

Insolvability of the Quintic

An unofficial sequel to [An Inquiry-Based Approach to Abstract Algebra](#) by Dana C. Ernst

Joshua Wiscons
California State University, Sacramento

Spring 2019

© 2019 Joshua Wiscons. Some Rights Reserved.

The most up-to-date version of these notes on can be found on GitHub:

<https://github.com/jwiscons/IBL-InsolvabilityOfQuintic>

This work is licensed under the Creative Commons Attribution-Share Alike 4.0 United States License. You may copy, distribute, display, and perform this copyrighted work, but only if you give credit to Joshua Wiscons, and all derivative works based upon it must be published under the Creative Commons Attribution-Share Alike 4.0 International License. Please attribute this work to Joshua Wiscons, Mathematics Faculty at California State University, Sacramento, joshua.wiscons@csus.edu. To view a copy of this license, visit

<https://creativecommons.org/licenses/by-sa/4.0/>

or send a letter to Creative Commons, 171 Second Street, Suite 300, San Francisco, California, 94105, USA.



This work is designed to extend [An Inquiry-Based Approach to Abstract Algebra](#) by Dana C. Ernst. The presentation of the material is heavily influenced by the book [Abstract Algebra: A Concrete Introduction](#) by Robert H. Redfield. Many thanks to both Dana and Bob! I am also indebted to every student in my Modern Algebra 2 class from Fall 2019 at California State University, Sacramento for taking part, willingly or otherwise, in this experiment—thanks to you all!

Contents

1	Introduction	3
1.1	Prerequisites	3
1.2	An Inquiry-Based Approach	3
1.3	Rules of the Game	5
1.4	Structure of the Notes	5
2	Solving polynomial equations and the main question	6
2.1	Solving polynomial equations with formulas	6
2.2	The main question(s)	8
3	Fields	9
3.1	Complex Numbers	9
3.1.1	Definition and first principles	9
3.1.2	Roots of unity	12
3.1.3	Roots of polynomials over \mathbb{R} and \mathbb{C}	13
3.2	An aside: the quaternions	13
3.3	Abstract fields	15
3.3.1	Definition	15
3.3.2	Some examples and non-examples	16
3.3.3	Basic properties	17
3.3.4	Another example	18
3.3.5	Subfields	18
3.3.6	Generating subfields	19
A	Hints	20

Chapter 1

Introduction

This course is a story. A repackaging of a famous story, spanning more-or-less 4000 years, about solving polynomial equations. I hope you like it. I also hope enjoy the beautiful sights along the way, many of which were a long time in the making and most of which are still being heavily researched to this day.

1.1 Prerequisites

A first course in abstract algebra, focusing on the basics of group theory, together with exposure to foundational topics like primes and divisibility, functions and relations, differential calculus, and linear algebra form the core prerequisites. Comfort with basic proof techniques, including induction, is also more-or-less required. The following two free and open-source books developed by [Dana C. Ernst](#) will serve you well if you need to review.

- [An Inquiry-Based Approach to Abstract Algebra](#)
- [An Introduction to Proof via Inquiry-Based Learning](#)

1.2 An Inquiry-Based Approach

This section of the introduction as well as those that follow are (only slightly) modified from the introduction of [An Inquiry-Based Approach to Abstract Algebra](#). The use of “I” below, does indeed refer to me, but mainly just because I also believe the words that [Dana](#) originally wrote.

In many courses, math or otherwise, you sit and listen to a lecture. These lectures may be polished and well-delivered. You may have often been lured into believing that the instructor has opened up your head and is pouring knowledge into it. I love lecturing, and I do believe there is value in it, but I also believe that in reality most students do not learn by simply listening. You must be active in the learning process. Likely, each of you have said to yourselves, “Hmmm, I understood this concept when the professor was going over it, but now that I am alone, I am lost.” In order to promote a more active

participation in your learning, we will incorporate ideas from an educational philosophy called inquiry-based learning (IBL).

Loosely speaking, IBL is a student-centered method of teaching mathematics that engages students in sense-making activities. Students are given tasks requiring them to solve problems, conjecture, experiment, explore, create, communicate. Rather than showing just facts or a clear, smooth path to a solution, the instructor guides and mentors students via well-crafted problems through an adventure in mathematical discovery. Effective IBL courses encourage deep engagement in rich mathematical activities and provide opportunities to collaborate with peers (either through class presentations or group-oriented work).

Perhaps this is sufficiently vague, but I believe that there are two essential elements to IBL. Students should as much as possible be responsible for:

- (1) Guiding the acquisition of knowledge, and
- (2) Validating the ideas presented. That is, students should not be looking to the instructor as the sole authority.

For additional information, check out [Dana's](#) blog post, [What the Heck is IBL?](#)

Much of the course will be devoted to students proving theorems on the board and a significant portion of your grade will be determined by the mathematics you produce. I use the word “produce” because I believe that the best way to learn mathematics is by doing mathematics. Someone cannot master a musical instrument or a martial art by simply watching, and in a similar fashion, you cannot master mathematics by simply watching; you must do mathematics!

Furthermore, it is important to understand that proving theorems is difficult and takes time. You should not expect to complete a single proof in 10 minutes. Sometimes, you might have to stare at the statement for an hour before even understanding how to get started.

In this course, everyone will be required to

- read and interact with course notes on your own;
- write up quality proofs to assigned problems;
- present proofs on the board to the rest of the class;
- participate in discussions centered around a student's presented proof;
- call upon your own prodigious mental faculties to respond in flexible, thoughtful, and creative ways to problems that may seem unfamiliar on first glance.

As the semester progresses, it should become clear to you what the expectations are. This will be new to many of you and there may be some growing pains associated with it.

Lastly, it is highly important to respect learning and to respect other people's ideas. Whether you disagree or agree, please praise and encourage your fellow classmates. Use ideas from others as a starting point rather than something to be judgmental about. Judgement is not the same as being judgmental. Helpfulness, encouragement, and compassion are highly valued.

1.3 Rules of the Game

You should *not* look to resources outside the context of this course for help. That is, you should not be consulting the Internet, other texts, other faculty, or students outside of our course. On the other hand, you may use each other, the course notes, me, and your own intuition.

However, there do exist some hints, collected in Appendix A. Everyone may use the hints, but they were included mostly to support those who need to miss a class and are not able to find a time to meet with their classmates (or me). If you use the hints, please keep in mind that (1) your own learning will significantly benefit from cognitive struggles (independently and with your peers), so don't turn to the hints too early; and (2) the hints are really just some possible ways to get started—they may very well not be the way that makes the most sense to you, so I encourage you to follow your own paths.

In this class, earnest failure outweighs counterfeit success; you need not feel pressure to hunt for solutions outside your own creative and intellectual reserves.

1.4 Structure of the Notes

As you read the notes, you will be required to digest the material in a meaningful way. It is your responsibility to read and understand new definitions and their related concepts. However, you will be supported in this sometimes difficult endeavor. In addition, you will be asked to complete problems aimed at solidifying your understanding of the material. Most importantly, you will be asked to make conjectures, produce counterexamples, and prove theorems.

The items labeled as **Definition** and **Example** (and occasionally **Fact**) are meant to be read and digested. However, the items labeled as **Problem**, **Lemma**, **Theorem**, and **Corollary** require action on your part. Items labeled as **Problem** are sort of a mixed bag. Some Problems are computational in nature and aimed at improving your understanding of a particular concept while others ask you to provide a counterexample for a statement if it is false or to provide a proof if the statement is true. Items with the **Lemma**, **Theorem**, and **Corollary** designation are mathematical facts and the intention is for you to produce a valid proof of the given statement. **Lemma's** are usually stepping stones to the next theorem, though they are often interesting in their own right. **Corollaries** are typically statements that follow quickly from a previous theorem. In general, you should expect corollaries to have very short proofs. However, that doesn't mean that you can't produce a more lengthy yet valid proof of a corollary.

It is important to point out that there are very few examples in the notes. This is intentional. One of the goals of the items labeled as **Problem** is for you to produce the examples.

Lastly, there are many situations where you will want to refer to an earlier definition, problem, lemma, theorem, or corollary. In this case, you should reference the statement by number (or by name if it has one).

Chapter 2

Solving polynomial equations and the main question

The story begins. Can you count all of the times in your career that you've had to find the zeros of a quadratic polynomial? What about a cubic polynomial? A quartic? Likely your answers are decreasing rapidly, and it's also likely that you have only solved cubic and quartic equations in very special situations. Why? Is it just that cubic and quartic equations are difficult to solve or could it be that some are impossible to "solve."

People have been investigating how to solve polynomial equations for about 4000 years. Let's get started.

Problem 2.1. Determine the roots (i.e. zeros) of each of the following. Try to use tools you've accumulated over the years, but you may well need a computer program (e.g. [WolframAlpha](#)) for some of them. For each problem, make a note about *how* you found the roots. Try for exact answers, but you can approximate if needed.

(1) $p(x) = x^2 - 5x + 6$

(5) $f(x) = x^3 - 5$

(2) $q(x) = (x - 3)^2 - 2$

(6) $g(x) = x^4 - 1$

(3) $r(x) = x^2 + x + 1$

(7) $a(x) = x^5 - 1$

(4) $s(x) = x^3 - 3x - 2$

(8) $b(x) = x^5 + 5x^4 - 5$

Problem 2.2. For each part of Problem 2.1, write down the "smallest" number system needed to express the roots of the given polynomial. Possible answers might be \mathbb{Z} (integers), \mathbb{Q} (rational numbers), \mathbb{Z} together with $\sqrt{3}$, \mathbb{Q} together with $\sqrt{-1}$ and $\sqrt[3]{5}$, etc.

2.1 Solving polynomial equations with formulas

Though you may have solved the first three parts of Problem 2.1 different ways, there was one tool that would have solved them all: the quadratic formula. It will be valuable to (re)discover why it's true.

First, let's slightly simplify things. Notice that α is a root of $ax^2 + bx + c$ if and only if α is a root of $x^2 + \frac{b}{a}x + \frac{c}{a}$ (assuming $a \neq 0$). This means that an arbitrary quadratic polynomial can always be converted to a quadratic polynomial whose leading coefficient is 1 and in such a way that they have the same roots. Thus, if we have a formula that finds the roots of so-called *monic* quadratic polynomials, we can actually use it to find the roots of *all* quadratic polynomials.

Definition 2.3. A polynomial whose leading coefficient is 1 is called a **monic** polynomial.

Now, let's (re)derive the quadratic formula for monic polynomials. Remember, we are (re)deriving it, so *please don't use the quadratic formula in your proof of the next theorem*.

Theorem 2.4. The roots of $p(x) = x^2 + bx + c$ are

$$\frac{-b \pm \sqrt{b^2 - 4c}}{2}.$$

Problem 2.5. Describe a number system, as small as possible, that is capable of expressing the roots of *any* quadratic polynomial whose *coefficients are all rational numbers*.

Well, that takes care of quadratic polynomials. What about finding the roots of cubic polynomials? Well, it turns out that there is indeed a cubic formula, though it's decidedly more complicated than the quadratic formula.

A method for deriving a cubic formula, due to [Scipione del Ferro](#) and [Tartaglia](#), was published in a book by [Cardano](#) in 1545. The starting point is to take a general cubic polynomial and first convert it to a monic polynomial (as we did above) and then convert it to a cubic of the form $x^3 + px + q$, always with the same roots as the original. Then, with work, one arrives at the following formula.

Fact 2.6. The roots of $p(x) = x^3 + px + q$ are

$$\alpha + \beta, \left(-\frac{1}{2} + \frac{\sqrt{-3}}{2}\right)\alpha + \left(-\frac{1}{2} - \frac{\sqrt{-3}}{2}\right)\beta, \left(-\frac{1}{2} - \frac{\sqrt{-3}}{2}\right)\alpha + \left(-\frac{1}{2} + \frac{\sqrt{-3}}{2}\right)\beta$$

where $\alpha = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$ and $\beta = \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$

Problem 2.7. Describe a number system, as small as possible, that is capable of expressing the roots of *any* cubic polynomial of the form $x^3 + px + q$ where $p, q \in \mathbb{Q}$.

Problem 2.8. Use Fact 2.6 to write out the roots of $p(x) = x^3 - 2x - 4$. Are any of the roots integers? Check your answer with [WolframAlpha](#). Does this expose any issues with using the formula?

For more details on solving cubic equations, you can use start with the [Wikipedia page about cubic functions](#). And now... quartic functions? Perhaps you have a guess.

Problem 2.9. Use the internet and/or library to determine if there is a quartic formula, i.e. a formula to find the roots of fourth-degree polynomials. If there is a quartic formula, who are some people that discovered methods to derive it and when did they discover their method?

2.2 The main question(s)

We now turn our attention to finding the roots of polynomials of degree five and higher. Well, what do you think: is there a quintic formula? Actually, there are two questions here: (1) what do we mean by “formula” (e.g. what symbols/functions can we use), and (2) whatever we mean by formula, is there one that works for *all* quintic polynomials?

You investigated two particular quintics in Problem 2.1—what did you find? Did you find exact expressions for the roots? If so, *how* were the roots expressed; that is, what symbols/functions were needed to write out the roots?

Let’s first try to tackle the “what do we mean by formula” question. Guided by the quadratic and cubic formulas, let’s agree that we are looking for a formula that expresses the roots of an arbitrary quintic polynomial, in terms of the coefficients of the polynomial, using just rational numbers together with the operations of addition, subtraction, multiplication, division, and the extraction of roots (square roots, cube roots,...). This leads to the following intuitive definition, that we will work to sharpen later.

Intuitive Definition 2.10. A polynomial is said to be **solvable by radicals** if every root of the polynomial can be expressed, in terms of the coefficients of the polynomial, using rational numbers together with the operations of addition, subtraction, multiplication, division, and $\sqrt[n]{}$ for any positive integer n .

Problem 2.11. Find the roots of $p(x) = x^4 - 2x^2 - 1$. Explain why $p(x)$ is solvable by radicals.

Problem 2.12. Explain why every quadratic polynomial is solvable by radicals.

Returning to quintic polynomials, our main question is as follows.

Main Question. Does there exist a “quintic formula” that expresses the roots of an arbitrary quintic polynomial, in terms of the coefficients of the polynomial, using just rational numbers together with the operations of addition, subtraction, multiplication, division, and the extraction of roots?

Well, if the answer is yes, then it must be that every quintic polynomial is solvable by radicals. *Spoiler Alert!* Our goal (for the rest of the book!) is to prove the following theorem, in a rather elegant way.

Main Theorem. Not every quintic polynomial is solvable by radicals.

Main Corollary. There is *no* “quintic formula” that expresses the roots of an arbitrary quintic polynomial, in terms of the coefficients of the polynomial, using just rational numbers together with the operations of addition, subtraction, multiplication, division, and the extraction of roots.

Boom!

Chapter 3

Fields

In Chapter 2, we explored problems about finding and expressing roots of polynomials, finally arriving at the goal of the course: proving that there are quintic polynomials that are *not* solvable by radicals. This chapter serves two main purposes. First, as we look at roots of polynomials and how they can be expressed, it will be convenient to have a common world (i.e. number system) in which they live. For us, this will be the complex numbers, denoted \mathbb{C} , which will be reviewed below. Our work with complex numbers will also supply the necessary language to properly talk about n^{th} -roots. Second, we are still in need of a proper definition of what it means for a polynomial to be “solvable by radicals”; this is where the chapter will finish. But the middle of the chapter is perhaps the most interesting. There, on the way to defining “solvable by radicals”, we will be led to abstract the structure of \mathbb{C} (and of \mathbb{Q} and \mathbb{R}), arriving at the definition of a *field*.

3.1 Complex Numbers

As mentioned above, we want to work in a world that contains all of the roots of all of the polynomials that we will be studying. Considering the roots of polynomials such as $x^2 + 1$, $x^2 - 2$, $x^2 - 3$, etc., we see that we need to include numbers like $\sqrt{-1}$, $\sqrt{2}$, $\sqrt{3}$, etc., so although there are smaller worlds one could choose, we will opt for the world containing both $\sqrt{-1}$ and \mathbb{R} , namely \mathbb{C} .

But before we proceed, note that $\sqrt{-1}$ is not really well defined. There are *two* solutions to $x^2 + 1$, so when we write $\sqrt{-1}$, we are all agreeing that we mean the same one.

Definition 3.1. Let i (or alternatively $\sqrt{-1}$) denote one particular solution to $x^2 + 1$.

Of course, the previous definition implies that $i^2 = -1$. Using i and \mathbb{R} , we now build the complex numbers.

3.1.1 Definition and first principles

Definition 3.2. The **complex numbers** is the set $\mathbb{C} := \{a + bi \mid a, b \in \mathbb{R}\}$. If $z = a + bi$, then a is called the **real part** of z and b is called the **imaginary part** of z .

Note that every complex number $z = a + bi$ is uniquely determined by two numbers: the real and imaginary parts a and b . As such, we often graph complex numbers in the coordinate plane with the x -axis denoting the real part and the y -axis denoting the imaginary part. This will be called the **complex plane**.

Example 3.3. We graph $-2 + 2i$ and $1 - 3i$ below.



We also define some operations on complex numbers.

Definition 3.4. We define the following operations on elements of \mathbb{C} .

- **Addition:** $(a + bi) + (c + di) := (a + b) + (c + d)i$
- **Multiplication:** $(a + bi) \cdot (c + di) := (ac - bd) + (ad + bc)i$
- **Complex Conjugation:** $\overline{a + bi} := a - bi$

Notice that in the definition of complex multiplication we are just using the normal distributive law (or FOIL if you like) together with the fact that $i^2 = -1$. Many of the familiar algebraic properties of \mathbb{R} also hold for \mathbb{C} , which we will take as a fact.

Fact 3.5. The following are true for \mathbb{C} .

- **Addition Laws:** Addition is associative and commutative. There is a unique additive identity, namely $0 = 0 + 0i$, and every number has a unique additive inverse, denoted $-(a + bi)$.
- **Multiplication Laws:** Multiplication is associative and commutative. There is a unique multiplicative identity, namely $1 = 1 + 0i$, and every nonzero number has a unique multiplicative inverse, denote $(a + bi)^{-1}$ or $\frac{1}{a+bi}$.
- **Distributivity Laws:** For all $x, y, z \in \mathbb{C}$, $x(y + z) = xy + xz$ and $(y + z)x = yx + zx$.
- **Conjugation Laws:** For all $x, y \in \mathbb{C}$, $\overline{\overline{x + y}} = x + y$ and $\overline{xy} = \overline{x}\overline{y}$.

Problem 3.6. Thinking of a complex number $z = a + bi$ as a point in the complex plane, describe *geometrically* what happens when $(c + di)$ is added to z . Also, describe *geometrically* how to find \bar{z} from z .

When we plot points, there are different coordinate systems we could use. It turns out that rectangular coordinates are good for adding complex numbers, but polar coordinates are better for multiplication. This lead to the following definition.

Definition 3.7. Let $z = a + bi$.

- (1) The **modulus** of z , denoted $|z|$, is the radius of the point (a, b) when written in polar coordinates. Thus, $|z| = \sqrt{a^2 + b^2}$.
- (2) The **argument** of z , denoted $\text{Arg}(z)$, is the angle of the point (a, b) when written in polar coordinates. Thus, $\text{Arg}(z)$ is the angle θ *in the appropriate quadrant* such that $0 \leq \theta < 2\pi$ and $\tan \theta = \frac{b}{a}$. The argument of 0 is undefined.

Example 3.8. We have that $|-2 + 2i| = \sqrt{(-2)^2 + 2^2} = 2\sqrt{2}$ and $\text{Arg}(-2 + 2i) = \frac{3\pi}{4}$. (But be careful, $\arctan\left(\frac{2}{-2}\right) = \frac{\pi}{4}$; you must pay attention to which quadrant the number is in.)



Problem 3.9. For each of the following complex numbers,

- write it in the form $a + bi$ (if it is not already),
- plot it in the complex plane,
- find the modulus and argument (if not exact, then a decimal approximation is okay).

(1) $u = -1 - i$

(3) $w = \frac{(2-i)(1+2i)}{2+3i}$

(2) $v = \frac{1}{1+i}$

(4) $z \in \mathbb{C}$ with $|z| = 3$ and $\text{Arg}(z) = \frac{4\pi}{3}$

Theorem 3.10. Let $z \in \mathbb{C}$. If $z \neq 0$, then $z^{-1} = \frac{\bar{z}}{|z|^2}$.

The next theorem shows how to find an expression for a complex number given its modulus and argument.

Theorem 3.11. Let $z \in \mathbb{C}$. Then $|z| = r$ and $\text{Arg}(z) = \theta$ if and only if $z = r \cos \theta + ir \sin \theta$ with $0 \leq \theta < 2\pi$.

We now derive some properties of multiplication. The first is quite useful and illustrates how multiplication is rather easy to deal with when numbers are in “polar form”.

Theorem 3.12. If $z_1 = r_1 \cos \theta_1 + ir_1 \sin \theta_1$ and $z_2 = r_2 \cos \theta_2 + ir_2 \sin \theta_2$, then

$$z_1 z_2 = r_1 r_2 \cos(\theta_1 + \theta_2) + ir_1 r_2 \sin(\theta_1 + \theta_2).$$

Corollary 3.13. If $z_1, z_2 \in \mathbb{C}$, then $|z_1 z_2| = |z_1| |z_2|$ and $\text{Arg}(z_1 z_2) = \text{Arg}(z_1) + \text{Arg}(z_2)$.

Corollary 3.14 (De Moivre's formula). For each positive $n \in \mathbb{Z}$,

$$(r \cos(\theta) + ir \sin(\theta))^n = r^n \cos(n\theta) + ir^n \sin(n\theta).$$

3.1.2 Roots of unity

We now arrive at an *extremely important* definition.

Definition 3.15. For each positive $n \in \mathbb{Z}$, define

$$\zeta_n := \cos\left(\frac{2\pi}{n}\right) + i \sin\left(\frac{2\pi}{n}\right).$$

Thus, ζ_n (read as “zeta n”) is the unique number with magnitude 1 and argument $\frac{2\pi}{n}$.

Problem 3.16. Plot each of the following in the same complex plane: $\zeta_2, \zeta_3, \zeta_4, \zeta_5$.

Problem 3.17. Plot each of the following in the same complex plane: $\zeta_6, (\zeta_6)^2, (\zeta_6)^3, (\zeta_6)^4, (\zeta_6)^5, (\zeta_6)^6$.

Problem 3.18. Write $\overline{\zeta_8}$ as a power of ζ_8 . Conjecture and prove a formula that expresses $(\zeta_n)^k$ as a power of ζ_n , but with no bar on top.

We now turn our attention back to solving polynomial equations, focusing on those of the form $x^n - a$.

Definition 3.19. Let $a \in \mathbb{C}$. A number $z \in \mathbb{C}$ is called an n^{th} **root of** a if $z^n = a$. In other words, the n^{th} roots of a are the roots of the polynomial $x^n - a$. The n^{th} roots of 1 are also called n^{th} **roots of unity**.

Problem 3.20. Find a 4th root of each of the following: ζ_3 and $-1 + i\sqrt{3}$.

Theorem 3.21. For each non-negative $k \in \mathbb{Z}$, $(\zeta_n)^k$ is an n^{th} root of 1.

Lemma 3.22. If z is an n^{th} root of 1, then $z = (\zeta_n)^k$ for some non-negative $k \in \mathbb{Z}$.

Lemma 3.23. For each non-negative $k \in \mathbb{Z}$, $(\zeta_n)^k = (\zeta_n)^m$ for some $0 \leq m \leq n-1$.

Theorem 3.24. The set

$$\{1, \zeta_n, (\zeta_n)^2, \dots, (\zeta_n)^{n-1}\}$$

is the set of *all* n^{th} roots of unity. Thus, there are n distinct n^{th} roots of unity.

Lemma 3.25. Let $a \in \mathbb{C}$ be nonzero, and let b be any one particular n^{th} root of a . Then z is an n^{th} root of a if and only if $\frac{z}{b}$ is an n^{th} root of 1.

Theorem 3.26. Let $a \in \mathbb{C}$ be nonzero, and let b be any one particular n^{th} root of a . The set

$$\{b, b\zeta_n, b(\zeta_n)^2, \dots, b(\zeta_n)^{n-1}\}$$

is the set of *all* n^{th} roots of a . Thus, there are n distinct n^{th} roots of a .

Problem 3.27. Find *all* 4th roots of each of the following: ζ_3 and $-1 + i\sqrt{3}$.

3.1.3 Roots of polynomials over \mathbb{R} and \mathbb{C}

We conclude this section with a couple of general results about roots of polynomials.

Theorem 3.28. Suppose that $p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0$ with all $a_i \in \mathbb{R}$. If z is a root of $p(x)$, then \bar{z} is also a root of $p(x)$.

In words, the previous theorem says that if a polynomial has coefficients in \mathbb{R} , then the set of roots is “closed under complex conjugation.” We end with an extremely important theorem, which will be quite useful for us. However, since its proof is not our main goal (and since it requires sophisticated techniques), we will take it as fact.

Fact 3.29 (Fundamental Theorem of Algebra). If $p(x)$ is a non-constant polynomial with all coefficients in \mathbb{C} , then $p(x)$ has a root in \mathbb{C} .

In fact, we will see that this implies that *all* roots of such a $p(x)$ lie in \mathbb{C} , so in our of study polynomials (often with all coefficients even in \mathbb{Q}), \mathbb{C} serves as a uniform world in which we can study the roots.

3.2 An aside: the quaternions

Our construction of the complex numbers creates a structure that contains the real numbers and possesses some nice properties not enjoyed by the real numbers, e.g. every non-constant polynomial with complex coefficients has a complex root. This raises the question: could we further extend the complex numbers to an even larger structure?

Concisely, we built the complex numbers as the set $\mathbb{C} = \mathbb{R} + \mathbb{R}i$ together with the operations of addition and multiplication, which were defined in a natural way from the key identity that $i^2 = -1$. Here, we briefly explore what happens if we build a larger structure in a similar way: $\mathbb{H} = \mathbb{C} + \mathbb{C}j$ where, again, $j^2 = -1$.

Following this path, we formally arrive at $\mathbb{H} = \mathbb{C} + \mathbb{C}j = (\mathbb{R} + \mathbb{R}i) + (\mathbb{R} + \mathbb{R}i)j$, and any definition we give for multiplication of two elements of \mathbb{H} must first define how to multiply i and j (or rather, what properties ij should have). If we set $k = ij$, it turns out that a good route to follow is to decide that k also has the property that it squares to 1, i.e. $k^2 = -1$. There is another important choice one is “forced” to make, namely that $ji = -k$.

Definition 3.30. The **quaternions** are the elements of $\mathbb{H} := \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$, where $i^2 = j^2 = k^2 = -1$. We also define the following operations on elements of \mathbb{H} .

- **Addition:** $(a_1 + b_1 i + c_1 j + d_1 k) + (a_2 + b_2 i + c_2 j + d_2 k) := (a_1 + a_2) + (b_1 + b_2)i + (c_1 + c_2)j + (d_1 + d_2)k$
- **Multiplication:** use the usual distributive laws together with the identities:

$$\begin{aligned} ij &= k, & jk &= i, & ki &= j, \\ ji &= -k, & kj &= -i, & ik &= -j. \end{aligned}$$

- **Conjugation:** $\overline{a + bi + cj + dk} := a - bi - cj - dk$

Indeed, \mathbb{H} extends the complex numbers, and we have the following containments: $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \subset \mathbb{H}$. It turns out that \mathbb{H} satisfies nearly all of the common algebraic properties of \mathbb{R} and \mathbb{C} , with one notable exception, which is highlighted in bold below.

Fact 3.31. The following are true for \mathbb{H} .

- **Addition Laws:** Addition is associative and commutative. There is a unique additive identity, namely $0 = 0 + 0i + 0j + 0k$, and every number has a unique additive inverse.
- **Multiplication Laws:** Multiplication is associative but **noncommutative**. There is a unique multiplicative identity, namely $1 = 1 + 0i + 0j + 0k$, and every nonzero number has a unique multiplicative inverse.
- **Distributivity Laws:** For all $x, y, z \in \mathbb{H}$, $x(y + z) = xy + xz$ and $(y + z)x = yx + zx$.
- **Conjugation Laws:** For all $x, y \in \mathbb{H}$, $\overline{x + y} = \overline{x} + \overline{y}$ and $\overline{xy} = \overline{y}\overline{x}$.

We can also define the modulus of a quaternion, analogous to how we defined it for a complex number.

Definition 3.32. The **modulus** of $h = a + bi + cj + dk$, denoted $|h|$, is $|h| = \sqrt{a^2 + b^2 + c^2 + d^2}$.

Problem 3.33. Write each of the following quaternions in the form $a + bi + cj + dk$, and find its modulus.

(1) $h = (2i + 4k)(7 - 3j + k)$

(3) $w = (i + j)^{-1}$

(2) k^{-1}

Theorem 3.34. Let $h \in \mathbb{H}$. If $h \neq 0$, then $h^{-1} = \frac{\overline{h}}{|h|^2}$.

And as in the complex numbers, the modulus function is multiplicative—we will take this as fact.

Fact 3.35. If $h_1, h_2 \in \mathbb{H}$, then $|h_1 h_2| = |h_1| |h_2|$.

We conclude this section by looking at multiplication of quaternions a little closer. As we do, we return to the mathematical notion of a *group*. Please feel free to look over old notes or other books to review the basics. As mentioned in the introduction, our main reference for groups will be [An Inquiry-Based Approach to Abstract Algebra](#).

Problem 3.36. Let G be the subset of \mathbb{H} defined as $G := \{\pm 1, \pm i, \pm j, \pm k\}$. Show that G , together with the operation of quaternion multiplication, is a nonabelian group. If you have encountered this group before, what name (or symbol) did you know it by?

Problem 3.37. Let S be the subset of \mathbb{H} consisting of all quaternions with modulus equal to 1, i.e. $S := \{h \in \mathbb{H} \mid |h| = 1\}$. Show that S , together with the operation of quaternion multiplication, is an infinite, nonabelian group.

It turns out that the group S from the previous problem is isomorphic to the group $SU(2)$ (one the the so-called special unitary groups), which is quite important in theoretical physics. If you want to learn more, you can start on [Wikipedia](#).

3.3 Abstract fields

Notice that \mathbb{Q} , \mathbb{R} , and \mathbb{C} satisfy many common algebraic properties with respect to addition and multiplication. Of course, \mathbb{H} does too, though it lacks commutativity of multiplication. When objects have common properties, it can be extremely valuable to abstract those properties and study them once and for all (as opposed to trying to prove things about each individual structure). This is where we are headed, but first we highlight some related structures (again with algebraic properties similar to \mathbb{Q} , \mathbb{R} , and \mathbb{C}) that help to connect this work to our main goal of expressing roots of polynomials.

Problem 3.38. Let $p(x) = x^2 + 3x + 1$. Find the roots of $p(x)$, and show that each root can be written in the form $a + b\sqrt{5}$ with $a, b \in \mathbb{Q}$.

Problem 3.39. Let $S = \{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\}$.

- (1) Show that S is closed under addition; that is, show that for all $x, y \in S$, $x + y \in S$.
- (2) Show that S is closed under multiplication; that is, show that for all $x, y \in S$, $xy \in S$.
- (3) Use that $S \subset \mathbb{R}$ to explain why both addition and multiplication of elements of S are associative and commutative and why multiplication distributes over addition.

Problem 3.40. Let $S = \{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\}$. Prove or disprove: if $x \in S$ and $x \neq 0$, then x has a multiplicative inverse in S (i.e. there is a $y \in S$ such that $xy = 1$).

3.3.1 Definition

We now abstract the common properties of \mathbb{Q} , \mathbb{R} , and \mathbb{C} (and also S from Problem 3.39), arriving at the definition of a field.

Definition 3.41. A **field** is a structure $(F, +, \cdot)$ consisting of a set F , containing at least two elements, together with two binary operations $+$ and \cdot (which we call *addition* and *multiplication*) such that for some elements $0, 1 \in F$ the following axioms hold.

- **Addition Axioms:** Addition is associative and commutative; the element 0 is an additive identity; every $x \in F$ has an additive inverse with respect to 0 , denoted $-x$.
- **Multiplication Axioms:** Multiplication is associative and commutative; the element 1 is a multiplicative identity; every $x \in F \setminus \{0\}$ has a multiplicative inverse with respect to 1 , denoted x^{-1} .
- **Distributivity Axioms:** For all $x, y, z \in F$, $x(y + z) = xy + xz$ and $(y + z)x = yx + zx$.

Recall that “ 0 is an additive identity” means that “for all $x \in F$, $0 + x = x + 0 = x$,” and “ $x \in F$ has an additive inverse with respect to 0 ” means that “there exists some $y \in F$ such that $x + y = y + x = 0$.” The meanings of multiplicative identities and inverses are similar to those for addition. Also, recall that $F \setminus \{0\}$ denotes the set obtained by removing the element 0 from F . We introduce some notation for this.

Definition 3.42. If F is a field, then $F \setminus \{0\}$ is denoted by F^* , i.e. F^* is the set of nonzero elements of F .

Using the language of groups, fields can be concisely defined as structures of the form $(F, +, \cdot)$ such that $(F, +)$ is an abelian group with identity 0, (F^*, \cdot) is an abelian group with identity 1, and multiplication distributes over addition.

Now, as with any new definition, we look for examples and basic properties.

3.3.2 Some examples and non-examples

It is not hard to verify that \mathbb{Q} , \mathbb{R} , \mathbb{C} , and S from Problem 3.39 are all fields (with their usual definitions of addition and multiplication). Let's search for more examples and non-examples.

Problem 3.43. Explain why \mathbb{Z} is not a field.

Problem 3.44. Determine if each of the following is a field. If it is a field, identify an additive and multiplicative identity; if it is not a field, explain why not.

(1) $(F, +, \cdot)$ where $F = \{a, b, c\}$ and $+$ and \cdot are defined as follows:

$+$	a	b	c
a	b	c	a
b	c	a	b
c	a	b	c

\cdot	a	b	c
a	a	b	c
b	b	a	c
c	c	c	c

(2) $(F, +, \cdot)$ where $F = \{0, 1, 2, 3\}$ and $+$ and \cdot are defined as follows:

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

\cdot	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

(3) $(F, +, \cdot)$ where $F = \{0, 1, 2, 3\}$ and $+$ and \cdot are defined as follows:

$+$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

\cdot	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Problem 3.45. Look back at Problem 3.44. For those that are fields, determine which familiar group each of $(F, +)$ and (F^*, \cdot) is isomorphic to.

To find more examples of fields, Problem 3.44 hints at the fact we may want to look back to modular arithmetic. Following [An Inquiry-Based Approach to Abstract Algebra](#), we define the structures $(\mathbb{Z}_n, +_n, \cdot_n)$ as follows.

Definition 3.46. Let n be a positive integer. The the structure $(\mathbb{Z}_n, +_n, \cdot_n)$ consists of the set $\mathbb{Z}_n := \{0, 1, 2, \dots, n-1\}$ together with the operations $+_n$ and \cdot_n defined as follows.

- **Addition:** $x +_n y$ is the least non-negative number congruent to $x + y$ modulo n .
- **Multiplication:** $x \cdot_n y$ is the least non-negative number congruent to $x \cdot y$ modulo n .

We often refer to the entire structure $(\mathbb{Z}_n, +_n, \cdot_n)$ as simply \mathbb{Z}_n . Also, when the context is clear, we may write $+$ and \cdot in place of $+_n$ and \cdot_n .

Problem 3.47. Show that \mathbb{Z}_5 is a field but \mathbb{Z}_6 is not.

Problem 3.48. Make a conjecture as to when \mathbb{Z}_n is a field and when it is not. That is, try to fill in the blank: “ \mathbb{Z}_n is a field provided (something about n).” What evidence do you have to support this?

3.3.3 Basic properties

Let’s now explore some basic properties of fields that follow from the definition. We list some of these as facts since they follow directly from basic group theory, since $(F, +)$ and (F^*, \cdot) are both groups.

From now on, when we write “let F be a field,” we tacitly mean “let $(F, +, \cdot)$ be a field.”

Fact 3.49. Let F be a field.

- (1) The additive identity and the multiplicative identity are both unique.
- (2) Additive inverses and multiplicative inverses are unique.

Theorem 3.50. Let F be a field.

- (1) For all $x \in F$, $x \cdot 0 = 0$.
- (2) For all $x, y \in F$, $(-x)y = -(xy)$ and $x(-y) = -(xy)$.
- (3) For all $x \in F^*$, $-x \in F^*$ and $(-x)^{-1} = -(x^{-1})$.
- (4) For all $x, y \in F$, if $xy = 0$, then $x = 0$ or $y = 0$.
- (5) The additive and multiplicative identities are different, i.e. $0 \neq 1$.

3.3.4 Another example

We now return to the conjecture you made in Problem 3.48. Combining the next theorem with Theorem 3.50, we see that \mathbb{Z}_n has no hope to be a field unless n is prime.

Theorem 3.51. Let n be a positive integer. If n is not prime, then there exist $a, b \in (\mathbb{Z}_n)^*$ such that $ab = 0$.

And now we completely answer the question. As you explore the next theorem, you can use properties of modular arithmetic that you know from before. For example, you can take for granted that addition and multiplication are both associative and commutative. The crux is in showing that every nonzero element has a multiplicative inverse when n is prime. There are many ways to approach this; one way uses [Bézout's lemma](#) from basic number theory. Even if you don't use it now, it's a useful fact to remember.

Fact 3.52 (Bézout's lemma). If $a, b \in \mathbb{Z}$, then there exist $k, l \in \mathbb{Z}$ such that $ka + lb = \gcd(a, b)$.

Theorem 3.53. Let n be a positive integer. Then \mathbb{Z}_n is a field if and only if n is prime.

3.3.5 Subfields

Just as with groups and subgroups, the notion of a subfield is extremely important. Analyzing the subfields of a field F can often yield a better understanding of the whole field F , and vice versa. Also, this will allow us to generate more examples of fields.

Definition 3.54. Let $(E, +, \cdot)$ be a field, and let F be a subset of E . Then F is a **subfield** of E if F is a field in its own right with respect to operations $+$ and \cdot inherited from E . When F is a subfield of E , E is called an **extension field** of F .

To check that a subset F of a field E is a subfield, it turns out that F will automatically satisfy many of the field axioms, leaving only a handful of things to check.

Theorem 3.55. Let E be a field, and let $F \subseteq E$. Then F is a subfield of E if and only if

- (1) F contains at least 2 elements;
- (2) for all $x, y \in F$, $x + y \in F$ and $xy \in F$;
- (3) for all $x \in F$, $-x \in F$; and
- (4) for all $x \in F^*$, $x^{-1} \in F$.

The second item in the above theorem is stating that F is closed under the addition and multiplication inherited from E . The last two items could be read as F being closed additive and multiplicative inverses.

It is easy to check that \mathbb{Q} and \mathbb{R} are both subfields of \mathbb{C} ; S from Problem 3.39 is also a subfield of \mathbb{C} (and of \mathbb{R}). Let's look for more that are similar to S .

Problem 3.56. Determine which of the following are subfields of \mathbb{C} .

- (1) $T_1 = \{a + bi \mid a, b \in \mathbb{Q}\}$
- (2) $T_2 = \{a + bi \mid a, b \in \mathbb{Z}\}$
- (3) $T_3 = \{a + b\alpha \mid a, b \in \mathbb{Q}\}$ where $\alpha = \sqrt{2} + i$

3.3.6 Generating subfields

Appendix A

Hints

Below are some hints, which should be interpreted as possible (but not the only!) ways to get started.

Hint (Theorem 2.4). You are solving $x^2 + bx + c = 0$. Try “completing the square” first; then solve for x .

Hint (Problem 3.9). Multiplying a fraction by the complex conjugate of the denominator can be an effective way to simplify an expression.

Hint (Theorem 3.11). Think back to changing from polar to rectangular coordinates (or parametrizing circles or solving triangles).

Hint (Theorem 3.12). Try using Theorem 3.11 + trigonometric identities.

Hint (Lemma 3.22). You are working with powers (hence multiplication) so try writing z in the form $z = r \cos \theta + ir \sin \theta$. Now, what does $z^n = 1$ imply about r and θ ?

Hint (Theorem 3.24). You may want to view this as the following “if and only if” statement: z is an n^{th} root of 1 $\iff z = (\zeta_n)^k$ for some $0 \leq k \leq n - 1$. Now make use of the previous lemma and theorems you proved. Don’t forget to explain why each of $1, \zeta_n, (\zeta_n)^2, \dots, (\zeta_n)^{n-1}$ are all different.

Hint (Theorem 3.28). Suppose that z is a root of $p(x)$. Then $p(z) = 0$, so $a_n z^n + a_{n-1} z^{n-1} + \dots + a_2 z^2 + a_1 z + a_0 = 0$. This last equation is just comparing two complex numbers—try taking the conjugate of both sides. Fact 3.5 is helpful.

Hint (Problem 3.40). You are trying to find $(a + b\sqrt{5})^{-1} = \frac{1}{a + b\sqrt{5}}$. Try multiplying top and bottom by the conjugate: $a - b\sqrt{5}$.

Hint (Theorem 3.50). For the first part, notice that $x \cdot 0 = x(0 + 0)$. For the last part, remember that the definition of a field ensures that F has at least two elements, so there is some $a \in F$ with $a \neq 0$. Now, what happens if $0 = 1$?

Hint (Theorem 3.53). The crux is to show that every nonzero element has a multiplicative inverse when n is prime. Let $a \in (\mathbb{Z}_n)^*$. You need to find some integer b such that $ab = 1$ modulo p . Now, since $a \in (\mathbb{Z}_n)^*$ and n is prime, $\gcd(a, p) = 1$. By Bézout’s Lemma, there exist $k, l \in \mathbb{Z}$ such that $1 = ka + lp$. What happens when you consider the equation $1 = ka + lp$ modulo p ?

Hint (Problem [3.56](#)). If T_3 is a subfield, then, in particular, it is closed under multiplication, so it must be that $\alpha^2 \in T_3$. What does this imply?