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

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

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

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!

Contents

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. In this class, earnest failure outweighs counterfeit success; you need not feel pressure to hunt for solutions outside your own creative and intellectual reserves. For more details, check out the Syllabus.

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**, **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 **Theorem** and **Corollary** designation are mathematical facts and the intention is for you to produce a valid proof of the given statement. The main difference between a **Theorem** and a **Corollary** is that 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, 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 can also use a computer program (e.g. WolframAlpha) if you need. For each problem, make a note about *how* you found the roots. Try for exact answers, but you can approximate if needed.

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

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

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

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

(5) $f(x) = x^4 - 1$

(6) $g(x) = x^4 - 5x^2 + 6$

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

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

Problem 2.2. For each part of Problem **??**, 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 **??** 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.

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.

Problem 2.8. Use Fact **??** 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 **??**—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? Feel free to look up quintic functions on Wikipedia.

Let's first try to tackle the "what do we mean by formula" question. You should be guided by your previous responses to the problems of the form "describe a number system, as small as possible, that is capable of expressing the roots of..." This leads to the following intuitive definition, that we will work to sharpen later.

Intuitive Definition 2.10. A polynomial (with coefficients in $\mathbb{Q}$) is said to be **solvable by radicals** if every root of the polynomial can be expressed 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 $p(x) = x^4 - 2x^2 - 1$, and explain why $p(x)$ is solvable by radicals.

Theorem 2.12. Every quadratic and cubic polynomial is solvable by radicals.

Our goal is to prove the following theorem, in a rather elegant, Galois-ian way.

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

Boom!

Chapter 3

Fields

In Chapter **??**, 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.

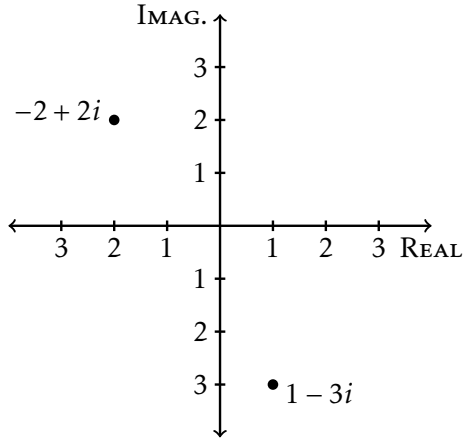
Of course, the previous definition implies that $i^2 = -1$. Using i and $\mathbb{R}$, we now build the complex numbers.

Definition 3.2. The **complex numbers**, denoted $\mathbb{C}$, is the set $\{a+bi \mid a,b \in \mathbb{R}\}$. If $z \in \mathbb{C}$ and z is written as $z = a+bi$, 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. Consider the complex numbers $a+bi$ and $c+di$. We define the following operations.

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 $i^2=-1$.

Problem 3.5. Thinking of a complex number z as a point in the complex plane, describe *geometrically* what happens when $(c+di)$ is added to z. Also, describe *geometrically* how to find $\overline{z}$ from z.

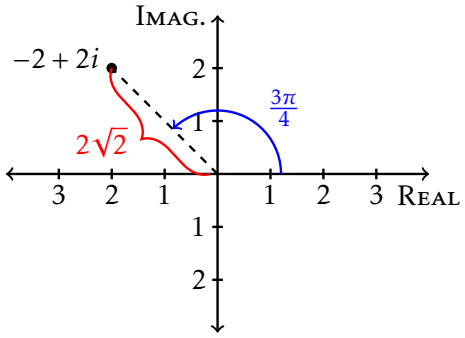
When we plot points, there are different coordinate systems we could use. It turns out that rectangular coordinates are good for adding complex numbers, but polar coordinates are better for multiplication. This lead to the following definition.

Definition 3.6. 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 $\mathrm{Arg}(z)$, is the angle of the point (a,b) when written in polar coordinates. Thus, $\mathrm{Arg}(z)$ is the angle θ *in the appropriate quadrant* such that $0\le\theta<2\pi$ and $\tan\theta=\frac{b}{a}$. The argument of 0 is undefined.

Example 3.7. We have that $|-2+2i| = \sqrt{(-2)^2+2^2} = 2\sqrt{2}$ and $\operatorname{Arg}(-2+2i) = \frac{3\pi}{4}$. But be careful, $\arctan(-1) = \frac{\pi}{4}$; you must pay attention to which quadrant the number is in.



Problem 3.8. 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) $u = -1-i$

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

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

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

Given a complex number in the form $a+ib$, we know how to find the modulus and argument (by just using the definition). The next theorem highlights how to go in the reverse direction.

Theorem 3.9. Let $z \in \mathbb{C}$. Then $|z| = r$ and $\operatorname{Arg}(z) = \theta$ if and only if $z = r\cos\theta + ir\sin\theta$ with $0 \le \theta < 2\pi$.

Theorem 3.10. 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

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

The previous theorem shows that multiplying two complex numbers is rather easy when they are in "polar form". It yields two nice corollaries.

Corollary 3.11. If $z_1, z_2 \in \mathbb{C}$, then $|z_1 z_2| = |z_1||z_2|$ and $\operatorname{Arg}(z_1 z_2) = \operatorname{Arg}(z_1) + \operatorname{Arg}(z_2)$.

Corollary 3.12 (De Moivre's formula)**.** For each positive $n \in \mathbb{Z}$,

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

We now arrive at an *extremely important* definition.

Definition 3.13. 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 3.14. Plot each of the following in the same complex plane: ζ_2, ζ_3, ζ_4, ζ_5.

Problem 3.15. Plot each of the following in the same complex plane: ζ_6, $(\zeta_6)^2$, $(\zeta_6)^3$, $(\zeta_6)^4$, $(\zeta_6)^5$, $(\zeta_6)^6$.

Problem 3.16. Write $\overline{\zeta_8}$ as a power of ζ_8. Conjecture a formula that expresses $\overline{(\zeta_n)^k}$ as a power of ζ_n, but with no bar on top.

Appendix A

Hints

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

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

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

Hint (Theorem **??**)**.** Try using Theorem **??** + trigonometric identities.