theta_n < n,
\end{aligned}$$

or equivalently,

$$\begin{aligned}
F(1) - eF(0) &= -e^{1-\theta_1}f(\theta_1) = \delta_1\,,\\
F(2) - e^2F(0) &= -2e^{2-\theta_2}f(\theta_2) = \delta_2\,,\\
&\vdots\\
F(n) - e^nF(0) &= -ne^{n-\theta_n}f(\theta_n) = \delta_n\,.
\end{aligned}$$

Now multiply the jth equation by a_j, the coefficient of e^j in the relation that we assumed e to satisfy. Noting that

$$-a_1e - a_2e^2 - a_3e^3 - \cdots - a_ne^n = a_0\,,$$

we add and obtain

$$a_1F(1) + a_2F(2) + \cdots + a_nF(n) + a_0F(0) = a_1\delta_1 + \cdots + a_n\delta_n\,. \tag{5.7}$$

Again, the strategy is similar to that used in Section 5.4. We will show the following:

(i) For large enough p, the left-hand side of equation (5.7) is an integer not divisible by p.

(ii) As $p \to \infty$, the right-hand side goes to 0.

Here we go ...

For the left-hand side, the Hermite function may be written in the form

This is a finite sum.

$$f(x) = \frac{\pm n!}{(p-1)!}x^{p-1} + \frac{c_0x^p}{(p-1)!} + \frac{c_1x^{p+1}}{(p-1)!} + \cdots, \tag{5.8}$$

where the c_i are integers. You can check (Exercise 5.6) that when $i \geq p$, the coefficients of $f^{(i)}$ are all integers divisible by p. Hence for $i \geq p$ and all integers k, we have $p \mid f^{(i)}(k)$.

For $i \geq p$ and all integers k, we have $p \mid f^{(i)}(k)$. Hold onto this.

Now look at the definition of f in Section 5.6 to see that f has a root of multiplicity p at $1, 2, \ldots, n$. Hence all the derivatives $f^{(i)}$ for $i = 0, \ldots, p-1$ vanish at $1, 2, \ldots, n$.

And ... the derivatives $f^{(i)}$ for $0 \leq i \leq p-1$ vanish at $1, 2, \ldots, n$. Hold onto this.

Remember F?

$$F(x) = \sum_{j=0}^{\infty} f^{(j)}(x) = f(x) + f^{(1)}(x) + \cdots + f^{(p-1)}(x) + f^{(p)}(x) + f^{(p+1)}(x) + \cdots . \tag{5.9}$$

Put the two side notes together to see that $F(k)$ is an integer multiple of p for $k = 1, \ldots, n$.

This looks like trouble, because we want to show that for large enough p, the left-hand side of equation (5.7) is an integer not divisible by p. But we have just shown that all the terms but the last in that left-hand side of (5.7) are divisible by p. Everything now hinges on the nature of the last term: $a_0 F(0)$.

It all hinges on our hope that $p \nmid a_0 F(0)$.

Look again at equation (5.8) to see that f has a root of multiplicity $p-1$ at $x = 0$. So

$$f(0) = f^{(1)}(0) = f^{(2)}(0) = \cdots = f^{(p-2)}(0) = 0 .$$

And as the side note reminds us, $f^{(i)}(0)$ is divisible by p for $i \geq p$. So on canceling everything that is divisible by p (including 0), we have

$$F(0) = \cancel{f(0) + f^{(1)}(0) + \ldots} + f^{(p-1)}(0) + \cancel{f^{(p)}(0) + f^{(p+1)}(0) + \ldots}, \tag{5.10}$$

So now everything depends on $i = p-1$. That is, what can we say about $f^{(p-1)}(0)$?

Looking at (5.8), we see that

$$f(x) = \frac{\pm n!}{(p-1)!} x^{p-1} + \text{higher-degree terms},$$

so we keep whittling it down to obtain

$$f^{(p-1)}(0) = \pm(n!) .$$

Choose p so large that $p \nmid (n!)$ and $p \nmid a_0$.

So far, we haven't restricted the prime p. But choose it now so that $p \nmid (n!)$ and $p \nmid a_0$. Bingo: We can now conclude with no further ado that

$$a_1 F(1) + a_2 F(2) + \cdots + a_n F(n) + a_0 F(0) \tag{5.11}$$

is an integer not divisible by p. This is half of what we want to show.

The other half is that the right-hand side of our favorite equation,

$$a_1 F(1) + a_2 F(2) + \cdots + a_n F(n) + a_0 F(0) = a_1 \delta_1 + \cdots + a_n \delta_n , \tag{5.12}$$

goes to 0 as $p \to \infty$. To see this, recall that

$$\delta_i = -e^{i-\theta_i} f(\theta_i) = \frac{-e^{i-\theta_i} \theta_i^{p-1} (\theta_i - 1)^p (\theta_i - 2)^p \cdots (\theta_i - n)^p}{(p-1)!} .$$

Now, recalling that $0 < \theta_i < i < n$, we have

$$e^{i-\theta_i} < e^n, \quad \theta_i^{p-1} < n^{p-1} < n^p, \quad (\theta_i - 1)^p(\theta_i - 2)^p \cdots (\theta_i - n)^p < (n!)^p .$$

Sooo...

$$|\delta_i| = \frac{e^{i-\theta_i}\theta_i^{p-1}(\theta_i - 1)^p(\theta_i - 2)^p \cdots (\theta_i - n)^p}{(p-1)!} < \frac{e^n n^p (n!)^p}{(p-1)!} .$$

Recalling now that n is fixed, we see that the right-hand side of the equality above goes to 0 as $p \to \infty$ (Exercise 5.5). So we can choose p so large that

$$|a_1\delta_1 + \cdots + a_n\delta_n| < 1 .$$

But the left-hand side of (5.12) is an integer. So the right-hand side must be 0. But p doesn't divide the left-hand side. It's all impossible.

And that does it. If e were algebraic, it would have to be a positive integer less than 1 not divisible by p, and that's crazy. So we have (applause) the following theorem.

Theorem 5.8 (e is not algebraic). *e is transcendental.*

Except for staring intently at a more complicated polynomial, the idea is the same as the proof of the irrationality of π. We were concerned with $e^{-x}f(x)$ instead of $f(x)\sin x$. A very instructive exercise is to carry out the proof explicitly for $n = 1$ and 2. This gives a proof that e is irrational, which is a very simple fact, and a proof that e is neither a rational number nor a quadratic irrationality, a less simple fact. Of course, living with the general proof is most satisfying of all.

Exercises

5.6 Show that if $h(x) \in \mathbb{Z}[x]$ and p is a prime, then for $i \geq p$,

$$\frac{d^i}{dx}\left(\frac{h(x)}{(p-1)!}\right)$$

is a polynomial in $\mathbb{Z}[x]$ whose coefficients are all congruent to 0 mod p.

5.7 If $\ell \in \mathbb{Q}$, show that e^ℓ is transcendental.

5.6 π Is Transcendental

We showed earlier that π is irrational. In this section we will establish, by a nontrivial extension of the basic idea underlying the irrationality proof, that π is not an algebraic number. The proof we give is due to Ivan Niven and was published in 1939 in the *American Mathematical Monthly*.

See Lookout Point 5.2 for the basic idea.

5.6.1 More About Symmetric Functions

In our proof we need a corollary to the symmetric function theorem (Theorem 4.10 in Section 4.4):

Lemma 5.9. *Consider the following polynomial in* $\mathbb{Z}[x]$*:*

$$f(x) = x^n + a_1 x^n + \cdots + a_n = (x - \theta_1)\cdots(x - \theta_n).$$

If $g(x_1, \ldots, x_n)$ *is a symmetric polynomial in variables* $x_1, \ldots, x_n$ *with coefficients in* $\mathbb{Z}$*, then* $g(\theta_1, \theta_2, \ldots, \theta_n)$ *is an integer.*

Proof. By the symmetric function theorem, $g(x_1, \ldots, x_n) = h(\sigma_1, \ldots, \sigma_n) \in \mathbb{Z}[\sigma_1, \ldots, \sigma_n]$, where $\sigma_1, \ldots, \sigma_n$ are the elementary symmetric functions in $x_1, \ldots, x_n$. Now substitute $(\theta_1, \ldots, \theta_n)$ for $(x_1, \ldots, x_n)$. The σ_i evaluated at $\theta_1, \ldots, \theta_n$ are precisely the integers $a_1, \ldots, a_n$ up to a $\pm$ sign. Hence the result. ■

In the application we have in mind, the values of θ that arise satisfy polynomials in $\mathbb{Z}[x]$ that are not monic. But by a change of variable, we can transform any polynomial in $\mathbb{Z}[x]$ into a monic one. If

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 = a_n(x - \theta_1)\cdots(x - \theta_n),$$

then

$$a_n^{n-1}\left(a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0\right) = a_n^n (x - \theta_1)\cdots(x - \theta_n),$$

so

$$\begin{aligned}
&(a_n x)^n + a_n a_{n-1}(a_n x)^{n-1} + a_n^2 a_{n-2}(a_n x)^{n-2} + \cdots + a_n^{n-1} a_0 \\
&\quad = (a_n x)^n + a'_{n-1}(a_n x)^{n-1} + a'_{n-2}(a_n x)^{n-2} + \cdots + a'_0 \\
&\quad = (a_n x - a_n\theta_1)(a_n x - a_n\theta_2)\cdots(a_n x - a_n\theta_n),
\end{aligned}$$

where $a'_{n-1}, \ldots, a'_0$ are integers. It follows that if $g(x_1, \ldots, x_n)$ is a symmetric polynomial with coefficients in $\mathbb{Z}$ and leading coefficient a_n, then $g(a_n\theta_1, \ldots, a_n\theta_n)$ is in $\mathbb{Z}$. In particular, if $g(x_1, \ldots, x_n)$ is *homogeneous* of degree s, which means that

$$g(tx_1, \ldots, tx_n) = t^s g(x_1, \ldots, x_n),$$

then $a_n^s g(\theta_1, \ldots, \theta_n)$ is in $\mathbb{Z}$. We will make use of this observation later in this section, so let us state it as a lemma.

Lemma 5.10. *Suppose*

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 = a_n(x - \theta_1)\cdots(x - \theta_n),$$

where the coefficients are in $\mathbb{Z}$*. If* $g(x_1, \ldots, x_n)$ *is a symmetric polynomial with coefficients in* $\mathbb{Z}$ *and leading coefficient* a_n*, then* $g(a_n\theta_1, \ldots, a_n\theta_n)$ *is in* $\mathbb{Z}$*. In particular, if* $g(x_1, \ldots, x_n)$ *is homogeneous of degree* s*, then we also have that* $a_n^s g(\theta_1, \ldots, \theta_n)$ *is in* $\mathbb{Z}$*.*

5.6.2 Euler's Identity

We now prove that π is transcendental. The basic strategy is similar to that used for e: assuming that π is algebraic, we construct a nonzero integer that is of absolute value less than 1.

See Lookout Point 5.2.

The function that plays the central role is somewhat more complicated than the one used for e. Here is how we define it. If π were algebraic, then $i\pi$ would also be algebraic. Recall that e^x is a complex-valued function of the complex variable x. We have

$$e^x = 1 + x + \frac{x^2}{2!} + \cdots,$$

and this holds for complex x. Substituting $x = it$, where t is real, we have

$$e^{it} = 1 + it + \frac{i^2t^2}{2!} + \frac{i^3t^3}{3!} + \cdots,$$

and on rearranging the (absolutely convergent!) series, we obtain

See formula 2.1 in Section 2.1.

$$e^{it} = 1 - \frac{t^2}{2!} + \frac{t^4}{4!} + \cdots + i\left(t - \frac{t^3}{3!} + \frac{t^5}{5!} + \cdots\right) = \cos t + i \sin t\,.$$

On substituting $t = \pi$, we obtain

$$e^{i\pi} = -1.$$

This is a very famous and celebrated formula. Google "Euler's Identity."

5.6.3 Setting the Stage

This is our beginning point. Suppose that $i\pi = \alpha_1$ satisfies an irreducible polynomial over $\mathbb{Q}$ with roots $\alpha_1, \alpha_2, \ldots, \alpha_n$. Then since $e^{\alpha_1} + 1 = 0$, we have

$$(e^{\alpha_1} + 1)(e^{\alpha_2} + 1) \cdots (e^{\alpha_n} + 1) = 0\,. \tag{5.13}$$

Multiplying out yields

$$1 + e^{\alpha_1} + e^{\alpha_2} + \ldots + e^{\alpha_n} + e^{\alpha_1+\alpha_2} + \cdots + e^{\alpha_{n-1}+\alpha_n} + e^{\alpha_1+\alpha_2+\alpha_3} + \cdots + e^{\alpha_1+\alpha_2+\cdots+\alpha_n}.$$

The exponents are the various sums of subsets of $\{\alpha_1, \ldots, \alpha_n\}$. There are $2^n - 1$ such numbers (why?). Call them $\rho_1, \ldots, \rho_s$, where $s = 2^n - 1$, and form the polynomial that has them as roots: $\prod_{i=1}^{s}(x - \rho_i) = g(x)$. Then $g(x) \in \mathbb{Q}[x]$. This follows from the symmetric function theorem and the observation that $g(x) = \prod_{j=1}^{n} h_j(x)$, where $h_j(x)$ is the polynomial whose roots are the various sums of j of the α's. Since the set of sums taken j at a time is invariant under the various permutations of $\alpha_1, \ldots, \alpha_n$, it follows that $h_j(x) \in \mathbb{Q}[x]$, and from this it follows that $g(x) \in \mathbb{Q}[x]$.

On clearing the denominators, we may now assume that $g(x)$ has integer coefficients. There is one more comment: It may happen that various sums of

the α's are 0, and that will contribute a factor of x to $g(x)$. Cancel them out so that we may write

$$\alpha(x) = cx^r + c_1x^{r-1} + \cdots + c_0, \tag{5.14}$$

where $c, c_1, \ldots, c_0$ are in $\mathbb{Z}$ and $c_0 \neq 0$. Furthermore, now the roots of $\alpha(x)$ are the *nonzero* roots of $g(x)$. Call these roots $\beta_1, \ldots, \beta_r$, so that

$$\alpha(x) = c(x-\beta_1)(x-\beta_2)\cdots(x-\beta_r). \tag{5.15}$$

Notice also that from equation (5.13), we have

$$e^{\beta_1} + e^{\beta_2} + \cdots + e^{\beta_r} + k = 0, \tag{5.16}$$

where k is an integer arising from the various zero exponents.

5.6.4 And Now . . . the Proof

With these preliminaries out of the way, we can construct the analogue of the Hermite beast. We define $f(x)$ by

$$f(x) = \frac{c^m x^{p-1}(\alpha(x))^p}{(p-1)!} = \frac{c^{m+p}x^{p-1}\left(\prod_{i=1}^r (x-\beta_i)\right)^p}{(p-1)!}, \tag{5.17}$$

where m is any fixed integer greater than rp, the degree of $\alpha(x)^p$. Now we proceed as earlier. Form

$$\begin{aligned} F(x) &= f(x) + f'(x) + f^{(2)}(x) + \cdots, \\ F'(x) &= f'(x) + f^{(2)}(x) + \cdots, \\ F(x) - F'(x) &= f(x). \end{aligned}$$

A worthwhile timeout: count the number of times you have seen a calculation like this.

Hence, we have (as usual)

$$\left(e^{-x}F(x)\right)' = e^{-x}F'(x) - e^{-x}F(x) = e^{-x}\left(F'(x) - F(x)\right) = -e^{-x}f(x).$$

The various β_i are complex numbers. Draw line segments to the various β_i in the complex plane as in Figure 5.1. These segments play the role of closed intervals in calculus, so that we can write $\int_0^{\beta_1} -e^{-x}f(x)dx$ and so on.

The function $e^{-x}f(x)$ is a complex-valued continuous function of the complex variable x. Thus we may integrate $e^{-x}f(x)$ along segments, and the fundamental theorem of calculus carries over without difficulty. The derivative of $e^{-x}F(x)$ is $-e^{-x}f(x)$ (in the complex sense), and so we obtain, for the various β_i,

"carries over without difficulty. . ." See **Lookout Point** 5.3.

$$\int_0^{\beta_i} -e^{-x}f(x)dx = e^{-\beta_i}F(\beta_i) - F(0).$$

And then

$$e^{\beta_i}\int_0^{\beta_i} -e^{-x}f(x)dx = F(\beta_i) - e^{\beta_i}F(0).$$

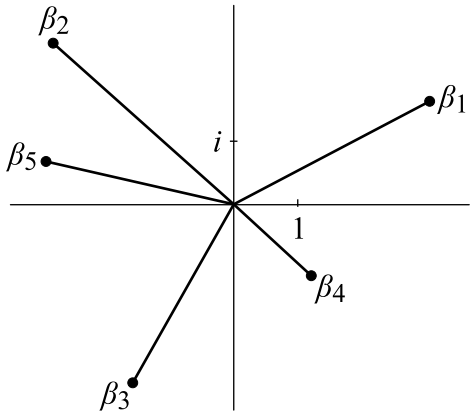


Figure 5.1. The segments to the various β_i.

Summing over $i = 1, \ldots, r$ and using equation (5.13), we obtain the basic relation

$$F(\beta_1) + \cdots + F(\beta_r) + kF(0) = \sum_{i=1}^{r} \left(- \int_0^{\beta_i} e^{\beta_i - x} f(x) dx \right). \tag{5.18}$$

The remainder of the proof consists in showing (as is our custom) that for a suitable prime p, the left-hand side is a nonzero integer, while the right-hand side is less than 1 in absolute value.

Let us handle the left-hand side first, and begin with $kF(0)$. Recall the definition of f from equation (5.17):

$$f(x) = \frac{c^m x^{p-1} (\alpha(x))^p}{(p-1)!} = \frac{c^m x^{p-1} \left(cx^r + c_1 x^{r-1} + \cdots + c_0 \right)^p}{(p-1)!}.$$

We see that at 0, all derivatives up to the $(p-2)$nd are 0. The $(p-1)$st derivative at 0 is $c^{m+p} c_0^p$, and all subsequent derivatives are integers divisible by p. Thus if we choose the prime p so large that $p \nmid cc_0$, then it won't divide $c^{m+p} c_0^p$, and thus $f(0) + f'(0) + f^{(2)}(0) + \cdots$ must be an integer not divisible by p. Hence for p sufficiently large, $kF(0)$ is not divisible by p.

Now we examine the integrality of $F(\beta_1) + \cdots + F(\beta_r)$. First, each β_i is a root of $\alpha(x)$ (see equation (5.13)), so each β_i is a root of $f(x)$ of multiplicity p. This implies that

$$f^{(j)}(\beta_i) = 0 \quad \text{for } j = 1, \ldots, p-1,$$

and this implies that for $j = 1, \ldots, p-1$, we have

$$F^{(j)}(\beta_1) + F^{(j)}(\beta_2) + \cdots + F^{(j)}(\beta_r) = 0. \tag{5.19}$$

Hence $f^{(t)}(\beta_1) + f^{(t)}(\beta_2) + \cdots + f^{(t)}(\beta_r) = 0$ for $t = 1, 2, \ldots, p-1$.

Now consider the above sum for $t = p, p+1, \ldots$:

$$f^{(t)}(\beta_1) + \cdots + f^{(t)}(\beta_r).$$

First of all, $f^{(t)}(x)$ in this range of t has integer coefficients divisible by p, and furthermore, each coefficient is divisible by c^m. The degree of $f(x)$ is $rp + p - 1$. Therefore, after $p - 1$ differentiations, it has degree $rp = s$. Since $m > rp$, we conclude that pc^s divides each coefficient of $f^{(t)}(x)$ for $t = p, p + 1, \ldots$.

Now substitute β_j into $f^{(t)}(x)$, giving $f^{(t)}(\beta_j)$. This quantity is a polynomial in β_j each of whose coefficients is divisible by pc^s.

Now, $f^{(t)}(\beta_1) + \cdots + f^{(t)}(\beta_r)$ is symmetric in $\beta_1, \ldots, \beta_r$, and furthermore, it is a sum of homogeneous symmetric polynomials each of degree at most s. Hence by Lemma 5.10, we see that $f^{(t)}(\beta_1) + \cdots + f^{(t)}(\beta_1)$ is an integer divisible by p. It follows that $F(\beta_1) + \cdots + F(\beta_r)$ is an integer divisible by p. Finally, we conclude that the left-hand side of equation (5.18) is an integer not divisible by the prime p. Hence it is not zero. Whew!

Recall that $f(x) = \frac{c^m x^{p-1}(\alpha(x))^p}{(p-1)!}$.

In order to estimate the right-hand side of equation (5.18), we use a standard estimate for $\int_L h(x)dx$, where L is a path in the complex plane and $h(x)$ is a continuous complex-valued function on L. If $|L|$ denotes the length of L, then the estimate is

$$\left| \int_L h(x)dx \right| \leq |L|\, M\,, \tag{5.20}$$

where M is the maximum (least upper bound) of $|h(x)|$ on L. That the right-hand side is less than 1 in absolute value for some p follows just as in all the other proofs. It boils down to Exercise 5.5:

$$\lim_{p\to\infty} \frac{R^{p-1}}{(p-1)!} = 0\,.$$

The proof is finished by observing that p had to be chosen big enough to satisfy a (small) and finite number of conditions. Hooray!

Lookout Point 5.3. Don't consider the introduction of the complex line integral in this proof as a serious violation of the request for simplicity and elementary technique. The integral is defined simply in terms of ordinary Riemann integrals. More precisely, if $(\phi(t), \psi(t))$ parametrizes an arc Γ as t goes from 0 to 1 and if $f(z) = u(x, y) + iv(x, y)$, then one defines

$$\begin{aligned}\int_\Gamma f(z)dz := &\int_0^1 u(\phi(t),\psi(t))\phi'(t) - v(\phi,\psi)\psi'(t)\,dt \\ &+ i\int_0^1 v(\phi,\psi)\phi' + u(\phi,\psi)\psi'(t)\,dt.\end{aligned}$$

This follows formally from

$$f(z)\,dz = (u + iv)(dx + i\,dy) = u\,dx - v\,dy + i(v\,dx + u\,dy)\,.$$

Suppose that $F(z) = U(x, y) + iV(x, y)$ satisfies the Cauchy–Riemann equations

$$\frac{\partial U}{\partial x} = \frac{\partial V}{\partial y}, \quad \frac{\partial U}{\partial y} = \frac{\partial V}{\partial x}\,. \tag{5.21}$$

Write $F'(z) = U_x + iV_x$. It is shown in every text on complex analysis that this definition is consistent with the definition in terms of differential quotients. For our functions $e^{-x}F(x)$, it is a simple exercise. Then $F'(z) = f(z)$ is a simple application of the definition and the ordinary fundamental theorem of calculus which states that

$$\int_\alpha^\beta f(z)\,dz = F(\beta) - F(\alpha)\,,$$

where Γ begins at α and ends at β. Finally, by referring everything to Riemann sums, it is possible to derive the basic estimate $\left|\int_L f(z)dz\right| \le |L| \max|f(z)|$.

For a proof of the transcendence of π that does not use calculus, see Hardy and Wright [35]. But the use of complex integration theory is essential to the modern theory of transcendental numbers.

One more thing: It is a good idea to have a simple infinite series for π, just as we had one for e. Such a series is given by the Leibnitz–Gregory series

$$\frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots.$$

A short proof of this identity has been noted by Donat Kazarinoff [44]. Consider

$$\alpha_n = \int_0^{\pi/4} \tan^n x\,dx, \quad n \ge 2\,.$$

Since $\tan x$ is between 0 and 1 on $[0, \pi/4]$, we see that α_n is a monotonically decreasing sequence. Suppose $\alpha_n \to \alpha$. Now

$$\begin{aligned}\alpha_n &= \int_0^{\pi/4} \tan^{n-2} x \tan^2 x\,dx = \int_0^{\pi/4} \tan^{n-2} x(\sec^2 x - 1)dx \\ &= \int_0^{\pi/4} \tan^{n-2} x \sec^2 x\,dx - \int_0^{\pi/4} \tan^{n-2} x\,dx \\ &= \frac{\tan^{n-1} x}{n-1}\bigg|_0^{\pi/4} - \alpha_{n-2} = \frac{1}{n-1} - \alpha_{n-2}\,.\end{aligned}$$

Thus $\alpha_n + \alpha_{n-2} = \frac{1}{n-1}$.

Letting $n \to \infty$, we see that $\alpha + \alpha = 0$, and therefore $\alpha = 0$. Now replace n by $2n$ and use the recurrence relation

$$\begin{aligned}\alpha_{2n} &= \frac{1}{2n-1} - \alpha_{2n-2} = \frac{1}{2n-1} - \frac{1}{2n-3} + \alpha_{2n-4} + \cdots \\ &= \frac{1}{2n-1} - \frac{1}{2n-3} + \frac{1}{2n-5} + \cdots \pm \frac{1}{3} \mp \alpha_2\,.\end{aligned}$$

We have

$$\alpha_2 = \int_0^{\pi/4} \tan^2 x\,dx = \int_0^{\pi/4} \left(\sec^2 x - 1\right) dx = 1 - \frac{\pi}{4}\,.$$

Transposing gives

$$\frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots \pm \frac{1}{2n-1} \mp \alpha_{2n}\,.$$

Since $\alpha_{2n} \to 0$, we have proved the desired formula.

If we begin instead with α_{2n+1}, we get another nice formula:

$$\alpha_{2n+1} = \frac{1}{2n} - \frac{1}{2n-2} + \cdots \pm \frac{1}{2} \mp \alpha_1 .$$

But

$$\alpha_1 = \int_0^{\pi/4} \tan x \, dx = \log \sec x \Big|_0^{\pi/4} = \ln \sqrt{2} = \frac{1}{2} \ln 2 .$$

In case you didn't notice, this is Dialing In 131.

Thus

$$\frac{1}{2} \ln 2 = \frac{1}{2} - \frac{1}{4} + \frac{1}{6} - \cdots \pm \frac{1}{2n} \mp \alpha_{2n+1} .$$

Since $\alpha_{2n+1} \to 0$, we have

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

Exercises

5.8 Show that if $g(z) \in \mathbb{C}[z]$, then $e^{-z} g(z)$ satisfies the Cauchy–Riemann equations (5.21).

5.9 Suppose that f and g are polynomials in $\mathbb{C}[x]$ and n is a nonnegative integer. Show that

$$(fg)^{(n)}(x) = \sum_{k=0}^{n} \binom{n}{k} f^{(k)}(x) g^{(n-k)}(x) .$$

5.10 **Take It Further.** The proofs in this chapter involved concocting certain functions that were at the core of the results:

(i) $f(x) = \frac{x^n (a-bx)^n}{n!}$ is used in the proof that π is irrational.

(ii) $f(x) = \frac{x^n (1-x)^n}{n!}$ is used in the proof that e^c is irrational.

(iii)

$$f(x) = \frac{x^{p-1}[(x-1)(x-2)\cdots(x-n)]^p}{(p-1)!}$$

is used in the proof that e is transcendental.

(iv) In the proof that π is transcendental, we used this:

$$f(x) = \frac{c^m x^{p-1} (\alpha(x))^p}{(p-1)!} = \frac{c^{m+p} x^{p-1} [\prod_{i=1}^{r} (x - \beta_i)]^p}{(p-1)!} .$$

What are some structural similarities among these beasts? How are their definitions related to the results in which they are used?

5.11 Show that a rectangle is determined by its perimeter and area.

5.12 Show that a rectangular box is is determined by its edge perimeter, surface area, and volume.

5.13 Find two different rectangular boxes with the same edge perimeter and volume. Can you find two such that have rational side lengths?

6 Fourier Series and Gauss Sums

The basic functions that we will be concerned with in this chapter are

$$x \mapsto \sin nx \quad \text{and} \quad x \mapsto \cos nx$$

for $n = 0, 1, 2, 3, \ldots$. The elements of the vector spaces over $\mathbb{R}$ spanned by these functions are called *finite trigonometric series*. Thus a finite trigonometric series of degree at most n is a function of the form

$$\begin{aligned} f(x) = c_0 &+ c_1 \sin x + d_1 \cos x + c_2 \sin 2x + d_2 \cos 2x + \cdots \\ &+ c_n \sin nx + d_n \cos nx, \end{aligned} \tag{6.1}$$

where $c_0, c_1, \ldots, c_n, d_1, \ldots, d_n$ are in $\mathbb{R}$. For example, $1 + \cos 2x$ is a trigonometric series that defines the same function as $2\cos^2 x$. Similarly, the function $4\cos^3 x$ is the trigonometric series $3\cos x + \cos 3x$.

And there's more to come: See Exercise 6.1.

If one is given a function f that can be expressed as a finite trigonometric series, is it possible to express the coefficients $c_0, c_1, d_1, \ldots, c_n, d_n$ in terms of f?

This is where the chapter will begin, showing that there are indeed explicit expressions for the coefficients in a finite trigonometric series in terms of the function so expressed. And there's more: we shall investigate the extent to which an arbitrary function (with some restrictions) can be expressed as a (possibly infinite) trigonometric series called its *Fourier series*. Fourier series will lead us into a wonderful garden of formulas that involve trigonometric functions and to a generalization of the "Gauss sum" that we met way back in Section 2.2.

6.1 The Fourier Series of a Differentiable Function and $\zeta(2)$

This chapter opened with a question:

> If one is given a finite trigonometric series $f(x)$ of the above form, is it possible to express the coefficients $c_0, c_1, d_1, \ldots, c_n, d_n$ in terms of the function f?

The answer is supplied by recalling the basic "orthogonality relations" between the functions $\sin nx$ and $\cos nx$. Namely, if n and m are nonnegative integers, then

K. Ireland and A. Cuoco, *Excursions in Number Theory, Algebra, and Analysis*, Readings in Mathematics, https://doi.org/10.1007/978-3-031-13017-5_6

$$\text{(i)}\quad \int_{-\pi}^{\pi} \cos nx \cos mx\, dx = \begin{cases} \pi & \text{if } n = m \neq 0, \\ 0 & \text{if } n \neq m; \end{cases}$$

$$\text{(ii)}\quad \int_{-\pi}^{\pi} \sin nx \cos mx\, dx = 0 \text{ for all } n, m;$$

$$\text{(iii)}\quad \int_{-\pi}^{\pi} \sin nx \sin mx\, dx = \begin{cases} \pi & \text{if } n = m \neq 0, \\ 0 & \text{if } n \neq m. \end{cases}$$

In order to verify these formulas, recall the formulas

$$\begin{aligned} 2\,\cos nx \cos mx &= \cos(n+m)x + \cos(n-m)x, \\ 2\,\sin nx \sin mx &= \cos(n-m)x - \cos(n+m)x, \\ 2\,\sin nx \cos mx &= \sin(n+m)x + \sin(n-m)x. \end{aligned}$$

To check equality (i), for example, we use the first identity: If $n = m$, then $2\cos^2 nx = \cos 2nx + 1$, so that

$$2\int_{-\pi}^{\pi} \cos^2 nx\, dx = \int_{-\pi}^{\pi} \cos 2nx\, dx + \int_{-\pi}^{\pi} 1 \cdot dx = \frac{\sin 2nx}{2n}\Big|_{-\pi}^{\pi} + 2\pi = 0 + 2\pi,$$

or equivalently,

$$\int_{-\pi}^{\pi} \cos^2 nx\, dx = \pi.$$

If $n \neq m$, then

$$2\int_{-\pi}^{\pi} \cos nx \cos mx\, dx = \frac{\sin(n+m)x}{(n+m)}\Big|_{-\pi}^{\pi} + \frac{\sin(n-m)x}{(n-m)}\Big|_{-\pi}^{\pi} = 0.$$

Exercise 6.3. The remaining orthogonality relations are left as an (important!) exercise.

In order to answer our question about expressing the c's and d's in terms of $f(x)$, we proceed as follows. To get c_0, we simply integrate both sides of equation (6.1) from $-\pi$ to π. That gives

$$\int_{-\pi}^{\pi} f(x)\, dx = 2\pi c_0,$$

or equivalently,

$$c_0 = \frac{1}{2\pi}\int_{-\pi}^{\pi} f(x)\, dx.$$

For c_n when $n > 0$, multiply by $\sin nx$ and integrate from $-\pi$ to π, obtaining

$$\int_{-\pi}^{\pi} f(x) \sin nx\, dx = c_n \int_{-\pi}^{\pi} \sin^2 nx\, dx = c_n \pi,$$

or equivalently,

$$c_n = \frac{1}{\pi}\int_{-\pi}^{\pi} f(x) \sin nx\, dx. \tag{6.2}$$

Similarly,

$$d_n = \frac{1}{\pi}\int_{-\pi}^{\pi} f(x) \cos nx\, dx. \tag{6.3}$$

In this way, we have expressed the coefficients c_n and d_n in terms of the integrals of f multiplied by $\sin nx$ and $\cos nx$, the range of integration being the interval from $-\pi$ to π. As a simple example, taking $n = 3$ and using the identity $4\cos^3 x = 3\cos x + \cos 3x$, a computation shows that that

$$\int_{-\pi}^{\pi} \cos^3 x \cos 3x \, dx = \frac{\pi}{4}.$$

If $f(x)$ is any function integrable on $[-\pi, \pi]$ (say, continuous or piecewise continuous), then the above observations motivate the definition of a series of constants called the *Fourier coefficients* of f. They are defined by the following formulas:

$$\begin{aligned} a_n &= \frac{1}{\pi} \int_{-\pi}^{\pi} f(x) \cos nx \, dx, \quad n = 0, 1, \ldots, \\ b_n &= \frac{1}{\pi} \int_{-\pi}^{\pi} f(x) \sin nx \, dx, \quad n = 1, 2, \ldots. \end{aligned} \tag{6.4}$$

Notice that the a_n begin with

$$a_0 = \frac{1}{\pi} \int_{-\pi}^{\pi} f(x) \, dx,$$

Keep in mind that the a_n belong to the "cosine" coefficients and the b_n belong to the "sine" coefficients.

while the b_n begin with $b_1, b_2, \ldots$. Formulas (6.2) and (6.3) can now be stated like this:

Lemma 6.1. *If $f(x)$ is a finite trigonometric series of degree n,*

$$f(x) = \frac{a_0}{2} + \sum_{k=1}^{n} a_k \cos kx + b_k \sin kx,$$

then $a_0, a_1, \ldots, a_n, b_1, \ldots, b_n$ are the Fourier coefficients of f.

If $f(x)$ is not a finite trigonometric series, then the Fourier coefficients a_n and b_n need not be zero for n large. But it is natural to ask whether the resulting infinite series

$$\frac{a_0}{2} + \sum_{k=1}^{\infty} (a_k \cos kx + b_k \sin kx) \tag{6.5}$$

converges for $x \in (-\pi, \pi)$ and whether, if it does, it equals $f(x)$. When it does equal $f(x)$, we call it the *Fourier series* of f.

This is the basic problem in the elementary theory of Fourier series. A partial solution to the problem was supplied by Johann Peter Gustav Lejeune Dirichlet (1805–1859) in 1829 when he proved that if $f(x)$ has a derivative at x_0 in $(-\pi, \pi)$, then indeed, the series of numbers

$$\frac{a_0}{2} + \sum_{n=1}^{\infty} a_n \cos nx_0 + b_n \sin nx_0$$

converges to the number $f(x_0)$. We will prove this result in the next section. But there is a special case of a lemma due to Riemann that implies that the infinite sum above has a chance of converging to *something*.

Lemma 6.2 (Riemann). *If $f(x)$ is continuous on $[a,b]$ and has a continuous derivative on (a,b), then the Fourier coefficients of f go to zero as n approaches infinity. In symbols,*

$$b_n = \frac{1}{\pi}\int_{-\pi}^{\pi} f(x)\sin nx\,dx \to 0 \quad as\, n\to\infty,$$
$$a_n = \frac{1}{\pi}\int_{-\pi}^{\pi} f(x)\cos nx\,dx \to 0 \quad as\, n\to\infty.$$

Proof. On integrating by parts, we have

$$\int_{-\pi}^{\pi} f(x)\sin nx\,dx = -f(x)\frac{\cos nx}{n}\Big|_{-\pi}^{\pi} + \frac{1}{n}\int_{-\pi}^{\pi} f'(x)\cos nx\,dx.$$

Each term goes to 0 as $n\to\infty$. The proof of the second statement is similar. ∎

Lookout Point 6.1. Actually, the above lemma holds for every function $f(x)$ that has an integral on $[a,b]$. Recall that this condition imposes restrictions on f. It turns out that the requirement of (Riemann) integrability is equivalent to the requirement that the set of discontinuities have "measure" zero. In particular, a function with a countable set of discontinuities has a Riemann integral. (As an example of a function that does not have a Riemann integral, consider the so-called Dirichlet function, which equals 1 for x rational and 0 for x irrational. It does not have a Riemann integral on any finite interval because it is discontinuous everywhere.) Although we will use only the case in which $f(x)$ is composed of a finite number of continuously differentiable pieces (piecewise C^1), let us show how the general Riemann lemma follows from an important inequality due to Bessel. The proof of Bessel's inequality (up next) is actually more elementary than the proof of Lemma 6.2, because it doesn't use integration by parts. However, the basic idea is sophisticated, since it asks for the "mean square" approximation of $f(x)$ by the partial sums of its Fourier series. More precisely, we prove the following lemma.

For a discussion and proof of this situation (and more), see Casper Goffman's *Real Analysis* [85]. And, as you'll soon see, "elementary" is not the same as "simple."

Lemma 6.3 (Bessel's inequality). *If $f(x)$ is integrable on $[-\pi,\pi]$, then*

$$\frac{a_0^2}{2} + \sum_{n=1}^{\infty} a_n^2 + b_n^2 \le \frac{1}{\pi}\int_{-\pi}^{\pi} f(x)^2\,dx,$$

where the a_n and b_n are the Fourier coefficients of $f(x)$.

Proof. Consider (of course)

$$0 \le \int_{-\pi}^{\pi}\left(f(x) - \left(\frac{a_0}{2} + \sum_{m=1}^{n} a_m\cos mx + b_m\sin mx\right)\right)^2 dx.$$

The integrand is a (complicated) square of a binomial, so we pick it apart. Note first that if we apply the orthogonality relations from Section 6.1, we

find that (check this)

$$\int_{-\pi}^{\pi} \left(\sum_{m=1}^{n} a_m \cos mx + b_m \sin mx \right)^2 dx = \pi \sum_{m=1}^{n} a_m^2 + b_m^2 .$$

Next, check that

$$a_m \int_{-\pi}^{\pi} f(x) \cos mx \, dx = \pi a_m^2 \quad \text{and} \quad b_m \int_{-\pi}^{\pi} f(x) \sin mx \, dx = \pi b_m^2 .$$

The checks are yours in Exercise 6.5.

Using this and the rule for squaring a sum, we have

$$\begin{aligned} 0 &\le \int_{-\pi}^{\pi} \left(f(x) - \left(\frac{a_0}{2} + \sum_{m=1}^{n} a_m \cos mx + b_m \sin mx \right) \right)^2 dx \\ &= \int_{-\pi}^{\pi} f(x)^2 \, dx + \frac{2\pi {a_0}^2}{4} + \pi \sum_{m=1}^{n} {a_m}^2 + {b_m}^2 - 2 \int_{-\pi}^{\pi} f(x) \frac{a_0}{2} \, dx \\ &\quad - 2 \sum_{m=1}^{n} b_m \int_{-\pi}^{\pi} f(x) \sin \, mx \, dx - 2 \sum_{m=1}^{n} a_m \int_{-\pi}^{\pi} f(x) \cos mx \, dx \\ &= \int_{-\pi}^{\pi} f(x)^2 dx - \pi \frac{a_0^2}{2} - \pi \sum_{m=1}^{n} \left({a_m}^2 + {b_m}^2 \right) . \end{aligned}$$

Hence

$$\frac{1}{\pi} \int_{-\pi}^{\pi} f(x)^2 \, dx \ge \frac{a_0^2}{2} + \sum_{m=1}^{n} \left(a_m^2 + {b_m}^2 \right) .$$

We did it! ∎

For each n, consider the partial sums in Bessel's inequality summed up to n. Since the left-hand side is positive, it gives a bounded monotonically increasing sequence. Thus the limit exists, which is, of course, the infinite series

$$\frac{a_0^2}{2} + \sum_{m=1}^{\infty} \left({a_m}^2 + {b_m}^2 \right) .$$

Furthermore, the series is bounded by $\frac{1}{\pi} \int_{-\pi}^{\pi} f(x)^2 \, dx$.
Hence

$$\frac{a_0^2}{2} + \sum_{m=1}^{\infty} \left({a_m}^2 + {b_m}^2 \right) \le \frac{1}{\pi} \int_{-\pi}^{\pi} f(x)^2 dx .$$

This can be viewed as a weak Pythagorean theorem. The sum of the squares of the "components" or "sides" of $f(x)$ is at most the square of the "hypotenuse." It turns out, although it is harder to prove, that for a large class of functions (including continuous ones), *equality* holds. That equality is called Parseval's theorem. The abstract development of the allusion to geometry is called the theory of Hilbert and Banach spaces and is part of a large branch of contemporary mathematics called functional analysis. A pleasant essay on the development of these ideas in the first part of the

twentieth century can be found in Hermann Weyl's article "A Half Century of Mathematics" [87].

Oh, and by the way, Bessel's inequality implies Lemma 6.2 (this is Exercise 6.6).

Before we prove the general result on Fourier series, let's do a calculation that contains the basic strategy and that delights many people who see it for the first time.

Small world: This series is $\zeta(2)$, where ζ is the Riemann zeta function defined in Section 3.4.

Theorem 6.4.

$$\frac{\pi^2}{6} = 1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \cdots .$$

This proof was pointed out by D. Giesy [30].

Proof. We need the following identity, which will be used any number of times during this chapter, so let's make it a lemma. ∎

Lemma 6.5. *For $x \in [-\pi, \pi]$, we have the equality*

$$\frac{1}{2} + \cos x + \cos 2x + \cdots + \cos nx = \frac{\sin\left(n + \frac{1}{2}\right)x}{2\sin\frac{x}{2}} . \tag{6.6}$$

This is even true for $x = 0$ if one defines the right-hand side at 0 to be its continuous extension at 0, namely $n + \frac{1}{2}$ (use l'Hospital).

Proof. To see this, simply multiply both sides by $2\sin\frac{x}{2}$ to obtain

$$\sin\frac{x}{2} + 2\sin\frac{x}{2}\cos x + 2\sin\frac{x}{2}\cos 2x + \cdots + 2\sin\frac{x}{2}\cos nx .$$

Using $2\sin A\cos B = \sin(A+B) + \sin(A-B)$, we find that this sum nicely telescopes (always a good sign):

$$\sin\frac{x}{2} + \left(\sin\frac{3}{2}x - \sin\frac{1}{2}x\right) + \left(\sin\frac{5}{2}x - \sin\frac{3}{2}x\right) + \cdots + \left(\sin\left(n+\frac{1}{2}\right)x - \sin\left(n-\frac{1}{2}\right)x\right),$$

which is simply $\sin\left(n + \frac{1}{2}\right)x$, as desired. ∎

Back at the ranch, to prove Theorem 6.4, multiply both sides of equation (6.6) by x and integrate from 0 to π. We obtain

$$\frac{\pi^2}{4} + \int_0^\pi x\cos x\,dx + \int_0^\pi x\cos 2x\,dx + \cdots + \int_0^\pi x\cos nx\,dx = \int_0^\pi \frac{x\sin\left(n+\frac{1}{2}\right)x}{2\sin\frac{x}{2}}\,dx . \tag{6.7}$$

$\sin(\alpha+\beta) = \cos\alpha\sin\beta + \sin\alpha\cos\beta$

Let's take up the right-hand side first and show that it approaches 0 as n goes to infinity. Using the addition formula for sine, we see that the numerator of the integrand splits, so that

$$\int_0^\pi \frac{x\sin\left(n+\frac{1}{2}\right)x}{2\sin\frac{x}{2}}\,dx = \int_0^\pi \frac{x\cos\frac{x}{2}}{2\sin\frac{x}{2}}\sin nx\,dx + \int_0^\pi \frac{x}{2}\cos nx\,dx \tag{6.8}$$

$$= \int_0^\pi \frac{\frac{x}{2}}{\sin\frac{x}{2}}\cos\frac{x}{2}\sin nx\,dx + \int_0^\pi \frac{x}{2}\cos nx\,dx .$$

Both integrals in (6.8) satisfy the conditions of Riemann's lemma (Lemma 6.2), since $\frac{x}{2}/\sin\frac{x}{2}$ is continuous on $[0,\pi]$ and goes to 1 as $x \to 0$, so applying Riemann, we see that

$$\lim_{n\to\infty} \int_0^\pi \frac{x \sin\left(n+\frac{1}{2}\right)x}{2\sin\frac{x}{2}}\,dx$$
$$= \lim_{n\to\infty} \int_0^\pi \frac{x\cos\frac{x}{2}}{2\sin\frac{x}{2}} \sin nx\,dx + \lim_{n\to\infty} \int_0^\pi \frac{x}{2}\cos nx\,dx = 0\,.$$

On to the left-hand side of equation (6.7). This is a little easier:

$$\int_0^\pi x\cos kx\,dx = \frac{x\sin kx}{k}\bigg|_0^\pi - \frac{1}{k}\int_0^\pi \sin kx\,dx$$
$$= \frac{1}{k^2}\cos kx\bigg|_0^\pi = \frac{1}{k^2}\left((-1)^k - 1\right),$$

which is 0 if k is even and $-2/k^2$ if k is odd. Therefore, replacing n by $2n+1$, we obtain

$$\frac{\pi^2}{4} - 2\left(1 + \frac{1}{3^2} + \frac{1}{5^2} + \frac{1}{7^2} + \cdots + \frac{1}{(2n+1)^2}\right) = \int_0^\pi \frac{x\sin\left(n+\frac{3}{2}\right)x}{2\sin\frac{x}{2}}\,dx\,.$$

Now letting $n \to \infty$, we have, by the same reasoning as above,

$$\frac{\pi^2}{8} = 1 + \frac{1}{3^2} + \frac{1}{5^2} + \cdots.$$

A little juggling gives the desired result. (The one just proved is already interesting.) And we also have

$$\frac{1}{2^2} + \frac{1}{4^2} + \frac{1}{6^2} + \cdots = \frac{1}{4}\left(1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \cdots\right).$$

Also,

$$\left(1 + \frac{1}{3^2} + \frac{1}{5^2} + \cdots\right) + \left(\frac{1}{2^2} + \frac{1}{4^2} + \cdots\right)$$

is equal to

$$1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \cdots$$

on the one hand, and to

$$\frac{\pi^2}{8} + \frac{1}{4}\left(1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots\right)$$

on the other. Equating the two results yields

$$\frac{\pi^2}{8} = \frac{3}{4}\left(1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots\right),$$

or equivalently (applause),

$$\frac{\pi^2}{6} = 1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \cdots.$$

■

Lookout Point 6.2. The ubiquitous $\pi^2/6$. What is the probability that two integers chosen at random are relatively prime? In spite of the fact that the notion of "a randomly chosen integer" is a strange one, there is at least an intuitive idea of what the question means. Indeed, if we set up an experiment that picks two random integers and calculates their greatest common divisor and we repeat this thousands of times, then the ratio of the number of relatively prime pairs to the number of trials is a good approximation to the answer to our question. Of course, we are only picking numbers between 1 and 100,000 (or whatever), and that is precisely the difference between what we can do experimentally and what it might mean to choose an integer at random from all of $\mathbb{Z}$.

And it reinforces the belief that questions about integers are questions about real things.

To get a feel for the situation, you can set up an experiment in your favorite computational environment, run it many times, and see whether the results seem to cluster around a particular value. Try it—it's fun. And if you run the experiment many times, you will see that it almost always outputs a number close to 0.6. What is that trying to tell us? Put the computer away, and let's settle on a meaning for our question.

Think for a minute. Why is this assumption reasonable?

Let us assume that if p is a prime, the probability that an integer chosen at random is divisible by p is $\frac{1}{p}$. Thus the probability that an integer is even is $\frac{1}{2}$, the probability that an integer is divisible by 3 is $\frac{1}{3}$, and so on.

$1 - \frac{1}{p^2}$? Things are heating up.

It follows from this assumption that the probability that two integers chosen at random are both divisible by p is $\frac{1}{p^2}$. So the probability that two integers chosen at random are not both divisible by p is $1 - 1/p^2$.

Under these assumptions, we see that the probability that two randomly chosen integers are not both divisible by 2, 3, 5, 7, 11, or 13 is

$$\left(1 - \frac{1}{2^2}\right)\left(1 - \frac{1}{3^2}\right)\left(1 - \frac{1}{5^2}\right)\left(1 - \frac{1}{7^2}\right)\left(1 - \frac{1}{11^2}\right)\left(1 - \frac{1}{13^2}\right) \approx 0.6180\,.$$

Perhaps you can now see what is happening here—we have seen a product like this before. With a (small) leap of faith, we can pass to the limit: a and b are relatively prime if they are not both divisible by *any* prime. So, the probability that two integers a and b are relatively prime is

$$\prod_p \left(1 - \frac{1}{p^2}\right),$$

where the product is over all primes p.

Oh, my! Remember equation (3.6) in Section 3.4? Just in case, here it is:

$$\zeta(s) = 1 + \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \cdots = \prod_p \frac{1}{1 - \frac{1}{p^s}}.$$

It follows that our favorite product can be expressed in terms of the Riemann zeta function:

$$\prod_p \left(1 - \frac{1}{p^2}\right) = \frac{1}{\zeta(2)}\,.$$

Combine this with Theorem 6.4:

$$\frac{\pi^2}{6} = \zeta(2) = 1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \cdots,$$

and we have this remarkable result:

Theorem 6.6. *The probability that two integers chosen at random are relatively prime is*

$$\frac{6}{\pi^2}.$$

Note that $\pi^2/6 = 0.60792710\ldots \approx 0.6$, the experimental result proposed above. Most people who hear this result (without proof) wonder what in the world π has to do with it. Now you know.

See https://mathworld.wolfram.com/RelativelyPrime.html for more detail about these ideas.

Exercises

6.1 Consider the following recursively defined sequence of polynomials $\{T(k)\}$ in $\mathbb{Z}[x]$:

$$T(k) = \begin{cases} 1 & \text{if } k = 0, \\ x & \text{if } k = 1, \\ 2xT(k-1) - T(k-2) & \text{if } k > 1\,. \end{cases}$$

For example,

$$T(0) = 1, \quad T(1) = x, \quad T(2) = 2x^2 - 1, \quad T(3) = 4x^3 - 3x\,.$$

(i) Calculate a few more of the (six, say) terms $T(k)$ in the sequence and find some patterns in it. Prove your conjectures.

(ii) The $T(k)$ are formal polynomials in x, so you can substitute values for x and get identities about numbers. Show that for every real value of θ,

$$T(n)(\cos\theta) = \cos n\theta\,.$$

This generalizes the high-school "double-angle formula" for $\cos 2\theta$.

(iii) **Take It Further.** How about a closed form for T?

6.2 Show that

$$\int_{-\pi}^{\pi} \cos^3 x \cos 3x\, dx = \frac{\pi}{4}\,.$$

6.3 Prove the remaining orthogonality relations from this section:

(ii) $\int_{-\pi}^{\pi} \sin nx \cos mx\, dx = 0$ for all n, m,

(iii) $\int_{-\pi}^{\pi} \sin nx \sin mx\, dx = \begin{cases} \pi & \text{if } n = m \neq 0, \\ 0 & \text{if } n \neq m\,. \end{cases}$

6.4 Interpret the expression

$$\int_{-\pi}^{\pi} \left(f(x) - \left(\frac{a_0}{2} + \sum_{m=1}^{n} a_m \cos mx + b_m \sin mx \right) \right)^2 dx$$

as an "average (mean) square distance."

6.5 Using the notation of this section, show that

(i)

$$\left(\sum_{m=1}^{n} a_m \cos mx + b_m \sin mx\right)^2 = \pi \sum_{m=1}^{n} a_m^2 + b_m^2,$$

(ii)

$$a_m \int_{-\pi}^{\pi} f(x) \cos mx \, dx = \pi a_m^2 \quad \text{and} \quad b_m \int_{-\pi}^{\pi} f(x) \sin mx \, dx = \pi b_m^2 .$$

6.6 Show that Bessel's inequality (Lemma 6.3) implies Riemann's lemma (Lemma 6.2).

6.7 What is the probability that an integer picked at random has no perfect square factor?

6.2 Dirichlet's Theorem

Let us state at once what we want to prove.

Theorem 6.7 (Dirichlet, 1829). *Let $f(x)$ be continuous on $[-\pi, \pi]$ and differentiable at a point $x_0 \in (-\pi, \pi)$. Then*

$$f(x_0) = \frac{a_0}{2} + \sum_{n=1}^{\infty} (a_n \cos nx_0 + b_n \sin nx_0),$$

where

$$a_n = \frac{1}{\pi} \int_{-\pi}^{\pi} f(x) \cos nx \, dx, \quad n = 0, 1, 2, \ldots,$$
$$b_n = \frac{1}{\pi} \int_{-\pi}^{\pi} f(x) \sin nx \, dx, \quad n = 1, 2, \ldots .$$

This is not a superficial statement, since the coefficients a_n and b_n are determined by the values of the functions on the whole interval.

Notice that we have assumed $f(x)$ to be differentiable only at $x = x_0$. It can be quite nasty away from x_0. In fact, the proof we give will show that whether the series converges depends only on the behavior of f *near* x_0.

Proof. To prove the result, form the number

$$S_n = \frac{a_0}{2} + \sum_{k=1}^{n} (a_k \cos kx_0 + b_k \sin kx_0) .$$

We must show that

$$S_n \to f(x_0) \quad \text{as } n \to \infty .$$

Our first (and major) task is to express S_n as a definite integral. Replace $a_0, a_1, \ldots, a_n, b_1, b_2, \ldots, b_n$ in S_n by their values as definite integrals to obtain

$$
\begin{aligned}
S_n &= \frac{1}{2\pi}\int_{-\pi}^{\pi} f(x)dx + \sum_{k=1}^{n}\frac{1}{\pi}\int_{-\pi}^{\pi} f(x)(\cos kx\cos kx_0 + \sin kx\sin kx_0)\,dx \\
&= \frac{1}{\pi}\int_{-\pi}^{\pi} f(x)\left\{\frac{1}{2} + \sum_{k=1}^{n}\cos kx\cos kx_0 + \sin kx\sin kx_0\right\}dx \\
&= \frac{1}{\pi}\int_{-\pi}^{\pi} f(x)\left\{\frac{1}{2} + \sum_{k=1}^{n}\cos k(x-x_0)\right\}dx \\
&= \frac{1}{\pi}\int_{-\pi}^{\pi} f(x)\frac{\sin(n+\frac{1}{2})(x-x_0)}{2\sin\left(\frac{x-x_0}{2}\right)}\,dx\,.
\end{aligned}
$$

This last equality is thanks to Lemma 6.5.

This expresses the finite sum S_n of the series we are investigating as a definite integral involving $f(x)$. Next we want to change the variable by replacing $x-x_0$ with t. However, f is defined only on $[-\pi,\pi]$. Extend $f(x)$ periodically to $\mathbb{R}$ by defining $f(x+2\pi) = f(x)$, so that that f now is periodic of period 2π.

Check that the *entire* integrand is now periodic of period 2π.

On effecting the change of variable $x - x_0 = t$, we obtain

$$
S_n = \frac{1}{\pi}\int_{-\pi-x_0}^{\pi-x_0} f(x_0+t)\frac{\sin(n+\frac{1}{2})t}{2\sin\frac{t}{2}}\,dt\,,
$$

which by periodicity is just the integral from $-\pi$ to π. For the record:

$$
S_n = \frac{1}{\pi}\int_{-\pi}^{\pi} f(x_0+t)\frac{\sin(n+\frac{1}{2})t}{2\sin\frac{t}{2}}\,dt\,. \tag{6.9}
$$

We need to show that $S_n - f(x_0)$ has limit zero. The idea is to absorb $f(x_0)$ under the integral sign and estimate the difference using Riemann's lemma and the hypothesis of differentiability. The absorption is achieved by going back to our favorite identity:

$$
\frac{1}{2} + \cos x + \cos 2x + \cdots + \cos nx = \frac{\sin(n+\frac{1}{2})x}{2\sin\frac{x}{2}}\,.
$$

Integrating from $-\pi$ to π gives

$$
\pi + 0 + 0 + \cdots + 0 = \int_{-\pi}^{\pi}\frac{\sin(n+\frac{1}{2})t}{2\sin\frac{t}{2}}\,dt\,.
$$

Multiplying by $f(x_0)$ (a constant!) and dividing by π shows that

$$
f(x_0) = \frac{1}{\pi}\int_{-\pi}^{\pi} f(x_0)\frac{\sin(n+\frac{1}{2})t}{2\sin\frac{t}{2}}\,dt.
$$

Subtracting $f(x_0)$ from our expression for S_n gives the lovely relation

$$
S_n - f(x_0) = \frac{1}{\pi}\int_{-\pi}^{\pi}(f(x_0+t) - f(x_0))\cdot\frac{\sin(n+\frac{1}{2})t}{2\sin\frac{t}{2}}\,dt\,. \tag{6.10}
$$

Next, let $g(t) = f(x_0+t) - f(x_0)$.

We are ready to operate. Consider

$$\frac{1}{t} - \frac{1}{2\sin\frac{t}{2}} = \frac{2\sin\frac{t}{2} - t}{2t\sin\frac{t}{2}}\,. \tag{6.11}$$

We apply l'Hospital a few times to see the behavior of the right-hand side at 0:

$$\lim_{t\to 0} \frac{2\sin\frac{t}{2} - t}{2t\sin\frac{t}{2}} = \lim_{t\to 0} \frac{\cos\frac{t}{2} - 1}{t\cos\frac{t}{2} + 2\sin\frac{t}{2}} = \lim_{t\to 0} \frac{-\sin\frac{t}{2}}{\cos\frac{t}{2} - \frac{t}{2}\sin\frac{t}{2} + \frac{\cos t}{2}} = 0\,.$$

So, thanks to l'Hospital, we see that

$$\frac{1}{t} - \frac{1}{2\sin\frac{t}{2}}$$

is continuous at 0.

Thus, with some fancy footwork, we can write

$$S_n(x) - f(x_0) = \tag{6.12}$$
$$\frac{1}{\pi}\int_{-\pi}^{\pi} g(t)\frac{\sin\left(n+\frac{1}{2}\right)t}{t}\,dt - \frac{1}{\pi}\int_{-\pi}^{\pi} g(t)\left(\frac{1}{t} - \frac{1}{2\sin\frac{t}{2}}\right)\sin\left(n+\frac{1}{2}\right)t\,dt\,.$$

But

$$\frac{1}{\pi}\int_{-\pi}^{\pi} g(t)\left(\frac{1}{t} - \frac{1}{2\sin\frac{t}{2}}\right)\sin\left(n+\frac{1}{2}\right)t\,dt = \frac{1}{\pi}\int_{-\pi}^{\pi} H(t)\sin\left(n+\frac{1}{2}\right)t\,dt\,,$$

where H is continuous. So again by Riemann (Lemma 6.2), we have

$$\lim_{n\to\infty}\frac{1}{\pi}\int_{-\pi}^{\pi} H(t)\sin\left(n+\frac{1}{2}\right)t\,dt = 0\,.$$

Next, passing to ∞, we have

$$\begin{aligned}\lim_{n\to\infty}\left(S_n(x) - f(x_0)\right) &= \lim_{n\to\infty}\frac{1}{\pi}\int_{-\pi}^{\pi} g(t)\frac{\sin(n+\frac{1}{2})t}{t}\,dt \\ &= \lim_{n\to\infty}\frac{1}{\pi}\int_{-\pi}^{\pi}\frac{f(x_0+t)-f(x_0)}{t}\sin\left(n+\frac{1}{2}\right)t\,dt\,.\end{aligned}$$

Here is where differentiability enters the action, because the differential quotient

$$\frac{f(x_0+t)-f(x_0)}{t}$$

is continuous at x_0. And once again, Riemann comes to the rescue, so that (at last)

$$\lim_{n\to\infty} S_n(x) - f(x_0) = 0\,.$$

We did it! ∎

Although l'Hospital is convenient, it is useful (and fun) to derive Theorem 6.7 directly from the mean value theorem. Here are the details.

Proof. Applying the mean value theorem to $2\sin\frac{t}{2}$ on $[0,t]$ gives

$$2\sin\frac{t}{2} - 0 = t\cos\xi_t, \quad \text{where } 0 < \xi_t < t\,.$$

Hence

$$\frac{1}{t} - \frac{1}{2\sin\frac{t}{2}} = \frac{1}{t}\left(1 - \frac{1}{\cos\xi_t}\right) = \frac{\cos\xi_t - 1}{\xi_t}\cdot\frac{\xi_t}{t\cos\xi_t}.$$

Now, $(\cos\xi_t - 1)/t$ approaches 0 as $\xi_t \to 0$, as follows from the mean value theorem again applied to $\cos x$, since $\xi_t/t < 1$ and $\cos\xi_t$ approaches 1 as $\xi_t \to 0$.

After all, how does one *prove* l'Hospital!?

A double application of the mean value theorem replaces a double application of l'Hospital. Returning to $S_n - f(x_0)$, we write

$$\begin{aligned} S_n - f(x_0) = {} & \frac{1}{\pi}\int_{-\pi}^{\pi}\frac{f(x_0+t)-f(x_0)}{t}\cdot\sin\left(n+\frac{1}{2}\right)t\,dt \qquad (6.13)\\ & -\frac{1}{\pi}\int_{-\pi}^{\pi}(f(x_0+t)-f(x_0))\left(\frac{1}{t}-\frac{1}{2\sin t/2}\right)\cdot\sin\left(n+\frac{1}{2}\right)t\,dt\,. \end{aligned}$$

The second integral approaches zero as $n \to \infty$ by Riemann's lemma. As for the first integral, we will see that its behavior is concentrated at 0. More precisely, let $\delta > 0$ be very small. Write the first integral of (6.13) as the sum of three integrals by splitting the interval of integration at $t = -\delta$ and $t = \delta$. Away from 0, the denominator of t is harmless, and Riemann's lemma tells us that two of the three integrals go to 0 as $n \to \infty$. In other words,whether the series S_n converges to $f(x_0)$ depends solely on the remaining integral

$$\int_{-\delta}^{\delta}\frac{f(x_0+t)-f(x_0)}{t}\cdot\sin\left(n+\frac{1}{2}\right)t\,dt\,.$$

If we assume that $f(x)$ is differentiable at x_0, then by definition,

$$\frac{f(x_0+t)-f(x_0)}{t}$$

is continuous at 0, and a final application of Riemann's lemma finishes the proof of Dirichlet's theorem. ∎

Lookout Point(s) 6.3. It turns out that without some restriction on the behavior of $f(x)$ at x_0 (i.e., of $f(x_0+t)$ at $t = 0$), one cannot prove that $S_n \to f(x_0)$. In 1910, Lipót Fejér (1880–1959) produced an example of a *continuous* function for which the sequence $S_n(x_0)$ is unbounded. The assumption of differentiability at x_0 is stronger than needed, but it illustrates the method and suffices for many applications.

Dirichlet's paper in which he establishes this result leaves nothing to be desired in terms of modern-day rigor. An examination of the proof shows that

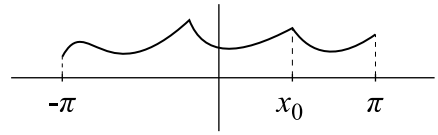


Figure 6.1. There can be cusps in the graph of $y = f(x)$.

it still goes through if we assume $f(x)$ to have only left and right derivatives at x_0. It is only necessary to break the integral $\int_{-\delta}^{\delta} f(x)\,dx$ into $\int_{-\delta}^{0} f(x)\,dx + \int_{0}^{\delta} f(x)\,dx$ and use Riemann's lemma on each integral, observing that the existence of a left and right derivative gives continuity at the critical endpoint. Thus the situation illustrated in Figure 6.1 is allowed to happen.

Furthermore, one can handle the case of a simple jump discontinuity as in Figure 6.2. For this we assume that left- and right-hand derivatives

$$\lim_{t\to 0+} \frac{f(x_0+t)-f(x_0)}{t} \quad \text{and} \quad \lim_{t\to 0-} \frac{f(x_0+t)-f(x_0)}{t}$$

It's a good exercise to carry out the translation.

exist. For you can just push the pieces together and use the proof above. The result is that $S_n(x_0)$ approaches the average

$$\frac{f(x_0{}^+)+f(x_0{}^-)}{2}.$$

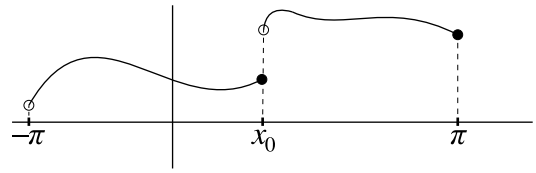


Figure 6.2. There can be jumps.

Finally, we mention that due to the fact that f has been extended to have period 2π, the limits $-\pi$ and π can be replaced by a and $a+2\pi$. In other words, it is just the length of the interval that matters. Often you will see integrals from $-\pi$ to π replaced with the same integrand with limits from 0 to 2π. Thus we can state a corollary.

Corollary 6.8. *If $f(x)$ is defined on $[0, 2\pi]$ and differentiable at $x_0 \in (0, 2\pi)$, then*

$$f(x_0) = \frac{a_0}{2} + \sum_{k=1}^{\infty} (a_k \cos kx_0 + b_k \sin kx_0),$$

where

$$a_n = \frac{1}{\pi}\int_{-\pi}^{\pi} f(x)\cos nx\,dx, \quad n = 0, 1, 2, \ldots,$$
$$b_n = \frac{1}{\pi}\int_{-\pi}^{\pi} f(x)\sin nx\,dx, \quad n = 1, 2, \ldots.$$

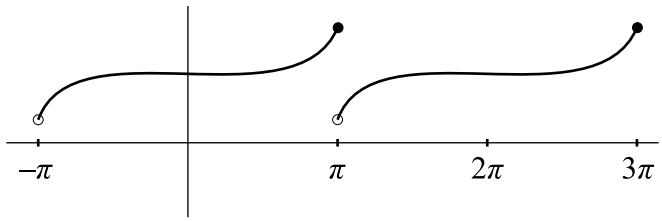


Figure 6.3. Endpoint discontinuities at odd multiples of π.

Another thing: if f is continuous on $[-\pi, \pi]$, its periodic extension need not be continuous at an endpoint of the interval (see Figure 6.3). However, the above observations show that if we shift the interval of integration so that the jump discontinuity falls inside, then we may conclude that the Fourier series at $x = \pi$ is $\frac{f(\pi)+f(-\pi)}{2}$ when the graph of f has left and right derivatives at π. We shall use this observation later.

And one *more* thing: In our evaluation of Gauss sums we need to work on $[0, 1]$, which doesn't have length 2π. But if $f(x)$ is defined on $[0, 1]$, then $f(\frac{x}{2\pi})$ is defined on $[0, 2\pi]$. Applying the theorem on $[0, 2\pi]$ and simplifying gives the following normalized result.

Theorem 6.9 (Theorem 6.7, version 2). *If $f(x)$ is continuous on $[0, 1]$ and differentiable there, then for all x in $(0, 1)$, one has*

$$f(x) = \frac{\alpha_0}{2} + \sum_{k=1}^{\infty}(\alpha_k \cos 2\pi kx + \beta_k \sin 2\pi kx),$$

where

$$\alpha_k = 2\int_0^1 f(t)\cos 2\pi kt\,dt, \quad k = 0, 1, \ldots,$$
$$\beta_k = 2\int_0^1 f(t)\sin 2\pi kt\,dt, \quad k = 1, 2, \ldots.$$

Furthermore, when $f(x)$ has a right derivative at 0 and a left derivative at 1, one has

$$\frac{\alpha_0}{2} + \sum_{k=1}^{\infty}\alpha_k = \frac{f(0) + f(1)}{2}.$$

6.3 Applications to Numerical Series

Doing the first thing will show up in the exercises.

One thing to do with Dirichlet's theorem is to calculate the Fourier series for some familiar functions. Another is to find a function with a given series. In this section, we will do the second thing and end up with some very pretty identities.

Example 1. One of the earliest series investigated was

$$\sin x + \frac{\sin 2x}{2} + \frac{\sin 3x}{3} + \cdots .$$

For this, consider (of course) the function f defined by $f(x) = \frac{\pi - x}{2}$ on $[0, \pi]$. In order to apply Dirichlet's theorem (Theorem 6.7), we need to extend its domain to $[-\pi, \pi]$, so let's consider (again, of course) the function f that is $\frac{\pi - x}{2}$ on $[0, \pi]$ and $\frac{-\pi - x}{2}$ on $[-\pi, 0)$. Its graph is pictured in Figure 6.4.

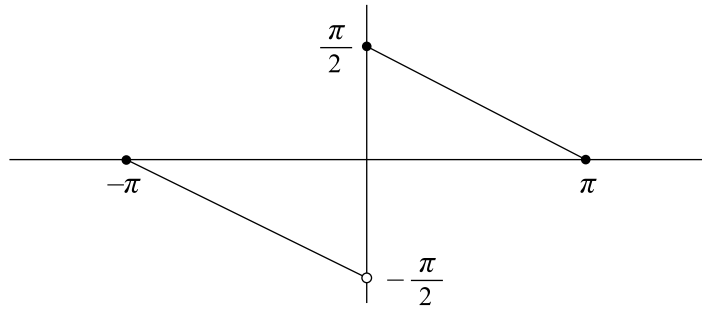


Figure 6.4. $f(x) = \frac{\pi - x}{2}$ on $[0, \pi]$ and $\frac{-\pi - x}{2}$ on $[-\pi, 0)$.

We have, by construction,

$$f(x) = -f(-x) \text{ for } x \in [0, \pi].$$

And how would you define an *even* function? How about an example of each kind? See Exercises 6.8 and 6.9 for more about even and odd functions.

Such a function is called *odd*. All the "even" Fourier coefficients for an *odd* function are zero, since

$$\begin{aligned} a_n &= \frac{1}{\pi}\int_{-\pi}^{\pi} f(x)\cos nx\,dx = \frac{1}{\pi}\int_{\pi}^{-\pi} f(-x)\cos n(-x)\,d(-x) \\ &= \frac{1}{\pi}\int_{\pi}^{-\pi} f(x)\cos nx\,dx = -\frac{1}{\pi}\int_{-\pi}^{\pi} f(x)\cos nx\,dx = -a_n. \end{aligned}$$

Thus $2a_n = 0$, which implies $a_n = 0$. Furthermore, we can simplify calculation of the "odd" coefficients by showing in the same way that

This is Exercise 6.10.

$$b_n = \frac{2}{\pi}\int_0^{\pi} f(x)\sin nx\,dx.$$

On $[0, \pi]$, we have $f(x) = \frac{\pi - x}{2}$. Therefore,

$$\begin{aligned} b_n &= \frac{2}{\pi}\int_0^\pi \left(\frac{\pi - x}{2}\right)\sin nx\,dx \\ &= \frac{2}{\pi}\int_0^\pi \frac{\pi}{2}\sin nx\,dx - \frac{1}{\pi}\int_0^\pi x\sin nx\,dx \\ &= \int_0^\pi \sin nx\,dx - \frac{1}{\pi}\left[\frac{-x\cos nx}{n}\Big|_0^\pi + \frac{1}{n}\int_0^\pi \cos nx\,dx\right] \\ &= -\frac{1}{n}\cos nx\Big|_0^\pi + \frac{(-1)^n}{n} + 0 \\ &= -\frac{(-1)^n}{n} + \frac{1}{n} + \frac{(-1)^n}{n} + 0 = \frac{1}{n}. \end{aligned}$$

Applying Dirichlet's theorem gives us the following result.

Theorem 6.10. *For $x \in (0, \pi)$,*

$$\frac{\pi - x}{2} = \sin x + \frac{\sin 2x}{2} + \cdots. \tag{6.14}$$

How nice. Substitute $x = \pi/2$ to obtain

$$\frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots, \tag{6.15}$$

which is our friend the Leibniz–Gregory series. See Exercise 6.11.

Example 2. As a second application, consider the function f defined by

$$f(x) = \begin{cases} \frac{\pi}{4} & \text{if } x \in (0, \pi), \\ \frac{-\pi}{4} & \text{if } x \in (-\pi, 0), \end{cases}$$

and then further defined indefinitely in both directions so that it has period 2π. Since the Fourier series insists on the value 0 at the origin, we might as well put $f(0) = 0$. Hence the graph of $y = f(x)$ is as in Figure 6.5.

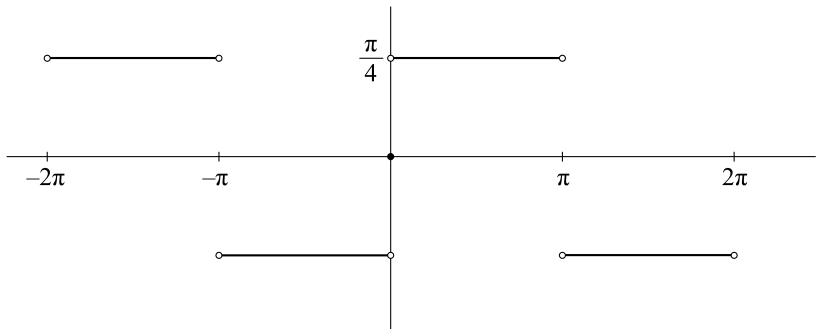


Figure 6.5. An odd function.

Since f is odd, the "even" coefficients a_{2n} are all zero, and

$$b_n = \frac{2}{\pi}\int_0^\pi f(x)\sin nx\,dx = \frac{2}{\pi}\int_0^\pi \frac{\pi}{4}\sin nx\,dx = \frac{1}{2}\int_0^\pi \sin nx\,dx$$
$$= \frac{1}{2}\left|-\frac{\cos nx}{n}\right|_0^\pi = \frac{-1}{2n}\left((-1)^n - 1\right),$$

which is equal to $\frac{1}{n}$ if n is odd, and 0 if n is even.

Hence if $x \in (0,\pi)$, then

$$\frac{\pi}{4} = \sin x + \frac{\sin 3x}{3} + \frac{\sin 5x}{5} + \cdots.$$

Putting $x = \frac{\pi}{6}$ gives

This expression for $\frac{\pi}{3}$ might require a "little think" in order to convince yourself that it is true.

$$\frac{\pi}{3} = 1 + \frac{1}{5} - \frac{1}{7} - \frac{1}{11} + \frac{1}{13} + \frac{1}{17} - \frac{1}{19} - \frac{1}{23} + \cdots.$$

Take It Further

Here is another pretty formula. For $x \in [0,\pi]$,

$$\frac{\pi^2}{8} - \frac{\pi x}{4} = \frac{\cos x}{1^2} + \frac{\cos 3x}{3^2} + \frac{\cos 5x}{5^2} + \cdots.$$

This is Exercise 6.12.

For the proof, just calculate the Fourier series of the left-hand side. You might ask how one invents the left-hand side. Well, it is linear in x. But x is an odd function, and the right-hand side is even. So any Fourier series experimenter who tried $|x|$, which is x made even, will arrive at the desired series. You should make x^2 odd and see what happens. Incidentally, putting $x = 0$ gives once again

$$\frac{\pi^2}{8} = 1 + \frac{1}{3^2} + \frac{1}{5^2} + \cdots.$$

Example 3. As a third application of Fourier series we will see how the Fourier series for certain functions that depend on a parameter give non-trigonometric expansions for other functions. The example we use here is $\cos ax$, where a is a fixed real number, but not an integer. If you calculate the Fourier series on $[-\pi,\pi]$, you get

$$\cos ax = \frac{\sin a\pi}{\pi}\left|\frac{1}{a} - \frac{2a}{a^2-1^2}\cos x + \frac{2a}{a^2-2^2}\cos 2x - \cdots\right|.$$

Putting $x = 0$ and viewing a as a variable, we have

$$\frac{\pi}{\sin a\pi} = \frac{1}{a} - \frac{2a}{a^2-1} + \frac{2a}{a^2-4} - \frac{2a}{a^2-9} - \cdots.$$

In other words, on replacing a by x, we have the result that if $x \notin \mathbb{Z}$, then

$$\frac{\pi\csc(\pi x)}{2x} = \frac{1}{2x^2} - \frac{1}{x^2-1} + \frac{1}{x^2-4} - \frac{1}{x^2-9} + \cdots,$$

which yields an infinite partial fraction expression for for the cosecant function $\csc(\pi x)$.

Exercises

6.8 Show that every real-valued function is the sum of an even function and an odd function.

6.9 What polynomial functions are even functions? Odd functions? Prove what you state.

6.10 Show that for an odd function, the odd Fourier coefficients b_n are given by

$$b_n = \frac{2}{\pi}\int_0^\pi f(x)\sin nx\,dx.$$

6.11 Show that $\sin n\pi/2$ is a Dirichlet character modulo 4. In other words,

$$\sin\frac{n\pi}{2} = \begin{cases} 0 & \text{if } n \equiv 0 \pmod 4, \\ 0 & \text{if } n \equiv 2 \pmod 4, \\ 1 & \text{if } n \equiv 1 \pmod 4, \\ -1 & \text{if } n \equiv 3 \pmod 4. \end{cases}$$

6.12 Calculate the Fourier series for $f(x) = |x|$.

6.13 Let f and g be continuous on $[-1,1]$ and differentiable on $(0,1)$. Show that the Fourier coefficients of a linear combination of f and g, say $cf + dg$, where c and d are real numbers, are the corresponding linear combinations of the Fourier coefficients of f and g.

6.14 **Take It Further.** Calculate the Fourier coefficients on $[-\pi,\pi]$ for $f_n(x) = |x|^n$, $n = 1,2,3,4$. State and prove any regularity (in terms of n) that you find in the formulas.

6.4 Gauss Sums

In Chapter 2, we met a certain sum of roots of unity called a *Gauss sum*. A special case came up in the construction of a regular pentagon. Recall what a Gauss sum is: if $\zeta = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n} = e^{2\pi i/n}$, then

See equation (2.10) in Section 2.2.

$$G_n = 1 + \zeta + \zeta^4 + \zeta^9 + \cdots + \zeta^{(n-1)^2}.$$

Note that $G_1 = 1$. We will use this in a bit.

Gauss succeeded in evaluating G_n. The answer is rather amazing. One has

$$G_n = \begin{cases} (1+i)\sqrt{n} & \text{if } n \equiv 0\ (4), \\ \sqrt{n} & \text{if } n \equiv 1\ (4), \\ i\sqrt{n} & \text{if } n \equiv 3\ (4), \\ 0 & \text{if } n \equiv 2\ (4). \end{cases}$$

This remarkable result has been proved many times over. The proof we give here is due to Dirichlet and amounts to an ingenious application of a Fourier series. More precisely, the evaluation of G_n will be achieved by evaluating $\int_0^\infty \cos(x^2)\,dx$ and $\int_0^\infty \sin(x^2)\,dx$ in two different ways, coupled with the Fourier series for $\cos(x^2)$ and $\sin(x^2)$. Here we go ...

6.4.1 A Brief Review of Infinite Integrals

We need some facts about real-valued functions f defined on $[a, \infty)$. Suppose $\int_a^N f(x)\,dx$ exists for each $N \geq a$. If $\lim_{N\to\infty} \int_a^N f(x)\,dx$ exists, then we denote it by $\int_a^\infty f(x)\,dx$. The only lemma we need concerns integrals of the type $\int_0^\infty f(x)\cos x\,dx$ and $\int_0^\infty f(x)\sin nx\,dx$, where $f(x)$ is a positive monotonically decreasing function with limit zero as $x \to \infty$. We prove the lemma for the sine integral and leave to you the other case.

It's left to you as Exercise 6.15.

Lemma 6.11. *If $f(x)$ is integrable on $[a, N)$ for every $N > a$ and if $f(x)$ is positive and monotonically decreasing to 0 as $x \to \infty$, then $\int_a^\infty f(x)\sin x\,dx$ exists.*

Proof. Since $f(x) > 0$ and $\sin x$ alternates sign, the graph of $y = f(x)\sin x$ is as in Figure 6.6.

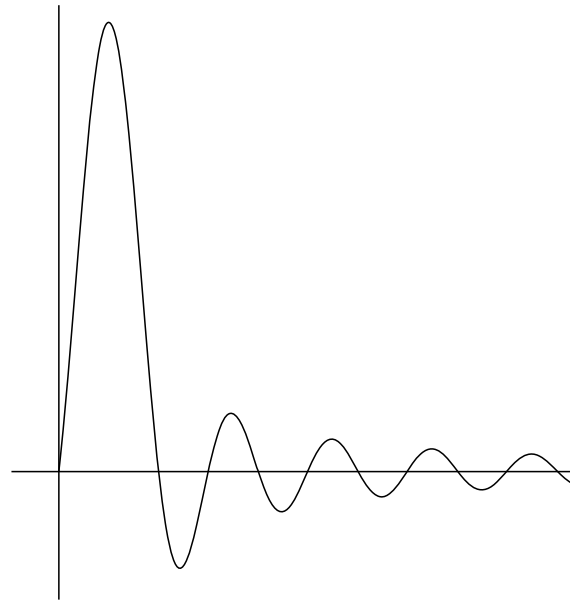


Figure 6.6. $y = f(x)\sin(x)$.

We must show, by definition, that

$$\lim_{N\to\infty} \int_a^N f(x)\sin x\,dx$$

exists. For that, divide $[a, \infty)$ as pictured in Figure 6.7.

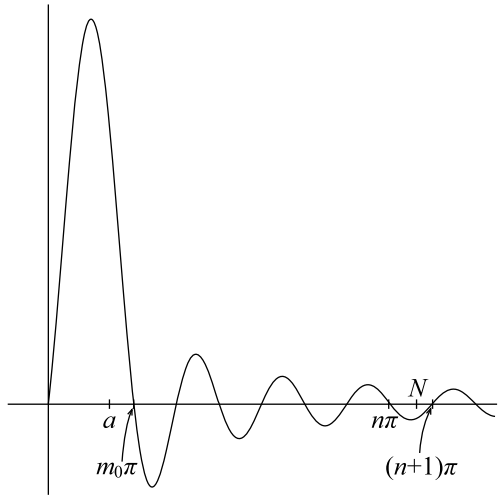


Figure 6.7. A partition of $[a, \infty)$.

That is, $m_0\pi$ is the first multiple of π after a, and N is chosen such that $n\pi < N \le (n+1)\pi$. Then

The Archimedean property of $\mathbb{R}$ raises its head again.

$$\int_a^N f(x)\sin x\,dx = \int_a^{m_0\pi} f(x)\sin x\,dx + \int_{m_0\pi}^{(m_0+1)\pi} f(x)\sin x\,dx + \cdots + \int_{(n-1)\pi}^{n\pi} f(x)\sin x\,dx + \int_{n\pi}^{N} f(x)\sin x\,dx.$$

Convince yourself that since $f(x)$ is positive and monotonically decreasing, we have

$$\left|\int_{n\pi}^{N} f(x)\sin x\,dx\right| \le f(n\pi)\int_{n\pi}^{(n+1)\pi} |\sin x|\,dx = 2f(n\pi). \tag{6.16}$$

Hence (using equation (6.16)), we have

$$\left|\int_{k\pi}^{(k+1)\pi} f(x)\sin x\,dx\right| = \int_{k\pi}^{(k+1)\pi} f(x)|\sin x|\,dx \le 2f(k\pi) \le \left|\int_{(k-1)\pi}^{k\pi} f(x)\sin x\,dx\right|.$$

So by Leibniz's result on alternating series whose nth term goes to zero, we see that

Leibniz's result on alternating series is also known as the alternating series test.

$$\int_{m_0\pi}^{(m_0+1)\pi} f(x)\sin x\,dx + \cdots + \int_{(n-1)\pi}^{n\pi} f(x)\sin x\,dx$$

converges. Hence

$$\lim_{N\to\infty}\int_a^N f(x)\sin x\,dx$$

exists. That is the same as saying that $\int_a^\infty f(x)\sin x\,dx$ exists, as promised.

■

Corollary 6.12. *It follows that the integrals*

$$\int_0^\infty \sin\left(x^2\right)\,dx = \frac{1}{2}\int_0^\infty \frac{\sin x}{\sqrt{x}}\,dx$$

and

Let $u = x^2$, so that $dx = \frac{du}{2\sqrt{u}}$.

$$\int_0^\infty \cos\left(x^2\right)\,dx = \frac{1}{2}\int_0^\infty \frac{\cos x}{\sqrt{x}}\,dx$$

exist.

6.4.2 Using Complex Numbers

Moving up to $\mathbb{C}$ will make the calculations simpler and highlight the essential ideas in the proof.

Next, we up the ante a little and look at functions defined on $\mathbb{R}$ and taking values in $\mathbb{C}$. If $f(x)$ is a complex-valued function of a real variable x, then one may define $\int_a^b f(x)\,dx = \int_a^b f_1(x)\,dx + i\int_a^b f_2(x)\,dx$, where $f_1(x)+if_2(x) = f(x)$. We say that f is differentiable if f_1 and f_2 are. In this way, all of our results on Fourier series carry over formally, and we can state the following theorem.

Theorem 6.13. *If $f(x)$ is complex-valued on $[0,1]$ and differentiable at $x_0 \in (0,1)$, then*

$$f(x_0) = \frac{\alpha_0}{2} + \sum_{n=1}^{\infty}(\alpha_n \cos 2\pi n x_0 + \beta_n \sin 2\pi n x_0),$$

where

$$\alpha_n = 2\int_0^1 f(t)\cos 2\pi n t\,dt, \quad n = 0, 1, \ldots,$$

$$\beta_n = 2\int_0^1 f(t)\sin 2\pi n t\,dt, \quad n = 1, 2, \ldots.$$

Furthermore, if $f(x)$ has a right-hand limit at 0 and a left-hand limit at 1, then

$$\frac{\alpha_0}{2} + \sum_{n=1}^{\infty}\alpha_n = \frac{f(0)+f(1)}{2}.$$

If we write $\exp t = e^t$ and define $f(x)$ by the formula

$$f(x) := \exp\left(\frac{2\pi i x^2}{n}\right) = \cos\left(\frac{2\pi x^2}{n}\right) + i\sin\left(\frac{2\pi x^2}{n}\right),$$

then $f(1) = \zeta_n$ and $f(j) = \zeta_n^{j^2}$ when j is an integer. So the Gauss sum G_n is simply $f(0) + f(1) + \cdots + f(n-1)$.

6.4.3 The Value of the Gauss Sum

We are now ready to compute G_n. Recall that if $f(x)$ is differentiable and complex-valued on $[0,1]$, then we have

$$\frac{\alpha_0}{2} + \sum_{n=1}^{\infty}\alpha_n = \frac{f(0)+f(1)}{2}, \tag{6.17}$$

where $\alpha_0, \alpha_1, \ldots$ are the even "normalized" Fourier coefficients for the interval $[0,1]$:

$$\alpha_n = 2\int_0^1 f(t)\cos 2\pi nt\, dt\,.$$

If we extend the definitions of α_n and β_n to negative n, we can symmetrize the above identity. For if $n \geq 0$, then

$$\alpha_{-n} = 2\int_0^1 f(t)\cos 2\pi(-n)t\, dt = \alpha_n\,,$$
$$\beta_{-n} = 2\int_0^1 f(t)\sin 2\pi(-n)t\, dt = -\beta_n.$$

Hence

$$\sum_{n=-\mathrm{N}}^{N}(\alpha_n + i\beta_n) = \alpha_0 + 2\sum_{n=1}^{N}\alpha_n\,.$$

But

$$\begin{aligned}\alpha_n + i\beta_n &= 2\int_0^1 f(t)(\cos 2\pi nt + i\sin 2\pi nt)\, dt\\ &= 2\int_0^1 f(t)\exp(2\pi int)\, dt\,.\end{aligned}$$

Hence on summing from $-N$ to N, we have

$$\sum_{n=-N}^{N}(\alpha_n + i\beta_n) = 2\sum_{r=-N}^{N}\int_0^1 f(t)\exp(2\pi irt)\, dt\,.$$

It follows that

$$\frac{\alpha_0}{2} + \sum_{n=1}^{N}\alpha_n = \sum_{r=-N}^{N}\int_0^1 f(t)\exp(2\pi irt)\, dt.$$

But the limit as $N \to \infty$ of the left-hand side is $\frac{f(0)+f(1)}{2}$ by equation (6.17), and we end up with the beautiful formula

$$\frac{f(0)+f(1)}{2} = \lim_{N\to\infty}\sum_{r=-N}^{N}\int_0^1 f(t)\exp 2\pi irt\, dt\,.$$

Next, consider our function on the interval $[j, j+1]$. Then just as for the $[0,1]$ Fourier theorem, we have

$$\frac{f(j)+f(j+1)}{2} = \lim_{N\to\infty}\sum_{r=-N}^{N}\int_j^{j+1} f(t)\exp\,(2\pi irt)\, dt. \tag{6.18}$$

So we consider $f(x) = \exp\left(\frac{2\pi ix^2}{n}\right)$ on $[0,1],[1,2],\ldots,[n-2,n-1]$ and sum (6.18) on j from 0 to $n-1$. The left-hand side is

$$\begin{aligned}&\frac{1}{2}(f(0)+f(1)+f(1)+f(2)+f(2)+f(3)+\cdots+f(n-1)+f(n))\\ &\quad = f(0)+f(1)+\cdots+f(n-1) \qquad (\text{since } f(0)=f(n))\\ &\quad = G_n\,,\end{aligned}$$

while the right-hand side is the unsightly mess

$$\lim_{N\to\infty} \sum_{r=-N}^{N} \int_0^n \exp\left(\frac{2\pi i t^2}{n} + 2\pi i r t\right) dt\,.$$

$t = nt', dt = ndt', \frac{t}{n} = t'.$

The change of variable $t = nt'$ changes the limit of integration, and the expression becomes

$$\begin{aligned}\lim_{N\to\infty} \sum_{r=-N}^{N} n \int_0^1 \exp\left(\frac{2\pi i n^2 t'^2}{n} + 2\pi i r n t'\right) dt' \\ = \lim_{N\to\infty} \sum_{r=-N}^{N} n \int_0^1 \exp\left(2\pi i n\left(t'^2 + r t'\right)\right) dt'\,.\end{aligned}$$

Dropping the $'$ decoration, this becomes

$$G_n = n \lim_{N\to\infty} \sum_{r=-N}^{N} \int_0^1 \exp\left(2\pi i n\left(t^2 + r n t\right)\right) dt\,. \tag{6.19}$$

If you've hung on so far, keep going. The rest will be worth the effort.

So far, so good. Now we operate on $\int_{-\infty}^{\infty} \exp(2\pi i x^2)\, dx$. Call its value T. This integral is simply $2\int_0^{\infty} \exp(2\pi i x^2)\, dx$. However, we symmetrize around zero to fit the earlier discussion. Then

$$\int_{-\infty}^{\infty} \exp(2\pi i x^2)\, dx = \lim_{N\to\infty} \int_{-N}^{N} \exp(2\pi i x^2)\, dx\,.$$

Change the variable by setting $x = \sqrt{n}y$. Then

$$\begin{aligned}T = \int_{\infty}^{\infty} \exp(2\pi i x^2) &= \lim_{N\to\infty} \sqrt{n} \int_{-\sqrt{n}N}^{\sqrt{n}N} \exp(2\pi i n y^2)\, dy \\ &= \sqrt{n} \lim_{N\to\infty} \int_{-N}^{N} \exp(2\pi i n y^2)\, dy,\end{aligned} \tag{6.20}$$

since replacing $\sqrt{n}N$ by N doesn't change the limit. (We already know that it exists!)

To keep notation down, let $h(y) = \exp(2\pi i n y^2)$. Now the idea (due to Dirichlet) is to compute the limit in two ways, breaking up the interval of integration at integers:

$$\int_{-N}^{N} h(y)\, dy = \int_{-N}^{-N+1} h(y)\, dy + \int_{-N+1}^{-N+2} h(y)\, dy + \cdots + \int_{N-1}^{N} h(y)\, dy, \tag{6.21}$$

and then by half-integers, considering the partial sum:

$$\int_{-N-\frac{1}{2}}^{N+\frac{1}{2}} h(y)\, dy = \int_{-N-\frac{1}{2}}^{-N+\frac{1}{2}} h(y)\, dy + \int_{-N+\frac{1}{2}}^{-N+\frac{3}{2}} h(y)\, dy + \cdots + \int_{N-\frac{1}{2}}^{N+\frac{1}{2}} h(y)\, dy. \tag{6.22}$$

Changing the integration interval to $[0, 1]$ in 6.20 gives

$$T = \sqrt{n} \lim_{N\to\infty} \sum_{k=-N}^{N} \int_0^1 \exp\left(2\pi i n\left(x^2 + 2kx\right)\right) dx. \tag{6.23}$$

On the sum by half-integers, change the variable again, referring everything to $[0, 1]$. A typical term in the sum is

$$\int_{k-\frac{1}{2}}^{k+\frac{1}{2}} \exp\left(2\pi i n y^2\right)\, dy.$$

The substitution $y = k - \frac{1}{2} + x$ transforms the integral to

$$\begin{aligned}
&\int_0^1 \exp\left(2\pi i n\left(k - \frac{1}{2} + x\right)^2\right) dx \\
&= \int_0^1 \exp\left(2\pi i n\left(k^2 - k + \frac{1}{4} + (2k-1)\,x + x^2\right)\right) dx \\
&= \exp\left(\frac{2\pi i n}{4}\right) \int_0^1 \exp\left(2\pi i n(x^2 + (2k-1)x\right)\, dx\,.
\end{aligned}$$

However, $\exp\left(\frac{2\pi i n}{4}\right) = i^n$. Hence equation (6.22) becomes

$$T = \sqrt{n}\, i^n \lim_{N\to\infty} \sum_{k=-N}^{N} \int_0^1 \exp\left(2\pi i n\left(x^2 + (2k-1)x\right)\right)\, dx\,. \tag{6.24}$$

Let us now examine (6.23) and (6.24) (repeated here for reference):

$$T = \sqrt{n} \lim_{N\to\infty} \sum_{k=-N}^{N} \int_0^1 \exp\left(2\pi i n\left(x^2 + 2kx\right)\right)\, dx\,, \tag{6.23}$$

$$T = \sqrt{n}\, i^n \lim_{N\to\infty} \sum_{k=-N}^{N} \int_0^1 \exp\left(2\pi i n\left(x^2 + (2k-1)x\right)\right)\, dx\,. \tag{6.24}$$

In (6.23), we have a sum on k from $-N$ to N with $2k$ appearing under the integral, and in (6.24) we have the sum over the odd integers $2k - 1$. In other words, we have summed $\int_0^1 \exp(2\pi i n(x^2 + sx))dx$ for *all* s from $-2N$ to $2N$.

That is to say, dividing (6.23) by $\sqrt{n}$ and (6.24) by $\sqrt{n}\, i^n$ and adding gives (replacing $2N$ by N, of course)

$$\frac{T}{\sqrt{n}}\left(1 + i^{-n}\right) = \lim_{N\to\infty} \sum_{s=-N}^{N} \int_0^1 \exp\left(2\pi i n\left(x^2 + sx\right)\right)\, dx\,.$$

Comparing this with equation (6.19), we have the remarkable result, and the aim of the entire investigation,

$$\frac{T}{\sqrt{n}}\left(1 + i^{-n}\right) = \frac{G_n}{n}\,.$$

This gives

$$G_n = \sqrt{n}\, T\left(1 + i^{-n}\right)\,. \tag{6.25}$$

The magic isn't over yet. In this relation, let $n = 1$. Since $G_1 = 1$ (and $\sqrt{1} = 1$), we have

$$T = \frac{1}{1 - i} = \frac{1 + i}{2}\,.$$

That is,

$$\int_{-\infty}^{\infty} \exp\left(2\pi i x^2\right)\, dx = \frac{1}{2} + \frac{1}{2}i\,.$$

Equating the real and imaginary parts gives

$$\int_{-\infty}^{\infty} \cos\left(2\pi x^2\right)\, dx = \frac{1}{2}$$

and

$$\int_{-\infty}^{\infty} \sin\left(2\pi x^2\right)\, dx = \frac{1}{2}\,.$$

Let $u = x^2$, so that $dx = \frac{du}{2\sqrt{u}}$.

Changing variables gives

$$\int_0^{\infty} \frac{\cos x}{\sqrt{x}}\, dx = \sqrt{\frac{\pi}{2}} \tag{6.26}$$

and

$$\int_0^{\infty} \frac{\sin x}{\sqrt{x}}\, dx = \sqrt{\frac{\pi}{2}}\,. \tag{6.27}$$

However, knowing

$$T = \frac{1}{2} + \frac{1}{2}i$$

gives (at last) the value of the Gauss sum G_n:

Theorem 6.14 (The value of the Gauss sum). *The Gauss sum*

$$G_n = \sqrt{n}\,\frac{\left(1 + i^{-n}\right)(1 + i)}{2} \tag{6.28}$$

can be simplified depending on the value of n modulo 4:

(i) *If* $n \equiv 0 \mod 4$, *then*

$$G_n = \sqrt{n}\,\frac{(1+1)(1+i)}{2} = \sqrt{n}\,(1+i)\,.$$

(ii) *If* $n \equiv 1 \mod 4$, *then*

$$G_n = \sqrt{n}\,\frac{\left(1 + i^{-1}\right)(1 + i)}{2} = \sqrt{n}\,.$$

(iii) *If* $n \equiv 3 \mod 4$, *then*

$$G_n = \sqrt{n}\,\frac{\left(1 + i^{-3}\right)(1 + i)}{2} = i\sqrt{n}\,.$$

(iv) *If* $n \equiv 2 \mod 4$, *then*

$$G_n = \sqrt{n}\,\frac{\left(1 + i^{-2}\right)(1 + i)}{2} = 0\,.$$

In particular, if n is a prime p, we have the famous result of Gauss that we cited earlier in Section 2.2:

Corollary 6.15. *If* $\zeta = \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right)$, *we have*

$$1 + \zeta + \zeta^4 + \zeta^9 + \cdots + \zeta^{(p-1)^2} = \begin{cases} \sqrt{p} & \text{if } p \equiv 1(4), \\ i\sqrt{p} & \text{if } p \equiv 3(4). \end{cases}$$

Exercises

6.15 Show that if $f(x)$is integrable on $[a, N)$ for every $N > a$ and if $f(x)$ is positive and monotonically decreasing to 0 as $x \to \infty$, then $\int_a^\infty f(x)\cos x\,dx$ exists.

6.5 On $\int_0^\infty \frac{\sin t}{t}\,dt$ and $\sum_{k=1}^\infty \frac{\sin kx}{k}$

We have seen that a differentiable function defined on $[-\pi, \pi]$ may be expressed as a trigonometric series (its Fourier series). The proof depended on our favorite trigonometric identity ((6.30) below) and a lemma of Riemann's (Lemma 6.2). This technique was already used in the proof of the identity $\frac{\pi^2}{6} = 1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots$ that we gave in Section 6.1. And in the preceding section, using a somewhat more involved argument, we saw that Fourier series gave the value of the Gauss sum and the value of the integrals

$$\int_0^\infty \frac{\cos x}{\sqrt{x}}\,dx \quad \text{and} \quad \int_0^\infty \frac{\sin x}{\sqrt{x}}\,dx.$$

The use of trigonometric series can also be used to evaluate $\int_0^\infty \frac{\sin x}{x}\,dx$, and that is what we take up here to close out the chapter. The proof is an elegant application of all the methods developed in this chapter, and it shows simultaneously that for $x \in (0, \pi]$,

$$\frac{\pi - x}{2} = \sin x + \frac{\sin 2x}{2} + \frac{\sin 3x}{3} + \cdots \tag{6.29}$$

and

$$\int_0^\infty \frac{\sin x}{x}\,dx = \frac{\pi}{2}.$$

Of course, the infinite series (6.29) is, by Theorem 6.10, the Fourier series of $\frac{\pi - x}{2}$ made odd on $[-\pi, \pi]$. However, we shall not assume that fact. We will use a simple case of Riemann's lemma and the fact that $\int_0^\infty \frac{\sin x}{x}\,dx$ exists. The existence of $\int_0^\infty \frac{\sin x}{x}\,dx$ is a special case of Lemma 6.11, proved in the previous section. The proof then goes as follows ...

Lemma 6.11 says that $\int_0^\infty f(x)\sin x\,dx$ exists when $f(x)$ is positive and monotonically decreasing to zero as $x \to \infty$.

Beginning (of course) with the identity

$$\frac{1}{2} + \cos t + \cos 2t + \cdots + \cos nt = \frac{\sin(n + \frac{1}{2})t}{2\sin\frac{t}{2}}, \tag{6.30}$$

we integrate both sides from 0 to x for $0 < x \le \pi$. That gives

$$\frac{x}{2} + \sin x + \frac{\sin 2x}{2} + \frac{\sin 3x}{3} + \cdots + \frac{\sin nx}{n} = \int_0^x \frac{\sin(n+\frac{1}{2})t}{2\sin\frac{t}{2}}\,dt\,. \qquad (6.31)$$

Think of x as fixed on $(0,\pi]$. Write

$$\int_0^x \frac{\sin\left(n+\frac{1}{2}\right)t}{2\sin\frac{t}{2}}\,dt$$
$$= -\int_0^x \left(\frac{1}{t} - \frac{1}{2\sin\frac{t}{2}}\right)\sin\left(n+\frac{1}{2}\right)t\,dt + \int_0^x \frac{\sin\left(n+\frac{1}{2}\right)t}{t}\,dt\,.$$

For fixed x, the first integral goes to zero as $n \to \infty$ by Riemann's lemma. We need to know, of course, that

$$\frac{1}{t} - \frac{1}{2\sin\frac{t}{2}}$$

is well behaved at the origin, a point we established in Section 6.2 with a double application of l'Hospital. As for the second integral, we change the variable by writing

$$\left(n+\frac{1}{2}\right)t = \xi\,.$$

Then

$$\int_0^x \frac{\sin(n+\frac{1}{2})t}{t}dt = \int_0^{(n+\frac{1}{2})x} \frac{\sin\xi}{\xi}d\xi\,.$$

But this integral approaches $\int_0^\infty \frac{\sin\xi}{\xi}\,d\xi$ as $n \to \infty$, since $x \neq 0$. It follows that (6.31) has a limit as $n \to \infty$, and that limit is $\int_0^\infty \frac{\sin t}{t}\,dt$. In other words,

$$\frac{x}{2} + \sum_{k=1}^{\infty} \frac{\sin kx}{k} = \int_0^\infty \frac{\sin t}{t}\,dt \quad \text{for } 0 < x \le \pi\,.$$

And now (*more* magic) ... let $x = \pi$ (note that $x = 0$ is forbidden). We obtain the following lovely result.

Theorem 6.16.

$$\frac{\pi}{2} = \int_0^\infty \frac{\sin t}{t}\,dt\,.$$

And there's even more: On substituting back, we have

$$\frac{\pi - x}{2} = \sum_{k=1}^{\infty} \frac{\sin kx}{k} \quad \text{for } 0 < x \le \pi\,.$$

We can't resist then putting $x = \pi/2$ to obtain (again)

$$\frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \cdots\,.$$

We met this identity before—equation (6.15).

Thus the formal analogy between the "continuous" sum $\int_0^\infty \frac{\sin t}{t}\,dt$ and the "discrete" sum $\sum_{k=1}^\infty \frac{\sin kx}{k}$ seems more than merely formal.

Epilogue

Looking Back

This text involves immersing oneself in two faces of the discipline:

(i) working on hard problems, accompanied by reflection on the habits of mind you use or develop during this process;

(ii) studying the work of others, trying to figure out how they might have been thinking when developing their methods and results.

There are many wonderful texts that address both faces of this Janus head, but the 1972 course by Ken Ireland was my first encounter with a design that integrates these two ways of doing mathematics in what might seem like a reversal of the customary order—what I called in the preface "experience before formality."

Experience before formality became a foundation not only for my own mathematical work (where it is the typical way new results emerge), but also for my approach to *teaching* mathematics. It is quite difficult to explain how effective this teaching practice is to someone who hasn't experienced it as a student, but you have just been through a text that is based on this principle. Take some time to reflect on what you have done. Think about how it would play out in your future work in mathematics. Think about how it would play out in your teaching. This is beginning to sound preachy, so I'll make only one suggestion: Just try it.

Another instance of why experience precedes formality ....

One way to think about the results developed in these chapters is a theme I mentioned in the preface: in high school, and, to some extent, in undergraduate courses, many results of fundamental importance in the history of mathematics are stated without proof. There are good reasons for this: Many of the proofs are quite technical (as you have just seen) and involve background that may not be current (or may not exist) for some students. Developing the prerequisite knowledge would take more time than a syllabus allows. But the proof of a result does more than establish a fact; it gives you a sense of why the fact was of interest to mathematicians in the first place, and it helps you to make teaching decisions about what to emphasize, what examples to use, and where the result fits into the overall mathematical landscape.

K. Ireland and A. Cuoco, *Excursions in Number Theory, Algebra, and Analysis*,
Readings in Mathematics, https://doi.org/10.1007/978-3-031-13017-5_0

You can't construct a regular heptagon with straightedge and compass; the fundamental theorem of algebra requires the odd-degree root theorem; e and π are transcendental; $\frac{\pi^2}{6} = \sum_{k=1}^{\infty} \frac{1}{k^2}$; every prime congruent to 1 mod 4 can be written as the sum of two squares; there is a formula for the number of representations of an integer as a sum of two squares .... All these and more appear somewhere in high-school and college programs, and one of the major goals of this book is to "mop up"—to fill in the details of why these things are true.

Many of the proofs of these central results that we present here have been revisited and polished for generations, so you are seeing a kind of finished product. But the elegance of the proofs are the capstones for long periods (sometimes years or decades) of intense work. Following a long proof often gives you the feeling of "I get it, but how would someone come up with that?"

A good example appears in Chapter 5, where the proofs of the main results follow a recognizable rhythm, each starting with a function we call the "Hermite beast." How in the world did someone come up with these? That's where some of the Dialing In problems come in. They provide ideas about, for example, how one might conceive of an expression that is a positive integer less than 1 and hence can't exist, negating the assumption that the number in question is rational or algebraic.

See, for example, Dialing In problems 114, 115, and 116.

Looking Forward

What next? I have some suggestions.

(i) **Join a professional organization.** These make available many useful resources for mathematical work:

(a) The American Mathematical Society (AMS.org) is aimed at the mathematics research community.

(b) The Mathematical Association of America (MAA.org) serves the mathematics teaching community, mainly undergraduate and high school.

(c) The National Council of Teachers of Mathematics (NCTM.org) is primarily for PK–12 mathematics teachers.

NCTM features a mix of pedagogy and mathematical activities.

Each of these organizations supports local, regional, and national conferences. Membership will keep you informed of when and where these take place, and, with a little careful curating, you will find in them some wonderful mathematics and very useful ideas about teaching.

(ii) **Present your work to the field.** Getting ideas out there is becoming easier all the time. Outlets include widely read blogs (each of the organizations above has at least one), journals (electronic and paper), presenting at conferences (like the ones mentioned above), and good old paper texts (like this one). Publishing or presenting serves many purposes, but one that is often overlooked is that it helps *you* clarify ideas and make new connections for yourself. Many of the problems and exercises in this book make ideal loci for a journal article or a blog post.

Just suggestions: Exercise 2.40, and Dialing In problems 22, 43, 95, 126, all make launchpads for interesting MAA, AMS, or NCTM papers.

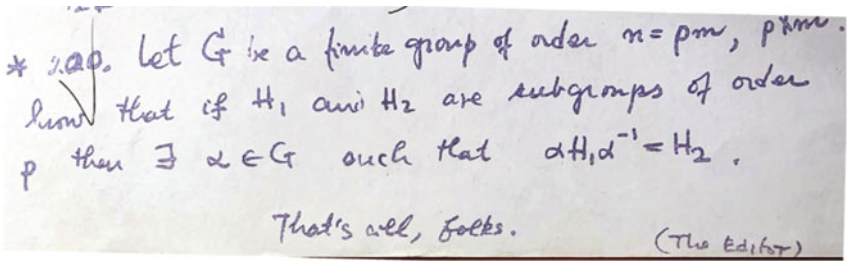
(iii) **Join a community of mathematical practice.** A mathematical investigation usually begins in solitude—you read or hear about something intriguing and you dive in, all by yourself, doodling, thinking, experimenting, and trying things. But when the insight comes, it really helps to brainstorm with friends and colleagues. Many teachers have formed informal study groups that meet regularly to work on specific topics. Many departments sponsor regular seminars. And there are national sites of mathematical practice. Two in particular use the "experience first" design:

(a) The *Park City Mathematics Institute* [82] offers summer programs for all parts of our community (mathematics research, undergraduate teaching, precollege teaching . . .).

(b) *PROMYS* at Boston University [81] is a longstanding program for advanced secondary-school students and practicing secondary-school teachers. The program is explicitly designed to give participants the experience of working as a mathematician.

These are just examples. The point is that staying connected with others who have similar mathematical dispositions greatly enhances your mathematical experience.

The 1972 version of the last Dialing In problem ended with a quotation from the *Looney Tunes* cartoons:



True to form, that was a joke; I sincerely hope that you keep doing and teaching mathematics in the style and spirit of this book.

—Al Cuoco
May 29, 2022

Bibliography

[1] Emil Artin. *Galois Theory*. Edited and supplemented with a section on applications by Arthur N. Milgram. Second edition, with additions and revisions. Fifth reprinting. Notre Dame Mathematical Lectures, No. 2. University of Notre Dame Press, South Bend, Ind., 1959.

[2] Emil Artin and Otto Schreier. Algebraische Konstruktion reeller Körper. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, 1927.

[3] George Bachman. *Introduction to p-adic Numbers and Valuation Theory*. Academic Press, New York–London, 1964.

[4] Jacob Barshay. *Topics in Ring Theory*. Mathematics Lecture Note Series. W. A. Benjamin, Inc., New York, 1969.

[5] Robert G. Bartle. *The Elements of Real Analysis*. John Wiley & Sons, New York-London-Sydney, second edition, 1976.

[6] Jörg Bewersdorff. *Galois Theory for Beginners: A Historical Perspective*, second edition. Translated from the German by David Kramer. American Mathematical Society, 2021.

[7] Ben Blum-Smith and Japheth Wood. Chords of an ellipse, Lucas polynomials, and cubic equations. *Amer. Math. Monthly*, 127(8):688–705, 2020.

[8] Zenon I. Borevich and Igor R. Shafarevich. *Number Theory*. Pure & Applied Mathematics. Academic Press, New York, NY, 1966.

[9] Nicolas Bourbaki. *Elements of Mathematics. Theory of Sets*. Translated from the French. Hermann, Publishers in Arts and Science, Paris; Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1968.

[10] W. G. Chinn and N. E. Steenrod. *First Concepts of Topology. The Geometry of Mappings of Segments, Curves, Circles, and Disks*. New Mathematical Library, Vol. 18. Random House, New York; The L. W. Singer Co., Syracuse, N.Y., 1966.

[11] S. Chowla. *The Riemann Hypothesis and Hilbert's Tenth Problem*. Mathematics and Its Applications, Vol. 4. Gordon and Breach Science Publishers, New York-London-Paris, 1965.

K. Ireland and A. Cuoco, *Excursions in Number Theory, Algebra, and Analysis*,
Readings in Mathematics, https://doi.org/10.1007/978-3-031-13017-5_0

[12] Keith Conrad. https://kconrad.math.uconn.edu/blurbs/galoistheory/cyclotomic.pdf.

[13] R. Courant. *Differential and Integral Calculus. Vol. II*. Wiley Classics Library. John Wiley & Sons, Inc., New York, 1988. Translated from the German by E. J. McShane, Reprint of the 1936 original, A Wiley-Interscience Publication.

[14] R. Courant and D. Hilbert. *Methods of Mathematical Physics. Vol. II: Partial Differential Equations*. (Vol. II by R. Courant.). Interscience Publishers (a division of John Wiley & Sons), New York-Lon don, 1962.

[15] Karl-Dieter Crisman. Number theory: in context and interactive. http://math.gordon.edu/ntic/ntic/ntic.html. Chapter 17.

[16] Al Cuoco. Constructing the complex numbers. *International Journal of Computers for Mathematical Learning 2*, pages 155–186, 1997.

[17] Al Cuoco. Searching for Möbius. *The College Mathematics Journal*, 37(2):137–142, 2006.

[18] Al Cuoco and Paul Goldenberg. Computational thinking in mathematics and computer science: what programming does to your head. *Journal of Humanistic Mathematics*, 11:346–363, 2021.

[19] Al Cuoco and Joseph J. Rotman. *Learning Modern Algebra*. MAA Textbooks. Mathematical Association of America, Washington, DC, 2013. From early attempts to prove Fermat's last theorem.

[20] Albert Cuoco, Kevin Waterman, Bowen Kerins, Elena Kaczorowski, and Michelle Manes. *Linear Algebra and Geometry*, volume 46 of *AMS/MAA Textbooks*. Providence, RI: MAA Press/American Mathematical Society (AMS), 2019.

[21] H. Davenport. *The Higher Arithmetic*. Cambridge University Press, Cambridge, eighth edition, 2008. An introduction to the theory of numbers, With editing and additional material by James H. Davenport.

[22] J. Dieudonné. *Foundations of Modern Analysis*. Pure and Applied Mathematics, Vol. X. Academic Press, New York-London, 1960.

[23] Jean Dieudonné. *Calcul infinitésimal*. Hermann, Paris, 1968.

[24] Harold M. Edwards. *Fermat's Last Theorem*, volume 50 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1996. A genetic introduction to algebraic number theory, Corrected reprint of the 1977 original.

[25] Education Development Center, Inc. *CME Project: Geometry, Algebra 2, Algebra 1, Precalculus*. Savvas Learning Company LLC, 2009.

[26] Leonard Euler. *Elements of Algebra*. Cambridge Library Collection. Cambridge University Press, Cambridge, third edition, 2009. Translated from the French by John Hewlett, with the notes of M. Bernoulli and the additions of M. de le Grange, With an essay "A memoir of the life and character of Euler" by Francis Horner.

[27] Pierre de Fermat. *Œuvres de Fermat*. Tome deuxième: Correspondance. Gauthier-Villars et fils, Paris, 1894.

[28] Lisl Gaal. *Classical Galois Theory*. AMS Chelsea Publishing, Providence, RI, 1998. With examples, Reprint of the third (1979) edition.

[29] Carl Friedrich Gauss. *Disquisitiones Arithmeticae*. Yale University Press, 1966. translated by Arthur A, Clarke.

[30] Daniel P. Giesy. Still another elementary proof that $\sum 1/k^2 = n^2/6$. *Math. Mag.*, 45(3):148–149, 1972.

[31] Casper Goffman. *Introduction to Real Analysis*. Harper & Row, Publishers, New York-London, 1966.

[32] Daniel Gorenstein. *Finite Groups*. Harper & Row, Publishers, New York-London, 1968.

[33] Fernando Q. Gouvêa. *p-adic Numbers*. Universitext. Springer-Verlag, Berlin, second edition, 1997. An introduction.

[34] Marvin J. Greenberg. *Lectures on Forms in Many Variables*. W. A. Benjamin, Inc., New York-Amsterdam, 1969.

[35] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers*. The Clarendon Press, Oxford University Press, New York, fifth edition, 1979.

[36] I. N. Herstein. *Topics in Algebra*. Blaisdell Publishing Co. Ginn and Co. New York-Toronto-London, 1964.

[37] I. N. Herstein. *Noncommutative Rings*. The Carus Mathematical Monographs, No. 15. Published by The Mathematical Association of America; distributed by John Wiley & Sons, Inc., New York, 1968.

[38] Einar Hille. Gelfond's solution of Hilbert's seventh problem. *Amer. Math. Monthly*, 49:654–661, 1942.

[39] Einar Hille. *Analytic Function Theory. Vol. 1*. Introduction to Higher Mathematics. Ginn and Company, Boston, 1959.

[40] A. Hurwitz. Ueber die composition der quadratischen formen von belibig vielen variablen. *Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse*, 1898:309–316, 1898.

[41] Kenneth Ireland and Michael Rosen. *A Classical Introduction to Modern Number Theory*, volume 84 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1990.

[42] James P. Jans. *Rings and Homology*. Holt, Rinehart and Winston, New York, 1964.

[43] Irving Kaplansky. *Commutative Rings*. The University of Chicago Press, Chicago, Ill.-London, revised edition, 1974.

[44] D. K. Kazarinoff. Classroom notes: a simple derivation of the Leibnitz–Gregory series for $\pi/4$. *Amer. Math. Monthly*, 62(10):726–727, 1955.

[45] Neal Koblitz. *p-adic Numbers*, *p-adic Analysis, and Zeta-Functions*, volume 58 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1984.

[46] Edmund Landau. *Differential and Integral Calculus*. AMS Chelsea Pub-

lishing, Providence, RI, third edition, 2001. Translated from the German by Melvin Hausner and Martin Davis.

[47] Serge Lang. *Cyclotomic Fields I and II*, volume 121 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1990. With an appendix by Karl Rubin.

[48] Serge Lang. *Algebraic Number Theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1994.

[49] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[50] Ian D. Macdonald. *The Theory of Groups*. Robert E. Krieger Publishing Co., Inc., Malabar, FL, 1988. Reprint of the 1968 original.

[51] Henry B. Mann. *Introduction to Algebraic Number Theory*. The Ohio State University Press, Columbus, Ohio, 1955. With a chapter by Marshall Hall, Jr.

[52] MathWorks. https://www.mathworks.com/.

[53] Ryota Matsuura. *A Friendly Introduction to Abstract Algebra*, AMS/MAA Textbooks 72. American Mathematical Society, 2022.

[54] Neal H. McCoy. *The Theory of Rings*. The Macmillan Co., New York; Collier-Macmillan Ltd., London, 1964.

[55] James H. McKay. Another proof of Cauchy's group theorem. *Amer. Math. Monthly*, 66:119, 1959.

[56] Van Morrison. https://en.wikipedia.org/wiki/It%27s_Too_Late_to_Stop_Now.

[57] George D. Mostow, Joseph H. Sampson, and Jean-Pierre Meyer. *Fundamental Structures of Algebra*. McGraw-Hill Book Co., Inc., New York-Toronto, Ont.-London, 1963.

[58] M. Pavaman Murthy, K. G. Ramanathan, C. S. Seshadri, U. Shukla, and R. Sridharan. *Galois Theory*, volume 3 of *Mathematical Pamphlets*. Tata Institute of Fundamental Research, Bombay, 1965.

[59] Trygve Nagell. *Introduction to Number Theory*. Chelsea Publishing Co., New York, second edition, 1964.

[60] Ivan Niven. *Irrational Numbers*, volume 11. Mathematical Association of America, 1 edition, 1985.

[61] Ivan Niven and Herbert S. Zuckerman. *An Introduction to the Theory of Numbers*. John Wiley & Sons, New York-Chichester-Brisbane, fourth edition, 1980.

[62] Albrecht Pfister. Zur Darstellung definiter Funktionen als Summe von Quadraten. *Invent. Math.*, 4:229–237, 1967.

[63] Harry Pollard. *The Theory of Algebraic Numbers*. Carus Monograph Series, no. 9. The Mathematical Association of America, Buffalo, NY, 1950.

[64] M. M. Postnikov. *Foundations of Galois Theory*. Dover Publications, Inc., Mineola, NY, 2004. With a foreword by P. J. Hilton, Reprint of

the 1962 edition, Translated from the 1960 Russian original by Ann Swinfen.

[65] Hans Rademacher. *Lectures on Elementary Number Theory*. Robert E. Krieger Publishing Co., Huntington, N.Y., 1977. Reprint of the 1964 original.

[66] Paulo Ribenboim. *13 Lectures on Fermat's Last Theorem*. Springer-Verlag, New York-Heidelberg, 1979.

[67] Werner Rogosinski. *Fourier Series*. Chelsea Publishing Company, New York, N. Y., 1950.

[68] Maxwell Rosenlicht. *Introduction to Analysis*. Scott, Foresman and Co., Glenview, Ill., 1968.

[69] Joseph Rotman. *Galois Theory*. Universitext. Springer-Verlag, New York, second edition, 1998.

[70] Joseph J. Rotman. *An Introduction to the Theory of Groups*, volume 148 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, fourth edition, 1995.

[71] H. L. Royden. *Real Analysis*. The Macmillan Co., New York; Collier-Macmillan Ltd., London, 1963.

[72] Walter Rudin. *Real and Complex Analysis*. McGraw-Hill Book Co., New York–Toronto, Ontario–London, 1966.

[73] Pierre Samuel. *Algebraic Theory of Numbers*. (Translated from the French by Allan J. Silberger). Boston, Mass.: Houghton Mifflin Co., 1970.

[74] Giovanni Sansone and Johan Gerretsen. *Lectures on the Theory of Functions of a Complex Variable. I. Holomorphic Functions*. P. Noordhoff, Groningen, 1960.

[75] Carl Ludwig Siegel. *Transcendental Numbers*. Annals of Mathematics Studies, no. 16. Princeton University Press, Princeton, N. J., 1949.

[76] Pierre Samuel. *Algebraic Theory of Numbers*. Translated from the French by Allan J. Silberger. Boston, Mass.: Houghton Mifflin Co., 1970.

[77] Joseph H Silverman. *A Friendly Introduction to Number Theory*. Pearson, Upper Saddle River, fourth edition, 2013.

[78] Richard A. Silverman. *Introductory Complex Analysis*. Prentice-Hall, Inc., Englewood Cliffs, N.J., 1967. Based, in part, on material by A. I. Markushevich.

[79] Harold M. Stark. *An Introduction to Number Theory*. MIT Press, Cambridge, Mass.-London, 1978.

[80] Jiro Suzuki. On coefficients of cyclotomic polynomials. *Proc. Japan Acad. Ser. A Math. Sci.*, 63(7):279–280, 1987.

[81] PROMYS for Teachers. https://promys.org/pft.

[82] The Park City Teacher Leadership Program. https://www.ias.edu/pcmi/programs/pcmi-2021-teacher-leadership-program.

[83] E. C. Titchmarsh. *The Theory of the Riemann Zeta-Function*. The Clarendon Press, Oxford University Press, New York, second edition, 1986. Edited and with a preface by D. R. Heath-Brown.

[84] Georgi P. Tolstov. *Fourier Series*. Translated from the Russian by Richard A. Silverman. Prentice-Hall, Inc., Englewood Cliffs, N.J., 1962.

[85] B. L. van der Waerden. *Modern Algebra. Vol. II*. Frederick Ungar Publishing Co., New York, N. Y., 1949. Translated from the second revised German edition by Fred Blum, With revisions and additions by the author.

[86] Lawrence C. Washington. *Introduction to Cyclotomic Fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1997.

[87] Hermann Weyl. A half-century of mathematics. *Amer. Math. Monthly*, 58:523–553, 1951.

[88] Helmut Wielandt. *Finite Permutation Groups*. Translated from the German by R. Bercov. Academic Press, New York-London, 1964.

[89] Oscar Zariski and Pierre Samuel. *Commutative Algebra. Vol. 1*. Graduate Texts in Mathematics, No. 28. Springer-Verlag, New York-Heidelberg-Berlin, 1975. With the cooperation of I. S. Cohen, Corrected reprinting of the 1958 edition.

Index

K. Ireland and A. Cuoco, *Excursions in Number Theory, Algebra, and Analysis*,
Readings in Mathematics, https://doi.org/10.1007/978-3-031-13017-5