MTH 461 **Spring 2020**
Course Notes **Drew Armstrong**

Introduction

What is algebra? The word "algebra" comes from the Arabic "al-jabr," meaning restoration or completion. In modern terms this refers to the method of simplifying an equation by adding the same positive quantity to each side. The word came into English from a Latin translation of the title of a 9th century work by Mohammed ibn Musa al-Khwarizmi (780–850).[1] This work is regarded as the first systematic treatise on the solution of equations.

Al-Khwarizmi's work was translated to Latin in the 12th century and exerted a strong influence on the development of mathematics in Europe. The word "algebra" came to refer to the general study of equations involving unknown quantities. The subject developed to a very high degree of sophistication, as summarized by Lagrange in his 1770 work on the "algebraic resolution of equations." In fact, the study of equations had become so complicated that a completely new language was necessary to make further progress.

This new language, today referred to as "abstract algebra," developed throughout the 1800s until it was systematized in van der Waerden's 1930 textbook called *Modern Algebra*. The word "algebra" no longer refers only to the study of equations, but more generally to the study of "abstract structure" in mathematics. The the most common kinds of abstract structures go by the technical names of "group," "ring," "field," "vector space," and "module." There has been an increasing tendency toward generalization and abstraction that brings the subject of algebra closer to logic and philosophy than to science.

The official title of MTH 461 is "Survey of Modern Algebra." This is also the title of a famous textbook written by Birkhoff and Mac Lane in 1941. Their goal was to translate the ideas from van der Waerden's German textbook into English for the benefit of undergraduate students at Harvard. Birkhoff and Mac Lane's book went through four editions and became a standard textbook at American universities. But today the textbook (and the term "modern algebra" itself) is slightly out of date.

In this course I will not follow any specific textbook because my teaching style is a bit unusual. There are a few different considerations one must take into account when designing a mathematics course:

(1) The logical structure of the ideas.

(2) Examples, problems and applications.

[1] Al-Khwarizmi was one of the earliest scholars working at the House of Wisdom in Baghdad. He is known today primarily for his work in arithmetic and algebra. His work on the Indian system of decimal arithmetic was translated into Latin as *Dixit Algorithmi* [thus spoke al-Khwarizmi]. This work was responsible for introducing Hindu-Arabic numeral system to the Western world and is the origin of the English word "algorithm."

(3) History and motivation.

The traditional teaching style for most of the twentieth century has been

$$(1) \rightsquigarrow (2) \rightsquigarrow (3).$$

In this style, one first presents formal definitions and then proves a series of lemmas and theorems. Afterward an example or two is given and applications are be mentioned. Finally, the instructor might say a word or two about the historical context in which the ideas developed (though this third step is often omitted). In this course I will use the opposite teaching style:

$$(3) \rightsquigarrow (2) \rightsquigarrow (1).$$

That is, I will introduce the ideas roughly in their order of historical development. Through the discussion of concrete and historical examples, I will try to present each new idea as the answer to a previous question. Finally, I will state formal definitions and prove some theorems in order to systematize what we have learned. The drawback of this teaching style is that we will not cover as much of the standard curriculum as a traditional course. The benefit, I hope, is that you will understand and appreciate the material at a deeper level.

If you are the kind of student who wants to see algebra at the maximum level of generality you might prefer to take the two-semester sequence of MTH 561/562. Alternatively, you might choose to take those courses next year if you enjoy this course; the way I teach 461 does not overlap very much with 561/562. If you want to see my own approach to the courses 561/562, take a look at the textbook I wrote called *Algebra: 1830–1930*.

Contents

1 Solving Equations

I mentioned that classical algebra is about solving equations, but what kind of equations?

Example: Solve the equation $2x - 6 = 0$ for the unknown x.

Solution: We have

$$\begin{aligned} 2x - 6 &= 0 \\ 2x - 6 + 6 &= 0 + 6 \\ 2x &= 6 \\ x &= 6/2 \\ x &= 3. \end{aligned}$$

Note that we obtained the solution by executing a mindless sequence of formal rules. In other words, an algorithm. When al-Khwarizmi first treated such problems in the 9th century he did not have any of this technology. Instead he expressed each step of the algorithm in terms of words. The first step, in which the quantity 6 is added to each side in order to remove the subtraction is an example of *al-jabr*, which means restoration or completion. Yes, once upon a time that was a big deal. The use of the letters x, y, z for unknown variables goes back to Descartes' *Geometry* (1637). Descartes also introduced the use the letters a, b, c for unknown constants.

Example: Solve the equation $ax + b = 0$ for the unknown x.

Solution: There are two cases:

- If $a \neq 0$ then we have

$$\begin{aligned} ax + b &= 0 \\ ax &= -b \\ x &= -b/a. \end{aligned}$$

- If $a = 0$ then we have

$$0x + b = 0.$$

  Now there are two sub-cases:

– If $b \neq 0$ then there is no solution.

– If $b = 0$ then every x is a solution.

So far, so good. We may also consider simultaneous equations in more than one unknown.

Example: Solve the following two simultaneous equations for x and y:

$$\begin{array}{ll} (i) & \left\{ \begin{array}{rcrcr} x & + & y & = & 2, \\ 2x & + & 3y & = & -1. \end{array} \right. \\ (ii) & \end{array}$$

Solution: There are two basic ways to solve a system of equations: substitution and elimination. With the method of substitution we would solve for x (or y) in one equation and then substitute this expression into the other. With the method of elimination we eliminate x (or y) by taking a suitable linear combination of the given equations. For example, we can define a new equation $(iii) = (ii) - 2(i)$ that has no x by subtracting twice the first equation from the second:

$$\begin{array}{rrcrcr} & 2x & + & 3y & = & -1 \\ - & 2x & + & 2y & = & 4 \\ \hline & & & y & = & -5 \end{array}$$

We conclude that $y = -5$ and then back-substituting into either of the previous equations gives $y = 7$.

The Problem of Linear Algebra

A general *linear equation* has the form

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b,$$

where

- $a_1, a_2, \ldots, a_n, b$ are constants and
- $x_1, x_2, \ldots, x_n$ are unknowns.

The general problem of linear algebra is to solve a system of m linear equations in n unknowns.

I assume that you know a bit about linear algebra because there is a whole course devoted to it (MTH 210), which is a prerequisite for this course. We tend to separate the topic of linear algebra from the rest of (non-linear) algebra for two reasons:

- Linear algebra is completely solved, i.e., there are no big open problems in the subject.
- Linear algebra is extremely important in applied mathematics. Therefore we want to teach it to everyone, without burdening them too much with abstraction.

The problem that we will consider in this course is much harder.

The Problem of Non-Linear Algebra

A *polynomial equation of degree* d in one variable x has the form

$$\sum_{k=0}^{d} a_k x^k = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_1 x + a_0 = 0,$$

where $a_0, a_1, \ldots, a_n$ are some constants, called the *coefficients*. A polynomial equation in two variasbles x, y has the form

$$\sum_{k,\ell \geqslant 0} a_{k\ell}\, x^k y^\ell = 0,$$

where only finitely many of the coefficients $a_{k\ell}$ are nonzero,[2] and a polynomial equation in n variables has the form

$$\sum_{k_1,k_2,\ldots,k_n \geqslant 0} a_{k_1,k_2,\ldots,k_n}\, x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n} = 0,$$

where only finitely many of the coefficients $a_{k_1,k_2,\ldots,k_n}$ are non-zero. The general problem of non-linear algebra is to solve a system of m polynomial equations in n unknowns.

This problem is not completely solved. In fact, it is one of the most active areas of current mathematical research.[3] In this course we will spend most of our time studying polynomial equations in just one variable. One of the major theorems in this subject is the *Abel-Ruffini Theorem* (1824), which says the following:

> It is **impossible** to express the solutions of the fifth degree equation
>
> $$ax^5 + bx^4 + cx^3 + dx^2 + ex + f = 0$$
>
> in terms of the coefficients and the algebraic operations $+$, $-$, $\times$, $\div$, $\sqrt{}$, $\sqrt[3]{}$, $\sqrt[4]{}$, $\ldots$

[2] For example, consider the polynomial equation $8x^2y + 3xy + 2y^2 + 2x + 3y - 12 = 0$. Unlike in the case of one variable, there is no very obvious way to put the terms in order. Note that it is also difficult to define the "degree" of a polynomial in two variables.

[3] The technical name of this subject is "algebraic geometry."

2 Quadratic Equations

2.1 Al-Khwarizmi

The general quadratic equation $ax^2 + bx + c = 0$ has the following solution:

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2}.$$

I'm sure you remember this formula from high school, but do you know why it is true? Specific examples were understood by the ancient Greeks, but the first person to write about "the general quadratic equation" was Mohammed ibn Musa al-Khwarizmi, in his work *Al-kitab al-mukhtasar fi hisab al-jabr wa'l-muqabala* ($\sim$ 820 AD) [The Compendious Book on Calculation by Completion and Balancing]. Since the concept of negative numbers was not accepted at the time, al-Khwarizmi divided the problem into three separate cases:[4]

Type I. $x^2 + ax = b$

Type II. $x^2 = ax + b$

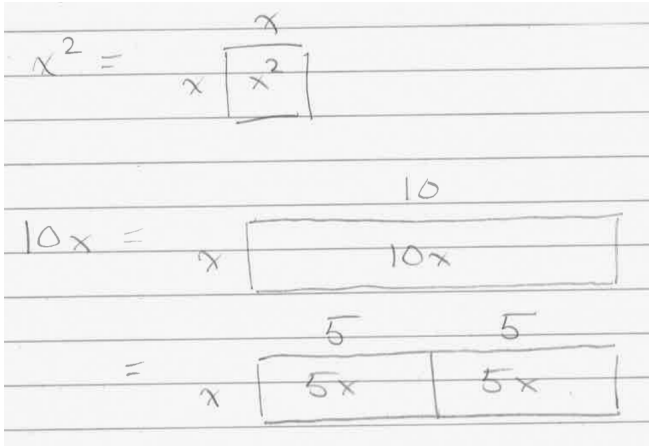
Type III. $x^2 + b = ax$

The solution to each case was illustrated with a specific example, though it was understood that the same reasoning could be applied in general. Here are his three examples.

Type I. *A square and ten Roots are equal to thirty-nine Dirhems*:

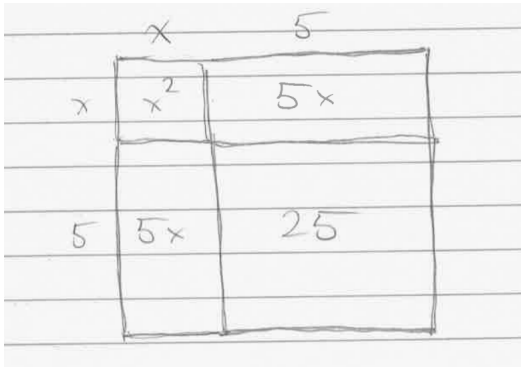
$$\boxed{x^2 + 10x = 39}$$

We think of x^2 as the area of a square and $10x$ are the area of a rectangle:



[4]Actually he divided quadratic equations into six cases. The other three are $x^2 = ax$, $x^2 = b$ and $ax = b$, which are too boring to discuss. He also describes equation in words, since he did not have a symbolic notation. For example, he expressed $x^2 + 10x = 39$ by saying that "a square and ten roots are equal to thirty-nine Dirhems."

Now we cut the rectangle into two equal rectangles of area $5x$ and "complete the square":



Since the big square has area $(x+5)^2$ we conclude that

$$\begin{aligned}
(x+5)^2 &= x^2 + 5x + 5x + 25 \\
(x+5)^2 &= \boxed{x^2 + 10x} + 25 \\
(x+5)^2 &= \boxed{39} + 25 \\
(x+5)^2 &= 64 \\
x+5 &= 8 \qquad\qquad \text{al-muqabala} \\
x &= 3.
\end{aligned}$$

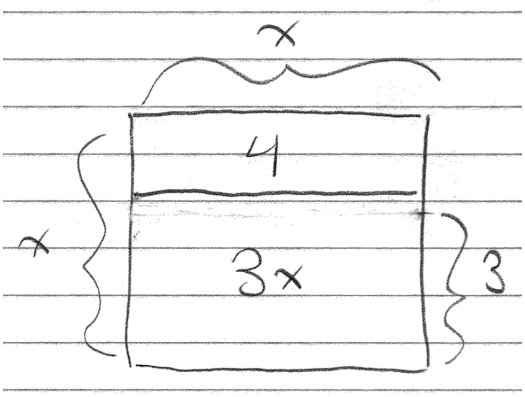
The final step is an example of *al-muqabala* [balancing] since we subtracted 5 from both sides. We will see the other fundamental operation *al-jabr* [completion] in the next example. It is clear from the geometry that an equation of Type I always has exactly one (positive, real) solution. In modern notation we can summarize the algorithm as follows:

$$x^2 + ax = b \quad \Longrightarrow \quad x = \sqrt{b + \frac{a^2}{4}} - \frac{a}{2}.$$

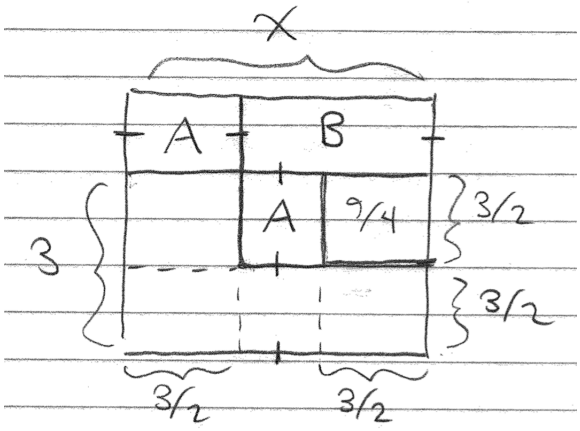
Type II. *Three roots and four of Simple Numbers are equal to a Square*:

$$\boxed{x^2 = 4 + 3x}$$

We cut a rectangle of area $3x$ from a square of area x^2 to obtain the following diagram:



Then we construct the following diagram:



Note that the two rectangles labeled A have equal area since they have equal dimensions. Furthermore, note that $A + B = 4$ by construction. Finally, note that the square comprised of A, B and $9/4$ has side length $x - 3/2$, so that

$$\begin{aligned}
(x - 3/2)^2 &= \boxed{A + B} + 9/4 \\
(x - 3/2)^2 &= \boxed{4} + 9/4 \\
(x - 3/2)^2 &= 25/4 \\
x - 3/2 &= 5/2 \\
x &= 5/2 + 3/2 \qquad \text{al-jabr} \\
x &= 4.
\end{aligned}$$

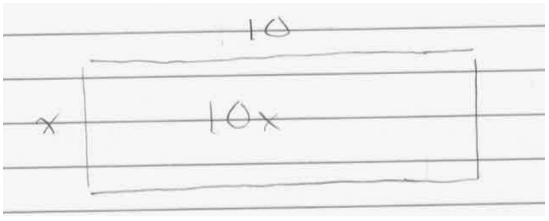
We note that this equation again has exactly one (positive, real) solution. In modern notation we can summarize the algorithm as follows:

$$x^2 = ax + b \quad \Longrightarrow \quad x = \sqrt{b + \frac{a^2}{4}} + \frac{a}{2}.$$

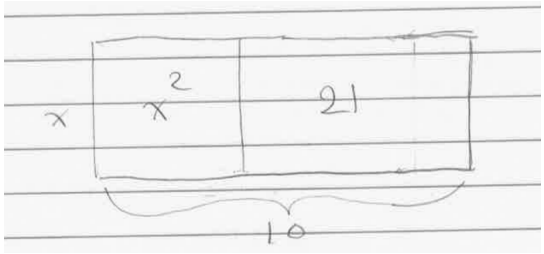
Type III. *A square and twenty-one Dirhems are equal to ten Roots*:

$$\boxed{x^2 + 21 = 10x}$$

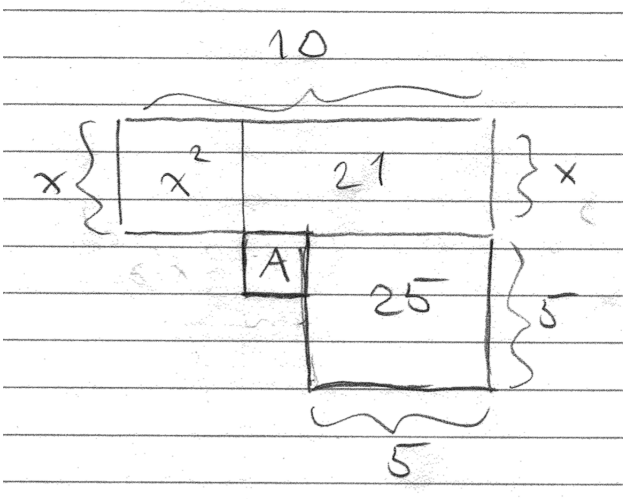
We think of $10x$ as the area of a rectangle:



Then we cut a square of length x from one side to obtain the following diagram:



Now al-Khwarizmi divides the problem in two subcases.[5] **Case i.** If $x < 5$ then we construct the following diagram:

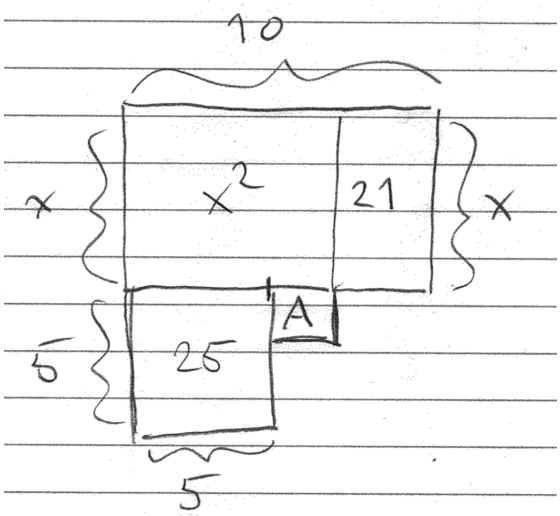


[5]Actually, he's not very clear about this, so I cleaned it up.

In this case he gives a geometric argument that $A+21 = 25$. (You will reproduce his argument on the first homework.) On the other hand, the square A has side length $5 - x$, so that

$$\begin{aligned} A + 21 &= 25 \\ (5-x)^2 + 21 &= 25 \\ (5-x)^2 &= 4 && \text{al-muqabala} \\ 5 - x &= 2 \\ 5 &= 2 + x && \text{al-jabr} \\ 3 &= x. && \text{al-muqabala} \end{aligned}$$

Here we see an example of *al-jabr*, when we add the positive quantity x to both sides of the equation $5 - x = 2$ in order to "complete" or "restore" the left hand side to its full value 5.
Case ii. If $x > 5$ then we construct the following diagram:



In this case, al-Khwarizmi gives a completely different geometric argument (which you will also reproduce on the homework) that $A + 21 = 25$. Then since $A = (x-5)^2$ we obtain

$$\begin{aligned} A + 21 &= 25 \\ (x-5)^2 + 21 &= 25 \\ (x-5)^2 &= 4 && \text{al-muqabala} \\ x - 5 &= 2 \\ x &= 7. && \text{al-jabr} \end{aligned}$$

We conclude that the equation $x^2 + 21 = 10x$ has two different solutions: $x = 3$ and $x = 7$.

In modern notation we can summarize the algorithm as follows:

$$x^2 + b = ax \quad \Longrightarrow \quad x = \frac{a}{2} + \sqrt{\frac{a^2}{4} - b} \quad \text{or} \quad x = \frac{a}{2} - \sqrt{\frac{a^2}{4} - b}.$$

If $a^2/4 - b > 0$ then we obtain two (positive, real) solutions. However, if $a^2/4 - b < 0$ then there are no solutions. Al-Khwarizmi mentions that this may happen, but he does not give any geometric explanation.

In summary: Al-Khwarizmi divides quadratic equations into three types since he only accepts positive numbers. Each of the first two types has a unique solution. The third type has either two or zero solutions. He provides an explicit algorithm to compute the solutions in each case.

2.2 The Quadratic Formula

The work of Al-Khwarizmi and other Arabic scholars was translated into Latin beginning in the 12th century and exerted a strong influence on the development of mathematics in Europe. The next major development in algebra was the solution of the general cubic equation by Italian scholars in the 16th century. (See the next chapter.) Meanwhile, there was slow progress in the development of a symbolic notation for the expression of "algorithms":

- The symbols $+$, $-$ and $\surd$ were introduced by German mathematicians in the late 1400s and early 1500s.
- The equals sign $=$ was introduced by Robert Recorde in *The Whetstone of Witte* (1557).[6]
- Francois Viète introduced letters for unknown quantities in his *Introduction to the Art of Analysis* (1591). He used vowels for unknowns and consonants for constants.
- René Descartes used the letters a, b, c for constants and x, y, z for variables in his *Geometry* (1637). In this work he also introduced the superscript notation x^y for exponents.

Descartes' *Geometry* is one of the most significant works in the history of mathematics. Because of its wide influence, it is also one of the earliest mathematical works that looks reasonable to modern eyes.

The benefit of symbolic notation is that it allows us to treat many separate geometric cases simultaneously. I refer to this phenomenon by the following slogan:

Algebra is smarter than geometry.

Let us now apply modern notation to the solution of quadratic equations. Let a, b, c represent any numbers with $a \neq 0$ and consider the equation

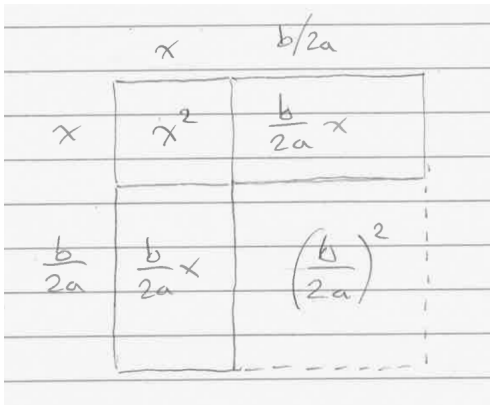
$$ax^2 + bx + c = 0.$$

[6]Here is his justification: *And to auoide the tediouse repetition of these woordes : is equalle to : I will sette as I doe often in woorke use, a paire of paralleles, or Gemowe lines of one lengthe, thus: =, bicause noe .2. thynges, can be moare equalle.*

Since $a \neq 0$ we may divide both sides by a to obtain

$$\begin{aligned} x^2 + \frac{b}{a}x + \frac{c}{a} &= 0 \\ x^2 + \frac{b}{a}x &= -\frac{c}{a} \\ x^2 + \frac{b}{2a}x + \frac{b}{2a}x &= -\frac{c}{a} \end{aligned}$$

This last step is inspired by the geometric trick of "completing the square":



The picture suggests that we should now add $(b/2a)^2$ to both sides, so the left hand side becomes equal to $(x + b/2a)^2$. Note that this algebraic identity is still true even in cases when the geometric picture makes no sense. Thus we have

$$\begin{aligned} x^2 + \frac{b}{2a}x + \frac{b}{2a}x &= -\frac{c}{a} \\ x^2 + \frac{b}{2a}x + \frac{b}{2a}x + \frac{b^2}{4a^2} &= -\frac{c}{a} + \frac{b^2}{4a^2} \\ \left(x + \frac{b}{2a}\right)^2 &= \frac{b^2 - 4ac}{4a^2}. \end{aligned}$$

Now what? Even though the quantity $b^2 - 4ac$ might be negative, let us **assume that there exists some number δ satisfying** $\delta^2 = b^2 - 4ac$. Then we also have

$$\left(\frac{\delta}{2a}\right)^2 = \frac{\delta^2}{4a^2} = \frac{b^2 - 4ac}{4a^2},$$

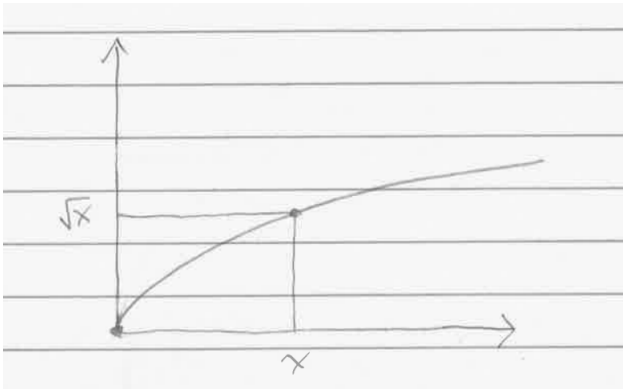
which allows us to solve for x as follows:

$$\left(x + \frac{b}{2a}\right)^2 = \frac{b^2 - 4ac}{4a^2}$$

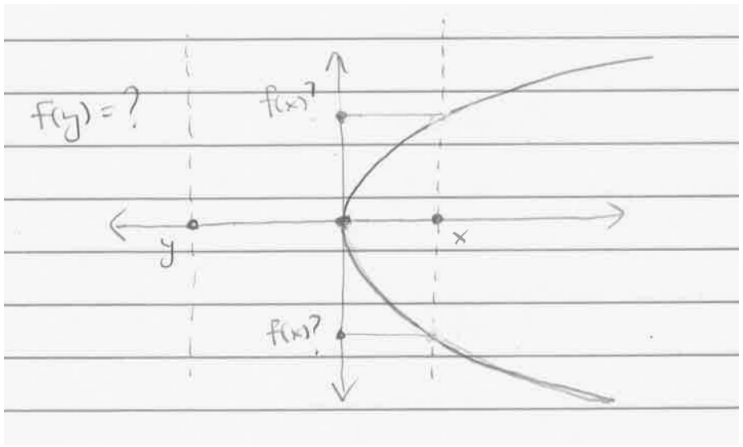
$$x + \frac{b}{2a} = \frac{\delta}{2a}$$
$$x = \frac{-b + \delta}{2a}.$$

Conversely, if δ is any number satisfying $\delta^2 = b^2 - 4ac$ then we can reverse all of these steps to show that the number $x = (-b + \delta)/2a$ satisfies the original equation $ax^2 + bx + c = 0$.

But what does this mean? I purposely avoided using the notation "$\sqrt{b^2 - 4ac}$" because this notation is ambiguous. We are accustomed to speaking about the "square root function" $f(x) = \sqrt{x}$, but this only defines a function if we restrict the domain and range to non-negative real numbers:



If we try to extend the domain and range to all real numbers then we find that negative numbers have no square roots, while positive numbers have two:



Later we will even see an exotic number system in which some numbers have infinitely many square roots! Because of these ambiguities I will state the following very carefully.

The Quadratic Formula

Let a, b, c be any numbers with $a \neq 0$ and consider the polynomial $f(x) = ax^2 + bx + c$. We define the *discriminant* of the polynomial as follows:

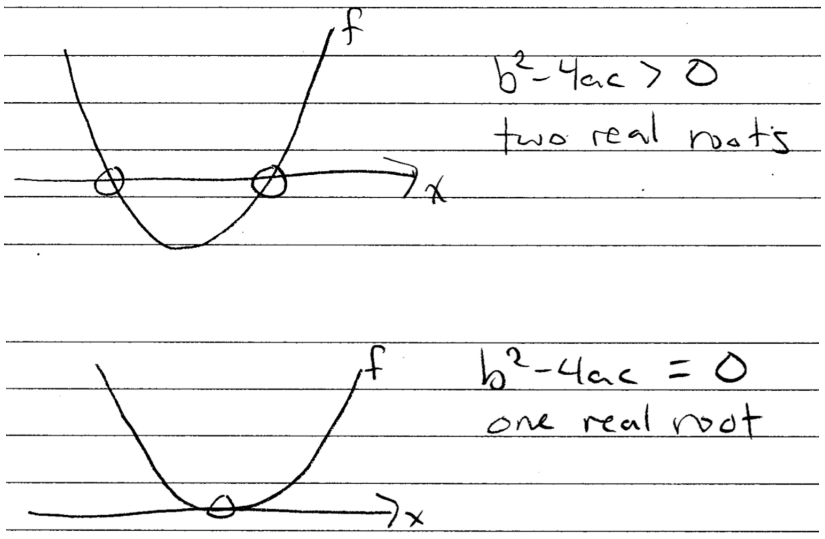
$$\Delta := b^2 - 4ac.$$

By the above reasoning we see that the equation $f(x) = 0$ has one solution $x = \frac{-b+\delta}{2a}$ for each square root of the discriminant: $\delta^2 = \Delta$. Depending on the number system, there may be zero, one or two such square roots. (Maybe even more.)

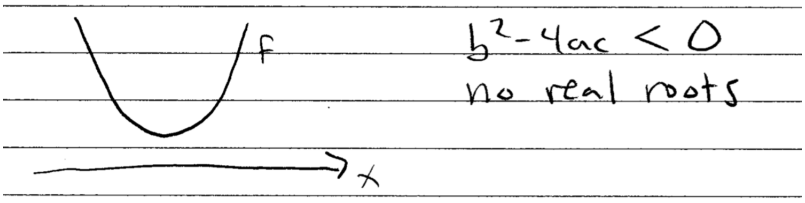
Of course, Descartes was only interested in the case when a, b, c are real numbers. In this case we can be more specific:

- The equation $f(x) = 0$ has two real solutions when $\Delta > 0$.
- The equation $f(x) = 0$ has one real solution when $\Delta = 0$.
- The equation $f(x) = 0$ has no real solutions when $\Delta < 0$.

We can illustrate each of these cases by drawing the graph of the function $f(x) = 0$ and observing where the graph intersects the x-axis (for these pictures we assume that $a > 0$):[7]



[7]Even though Descartes had a notion of coordinates (actually, one ordinate and one abscissa), he did not have the notion of functions and graphs. These conventions were standardized by Leonhard Euler in his *Introduction to the Analysis of the Infinite* (1748), over 100 years after Descartes.



It is a bit more difficult to determine whether these real roots are positive or negative. For this purpose Descartes came up with the following clever trick, which I will state without proof.

Descartes' Rule of Signs

Let $f(x)$ be a polynomial with real coefficients. Then the number of positive real solutions to the equation $f(x) = 0$ is at most the number of sign changes in the sequence of coefficients (omitting zero coefficients), or is less than this number by a multiple of 2.

For example, consider the equation $x^2+5x-2 = 0$, whose sequence of coefficients is $+1, +5, -2$. Since this sequence has one sign change we conclude that the equation has one positive real root. On the other hand, the coefficient sequence of the equation $x^2 - 5x + 2 = 0$ has two sign changes, so this equation has either two or zero positive real roots. [Which one is it?]

2.3 Does There Exist a Cubic Formula?

Inspired by our success with quadratic equations, we would like to find a formula for the roots of a general cubic equation:

$$ax^3 + bx^2 + cx + d = 0.$$

In other words, we would like to find some expression for x in terms of the coefficients a, b, c, d and the basic algebraic operations $+, -, \times, \div$. At some places in the formula we may also need to choose an arbitrary square root or a cube root of some expression.

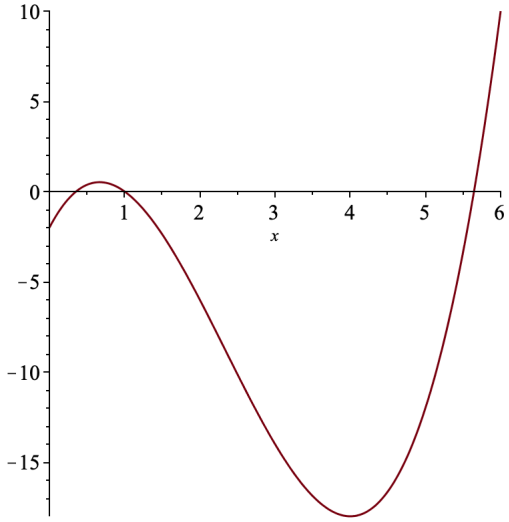
It turns out that such a formula does exist, but it is quite complicated. The formula was discovered in Italy during the 1500s and became known as "Cardano's formula." The reason it was not discovered earlier is because a geometric solution in the style of al-Khwarizmi would be far too complicated. The only efficient way to the solution is via symbolic algebra.

I will present Cardano's formula in Chapter 3, but first it is necessary to develop a better understanding of the abstract algebra of polynomials.

3 Rings, Fields, Polynomials

3.1 A Motivating Example

Consider the cubic polynomial $f(x) = x^3 - 7x^2 + 8x - 2$. By inspection we can see that $x = 1$ is a solution to the cubic equation $f(x) = 0$. Are there any other solutions? Consider the graph:



From this picture it appears that there are two more real solutions; one between 0 and 1 and the other between 5 and 6. It is always possible to find numerical approximations (for example, with Newton's method) but we would prefer to have exact formulas for these roots.

Descartes proved in his *Geometry* (1637) that if $x = 1$ is a solution of the polynomial equation $f(x) = 0$ then the polynomial $f(x)$ can be factored as $f(x) = (x-1)g(x)$, where $g(x)$ is some polynomial of one lower degree. We can find this polynomial by long division:

$$\begin{array}{r|l} & x^2 - 6x + 2 \\ \hline x - 1 & x^3 - 7x^2 + 8x - 2 \\ & -x^3 + x^2 \\ \hline & \quad -6x^2 + 8x \\ & \quad 6x^2 - 6x \\ \hline & \qquad 2x - 2 \\ & \qquad -2x + 2 \\ \hline & \qquad\quad 0 \end{array}$$

It follows that $f(x) = (x-1)g(x)$ where $g(x) = x^2 - 6x + 2$. Now suppose that $\alpha \neq 1$ is some other root of the equation $f(x) = 0$. By substitution we obtain

$$(\alpha - 1)g(\alpha) = f(\alpha) = 0.$$

Then since $(\alpha - 1) \neq 0$ we conclude that $g(\alpha) = 0$. Finally, we conclude from the quadratic formula that

$$\alpha = \frac{6 \pm \sqrt{36 - 8}}{2} = \frac{6 \pm \sqrt{28}}{2} = \frac{6 \pm 2\sqrt{7}}{2} = 3 \pm \sqrt{7}$$

In summary, we find that the polynomial $f(x) = x^3 - 7x^2 + 8x - 2$ has at least three roots: $x = 1$, $x = 3\sqrt{7}$ and $x = 3 - \sqrt{7}$. Could there be any others? It seems clear from the graph that there are no other real roots, but perhaps there is a complex root hiding somewhere? Or maybe a root in some more exotic number system?

Well, it depends on the type of number system. In the next section we will define a specific type of number system called a *field*. Later in this chapter we will prove the important theorem that "a polynomial of degree n with coefficients in a certain field can have at most n roots in that field."

3.2 Rings and Fields

I'm sure you are familiar with the following basic number systems:

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}.$$

To be a bit more specific:[8]

name	symbol	description
natural numbers	$\mathbb{N}$	$\{0, 1, 2, \ldots\}$
integers	$\mathbb{Z}$	$\{\ldots, -2, -1, 0, 1, 2, \ldots\}$
rational numbers	$\mathbb{Q}$	$\{a/b : a, b \in \mathbb{Z}, b \neq 0\}$
real numbers	$\mathbb{R}$	{limits of sequences of rational numbers}
complex numbers	$\mathbb{C}$	$\{a + b\sqrt{-1} : a, b \in \mathbb{R}\}$

But these descriptions are only intended to jog your memory; they do not count as formal definitions. In modern algebra (post-1930) it is necessary to define every concept in terms of formal axioms. The intuitive concept of "number system" is captured by the formal concept of a "ring" or a "field."

Definition of Rings

A *ring* is a set R together with two special elements $0, 1 \in R$ (called zero and one) and two binary operations $+, \cdot : R \times R \to R$ (called addition and multiplication), which satisfy the following eight axioms:

(A1) $\forall a, b \in R$, $a + b = b + a$ (commutative addition)

(A2) $\forall a, b, c \in R$, $a + (b + c) = (a + b) + c$ (associative addition)

[8] It is quite difficult to give a precise definition of real numbers. You will see such a thing in MTH 433 or 533, but it will not be important in this course.

(A3) $\forall a \in R,\ a + 0 = a$ (additive identity)

(A4) $\forall a \in R,\ \exists b \in R,\ a + b = 0$ (additive inversion)

(M1) $\forall a, b \in R,\ ab = ba$ (commutative multiplication)

(M2) $\forall a, b, c \in R,\ a(bc) = (ab)c$ (associative multiplication)

(M3) $\forall a \in R,\ a1 = a$ (multiplicative identity)

(D) $\forall a, b, c \in R,\ a(b + c) = ab + ac$ (distribution)

If we delete axiom (M1) then we obtain a structure called a *non-commutative ring*. In this course all rings will be commutative unless otherwise stated.

In other words, a ring is a number system in which any two numbers can be added or multiplied and in which all of the basic laws of arithmetic hold. Furthermore, axiom (A4) tells us that for any element $a \in R$ there exists at least one element $b \in R$ such that $a + b = 0$. I claim that this element is unique.

Proof. Suppose that we have $a + b = 0$ and $a + c = 0$ in a ring. It follows that

$$b = b + 0 = b + (a + c) = (b + a) + c = 0 + c = c.$$

□

Since the element is unique we should give it a name.

Subtraction in a Ring

Given any element $a \in R$ in a ring we have shown that there exists a unique element $b \in R$ satisfying $a + b = 0$. We will call this element *the additive inverse* of a and we will denote it by the symbol "$-a$." Then for any two elements $a, b \in R$ we define the notation

$$\text{“}a - b\text{”} := a + (-b).$$

The following "rules of signs" can be proved directly from the ring axioms:

$$(-a)b = -(ab) \qquad \textit{meno via più fa meno}$$
$$a(-b) = -(ab) \qquad \textit{più via meno fa meno}$$
$$(-a)(-b) = ab. \qquad \textit{meno via meno fa più}$$

These rules were first mentioned by Diophantus of Alexandria in the *Arithmetica* (3rd century AD). This work was unusual among all of Greek mathematics since it admitted the concept of negative numbers. Diophantus was translated in to Arabic shortly after the time of al-Khwarizmi and influenced the activities of Arabic mathematicians in the 10th and 11th centuries. The same rules appeared later in Italy in the works of Dardi of Pisa (1340s), Luca Pacioli (1494) and Rafael Bombelli (1572), who also translated Diophantus into Latin.[9] The abstract concept of a ring did not appear until the beginning of the twentieth century.

For example, the number systems $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are rings because they admit addition, subtraction and multiplication, whereas the number system $\mathbb{N}$ is not a ring because it does not admit subtraction. What about division?

Definition of Fields

Let $(\mathbb{F}, +, \cdot, 0, 1)$ be a ring.[10] We say that $\mathbb{F}$ is a *field* if it satisfies one further axiom:

$$\forall a \in \mathbb{F}\backslash\{0\},\ \exists b \in \mathbb{F},\ ab = 1.$$

In other words, a field is a (commutative) ring $\mathbb{F}$ in which for each nonzero element $a \in \mathbb{F}$ there exists at least one element $b \in \mathbb{F}$ satisfying $ab = 1$. Again, it is easy to show that this element is unique.

Proof. Suppose that we have $ab = 1$ and $ac = 1$ in a ring. It follows that

$$b = b1 = b(ac) = (ba)c = 1c = c.$$

□

Since the element is unique we should give it a name.

Division in a Field

Given any nonzero element $a \in \mathbb{F}$ in a field we have shown that there exists a unique element $b \in \mathbb{F}$ satisfying $ab = 1$. We will call this element *the multiplicative inverse* of a and we will denote it by the symbol "a^{-1}." Then for any two elements $a, b \in \mathbb{F}$ with

[9] Bombelli also played a prominent role in the introduction of complex numbers. See below.

[10] In this course I will tend to denote rings by R and fields by $\mathbb{F}$. The German word *Ring* was introduced by David Hilbert 1897. Some authors use A for a ring since the French term is *anneau*. Some authors use K for a field since the German term is *Körper* [body], introduced by Richard Dedekind in the 1870s. It is difficult to find good terminology for abstract mathematics.

$b \neq 0$ we define the notation

$$\text{“}\frac{a}{b}\text{”} := ab^{-1}.$$

For example, the rings $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are fields because they admit division by nonzero elements; whereas, I claim that the ring of integers $\mathbb{Z}$ is a **not** a field.

Proof. This follows from the fact that there are no integers “between” 0 and 1. For example, suppose for contradiction that there exists an integer $a \in \mathbb{Z}$ satisfying $2a = 1$ (i.e., suppose that we can divide by 2). It follows from this that $a > 0$ and therefore $a \geqslant 1$. But then multiplying both sides by 2 gives

$$\begin{aligned} a &\geqslant 1 \\ 2a &\geqslant 2 \\ 1 &\geqslant 2. \end{aligned}$$

Contradiction. □

Nevertheless, the integers are a very interesting and special ring We will have more to say about this in the next section.

3.3 Polynomials

The Greek approach to mathematics was *synthetic*, meaning that they would begin with known objects and then proceed to construct the desired thing. In contrast, the modern approach to mathematics is *analytic*, meaning that we first assume the hypothetical existence of the desired thing and then proceed to deduce its properties. Since Descartes' *Geometry* the desired thing in mathematics is usually denoted by x. But what is x really?

Definition of Polynomials

Let R be a ring and let x be an abstract symbol. By a *polynomial in x over R* we mean a formal expression of the form

$$f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \cdots = \sum_{k \geqslant 0} a_k x^k,$$

where the *coefficients* $a_0, a_1, a_2, \ldots$ are elements of R and only finitely many of these coefficients are nonzero. I want to emphasize that this expression is purely formal. For example, the symbol x^2 (invented by Descartes) does not mean $x \cdot x$ because x is not a number and therefore cannot be multiplied by anything.

Let us denote the set of all polynomials by

$$R[x] := \{\text{polynomials in } x \text{ over } R\}.$$

We can turn this set into a ring by pretending that x is a number and taking the abstract notation literally. To do this we first define the zero polynomial and the one polynomial:

$$0(x) := 0 + 0x + 0x^2 + 0x^3 + \cdots,$$
$$1(x) := 1 + 0x + 0x^2 + 0x^3 + \cdots.$$

Then for any polynomials $f(x) = \sum_{k\geqslant 0} a_k x^k$ and $g(x) = \sum_{k\geqslant 0} b_k x^k$ we define their sum and product as follows:

$$f(x) + g(x) := \sum_{k\geqslant 0} (a_k + b_k) x^k,$$

$$f(x) \cdot g(x) := \sum_{k\geqslant 0} \left(\sum_{i+j=k} a_i b_j \right) x^k.$$

One can check that the structure $(R[x], +, \cdot, 0(x), 1(x))$ satisfies the ring axioms, but we won't bother to do this. It is worth mentioning that for each element $a \in R$ of the base ring we can define the *constant polynomial*:

$$a(x) := a + 0x + 0x^2 + 0x^3 + \cdots.$$

This allows us to think of $R \subseteq R[x]$ a subset. In fact, we will call it a *subring*.

Don't worry too much about the details. As with all formal definitions, the definition of polynomials is only meant to formalize things that we already know; you should be okay if you just follow your intuition. The benefit of having a formal definition is that it allows us to be more precise.

It turns out that polynomials over a general ring can be quite complicated, but that polynomials over a field are very nice. In fact, there is a deep analogy between the ring of integers $\mathbb{Z}$ and the ring of polynomials $\mathbb{F}[x]$ over a field $\mathbb{F}$. The basic fact about these rings is that they both have a concept of "division with remainder." First I will state the theorem and then we'll discuss what it means.

The Division Theorem

For Integers: For all integers $a, b \in \mathbb{Z}$ with $b \neq 0$ there exist unique integers $q, r \in \mathbb{Z}$

(called the *quotient* and *remainder*) satisfying

$$\begin{cases} a = qb + r, \\ 0 \leqslant r < |b|. \end{cases}$$

For Polynomials Over a Field: Let $\mathbb{F}$ be a field. Then for all polynomials $f(x), g(x) \in \mathbb{F}[x]$ with $g(x) \neq 0(x)$ there exist unique polynomials $q(x), r(x) \in \mathbb{F}[x]$ (called the *quotient* and *remainder*) satisfying

$$\begin{cases} f(x) = q(x)g(x) + r(x), \\ \deg(r) < \deg(g). \end{cases}$$

Note that in each case the remainder must be in some sense "smaller" than the divisor. For integers we measure the size by the absolute value, while for polynomials we measure the size by the "degree," which is defined as follows.

Degree of a Polynomial

Let R be a ring and let $f(x) \in R[x]$ be a **nonzero** polynomial. Then there exists a unique integer $n \geqslant 0$ such that

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \quad \text{and} \quad a_n \neq 0,$$

in which case we say that $f(x)$ has *degree* n:

$$\deg(f) = n.$$

An important consequence of this definition is that

$$\deg(fg) = \deg(f) + \deg(g),$$

at least when $R = \mathbb{F}$ is a field.[11]

Proof. Suppose that $\deg(f) = m$ and $\deg(g) = n$, where $f(x)$ has leading term $a_m x^m$ and $g(x)$ has leading term $b_n x^n$. Since $a_m \neq 0$ and $b_n \neq 0$ we see that $a_m b_n \neq 0$. It follows that the leading term of the product $f(x)g(x)$ is $a_m b_n x^{m+n}$ and hence $\deg(fg) = m + n = \deg(f) + \deg(g)$. □

[11] The reason this doesn't hold for general rings is because there exist rings in which $a \neq 0$ and $b \neq 0$ do not necessarily imply $ab \neq 0$. Jargon: A ring R is called an *integral domain* if $a \neq 0$ and $b \neq 0$ always imply $ab \neq 0$. For example, $\mathbb{Z}$ is an integral domain.

For example, each nonzero constant polynomial $a(x)$ has degree 0. But what about the zero polynomial? Some authors say that the degree of $0(x)$ is undefined, but I prefer to say that

$$\deg(0) = \text{“}-\infty\text{.”}$$

This has the nice consequence that the formula $\deg(fg) = \deg(f) + \deg(g)$ is still “true” even when one or both of $f(x)$ and $g(x)$ is the zero polynomial. [Think about it!]

Now back to the Division Theorem. In each case (integers or polynomials) the proof of existence of the quotient and remainder is really an algorithm, called “long division.”[12] The formal statement of an algorithm is not very easy for humans to read so you can feel free to skip the proofs and go right to the examples.

Proof for Integers: Let $a, b \in \mathbb{Z}$ with $b \neq 0$ and consider the set

$$S = \{a - qb : q \in \mathbb{Z}\} = \{\ldots, a - 2b, a - b, a, a + b, a + 2b, \ldots\} \subseteq \mathbb{Z}.$$

Let r be the smallest non-negative element of this set. By definition we know that $a = qb + r$ for some integer $q \in \mathbb{Z}$ and we also know that $0 \leqslant r$. It remains only to show that $r < |b|$. So let us assume for contradiction that $r \geqslant |b|$. Since $b \neq 0$ this implies that

$$0 \leqslant r - |b| < r.$$

On the other hand, we observe that $r - |b| = (a - qb) - |b| = a - (q \pm 1)b \in S$. Thus we have found a non-negative element of S that is strictly smaller than r. Contradiction. □

Proof for Polynomials over a Field: Let $\mathbb{F}$ be a field and consider two polynomials $f(x), g(x) \in \mathbb{F}[x]$ with $g(x) \neq 0(x)$. Furthermore, consider the set

$$S = \{f(x) - q(x)g(x) : q(x) \in \mathbb{F}[x]\} \subseteq \mathbb{F}[x].$$

Let $r(x)$ be some element of S with **minimal degree** (allowing for the possibility that $r(x) = 0(x)$ and hence $\deg(0) = -\infty$). By definition we know that $f(x) = q(x)g(x) + r(x)$ for some $q(x) \in \mathbb{F}[x]$ and it remains only to show that $\deg(r) < \deg(g)$. So let us assume for contradiction that $\deg(r) \geqslant \deg(g)$. To be specific, since $g(x) \neq 0(x)$ we may write

$$g(x) = a_0 + a_1x + \cdots + a_mx^m \quad \text{and} \quad r(x) = b_0 + b_1x + \cdots + b_nx^n,$$

where a_m and b_n are nonzero elements of $\mathbb{F}$ and $m \leqslant n$. Then since $n - m \geqslant 0$ and $a_m \neq 0$ we may construct the following polynomial:[13]

$$h(x) := r(x) - \frac{b_n}{a_m}x^{n-m}g(x) = \left(b_n - \frac{b_n}{a_m}a_m\right)x^n + \text{ lower degree terms.}$$

[12] The uniqueness of the quotient and remainder is not important for us so I'll skip it.

[13] Here we are using the fact that $\mathbb{F}$ is a field.

Note that the coefficient of x^n in $h(x)$ is zero, and hence $\deg(h) < n = \deg(r)$. On the other hand, we observe that $h(x)$ is an element of S:

$$\begin{aligned} h(x) &= r(x) - \frac{b_n}{a_m} x^{n-m} g(x) \\ &= (f(x) - q(x)g(x)) - \frac{b_n}{a_m} x^{n-m} g(x) \\ &= f(x) - \left(q(x) + \frac{b_n}{a_m} x^{n-m} \right) g(x) \in S. \end{aligned}$$

Thus $h(x)$ is an element of S with strictly smaller degree than $r(x)$. Contradiction. □

I assume that you're familiar with long division of integers, so let's look at an example of polynomial long division. Consider the following polynomials in the ring $\mathbb{Z}[x]$:

$$\begin{aligned} f(x) &= 2x^5 - 6x^4 + 5x^3 - 2x^2 + 3x + 1, \\ g(x) &= 2x^2 + 1. \end{aligned}$$

Here is a picture of the algorithm:

$$\begin{array}{rr} & x^3 - 3x^2 + 2x + \frac{1}{2} \\ \cline{2-2} 2x^2 + 1 \big) & 2x^5 - 6x^4 + 5x^3 - 2x^2 + 3x + 1 \\ & \underline{-2x^5 \qquad - x^3} \\ & -6x^4 + 4x^3 - 2x^2 \\ & \underline{6x^4 \qquad + 3x^2} \\ & 4x^3 + x^2 + 3x \\ & \underline{-4x^3 \qquad - 2x} \\ & x^2 + x + 1 \\ & \underline{-x^2 \qquad - \frac{1}{2}} \\ & x + \frac{1}{2} \end{array}$$

In words: We initialize by setting $f_0(x) = f(x)$. Then we cancel the leading term of $f_0(x)$ by subtracting x^3 times the divisor:

$$f_1(x) = f_0(x) - x^3 g(x) = -6x^4 + 4x^3 - 2x^2 + 3x + 1.$$

Next we cancel the leading term of $f_1(x)$ by subtracting $-3x^2$ times the divisor:

$$f_2(x) = f_1(x) - (-3x^2)g(x) = 4x^3 + x^2 + 3x + 1.$$

We continue by cancelling the leading term of $f_2(x)$ as follows:

$$f_3(x) = f_2(x) - 2xg(x) = x^2 + x + 1.$$

But now we are stuck. It is impossible to cancel the leading term of $f_3(x) = x^2 + x + 1$ while remaining inside the ring $\mathbb{Z}[x]$ because it is impossible to divide by 2 inside the ring $\mathbb{Z}$. We

may continue, however, if we pass to the larger ring $\mathbb{Q}[x]$. Then we may cancel the leading term of $f_3(x)$ by subtracting $1/2$ times the divisor:

$$f_4(x) = f_3(x) - \frac{1}{2}g(x) = x + \frac{1}{2}.$$

Note that the degrees of the polynomials f_0, f_1, f_2, f_3, f_4 are decreasing. Finally, since the degree of $f_4(x)$ is less than the degree of the divisor $g(x)$, the algorithm stops.

This example illustrates why it is better to consider polynomials with coefficients from a field. If we regard $f(x)$ and $g(x)$ as elements of $\mathbb{Z}[x]$ then there is no quotient and remainder. However, if we regard $f(x)$ and $g(x)$ as elements of $\mathbb{Q}[x] \supseteq \mathbb{Z}[x]$, then we obtain the following (unique) quotient and remainder:

$$q(x) = x^3 - 3x^2 + 2x - \frac{1}{2},$$
$$r(x) = x + \frac{1}{2}.$$

In other words, have

$$2x^5 - 6x^4 + 5x^3 - 2x^2 + 3x + 1 = \left(x^3 - 3x^2 + 2x - \frac{1}{2}\right)(2x^2 + 1) + \left(x + \frac{1}{2}\right)$$

The same result holds in $\mathbb{R}[x]$, or $\mathbb{C}[x]$, or in any ring $\mathbb{F}[x]$ where $\mathbb{F}$ is a field containing $\mathbb{Z}$ as a subring.

I probably should have done the Euclidean algorithm right here, and Bézout's Identity should have been on the first homework. Oh well.

3.4 Descartes' Factor Theorem

In this section we will discuss the first true theorem of algebra, which appeared in the third book of Descartes' *Geometry* (1637). The theorem concerns the relationship between the roots of a polynomial and its factorization into polynomials of lower degree. In modern terms, it relates the concept of a "polynomial function" to the concept of polynomials as formal expressions. Before stating the theorem, let me be clear about this distinction.

Evaluation and Roots of Polynomials

We have defined a polynomial $f(x) \in \mathbb{F}[x]$ as an abstract expression of the form

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n.$$

But, as you know, this abstract expression can also be used to define a function $f : \mathbb{F} \to \mathbb{F}$, taking numbers to numbers. To be precise, for each number $\alpha \in \mathbb{F}$ we define the number

$f(\alpha) \in \mathbb{F}$ by *evaluating the polynomial at* $x = \alpha$:

$$f(\alpha) := a_0 + a_1\alpha + \cdots + a_n\alpha^n \in \mathbb{F}.$$

If $f(\alpha) = 0$ then we say that $\alpha \in \mathbb{F}$ is a *root* of the polynomial $f(x) \in \mathbb{F}[x]$.

If two polynomials $f(x), g(x) \in \mathbb{F}[x]$ are equal as abstract expressions (i.e., if they the same coefficients) then they clearly determine the same function (i.e., $f(\alpha) = g(\alpha)$ for all $\alpha \in \mathbb{F}$). The other direction is not true in general.[14] However, you will prove the following result on the homework: If $f(\alpha) = g(\alpha)$ for all $\alpha \in \mathbb{F}$ and if the field $\mathbb{F}$ has **infinitely many elements**, then it follows that the polynomials $f(x)$ and $g(x)$ have exactly the same coefficients. Descartes did not distinguish between polynomial functions and formal polynomials because he always worked over the infinite field $\mathbb{Q}$.

Now here is Descartes' Theorem in modern language.

Descartes' Factor Theorem (1637)

Let $\mathbb{F}$ be a field.

I. Let $f(x) \in \mathbb{F}[x]$ be a nonzero polynomial of degree $n \geqslant 1$. Then for any number $\alpha \in \mathbb{F}$ we have $f(\alpha) = 0$ if and only if $f(x) = (x - \alpha)g(x)$ for some polynomial $g(x) \in \mathbb{F}[x]$ of degree $n - 1$. In other words:

$$\left\{ \begin{array}{c} \alpha \in \mathbb{F} \text{ is a } \textit{root} \\ \text{of } f(x) \in \mathbb{F}[x] \end{array} \right\} \iff \left\{ \begin{array}{c} f(x) \text{ is } \textit{divisible} \text{ by } (x - \alpha) \\ \text{in the ring } \mathbb{F}[x] \end{array} \right\}.$$

II. Any polynomial $f(x) \in \mathbb{F}[x]$ of degree $n \geqslant 0$ has at most n distinct roots in $\mathbb{F}$.

Before giving the proof, let me show you a consequence. In section 3.1 we found that the polynomial $x^2 - 6x + 2$ has two real roots: $x = 3 + \sqrt{7}$ and $x = 3 - \sqrt{7}$. Since this polynomial has degree 2 it follows from Decartes' theorem that there are no other real roots. More generally, if $\mathbb{F}$ is **any field** containing the coefficients $1, -6, 2$ and the real numbers $3 \pm \sqrt{7}$ then Descartes' theorem tells us that there can be no other roots in this field. That's comforting, I guess.

Let me also show you an example to preview the main idea of the proof. Consider the polynomial $f(x) = x^3 + x^2 - x + 1$ with coefficients in, say, $\mathbb{Q}$. Note that the number $2 \in \mathbb{Q}$ is **not** a root of $f(x)$ because

$$f(2) = 2^3 + 2^2 - 2 + 1 = 8 + 4 - 1 + 1 = 11 \neq 0.$$

[14] We will see later that there exist fields with **finitely many elements**, in which case the converse is false.

According to the theorem, this means that $f(x)$ divided by $x-2$ in $\mathbb{Q}[x]$ must have a **nonzero** remainder. Let's check:

$$\begin{array}{r|l} & x^2+3x+5 \\ \hline x-2 & x^3+x^2-x+1 \\ & -x^3+2x^2 \\ \hline & 3x^2-x \\ & -3x^2+6x \\ \hline & 5x+1 \\ & -5x+10 \\ \hline & 11 \end{array}$$

Indeed, we find that the remainder is the constant polynomial 11. Where have we seen this number before? That's right, the remainder of $f(x)$ when divided by $x-2$ is equal to the constant polynomial $f(2)$. Since $f(2) \neq 0$ it follows that $f(x)$ is not divisible by the polynomial $x-2$. We will see that the same thing holds in general.

Proof of Descartes' Factor Theorem.

Part I. First suppose that $f(x) = (x-\alpha)g(x)$ for some polynomial $g(x) \in \mathbb{F}[x]$. By evaluating at $x = \alpha$ we find that

$$f(\alpha) = (\alpha - \alpha)g(\alpha) = 0 \cdot g(\alpha) = 0.$$

Conversely, suppose that $f(x) \in \mathbb{F}[x]$ has degree $n \geqslant 1$ and consider any number $\alpha \in \mathbb{F}$. Now let us divide $f(x)$ by the degree-one polynomial $x - \alpha$. From the Division Theorem we know that there exist (unique) polynomials $q(x), r(x) \in \mathbb{F}[x]$ satisfying

$$f(x) = q(x)(x-\alpha) + r(x),$$

and such that $\deg(r) < \deg(x-\alpha) = 1$. In particular, we must have $\deg(r) = 0$ (i.e., $r(x)$ is a nonzero constant) or $\deg(r) = -\infty$ (i.e., $r(x)$ is the zero polynomial). So let us write

$$f(x) = q(x)(x-\alpha) + c \quad \text{for some constant } c \in \mathbb{F}.$$

By substituting $x = \alpha$ we obtain

$$\begin{aligned} f(x) &= q(x)(x-\alpha) + c \\ f(\alpha) &= q(\alpha)(\alpha-\alpha) + c \\ f(\alpha) &= q(\alpha) \cdot 0 + c \\ f(\alpha) &= c, \end{aligned}$$

and hence

$$\boxed{f(x) = q(x)(x-\alpha) + f(\alpha).}$$

(You will give an alternate proof of this formula on the homework.) Finally, if α is a root of $f(x)$ then we fiund that $f(x) = q(x)(x-\alpha) + 0$ for some polynomial $q(x) \in \mathbb{F}[x]$. To see that this polynomial satisfies $\deg(q) = n-1$ we observe that

$$\deg(f) = \deg(q) + \deg(x-\alpha)$$

$$\begin{aligned} n &= \deg(q) + 1 \\ n - 1 &= \deg(q). \end{aligned}$$

Part II. We will prove by induction on n that any polynomial in $\mathbb{F}[x]$ of degree $n \geqslant 0$ has at most n distinct roots in $\mathbb{F}$. For the base case we note that a polynomial of degree $n = 0$ is just a nonzero constant polynomial, which of course has no roots. Now fix some $n \geqslant 0$ and **assume for induction** that every polynomial in $\mathbb{F}[x]$ of degree n has at most n roots in $\mathbb{F}$. In this case we will show that every polynomial of degree $n + 1$ has at most $n + 1$ roots. So consider some $f(x) \in \mathbb{F}[x]$ with degree n. If $f(x)$ has no roots in $\mathbb{F}$ then we are done, so let us suppose that $f(\alpha) = 0$ for some $\alpha \in \mathbb{F}$. From **Part I** we have

$$f(x) = (x - \alpha)g(x) \quad \text{for some } g(x) \in \mathbb{F}[x] \text{ of degree } n.$$

Now let $\beta \in \mathbb{F}$ be any number with $f(\beta) = 0$ and $\beta \neq \alpha$. By substitution we obtain

$$\begin{aligned} f(x) &= (x - \alpha)g(x) \\ f(\beta) &= (\beta - \alpha)g(\beta) \\ 0 &= (\beta - \alpha)g(\beta), \end{aligned}$$

which implies that $g(\beta) = 0$ because $\beta - \alpha \neq 0$. In other words, any root of $f(x)$ that is not equal to α must be a root of $g(x)$. But since $\deg(g) = n$ we know by induction that $g(x)$ has at most n distinct roots in $\mathbb{F}$. It follows that $f(x)$ has at most $n + 1$ roots in $\mathbb{F}$. □

For example, let's consider again the polynomial $f(x) = x^3 - 7x^2 + 8x - 2 \in \mathbb{Q}[x]$.[15] By inspection we see that $1 \in \mathbb{Q}$ is a root, and then by long division we obtain

$$f(x) = (x - 1)g(x) = (x - 1)(x^2 - 6x + 2).$$

Next let $\alpha \in \mathbb{F} \supseteq \mathbb{Q}$ be any element of an extension field and assume that $f(\alpha) = 0$ so that

$$0 = f(\alpha) = (\alpha - 1)g(\alpha).$$

If $\alpha \neq 1$ then it follows that $g(\alpha) = 0$, and the quadratic formula gives two possible solutions:

$$\alpha = \frac{6 \pm \sqrt{36 - 8}}{2} = 3 \pm \sqrt{7}.$$

These roots do not exist in $\mathbb{Q}$[16] however they do exist in the field of real numbers $\mathbb{R}$. In particular we have $g(3 + \sqrt{7}) = 0$, so Descartes' Theorem in $\mathbb{R}[x]$ tells us that

$$g(x) = \left(x - (3 + \sqrt{7})\right) h(x)$$

[16] We have not proved this, but you probably know from a previous course that $\sqrt{d}$ is an irrational real number whenever $d \in \mathbb{Z}$ and $d^2 \notin \mathbb{Z}$.

for some polynomial $h(x) \in \mathbb{R}[x]$ of degree 1. Next we can substitute $x = 3 - \sqrt{7}$ to obtain

$$0 = g(3-\sqrt{7}) = \left(3 - \sqrt{7} - (3+\sqrt{7})\right) h(3-\sqrt{7}) = 2\sqrt{7} \cdot h(3-\sqrt{7}),$$

which implies that $h(3-\sqrt{7}) = 0$. From one final application of Descartes' Theorem in $\mathbb{R}[x]$ we obtain

$$h(x) = (x - (3-\sqrt{7}))p(x),$$

where $p(x) \in \mathbb{R}[x]$ is a polynomial of degree 0 with real coefficients, i.e., $p(x) = c \in \mathbb{R}$ is a nonzero constant.[17] In summary we have shown that

$$f(x) = (x-1)\left(x - (3+\sqrt{7})\right)\left(x - (3-\sqrt{7})\right)c.$$

Could there possibly be another root somewhere? Let $\mathbb{F} \supseteq \mathbb{R}$ be any field containing $\mathbb{R}$ and suppose that we have $f(\alpha) = 0$ for some number $\alpha \in \mathbb{F}$ not equal to 1 or $3 \pm \sqrt{7}$. By substitution this would imply

$$0 = f(\alpha) = (\alpha - 1)\left(\alpha - (3+\sqrt{7})\right)\left(\alpha - (3-\sqrt{7})\right)c.$$

But this is **impossible**, because the four factors on the right are all **nonzero** elements of the hypothetical field $\mathbb{F}$. We conclude that the polynomial $f(x)$ has at most 3 roots in any field.

We found that the polynomial $f(x) = x^3 - 7x^2 + 8x - 2$ can be completely factored in the ring $\mathbb{R}[x]$, but not in the ring $\mathbb{Q}[x]$. This inspires the following definition.

Definition of Splitting

Consider a polynomial $f(x) \in \mathbb{F}[x]$ over a field $\mathbb{F}$ and let $\mathbb{E} \supseteq \mathbb{F}$ be any field containing $\mathbb{F}$ as a subring. (For example, let $\mathbb{E} = \mathbb{R}$ be the real numbers and and $\mathbb{F} = \mathbb{Q}$ the rational numbers.) We say that the polynomial $f(x) \in \mathbb{F}[x]$ *splits over* $\mathbb{E}$ if there exist some elements $c, \alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{E}$ such that

$$f(x) = c(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n).$$

In other words, we say that $f(x) \in \mathbb{F}[x]$ splits over $\mathbb{E}$ if it "has all of its roots" in $\mathbb{E}$.

For example, the polynomial x^2 splits over any field:

$$x^2 = (x-0)(x-0).$$

[16] Of course, this polynomial also lives in the ring $\mathbb{Z}[x]$, but I prefer to use $\mathbb{Q}$ because it is a field.

[17] By comparing coefficients on each side we see that $c = 1$, but this is not so important right now.

The polynomial $x^2 - 2 \in \mathbb{Q}[x]$ **does not** split over $\mathbb{Q}$ but it **does** split over $\mathbb{R}$:

$$x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2}).$$

And the polynomial $x^2 + 1 \in \mathbb{Q}[x]$ **does not** split over $\mathbb{Q}$ or $\mathbb{R}$, but it **does** split over $\mathbb{C}$:

$$x^2 + 1 = (x - \sqrt{-1})(x + \sqrt{-1}).$$

The complex numbers were not well understood in the time of Descartes. In fact, they were not fully accepted as numbers until the beginning of the 19th century. Later in this course we will prove the following important result, called the *fundamental theorem of algebra*, which is surprisingly difficult to prove:

Every polynomial with coefficients in $\mathbb{C}$ splits over $\mathbb{C}$.

4 Unique Prime Factorization

I should go back and rewrite the following sections in the language of Euclidean domains to save space. Need to define integral domains, Euclidean domains first. Maybe even mention "Gauss' Lemma" at the end of this chapter.

4.1 Euclidean Domains

4.2 Existence of Prime Factorization

Before moving on, there is one more property of formal polynomials that I need to mention. We saw above that the ring of integers $\mathbb{Z}$ and the ring of polynomials $\mathbb{F}[x]$ over a field $\mathbb{F}$ are similar in that they both have a notion of "division with remainder." It follows from this similarity that each ring also has a notion of "unique prime factorization."

First let me define what I mean by "prime."[18]

Definition of Prime Elements

For Integers: We say that an integer $n \in \mathbb{Z}$ is *prime* if:

- We have $|n| \geqslant 2$.
- For all integers $k, \ell \in \mathbb{Z}$ we have

$$n = k\ell \quad \Rightarrow \quad |k| = 1 \text{ or } |\ell| = 1.$$

[18]The concept defined here is called *irreducibility*. In general ring theory there is a distinction between primality and irreducibility, but for our purposes the two notions are the same, and I like the word "prime" better because it has fewer syllables.

For Polyomials over a Field: Let $\mathbb{F}$ be a field and consider a polynomial $f(x) \in \mathbb{F}[x]$. We say that this polynomial is *prime* if:

- We have $\deg(f) \geqslant 1$.
- for all polynomials $h(x), g(x) \in \mathbb{F}[x]$ we have

$$f(x) = g(x)h(x) \quad \Rightarrow \quad \deg(g) = 0 \text{ or } \deg(h) = 0.$$

For example, the integer $5 \in \mathbb{Z}$ is prime because it can only be factored in silly ways:

$$5 = 5 \cdot 1 = (-5)(-1) = 1 \cdot 5 = (-1)(-5).$$

Next we observe that the polynomial $x - 6 \in \mathbb{Q}[x]$ is a prime element of the ring $\mathbb{Q}[x]$. To see this, suppose that we have

$$x - 6 = g(x)h(x) \quad \text{for some polynomials } g(x), h(x) \in \mathbb{Q}[x].$$

Since $x - 6 \neq 0(x)$ we see that $g(x) \neq 0(x)$ and $h(x) \neq 0(x)$. Then comparing degrees gives

$$1 = \deg(x - 2) = \deg(g) + \deg(h),$$

which implies that we must have $\deg(g) = 0$ or $\deg(h) = 0$. Thus $x - 6$ has no "non-trivial factorization." On the other hand, recall that a polynomial of degree 0 is the same thing as a nonzero constant. Thus we have infinitely many "trivial factorizations":

$$x - 6 = \frac{1}{\alpha}(\alpha x - 6\alpha) \quad \text{for any non-zero constant } \alpha \in \mathbb{Q}.$$

If an element is **not prime** then we can always split it into a product of primes.

Existence of Prime Factorization

For Integers: For any integer $n \in \mathbb{Z}$ satisfying $n \geqslant 2$, there exist prime integers $p_1, \ldots, p_k \in \mathbb{Z}$ such that[19]

$$n = p_1 p_2 \cdots p_k.$$

For Polynomials over a Field: For any polynomial $f(x) \in \mathbb{F}[x]$ satisfying $\deg(f) \geqslant 1$, there exist prime polynomials $p_1(x), \ldots, p_k(x) \in \mathbb{F}[x]$ such that

$$f(x) = p_1(x)p_2(x) \cdots p_k(x).$$

[19]Let me remark that $k = 1$ is a valid option here. For example, $2 = 2$ is a product of just one prime. Some students disagree with this, but it is a well-established mathematical convention.

In each case the proof is by induction.

Proof for Integers: Suppose that $2 = k\ell$, hence $2 = |k||\ell|$. Since k and ℓ are both nonzero we must have $1 \leqslant |k| \leqslant 2$ and $1 \leqslant |\ell| \leqslant 2$. But then $|k| = 2$ implies $|\ell| = 1$ and if $2 = |k||\ell|$ implies $|k| = 1$. It follows that 2 is prime; in particular, 2 is a product of primes (itself times no other primes). Now fix some $n \geqslant 3$ and assume for induction that every number strictly between 1 and n is a product of primes. If n is itself prime then we are done. Otherwise, we have by definition that

$$n = k\ell \text{ for some } k, \ell \in \mathbb{Z} \text{ with } 1 < k < n \text{ and } 1 < \ell < n.$$

Since each of k and ℓ is smaller than n we may assume by induction that each of k and ℓ is a product of primes; say $k = p_1 \cdots p_r$ and $\ell = q_1 \cdots q_s$. We conclude that n is a product of primes:

$$n = k\ell = p_1 \cdots p_r q_1 \cdots q_s.$$

□

Proof for Polynomials over a Field: Consider a polynomial $f(x) \in \mathbb{F}[x]$ of degree 1 and suppose that we can write $f(x) = g(x)h(x)$ for some $g(x), h(x) \in \mathbb{F}[x]$. Since $g(x) \neq 0(x)$ and $h(x) \neq 0(x)$ we must have $\deg(g) \geqslant 0$ and $\deg(h) \geqslant 0$. But then comparing degrees gives

$$1 = \deg(f) = \deg(g) + \deg(h),$$

which implies that $\deg(g) = 0$ or $\deg(h) = 0$. It follows that $f(x)$ is prime; in particular $f(x)$ is a product of primes (itself times no other primes). Now fix some $n \geqslant 2$ and assume for induction that every polynomial with degree strictly between 0 and n is a product of primes. Our goal is to show that every polynomial of degree n is a product of primes. So consider any $f(x) \in \mathbb{F}[x]$ of degree n. If $f(x)$ is itself prime then we are done. Otherwise, we have by definition that

$$f(x) = g(x)h(x) \text{ for some } g(x), h(x) \in \mathbb{F}[x] \text{ satisfying } 0 < \deg(g) < n \text{ and } 0 < \deg(h) < n.$$

It follows by induction that each of $g(x)$ and $h(x)$ is a product of primes; say $g(x) = p_1(x) \cdots p_r(x)$ and $h(x) = q_1(x) \cdots q_s(x)$. We conclude that $f(x)$ is a product of primes:

$$f(x) = p_1(x) \cdots p_r(x) q_1(x) \cdots q_s(x).$$

□

In the next two sections we will prove that this factorization into primes is "essentially unique."

4.3 Bézout's Identity

Use the Euclidean algorithm.

4.4 Euclid's Lemma

In order to make the proof of unique factorization cleaner we will isolate the hardest part inside of inside a lemma. This result is commonly called Euclid's Lemma because it appeared in Book VII of the *Elements* (circa 300 BC), written by Euclid of Alexandria. Carl Friedrich Gauss extended the result to certain kinds of polynomials in his *Disquisitiones Arithmeticae* (1801) and the general version developed from there.

First we define the concept of "coprime elements."

Definition of Coprime Elements

For Integers: Given $d, a \in \mathbb{Z}$ we say that d *divides* a, and we write "$d|a$," when there exists some integer $q \in \mathbb{Z}$ such that $a = dq$. Then for any $a, b \in \mathbb{Z}$, not both zero, we say that $d \in \mathbb{Z}$ is the *greatest common divisor* of a and b, and write $d = \gcd(a, b)$, when

- $d \geqslant 1$,
- $d|a$ and $d|b$,
- $c|a$ and $c|b$ imply $c|d$.

We say that $a, b \in \mathbb{Z}$ are *coprime* when $\gcd(a, b) = 1$.

For Polynomials over a Field: Given $d(x), f(x) \in \mathbb{F}[x]$ we say that $d(x)$ *divides* $f(x)$, and we write "$d(x)|f(x)$," when there exists some $q(x) \in \mathbb{F}[x]$ such that $f(x) = d(x)q(x)$. Then for any $f(x), g(x) \in \mathbb{F}[x]$, not both the zero polynomial, we say that $d(x) \in \mathbb{F}[x]$ is the *greatest common divisor* of $f(x)$ and $g(x)$, and we write $d(x) = \gcd(f, g)$, when

- $d(x)$ has leading coefficient 1,
- $d(x)|f(x)$ and $d(x)|g(x)$,
- $h(x)|f(x)$ and $h(x)|g(x)$ imply $h(x)|d(x)$.

We say that $f(x), g(x) \in \mathbb{F}[x]$ are *coprime* when $\gcd(f, g) = 1$.

This definition implies that the greatest common divisor in each case is **unique**. Let us verify that this is, indeed, the case.

Proof. Firist, consider some $a, b \in \mathbb{Z}$ and suppose that $d, e \in \mathbb{Z}$ both satisfy the conditions of $\gcd(a, b)$. Thus we have $d \geqslant 1$ and $e \geqslant 1$, with $d|e$ and $e|d$. Let's say $e = dk$ and $d = e\ell$ for some $k, \ell \in \mathbb{Z}$. It follows from this that

$$d = e\ell$$

$$d = dk\ell$$
$$d(1 - k\ell) = 0.$$

Since $d \neq 0$ this implies that $1 - k\ell = 0$ and hence $k\ell = 1$. Then this implies that $k = \ell = \pm 1$ and hence $d = \pm e$. Finally, since $d \geqslant 1$ and $e \geqslant 1$ we conclude that $d = e$.

Next, consider some $f(x), g(x) \in \mathbb{F}[x]$ and suppose that $d(x), e(x) \in \mathbb{F}[x]$ both satisfy the conditions of $\gcd(f, g)$. Thus $d(x)$ and $e(x)$ both have leading coefficient 1, with $d(x)|e(x)$ and $e(x)|d(x)$. Let's say $e(x) = d(x)s(x)$ and $d(x) = e(x)t(x)$ for some $s(x), t(x) \in \mathbb{F}[x]$. It follows from this that

$$d(x) = e(x)t(x)$$
$$d(x) = d(x)s(x)t(x)$$
$$d(x)\left[1 - s(x)t(x)\right] = 0.$$

Since $d(x) \neq 0$ this implies that $1 - s(x)t(x) = 0$ and hence $s(x)t(x) = 1$. Then this implies that $s(x)$ and $t(x)$ are both constant, hence $d(x) = ce(x)$ for some $c \in \mathbb{F}$. Finally, since $d(x)$ and $e(x)$ both have leading coefficient 1 we conclude that $d(x) = e(x)$. □

Euclid's Lemma

For Integers: For all integers $n, a, b \in \mathbb{Z}$, we have

$$n|ab \quad \text{and} \quad \gcd(n, a) = 1 \quad \Rightarrow \quad n|b.$$

For all integers $p, a, b \in \mathbb{Z}$, with p prime, we have

$$p|ab \quad \text{and} \quad p \nmid a \quad \Rightarrow \quad p|b.$$

For Polynomials over a Field: For all polynomials $h(x), f(x), g(x) \in \mathbb{F}[x]$ we have

$$h(x)|f(x)g(x) \quad \text{and} \quad \gcd(h, f) = 1 \quad \Rightarrow \quad h(x)|g(x).$$

For all polynomials $p(x), f(x), g(x) \in \mathbb{F}[x]$, with $p(x)$ prime, we have

$$p(x)|f(x)g(x) \quad \text{and} \quad p(x) \nmid f(x) \quad \Rightarrow \quad p(x)|g(x).$$

The following proof is missing one important detail (Bézout's Identity), which you will complete on the homework.

Proof for Integers: Consider $n, a, b \in \mathbb{Z}$ with $\gcd(n, a) = 1$. You will show on the homework that there exist some $x, y \in \mathbb{Z}$ such that $nx + ay = 1$ (Bézout's Identity). Now if $n|ab$ then by

definition we have $ab = nq$ for some $q \in \mathbb{Z}$. It follows that

$$\begin{aligned} 1 &= nx + ay \\ b &= nbx + aby \\ b &= nbx + nqy \\ b &= n(bx + qy), \end{aligned}$$

and hence $n|b$. If $p \in \mathbb{Z}$ is prime with $p \nmid a$ then I claim that $\gcd(p, a) = 1$. Indeed, let $d = \gcd(p, a)$. Since p is prime with $d|p$ and $d \geqslant 1$ we must have $d = 1$ or $d = p$. Then since $d|a$ and $p \nmid a$ we must have $d = 1$. □

Proof for Polynomials over a Field: Consider $h(x), f(x), b(x) \in \mathbb{F}[x]$ with $\gcd(h, f) = 1$. You will show on the homework that there exist some $s(x), t(x) \in \mathbb{F}[x]$ such that $h(x)s(x) + f(x)t(x) = 1$ (Bézout's Identity). Now if $h(x)|f(x)g(x)$ then by definition we have $f(x)g(x) = h(x)q(x)$ for some $q(x) \in \mathbb{F}[x]$. It follows that

$$\begin{aligned} 1 &= h(x)s(t) + f(x)t(x) \\ g(x) &= h(x)g(x)s(x) + f(x)g(x)t(x) \\ g(x) &= h(x)g(x)s(x) + h(x)q(x)t(x) \\ g(x) &= h(x)\left[g(x)s(x) + q(x)t(x)\right], \end{aligned}$$

and hence $h(x)|g(x)$. If $p(x) \in \mathbb{F}[x]$ is prime with $p(x) \nmid f(x)$ then I claim that $\gcd(p, f) = 1$. Indeed, let $d(x) = \gcd(p, f)$. Since $p(x)$ is prime with $d(x)|p(x)$ and since $d(x)$ has leading coefficient 1 we must have $d(x) = 1$ or $d(x) = cp(x)$ for some nonzero constant $c \in \mathbb{F}$. Then since $d(x)|f(x)$ and $p(x) \nmid f(x)$ we must have $d(x) = 1$. □

For example, it is easy to see that this result is true when $p = 2$. Indeed, suppose that $2|ab$ and $2 \nmid a$ for some integers $a, b \in \mathbb{Z}$. Thus ab is even and a is odd. Then it must be the case that b is even, hence $2|b$. However, the same result does **not** hold for $p = 4$. For example, we have $4|6 \cdot 10$ even though $4 \nmid 6$ and $4 \nmid 10$. This can happen because 4 is not prime.

4.5 Uniqueness of Prime Factorization

We are now ready to consider the uniqueness of prime factorization. In order to determine exactly what this should mean, we need to look at an example of each type. First, we observe that the integer $12 \in \mathbb{Z}$ can be factored in infinitely many ways:

$$\begin{aligned} 12 &= 2 \cdot 2 \cdot 3 \\ &= 2 \cdot 3 \cdot 2 \\ &= 3 \cdot 2 \cdot 2 \\ &= (-3) \cdot 2 \cdot (-2) \\ &= (-3) \cdot (-2) \cdot 2 \cdot 1 \end{aligned}$$

$$= 3 \cdot 2 \cdot (-2) \cdot (-1) \cdot 1 \cdot 1 \cdot 1.$$

We can change the factorization in silly ways by permuting factors, inserting negative signs, or appending copies of ± 1. (In fact, our desire for uniqueness is the reason that we say that ± 1 are not prime numbers.) But we can never change the fact that there are "two copies of 2" and "one copy of 3."

Next we observe that the polynomial $x^3 - x^2 - 2x + 2 \in \mathbb{Q}[x]$ can be factored in infinitely many ways:

$$\begin{aligned} x^3 - x^2 - 2x + 2 &= (x-1)(x^2-2) \\ &= (2x-1)\left(\frac{1}{2}x^2 - 1\right) \\ &= (3x^2-3)\left(\frac{1}{3}x - \frac{1}{3}\right) \cdot 4 \cdot \frac{1}{2} \cdot \frac{1}{2}. \end{aligned}$$

We can change the factorization in silly ways by permuting factors and by appending nonzero constants. (In fact, our desire for uniqueness is the reason we say that polynomials of degree 0 are not prime.) But we can never change the fact that there is "one copy of the prime $x-1$" and "one copy of the prime x^2-2."[20] If we instead consider $x^3 - x^2 - 2x + 2$ as an element of the ring $\mathbb{R}[x]$ then we obtain the following prime factorization:

$$x^3 - x^2 - 2x + 2 = (x-1)(x-\sqrt{2})(x+\sqrt{2}).$$

Thus we observe that the notion of primality is relative to the field of coefficients.

Based on these examples we can officially state what we mean by "unique factorization."

Uniqueness of Prime Factorization

For Integers: Suppose we have prime integers $p_1, \ldots, p_r \in \mathbb{Z}$ and $q_1, \ldots, q_s \in \mathbb{Z}$ satisfying

$$p_1 p_2 \cdots p_r = \pm q_1 q_2 \cdots q_s.$$

It follows that $r = s$ and we can can re-index the q_i so that $p_i = \pm q_i$ for all i.

For Polynomials over a Field: Suppose we have prime polynomials $p_1(x), \ldots, p_r(x) \in \mathbb{F}[x]$ and $q_1(x), \ldots, q_s(x) \in \mathbb{F}[x]$ satisfying

$$p_1(x)p_2(x)\cdots p_r(x) = cq_1(x)q_2(x)\cdots q_s(x)$$

for some nonzero constant $c \in \mathbb{F}$. It follows that $r = s$ and we can reindex the $q_i(x)$ so that $p_i(x) = c_i q_i(x)$ for some nonzero constants $c_i \in \mathbb{F}$.

[20] We will prove in the next section that $x^2 - 2$ is indeed a prime element of $\mathbb{Q}[x]$.

In each case the proof is by induction on the minimum of the two numbers r and s. The key step is played by Euclid's Lemma.

Proof of Unique Factorization for Integers: Suppose that we have prime integers $p_1, \ldots, p_r, q_1, \ldots, q_s \in \mathbb{Z}$ satisfying

$$p_1 p_2 \cdots p_r = \pm q_1 q_2 \cdots q_s.$$

If one of r or s is zero then I claim that the other must be zero. Indeed, suppose for contradiction that $s = 0$ and $r \geqslant 1$, so that $p_1 p_2 \cdots p_r = \pm 1$. Then we have

$$|p_1||p_2| \cdots |p_r| = |p_1 \cdots p_r| = |\pm 1| = 1.$$

But this implies that $|p_i| = 1$ for all i, which contradicts the fact that the p_i are prime. The proof that $r = 0$ implies $s = 0$ is similar.

Now let us assume that $r \geqslant 1$ and $s \geqslant 1$. By definition we see that p_1 divides the product $\pm q_1 q_2 \ldots q_s$. Then since p_1 is prime it follows from Euclid's Lemma that we must have $p_1 | q_j$ for some j. In other words, we must have $p_1 k = q_j$ for some integer $k \in \mathbb{Z}$. Since q_j is prime this implies by definition that $|p_1| = 1$ or $|k| = 1$. But then since p_1 is prime we have by definition that $|p_1| \neq 1$. Therefore it follows that $|k| = 1$ and hence $p_1 = \pm q_j$. By re-indexing the factors we can assume that $j = 1$, so $p_1 = \pm q_1$. Finally, by canceling the common factor from both sides we obtain

$$p_2 \cdots p_r = \pm q_2 \cdots q_s,$$

and the result follows by induction. □

Proof of Unique Factorization for Polynomials over a Field: Suppose that we have

$$p_1(x) p_2(x) \cdots p_r(x) = c q_1(x) q_2(x) \cdots q_s(x),$$

If one of r or s is zero then I claim that the other must be zero. Indeed, suppose for contradiction that $s = 0$ and $r \geqslant 1$, so that $p_1(x) p_2(x) \cdots p_r(x) = c$. Then we have

$$\deg(p_1) + \deg(p_2) + \cdots + \deg(p_r) = \deg(p_1 p_2 \cdots p_r) = \deg(c) = 0.$$

But this implies that $\deg(p_i) = 0$ for all i, which contradicts the fact that the polynomials $p_i(x)$ are prime. The proof that $r = 0$ implies $s = 0$ is similar.

Now let us assume that $r \geqslant 1$ and $s \geqslant 1$. By definition we see that $p_1(x)$ divides the product $c q_1(x) q_2(x) \ldots q_s(x)$. Then since $p_1(x)$ is prime it follows from Euclid's Lemma that we must have $p_1(x) | q_j(x)$ for some j. In other words, we must have $p_1(x) f(x) = q_j(x)$ for some polynomial $f(x) \in \mathbb{F}[x]$. Since $q_j(x)$ is prime this implies by definition that $\deg(p_1) = 0$ or $\deg(f) = 0$. But then since $p_1(x)$ is prime we have by definition that $\deg(p_1) \neq 0$. It follows

that $\deg(f) = 0$ and hence $f(x) = c' \in \mathbb{F}$ is a nonzero constant. By re-indexing the factors we can assume that $j = 1$, so $c'p_1(x) = q_1(x)$. Finally, by canceling the common factor from both sides we obtain

$$p_2(x) \cdots p_r(x) = (cc')q_2(x) \cdots q_s(x),$$

and the result follows by induction. □

To end this chapter I will show you some specific examples of prime polynomials.

4.6 Some Examples of Prime Polynomials

I'm sure you are familiar with the prime integers $\pm 2, \pm 3, \pm 5, \pm 7, \pm 11, \ldots$. But the prime polynomials are less familiar. Let's begin with a basic observation.

Polynomials of Degree One are Prime

Let $\mathbb{F}$ be a field. Then every polynomial $f(x) \in \mathbb{F}[x]$ with $\deg(f) = 1$ is prime.

Proof: Consider any polynomial $f(x) \in \mathbb{F}[x]$ with $\deg(f) = 1$ and suppose that $f(x) = g(x)h(x)$ for some polynomials $g(x), h(x) \in \mathbb{F}[x]$. Since $f(x) \neq 0(x)$ we must have $g(x) \neq 0(x)$ and $h(x) \neq 0(x)$. Then comparing degrees gives

$$1 = \deg(f) = \deg(g) + \deg(h).$$

Finally, since $\deg(g) \geqslant 0$ and $\deg(h) \geqslant 0$ we conclude that $\deg(g) = 0$ or $\deg(h) = 0$. □

Thus we obtain the following important fact.

The Roots of a Polynomial are Unique

Let $f(x) \in \mathbb{F}[x]$ be a polynomial with coefficients in a field $\mathbb{F}$ and suppose that we have

$$f(x) = (x - a_1)(x - a_2) \cdots (x - a_r) = (x - b_1)(x - b_2) \cdots (x - b_m)$$

for some numbers $a_1, \ldots, a_r, b_1, \ldots, b_m \in \mathbb{F}$. Then:

- We have $r = s$.
- We can reindex the b_i so that $a_i = b_i$ for all i.

Proof: From unique prime factorization we conclude that $r = s$ and we may re-index the prime factors $x - b_i$ so that $(x - a_i) = c_i(x - b_i)$ for some nonzero constants $c_i \in \mathbb{F}$. Then comparing coefficients we have $c_i = 1$ and hence $a_i = b_i$. (On the homework you will give an alternate proof that does not assume unique factorization of polynomials.) □

We will see later that **every** prime polynomial in $\mathbb{C}[x]$ has degree 1. (This is another way to state the Fundamental Theorem of Algebra.) However, in $\mathbb{R}[x]$ we have the following.

Some Prime Quadratic Polynomials in $\mathbb{R}[x]$ and $\mathbb{Q}[x]$

For any positive real number $\alpha > 0$, the polynomial $x^2 + \alpha$ is a prime element of $\mathbb{R}[x]$. If $\alpha \in \mathbb{Q}$ is rational then the polynomial $x^2 + \alpha$ is also a prime element of $\mathbb{Q}[x]$.

Proof: Assume for contradiction that $f(x) = x^2 + \alpha$ is not prime. Thus we can write $f(x) = g(x)h(x)$ for some polynomials $g(x), h(x) \in \mathbb{R}[x]$ with $\deg(g) \geqslant 1$ and $\deg(h) \geqslant 1$. Comparing degrees gives

$$2 = \deg(f) = \deg(g) + \deg(h),$$

which implies that $\deg(g) = \deg(h) = 1$. Let's say that $g(x) = ax + b$ for some $a, b \in \mathbb{R}$ with $a \neq 0$. By substitution we obtain

$$f(-b/a) = g(-b/a)h(-b/a) = 0h(-b/a) = 0,$$

and hence $(-b/a)^2 + \alpha = 0$. But this implies that $(-b/a)^2 = -\alpha < 0$, which is impossible because the square of any real number is non-negative. The same proof works over $\mathbb{Q}$. □

It will also follow from the Fundamental Theorem of Algebra that every prime polynomial in $\mathbb{R}[x]$ has degree 1 or 2. However, it turns our that in the ring $\mathbb{Q}[x]$ **there exist prime polynomials of every degree**. This is actually quite tricky to prove; right now I can only show you an infinite family of prime quadratics.

More Prime Quadratic Polynomials in $\mathbb{Q}[x]$

For every integer $d \in \mathbb{Z}$, the polynomial $x^2 - d$ factors in $\mathbb{R}[x]$ as $x^2 - d = (x - \sqrt{d})(x + \sqrt{d})$. However, if d is not a perfect square then I claim that $x^2 - d$ is a prime element of $\mathbb{Q}[x]$.

Proof: Suppose that $d \in \mathbb{Z}$ is not a perfect square and assume for contradiction that $f(x) = x^2 - d \in \mathbb{Q}[x]$ is **not** prime. Then it follows as in the previous proof that $f(x)$ has a root in $\mathbb{Q}$. In other words, we have $f(a/b) = 0$ for some integers $a, b \in \mathbb{Z}$ with $b \neq 0$, and hence

$$\begin{aligned} f(a/b) &= 0 \\ (a/b)^2 - d &= 0 \\ a^2/b^2 &= d \\ a^2 &= db^2. \end{aligned}$$

Now we will consider the unique prime factorizations of the integers a^2 and db^2. Since d is **not** a perfect square, there exists at least one prime $p \in \mathbb{Z}$ that occurs with odd multiplicity in the factorization of d. [Think about it.] Let $\nu_p(n) \geqslant 0$ denote the multiplicity of p in the factorization of any integer $n \in \mathbb{Z}$ and observe that for all $m, n \in \mathbb{Z}$ we have $\nu_p(mn) = \nu_p(n) + \nu_p(m)$. It follows that

$$\begin{aligned} \nu_p(a^2) &= \nu_p(db^2) \\ \nu_p(a) + \nu_p(a) &= \nu_p(d) + \nu_p(b) + \nu_p(b) \\ 2\nu_p(a) &= \nu_p(d) + 2\nu_p(b) \\ \text{(even number)} &= \text{(odd number)} + \text{(even number)}, \end{aligned}$$

which is a contradiction. □

It's a bit harder to find a prime polynomial in $\mathbb{Q}[x]$ of degree 3. For example, you will prove on the homework that the polynomial $x^3 + x + 1 \in \mathbb{Q}[x]$ is prime, by first showing that it has no roots in $\mathbb{Q}$. However, it is much harder[21] to find a prime in $\mathbb{Q}[x]$ of degree 4.

To end this chapter I will give you a problem to think about:

Find the prime factors of $x^6 - 1$ *in the ring* $\mathbb{Q}[x]$.

First we observe that $x = 1$ and $x = -1$ are roots. Then from Descartes' Theorem we obtain

$$\begin{aligned} x^6 - 1 &= (x-1)(x^5 + x^4 + x^3 + x^2 + x + 1) \\ &= (x-1)(x+1)(x^4 + x^2 + 1). \end{aligned}$$

But now what? Is the polynomial $x^4 + x^2 + 1$ prime in $\mathbb{Q}[x]$?

[21] The easiest way to prove the existence of prime polynomials in $\mathbb{Q}[x]$ is called *Eisenstein's criterion.*

4.7 Gauss' Lemma

In the previous two chapters I was careful only to discuss $R[x]$ when R is a field. What about when R is not a field, for example $R = \mathbb{Z}$? Does the ring $\mathbb{Z}[x]$ still have unique prime factorization? Well, this is more subtle.

5 Cubic Equations

5.1 Intermediate Value Theorem

In the previous chapter we discussed the relationship between the roots of a polynomial function $f : \mathbb{F} \to \mathbb{F}$ and the divisibility properties of the formal polynomial expression $f(x) \in \mathbb{F}[x]$. This gives us a convenient language to discuss hypothetical solutions of polynomial equations, but it does not yet help us to **find** solutions.

In applications we are usually interested in real solutions of a real polynomial equation $f(x) = 0$. There are three kinds of questions that we might ask:

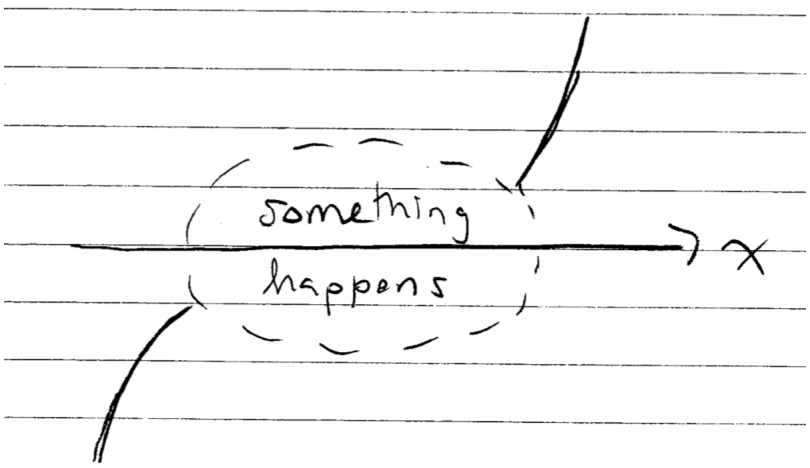
- Prove that a solution exists.
- Find an approximate solution.
- Find an exact formula for a solution.

The first two questions can be answered with calculus.

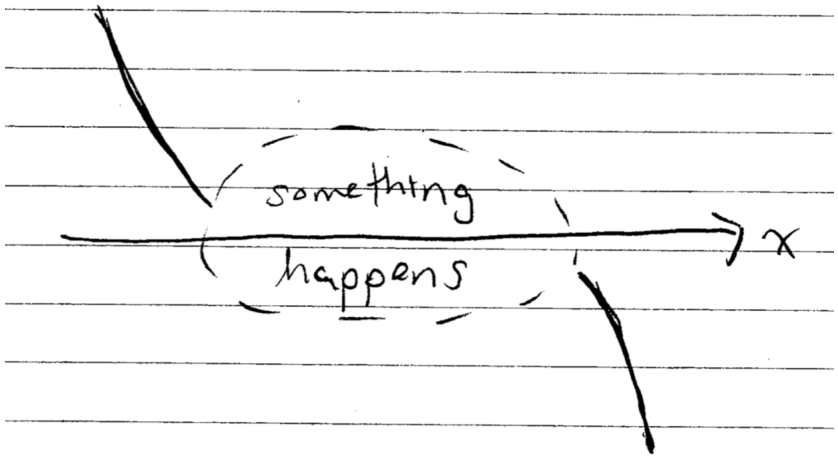
Every Odd Polynomial Has a Real Root

Let $f(x) \in \mathbb{R}[x]$ be a polynomial of **odd degree** with real coefficients. I claim that the equation $f(x) = 0$ has **at least one real solution**.

Proof. Let $n \geqslant 1$ be odd and consider a real polynomial $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{R}[x]$. It the leading coefficient satisfies $a_n > 0$ then the graph of the function $f(x)$ looks like this:



And if the leading coefficient satisfies $a_n < 0$ then the graph looks like this:



In either case, we conclude that the graph must cross the x-axis somewhere. □

This kind of reasoning goes back to Descartes (1637) and his "rule of signs." The standard notations of Cartesian geometry developed over the next 50 years. Isaac Newton was probably the first person to consistently draw his graphs using negative coordinates. At this point in history it was **completely obvious** that the graph of a function is like an unbroken string; if it appears at one point above the x-axis and at another point below the x-axis then it must cross the x-axis at some point in between. The first mathematicians to try to **prove** this obvious fact were Bernard Bolzano (1817) and Augustin-Louis Cauchy (1821). This style of thinking gave birth to the modern subject of "analysis,"[22] which is the opposite of "algebra." Nevertheless, I will give you a quick taste.

[22] You will learn more about this in MTH 433 or 533.

The Intermediate Value Theorem

Consider a polynomial $f(x) \in \mathbb{R}[x]$ with real coefficients and suppose that we have real numbers $a < b$ with $f(a) < 0 < f(b)$. Then there exists some real number $a < c < b$ with the property that $f(c) = 0$.

Proof. Set $a_0 := a$ and $b_0 := b$ and denote the midpoint by $m_0 := (a_0 + b_0)/2$. If $f(m_0) = 0$ then we are done. Otherwise, there are two cases:

- If $f(m_0) > 0$ then we define $a_1 := a_0$ and $b_1 := m_0$.
- If $f(m_0) < 0$ then we define $a_1 := m_0$ and $b_1 := b_0$.

Now we define the midpoint $m_1 := (a_1 + b_1)/2$ and repeat the process. If we never hit on an exact root then we will obtain two infinite sequences

$$a_0 \leqslant a_1 \leqslant a_2 \leqslant \cdots \leqslant b_2 \leqslant b_1 \leqslant b_0$$

with the following properties:

- The distance $b_n - a_n$ gets cut in half each time.
- We have $f(a_n) < 0$ and $f(b_n) > 0$ for all n.

Bolzano and Cauchy both claimed that the sequences a_n and b_n must approach a common limit $c \in \mathbb{R}$,[23] and then they argued by contradiction that the number c must satisfy $f(c) = 0$. There are two cases:

- On the homework you proved that $f(c) - f(a_n) = (c - a_n)g(c, a_n)$ for some polynomial expression $g(c, a_n)$. Since $c - a_n$ goes to zero this this proves that $f(c) - f(a_n)$ goes to zero. Then since $f(a_n) < 0$ for all n this implies that $f(c)$ is not greater than zero.
- But we also have the factorization $f(b_n) - f(c) = (b_n - c)g(b_n, c)$. Since $b_n - c$ goes to zero this proves that $f(b_n) - f(c)$ goes to zero. Finally, since $f(b_n) > 0$ for all n we conclude that $f(c)$ is not less than zero.

The only remaining possibility is that $f(c) = 0$. □

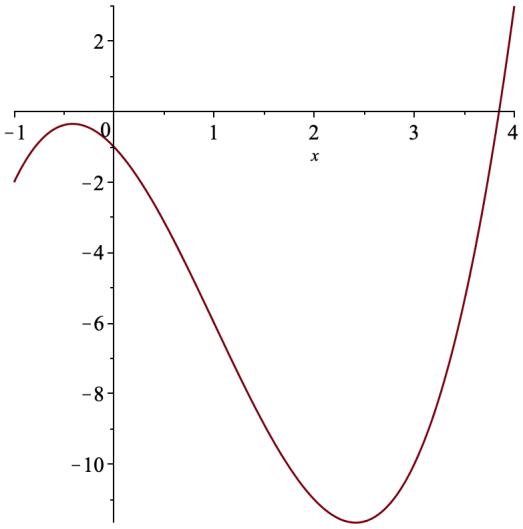
5.2 Newton's Method

We have proved that every real polynomial of odd degree has a real root. For example, let us consider the following cubic polynomial:

$$f(x) = x^3 - 3x^2 - 3x - 1 \in \mathbb{R}[x].$$

By plotting the graph, we observe that there is a root somewhere between 3.5 and 4:

[23] Today we would take this as part of the **definition** of the real numbers.



In this section I will describe a method for approximating this root with any desired degree of accuracy. This method is typically called *Newton's method*, but the history is a bit complicated.[24] Specific examples of this method go back to the ancient Babylonians and the modern version in terms of derivatives was described in 1740 by Thomas Simpson, 13 years after Newton's death.

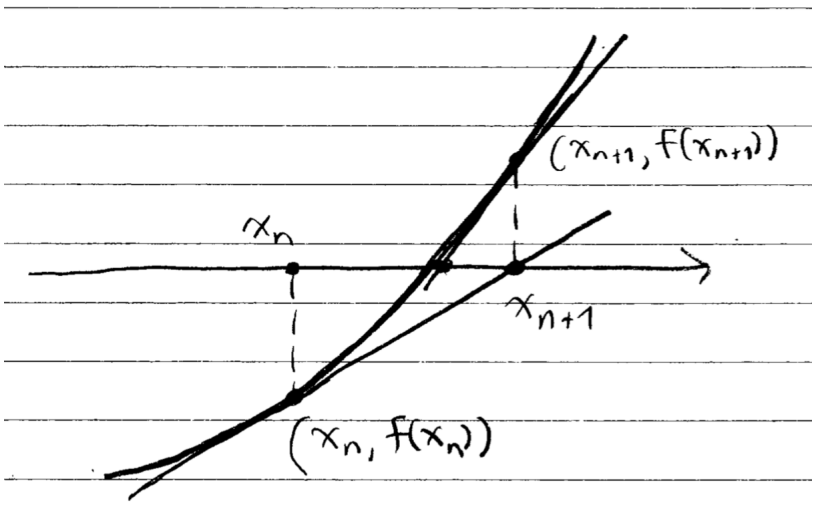
Newton's Method

Let $f(x)$ be a differentiable function of a real variable (not necessarily a polynomial function). In order to find a real solution of the equation $f(x) = 0$ we first make a guess $x_0 \in \mathbb{R}$. Then we successively improve this guess by defining

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)},$$

where $f'(x)$ is the derivative function. Geometrically, we may view x_{n+1} as the x-intercept of the tangent line to the graph of f at the point $(x_n, f(x_n))$, as in the following picture:

[24] See *A short history of Newton's method*, by Peter Deuflhard.



From the picture it seems clear that the sequence $x_0, x_1, x_2, \ldots$ will converge to a root of the function. (In fact, one can prove that after a certain point the number of accurate decimal places will **double** with each iteration.) To obtain the recurrence, we recall that the tangent line to the graph at $(x_n, f(x_n))$ has the equation

$$f'(x_n) = (y - f(x_n))/(x - x_n).$$

Then since the point $(x_{n+1}, 0)$ is supposed to be on this line, we must have

$$\begin{aligned} f'(x_n) &= (0 - f(x_n))/(x_{n-1} - x_n) \\ x_{n+1} - x_n &= -f(x_n)/f'(x_n) \\ x_{n+1} &= x_n - f(x_n)/f'(x_n). \end{aligned}$$

For example, consider the function $f : \mathbb{R} \to \mathbb{R}$ defined by the polynomial $f(x) = x^3 - 3x^2 - 3x - 1$. Since the derivative is $f'(x) = 3x^2 - 6x - 3$, we obtain the following recurrence formula:

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)} = x_n - \frac{x_n^3 - 3x_n^2 - 3x_n - 1}{3x_n^2 - 6x_n - 3}.$$

Let x_0 be any guess that you want; say $x_0 = 3.5$. Then my computer tells me that

$$\begin{aligned} x_0 &= 3.5 \\ x_1 &= 3.921568628 \\ x_2 &= 3.849765479 \\ x_3 &= 3.847324880 \\ x_4 &= 3.847322101 \\ x_5 &= 3.847322102 \end{aligned}$$

Note that we have obtained nine decimal places of accuracy after just five iterations. This amount of accuracy is sufficient for any practical purpose. But we might be curious whether there is a "closed formula" for this root. The answer for general polynomials is "no," but for cubic polynomials such as $x^3 - 6x - 6$ the answer is "yes." In the next section I will show you the famous *Cardano's formula*, which will give us the following exact expression:

$$\sqrt[3]{2} + \sqrt[3]{4} + 1 \approx 3.8473221018630726396.$$

5.3 Cardano's Formula

The first great achievement of European mathematics was the solution of cubic equations. This occurred in Italy in the early 1500s. We know some details of the discovery because of the spread of printed books, including first-hand accounts from two of the main participants (Cardano and Tartaglia). Here is the short version:

- Scipione del Ferro (died 1526) discovered a solution to the cubic equation $x^3 + px = q$. On his deathbed he passed the secret to his student Antonio Fiore.
- Fiore boasted that he was able to solve cubics. He issued a challenge to the well-known Niccolo Tartaglia in 1535, sending him 30 cubic equations of type $x^3 + px = q$.
- Tartaglia struggled with Fiore's problems until he discovered the solution on the night before the contest. Fiore suffered a humiliating defeat.
- Tartaglia divulged the method to Gerolamo Cardano under oath in 1539.
- Cardano generalized the method to other types of cubics and, together with his student Ludovico Ferrari, discovered a method for solving quartic equations.
- Cardano published these results in the *Ars Magna, or The Rules of Algebra* (1545).
- Tartaglia was furious. Tartaglia and Ferrari traded insults in a series of 12 printed pamphlets. This ended with a public contest in 1548, which Ferrari won.
- The solution to the general cubic became known as "Cardano's formula."

Recall that al-Khwarizmi interpreted quadratic equations in terms of areas of squares and rectangles. Similarly, Cardano presented the solution to cubic equations in terms of the volumes of cubes and rectangular boxes. However, it is unlikely that the method could have been **discovered** using geometry because the constructions are too complicated. Instead I believe that the method must have been found using algebraic manipulation, and this is why it was not discovered before the 1500s.

Before showing you Cardano's formula I will illustrate the method using our sample cubic:

$$x^3 - 3x^2 - 3x - 1 = 0.$$

For quadratic equations we needed the trick of "completing the square." For cubic equations we also need some tricks.

Trick 1. First we make the substitution $x = y + \alpha$ for some constant α. This gives

$$\begin{aligned}(y+\alpha)^3 - 3(y+\alpha)^2 - 3(y+\alpha) - 1 &= 0\\ (y^3 + 3\alpha y^2 + 3\alpha^2 y + \alpha^3) - 3(y^2 + 2\alpha y + \alpha^2) - 3(y+\alpha) - 1 &= 0\\ y^3 + (3\alpha - 3)y^2 + (3\alpha^2 - 6\alpha - 3)y + (\alpha^3 - 3\alpha^2 - 3\alpha - 1) &= 0.\end{aligned}$$

Then we set $\alpha = 1$ in order to eliminate the quadratic term:

$$y^3 + 0y^2 - 6y - 6 = 0.$$

Trick 2. Next we set $y = u + v$ to obtain

$$\begin{aligned}(u+v)^3 - 6(u+v) - 6 &= 0\\ (u^3 + 3u^2 v + 3uv^2 + v^3) - 6(u+v) - 6 &= 0.\end{aligned}$$

Trick 3. We can simplify this by also assuming that $uv = 2$. Then we must have

$$\begin{aligned}(u^3 + 3u^2 v + 3uv^2 + v^3) - 6(u+v) - 6 &= 0\\ (u^3 + 6u + 6v + v^3) - 6(u+v) - 6 &= 0\\ u^3 + v^3 &= 6.\end{aligned}$$

Trick 4. At this point we want to solve the following system of two equations:

$$\left\{\begin{array}{rcl} uv & = & 2,\\ u^3 + v^3 & = & 6.\end{array}\right.$$

This is easier if we cube both sides of the first equation:

$$\left\{\begin{array}{rcl} u^3 v^3 & = & 8,\\ u^3 + v^3 & = & 6.\end{array}\right.$$

Then we observe that u^3 and v^3 are the two roots of the following **quadratic** equation:

$$\begin{aligned}(z - u^3)(z - v^3) &= 0\\ z^2 - (u^3 + v^3)z + u^3 v^3 &= 0\\ z^2 - 6z + 8 &= 0.\end{aligned}$$

It follows from the quadratic formula that

$$u^3 \text{ and } v^3 = \frac{6 \pm \sqrt{36 - 4 \cdot 8}}{2} = \frac{6 \pm \sqrt{4}}{2} = \frac{6 \pm 2}{2} = 2 \text{ and } 4.$$

It doesn't matter which is which; we might as well say that $u^3 = 2$ and $v^3 = 4$, so that $u = \sqrt[3]{2}$ and $v = \sqrt[3]{4}$. Finally, we put everything back together to obtain

$$x = y + \alpha$$

$$= y + 1$$
$$= u + v + 1$$
$$= \sqrt[3]{2} + \sqrt[3]{4} + 1.$$

There was no guarantee that this sequence of seemingly random tricks would lead to a solution. However, once the final expression $x = \sqrt[3]{2} + \sqrt[3]{4} + 1$ is found, it is straightforward to check that this is indeed a solution to the equation $x^3 - 3x^2 - 3x - 1 = 0$. [Exercise: Check this.]

We can apply these same tricks to the general case.

Cardano's Formula

Let a, b, c, d be any numbers with $a \neq 0$ and consider the equation

$$ax^3 + bx^2 + cx + d = 0.$$

By substituting $x = y - \frac{b}{3a}$ we obtain the *depressed cubic equation*

$$y^3 + py + q = 0,$$

where the coefficients p, q can be expressed in terms of a, b, c, d as follows:

$$p = \frac{3ac - b^2}{3a} \quad \text{and} \quad q = \frac{27a^2d - 9abc + 2b^3}{27a^2}.$$

Next we substitute $y = u + v$ and $uv = -p/3$ to obtain

$$u^3 + v^3 = -q.$$

We observe that u^3 and v^3 are the roots of the quadratic polynomial

$$(z - u^3)(z - v^3) = z^2 - (u^3 + v^3)z + u^3v^3 = z^2 + qz - (p/3)^3,$$

hence from the quadratic formula we have

$$u^3 \text{ and } v^3 = \frac{-q \pm \sqrt{q^2 + 4(p/3)^3}}{2} = -(q/2) \pm \sqrt{(q/2)^2 + (p/3)^3}.$$

Finally, we obtain

$$y = u + v = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}.$$

We won't bother to express $x = y - \frac{b}{3a}$ in terms of the original coefficients a, b, c, d because the formula will certainly not fit on the page.

That's a reasonably nice formula, but—as with the quadratic formula—the main difficulty is to interpret the different cases. For example, how can we tell if this formula represents one, two or three real solutions? How can we tell if there is a repeated solution? Is there some cubic version of a "discriminant"? Luckily, when it comes to real numbers, cube roots are less problematic than square roots.

The Real Cube Root of a Real Number

For each real number $a \in \mathbb{R}$ there exists exactly one real number $\alpha \in \mathbb{R}$ satisfying $\alpha^3 = a$. Thus it makes sense to talk about **the** cube root of a real number:

$$\sqrt[3]{a} = \alpha.$$

Proof. This will follow later from our discussion of the cube roots of complex numbers. □

However, the square root in the formula is still ambiguous. Let's test our understanding on the simple equation $x^3 - 1 = 0$. On the one hand we know that $x = 1$ is the only real solution. On the other hand, we can apply Cardano's formula with $p = 0$ and $q = -1$ to obtain

$$\begin{aligned} x &= \sqrt[3]{-(q/2) + \sqrt{(q/2)^2 + (p/3)^3}} + \sqrt[3]{-(q/2) - \sqrt{(q/2)^2 + (p/3)^3}} \\ &= \sqrt[3]{1/2 + \sqrt{1/4}} + \sqrt[3]{1/2 - \sqrt{1/4}}. \end{aligned}$$

Note that we must interpret the symbol $\sqrt{1/4}$ in the same way for each summand. For example, if we fix $\sqrt{1/4} = 1/2$ throughout then we obtain the correct answer

$$x = \sqrt[3]{1/2 + 1/2} + \sqrt[3]{1/2 - 1/2} = \sqrt[3]{1} + \sqrt[3]{0} = 1 + 0 = 1.$$

However, if we choose $\sqrt{1/4} = 1/2$ in the first summand and $\sqrt{1/4} = -1/2$ in the second summand then we obtain the wrong answer:

$$x = \sqrt[3]{1/2 + 1/2} + \sqrt[3]{1/2 + 1/2} = \sqrt[3]{1} + \sqrt[3]{1} = 1 + 1 = 2.$$

So be careful.

The following more difficult example comes from Cardano's *Ars Magna* (1545):

$$x^3 + 6x - 20 = 0.$$

On the one hand, we observe that $x = 2$ is a solution. Then we can apply Descartes' Factor Theorem to obtain

$$x^3 + 6x - 20 = (x - 2)(x^2 + 2x + 10).$$

Since the quadratic equation $x^2+2x+10 = 0$ has no real solution we conclude that the original cubic has only one real solution. On the other hand, we can apply Cardano's formula with $p = 6$ and $q = -20$ to obtain

$$\begin{aligned} x &= \sqrt[3]{-10 + \sqrt{10^2 + 2^3}} + \sqrt[3]{-10 - \sqrt{10^2 + 2^3}} \\ &= \sqrt[3]{10 + \sqrt{108}} + \sqrt[3]{10 - \sqrt{108}}. \end{aligned}$$

We observe that this expression defines a real number. But we also know that $x = 2$ is the **only** real solution, so it must be the case that

$$\sqrt[3]{10 + \sqrt{108}} + \sqrt[3]{10 - \sqrt{108}} = 2.$$

I will ask you to verify this identity on the homework. The trick is to express the cube roots of $10 + \sqrt{108}$ and $10 - \sqrt{108}$ in the form $a + b\sqrt{3}$ for some integers $a, b \in \mathbb{Z}$.

5.4 Bombelli and "Imaginary Numbers"

For any real numbers $p, q \in \mathbb{R}$ satisfying $(q/2)^2 + (p/3)^3 > 0$ there exists a unique positive real number s satisfying $s^2 = (q/2)^2 + (p/3)^3$. Then, according to Cardano, the equation $x^3 + px + q = 0$ has at least one real solution:

$$x = \sqrt[3]{-q/2 + s} + \sqrt[3]{-q/2 - s}.$$

This was an important achievement, but it was not a complete solution to the cubic equation because it left the following issues unresolved:

- Every real cubic has at least one real root. However, if $(q/2)^2+(p/3)^3 < 0$ then Cardano's formula seems to produce no solutions.
- Some cubic equations have more than one real solution, but Cardano's formula seems to produce only one solution.

The first issue was resolved by Rafael Bombelli in his *Algebra* (1572). His main innovation was to treat the abstract symbol "$\sqrt{-1}$" as though it were a number, satisfying all the usual

rules of arithmetic, together with the fact that $(\sqrt{-1})^2 = -1$. It is easy to make mistakes with this notation; for example, consider the following paradox:[25]

$$1 = \sqrt{1} = \sqrt{(-1)(-1)} = \sqrt{-1}\sqrt{-1} = -1.$$

Bombelli carefully avoided these mistakes, however. He realized that the number -1 should have **two distinct square roots**, which he called *più di meno* [plus from minus] and *meno di meno* [minus from minus]. Today we refer to the two square roots of -1 by the symbols i and $-i$.[26] There is no way to distinguish between these symbols, so let us say that i is Bombelli's *più di meno*. He then set down the following table:

$i \cdot i = -1$	*più di meno via più di meno fa meno*
$i(-i) = 1$	*più di meno via meno di meno fa più*
$(-i)i = 1$	*meno di meno via più di meno fa più*
$(-i)(-i) = -1.$	*meno di meno via meno di meno fa meno*

These ideas were slow to catch on, and were regarded as useless speculation well into the 18th century. Nevertheless, Bombelli showed that the the symbols i and $-i$ can be used to resolve some problems with Cardano's formula. For example, he considered the equation

$$x^3 - 15x - 4 = 0.$$

On the one hand, we observe that $x = 4$ is a solution. On the other hand, we can apply Cardano's formula with $p = -15$ and $q = -4$ to obtain

$$\begin{aligned} x &= \sqrt[3]{2 + \sqrt{2^2 + (-5)^3}} + \sqrt[3]{2 - \sqrt{2^2 + (-5)^3}} \\ &= \sqrt[3]{2 + \sqrt{4 - 125}} + \sqrt[3]{2 - \sqrt{4 - 125}} \\ &= \sqrt[3]{2 + \sqrt{-121}} + \sqrt[3]{2 - \sqrt{-121}} \\ &= \sqrt[3]{2 + \sqrt{121(-1)}} + \sqrt[3]{2 - \sqrt{121(-1)}} \\ &= \sqrt[3]{2 + \sqrt{121}\sqrt{-1}} + \sqrt[3]{2 - \sqrt{121}\sqrt{-1}} \\ &= \sqrt[3]{2 + 11i} + \sqrt[3]{2 - 11i}. \end{aligned}$$

Clearly there is no real number $\alpha \in \mathbb{R}$ with the property $\alpha^3 = 2 + 11i$, but perhaps there is an abstract symbol $\alpha = a + bi$ with this property. Bombelli computed[27]

$$(a + bi)^3 = a^3 + 3a^3bi + 3ab^2i^2 + b^3i^3$$

[25] Today we recognize that the identity $\sqrt[n]{a}\sqrt[n]{b} = \sqrt[n]{ab}$ is not generally valid because it depends on the particular choices of nth roots.

[26] This notation was introduced by Euler in his book *Institvtionvm calcvli integralis*, 2nd. ed., IV, 1794, p. 184. It was later standardized by Gauss when it appeared in his *Disquisitiones Arithmeticae*, 1801.

[27] He did not use this language, nor did he show the details, but we assume that he performed a similar computation.

$$= a^3 + 3a^3bi - 3ab^2 - b^3i$$
$$= (a^3 - 3ab^2) + (3a^2b - b^3)i.$$

Then he observed that the values $(a, b) = (2, 1)$ and $(a, b) = (2, -1)$ give the following formulas:

$$(2 + i)^3 = 2 + 11i$$
$$(2 + i)^3 = 2 - 11i.$$

Finally, he substituted these "imaginary numbers" into Cardano's formula to obtain

$$x = \sqrt[3]{2 + 11i} + \sqrt[3]{2 - 11i} = (2 + i) + (2 - i) = 4.$$

5.5 Cardano's Formula (Modern Version)

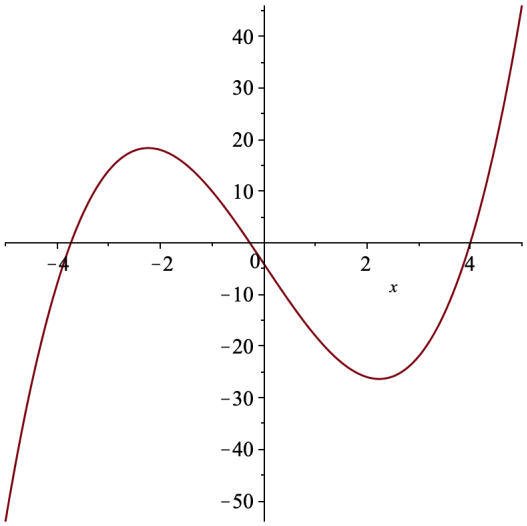
Unfortunately, Bombelli still could not answer the question of multiple real roots. Since $x = 4$ is a root of $x^3 - 15x - 4$, we can use long division to factor out $x - 4$:

$$x^3 - 15x - 4 = (x - 4)(x^2 + 4x + 1).$$

Then from the quadratic formula we obtain two more real roots:

$$x = \frac{-4 \pm \sqrt{16 - 4}}{2} = \frac{-4 \pm 2\sqrt{3}}{2} = -2 \pm \sqrt{3}.$$

Here is a picture:



The key idea that Bombelli missed is the fact that every nonzero complex number $a + bi$ has not one but **three distinct cube roots**. Using this fact, we can cook up all three solutions from Cardano's formula. First I will state and prove a completely modern version of the theorem, then we will apply it to Bombelli's example.

Cardano's Formula (Modern Version)

Let $p, q \in \mathbb{F}$ be any two elements of a field and consider the depressed cubic equation

$$x^3 + px + q = 0.$$

We define the *discriminant* of the cubic as follows:

$$\Delta := \left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3 \in \mathbb{F}.$$

Let $\delta \in \mathbb{F}$ be any number satisfying $\delta^2 = \Delta$ (which may or may not exist). Let $\omega \in \mathbb{F}$ be any number with the properties $\omega^3 = 1$ and $\omega \neq 1$ (which may or may not exist). And let $u, v \in \mathbb{F}$ be any numbers with the properties

$$u^3 = \frac{-q}{2} + \delta, \quad v^3 = \frac{-q}{2} - \delta \quad \text{and} \quad uv = \frac{-p}{3}$$

(which may or may not exist). Then I claim that we have

$$x^3 + px + q = (x - \alpha)(x - \beta)(x - \gamma),$$

where the numbers $\alpha, \beta, \gamma \in \mathbb{F}$ are defined as follows:

$$\boxed{\begin{array}{rcl} \alpha & = & u + v, \\ \beta & = & \omega u + \omega^2 v, \\ \gamma & = & \omega^2 u + \omega v. \end{array}}$$

If $\Delta \neq 0$ then the three roots α, β, γ are distinct; otherwise, if $\Delta = 0$ then two of the roots (and possibly all three) are equal.

The proof is short but not very enlightening. It will make more sense later.

Proof. First we observe that $\omega^3 = 1$ and $\omega \neq 1$ imply $\omega^2 + \omega + 1 = 0$. Indeed, we can factor the polynomial $x^3 - 1 \in \mathbb{F}[x]$ as follows:

$$x^3 - 1 = (x - 1)(x^2 + x + 1).$$

Then since $\omega^3 = 1$ we have $(\omega - 1)(\omega^2 + \omega + 1) = \omega^3 - 1 = 0$ and since $\omega - 1 \neq 0$ we conclude that $\omega^2 + \omega + 1 = 0$. By applying this and the properties of u and v, one can check that

$$\begin{aligned} \alpha + \beta + \gamma &= 0, \\ \alpha\beta + \alpha\gamma + \beta\gamma &= p, \\ \alpha\beta\gamma &= -q. \end{aligned}$$

Therefore we obtain

$$\begin{aligned}(x-\alpha)(x-\beta)(x-\gamma) &= x^3 - (\alpha+\beta+\gamma)x^2 + (\alpha\beta+\alpha\gamma+\beta\gamma)x - \alpha\beta\gamma \\ &= x^3 + 0x^2 + px + q,\end{aligned}$$

as desired. It follows from this that the numbers $\alpha, \beta, \gamma \in \mathbb{F}$ are the roots of $x^3 + px + q$. Next, one can check (just believe me) that

$$(\alpha-\beta)^2(\alpha-\gamma)^2(\beta-\gamma)^2 = -\left(\frac{q}{2}\right)^2 - \left(\frac{p}{3}\right)^3 = -\Delta.$$

It follows from this that the three roots α, β, γ are distinct if and only if $\Delta \neq 0$. □

I call this the "modern version" because it is stated for a general field $\mathbb{F}$. In applications we are probably interested in the rational numbers $\mathbb{Q}$ or the real numbers $\mathbb{R}$. However, if the discriminant $\Delta \in \mathbb{R}$ is negative[28] then we need to pass to the complex numbers:

$$\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}.$$

We will show in the next chapter that $\mathbb{C}$ is a field. We will also prove that every nonzero complex number has n distinct complex nth roots. This implies that for all $p, q \in \mathbb{C}$, we can always find numbers $s, u, v, \omega \in \mathbb{C}$ satisfying the requirements of Cardano's formula, and it follows that every cubic polynomial splits over $\mathbb{C}$ (which is a special case of the Fundamental Theorem of Algebra).

To end the chapter we will apply the modern version Cardano's formula to Bombelli's example:

$$x^3 - 15x - 4 = 0.$$

Since $p = -15$ and $q = -4$, the discriminant is $\Delta = (-2)^2 + (-5)^3 = -121 \neq 0$. Thus we can expect three distinct solutions. Let $s = 11i$ be one of the two complex square roots of Δ, so that $-q/2 \pm s = 2 \pm 11i$. As in the previous section we observe that the numbers $u = 2 + i$ and $v = 2 - i$ satisfy $u^3 = 2 + 11i$ and $v^3 = 2 - 11i$. We also observe that

$$uv = (2+i)(2-i) = 2^2 - i^2 = 4 + 1 = 5 = \frac{-p}{3}$$

as desired. The first root is the one that Bombelli found:

$$\alpha = u + v = (2+i) + (2-i) = 4.$$

To find the other two roots we need to choose some complex number $\omega \in \mathbb{C}$ satisfying $\omega^3 = 1$ and $\omega \neq 1$. In the proof above we observed that these two conditions are equivalent to the single condition $\omega^2 + \omega + 1 = 0$. Thus we can solve for ω using the quadratic formula:

$$\omega = \frac{-1 \pm \sqrt{1-4}}{2} = \frac{-1 \pm \sqrt{-3}}{2} = \frac{-1 \pm i\sqrt{3}}{2}.$$

[28] From the formula $(\alpha-\beta)^2(\alpha-\gamma)^2(\beta-\gamma)^2 = -\Delta$, one can show that Δ is negative and real precisely when there are three distinct real roots.

It doesn't matter which we choose, so let's say $\omega = (-1+\sqrt{3})/2$. Then since $(\omega^2)^2+(\omega^2)+1 = \omega^4+\omega^2+1 = \omega+\omega^2+1 = 0$ we observe that $\omega^2 = (-1-i\sqrt{3})/2$ is the other root. Finally, after a few computations we obtain

$$\beta = \omega u + \omega^2 v = \left(\frac{-1+i\sqrt{3}}{2}\right)(2+i) + \left(\frac{-1-i\sqrt{3}}{2}\right)(2-i) = -2-\sqrt{3},$$
$$\gamma = \omega^2 u + \omega v = \left(\frac{-1-i\sqrt{3}}{2}\right)(2+i) + \left(\frac{-1+i\sqrt{3}}{2}\right)(2-i) = -2+\sqrt{3}.$$

Note that all three roots are real numbers.

To summarize: The cubic equation $x^3 - 15x - 4 = 0$ has three **real** solutions, but these can only be found by temporarily passing through the domain of **imaginary** numbers.[29] This phenomenon was observed by Jacques Hadamard his *Essay on the Psychology of Invention in the Mathematical Field* (1945, page 123):

> *It has been written that the shortest and best way between two truths of the real domain often passes through the imaginary one.*

6 Complex Numbers

6.1 Formal Symbols

When Bombelli introduced the "imaginary units" i and $-i$, he had to address many subtle issues. It is one thing to declare that $i \cdot i = (-i)(-i) = -1$, but how should we interpret more complicated expressions such as $(2+i)^3(5+7i+12i^5)$? Bombelli's solution was to define a "complex number" as an abstract expression of the form "$a+bi$" where a and b are real numbers. Then he carefully spelled out the rules that these expressions must satisfy. Of course, he did this in the language of 16th century Italian mathematics. In this section I will present the modern version of his construction. The modern "formal" point of view was first suggested by William Rowan Hamilton around 1830. Basically, we refuse to say what the symbol "i" **is**; we will only say what it **does**.

To be specific, we define a *complex number* as an abstract expression "$a+bi$," with $a, b \in \mathbb{R}$. We denote the set of such expressions with the blackboard bold letter C:

$$\mathbb{C} = \{a+bi : a, b \in \mathbb{R}\}.$$

Now we wish to interpret these abstract symbols as "numbers." To be specific, we want to define a "ring structure" on the set $\mathbb{C}$. The definitions of "addition" and "multiplication" are basically forced on us by the intuition that i is a "number" satisfying $i^2 = -1$:

$$(a+bi) + (c+di) := (a+c) + (b+d)i,$$

[29] Well, you could just guess the solution, but the only systematic way passes through the imaginary numbers.

$$(a+bi)(c+di) := (ac-bd)+(ad+bc)i.$$

After a lot of boring work (omitted), one can show that these operations indeed define a ring structure on $\mathbb{C}$ with "zero element" $0+0i$ and "one element" $1+0i$.[30] Furthermore, there is a natural way to regard the real numbers as a *subring* $\mathbb{R} \subseteq \mathbb{C}$; that is, we simply identify each real number $a \in \mathbb{R}$ with the formal symbol $a+0i \in \mathbb{C}$. In other words, **every real number is complex, but not every complex number is real**.

So far, so good. Now we can proceed to develop the basic properties of this number system. Our first theorem could perhaps be taken as a definition, but I prefer to prove it.

Equality of Complex Numbers

I claim that the complex number $i = 0+1i \in \mathbb{C}$ is **not real**. It follows from this that for all real numbers $a, b, c, d \in \mathbb{R}$ we have

$$a+bi = c+di \text{ in } \mathbb{C} \quad \Leftrightarrow \quad a = c \text{ and } b = d \text{ in } \mathbb{R}.$$

In the jargon of linear algebra, we say that $\mathbb{C}$ is a vector space over $\mathbb{R}$ with basis $\{1, i\}$.

Proof. Suppose for contradiction that $i \in \mathbb{R} \subseteq \mathbb{C}$ is real. Then from the law of trichotomy we must have $i < 0$ or $i = 0$ or $i > 0$. But each of these possibilities leads to a contradiction:

- If $i < 0$ then $0^2 < i^2$, hence $0 < -1$.
- If $i = 0$ then $0^2 = i^2$, hence $0 = -1$.
- If $i > 0$ then $0^2 < i^2$, hence $0 < -1$.

Now consider any real numbers $a, b, c, d \in \mathbb{R}$ with $a+bi = c+di$ in $\mathbb{C}$. If $b \neq d$ then we conclude that

$$i = \frac{a-c}{d-b} \in \mathbb{R},$$

which is a contradiction. Therefore we must have $b = d$ and it follows that

$$\begin{aligned} a+bi &= c+bi \\ (a+bi)-(0+bi) &= (c+bi)-(0+bi) \\ a+0i &= c+0i \\ a &= c. \end{aligned}$$

□

[30] It might seem miraculous that all of the details work out. Later we will see some good reasons for this.

If that proof was too pedantic for you, then don't worry about it. The key idea is that **the complex numbers cannot be ordered in a way that is compatible with the ordering on** $\mathbb{R}$. This is one of the reasons that they were regarded with skepticism for so long. Consider the following quote from Leonhard Euler's *Introduction to Algebra* (1770):

> *Because all conceivable numbers are either greater than zero or less than 0 or equal to 0, then it is clear that the square roots of negative numbers cannot be included among the possible numbers. Consequently we must say that these are impossible numbers. And this circumstance leads us to the concept of such number, which by their nature are impossible, and ordinarily are called imaginary or fancied numbers, because they exist only in imagination.*

The next important fact is that we can divide by any nonzero complex number.

Complex Numbers form a Field

For any complex number $a + bi \in \mathbb{C}$ satisfying $a + bi \neq 0 + 0i = 0$, there exists a (unique) complex number $c + di \in \mathbb{C}$ satisfying

$$(a + bi)(c + di) = 1 + 0i = 1.$$

The following proof is surprising if you have not seen the trick before. Luckily, you have all seen the trick before. It is called "rationalizing the denominator."

Proof. Consider any $a + bi \in \mathbb{C}$ with $a + bi \neq 0 + 0i$. From the previous theorem this means that $a \neq 0$ or $b \neq 0$ (or both). The goal is to express the hypothetical fraction "$1/(a + bi)$" in the form $c + di$ for some specific $c, d \in \mathbb{R}$. The following hypothetical computation is not yet justified, but it helps us to guess the correct solution:

$$\frac{1}{a+bi} = \frac{1}{a+bi} \cdot \frac{a-bi}{a-bi} = \frac{a-bi}{(a+bi)(a-bi)} = \frac{a-bi}{a^2+b^2} = \left(\frac{a}{a^2+b^2}\right) + \left(\frac{-b}{a^2+b^2}\right) i.$$

Since a and b are not both zero, we know that $a^2 + b^2 \neq 0$. Therefore we may define the real numbers $c := a/(a^2 + b^2)$ and $d := -b/(a^2 + b^2)$. Finally, one can check that

$$(a + bi)(c + di) = 1 + 0i.$$

□

The trick of "rationalizing the denominator" is so useful that we decide to turn it into a general concept. I regard the following facts as absolute truths that were discovered, not created,

by humans.[31] One can say that the formula $|\alpha\beta| = |\alpha||\beta|$ was glimpsed by Diophantus of Alexandria in the 3rd century, with his "two-square identity" for whole numbers:

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

However, the general theory was not understood until the 19th century.

Definition/Theorem (Complex Conjugation and Absolute Value)

For any complex number $\alpha = a + bi \in \mathbb{C}$ we define its *complex conjugate* $\alpha^* \in \mathbb{C}$ as follows:

$$(a + bi)^* := a - bi.$$

Then we define the *absolute value* $|\alpha| \in \mathbb{R}$ as the real non-negative square root of $a^2 + b^2 \in \mathbb{R}$ and we observe that

$$\alpha\alpha^* = (a + bi)(a - bi) = (a^2 + b^2) + 0i = a^2 + b^2 = |\alpha|^2.$$

We also observe that $|a + bi|$ is the length of the vector $(a, b) \in \mathbb{R}^2$ in the Cartesian plane. In particular, we have $|\alpha| = 0$ if and only if $\alpha = 0 + 0i$.

Then for all complex numbers $\alpha, \beta \in \mathbb{C}$, I claim that the following properties hold:

(1) $\alpha = \alpha^*$ if and only if $\alpha \in \mathbb{R}$,

(2) $(\alpha + \beta)^* = \alpha^* + \beta^*$,

(3) $(\alpha\beta)^* = \alpha^*\beta^*$,

(4) $|\alpha\beta| = |\alpha||\beta|$.

Proof. (1): Let $\alpha = a + bi$. If $\alpha \in \mathbb{R}$ then $b = 0$ and hence

$$\alpha^* = (a + 0i)^* = a - 0i = a + 0i = \alpha.$$

Conversely, suppose that $\alpha = \alpha^*$, so that $a + bi = a - bi$. Subtracting a from each side gives $bi = -bi$ and hence $2bi = 0$. In other words: $0 + 2bi = 0 + 0i$. Comparing real and imaginary parts gives $2b = 0$ and hence $b = 0$.

(2) and (3) are a bit tedious.[32] You will verify them on the homework.

[31] The same cannot be said of every kind of mathematics.

[32] Actually there is a fancier way to prove these identities, called "extension of field automorphisms," but right now it is too abstract for us.

(4): By applying (3) we have

$$|\alpha\beta|^2 = (\alpha\beta)(\alpha\beta)^* = \alpha\beta\alpha^*\beta^* = (\alpha\alpha^*)(\beta\beta^*) = |\alpha|^2|\beta|^2.$$

Then taking the square root of each side gives the result. □

It is hard to overstate the significance of the identity $|\alpha\beta| = |\alpha||\beta|$. For example, it easily shows that $\alpha\beta = 0$ implies $\alpha = 0$ or $\beta = 0$ for all $\alpha, \beta \in \mathbb{C}$, which was not obvious from the definitions. It also gives us a different route to the "field structure" of $\mathbb{C}$. To see this we observe for all $\alpha \neq 0$ that

$$\alpha\alpha^* = |\alpha|^2 \neq 0 \quad \Rightarrow \quad \alpha\left(\frac{1}{|\alpha|^2}\alpha^*\right) = 1.$$

If $\alpha = a + bi \in \mathbb{C}$ then it follows that

$$\alpha^{-1} = \frac{1}{|\alpha|^2}\alpha^* = \frac{1}{a^2+b^2}(a - bi) = \left(\frac{a}{a^2+b^2}\right) + \left(\frac{-b}{a^2+b^2}\right)i.$$

You might feel that the ideas in this section were a bit magical. That is also the general opinion of most mathematicians. In the 1840s, the Irish mathematician and physicist William Rowan Hamilton discovered a more general system of "imaginary numbers," which he called the quaternions.[33] He defined these as abstract symbols $a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ with real coefficients $a, b, c, d \in \mathbb{R}$:

$$\mathbb{H} = \{a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} : a, b, c, d \in \mathbb{R}\}.$$

Then he defined a "ring structure" on these symbols by specifying that

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = \mathbf{ijk} = -1.$$

It turns out that this system has magical properties analogous to the complex numbers, the main difference being that multiplication in $\mathbb{H}$ is not commutative. (For example, $\mathbf{ij} = \mathbf{k} \neq -\mathbf{k} = \mathbf{ji}$.) The properties of $\mathbb{H}$ led to the invention of the dot product and cross product of vector analysis, which were quickly adopted into the theory of electromagnetism.

Upon learning of the quaternions, Hamilton's colleague John Graves was impressed, but he also had the following to say:

> *There is still something in the system which gravels me. I have not yet any clear views as to the extent to which we are at liberty arbitrarily to create imaginaries, and to endow them with supernatural properties.*

It was in response to Graves that Hamilton proposed the formal interpretation of complex numbers.[34] However, as Hamilton knew, it is also possible to give an intuitive geometric interpretation of complex numbers. We will discuss this in the following sections.

[33] You are invited to investigate this number system in the optional writing assignment.

[34] *On conjugate functions, or algebraic couples, as tending to illustrate generally the doctrine of imaginary quantities, and as confirming the results of Mr Graves respecting the existence of two independent Integers in the complete expression of an imaginary logarithm*, (1834).

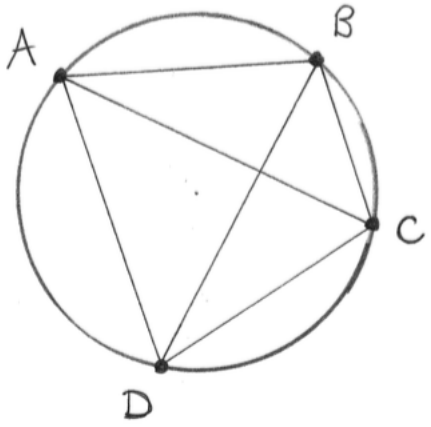
6.2 Trigonometry and Cubic Equations

It turns out that the most intuitive interpretation of complex numbers comes from trigonometry. You may be surprised to learn that trigonometry was not studied by the classical Greeks. Instead, it emerged during the Hellenistic period from a synthesis of Greek geometry and Babylonian astronomy.[35] The reason that astronomy requires trigonometry is because we cannot measure the **distances** between astronomical objects, only the **angles** between them.

The most famous astronomical text ever written is the *Almagest* (2nd century AD) of Claudius Ptolemy. From a mathematical point of view, this work is famous for the following theorem.

Ptolemy's Theorem

Consider any four points A, B, C, D on the boundary of a circle:

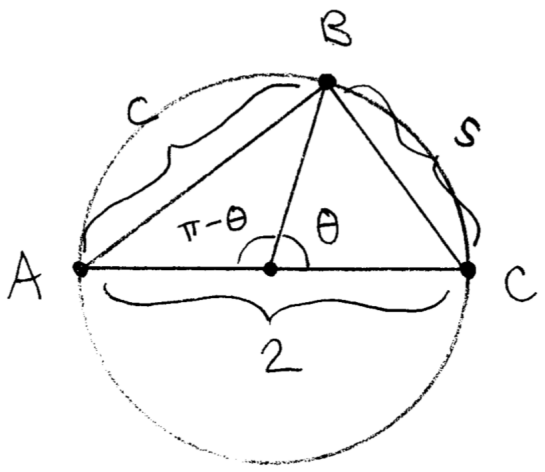


Then the six distances between these points are related by the following algebraic identity:

$$AC \cdot BD = AB \cdot CD + AD \cdot BC.$$

The proof of this theorem is not important. I'm sure you can come up with an elementary geometric argument if you try hard enough. The reason I bring it up now is because of its relationship to the "angle sum formulas" of trigonometry. To see the relationship between chord length and modern trigonometric functions, consider the following diagram:

[35] This is why we still use the Babylonian "base 60" numerical system to measure angles.



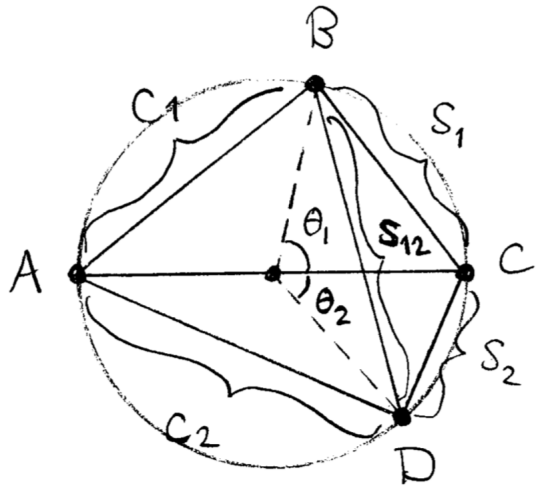
Here we have a right triangle inscribed in a circle of radius 1. In modern language, one can check that the chord lengths s and c satisfy

$$s = 2\sin(\theta/2) \quad \text{and} \quad c = 2\cos(\theta/2).$$

The Pythagorean Theorem applied to this triangle tells us that

$$\begin{aligned} s^2 + c^2 &= 2^2 \\ 4\sin^2(\theta/2) + 4\cos^2(\theta/2) &= 4 \\ \sin^2(\theta/2) + \cos^2(\theta/2) &= 1, \end{aligned}$$

as expected. Now consider the following configuration made of two right triangles:



As in the above diagram, one can check that the chord lengths $s_1, c_2, s_2, c_2, s_{12}$ satisfy

$$\begin{aligned} s_1 &= 2\sin(\theta_1/2), \\ c_1 &= 2\cos(\theta_1/2), \\ s_2 &= 2\sin(\theta_2/2), \\ c_2 &= 2\cos(\theta_2/2), \\ s_{12} &= 2\sin((\theta_1+\theta_2)/2). \end{aligned}$$

Therefore by applying Ptolemy's Theorem we obtain the "angle sum formula":

$$\begin{aligned} AC \cdot BD &= AB \cdot CD + AD \cdot BC \\ 2s_{12} &= c_1 s_2 + s_1 c_2 \\ 4\sin((\theta_1+\theta_2)/2) &= 4\cos(\theta_1/2)\sin(\theta_2/2) + 4\sin(\theta_1/2)\cos(\theta_2/2) \\ \sin((\theta_1+\theta_2)/2) &= \cos(\theta_1/2)\sin(\theta_2/2) + \sin(\theta_1/2)\cos(\theta_2/2). \end{aligned}$$

Ptolemy gave a similar proof for the "angle difference formula":

$$\sin((\theta_1-\theta_2)/2) = \cos(\theta_1/2)\cos(\theta_2/2) - \sin(\theta_1/2)\sin(\theta_2/2).$$

He then proceeded to use these formulas to compile an extensive table of chord lengths (i.e., values of the sine function) for each half-degree angle between 0° and 180°. In summary, here are Ptolemy's angle sum and difference formulas in modern notation.

Angle Sum/Difference Formulas

For any angles $\alpha, \beta \in \mathbb{R}$ we have

$$\begin{cases} \sin(\alpha \pm \beta) &= \sin\alpha\cos\beta \pm \cos\alpha\sin\beta, \\ \cos(\alpha \pm \beta) &= \cos\alpha\cos\beta \mp \sin\alpha\sin\beta. \end{cases}$$

There is no need to memorize these formulas because we will shortly have a much easier way to derive them. For now, let me observe that the angle sum formula can be used to expand $\cos(n\theta)$ as a polynomial expression in $\cos\theta$ whenever $n \geqslant 0$ is a whole number.

Multiple Angle Formulas

Let $\theta \in \mathbb{R}$ and $n \in \mathbb{Z}$. Then applying the angle sum and difference formulas gives

$$\cos(n\theta) = 2\cos\theta\cos((n-1)\theta) - \cos((n-2)\theta).$$

It follows by induction that for all integers $n \geqslant 0$ we can expand $\cos(n\theta)$ as a polynomial expression in $\cos\theta$ with integer coefficients.

The proof is short but tricky. You do not need to memorize it.

Proof. For all $\theta \in \mathbb{R}$ and $n \in \mathbb{Z}$ we apply the angle sum and difference formulas to obtain

$$\begin{aligned}
&\cos(n\theta) + \cos((n-2)\theta) \\
&= \cos((n-1)\theta + \theta) + \cos((n-1)\theta - \theta) \\
&= \big[\cos\theta\cos((n-1)\theta) + \cancel{\sin\theta\sin((n-1)\theta)}\big] + \big[\cos\theta\cos((n-1)\theta) - \cancel{\sin\theta\sin((n-1)\theta)}\big] \\
&= 2\cos\theta\cos((n-1)\theta).
\end{aligned}$$

□

Let us use this recursive formula to obtain the first few multiple angle formulas. To begin, we observe that $\cos(0\theta) = 1$ and $\cos(1\theta) = \cos\theta$. Next we obtain the "double angle formula":

$$\begin{aligned}
\cos(2\theta) &= 2\cos\theta\cos(1\theta) - \cos(0\theta) \\
&= 2\cos\theta\cos\theta - 1 \\
&= 2\cos^2\theta - 1.
\end{aligned}$$

And after that the "triple angle formula":

$$\begin{aligned}
\cos(3\theta) &= 2\cos\theta\cos(2\theta) - \cos(1\theta) \\
&= 2\cos\theta\big[2\cos^2\theta - 1\big] - \cos\theta \\
&= 4\cos^3\theta - 3\cos\theta.
\end{aligned}$$

Today these expressions are called *Chebyshev polynomials*, since their general theory was developed by Pafnuty Chebyshev in 1854. However, the identities were certainly known much earlier. The first application is probably due to Francois Viète, who in his *Supplement to Geometry* (1593) used the triple angle formula to give a trigonometric solution of the cubic equation. The main innovation of this solution is that it seems to avoid the use of imaginary numbers. To see how this works, let us consider the depressed cubic equation

$$x^3 + px + q = x^3 - 3x - 1 = 0.$$

Since $p/3 = -1$ and $q/2 = -1/2$ we see that $(q/2)^2 + (p/3)^3 = -3/4 < 0$, which means that Cardano's Formula will involve taking the square root of a negative number:

$$\begin{aligned}
x &= \sqrt[3]{1/2 + \sqrt{(-1/2)^2 + (-1)^3}} + \sqrt[3]{1/2 + \sqrt{(-1/2)^2 + (-1)^3}} \\
&= \sqrt[3]{1/2 + \sqrt{-3/4}} + \sqrt[3]{1/2 + \sqrt{-3/4}}.
\end{aligned}$$

Instead, Viète suggested that we should look at the triple angle formula:

$$\begin{aligned} 4\cos^3\theta - 3\cos\theta - \cos(3\theta) &= 0 \\ 8\cos^3\theta - 3\cdot 2\cos\theta - 2\cos(3\theta) &= 0 \\ (2\cos\theta)^3 - 3(2\cos\theta) - 2\cos(3\theta) &= 0. \end{aligned}$$

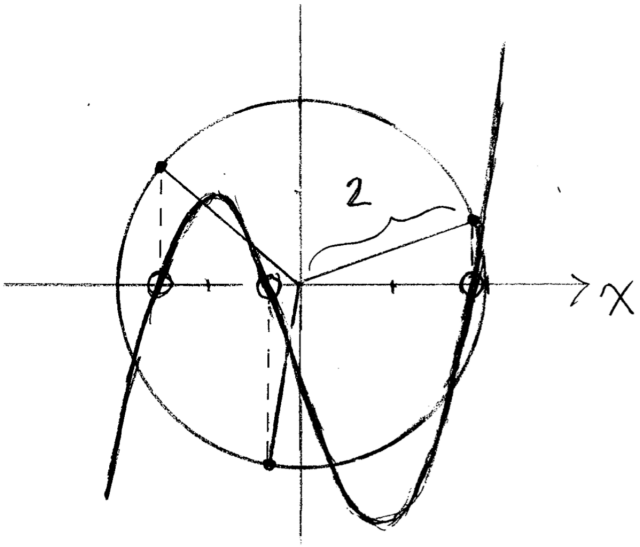
Observe that this equation becomes $x^3 - 3x - 1 = 0$ when we substitute $x = 2\cos\theta$ and $\cos(3\theta) = 1/2$. The second condition has **exactly three solutions**:

$$\begin{aligned} \cos(3\theta) &= 1/2 \\ 3\theta &= \pi/3 + 2\pi k && \text{for any } k \in \mathbb{Z} \\ \theta &= \pi/9 + 2\pi k/3 && \text{for any } k \in \mathbb{Z} \\ &= \pi/9 \quad \text{or} \quad 7\pi/9 \quad \text{or} \quad 13\pi/9. \end{aligned}$$

Hence we obtain **three real solutions** for x:

$$\begin{aligned} x &= 2\cos(\pi/9) \quad \text{or} \quad 2\cos(7\pi/9) \quad \text{or} \quad 2\cos(13\pi/9) \\ &= 2\cos(20^\circ) \quad \text{or} \quad 2\cos(140^\circ) \quad \text{or} \quad 2\cos(260^\circ) \\ &\approx 1.879 \quad \text{or} \quad -1.532 \quad \text{or} \quad -0.347. \end{aligned}$$

Here is a picture:



There is an important principle in this solution that I want to emphasize. When we divided the angle $\pi/9$ by 3 we obtained not one, but three distinct angles.

Angle Division

Consider some angle $\theta \in \mathbb{R}$ and a positive integer $n \geqslant 1$. Since angles are only defined up to integer multiples of 2π, we observe that dividing θ by n gives n distinct answers:

$$\begin{aligned} \theta &= \theta + 2\pi k && \text{for any } k \in \mathbb{Z} \\ \frac{\theta}{n} &= \frac{\theta}{n} + \frac{2\pi k}{n} && \text{for any } k \in \mathbb{Z} \\ &= \frac{\theta}{n}, \frac{\theta + 2\pi}{n}, \ldots, \frac{\theta + 2\pi(n-1)}{n}. \end{aligned}$$

This will be important below when we discuss the nth roots of complex numbers.

Actually, Viète expressed his solution in geometric terms by showing that solving a cubic equation with three real roots is equivalent to "trisecting an angle." Instead of regarding his construction as a solution to the cubic, it seems that he viewed it as a solution to the angle trisection problem, which was a difficult problem from Greek antiquity.[36]

Here is the general statement of Viète's solution in modern terms.

Viète's Trigonometric Solution of the Cubic

Let $p, q \in \mathbb{R}$ be any real numbers satisfying $(q/2)^2 + (p/3)^3 < 0$. In this case we know that Cardano's formula inevitably leads to complex numbers. To get around this, we will compare the equation $x^3 + px + q = 0$ to the triple angle formula:

$$y^3 - 3y - 2\cos(3\theta) = 0.$$

If the value of $\cos(3\theta)$ is given, then there are three distinct angles $\theta = \theta_0, \theta_1, \theta_2$, which lead to three distinct real solutions $y = 2\cos\theta_0, 2\cos\theta_1, 2\cos\theta_2$.

In order to express p and q in the correct form, we first observe that $(q/2)^2 < -(p/3)^3$ implies $p < 0$. Therefore it is possible to write $p = -3r^2$ and $q = -cr^2$ for some unique real numbers $c, r \in \mathbb{R}$ satisfying $r > 0$. Furthermore, since

$$\begin{aligned} (q/2)^2 &< -(p/3)^3 \\ (-cr^2/2)^2 &< -(-r^2)^3 \\ c^2r^2/4 &< r^6 \\ c^2 &< 4r^2 \end{aligned}$$

[36] It was proved in the early 1800s that angle trisection is actually **impossible** within the rules of Euclidean geometry. See the chapter on Impossible Constructions below.

$$|c| < 2r,$$

we observe that it possible to write $c = 2r\cos(3\theta)$ for some three angles $\theta = \theta_0, \theta_1, \theta_2$. After making these substitutions, our original equation becomes

$$\begin{aligned} x^3 + px + q &= 0 \\ x^3 - 3r^2 - 2r^3\cos(3\theta) &= 0 \\ (x/r)^3 - 3(x/r) - 2\cos(3\theta) &= 0, \\ y^3 - 3y - 2\cos(3\theta) &= 0, \end{aligned}$$

from which we obtain three real solutions: $x/r = y = 2\cos\theta_0, 2\cos\theta_1, 2\cos\theta_2$.

If you insist, we can express these solutions in terms of p and q by first noting that $p = -3r^2$ implies $r = \sqrt{-p/3}$ (positive real square root). Then $q = -cr^2 = -2r^3\cos(3\theta)$ implies that

$$\cos(3\theta) = \frac{q}{-2r^3} = \frac{q}{-2(\sqrt{-p/3})^3} = \frac{3q}{2p}\sqrt{\frac{-3}{p}}.$$

If we let $\psi = \arccos(3q\sqrt{-3/p}/(2p))$ denote any **specific value** of the inverse cosine (you can choose your favorite), then the three corresponding angles are

$$\theta_k = \frac{\psi}{3} + \frac{2\pi k}{3} \quad \text{for } k = 0, 1, 2.$$

Finally, we obtain the three real solutions in terms of p and q:

$$x = 2\sqrt{\frac{-p}{3}} \cdot \cos\left(\frac{\psi}{3} + \frac{2\pi k}{3}\right) \quad \text{for } k = 0, 1, 2.$$

For example, let us apply the general formula to Bombelli's equation $x^3 - 15x - 4 = 0$. Here we have $p = -15$ and $q = -4$, so that

$$\frac{3q}{2p}\sqrt{\frac{-3}{p}} = \frac{2\sqrt{5}}{25} \approx 0.1789.$$

Since this number is between -1 and 1, there exists a unique pair of angles $\pm\psi$ with $\cos(\pm\psi) = 2\sqrt{5}/25$. Let's choose the "principal value" $\psi = 79.695^\circ$ between 0° and 180°. Then the three real solutions of Bombelli's equation are

$$x = 2\sqrt{5}\cos(26.565^\circ) \text{ or } 2\sqrt{5}\cos(26.565^\circ + 120^\circ) \text{ or } 2\sqrt{5}\cos(26.565^\circ + 240^\circ).$$

But we have already seen that this equation has the solutions 4, $-2 - \sqrt{3}$ and $-2 + \sqrt{3}$, thus we obtain a very strange trigonometric identity:

$$\cos\left(\frac{1}{3}\arccos\left(\frac{2\sqrt{5}}{25}\right) + \frac{2\pi k}{3}\right) = \frac{4}{2\sqrt{5}} \quad \text{or} \quad \frac{-2-\sqrt{3}}{2\sqrt{5}} \quad \text{or} \quad \frac{-2+\sqrt{3}}{2\sqrt{5}}.$$

Well, that was really horrible. Let me reassure you that you do **not** need to memorize complicated trigonometric identities. In the next section I will present a major breakthrough that simplified the whole subject.

6.3 Euler's Formula

Francois' Viète's posthumous work *On Angular Sections* (1615) is devoted to trigonometric identities. For example, in this work he presented that the "quadruple angle identities"

$$\begin{aligned}\cos(4\theta) &= \cos^4\theta - 6\cos^2\theta\sin^2\theta + \sin^4\theta,\\ \sin(4\theta) &= 4\cos^3\theta\sin\theta - 4\cos\theta\sin^2\theta,\end{aligned}$$

and he observed that these identities are related to the following binomial expansion:

$$(\cos\theta + \sin\theta)^4 = \cos^4\theta + 4\cos^3\theta\sin\theta + 6\cos^2\theta\sin^2\theta + 4\cos\theta\sin^3\theta + \sin^4\theta.$$

Indeed, the only difference between $(\cos\theta + \sin\theta)^4$ and $\cos(4\theta) + \sin(4\theta)$ is the presence of certain negative signs. By looking at many examples, Viète was able to guess the correct rule for these negative signs. However, it turns out that the rule is vastly simplified by working over the complex numbers. The following result was first stated (in a slightly different form) by Abraham de Moivre in 1707. However, the version stated here is due to Euler.

De Moivre's Formula

For all angles $\alpha, \beta \in \mathbb{R}$ we have

$$(\cos\alpha + i\sin\alpha)(\cos\beta + i\sin\beta) = \cos(\alpha+\beta) + i\sin(\alpha+\beta).$$

It follows that for all angles $\theta \in \mathbb{R}$ and integers $n \geqslant 0$ we have

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

The difficult part is to guess the formula. Then the proof is trivial.

Proof. The first identity follows from Ptolemy's angle sum identities:

$$\begin{aligned}&(\cos\alpha + i\sin\alpha)(\cos\beta + i\sin\beta)\\ &= (\cos\alpha\cos\beta - \sin\alpha\sin\beta) + (\cos\alpha\sin\beta + \sin\alpha\cos\beta)i\\ &= \cos(\alpha+\beta) + i\sin(\alpha+\beta).\end{aligned}$$

Then the second identity follows by induction:

$$\begin{aligned}(\cos\theta + i\sin\theta)^{n+1} &= (\cos\theta + i\sin\theta)^n(\cos\theta + i\sin\theta)\\ &= (\cos(n\theta) + i\sin(n\theta))(\cos\theta + i\sin\theta)\\ &= \cos(n\theta+\theta) + i\sin(n\theta+\theta) \qquad \alpha = n\theta \text{ and } \beta = \theta\\ &= \cos((n+1)\theta) + i\sin((n+1)\theta).\end{aligned}$$

□

De Moivre's formula is an extremely useful mnemonic. For example, we can use it to quickly derive the double angle formulas. Observe that for any angle θ we have

$$\begin{aligned}\cos(2\theta) + i\sin(2\theta) &= (\cos\theta + i\sin\theta)^2\\ &= (\cos\theta + i\sin\theta)(\cos\theta + i\sin\theta)\\ &= (\cos\theta\cos\theta - \sin\theta\sin\theta) + (\cos\theta\sin\theta - \sin\theta\cos\theta)i\\ &= (\cos^2\theta - \sin^2\theta) + (2\cos\theta\sin\theta)i.\end{aligned}$$

Then comparing real and imaginary parts gives

$$\begin{cases} \cos(2\theta) &= \cos^2\theta - \sin^2\theta,\\ \sin(2\theta) &= 2\cos\theta\sin\theta. \end{cases}$$

This is the reason that I never memorize trig identities.

As I mentioned before the proof, this statement of de Moivre's Formula is really due to Leonhard Euler. In fact, Euler stated these identities more elegantly in terms of "exponential functions" in his *Introduction to the Analysis of the Infinite* (1748), which is one of the most influential textbooks of all time.[37] This work is well-known for standardizing the so-called "transcendental functions," including the older trigonometric functions "$\sin, \cos, \tan$," and the more recently defined exponential and logarithmic functions "$\exp, \log$." Let me present Euler's definition of the exponential function in modern terms.

Definition/Theorem (The Exponential Function)

For any complex number $\alpha \in \mathbb{C}$, Euler consider the following power series:

$$\exp(\alpha) := 1 + \alpha + \frac{\alpha^2}{2} + \frac{\alpha^3}{6} + \cdots = \sum_{k=0}^{\infty} \frac{\alpha^k}{k!}.$$

I claim that this series always converges to a complex number. Furthermore, I claim that

[37] According to Carl Boyer: *The* Introductio *of Euler is referred to frequently by historians, but its significance is generally underestimated. This book is probably the most influential textbook of modern times.*

for all complex numbers $\alpha, \beta \in \mathbb{C}$ we have

$$\exp(\alpha)\exp(\beta) = \exp(\alpha+\beta).$$

In particular, it follows that for any integer $n \geqslant 1$ we have

$$\exp(n) = \exp(1+1+\cdots+1) = \exp(1)^n = e^n,$$

where $e := \exp(1) \approx 2.17828$ is the so-called *Euler constant*. For this reason we will use the suggestive notation

$$\text{“}e^{\alpha}\text{”} := \exp(\alpha)$$

for any complex number $\alpha \in \mathbb{C}$. Keep in mind that this is merely a notation. It is not really possible, for example, to multiply the number e with itself π times. However, the number $e^{\pi} := \exp(\pi) \approx 23.14$ is perfectly well-defined.

Proof. This is not an analysis class, so I will just give a sketch. First let me observe that complex numbers satisfy the *triangle inequality*:[38]

$$|\alpha+\beta| \leqslant |\alpha| + |\beta| \quad \text{for all } \alpha, \beta \in \mathbb{C}.$$

For all $\alpha \in \mathbb{C}$ and integers $n \geqslant 0$ we apply the triangle inequality and the multiplicative property of absolute value to obtain

$$\left|\sum_{k=0}^{n} \frac{\alpha^k}{k!}\right| \leqslant \sum_{k=0}^{n} \left|\frac{\alpha^k}{k!}\right| = \sum_{k=0}^{n} \frac{|\alpha|^k}{k!}.$$

If the sequence on the right converges to a real number as $n \to \infty$ (which is does), then the sequence on the left also converges. To prove the identity $\exp(\alpha+\beta) = \exp(\alpha)\exp(\beta)$, we first recall the *binomial theorem*:

$$(\alpha+\beta)^k = \sum_{i=1}^{k} \frac{k!}{i!(k-i)!} \alpha^i \beta^{k-i}.$$

Then we apply this to the multiplication of power series:

$$\begin{aligned}
\exp(\alpha)\exp(\beta) &= \left(\sum_{k\geqslant 0} \frac{\alpha^k}{k!}\right)\left(\sum_{k\geqslant 0} \frac{\beta^k}{k!}\right) \\
&= \sum_{k\geqslant 0} \left(\sum_{i=0}^{k} \frac{\alpha^i}{i!} \frac{\beta^{k-i}}{(k-i)!}\right) \\
&= \sum_{k\geqslant 0} \frac{1}{k!} \left(\sum_{i=0}^{k} \frac{k!}{i!(k-i)!} \alpha^i \beta^{k-i}\right)
\end{aligned}$$

[38] We will see that this has to do with triangles in the next section.

$$= \sum_{k \geqslant 0} \frac{1}{k!}(\alpha + \beta)^k$$
$$= \exp(\alpha + \beta).$$

□

Euler was never careful about the convergence of power series, but it worked out fine for him. And it will work out fine for us too. We are now ready to state Euler's exponential version of de Moivre's Formula.

Euler's Formula

For all angles $\theta \in \mathbb{R}$ we have

$$e^{i\theta} = \cos\theta + i\sin\theta.$$

Let me observe that de Moivre's formula follows immediately from Euler's formula and the multiplicative property of the exponential function:

$$\cos(\alpha + \beta) + i\sin(\alpha + \beta) = e^{i(\alpha+\beta)} = e^{i\alpha}e^{i\beta} = (\cos\alpha + i\sin\alpha)(\cos\beta + i\sin\beta).$$

This reasoning is a bit circular, however, because Euler used de Moivre's formula as the main ingredient in his proof. (I won't present Euler's proof because it's not very enlightening.) This means that Euler's formula still depends on the mysterious angle sum trigonometric identities.

I will explain the deeper reason for the angle sum identities in the next two sections. The key idea, as we will see, is that one can view the complex number $e^{i\theta} \in \mathbb{C}$ as a **function** that rotates each point of the Cartesian plane $\mathbb{R}^2$ counterclockwise[39] by angle θ around the origin.

6.4 Polar Form and Roots of Unity

Since $\mathbb{C}$ is a field, we know that the ring of polynomials $\mathbb{C}[x]$ has certain nice properties. And this may help us to better understand polynomials with **real** coefficients. In this section we will study the specific family of polynomials $x^n - 1 \in \mathbb{R}[x]$. To begin, we observe that the polynomials $x^2 - 1$ and $x^4 - 1$ split over $\mathbb{C}$:

$$x^2 - 1 = (x - 1)(x + 1)$$
$$x^4 - 1 = (x^2 - 1)(x^2 + 1) = (x - 1)(x + 1)(x - i)(x + i).$$

[39] Or clockwise. The choice is arbitrary.

We also know that the polynomial $x^3 - 1$ splits over $\mathbb{C}$. To see this, we first factor out $x - 1$:

$$x^3 - 1 = (x - 1)(x^2 + x + 1).$$

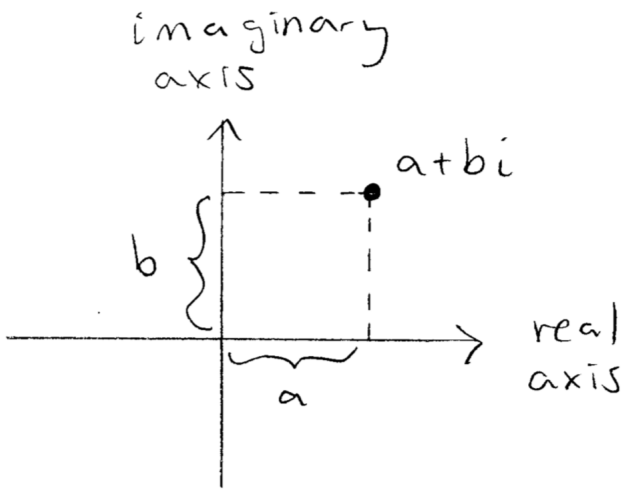
And then we use the quadratic formula to find the other two roots $(1 \pm i\sqrt{3})/2$. It follows that

$$x^3 - 1 = (x - 1)\left(x - \frac{1 + i\sqrt{3}}{2}\right)\left(x - \frac{1 - i\sqrt{3}}{2}\right).$$

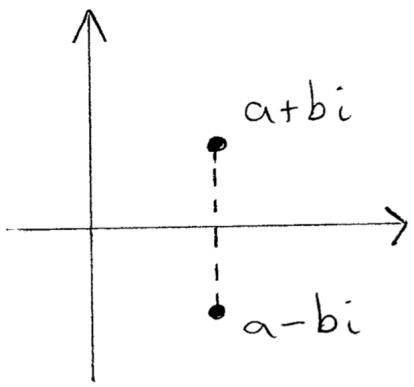
Now what about $x^5 - 1$? Does this polynomial also split over $\mathbb{C}$? In order to solve this problem it is helpful to view complex numbers as points in the Cartesian plane.

Definition of the Complex Plane

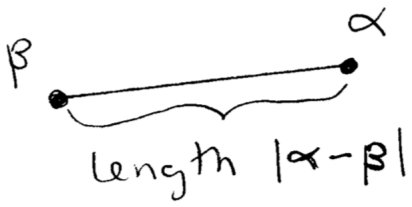
We have seen that every complex number $\alpha \in \mathbb{C}$ has the form $\alpha = a + bi$ for some **unique** real numbers $a, b \in \mathbb{R}$. This suggests that we should identify $a + ib$ with the point $(a, b) \in \mathbb{R}^2$ in the Cartesian plane:



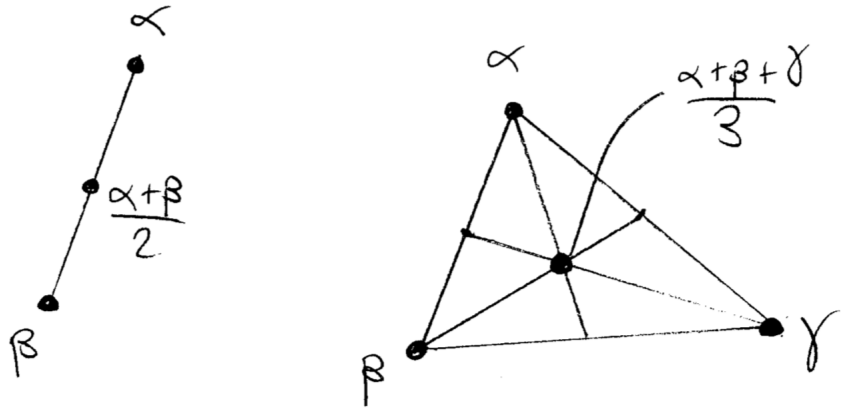
In this language, we observe that conjugate pairs of complex numbers correspond to "mirror images" across the real axis:



And we also observe that the distance between any complex numbers $\alpha, \beta \in \mathbb{C}$ is equal to the absolute value of their difference:



Finally, we observe that the "numerical average" of any collection of complex numbes is the "center of mass" (or "centroid") of the corresponding points:

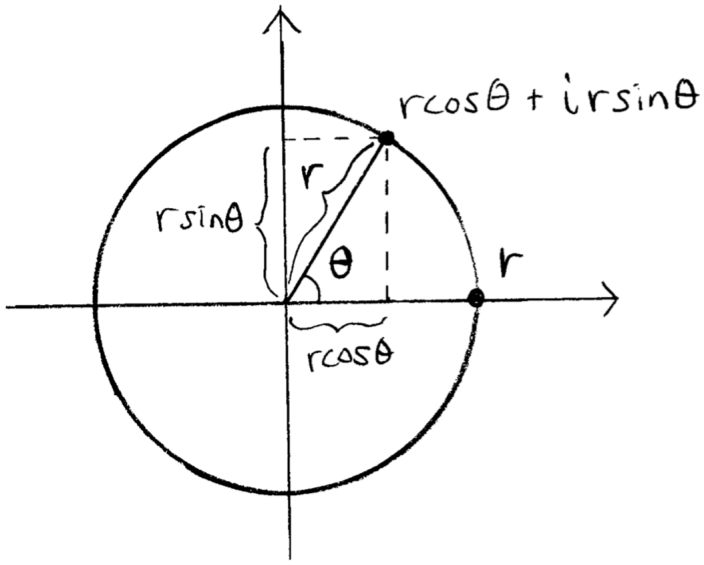


As with the complex numbers themselves, the concept of the "complex plane" was slow to

be accepted. John Wallis made an early attempt at a geometric representation in his *Algebra* (1673). One could also say that the geometric picture is implicit in the work of de Moivre (1707) and Roger Cotes (1722). However, the true geometric meaning of complex numbers only emerges when we combine the complex plane with Euler's formula, to obtain the *polar form* of complex numbers.

The Polar Form of Complex Numbers

For any complex number $\alpha = a + bi \in \mathbb{C}$, the following diagram shows that we can write $a = r\cos\theta$ and $b\sin\theta$ for some real numbers $r \geqslant 0$ and $0 \leqslant \theta < 2\pi$:



Then it follows from Euler's formula that

$$\alpha = r\cos\theta + ri\sin\theta = r(\cos\theta + i\sin\theta) = re^{i\theta}.$$

We call this the *polar form* of α. Since $r \geqslant 0$ and since the absolute value preserves multiplication, we observe that

$$\begin{aligned} |\alpha| &= |re^{i\theta}| \\ &= |r||e^{i\theta}| \\ &= r|\cos\theta + i\sin\theta| \\ &= r(\cos^2\theta + \sin^2\theta) \\ &= r. \end{aligned}$$

Thus the "radius coordinate" r is uniquely determined by α. However, the "angle coordinate" is only unique up to integer multiples of 2π. In other words, for all real numbers $\theta_1, \theta_2 \in \mathbb{R}$ we have

$$e^{i\theta_1} = e^{i\theta_2} \quad \Leftrightarrow \quad \theta_1 - \theta_2 = 2\pi k \text{ for some } k \in \mathbb{Z}.$$

Finally, we observe that the multiplication of complex numbers becomes particularly meaningful when expressed in polar form:

$$(r_1 e^{i\theta_1})(r_2 e^{i\theta_2}) = (r_1 r_2) e^{i(\theta_1+\theta_2)}.$$

In other words, to multiply complex numbers in polar form we simply **multiply the radii** and **add the angles**.

The polar form of complex numbers is an extremely powerful tool. In order to illustrate this we will now compute the complex roots of the polynomial $x^5 - 1$. If $x = re^{i\theta}$ is a root then we must have

$$\begin{aligned} x^5 &= 1 \\ (re^{i\theta})^5 &= 1 \\ r^5 e^{i5\theta} &= 1. \end{aligned}$$

By taking the absolute value of each side we observe that

$$1 = |1| = |r^5 e^{i5\theta}| = |r|^5 |e^{i5\theta}| = |r|^5 \cdot 1 = |r|^5.$$

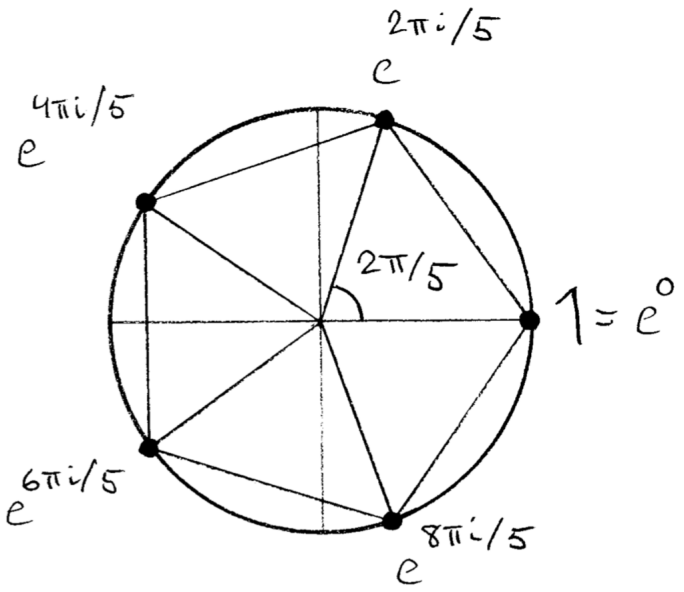
Then since $r \geqslant 0$ we must have $r = 1$. It follows that $e^{i5\theta} = 1$, and hence

$$\begin{aligned} 5\theta &= 2\pi k \\ \theta &= 2\pi k/5 \end{aligned}$$

for some integer $k \in \mathbb{Z}$. Note that the formula $\theta = 2\pi k/5$ represents **five distinct angles** $0 \leqslant \theta < 2\pi$, corresponding to **five distinct complex roots**:

$$x = e^{0\pi i/5}, \quad e^{2\pi i/5}, \quad e^{4\pi i/5}, \quad e^{6\pi i/5}, \quad e^{8\pi i/5}.$$

And we can view these in the complex plane as the **vertices of a regular pentagon**:



Of course, there are infinitely many different ways to name these roots, since the angles are only defined up to integer multiples of 2π. For example, we could write

$$x = e^{0\pi i/5}, \quad e^{2\pi i/5}, \quad e^{4\pi i/5}, \quad e^{-4\pi i/5}, \quad e^{-2\pi i/5},$$

or even

$$x = e^{10\pi i/5}, \quad e^{-8\pi i/5}, \quad e^{14\pi i/5}, \quad e^{-4\pi i/5}, \quad e^{8\pi i/5}.$$

In order to keep things as simple as possible, it is often convenient to define the number $\omega = e^{2\pi i/5} \in \mathbb{C}$, so that $\omega^k = e^{2\pi ik/5}$. Then the complex roots of $x^5 - 1$ are $1, \omega, \omega^2, \omega^3, \omega^4$, and we have the following factorization:

$$x^5 - 1 = (x-1)(x-\omega)(x-\omega^2)(x-\omega^2)(x-\omega^3)(x-\omega^4).$$

Once we have understood the polynomial $x^n - 1$ for $n = 5$, the general case is no more difficult. The general theorem is really just a disguised version of the Division Theorem for integers.

Theorem (Roots of Unity)

Consider a positive integer $n \geqslant 1$ and define the complex number

$$\omega = e^{2\pi i/n} = \cos(2\pi/n) + i\sin(2\pi/n).$$

For any integer $k \in \mathbb{Z}$ we observe that $(\omega^k)^n = (\omega^n)^k = 1^k = 1$. Therefore every integral power of ω is a root of the polynomial $x^n - 1$. But this polynomial has at most n distinct complex roots, so there must be some repetition among the powers of ω. To be precise,

I claim that for all integers $k, \ell \in \mathbb{Z}$ we have

$$\omega^k = \omega^\ell \text{ in } \mathbb{C} \quad \Leftrightarrow \quad n|(k-\ell) \text{ in the ring } \mathbb{Z}.$$

It follows that the polynomial $x^n - 1$ has n distinct complex roots, which can be expressed in the standard form ω^r with $0 \leqslant r < n$:

$$x^n - 1 = (x-1)(x-\omega)(x-\omega^2)\cdots(x-\omega^{n-1}).$$

Geometrically, these roots are the vertices of a regular n-gon in the complex plane.

Proof. Recall that $e^{i\theta_1} = e^{i\theta_2}$ if and only if $\theta_1 - \theta_2 = 2\pi q$ for some $q \in \mathbb{Z}$, i.e., if and only if the real numbers $\theta_1, \theta_2 \in \mathbb{R}$ represent the same angle. It follows that

$$\omega^n = (e^{2\pi i/n})^n = e^{2\pi i} = e^{0i} = e^0 = 1.$$

More generally, for any integers $k, \ell \in \mathbb{Z}$ we see that

$$\begin{aligned} \omega^k = \omega^\ell &\Leftrightarrow e^{2\pi ik/n} = e^{2\pi i\ell/n} \\ &\Leftrightarrow 2\pi k/n - 2\pi\ell/n = 2\pi q \text{ for some } q \in \mathbb{Z} \\ &\Leftrightarrow k - \ell = nq \text{ for some } q \in \mathbb{Z} \\ &\Leftrightarrow n|(k-\ell). \end{aligned}$$

Next, I claim that for each $k \in \mathbb{Z}$ there exists some integer $0 \leqslant r < n$ satisfying $\omega^k = \omega^r$. Indeed, since $n \geqslant 1$ we can divide k by n to obtain some $q, r \in \mathbb{Z}$ satisfying

$$\begin{cases} k = nq + r, \\ 0 \leqslant r < n. \end{cases}$$

And it follows that

$$\omega^k = \omega^{nq+r} = (\omega^n)^q \omega^r = 1^q \omega^r = \omega^r.$$

Finally, I claim that for all $0 \leqslant r_1 < n$ and $0 \leqslant r_2 < n$ we have

$$\omega^{r_1} = \omega^{r_2} \text{ in } \mathbb{C} \quad \Leftrightarrow \quad r_1 = r_2 \text{ in } \mathbb{Z}.$$

Indeed, one direction is trivial. For the other direction, suppose that $\omega^{r_1} = \omega^{r_2}$. Then from the above remarks we have $n|(r_1 - r_2)$ and hence $r_1 - r_2 = nq$ for some $q \in \mathbb{Z}$. If $q \neq 0$ then this implies that $|r_1 - r_2| = |n||q| = n|q| \geqslant n$. On the other hand, since $0 \leqslant r_1 < n$ and $0 \leqslant r_2 < n$ we must have $|r_1 - r_2| < n$. This contradiction shows that $q = 0$ and hence $r_1 = r_2$. $\square$

Remark: Actually, the theorem still holds as stated if we replace $\omega = e^{2\pi i/n}$ by $\omega = e^{2\pi im/n}$ for any integer m satisfying $\gcd(m, n) = 1$. I will say more about this at the end of the chapter.

To end this section we will discuss several interesting corollaries of the previous theorem. First, by expanding the right hand side of the equation

$$x^n + 0x^{n-2} + \cdots + 0x - 1 = (x - \omega^0)(x - \omega^2) \cdots (x - \omega^{n-1})(x - \omega^{n-1})$$

and then comparing coefficients, we obtain the following identities:

$$\begin{aligned}
0 &= \omega^0 + \omega^2 + \cdots + \omega^{n-1}, \\
0 &= \omega^0\omega^1 + \omega^0\omega^2 + \cdots + \omega^{n-2}\omega^{n-1}, \\
&\vdots \\
0 &= \omega^0\omega^1 \cdots \omega^{n-2} + \omega^0\omega^1 \cdots \omega^{n-3}\omega^{n-1} + \cdots + \omega^1\omega^2 \cdots \omega^{n-1}.
\end{aligned}$$

In other words, the sum of the products of the nth roots of unity, taken k at a time, equals zero whenever $1 \leqslant k \leqslant n-1$. The first of these identities is the least surprising. In fact, we could prove this first identity more simply by substituting $x = \omega$ into the factorization of $x^n - 1$ as a difference of powers:

$$\begin{aligned}
x^n - 1 &= (x-1)(x^{n-1} + x^{n-2} + \cdots + x + 1) \\
\omega^n - 1 &= (\omega - 1)(\omega^{n-1} + \omega^{n-2} + \cdots + \omega + 1) \\
0 &= (\omega - 1)(\omega^{n-1} + \omega^{n-2} + \cdots + \omega + 1).
\end{aligned}$$

Then since $\omega - 1 \neq 0$ we conclude that $\omega^{n-1} + \omega^{n-2} + \cdots + \omega + 1 = 0$. Alternatively, we can view this identity as saying that the center of mass of the nth roots of unity is at the origin of the complex plane.

To prepare for the next corollary, let use observe how complex conjugation interacts with the polar form.

Complex Conjugation and Polar Form

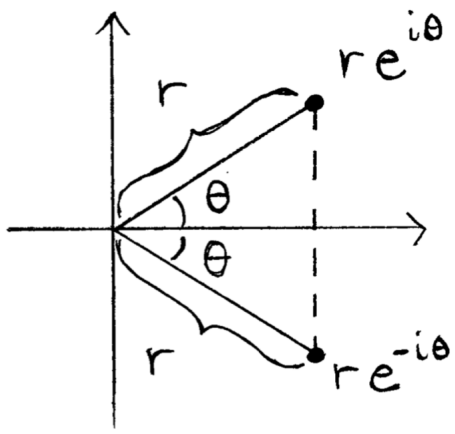
For any real number $\theta \in \mathbb{R}$ we recall that $\cos(-\theta) = \cos\theta$ and $\sin(-\theta) = -\sin\theta$. It follows from this that $e^{-i\theta}$ is the complex conjugate of $e^{i\theta}$:

$$e^{-i\theta} = \cos(-\theta) + i\sin(-\theta) = \cos\theta - i\sin\theta = (\cos\theta + i\sin\theta)^* = (e^{i\theta})^*.$$

More generally, for any real numbers $r, \theta \in \mathbb{R}$ we have

$$(re^{i\theta})^* = r^*(e^{i\theta})^* = re^{-i\theta}.$$

This makes geometric sense since positive angles are measured **counterclockwise** from the positive real axis, while negative angles are measured **clockwise**:



We will combine this observation with the theorem on roots of unity to obtain the prime factorization of the polynomial $x^n - 1$ **over the real numbers**. This result was first obtained by Roger Cotes in 1716, and published posthumously in the *Harmonia Mensurarum* (1722). Cotes was the editor of the second edition of Isaac Newton's *Principia*. Sadly, he died at the age of 34, without having published any of his own work. His mathematical ability prompted Newton to remark that "if he had lived, we might have known something."

Factorization of $x^n - 1$ in the ring $\mathbb{R}[x]$

If $\omega = e^{2\pi i/n}$ then we observe that $\omega^{n-k} = \omega^n\omega^{-k} = 1\omega^{-k} = \omega^{-k}$ for all integers $k \in \mathbb{Z}$. This allows us to rewrite the factorization of $x^n - 1$ in the ring $\mathbb{C}[x]$ as follows:

$$x^n - 1 = (x-1)\prod_{k=1}^{(n-1)/2}(x-\omega^k)(x-\omega^{-k}) \qquad \text{if } n \text{ is odd,}$$

$$x^n - 1 = (x-1)(x+1)\prod_{k=1}^{(n-2)/2}(x-\omega^k)(x-\omega^{-k}) \qquad \text{if } n \text{ is even.}$$

Furthermore, for any integer $k \in \mathbb{Z}$ we observe that $\omega^{-k} = \cos(-2\pi k/n) + i\sin(-2\pi k/n) = \cos(2\pi k/n) - i\sin(2\pi k/n)$ is the complex conjugate of $\omega^k = \cos(2\pi i/n) + i\sin(2\pi k/n)$, and it follows that the polynomial $(x-\omega^k)(x-\omega^{-k})$ has **real coefficients**:

$$\begin{aligned}(x-\omega^k)(x-\omega^{-k}) &= x^2 - (\omega^k + \omega^{-k})x + \omega^k\omega^{-k} \\ &= x^2 - 2\cos(2\pi k/n)x + 1.\end{aligned}$$

Furthermore, if $1 < k < n/2$ then this quadratic polynomial is **prime** in $\mathbb{R}[x]$ because it has no real roots. (In this case,the complex roots ω^k, ω^{-k} are both non-real, and a quadratic polynomial can have at most two roots in the field $\mathbb{C}$.) Thus we obtain the prime factorization of $x^n - 1$ in the ring $\mathbb{R}[x]$:

$$x^n - 1 = (x-1) \prod_{k=1}^{(n-1)/2} \left(x^2 - 2\cos\left(\frac{2\pi k}{n}\right) x + 1 \right) \qquad \text{if } n \text{ is odd,}$$

$$x^n - 1 = (x-1)(x+1) \prod_{k=1}^{(n-2)/2} \left(x^2 - 2\cos\left(\frac{2\pi k}{n}\right) x + 1 \right) \qquad \text{if } n \text{ is even.}$$

Proof. There is not much more to say. I guess we only need to verify that

$$\omega^k + \omega^{-k} = (\cos(2\pi k/n) + \cancel{i \sin(2\pi k/n)}) + (\cos(2\pi k/n) - \cancel{i \sin(2\pi k/n)}) = 2\cos(2\pi k/n).$$

More generally, for any complex number $\alpha = a + bi \in \mathbb{C}$ we always have

$$(x-\alpha)(x-\alpha^*) = x^2 - (\alpha + \alpha^*)x + \alpha\alpha^* = x^2 - 2ax + (a^2 + b^2) \in \mathbb{R}[x].$$

□

For example, if $\omega = e^{2\pi i/5}$ then we obtain the prime factorization for $x^5 - 1$ over $\mathbb{R}$:

$$\begin{aligned}
x^5 - 1 &= (x-1)(x-\omega)(x-\omega^2)(x-\omega^3)(x-\omega^4) \\
&= (x-1)(x-\omega)(x-\omega^2)(x-\omega^{-2})(x-\omega^{-1}) \\
&= (x-1)(x-\omega)(x-\omega^{-1})(x-\omega^2)(x-\omega^{-2}) \\
&= (x-1)\left(x^2 - (\omega+\omega^{-1})x + \omega\omega^{-1}\right)\left(x^2 - (\omega+\omega^{-2})x + \omega\omega^{-2}\right) \\
&= (x-1)\left(x^2 - 2\cos(2\pi/5)x + 1\right)\left(x^2 - 2\cos(4\pi/5)x + 1\right).
\end{aligned}$$

We will see later that the real numbers $\cos(2\pi/5)$ and $\cos(4\pi/5)$ have explicit formulas in terms of rational numbers and square roots. However, the formulas are ugly enough that we do not force high school students to memorize them.

Next, if $\omega = e^{2\pi i/6}$ then we obtain the prime factorization of $x^6 - 1$ over $\mathbb{R}$:

$$\begin{aligned}
x^6 - 1 &= (x-1)(x-\omega)(x-\omega^2)(x-\omega^3)(x-\omega^4)(x-\omega^5) \\
&= (x-1)(x-\omega)(x-\omega^2)(x+1)(x-\omega^{-2})(x-\omega^{-1}) \\
&= (x-1)(x-1)(x-\omega)(x-\omega^{-1})(x-\omega^2)(x-\omega^{-2}) \\
&= (x-1)(x+1)\left(x^2 - 2\cos(2\pi/6)x + 1\right)\left(x^2 - 2\cos(4\pi/6)x + 1\right).
\end{aligned}$$

This time we have the easy simplifications $\cos(2\pi/6) = 1/2$ and $\cos(4\pi/6) = -1/2$, so that

$$x^6 - 1 = (x-1)(x+1)(x^2 - x + 1)(x^2 + x + 1).$$

That was lucky. Because of this simplification we have accidentally obtained the prime factorization of $x^6 - 1$ in the ring $\mathbb{Q}[x]$ (hence also in the ring $\mathbb{R}[x]$). This solves a puzzle that I posed to you at the end of Chapter 3.

In general, we will not be so lucky. For now let me state without proof the prime factorizations of the polynomial $x^n - 1$ over $\mathbb{Q}$ for $2 \leqslant n \leqslant 7$:

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

Do you see any pattern? It seems that the polynomial factors of $x^n - 1$ have something to do with the integer factors of n. Here is the general statement.

Definition/Theorem (Cyclotomic Polynomials)

Let $\omega = e^{2\pi i/n}$ for some integer $n \geqslant 2$. We say that ω^k is a *primitive nth root of unity* when $\gcd(k, n) = 1$, and we define the *nth cyclotomic polynomial* as follows:

$$\Phi_n(x) := \prod_{\substack{1 \leqslant k \leqslant n \\ \gcd(k,n)=1}} (x - \omega^k).$$

In other words, the roots of $\Phi_n(x)$ are the primitive nth roots of unity. For convenience we will also define $\Phi_1(x) := x - 1$. Then for all $n \geqslant 1$ one can show that

$$x^n - 1 = \prod_{\substack{1 \leqslant d \leqslant n \\ d|n}} \Phi_d(x),$$

where the product is taken over all positive integer divisors $d|n$. One can use this factorization to prove by induction that for all $n \geqslant 1$ the polynomial $\Phi_n(x)$ **has integer coefficients**. Furthermore, one can show for all $n \geqslant 1$ that the polynomial $\Phi_n(x)$ is **prime** in the ring $\mathbb{Q}[x]$.[40] Thus we have obtained the prime factorization of $x^n - 1 \in \mathbb{Q}[x]$.

[40] I have carefully avoided discussing prime elements of the ring $\mathbb{Z}[x]$. This concept is more delicate because $\mathbb{Z}$ is not a field. Basically, the same ideas hold for $\mathbb{Z}[x]$ as for $\mathbb{Q}[x]$, but the proofs are harder.

Instead of proving this now, I will explain how it works in the case $n = 6$. If $\omega = e^{2\pi i/6}$, then the 6th roots of unity are $\omega^0, \omega^1, \omega^2, \omega^4, \omega^5$. Among these exponents, only 1 and 5 are coprime to 6. Therefore we have

$$\Phi_6(x) := (x - \omega^1)(x - \omega^5).$$

But note that this polynomial can be simplified. Indeed, since $\omega^6 = 1$ and $\omega \neq 0$ we know that $\omega^5 = \omega^{-1}$, and it follows that

$$\begin{aligned}\Phi_6(x) &= (x - \omega^1)(x - \omega^{-1}) \\ &= x^2 - 2\cos(2\pi/6)x + 1 \\ &= x^2 - x + 1.\end{aligned}$$

As promised, this polynomial has integer coefficients. Furthermore, it is prime over $\mathbb{Q}$ because it has no roots in $\mathbb{Q}$. And what about the factorization of $x^6 - 1$? I claim that this follows from reducing each fraction $k/6$ into lowest terms. To be specific, let us define the notation $\omega_d = e^{2\pi i/d}$ for each integer $d \geqslant 1$. Then for any equivalent fractions $a/b = c/d$ we have

$$\omega_b^a = e^{2\pi i a/b} = e^{2\pi i c/d} = \omega_d^c.$$

Next we observe that $\Phi_2(x) = (x - \omega_2^1) = x + 1$ and $\Phi_3(x) = (x - \omega_3^1)(x - \omega_3^2) = x^2 + x + 1$. Finally, by expressing each 6th root of unity ω_6^k in "lowest terms," we observe that

$$\begin{aligned}x^6 - 1 &= (x-1)(x-\omega_6^1)(x-\omega_6^2)(x-\omega_6^3)(x-\omega_6^4)(x-\omega_6^5) \\ &= (x-1)(x-\omega_6^1)(x-\omega_3^1)(x-\omega_2^1)(x-\omega_3^2)(x-\omega_6^5) \\ &= (x-1)(x-\omega_2^1)\left[(x-\omega_3^1)(x-\omega_3^2)\right]\left[(x-\omega_6^1)(x-\omega_6^5)\right] \\ &= \Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_6(x).\end{aligned}$$

You will perform a similar computation for $n = 8$ on the next homework, and on a future homework you will verify that this factorization process works in general.

The cyclotomic polynomials were studied by Carl Friedrich Gauss in the *Disquisitiones Arithmeticae* (1801). This work is one of the most significant in the history of mathematics. For example, by using the fact that the polynomial $\Phi_{17}(x) = x^{16} + x^{15} + \cdots + x + 1$ is prime over $\mathbb{Q}$, Gauss was able to prove that a regular 17-gon is constructible with straightedge and compass alone. This was a surprising result that seemed to beat the ancient Greeks at their own game. More generally, Gauss explained how to express the real number $\cos(2\pi/n)$ in the simplest possible terms using only integers, field operations and radicals.

We will continue this discussion below in the chapter on Impossible Constructions. However, you will not see a proof in this course that the polynomial $\Phi_n(x)$ is prime over $\mathbb{Q}$. Gauss did not include a full proof of this result in the *Disquisitiones*,[41] and it is doubtful whether he even knew a proof. The easiest proof that I know, due to Richard Dedekind in the 1850s, is still too difficult for us.

[41] He only proved this when n is prime.

6.5 The Functional Interpretation

At the beginning of 19th century there were two alternative interpretations of complex numbers. (1) As points in the complex plane. (2) As pairs of real numbers (a, b) with a reasonable addition operation and a strange multiplication operation. Augustin-Louis Cauchy found (1) to be too informal and (2) to be too arbitrary. We will see his definition $\mathbb{C} := \mathbb{R}[x]/(x^2 + 1)$ in chapter blah below. In this section we will describe a modern synthesis between (1) and (2), which seems to be completely satisfactory.

CORONAVIRUS HAPPENED RIGHT HERE

In order to describe the complex numbers in completely modern terms, I must present to you the abstract definition of a "vector space." Early versions of this concept were written down by Hermann Grassman (in the 1850s) and Giuseppe Peano (in the 1880s), but the purely abstract version did not become widespread until it was used by Hermann Weyl (in the 1920s) in his mathematical foundations of quantum physics. After presenting the definition and a couple of basic properties, we will proceed quickly to concrete examples.

Definition of Vector Spaces

A *vector space* consists of a set V (of vectors), a field $\mathbb{F}$ (of scalars), an operation $+ : V \times V \to V$ (called vector addition), and an operation $\cdot : \mathbb{F} \times V \to V$ (called scalar multiplication), which satisfy the following eight axioms:[42]

(V1) $\forall \mathbf{u}, \mathbf{v} \in V,\ \mathbf{u} + \mathbf{v} = \mathbf{v} + \mathbf{u}$ (commutative addition)

(V2) $\forall \mathbf{u}, \mathbf{v}, \mathbf{w} \in V,\ \mathbf{u} + (\mathbf{v} + \mathbf{w}) = (\mathbf{u} + \mathbf{v}) + \mathbf{w}$ (associative addition)

(V3) $\exists \mathbf{0} \in V, \forall \mathbf{u} \in V,\ \mathbf{u} + \mathbf{0} = \mathbf{u}$ (zero vector)

(V4) $\forall \mathbf{u} \in V,\ \exists \mathbf{v} \in V,\ \mathbf{u} + \mathbf{v} = \mathbf{0}$ (subtraction)

(V5) $\forall \mathbf{u} \in V,\ 1\mathbf{u} = \mathbf{u}$ (unit scalar)

(V6) $\forall a, b \in \mathbb{F},\ \mathbf{u} \in V,\ a(b\mathbf{u}) = (ab)\mathbf{u}$ (associative multiplication)

(V7) $\forall a, b \in \mathbb{F},\ \mathbf{u} \in V,\ (a + b)\mathbf{u} = a\mathbf{u} + b\mathbf{u}$ (distribution)

(V8) $\forall a \in \mathbb{F},\ \mathbf{u}, \mathbf{v} \in V,\ a(\mathbf{u} + \mathbf{v}) = a\mathbf{u} + a\mathbf{v}$ (distribution)

Let me emphasize that we are allowed to multiply two scalars to obtain a scalar, and we are allowed to multiply a scalar with a vector to obtain a vector, but **we are not allowed to multiply a vector with a vector**. In fact, one can show that in general there is no reasonable way to define a vector multiplication $\cdot : V \times V \to V$.[43]

As with rings, I claim that the vector $\mathbf{v}$ satisfying $\mathbf{u} + \mathbf{v} = \mathbf{0}$ is unique, and for the same reasons.

Proof. Suppose that we have $\mathbf{u} + \mathbf{v} = \mathbf{0}$ and $\mathbf{u} + \mathbf{w} = \mathbf{0}$ in a vector space. It follows that

$$\mathbf{v} = \mathbf{v} + \mathbf{0} = \mathbf{v} + (\mathbf{u} + \mathbf{w}) = (\mathbf{u} + \mathbf{v}) + \mathbf{w} = \mathbf{0} + \mathbf{w} = \mathbf{w}.$$

□

Since this element is unique we should give it a name.

Subtraction in a Vector Space

Given any vector $\mathbf{u} \in V$ we have shown that there exists a unique vector $\mathbf{v} \in V$ satisfying $\mathbf{u} + \mathbf{v} = \mathbf{0}$. We will denote this vector by "$-\mathbf{u}$." Then for any vectors $\mathbf{u}, \mathbf{v} \in V$ we define the notation

$$\text{“}\mathbf{u} - \mathbf{v}\text{”} := \mathbf{u} + (-\mathbf{v}).$$

The concept of subtraction can be used to establish the following facts (proof omitted):

- $\forall a \in \mathbb{F}$, $\mathbf{u} \in V$, $(-a)\mathbf{u} = a(-\mathbf{u}) = -(a\mathbf{u})$.
- $\forall a \in \mathbb{F}$, $a\mathbf{0} = \mathbf{0}$.
- $\forall u \in V$, $0\mathbf{u} = \mathbf{0}$.

The general concept of is quite abstract, but it is based on the following familiar example.

The Prototype: Cartesian Coordinates

Let $\mathbb{R}^n$ denote the set of ordered $n$tuples of real numbers:

$$\mathbb{R}^n := \{\mathbf{x} = (x_1, \ldots, x_n) : x_i \in \mathbb{R} \text{ for all } i\}.$$

It is easy (and boring) to check that the following operations make the set $\mathbb{R}^n$ in to a vector space over the field of scalars $\mathbb{R}$:

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) := (x_1 + y_1, \ldots, x_2 + y_2)$$

[42] I will use boldface font to distinguish vectors from scalars.

[43] There are some very special exceptions. For example, we will see below that there is a reasonable vector product in the Cartesian plane $\mathbb{R}^2$ which is defined by complex numbers. Also, it is sometimes possible to define a "dot product" operation $\bullet : V \times V \to \mathbb{F}$ taking pairs of vectors to scalars.

$$a \cdot (x_1, \ldots, x_n) := (ax_1, \ldots, ax_n).$$

Furthermore, the vector space structure of Cartesian coordinates can be viewed in terms of "head-to-tail addition" of direct line segments in Euclidean space. This idea goes back at least to Isaac Newton, who used it to describe forces acting on rigid bodies.

Head-To-Tail Addition of Vectors

The vector $\mathbf{u} = (u_1, \ldots, u_n) \in \mathbb{R}^n$ can be viewed as a directed line segment with tail at the origin $\mathbf{0} = (0, \ldots, 0)$ and head at the point $(u_1, \ldots, u_n)$. (Picture omitted.) Then we can compute the sum of two vectors by lifting one line segment and placing its tail at the head of the other line segment. (Picture omitted again.) The length of any line segment can be computed using the generalized Pythagorean Theorem

$$\|\mathbf{u}\| = +\sqrt{u_1^2 + \cdots + u_n^2},$$

which can be used to establish the following *triangle inequality for vector addition*:

$$\|\mathbf{u} + \mathbf{v}\| \leqslant \|\mathbf{u}\| + \|\mathbf{v}\|.$$

(Picture omitted.)

So what? The point is that the complex numbers $\mathbb{C}$ can be viewed as a vector space over the field $\mathbb{R}$. In fact, this structure is isomorphic to (essentially the same as) as the vector space structure on the Cartesian plane.

The Complex Plane as a Real Vector Space

For all real numbers $a, b, c, d \in \mathbb{R}$ recall that we have

$$\begin{aligned} a + bi = c + di \text{ in } \mathbb{C} &\Leftrightarrow a = c \text{ and } b = d \text{ in } \mathbb{R} \\ &\Leftrightarrow (a, b) = (c, d) \text{ in } \mathbb{R}^2. \end{aligned}$$

Following Hamilton, this allows us to identify the complex number $a + bi \in \mathbb{C}$ with the ordered pair of real numbers $(a, b) \in \mathbb{R}^2$. This is more than just a convenient notation, because of the following two facts:

- Addition of vectors corresponds to addition of complex numbers.

- Scalar multiplication of vectors by real numbers corresponds to regular multiplication of complex numbers by real numbers.

This observation seems rather trivial, but it has far-reaching consequences. In particular, it allows us to view each complex number as a 2×2 matrix with real entries, and this unlocks the true meaning of complex numbers. To see this, let me recall the relationship between linear functions and matrices. I'm sure you have used this idea in your linear algebra class, even if you didn't see it spelled out abstractly.

Linear Functions and Matrices

Consider the vector space $\mathbb{R}^n$ over the field $\mathbb{R}$. We say that a function $f : \mathbb{R}^n \to \mathbb{R}^n$ is *linear*[44] if for all scalars $a, b \in \mathbb{R}$ and for all vectors $\mathbf{u}, \mathbf{v} \in \mathbb{R}^n$ we have

$$f(a\mathbf{u} + b\mathbf{v}) = af(\mathbf{u}) + bf(\mathbf{v}).$$

In this case, I claim that we can represent the function f as an $n \times n$ matrix $[f]$ of real numbers. To be specific, we define the standard basis vector $\mathbf{e}_i$ with ith coordinate equal to 1 and all other coordinates equal to 0:

$$\mathbf{e}_i := (0, 0, \ldots, 0, 1, 0, \ldots, 0).$$

Then we let $[f]$ be the $n \times n$ array of numbers whose ith column is the vector $f(\mathbf{e}_i)$:

$$[f] := \begin{pmatrix} | & | & & | \\ f(\mathbf{e}_1) & f(\mathbf{e}_2) & \cdots & f(\mathbf{e}_n) \\ | & | & & | \end{pmatrix}.$$

For any $\mathbf{x} \in \mathbb{R}^n$ we let $[\mathbf{x}]$ denote the vertical column vector with the same entries. Then we define the column vector $[f][\mathbf{x}]$ as follows:

$$[f][\mathbf{x}] := [f(\mathbf{x})].$$

We can think of this as some kind of "multiplication." Finally, for any two linear functions $f, g : \mathbb{R}^n \to \mathbb{R}^n$ we define the "matrix product" $[f][g]$ as the matrix of the composite function $f \circ g : \mathbb{R}^n \to \mathbb{R}^n$:

$$[f][g] := [f \circ g].$$

In summary, we have defined a "multiplication" operation on the set of $n \times n$ matrices, which is associative but not generally commutative. The details for how to compute this multiplication were spelled out in your linear algebra class.

[44] To emphasize the field of scalars, we sometimes say that this function is $\mathbb{R}$-*linear*.

Let's see some examples. First, let $\mathrm{id} : \mathbb{R}^2 \to \mathbb{R}^2$ be the *identity function* (i.e., the "do-nothing function") which sends each vector to itself:

$$\mathrm{id}(x, y) = (x, y) \text{ for all } (x, y) \in \mathbb{R}^2.$$

To compute the matrix $[\mathrm{id}]$ we need to know what the function id does to the standard basis vectors $(1, 0)$ and $(0, 1)$, which is very easy:

$$\mathrm{id}(1, 0) = (1, 0) \quad \text{and} \quad \mathrm{id}(0, 1) = (0, 1).$$

Then the matrix is defined by

$$[\mathrm{id}] := \begin{pmatrix} | & | \\ \mathrm{id}(1,0) & \mathrm{id}(0,1) \\ | & | \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

We observe that this matrix, indeed, sends each column vector to itself:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1x + 0y \\ 0x + 1y \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix}.$$

Next, let $r : \mathbb{R}^2 \to \mathbb{R}^2$ be the function that rotates each vector counterclockwise by 90° around the origin. It is easy to see that this function is **linear** because rotation preserves scaling and addition of vectors. To compute the matrix, we observe (picture omitted) that

$$r(1, 0) = (0, 1) \quad \text{and} \quad r(0, 1) = (-1, 0).$$

Thus the matrix is defined by

$$[r] := \begin{pmatrix} | & | \\ r(1,0) & r(0,1) \\ | & | \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

and the general column vector gets rotated as follows:

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0x - 1y \\ 1x + 0y \end{pmatrix} = \begin{pmatrix} -y \\ x \end{pmatrix}.$$

More generally, let $r_\theta : \mathbb{R}^2 \to \mathbb{R}^2$ be the function that rotates every vector counterclockwise by angle θ around the origin. This function is also linear. To compute the matrix we observe (picture omitted) that

$$r_\theta(1, 0) = (\cos\theta, \sin\theta) \quad \text{and} \quad r_\theta(0, 1) = (-\sin\theta, \cos\theta).$$

Thus we have

$$[r_\theta] := \begin{pmatrix} | & | \\ r_\theta(1,0) & r_\theta(0,1) \\ | & | \end{pmatrix} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix},$$

and the general column vector gets rotated as follows:

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x\cos\theta - y\sin\theta \\ x\sin\theta + y\cos\theta \end{pmatrix}.$$

(Pictures omitted.)

These ideas lead to a much more conceptual proof of Ptolemy's angle sum identities. If you remember this proof then you will never need to memorize a trigonometric identity again.

Modern Proof of the Angle Sum Identities. Let $\alpha, \beta \in \mathbb{R}$ be any angles, and consider the rotation functions $r_\alpha, r_\beta : \mathbb{R}^2 \to \mathbb{R}^2$. Observe that the composite function satisfies

$$r_\alpha \circ r_\beta = r_{\alpha+\beta}.$$

Indeed, if we first rotate the plane by β, and then by α, then the net result is to rotate the plane by angle $\alpha + \beta$. (What could be easier?) Then since composition of linear functions corresponds to matrix multiplication, we obtain

$$\begin{aligned}
&\begin{pmatrix} \cos(\alpha+\beta) & -\sin(\alpha+\beta) \\ \sin(\alpha+\beta) & \cos(\alpha+\beta) \end{pmatrix} \\
&= [r_{\alpha+\beta}] \\
&= [r_\alpha \circ r_\beta] \\
&= [r_\alpha][r_\beta] \\
&= \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \begin{pmatrix} \cos\beta & -\sin\beta \\ \sin\beta & \cos\beta \end{pmatrix} \\
&= \begin{pmatrix} \cos\alpha\sin\beta - \sin\alpha\cos\beta & -\cos\alpha\sin\beta - \sin\alpha\cos\beta \\ \sin\alpha\cos\beta + \cos\alpha\sin\beta & -\sin\alpha\sin\beta + \cos\alpha\cos\beta \end{pmatrix}.
\end{aligned}$$

And comparing entries gives the result. □

Now we come to the main point of this section. We will use the ideas of vector spaces and linear functions to express each complex number as a real 2×2 matrix in such a way that addition and multiplication of complex numbers becomes addition and multiplication of matrices.[45] Here is the statement.

Complex Numbers as Real Matrices

For any complex number $\alpha \in \mathbb{C}$ we define the function $f_\alpha : \mathbb{C} \to \mathbb{C}$ by multiplication:

$$f_\alpha(\beta) := \alpha\beta \text{ for all } \beta \in \mathbb{C}.$$

[45] Other important operations on complex numbers such as conjugation and absolute value also get sent to natural operations on matrices. You will investigate this on the homework.

I claim that these functions satisfy the following properties:

$$f_{\alpha+\beta} = f_\alpha + f_\beta \quad \text{and} \quad f_{\alpha\beta} = f_\alpha \circ f_\beta.$$

Furthermore, if we view $\mathbb{C} = \mathbb{R}^2$ as a real vector space then I claim that the function $f_\alpha : \mathbb{R}^2 \to \mathbb{R}^2$ is $\mathbb{R}$-linear, and if $\alpha = a + ib$ then the corresponding matrix is

$$[f_\alpha] = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

Proof. For all $\alpha, \beta, \gamma \in \mathbb{C}$ we observe that

$$f_{\alpha+\beta}(\gamma) = (\alpha + \beta)\gamma = \alpha\gamma + \beta\gamma = f_\alpha(\gamma) + f_\beta(\gamma),$$

which implies that $f_{\alpha+\beta}$ and $f_\alpha + f_\beta$ are the same function. And we observe that

$$f_{\alpha\beta}(\gamma) = (\alpha\beta)\gamma = \alpha(\beta\gamma) = f_\alpha(f_\beta(\gamma)) = (f_\alpha \circ f_\beta)(\gamma),$$

which implies that $f_{\alpha\beta}$ and $f_\alpha \circ f_\beta$ are the same function. Next, for all complex numbers $\alpha, \beta, \gamma \in \mathbb{C}$ and real numbers $b, c \in \mathbb{R}$ we observe that

$$\begin{aligned} f_\alpha(b\beta + c\gamma) &= \alpha(b\beta + c\gamma) \\ &= b(\alpha\beta) + c(\alpha\gamma) \\ &= bf_\alpha(\beta) + cf_\alpha(\gamma), \end{aligned}$$

hence the function f_α is $\mathbb{R}$-linear. To compute the matrix, suppose that $\alpha = a + bi$ for $a, b \in \mathbb{R}$. Then we observe how f_α acts on the standard basis vectors $1 = 1 + 0i$ and $i = 0 + 1i$:

$$f_\alpha(1 + 0i) = (a + bi)(1 + 0i) = a + bi \quad \text{and} \quad f_\alpha(0 + 1i) = (a + bi)(0 + 1i) = -b + ai.$$

It follows that

$$[f_\alpha] = \begin{pmatrix} | & | \\ f_\alpha(1) & f_\alpha(i) \\ | & | \end{pmatrix} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

□

One can check that the matrix representation of complex numbers sends addition and multiplication of numbers to addition and multiplication of matrices, and there are two ways to do this. First, we can use the fact that addition and multiplication of matrices correspond to addition and composition of linear functions. Thus, for all $\alpha, \beta \in \mathbb{C}$ we have

$$[f_{\alpha+\beta}] = [f_\alpha + f_\beta] = [f_\alpha] + [f_\beta] \quad \text{and} \quad [f_{\alpha\beta}] = [f_\alpha \circ f_\beta] = [f_\alpha][f_\beta].$$

Alternatively, you will verify these identities on the homework using matrix computations.

Let me emphasize what we have done here. We have represented each complex number as a real 2×2 matrix in such as way that the structure of the complex numbers is reflected in the structure of the corresponding matrices. This is similar in spirit to Hamilton's interpretation of complex numbers as formal pairs of real numbers with a strange multiplication operation. However, the matrix interpretation is more natural because the multiplication is not strange; indeed, it is just the multiplication of matrices, which corresponds to functional composition. Furthermore, this interpretation naturally incorporates de Moivre's Formula via the properties of rotation functions.

Let's see some examples. First, we observe that $1 \in \mathbb{C}$ gets sent to the identity matrix:

$$[f_1] = [f_{1+0i}] = \begin{pmatrix} 1 & -0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Indeed, "multiplication by 1" is the same as the "do-nothing function." Next, we observe that any real number $r \in \mathbb{R} \subseteq \mathbb{C}$ gets send to a so-called "scalar matrix":

$$[f_r] = [f_{r+0i}] = \begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix} = r \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

This corresponds to the function $f_r : \mathbb{R}^2 \to \mathbb{R}^2$ that scales every vector simultaneously by the factor r. We call this a "dilation function." Finally, we observe that a general complex number $r\cos\theta + ir\sin\theta$ gets sent to the following matrix:

$$[f_{r\cos\theta + ir\sin\theta}] = \begin{pmatrix} r\cos\theta & -r\sin\theta \\ r\sin\theta & r\cos\theta \end{pmatrix} = r \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}.$$

Geometrically, this is the function that simultaneously rotates the plane counterclockwise by angle θ and dilates the plane by the factor r.

This point of view was first stated by Arthur Cayley in *A Memoir on the Theory of Matrices* (1858). However the notation of matrix multiplication was not taken seriously until the 1920s, when it became a necessary ingredient in Werner Heisenberg's interpretation of quantum mechanics. As far as I know, the first appearance of complex numbers as real matrices appears in Joseph Wedderburn's *Lectures on Matrices* (1934), which is based on his lectures given in the 1920s at Princeton University.

In summary, if you ask a mathematician today what the complex numbers "really are," they will probably respond with the following interpretation.

The Functional Interpretation of Complex Numbers

The complex numbers can be viewed as the collection of rotation-dilation functions in the plane. To be specific, the complex number $r(\cos\theta + i\sin\theta)$ in polar coordinates corresponds to the function $\mathbb{R}^2 \to \mathbb{R}^2$ that rotates counterclockwise by θ and (simultaneously) dilates by a factor of r. (These kinds of functions are sometimes called *amplitwists*.) This

interpretation has the advantage of

- being expressed purely in terms of real numbers,
- and still preserving the geometric meaning of complex numbers.

In particular, the imaginary number "$\sqrt{-1}$" has a non-imaginary interpretation:

$$\text{“}\sqrt{-1}\text{”} = \text{ rotation by } 90^\circ.$$

7 Fundamental Theorem of Algebra

7.1 Introduction

The Fundamental Theorem of Algebra (FTA) can be stated in many equivalent ways. In its most basic form, it says that every non-constant polynomial $f(x) \in \mathbb{C}[x]$ with coefficients in $\mathbb{C}$ has a root in $\mathbb{C}$.[46] Suppose that $\deg(f) = n \geqslant 1$ and call this root $\alpha_1 \in \mathbb{C}$. Then from Descartes' Theorem we can write

$$f(x) = (x - \alpha_1)g(x) \text{ for some polynomial } g(x) \in \mathbb{C}[x] \text{ with } \deg(g) = n - 1.$$

If $n - 1 \geqslant 1$ then by applying the FTA again we conclude that $g(x)$ has some complex root $\alpha_2 \in \mathbb{C}$, and hence

$$f(x) = (x - \alpha_1)(x - \alpha_2)h(x) \text{ for some polynomial } h(x) \in \mathbb{C}[x] \text{ with } \deg(h) = n - 2.$$

By continuing in this way we conclude that that

$$f(x) = (x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n)c \quad \text{ for some } \alpha_1, \ldots, \alpha_n, c \in \mathbb{C}.$$

In other words, every non-constant polynomial in $\mathbb{C}[x]$ splits over $\mathbb{C}$, which is an equivalent way to state the FTA. Furthermore, if $f(x) \in \mathbb{R}[x]$ has **real** coefficients, then we will see below that the non-real roots come in complex conjugate pairs. Thus we conclude that

$$f(x) = c(x - a_1)\cdots(x - a_k)(x - \alpha_1)(x - \alpha_1^*)\cdots(x - \alpha_\ell)(x - \alpha_\ell^*)$$

for some real numbers $a_1, \ldots, a_k, c \in \mathbb{R}$ and non-real complex numbers $\alpha_1, \ldots, \alpha_\ell$. But for all $\alpha \in \mathbb{C}$ we know that $\alpha + \alpha^*$ and $\alpha\alpha^*$ are **real numbers**, hence we conclude that any non-constant real polynomial can be factored as a product of real polynomials of degrees 1 and 2:

$$f(x) = c\prod_{i=1}^{k}(x - a_i)\prod_{j=1}^{\ell}(x^2 - (\alpha_j + \alpha_j^*)x + \alpha_j\alpha_j^*).$$

[46] The FTA is similar in spirit to the Intermediate Value Theorem, which guarantees the existence of a real root, but does not give any formula for this root. For this reason one might say that the Fundamental Theorem of Algebra is not very "algebraic." In fact, it is more common to see a proof of the FTA in courses on complex analysis or topology. In this course I will present the most algebraic proof that I know, due to Pierre-Simon Laplace (1795). This proof will lead us through several important topics of algebra, and the only non-algebraic ingredient will be the Intermediate Value Theorem, which we already discussed.

We will see below that that this statement is also equivalent to the FTA; in fact it was the original form of the theorem.

Before going into more detail, here is a brief historical sketch:

- Since the introduction of the complex numbers, it was generally believed that any real polynomial of degree n should possess n roots (possibly repeated); if not in the complex domain, then in some larger numerical domain. This thesis was first stated by Albert Girard in *L'invention en algèbre* (1629).
- Gottried Wilhelm Leibniz raised some doubts in 1702 when he claimed that the real polynomial $x^4 + a^4$ ($a \in \mathbb{R}$) **cannot** be factored into two real quadratic polynomials. We will see below that he was mistaken.
- Euler (1749) cleared up the matter by proving rigorously that every real polynomial of degree 4 is a product of two real polynomials of degree 2. He confidently stated that the FTA should hold in general and he sketched out some ideas for a proof, but the algebraic computations became too difficult to manage.
- Lagrange cleaned up Euler's argument, but it was still too complicated to be convincing. Laplace used a clever trick to simplify the Euler-Lagrange proof. This is the proof that we will see below.
- But this was not the last word. Gauss objected that Laplace's proof assumes without justification that the roots exist in some field containing $\mathbb{C}$, before proving that the roots actually lie in $\mathbb{C}$. This gap was finally filled by Leopold Kronecker in 1887.
- Meanwhile, another method of attack used "topological reasoning" similar to the Intermediate Value Theorem.[47] Gauss gave a proof along these lines, which was generally accepted as the first correct proof of the FTA.
- However, from the modern point of view, Gauss' topological proof is also not completely rigorous. One could say that the details were filled in by Karl Weierstrass, a colleague of Leopold Kronecker at the University of Berlin.
- Thus, despite the existence of many diverse purported proofs of the FTA, the matter was not completely settled until the late 19th century. This is a testament to the subtlety of the theorem.

In this chapter we will follow one thread of this story, starting with Leibniz' mistake and ending with Laplace's proof. The context for Leibniz' work is the integration of rational functions by partial fractions.

[47] By this I mean that two curves in the plane that seem to cross based on their pictures, do indeed cross at some point.

7.2 Partial Fractions

The Fundamental Theorem of Calculus was discovered in the 1660s, independently by Isaac Newton and Gottfried Wilhelm Leibniz. For the next 100 years mathematicians were engaged with working out all of the details, until the final form of the theory was written down in Euler's *Introductio* (1770). Students of calculus will know that derivation is much easier than integration/antiderivation. Thus, the most difficult problem in these early years was to compute integrals for all of the basic functions.

The foundational result was actually discovered in the 1630s by Pierre de Fermat, and was one of main inspirations for the Fundamental Theorem of Calculus. I will present the result in modern form.[48]

Fermat's Power Rule

For all integers $n \in \mathbb{Z}$ we have

$$\int x^n \, dx = \begin{cases} \frac{1}{n+1} x^{n+1} & \text{if } n \neq -1, \\ \ln|x| & \text{if } n = -1. \end{cases}$$

Note that this result allows us to integrate any polynomial function:

$$\int \left(\sum_{k \geqslant 0} a_k x^k \right) dx = \sum_{k \geqslant 0} a_k \int x_k \, dx = \sum_{k \geqslant 0} \frac{a_k}{k+1} x^{k+1}.$$

The next most basic kind of functions are the so-called "rational functions." In modern terms these defined as "formal fractions of polynomials."

The Field of Rational Functions

Consider the ring of polynomials $\mathbb{R}[x]$ with real coefficients and let $\mathbb{R}(x)$ denote the set of formal fractions of polynomials, where the denominator is not the zero polynomial:

$$\mathbb{R}(x) := \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in \mathbb{R}[x] \text{ and } g(x) \neq 0(x) \right\}.$$

[48] Actually, this result was independently discovered by several mathematicians in the 1630s and 1640s, but Fermat's proof was the most convincing. See Boyer's *History of Calculus and its Conceptual Development.*

By convention, we define equality of formal fractions as follows:

$$\frac{f_1(x)}{g_1(x)} = \frac{f_2(x)}{g_2(x)} \quad \Leftrightarrow \quad f_1(x)g_2(x) = f_2(x)g_1(x).$$

With this identification, one can check that the usual addition and multiplication of fractions makes the set $\mathbb{R}(x)$ into a field. We can think of the polynomials as a subring $\mathbb{R}[x] \subseteq \mathbb{R}(x)$ by making the following identification:

$$f(x) = \frac{f(x)}{1} \quad \text{for all } f(x) \in \mathbb{R}[x].$$

This is completely analogous to the construction of the field $\mathbb{Q}$ from the ring $\mathbb{Z}$.

I'm sure you have seen the method of partial fractions in your Calculus course.

It is possible to integrate certain rational functions by substitution. Thus, for any real number $a \in \mathbb{R}$ and for any integer $n \geqslant 2$ we have

$$\int \frac{1}{(x+a)^n}\,dx = \frac{-1}{(n-1)(x+a)^{n-1}}.$$

And for any nonzero polynomial $f(x) \in \mathbb{R}[x]$ with derivative $f'(x)$ we have

$$\int \frac{f'(x)}{f(x)}\,dx = \ln|f(x)|.$$

For example, if $f(x) = x^2 + c$ for some $c \in \mathbb{R}$ then this becomes

$$\int \frac{2x}{x^2+c}\,dx = \ln|x^2+c|.$$

These results were known to Leibniz. However, he described the natural logarithm as the "quadrature of the hyperbola," i.e., the area under the graph of the function $1/x$.[49] Leibniz also discovered the integral of $1/(x^2+1)$ is related to the "quadrature of the circle." In modern language, this means that

$$\int \frac{1}{x^2+1}\,dx = \arctan(x).$$

It might seem that these few examples represent meager progress toward the integration of all rational functions. Amazingly, however, it follows from the FTA that any rational function whatsoever can be reduced to the previous basic forms. The following result was proved by Leibniz in 1702 paper, using the method of "partial fractions."

[49]The modern notation of exponential and logarithmic functions was developed by Euler.

Integration of Rational Functions

Consider any rational function $f(x)/g(x) \in \mathbb{R}(x)$ with $\deg(g) \geqslant 1$, and suppose that the polynomial $g(x)$ can be factored as a product of real polynomials of degrees 1 and 2. Then the integral of $f(x)/g(x)$ can be expressed explicitly in terms the "quadrature of the hyperbola" (i.e., the natural logarithm) and the "quadrature of the circle" (i.e., the inverse tangent function).

The theorem on partial fractions can be stated for any Euclidean domain, including the integers $\mathbb{Z}$ and and the ring of polynomials $\mathbb{F}[x]$ over any field $\mathbb{F}$. Before stating the general theorem I will show you a few illustrative examples. First we will use the method to compute the following integral:

$$\int \frac{x^2 + 2x + 1}{(x-1)(x^2+1)}\, dx.$$

The theorem below tells us that there exist some constants $a, b, c \in \mathbb{R}$ such that we have the following identity of formal fractions of polynomials:

$$\begin{aligned}\frac{x^2 + 2x + 1}{(x-1)(x^2+1)} &= \frac{a}{x-1} + \frac{bx+c}{x^2+1} \\ &= \frac{a(x^2+1) + (bx+c)(x-1)}{(x-1)(x^2+1)} \\ &= \frac{(a+b)x^2 + (c-b)x + (a-c)}{(x-1)(x^2+1)}.\end{aligned}$$

Since the denominators are the same, the numerators must also be the same:

$$x^2 + 2x + 1 = (a+b)x^2 + (c-b)x + (a-c).$$

And since this is an identity of formal polynomials, the coefficients must be the same:

$$\begin{cases} a & + & b & + & 0 & = & 1, \\ 0 & - & b & + & c & = & 2, \\ a & + & 0 & - & c & = & 1. \end{cases}$$

By solving this linear system we obtain $(a, b, c) = (2, -1, 1)$, and hence

$$\begin{aligned}\int \frac{x^2 + 2x + 1}{(x-1)(x^2+1)}\, dx &= \int \left(\frac{2}{x-1} + \frac{-x+1}{x^2+1} \right) dx \\ &= \int \frac{2}{x-1}\, dx + \int \frac{-x}{x^2+1}\, dx + \int \frac{1}{x^2+1}\, dx \\ &= 2\ln|x-1| - \frac{1}{2}\ln|x^2+1| + \arctan(x).\end{aligned}$$

Next I will show you how the theory of partial fractions applies to integers. This is not strictly relevant to the Fundamental Theorem of Algebra, but it fits well with other topics in this course. For example, we will try to expand 7/15 into "partial fractions," based on the factorization of the denominator:

$$\frac{7}{15} = \frac{7}{3 \cdot 5} = \frac{?}{3} + \frac{?}{5}.$$

The key here is that the factors 3 and 5 have no common prime divisor; in other words, that $\gcd(3, 5) = 1$. It follows from Bézout's Identity that there exist some (non-unique) integers $x, y \in \mathbb{Z}$ satisfying $1 = 5x + 3y$. By trial and error we see that $1 = 5(2) + 3(-3)$. Then we divide both sides by 15 to obtain

$$\frac{1}{15} = \frac{5(2) + 3(-3)}{15} = \frac{5(2)}{15} + \frac{3(-3)}{15} = \frac{2}{3} + \frac{-3}{5}.$$

Now we multiply both sides by 7:

$$\frac{7}{15} = \frac{14}{3} + \frac{-21}{5}.$$

You might be satisfied with this, but I don't like it because the solution is not unique. Indeed, we also have

$$\frac{7}{15} = \frac{11}{3} + \frac{-16}{5}.$$

In order to get a unique result, we should express each of the partial fractions 14/3 and −21/5 in proper form. To do this we compute the quotient and remainder of each numerator, modulo its denominator:

$$\begin{aligned} 14 &= 4 \cdot 3 + 2, \\ -21 &= (-5) \cdot 5 + 4. \end{aligned}$$

(Note that the quotient is allowed to be negative, while the remainder is always positive.) It follows from this that

$$\frac{14}{3} = \frac{4 \cdot 3 + 2}{3} = 4 + \frac{2}{3}$$

and

$$\frac{-21}{5} = \frac{(-5) \cdot 5 + 4}{5} = -5 + \frac{4}{5}.$$

Finally, adding these two expressions gives

$$\begin{aligned} \frac{7}{15} &= \frac{14}{3} + \frac{-21}{5} = \left(4 + \frac{2}{3}\right) + \left(-5 + \frac{4}{5}\right) \\ \frac{7}{15} &= -1 + \frac{2}{3} + \frac{4}{5}. \end{aligned}$$

This is the **unique** partial fraction expansion of 7/15. Finally, I will show you an example that illustrates a possible complication:

The denominator might have a repeated prime factor.

Consider the fraction 5/12 and note that 2 is repeated in the prime factorization of 12:

$$12 = 2 \cdot 2 \cdot 3 = 2^2 \cdot 3 = 4 \cdot 3.$$

First we use the fact that $\gcd(4, 3) = 1$ to find some (non-unique) $x, y \in \mathbb{Z}$ satisfying $1 = 4x + 3y$. By trial and error we find that $1 = 4(1) + 3(-1)$. Then we divide by 12 to obtain

$$\frac{1}{12} = \frac{4(1) + 3(-1)}{12} = \frac{4(1)}{12} + \frac{3(-1)}{12} = \frac{1}{3} + \frac{-1}{4}$$

and multiply by 5 to obtain

$$\frac{5}{12} = \frac{5}{3} + \frac{-5}{4}.$$

As before, we put 5/3 in proper form by computing the quotient and remainder of 5 mod 3:

$$\frac{5}{3} = \frac{1 \cdot 3 + 2}{3} = 1 + \frac{2}{3}.$$

But the procedure for $-5/4$ is slightly different because 4 is **not prime**. Instead, it is a power of the prime 2, so we compute the quotient and remainder of the numerator -5 modulo 2:

$$\frac{-5}{4} = \frac{(-3) \cdot 2 + 1}{4} = \frac{-3}{2} + \frac{1}{4}.$$

Then we repeat the process for the fraction $-3/2$:

$$\frac{-3}{2} = \frac{(-2) \cdot 2 + 1}{2} = -2 + \frac{1}{2}.$$

(More generally, for any fraction a/p^e with p prime, we will repeatedly divide the numerator by p to obtain an expansion of the form

$$\frac{a}{p^e} = c + \frac{r_1}{p} + \frac{r_2}{p^2} + \cdots + \frac{r_e}{p^e},$$

where each remainder r_i satisfies $0 \leqslant r_i < p$.) Finally, we put everything together to obtain the unique partial fraction expansion of 5/12:

$$\begin{aligned}
\frac{5}{12} &= \frac{5}{3} + \frac{-5}{4} \\
&= \left(1 + \frac{2}{3}\right) + \frac{-5}{4} \\
&= 1 + \frac{2}{3} + \left(\frac{-3}{2} + \frac{1}{4}\right) \\
&= 1 + \frac{2}{3} - 2 + \frac{1}{2} + \frac{1}{4}
\end{aligned}$$

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

It is important to observe that the numerator of $1/4$ must be less than 2 because 4 is a power of the prime 2.

Now that you have seen all of the possible complications, I will state and prove the general theorem.

Theorem (Partial Fraction Expansion)

Let (R, N) be a Euclidean domain. Recall, this means that R is an integral domain and $N : R\backslash\{0\} \to \mathbb{N}$ is a "norm function" sending nonzero elements to positive integers and satisfying "division with remainder":

For all $a, b \in R$ with $b \neq 0$ there exist some $q, r \in R$ such that

$$\begin{cases} a = qb + r, \\ r = 0 \text{ or } N(r) < N(b). \end{cases}$$

Recall from Chapter ? that any nonzero element of a Euclidean domain has a unique prime factorization. Now consider any elements $a, b \in R$ with $b \neq 0$ and suppose that b has the following prime factorization:

$$b = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}.$$

Then I claim that there exist[50] some elements $c, r_{ij} \in R$ satisfying

$$\frac{a}{b} = c + \sum_{i=1}^{k} \sum_{j=1}^{e_i} \frac{r_{ij}}{p_j},$$

where for all indices i, j we have either $r_{ij} = 0$ or $N(r_{ij}) < N(p_i)$.

Proof. Since $p_1^{e_1}$ is coprime to $p_2^{e_2} p_3^{e_3} \cdots p_k^{e_k}$ we know from Bèzout's Identity that there exist some elements $c_1, c \in R$ such that

$$1 = c_1 p_2^{e_2} p_3^{e_3} \cdots p_k^{e_k} + c p_1^{e_1}.$$

Now multiply both sides by the fraction a/b to obtain

$$\frac{a}{b} = \frac{a c_1 p_2^{e_2} p_3^{e_3} \cdots p_k^{e_k}}{b} + \frac{a c p_1^{e_1}}{b}.$$

[50] In many cases, including all cases in this course, these elements are also unique, but we won't bother to prove this because we don't need it.

Then we can factor the denominator and cancel common factors to obtain

$$\frac{a}{b} = \frac{ac_1 \cancel{p_2^{e_2} p_3^{e_3} \cdots p_k^{e_k}}}{p_1^{e_1} \cancel{p_2^{e_2} \cdots p_k^{e_k}}} + \frac{ac \cancel{p_1^{e_1}}}{\cancel{p_1^{e_1}} p_2^{e_2} \cdots p_k^{e_k}} = \frac{ac_1}{p_1^{e_1}} + \frac{ac}{p_2^{e_2} p_3^{e_3} \cdots p_k^{e_k}}.$$

It follows by induction on k that there exist elements $a_1, a_2, \ldots, a_k \in R$ satisfying

$$\frac{a}{b} = \frac{a_1}{p_1^{e_1}} + \frac{a_2}{p_2^{e_2}} + \cdots + \frac{a_k}{p_k^{e_k}}.$$

Finally, we will expand each fraction a/p^e in the standard form $c + r_1/p + r_2/p^2 + \cdots + r_e/p^e$ for some elements $r_1, \ldots, r_e \in R$ satisfying r_j or $N(r_j) < N(p)$. We do this by dividing the numerator by the prime p to obtain

$$\frac{a}{p^e} = \frac{q_e p + r_e}{p^e} = \frac{q_e}{p^{e-1}} + \frac{r_e}{p^e} \quad \text{with } r_e = 0 \text{ or } N(r_e) < N(p).$$

Then we apply the same process to q_e/p^{e-1}, and the result follows by induction. □

This proof really just describes an algorithm. To end this chapter, let me show you how the algorithm works in the case of polynomials. This is not necessarily the fastest way to compute partial fractions expansions of rational functions, but it illustrates the general theory. To be specific, we will compute the following integral:

$$\int \frac{1}{(x+1)^2(x^2+1)}\, dx.$$

Bézout's Identity tells us that there exist some polynomials $f(x), g(x) \in \mathbb{R}[x]$ satisfying

$$1 = f(x)(x+1)^2 + g(x)(x^2+1),$$

We can find such polynomials using the Euclidean algorithm. Since the two factors have the same degree 2, it doesn't matter which is the divisor. First we divide $(x+1)^2 = x^2 + 2x + 1$ by $x^2 + 1$ to obtain

$$(x+1)^2 = 1(x^2+1) + 2x.$$

Then we divide $x^2 + 1$ by $2x$ to obtain

$$x^2 + 1 = (x/2)(2x) + 1.$$

Finally, we divide $2x$ by 1 to obtain

$$2x = 1(2x) + 0.$$

Since the last nonzero remainder 1, this confirms that $\gcd((x+1)^2, x^2+1) = 1$ in the ring $\mathbb{R}[x]$. We could now find $f(x)$ and $g(x)$ by back-substitution, but I prefer the following method. Consider the set of triples $f(x), g(x), h(x) \in \mathbb{R}[x]$ satisfying $f(x)(x+1)^2 + g(x)(x^2+1) = h(x)$.

We begin with the obvious triples $1, 0, (x+1)^2$ and $0, 1, x^2+1$. Then we perform row operations corresponding to the computations above, to obtain the following table:

$f(x)$	$g(x)$	$h(x)$	row operation
1	0	$(x+1)^2$	R_1
0	1	x^2+1	R_2
1	-1	$2x$	$R_3 = R_1 - 1 \cdot R_2$
$-x/2$	$1+x/2$	1	$R_4 = R_2 - (x/2)R_3$

The final row tells us that

$$(-x/2)(x+1)^2 + (1+x/2)(x^2+1) = 1.$$

Then we divide both sides by $(x+1)^2(x^2+1)$ to obtain

$$\begin{aligned}\frac{1}{(x+1)^2(x^2+1)} &= \frac{(-x/2)\cancel{(x+1)^2}}{\cancel{(x+1)^2}(x^2+1)} + \frac{(1+x/2)\cancel{(x^2+1)}}{(x+1)^2\cancel{(x^2+1)}} \\ &= \frac{-x/2}{x^2+1} + \frac{1+x/2}{(x+1)^2}.\end{aligned}$$

To complete the algorithm, we put the fraction $(1+x/2)/(x+1)^2$ in standard form by dividing the numerator by the prime factor $x+1$:

$$\frac{1+x/2}{(x+1)^2} = \frac{\frac{1}{2}(x+1)+\frac{1}{2}}{(x+1)^2} = \frac{1/2}{x+1} + \frac{1/2}{(x+1)^2}.$$

Finally, we conclude that

$$\begin{aligned}\frac{1}{(x+1)^2(x^2+1)} &= \frac{-x/2}{x^2+1} + \frac{1/2}{x+1} + \frac{1/2}{(x+1)^2} \\ \int \frac{1}{(x+1)^2(x^2+1)}\,dx &= \int \frac{-x/2}{x^2+1}\,dx + \int \frac{1/2}{x+1}\,dx + \int \frac{1/2}{(x+1)^2}\,dx \\ &= -\frac{1}{2}\cdot\frac{1}{2}\cdot\ln(x^2+1) + \frac{1}{2}\ln|x+1| + \frac{1}{2}\cdot\frac{-1}{x+1}.\end{aligned}$$

The question remains, whether every non-constant real polynomial can be factored into real polynomials of degree 1 and 2. Today we know that the FTA is true, and hence the answer is yes. In 1702, however, the situation was not so clear.

7.3 Leibniz' Mistake

As mentioned in the previous section, Pierre Fermat developed the method of partial fractions in 1702 in order to integrate rational functions. He realized that this method works whenever the denominator can be factored into real polynomials of degrees 1 and 2. Thus he posed the following problem:[51]

[51] See *Galois' Theory of Algebraic Equations* (2001), by Jean-Pierre Tignol, pages 74–75.

> *Now, this leads us to a question of utmost importance: whether all the rational quadratures may be reduced to the quadrature of the hyperbola and of the circle, which by our analysis above amounts to the following: whether every algebraic equation or real integral formula in which the indeterminate is rational can be decomposed into simpIe or plane real factors [= real factors of degree 1or 2].*

But he seems to have believed that this is **not** always possible. In fact, he proposed that for any real number $a > 0$, the polynomial $x^4 + a^4 \in \mathbb{R}[x]$ can **not** be factored as a product of real polynomials (in our language, that this polynomial is a prime element of the ring $\mathbb{R}[x]$). To see this, he first treated $x^4 + a^4$ as a difference of squares:

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

And then he treated each factor as a difference of squares:

$$x^4 + a^4 = \left(x - a\sqrt{\sqrt{-1}}\right)\left(x + a\sqrt{\sqrt{-1}}\right)\left(x - a\sqrt{-\sqrt{-1}}\right)\left(x + a\sqrt{-\sqrt{-1}}\right).$$

Finally, he claimed that no combination of these linear factors yields a polynomial with real coefficients, hence the antiderivative of $1/(x^4 + a^4)$ must be some new kind of function:

> *Therefore, $\int \frac{dx}{x^4+a^4}$ cannot be reduced to the squaring of the circle or the hyperbola by our analysis above, but founds a new kind of its own.*

Of course, we know that this conclusion is false because it contradicts the Fundamental Theorem of Algebra. In this section I will explain where Leibniz went wrong, and why he might have gotten confused.

But first, let me present some generalities about prime polynomials. Our first result is an algorithm that allows us to compute the rational roots of an integer polynomial in a finite amount of time.

The Rational Root Test

Let $f(x) = c_n x^n + \cdots + c_1 x + c_0 \in \mathbb{Z}[x]$ be a polynomial of degree n with integer coefficients, and suppose that $f(x)$ has a rational root $a/b \in \mathbb{Q}$ in lowest terms, i.e., with $\gcd(a, b) = 1$. In this case, I claim that

$$a | c_0 \quad \text{and} \quad b | c_n.$$

This leads to a finite list of potential rational roots, which we can test one by one.

Proof. Let $f(a/b) = 0$ for some $a, b \in \mathbb{Z}$ with $b \neq 0$ and $\gcd(a, b) = 1$. After multiplying both sides of this equation by b^n we obtain an equation of integers:

$$f(a/b) = 0$$

$$\begin{aligned} c_n(a/b)^n + \cdots + c_1(a/b) + c_0 &= 0 \\ b^n\left[c_n(a/b)^n + \cdots + c_1(a/b) + c_0\right] &= 0 \\ c_n a^n + c_{n-1}a^{n-1}b + \cdots + c_1 ab^{n-1} + c_0 b^n &= 0. \end{aligned}$$

Now by taking the term $c_0 b^n$ to one side, we have

$$\begin{aligned} c_0 b^n &= -c_n a^n - c_{n-1}a^{n-1}b - \cdots - c_1 ab^{n-1} \\ &= a\left[-c_n a^{n-1} - c_{n-1}a^{n-2}b - \cdots - c_1 b^{n-1}\right]. \end{aligned}$$

which implies that $a|c_0 b^n$. Then since $\gcd(a,b) = 1$, Euclid's Lemma implies that $a|c_0$. Similarly, by taking the term $c_n a^n$ to one side, we have

$$\begin{aligned} c_n a^n &= -c_{n-1}a^{n-1}b - \cdots - c_1 ab^{n-1} - c_0 b^n \\ &= b\left[-c_{n-1}a^{n-1} - \cdots - c_1 ab^{n-2} - c_0 b^{n-1}\right], \end{aligned}$$

hence $b|c_n a^n$. Then since $\gcd(a,b) = 1$, Euclid's Lemma implies that $b|c_n$. □

For example, consider the polynomial $f(x) = 3x^3 - 6x + 2 \in \mathbb{Z}[x]$. If $f(a/b) = 0$ for some rational number $a/b \in \mathbb{Q}$ in lowest terms, then the theorem tells us that $a|2$ and $b|3$, which leads to the following set of 8 potential rational roots:

$$\frac{a}{b} \in \left\{\pm 1, \pm 2, \pm\frac{1}{3}, \pm\frac{2}{3}\right\}.$$

But one can check that none of these is a root of $f(x)$, and hence $f(x)$ **has no rational root**. Incidentally, this also implies that the polynomial $f(x) = 3x^2 - 6x + 2$ is a prime element of $\mathbb{Q}[x]$, because of the following theorem.

Testing Primality of Low Degree Polynomials

Let $\mathbb{F}$ be a field and let $f(x) \in \mathbb{F}[x]$ be a polynomial of degree 2 or 3. Then

$$f(x) \text{ is prime in } \mathbb{F}[x] \quad \Leftrightarrow \quad f(x) \text{ has no root in } \mathbb{F}.$$

Proof. First suppose that $f(x)$ has a root $a \in \mathbb{F}$. Then from Descartes' Theorem we have $f(x) = (x-a)g(x)$ for some polynomial $g(x) \in \mathbb{F}[x]$ of strictly positive degree, and it follows that $f(x)$ is not prime. Conversely, suppose that $f(x)$ is not prime, so that $f(x) = g(x)h(x)$ for some polynomials $g(x), h(x) \in \mathbb{F}[x]$ of strictly positive degree. But then since

$$\deg(g) + \deg(h) = \deg(f) \in \{2, 3\}$$

we must have either $\deg(g) = 1$ or $\deg(h) = 1$ (or both). Without loss of generality, let us assume that $\deg(g) = 1$, so that $g(x) = ax + b$ for some $a, b \in \mathbb{F}$ with $a \neq 0$. It follows that $g(-b/a) = 0$ and hence $f(-b/a) = 0$. In other words, $f(x)$ has a root in $\mathbb{F}$. □

You may remember that we used this method at the end of Chapter 4 to prove that the polynomial $x^2 - d \in \mathbb{Q}[x]$ is prime whenever d is a non-square integer. Unfortunately, the same method is completely useless when it comes to polynomials of degree 4 and above. For example, consider the polynomial

$$f(x) = x^4 + x^3 + 2x^2 + x + 1 \in \mathbb{Z}[x].$$

If $f(a/b) = 0$ for some fraction $a/b \in \mathbb{Q}$ in lowest terms, then the Rational Root Test tells us that $a|1$ and $b|1$, hence $a/b = \pm 1$. But we can directly check that $f(1) = 6 \neq 0$ and $f(-1) = 2 \neq 0$, hence this polynomial has **no rational roots**. But this does not imply that $f(x)$ is a prime element of $\mathbb{Q}[x]$. Indeed, we have the following non-trivial factorization:

$$f(x) = (x^2 + 1)(x^2 + x + 1).$$

But it might have been difficult for you to find this factorization unless I gave it to you. This is also a difficulty with integers. If I give you a large integer $n \in \mathbb{Z}$ we believe that there is no fast algorithm to factor n as a product of primes.[52] In short:

Primality Testing is Hard

Nevertheless, it is rather easy to show that Leibniz' polynomial x^4+a^4 is not prime. The reason that Leibniz did not see this is because his understanding of complex numbers was limited. In particular, he did not understand that a nonzero complex number has four distinct 4th roots. The following theorem generalizes our theorem on the roots of unity.

Theorem (Roots of a General Complex Number)

Consider a positive integer $n \geqslant 1$ and a nonzero complex number $0 \neq \alpha \in \mathbb{C}$. Recall that we can express $\alpha = re^{i\theta}$ in polar form for some real numbers $r, \theta \in \mathbb{R}$ with $r > 0$. Since the polynomial $x^n - r \in \mathbb{R}[x]$ takes a negative value when $x = 0$ and positive values when $x > r$ we conclude from the Intermediate Value Theorem that there exists some real number $0 < r' \leqslant r$ satisfying $(r')^n = r$. Thus we observe that the complex number $\alpha' := r'e^{i\theta/n} \in \mathbb{C}$ is an nth root of α:

$$(\alpha')^n = (r'e^{i\theta/n})^n = (r')^n e^{i\theta} = re^{i\theta} = \alpha.$$

Furthermore, if we let $\omega = e^{2\pi i/n}$ then I claim that α has the following n distinct complex

[52] In fact, this difficulty is the foundation of the RSA Cryptosystem, which allows us to safely transmit our credit card information to Amazon.

nth roots:

$$\alpha', \quad \alpha'\omega, \quad \alpha'\omega^2, \quad \cdots \quad \alpha'\omega^{n-1}.$$

Geometrically, these roots are the vertices of a regular n-gon in the complex plane, which is centered at the origin, but need not have any vertices on the real axis.

Proof. Since $\omega^n = 1$, we observe that any number of the form $\alpha'\omega^k$ is an nth root of α:

$$(\alpha'\omega^k)^n = (\alpha')^n(\omega^n)^k = \alpha(1)^k = \alpha.$$

To show that the complex numbers $\alpha'\omega^r$ for $r = 0, 1, \ldots, n-1$ are distinct, recall from the theorem on roots of unity that for any integers $k, \ell \in \mathbb{Z}$ we have

$$\omega^k = \omega^\ell \text{ in the field } \mathbb{C} \quad \Leftrightarrow \quad n|(k-\ell) \text{ in the ring } \mathbb{Z}.$$

Now suppose for contradiction that we have $\alpha'\omega^{r_1} = \alpha'\omega^{r_2}$ for some $0 \leqslant r_1 < r_2 < n$. Then dividing both sides by α' gives $\omega^{r_1} = \omega^{r_2}$ which implies that $n|(r_2 - r_1)$ and hence $n \geqslant r_2 - r_1 < n$. Contradiction. Finally, we observe that α can have at most n distinct nth roots in the field $\mathbb{C}$ because the polynomial $x^n - \alpha \in \mathbb{C}[x]$ has degree n. □

The first person to clearly understand this theorem was probably Euler. Had Leibniz known the theorem then he certainly would have had no trouble factoring the polynomial $x^4 + a^4$. Indeed, note that a is a real 4th root of a^4. By writing $-a^4 = a^4(-1) = a^4 e^{i\pi}$ in polar form, we find that $ae^{i\pi/4}$ is one particular 4th root of a^4, and the other roots are $ae^{i3\pi/4}$, $ae^{i5\pi/4}$, $ae^{i7\pi/4}$. Actually, it is more convenient to define $\omega = e^{2\pi/8}$, so we can express the four roots as follows:

$$\begin{aligned} ae^{i\pi/4} &= a\omega \\ ae^{i3\pi/4} &= a\omega^3 \\ ae^{i5\pi/4} &= a\omega^5 = a\omega^{-3} \\ ae^{i7\pi/4} &= a\omega^7 = a\omega^{-1}. \end{aligned}$$

Here is a picture. (Omitted.) Then by grouping the roots into conjugate pairs we have

$$\begin{aligned} x^4 + a^4 &= (x - a\omega)(x - a\omega^{-1})(x - a\omega^3)(x - a\omega^{-3}) \\ &= (x^2 - a(\omega + \omega^{-1}x + a^2\omega\omega^{-1})(x^2 - a(\omega^3 + \omega^{-3}x + a^2\omega^3\omega^{-3}) \\ &= \left(x^2 - 2a\cos(2\pi/8) + a^2\right)\left(x^2 - 2a\cos(6\pi/8) + a^2\right). \end{aligned}$$

This is already enough to show that Leibniz was wrong, because each of these quadratic factors has real coefficients. But we can do even better if we recall that

$$2\cos(2\pi/8) = \sqrt{2} \quad \text{and} \quad 2\cos(6\pi/8) = \sqrt{2},$$

so that

$$x^4 + a^4 = \left(x^2 - a\sqrt{2}\,x + a^2\right)\left(x^2 + a\sqrt{2}\,x + a^2\right).$$

Finally, by applying the method of partial fractions, one can show that[53]

$$\begin{aligned}
&\int \frac{1}{x^4 + a^4}\,dx \\
&= \int \frac{1}{\left(x^2 - a\sqrt{2}\,x + a^2\right)\left(x^2 + a\sqrt{2}\,x + a^2\right)}\,dx \\
&= \text{ some work} \\
&= \frac{\sqrt{2}}{4a^3}\left[\arctan\left(\frac{\sqrt{2}}{a}\,x + 1\right) + \arctan\left(\frac{\sqrt{2}}{a}\,x - 1\right) + \frac{1}{2}\ln\left|\frac{x^2 + a\sqrt{2}\,x + a^2}{x^2 - a\sqrt{2}\,x + a^2}\right|\right].
\end{aligned}$$

7.4 Equivalent Statements of the FTA

Before moving on, we should clarify the statement of the FTA.

Theorem (Equivalent Statements of the FTA)

The following 6 statements are logically equivalent:

(i) Every prime element of $\mathbb{C}[x]$ has degree 1.

(ii) Every polynomial in $\mathbb{C}[x]$ splits.

(iii) Every (nonconstant) polynomial in $\mathbb{C}[x]$ has a root in $\mathbb{C}$.

(iv) Every (nonconstant) polynomial in $\mathbb{R}[x]$ has a root in $\mathbb{C}$.

(v) Every prime element of $\mathbb{R}[x]$ has degree 1 or 2.

(vi) Every (nonconstant) polynomial in $\mathbb{R}[x]$ can be expressed as a product of polynomials of degrees 1 and 2.

Proof. We will prove that (i)⇒(ii)⇒(iii)⇒(iv)⇒(v)⇒(vi)⇒(i).

(i)⇒(ii): Consider the prime factorization.

(ii)⇒(iii): If $f(x) = (x - \alpha_1)\cdots(x - \alpha_n)$ then α_1 is a root.

(iii)⇒(iv): This is automatically true because $\mathbb{R}[x] \subseteq \mathbb{C}[x]$.

(iv)⇒(v): Let $p(x) \in \mathbb{R}[x]$ be a prime polynomial and assume for contradiction that $\deg(p) \geqslant 3$. From (iv) we know that $p(\alpha) = 0$ for some $\alpha \in \mathbb{C}$. If $\alpha \in \mathbb{R}$ then from Descartes' Theorem we

[53] Actually, I let my computer do it. There is no need for humans to perform these kinds of computations.

have $p(x) = (x - \alpha)f(x)$ for some $f(x) \in \mathbb{R}[x]$ of positive degree, which contradicts the fact that $p(x) \in \mathbb{R}[x]$ is prime. So let us assume that $\alpha \notin \mathbb{C}$. Then from the above lemma we also know that $p(\alpha^*) = 0$, and from Descartes' Theorem we conclude that

$$p(x) = (x - \alpha)(x - \alpha^*)g(x) \quad \text{for some nonconstant } g(x) \in \mathbb{C}[x].$$

But note that $(x - \alpha)(x - \alpha^*) = (x^2 - (\alpha + \alpha^*)x + \alpha\alpha^*)$ actually has real coefficients. From the uniqueness of quotients and remainders in the ring $\mathbb{C}[x]$,[54] this implies that $g(x)$ also has real coefficients, again contradicting the fact that $f(x) \in \mathbb{R}[x]$ is prime.

(v)⇒(vi): Let $p(x) \in \mathbb{C}[x]$ be prime and assume for contradiction that $\deg(p) \geqslant 3$. From the above lemma we know that $f(x) := p(x)p^*(x)$ has real coefficients. From (v) we know that $f(x)$ is a product of real polynomials of degrees 1 and 2. Then by factoring the polynomials of degree 2 (using the quadratic formula) we conclude that $f(x)$ splits over $\mathbb{C}$. In other words, we have polynomials $q_1(x), \ldots, q_k(x) \in \mathbb{C}[x]$ of degree 1 such that

$$f(x) = p(x)p^*(x) = q_1(x)q_2(x)\cdots q_k(x).$$

Then since $p(x) \in \mathbb{C}[x]$ is prime and since $p(x)$ divides the product $q_1(x)\cdots q_k(x)$, we know from Euclid's Lemma in the ring $\mathbb{C}[x]$ that $p(x)|q_j(x)$ for some j, which implies that

$$2 \leqslant \deg(p) \leqslant \deg(q_j) = 1.$$

Contradiction. □

Lemma (Complex Roots Come in Conjugate Pairs)

Lemma (Conjugation of Polynomials)

Bad News: We still have not proved that any of these 6 statements is true.

Good News: In order to the prove the FTA, it is enough to prove any one of these 6 statements.

7.5 Euler's Attempt

Euler was the first to confidently state that the FTA must be true. He came to this belief through his correspondence with Nicholas Bernoulli in the 1740s. Bernoulli wrote a letter to Euler claiming that the following degree 4 polynomial cannot be factored over $\mathbb{R}$:

[54] You will spell out the details on the homework.

In proving that Bernoulli was wrong, Euler realized that he has a method to prove that **any** polynomial of $\mathbb{R}[x]$ of degree 4 factors as a product of two quadratics. Furthermore, he felt that he could extend the proof to polynomials of any degree, but the details got away from him and the proof was ultimately not convincing.

First I'll show you Euler's proof for degree 4 polynomials and then we'll discuss why it might not be convincing.

7.6 Symmetric Functions

There was a missing step in Euler's proof.

Fundamental Theorem of Symmetric Functions. Discriminant of a cubic.

7.7 Laplace's Proof

See *Numbers* (pg. 121) by Ebbinghaus et al.

Laplace's proof of the fundamental theorem. Gauss' objection.

7.8 Epilogue: Algebraic Geometry

Algebra is smarter than geometry. Curves of degree m and n intersect in $\leqslant mn$ points in any picture. But the algebra tells us that they always intersect in exactly mn points.

Geometric notion of degree defined by Newton (curve intersect with line). General intersection theorem stated by Maclaurin. First proof by Bézout, still flawed. It is tricky to precisely define the multiplicity of intersection.

The modern version is fancy.

8 Groups

8.1 The Concept of a Group

Let $\Omega_n \subseteq \mathbb{C}$ be the set of nth roots of unity. This set has the important property that it is "closed under multiplication."

The Concept of a Group

blah

Remark: The definition of groups allows us to shorten the definitions of rings and vector spaces.

Some other examples of groups. $U(1)$ is infinite, containing Ω_n as a "subgroup."

The Concept of a Subgroup

sd

In fact, we observe that Ω_a is a subgroup of Ω_b if and only if $a|b$.

Other examples: $(R, +, 0)$, $(R^\times, \times, 1)$, square invertible matrices show that groups are not necessarily commutative.

8.2 Congruence Modulo a Subgroup

Subgroups of $(\mathbb{Z}, +, 0)$. The set of congruence classes. The quotient group.

8.3 Isomorphism of Groups

Examples $\Omega_n \cong \mathbb{Z}/n\mathbb{Z}$, $U(1) \cong SO(2)$.

8.4 Order of an Element

8.5 The Fermat-Euler-Lagrange-Cauchy Theorem

Order of an element. Order of a power.

9 Other Rings and Fields

9.1 Modular Arithmetic

9.2 Quotient Rings in General

9.3 Cauchy's Construction of Complex Numbers

9.4 Kronecker's Construction of Splitting Fields

9.5 Galois' Finite Fields

10 Impossible Constructions

10.1 Angle Trisection and the Delian Problem

10.2 Descartes changed the rules

10.3 Quadratic Field Extensions

Proof of impossibility for angle trisection and cube doubling.

10.4 The Gauss-Wantzel Theorem

The 5-gon and 17-gon are constructible. Why? Cyclotomic polynomials. The Galois group of $\mathbb{Q}[\cos(2\pi/n)]$ is abelian of size $\phi(n)$.

Lemma: Let p be prime, $\omega = e^{2\pi i/p}$, and fix a primitive element $r \in (\mathbb{Z}/p\mathbb{Z})^\times$. Then there exists a field automorphism $\varphi : \mathbb{Q}[\omega] \to \mathbb{Q}[\omega]$ defined by $\omega \mapsto \omega^r$. Furthermore, the automorphism commutes with complex conjugation.

Proof: Note that ω and ω^r have the same minimal polynomial $\Phi_p(x)$ over $\mathbb{Q}$, and note that $\mathbb{Q}[\omega^r] = \mathbb{Q}[\omega]$. Compose the isomorphisms $\mathbb{Q}[\omega] \cong \mathbb{Q}[x]/\langle\Phi_p(x)\rangle$ and $\mathbb{Q}[\omega^r] \cong \mathbb{Q}[x]/\langle\Phi_p(x)\rangle$. This map commutes with complex conjugation because $(\omega^r)^* = \omega^{-r} = (\omega^{-1})^r = (\omega^*)^r$. $\square$

Theorem: Let $\varphi : \mathbb{Q}[\omega] \to \mathbb{Q}[\omega]$ be the automorphism from the lemma. Then for every divisor $d|(p-1)$ we consider the fixed field $K_d = \mathrm{Fix}(\varphi^d)$. Since $\varphi^{p-1} = \mathrm{id}$ we observe that $K_{p-1} = \mathbb{Q}[\omega]$ and for all $d|e|(p-1)$ we observe that $K_d \subseteq K_e$. I claim that every element of K_e satisfies an equation of degree e/d with coefficients in K_d. Moreover, if the element is real then the coefficients of the polynomial are real. Finally, I claim that $K_1 = \mathbb{Q}$.

Proof: For any $a \in K_e$, we consider the polynomial $(x-a)(x-\varphi^d(a))\cdots(x-\varphi^{d(d'-1)}(a))$ of degree d'. Note that $\varphi^d(\varphi^{d(d'-1)}(a)) = \varphi^e(a) = a$ because $a \in K_e$. Thus φ^d permutes the

roots of this polynomial, hence it fixes the coefficients. Moreover, if $a \in \mathbb{R}$ then $a^* = a$ implies $(\varphi^{dk}(a))^* = \varphi^{dk}(a^*) = \varphi^{dk}(a)$. This means that the roots, hence the coefficients are real.

For the final statement, recall that every element of $\mathbb{Q}[\omega]$ has the form $r(\omega)$ for some (unique) polynomial $r(x) \in \mathbb{Q}[x]$ of degree $< n$. If $\varphi(r(\omega)) = r(\omega)$ then we also have $\varphi^k(r(\omega)) = r(\omega)$, and hence $r(\varphi^k(\omega)) = r(\omega)$ for all $k \in \mathbb{Z}$. But then the polynomial $r(x) - r(\omega) \in \mathbb{Q}[\omega][x]$ of degree $< n$ has n distinct roots, hence $r(x) - r(\omega) = 0(x)$. This implies that $r(x) = r(\omega)$ is constant, which implies $r(\omega) \in \mathbb{Q}$ because $r(x) \in \mathbb{Q}[x]$. □

Corollary (Gauss): If p is prime and $p-1$ is a power of 2 then the regular p-gon is constructible with straightedge and compass. In particular, the regular 17-gon is constructible.

Remark: This actually leads to an algorithm. First take $a = 2\cos(2\pi/17) = \omega^1 + \omega^{-1}$ and choose the primitive root $3 \in (\mathbb{Z}/17\mathbb{Z})^\times$, so that $\varphi(\omega) = \omega^3$. Since $\varphi^8(\omega) = \omega^{3^8} = \omega^{16} = \omega^{-1}$, we observe that a is already in K_8. Then since $\varphi^4(\omega) = \omega^{3^4} = \omega^{13} = \omega^{-4}$ we observe that a is a root of the polynomial

$$(x-a)(x-\varphi^4(a)) = (x-(\omega^1+\omega^{-1}))(x-(\omega^4+\omega^{-4})) = x^2 + \alpha x + \beta,$$

with $\alpha = -\omega^1 - \omega^{-1} - \omega^4 - \omega^{-4} \in K_4$ and $\beta = (\omega^1+\omega^{-1})(\omega^4+\omega^{-4}) \in K_4$. Next, since $\varphi^2(\omega) = \omega^{3^2} = \omega^9 = \omega^{-8}$, we observe that α is a root of

$$\begin{aligned}(x-\alpha)(x-\varphi^2(\alpha)) &= (x+\omega^1+\omega^{-1}+\omega^4+\omega^{-4})(x+\omega^8+\omega^{-8}+\omega^2+\omega^{-2}) \\ &= x^2 + Ax + B,\end{aligned}$$

with $A, B \in K_2$, and β is a root of

$$\begin{aligned}(x-\beta)(x-\varphi^2(\beta)) &= (x-(\omega+\omega^{-1})(\omega^4+\omega^{-4}))(x-(\omega^8+\omega^{-8})(\omega^2+\omega^{-2})) \\ &= x^2 + Cx + D,\end{aligned}$$

with $C, D \in K_2$. Finally, we observe that each of $A, B, C, D \in K_2$ satisfies a quadratic equation over $K_1 = \mathbb{Q}$. It is possible to find these equations by hand (as Gauss did), but I used my computer to save time:

$$\begin{aligned}(x-A)(x-\varphi(A)) &= x^2 + x - 4, \\ (x-B)(x-\varphi(B)) &= x^2 + 2x + 1, \\ (x-C)(x-\varphi(C)) &= x^2 - x - 4, \\ (x-D)(x-\varphi(D)) &= x^2 + 2x + 1.\end{aligned}$$

From this we observe that $A = (-1+\sqrt{17})/2$, $C = (1+\sqrt{17})/2$ and $B = D = 1$. Finally, we can rewind all of the steps to obtain a closed formula for a.

Wantzel: The other direction.

11 Unsolvability of the Quintic

Permutations, something about groups. Will we get this far?