MTH 461 **Spring 2023**
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 But today the textbook (and the term "modern algebra" itself) is slightly out of date.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.

(3) History and motivation.

[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".

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 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.

To the experts: By adopting this teaching style, I put arithmetic (integers, polynomials and Euclidean domains) near the beginning of the course. Group theory, being more modern, gets pushed to the end. Unfortunately, this does not leave time for an abstract treatment of groups. Finite abelian groups appear as part of modular arithmetic. Permutations are mentioned but we do not study the symmetric group. Groups of geometric transformations do not appear.

Students who want (or need) to see a more thorough treatment should instead take the two-semester sequence 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 too much with 561/562. If you want to see my own approach to the courses 561/562, take a look at my typed course notes from Fall 2018 and Spring 2019.

Contents

1 Solving Equations **4**

2 Quadratic Equations **7**

2.1 Al-Khwarizmi . . . 7
2.2 The Quadratic Formula . . . 12
2.3 Does There Exist a Cubic Formula? . . . 17

3 Rings, Fields, Polynomials **17**

3.1 A Motivating Example . . . 17
3.2 Rings and Fields . . . 19
3.3 Polynomials . . . 22
3.4 Descartes' Factor Theorem . . . 27

4 Unique Prime Factorization **32**
4.1 Integral Domains . . . 32
4.2 The Group of Units . . . 33
4.3 The Language of Divisibility . . . 35
4.4 The Language of Principal Ideals . . . 36
4.5 Euclidean Domains . . . 38
4.6 The Euclidean Algorithm . . . 42
4.7 Unique Prime Factorization . . . 48
4.8 Epilogue: Gauss' Lemma . . . 54

5 Cubic Equations **55**
5.1 Intermediate Value Theorem . . . 55
5.2 Newton's Method . . . 58
5.3 Cardano's Formula . . . 60
5.4 Bombelli and "Imaginary Numbers" . . . 64
5.5 Cardano's Formula (Modern Version) . . . 66

6 Complex Numbers **69**
6.1 Formal Symbols . . . 69
6.2 Trigonometry and Cubic Equations . . . 73
6.3 Euler's Formula . . . 80
6.4 Polar Form and Roots of Unity . . . 84

7 Fundamental Theorem of Algebra **95**
7.1 Introduction . . . 95
7.2 Partial Fractions . . . 97
7.3 Leibniz' Mistake . . . 105
7.4 Equivalent Statements of the FTA . . . 109
7.5 Euler's Attempt . . . 114
7.6 Symmetric Functions . . . 116
7.7 Laplace's Proof . . . 116
7.8 Epilogue: Algebraic Geometry . . . 116

8 Other Rings and Fields **117**
8.1 Modular Arithmetic . . . 117
8.2 Quotient Rings in General . . . 117
8.3 Cauchy's Construction of Complex Numbers . . . 117
8.4 Kronecker's Construction of Splitting Fields . . . 117
8.5 Galois' Finite Fields . . . 117

9 Groups **117**
9.1 The Concept of a Group . . . 117
9.2 Congruence Modulo a Subgroup . . . 118
9.3 Isomorphism of Groups . . . 118
9.4 Order of an Element . . . 118

9.5 The Fermat-Euler-Lagrange-Cauchy Theorem 118
9.6 Existence of Primitive Roots 118

10 Impossible Constructions 118
10.1 Angle Trisection and the Delian Problem 118
10.2 Descartes changed the rules 118
10.3 Quadratic Field Extensions 118
10.4 Permuting the Roots 118
10.5 The Gauss-Wantzel Theorem 119

11 Unsolvability of the Quintic 120

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:

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

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:

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

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

$$a_1 x_1 + a_2 x_2 + \cdots + a_n x_n = b,$$

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

$$ax^5 + bx^4 + cx^3 + dx^2 + ex + f = 0$$

[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".

in terms of the coefficients and the algebraic operations $+, -, \times, \div, \sqrt{\ }, \sqrt[3]{\ }, \sqrt[4]{\ }, \ldots$

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. $x^2 + b = ax$

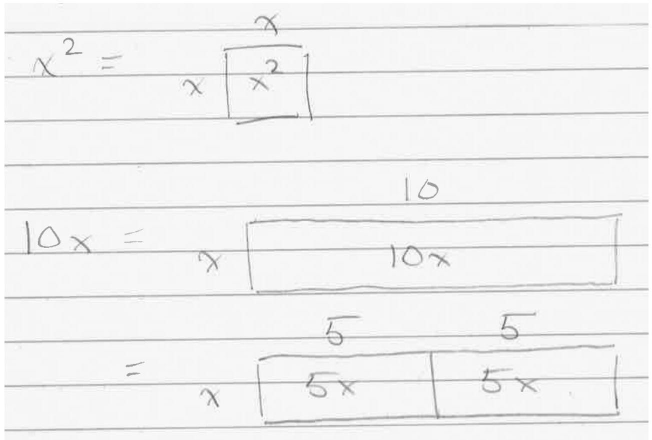
The solution to each case was illustrated with a specific example, though it was understood that the same reasoning could be applied in general. Here are his three examples.

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

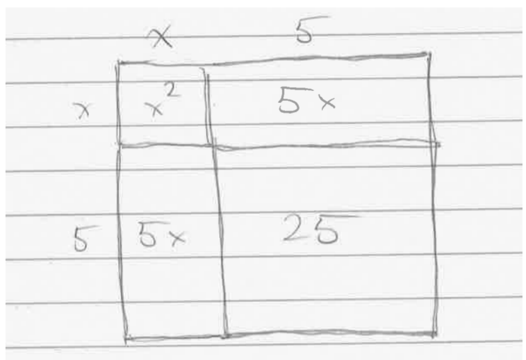
$$\boxed{x^2 + 10x = 39}$$

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

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

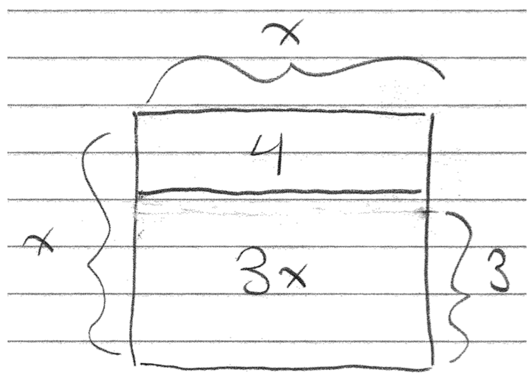
The final step is an example of *al-muqabala* [balancing] since we subtracted 5 from both sides. We will see the other fundamental operation *al-jabr* [completion] in the next example. It is clear from the geometry that an equation of Type I always has exactly one (positive, real) solution. In modern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

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

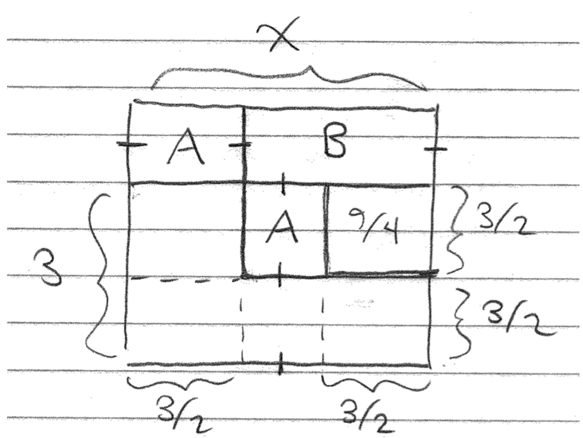
Type II. *Three roots and four of Simple Numbers are equal to a Square*:

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

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

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

$$\begin{aligned} x - 3/2 &= 5/2 \\ x &= 5/2 + 3/2 && \text{al-jabr} \\ x &= 4. \end{aligned}$$

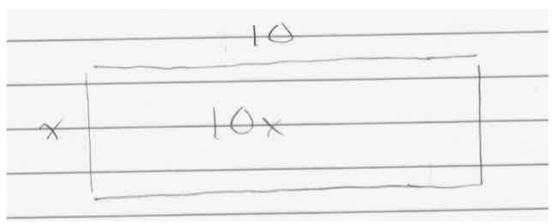
We note that this equation again has exactly one (positive, real) solution. In modern notation we can summarize the algorithm as follows:

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

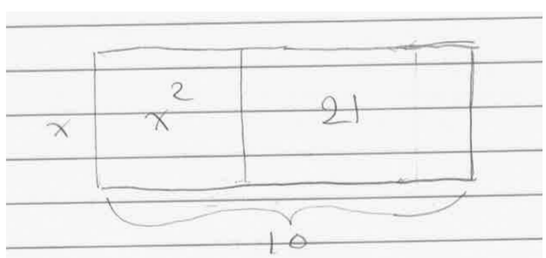
Type III. *A square and twenty-one Dirhems are equal to ten Roots*:

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

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

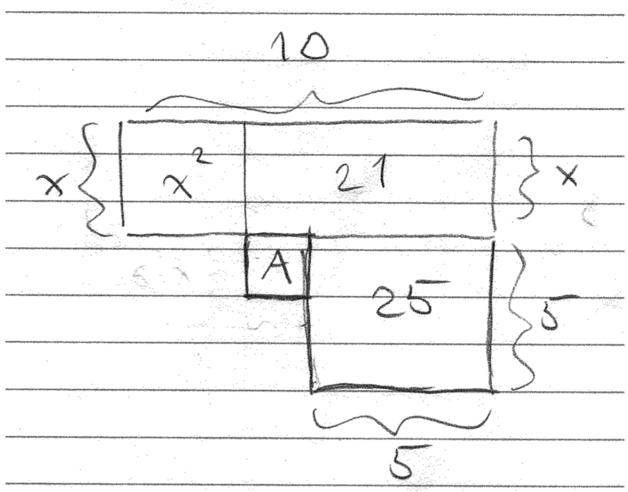


Then we cut a square of length x from one side to obtain the following diagram:



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

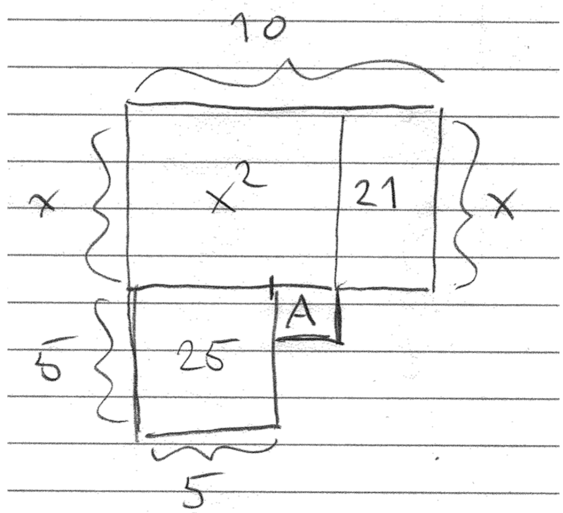
[5] Actually, he's not very clear about this, so I cleaned it up.



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 $\sqrt{}$ 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

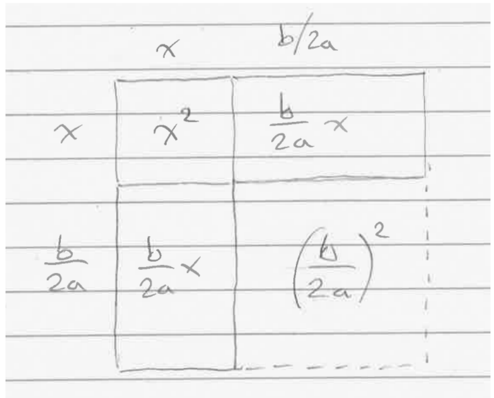
$$ax^2 + bx + c = 0.$$

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":

[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 vse, a paire of paralleles, or Gemowe lines of one lengthe, thus: =, bicause noe .2. thynges, can be moare equalle.*



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

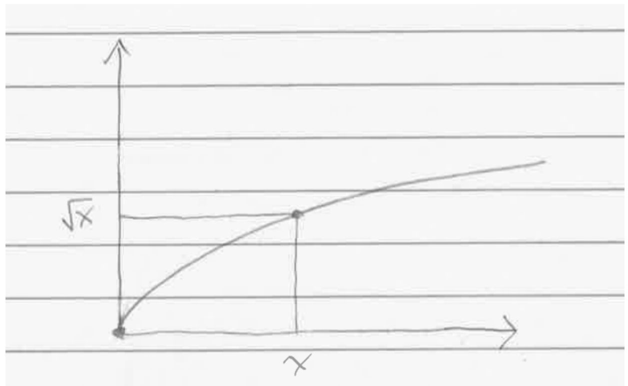
$$\left(\frac{\delta}{2a}\right)^2 = \frac{\delta^2}{4a^2} = \frac{b^2 - 4ac}{4a^2},$$

which allows us to solve for x as follows:

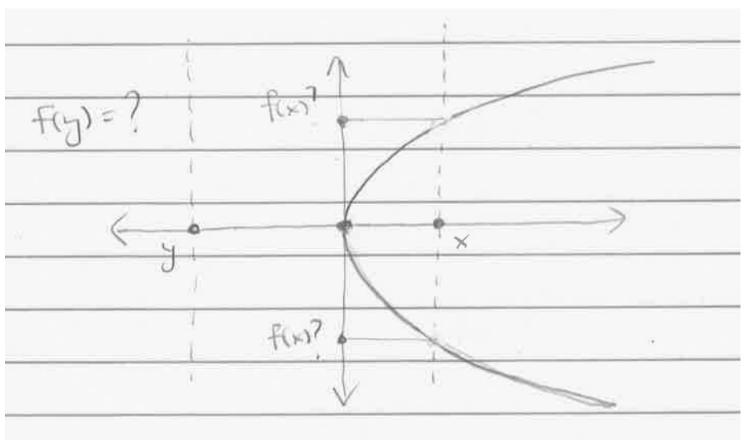
$$\begin{aligned} \left(x + \frac{b}{2a}\right)^2 &= \frac{b^2 - 4ac}{4a^2} \\ x + \frac{b}{2a} &= \frac{\delta}{2a} \\ x &= \frac{-b + \delta}{2a}. \end{aligned}$$

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:

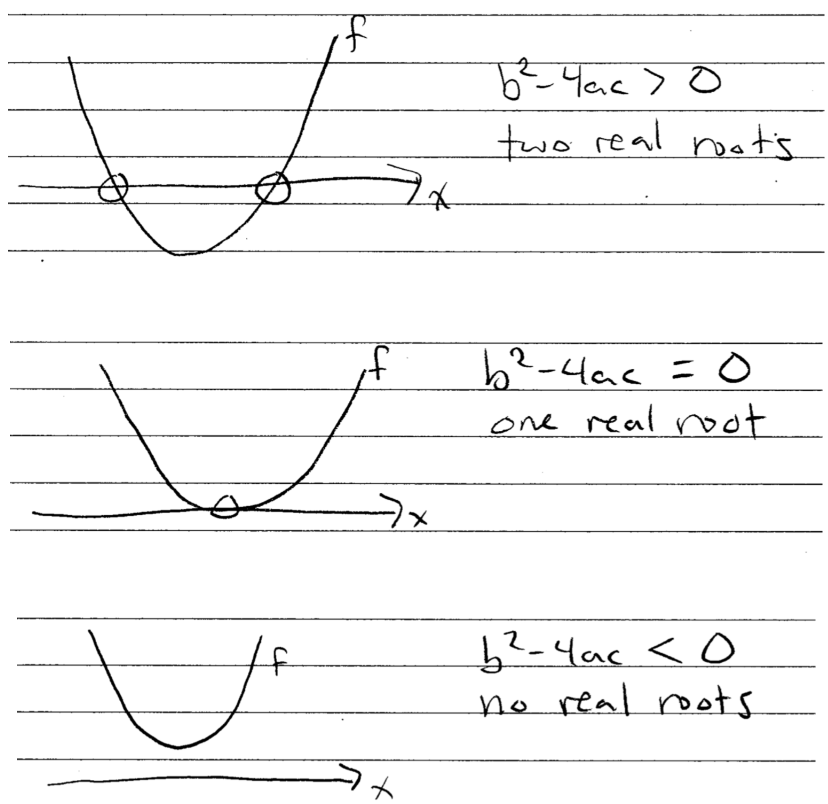
$$\Delta := b^2 - 4ac.$$

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]



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.

[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.

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.

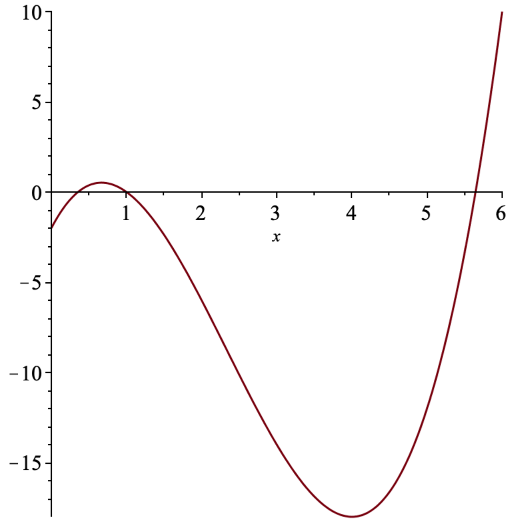
It turns out that such a formula does exist, but it is quite complicated. The formula was discovered in Italy during the 1500s and became known as "Cardano's formula". The reason it was not discovered earlier is because a geometric solution in the style of al-Khwarizmi would be far too complicated. The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

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

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)

(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)

[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.

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?

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

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

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

$\square$

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 $b \neq 0$ 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

$$a \geqslant 1$$

[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.

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

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

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

where the *coefficients* $a_0, a_1, a_2, \ldots$ are elements of R and **only finitely many of the coefficients are nonzero**. At first this is just a formal expression. Below we will define addition and multiplication of polynomials by pretending that the symbol x is a number. Then it will make sense say things like $x + x = 2x$ and $x \cdot x = x^2$.[11]

Let us denote the set of all polynomials by

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

To define a ring structure on $R[x]$ we first define the zero and one polynomials:

$$\begin{aligned} 0 &:= 0 + 0x + 0x^2 + 0x^3 + \cdots, \\ 1 &:= 1 + 0x + 0x^2 + 0x^3 + \cdots. \end{aligned}$$

Hopefully it will cause no confusion that we use the same symbols $0, 1$ to denote elements of R and $R[x]$. More generally, for any element $a \in R$ we define the *constant polynomial*:

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

This notation allows us to think of $R \subseteq R[x]$ as a subset.[12]

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 should check that the structure $(R[x], +, \cdot, 0, 1)$ satisfies the ring axioms, but we won't bother to do this. The trickiest part is to show that multiplication of polynomials is associative.

Polynomials over a general ring can be quite complicated, but it turns out 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:[13] 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

[11] The symbols x^2, x^3, ... were invented by Descartes.

[12] In fact, it is a *subring*.

[13] Technical Remark: In fact, our proof will show that the same result holds for the polynomial ring $R[x]$ where R is any ring satisfying: (1) for all $a, b \in R$ with $a \neq 0$ and $b \neq 0$ we have $ab \neq 0$; and (2) the leading coefficient of the divisor $g(x) \in R[x]$ has a multiplicative inverse in R. Note that (1) and (2) automatically hold when $R = \mathbb{F}$ is a field and $g(x)$ is nonzero.

by the "degree", which is defined as follows. Before giving the proof of the Division Theorem we need a rigorous definition of the degree.

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:

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

For any polynomials $f(x), g(x) \in R[x]$ and constants $\alpha, \beta \in R$ we observe that

$$\deg(\alpha \cdot f(x) + \beta \cdot g(x)) \leqslant \max\{\deg(f), \deg(g)\}.$$

Indeed, suppose that $\deg(f) = m$ and $\deg(g) = n$. To be specific, let $f(x) = \sum_k a_k x^k$ and $g(x) = \sum_k b_k x^k$ with $a_k = 0$ for all $k > m$ and $b_k = 0$ for all $k > n$. Then the coefficient of x^k in $\alpha f(x) + \beta g(x)$ is $\alpha a_k + \beta b_k$, which equals zero for all $k > \max\{m, n\}$.

More importantly, if R is a field[14] then the degree of a product is the sum of the degrees:

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

Proof. Homework.

Each nonzero constant polynomial a has degree 0. For example, $\deg(105) = 0$. But what about the zero polynomial? I claim that there is no reasonable way to define $\deg(0)$. Indeed, if we could define $\deg(0)$ then we would like the following formula to be true:

$$\begin{aligned} 0 &= 0 \cdot f(x) \\ \deg(0) &= \deg(0 \cdot f(x)) \\ \deg(0) &= \deg(0) + \deg(f). \end{aligned}$$

But this implies that $\deg(f) = 0$ for every polynomial $f(x)$, which is nonsense. Some authors just say that $\deg(0)$ is "undefined". Alternatively, we could give a fake definition:

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

[14] It suffices to let R be a domain, i.e., a commutative ring in which $ab = 0$ implies that $a = 0$ or $b = 0$. See the next section for more details.

This fake definition 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.

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".[15] 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.[16] 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. $\square$

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 $\deg(0) = -\infty$).[17] 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:[18]

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

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:

$$h(x) = r(x) - \frac{b_n}{a_m}x^{n-m}g(x)$$

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

[16] The *Well-Ordering Principle* says that any non-empty set of non-negative integers has a smallest element. This principle cannot be proved and must be taken as an axiom of the integers.

[17] Again, such a polynomial $r(x)$ exists because of the Well-Ordering Principle.

[18] Here we are using the fact that $\mathbb{F}$ is a field in order to divide by a_m.

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

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

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:

$$
\begin{array}{r|l}
 & \quad\quad\quad\quad\quad\quad x^3 - 3x^2 + 2x + \tfrac{1}{2} \\ \hline
2x^2+1 & 2x^5 - 6x^4 + 5x^3 - 2x^2 + 3x + 1 \\
 & -2x^5 \qquad\quad - x^3 \\ \cline{2-2}
 & \quad -6x^4 + 4x^3 - 2x^2 \\
 & \quad\;\; 6x^4 \qquad\; + 3x^2 \\ \cline{2-2}
 & \qquad\qquad 4x^3 + x^2 + 3x \\
 & \qquad\quad\; -4x^3 \qquad - 2x \\ \cline{2-2}
 & \qquad\qquad\qquad x^2 + x + 1 \\
 & \qquad\qquad\quad\; -x^2 \qquad - \tfrac{1}{2} \\ \cline{2-2}
 & \qquad\qquad\qquad\qquad x + \tfrac{1}{2}
\end{array}
$$

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:

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

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.

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.[19] 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

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

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:

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

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

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 $\mathbb{F}$. $\square$

For example, let's consider again the polynomial $f(x) = x^3 - 7x^2 + 8x - 2 \in \mathbb{Q}[x]$.[20] 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 $\mathbb{Q}$[21] 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

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

[21] 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.[22] 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:

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

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

[22] 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

In the previous section we showed that each of the rings $\mathbb{Z}$ and $\mathbb{F}[x]$ (where $\mathbb{F}$ is a field) has a division algorithm. This fact is responsible for a deep analogy between these rings, which we develop in this section. The main consequence is that each of $\mathbb{Z}$ and $\mathbb{F}[x]$ has a notion of "unique prime factorization".

4.1 Integral Domains

The rings $\mathbb{Z}$ and $\mathbb{F}[x]$ are not fields. In particular, the elements $2 \in \mathbb{Z}$ and $x \in \mathbb{F}[x]$ do not have multiplicative inverses. Instead, these rings satisfy a weaker property.

Definition of Integral Domains

Let $(R, +, \cdot, 0, 1)$ be a ring. We say that R is an *integral domain* (or just a *domain*) if for all elements $a, b \in R$ we have

$$ab = 0 \quad \Longrightarrow \quad a = 0 \text{ or } b = 0.$$

In particular, every field $\mathbb{F}$ is a domain. Indeed, suppose we have $ab = 0$ in a field $\mathbb{F}$. If $b = 0$ then we are done. Otherwise, the multiplicative inverse b^{-1} exists and we have

$$\begin{aligned} ab &= 0 \\ abb^{-1} &= 0b^{-1} \\ a &= 0. \end{aligned}$$

But not every domain is a field. In particular, $\mathbb{Z}$ and $\mathbb{F}[x]$ domains but not fields. We can't prove that $\mathbb{Z}$ is a domain because we haven't officially defined $\mathbb{Z}$, so I'll just take this as an axiom.[23] You will prove on the homework that $\mathbb{F}[x]$ is a domain for any field $\mathbb{F}$. To be more specific, you will prove the following formula for the degree of a product:

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

Then the result follows since $\deg(f) \geqslant 0$ if and only if $f(x) \neq 0$. (Recall that $\deg(0) = -\infty$.)

To demonstrate that the definition of integral domains is not vacuous, let me show you an example of a ring that is not a domain. This example comes from the theory of "modular arithmetic", which we will discuss later.

Example of a Non-Domain. The following addition and multiplication tables define a ring structure on the set of symbols $R = \{0, 1, 2, 3\}$:

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

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

This ring is not a domain because $2 \cdot 2 = 0$, but 2 is not equal to 0.

4.2 The Group of Units

When it comes to factorization in a ring, there are certain elements of the ring that don't matter. For example, the integer $6 \in \mathbb{Z}$ can be factored in two ways:

$$6 = 2 \cdot 3 = (-2)(-3),$$

And the polynomial $x^3 - 1 \in \mathbb{R}[x]$ can be factored in infinitely many ways:

$$x^3 - 1 = \left(\frac{1}{\alpha}x - \frac{1}{\alpha}\right)(\alpha x^2 + \alpha x + \alpha) \quad \text{for any nonzero constant } \alpha \in \mathbb{R}.$$

But we regard these factorizations as "essentially the same". To be specific, the integers $\pm 1 \in \mathbb{Z}$ and the nonzero constants $\alpha \in \mathbb{R}[x]$ are called "units".

[23] The first axiomatic definitions of $\mathbb{Z}$ we given by Peano and Dedekind in the 1880s. The key to the definition is the *Well-Ordering Principle*, which says that any non-empty set of positive integers has a smallest element. This is logically equivalent to the principle of induction. It is also logically equivalent to the statement that $a \neq 0$ implies $|a| \geqslant 1$ for all $a \in \mathbb{Z}$. That is, there are no integers between 0 and 1.

The Group of Units of a Ring

Let R be a commutative ring. We say that $u \in R$ is a *unit* when there exists an element $v \in R$ satisfying $uv = 1$. We denote the set of units by[24]

$$R^\times = \{u \in R : \text{ there exists } v \in R \text{ such that } uv = 1\}.$$

In other words, a unit of R is an element that has a multiplicative inverse.

If a multiplicative inverse exists then it must be unique. Indeed, if $uv = 1$ and $uw = 1$ then we must have

$$v = 1v = (uw)v = (uv)w = 1w = 1.$$

The unique multiplicative inverse of u is called u^{-1}. But not every element of R is a unit. For example, $0 \in R$ is not a unit because $0v$ is never equal to 1. The set of units is often referred to as a "group" because of the following three properties, which you will check on the homework:

- 1 is a unit.
- If u is a unit then u^{-1} is a unit.
- If u and v are units then uv is a unit.

We will talk more about groups in a future chapter.

Example: The Units of a Field. Let $\mathbb{F}$ be a field. Then, by definition, every nonzero element is a unit:

$$\mathbb{F}^\times = \mathbb{F}\backslash\{0\}.$$

Example: The Units of $\mathbb{Z}$. I claim that

$$\mathbb{Z}^\times = \{1, -1\}.$$

Indeed, one can check that 1 and -1 are units. To show that there are no other units, suppose we have $u \in \mathbb{Z}^\times$ satisfying $|u| \geqslant 2$. By definition of $\mathbb{Z}^\times$ there exists some $v \in \mathbb{Z}$ satisfying $uv = 1$. Then applying absolute value gives

$$\begin{aligned} uv &= 1 \\ |uv| &= 1 \\ |u||v| &= 1, \end{aligned}$$

[24]The superscript "$\times$" is the multiplication symbol. The notation R^* is also common, but there is no really standard notation.

which implies that $0 < |v| \leqslant 1/2$. Contradiction.

Example: The Units of $\mathbb{F}[x]$. Let $\mathbb{F}$ be a field. Then I claim that the units of the ring $\mathbb{F}[x]$ are just the nonzero constant polynomials:

$$\mathbb{F}[x]^\times = \mathbb{F}^\times = \mathbb{F}\backslash\{0\}.$$

Indeed, one can check that every nonzero constant is a unit. To show that there are no other units, suppose that we have $u(x)v(x) = 1$ for some polynomials $u(x), v(x) \in \mathbb{F}[x]$. Since $u(x)$ and $v(x)$ are nonzero we can apply degrees to obtain

$$0 = \deg(1) = \deg(uv) = \deg(u) + \deg(v).$$

Since $\deg(u) \geqslant 0$ and $\deg(v) \geqslant 0$, this implies that $\deg(u) = \deg(v) = 0$, so that $u(x)$ and $v(x)$ are nonzero constants. More generally, you will show on the homework that

$$R[x]^\times = R^\times \quad \text{for any ring } R.$$

4.3 The Language of Divisibility

The definition of divisibility is fundamental to the theory of factorization.

Definition of Divisibility

Let R be a ring and consider elements $a, b \in R$. We define the notation

$$\text{“}a|b\text{”} \quad \Longleftrightarrow \quad \text{there exists some } k \in R \text{ such that } ak = b.$$

In this case we say that “a divides b” or that “b is divisible by a”.

We observe that $1|a$ for all a because $a1 = a$. And since $0k = a$ implies $a = 0$ we observe that $0 \nmid a$ for all nonzero a. That is,

$$1 \textit{ divides everything and } 0 \textit{ divides nothing.}^{25}$$

Furthermore, one can check that the relation of divisibility is reflexive and transitive:

- $a|a$ for all a,
- if $a|b$ and $b|c$ then $a|c$.

[25] Technically zero divides itself, but opinions may differ on this.

Is it also antisymmetric? That is, if $a|b$ and $b|a$ do we necessarily have $a = b$? Let's check. Suppose that $a|b$ and $b|a$ so that $ak = b$ and $b\ell = a$ for some elements $k, \ell \in R$. Then

$$\begin{aligned} a &= b\ell \\ a &= ak\ell \\ a(1 - k\ell) &= 0. \end{aligned}$$

If R is a domain and if $a \neq 0$ then this implies $1 - k\ell = 0$, or $k\ell = 1$, so that k and ℓ must be units. For example, in the ring of integers $\mathbb{Z}$ we have

$$a|b \text{ and } b|a \quad \Longrightarrow \quad a = \pm b.$$

In the ring of polynomials $\mathbb{F}[x]$ we have

$$f(x)|g(x) \text{ and } g(x)|f(x) \quad \Longrightarrow \quad f(x) = \alpha g(x) \text{ for some nonzero constant } \alpha \in \mathbb{F}^\times.$$

When two elements of a ring differ by[26] a unit then they are "essentially the same" from the point of view of divisibility. Here is a formal definition. The concept is completely standard, but notation is strangely variable. I will follow the notation from Wikipedia:

`https://en.wikipedia.org/wiki/Unit_(ring_theory)`

Definition of Associatedness

Let R be a commutative ring. For any elements $a, b \in R$ we define the notation

$$a \sim b \quad \Longleftrightarrow \quad \text{there exists a unit } u \in R^\times \text{ such that } au = b.$$

In this case we say that a and b are *associates* in R.

If R is a domain then the above argument shows that

$$a \sim b \quad \Longleftrightarrow \quad a|b \text{ and } b|a.$$

4.4 The Language of Principal Ideals

Now I am going to play a trick on you. After having defined "units" and "associatedness", we will now switch the notation. The theory of divisibility is today usually expressed in the language of "principal ideals". For years I have resisted introducing this language in MTH 461 because it feels too abstract in this context. However, after bumbling through the theory one too many times, I finally acknowledge that the abstract approach makes the proofs much easier. I hope you will trust me on this.

[26]Literally: Differ by multiplication by a unit. Here I am using differ in the English sense, not in the sense of subtraction.

Definition of Principal Ideals

Consider an element $a \in R$ in a commutative ring. The *principal ideal generated by a* is just the set of multiples of a:

$$aR = \{ar : r \in R\}.$$

That's it.

Cultural Remark: The name "principal ideal" suggests that there are "non-principal ideals". An *ideal* of a ring R is a subset $I \subseteq R$ that is closed under taking R-linear combinations:

$$a_1, \ldots, a_n \in I \text{ and } r_1, \ldots, r_n \in R \quad \Longrightarrow \quad a_1 r_1 + \cdots + a_n r_n \in I.$$

One can check that a principal idea aR is, in fact, an ideal. This definition is absolutely central to the abstract theory of rings, but I still think it is too general for MTH 461. Here we are using the word "ideal" as a noun, not a verb. The concept was introduced by Richard Dedekind in the mid 1800s. The original name for "ideals" was "ideal numbers", but it eventually got shortened.

Let us now translate the language of **divisibility** into the language of **principal ideals**. First we observe that

$$\boxed{a|b \quad \Longrightarrow \quad bR \subseteq aR.}$$

Proof: Suppose that $a|b$, so that $ak = b$ for some $k \in R$. Then for any ℓ we have

$$b\ell = (ak)\ell = a(k\ell),$$

which implies that every multiple of b is also a multiple of a. In other words, $bR \subseteq aR$. Conversely, suppose that $bR \subseteq aR$. In particular, since b is in the set bR (because $b = b1$) we must have $b \in aR$. By definition, this means that $b = ak$ for some $k \in R$, which implies that $a|b$ as desired. □

John Stillwell summarizes this fact with the following slogan:

"To divide is to contain."

It follows from the previous fact that

$$\boxed{aR = bR \quad \Longleftrightarrow \quad a|b \text{ and } b|a.}$$

Indeed, the statement $aR = bR$ just means that $aR \subseteq bR$ and $bR \subseteq aR$. Your intuition from the integers might suggest that

$$a|b \text{ and } b|a \quad \stackrel{?}{\Longleftrightarrow} \quad a = b.$$

But this is not quite correct. **If R is a domain**[27] then we recall from the previous section that $a|b$ and $b|a$ if and only if a and b are associate, so that

$$\boxed{aR = bR \quad \Longleftrightarrow \quad a \sim b.}$$

In the integers, we recall that $a \sim b$ if and only if $a = \pm b$. In particular, we observe that the multiples of 2 are the same as the multiples of -2:

$$2\mathbb{Z} = (-2)\mathbb{Z}.$$

Here is a table comparing the language of divisibility and principal ideals:[28]

Divisibility	Principal Ideals
$a|b$	$bR \subseteq aR$
$a \sim b$	$aR = bR$
$a \in R^\times$	$aR = R$
$a = 0$	aR = 0R.

The material of these first few sections applies to general rings and integral domains. In the next section we will return to our discussion of the rings $\mathbb{Z}$ and $\mathbb{F}[x]$. In special rings such as these we will find that the principal ideals satisfy a special property:

For any $a, b \in R$ there exists $c \in R$ such that $aR + bR = cR$.

See the next section for details.

4.5 Euclidean Domains

Each of the rings $\mathbb{Z}$ and $\mathbb{F}[x]$ has a notion of "division with remainder". Instead of proving each theorem in the subject twice, it is convenient to introduce an abstract definition that applies to both kinds of rings. The general ideas of this section go back to Euclid's *Elements*, Book VII ($\sim$ 300 BC). Of course, we will express these ideas in modern abstract language.

Definition of Euclidean Domains

Let R be an integral domain. We say that R is a *Euclidean domain* if there exists a "size function" $N : R\backslash\{0\} \to \mathbb{N}$ with the following property:

For all $a, b \in R$ with $b \neq 0$, there exist $q, r \in R$ satisfying

$$\begin{cases} a = qb + r, \\ r = 0 \text{ or } N(r) < N(b). \end{cases}$$

[27]We will only study divisibility in domains.

[28]You will prove the remaining facts on the homework.

Examples: There are two main examples.

- The ring of integers $R = \mathbb{Z}$ with size function $N(a) = |a|$ is a Euclidean domain.
- For any field $\mathbb{F}$, the ring of polynomials $R = \mathbb{F}[x]$ with size function $N(f) = \deg(f)$ is a Euclidean domain.

Remarks:

- The size function $N : R\backslash\{0\} \to \mathbb{N}$ is sometimes called a "norm function", hence my choice the letter N. This notation is not completely standard.
- Because of the example $R = \mathbb{F}[x]$ with $N(f) = \deg(f)$, we don't in general define the "size" of the zero element $N(0)$.
- The quotient q and remainder r need not be unique. They **are** unique for $R = \mathbb{F}[x]$ and $N = \deg$, but they are **not** unique for $R = \mathbb{Z}$ and $N = |\cdot|$. To get uniqueness of integer remainders we must also insist that the remainder satisfy $0 \leqslant r$, but this statement makes no sense in a general ring because R need not be ordered. Indeed, the ring $\mathbb{F}[x]$ cannot be ordered in any sensible way.

Now we will prove the "fundamental theorem" of Euclidean domains. This theorem is usually expressed by saying that

every Euclidean domain is a Principal Ideal Domain (PID).

Instead of bothering you with extra jargon, I will try to explain what this means in plainer language.

Existence and Uniqueness of Greatest Common Divisors

For any two elements in a ring, $a, b \in R$, we may consider the set of *R-linear combinations*:

$$aR + bR = \{ax + by : x, y \in R\}.$$

If R is a Euclidean domain, then for any $a, b \in R$ we can always find a single element $c \in R$ such that

$$aR + bR = cR.$$

Such an element c is called *a greatest common divisor* (gcd) *of a and b*. This c is almost unique. Indeed, if $aR + bR = c_1R$ and $aR + bR = c_2R$ then we must have $c_1R = c_2R$, and we recall from the previous section that this implies $c_1 \sim c_2$. Hence:

Any two elements $a, b \in R$ of a Euclidean domain have a greatest common *divisor, which is unique up to multiplication by units. We denote this (almost-unique) element by* $\gcd(a, b)$.

Examples.

- Any two integers $a, b \in \mathbb{Z}$ have a greatest common divisor that is unique up to multiplication by ± 1. We will write

  $$\gcd(a, b) = \text{the unique } \textbf{non-negative} \text{ greatest common divisor.}$$

  For example, the greatest common divisors of 4 and 6 are ± 2, so we take

  $$\gcd(4, 6) = +2.$$

- Any two polynomials $f(x), g(x) \in \mathbb{F}[x]$ with coefficients in a field $\mathbb{F}$ have a greatest common divisor that is unique up to multiplication by nonzero scalars. We will write

  $$\gcd(f, g) = \text{the unique } \textbf{monic} \text{ greatest common divisor.}$$

  (Monic means the leading coefficient is 1.) For example, the polynomials $x^2 - 1$ and $x^3 - 1$ have greatest common divisors $\alpha(x - 1)$ for any nonzero $\alpha \in \mathbb{F}$, so we take

  $$\gcd(x^2 - 1, x^3 - 1) = 1x - 1.$$

Proof of the Theorem. Let R be a Euclidean domain with size function $N : R \backslash \{0\} \to \mathbb{N}$. Let $a, b \in R$ be any two elements and consider the set of R-linear combinations:

$$I := aR + bR = \{ax + by : x, y \in R\}.$$

Note that I always contains 0 because $0 = a0 + b0$. If $I = \{0\}$ then we have $I = 0R$ so we can take $c = 0$. Otherwise, let c be any element of I with minimal size.[29] I claim that $I = cR$.

Since $c \in I$ we have by definition that $c = ax + by$ for some $x, y \in R$. To show that $cR \subseteq I$, we observe that any multiple cz with $z \in R$ satisfies

$$cz = (ax + by)z = a(xz) + b(yz) \in I.$$

Conversely, we will show that $I \subseteq cR$, which is the hard direction. Consider any element $d \in I$, which by definition has the form $d = ax' + by'$ for some $x', y' \in R$. Since (R, N) is a Euclidean domain, we may divide d by c to obtain

$$\begin{cases} d = qc + r, \\ r = 0 \text{ or } N(r) < N(c). \end{cases}$$

[29]This means that $c \in I$, $c \neq 0$ and for all $d \in I$ with $d \neq 0$ we have $N(c) \leqslant N(d)$.

Our goal is to show that $r \neq 0$, so that $d = cq \in cR$. So assume for contradiction that $r \neq 0$. On the one hand, this implies that $N(r) < N(c)$. On the other hand, we observe that r is an element of I:

$$r = d - qc = (ax' + by') - q(ax + by) = a(x' - qx) + b(y' - qy).$$

Thus r is a nonzero element of I with size strictly smaller than c. Contradiction. □

In order to make this proof as slick as possible we defined the concept of "greatest common divisor" using the language of principal ideals. Now we'll translate this abstract definition back into the language of divisibility. Suppose that we have

$$aR + bR = cR$$
$$\{ax + by : x, y \in R\} = \{cz : z \in R\}$$

for some elements a, b, c of a ring R. In this case, you will prove on the homework that

- $c|a$ and $c|b$, so that c is a "common divisor" of a and b,
- if d is any common divisor of a and b, then we must also have $d|c$. This is the sense in which c is a "greatest common divisor" of a and b.

This notion of "greatest" is a bit surprising. In the case that (R, N) is a Euclidean domain we might be interested in common divisors that are "greatest" in the sense of the size function; that is, elements with $c|a$ and $c|b$ such that for any other element satisfying $d|a$ and $d|b$ we must have $N(d) \leqslant N(c)$.For our two favorite Euclidean domains $\mathbb{Z}$ and $\mathbb{F}[x]$ it turns out that these two notions of "greatest" are equivalent. However, I have gotten into trouble in previous semesters trying to make this precise.

It turns out that size functions are rather awkward. For our purposes, we only use $N : R\backslash\{0\} \to \mathbb{N}$ to prove the existence of gcd and then we never refer to N again, except in the special cases of $\mathbb{Z}$ and $\mathbb{F}[x]$.

Before moving on, I will show two examples of rings that are not Euclidean.

Two Rings that are not Euclidean.

- As we have seen, long division of polynomials sometimes requires fractional coefficients. This suggests that the ring $\mathbb{Z}[x]$ of polynomials with integer coefficients is not a Euclidean domain. We can prove this rigorously by considering the following set:

$$\begin{aligned} 2\mathbb{Z}[x] + x\mathbb{Z}[x] &= \{2f(x) + xg(x) : f(x), g(x) \in \mathbb{Z}[x]\} \\ &= \{\text{polynomials in } \mathbb{Z}[x] \text{ whose constant coefficient is even}\}. \end{aligned}$$

  I claim that this set cannot be expressed in the form $c(x)\mathbb{Z}[x] = \{c(x)h(x) : h(x) \in \mathbb{Z}[x]\}$, hence the elements 2 and x **do not have a greatest common divisor** in $\mathbb{Z}[x]$. *Proof:*

Let $I = 2\mathbb{Z}[x] + x\mathbb{Z}[x]$ and note that $2, x \in I$. Now suppose for contradiction that $I = c(x)\mathbb{Z}[x]$ for some $c(x) \in \mathbb{Z}[x]$. We cannot have $c(x) = \pm 1$ because polynomials with odd constant term are not in I. And if $c(x)$ has degree $\geqslant 1$ then every element of $c(x)\mathbb{Z}[x]$ (except zero) has degree $\geqslant 1$, so $c(x)\mathbb{Z}[x]$ does not contain 2. At this point we have shown that $c(x) = c \in \mathbb{Z}$ is a constant satisfying $|c| \geqslant 2$. Since every element of $c\mathbb{Z}[x]$ has coefficients divisible by c and since every element of I has even constant term, we must have $c = \pm 2$. But then then $c\mathbb{Z}[x]$ does not contain x. Contradiction. □

- Given a field $\mathbb{F}$, we may consider the ring of polynomials $\mathbb{F}[x, y]$ in two (commuting) variables x and y. Formally, we may define the ring $\mathbb{F}[x, y]$ as $(\mathbb{F}[y])[x]$, i.e., as polynomials in x whose coefficients are polynomials in y. In this case I claim that x and y **do not have a greatest common denominator** in $\mathbb{F}[x, y]$. That is, I claim that the set

$$\begin{aligned} x\mathbb{F}[x,y] + y\mathbb{F}[x,y] &= \{xf(x,y) + yg(x,y) : f(x,y), g(x,y) \in \mathbb{F}[x,y]\} \\ &= \{\text{polynomials in } \mathbb{F}[x,y] \text{ whose constant coefficient is zero}\}, \end{aligned}$$

can not be expressed in the form $c(x,y)\mathbb{F}[x,y] = \{c(x,y)h(x,y) : h(x,y) \in \mathbb{F}[x,y]\}$. I omit the proof because it is similar to the previous item.

We will prove soon that Euclidean domains have unique prime factorization. The rings $\mathbb{Z}[x]$ and $\mathbb{F}[x, y]$ also have unique prime factorization but our proof will not apply to them. One further step is needed, which goes under the name *Gauss' Lemma*. We may or may not discuss this.

4.6 The Euclidean Algorithm

In the previous section we proved that greatest common divisors exist in Euclidean domains, but we gave no hint how to compute them. For example, suppose we want to compute the greatest common divisor of 2513 and 3094 in the ring $\mathbb{Z}$. The obvious way to do this is to test every integer in the range $1 \leqslant c \leqslant 2513$ to see if $c|2513$ and $c|3094$. Then $\gcd(2513, 3094)$ is the largest such c. But there is a **much faster way**.

The following result applies to general Euclidean domains; hence the name.

The Euclidean Algorithm

Let (R, N) be a Euclidean domain and consider elements $a, b \in R$.

- If $b = 0$ then $\gcd(a, b) = a$. Indeed, in this case we have $aR + bR = aR + 0R = aR$.
- So suppose that $b \neq 0$ and divide a by b to obtain

$$\begin{cases} a = qb + r, \\ r = 0 \text{ or } N(r) < N(b). \end{cases}$$

- If $r = 0$ then we have $\gcd(a, b) = b$. Indeed, in this case we have $b|a$ so that $a\mathbb{Z} \subseteq b\mathbb{Z}$ and hence $a\mathbb{Z} + b\mathbb{Z} = b\mathbb{Z}$.
- If $r \neq 0$ then we can divide b by r to obtain

$$\begin{cases} b = q'r + r', \\ r' = 0 \text{ or } N(r') < N(r). \end{cases}$$

- If $r' = 0$ then we stop. Otherwise, we continue to divide each new remainder by the previous, to obtain a sequence of remainders $r, r', r'', r''', \ldots, r^{(k)} \in R$ with

$$N(r) > N(r') > N(r'') > \cdots .$$

  Since the size function is a non-negative integer this implies that there exists some k such that $r^{(k)} \neq 0$ and $r^{(k+1)} = 0$. In this case I claim that

$$\gcd(a, b) = r^{(k)} = \text{the last nonzero remainder.}$$

Before proving that the algorithm works, we give an example.

Example: To compute $\gcd(2513, 3094)$ we first divide 3094 by 2513. Then we continue to divide each successive remainder by the previous:

$$\begin{array}{rcrcr} 3094 & = & 1 \cdot 2513 & + & 581 \\ 2513 & = & 4 \cdot 581 & + & 189 \\ 581 & = & 3 \cdot 189 & + & 14 \\ 189 & = & 13 \cdot 14 & + & 7 \\ 14 & = & 2 \cdot 7 & + & 0. \end{array}$$

Since 7 is the last nonzero remainder we conclude that $\gcd(2513, 3094) = 7$. Note that this algorithm took 5 steps, instead of 2513×2 steps for the slow algorithm. That's a huge improvement.[30]

Proof that the Algorithm Works. Let R any ring and consider any elements $a, b, c, x \in R$ satisfying $a = bx + c$. On the homework you will prove that this implies

$$aR + bR = bR + cR.$$

In particular, the pairs (a, b) and (b, c) have the same common divisors. Since R is a Euclidean domain, the greatest common divisors exist and we must have

$$\gcd(a, b) = \gcd(b, c).$$

[30] If d is the number of decimal digits in b then one can show that the Euclidean Algorithm uses less than (sometimes much less than) $5d + 2$ steps. This is called *Lamé's Theorem.*

We will apply this observation to the Euclidean algorithm. Suppose the sequence of remainders stops with $r^{(k)} \neq 0$ and $r^{(k+1)} = 0$. Then we have

$$\begin{aligned}
a &= qb + r & \gcd(a,b) &= \gcd(b,r) \\
b &= q'r + r' & \gcd(b,r) &= \gcd(r,r') \\
r &= q''r' + r'' & \gcd(r,r') &= \gcd(r',r'') \\
&\vdots & &\vdots \\
r^{(k-2)} &= q^{(k)}r^{(k-1)} + r^{(k)} & \gcd(r^{(k-2)},r^{(k-1)}) &= \gcd(r^{(k-1)},r^{(k)}) \\
r^{(k-1)} &= q^{(k+1)}r^{(k)} + 0, & \gcd(r^{(k-1)},r^{(k)}) &= \gcd(r^{(k)},0)
\end{aligned}$$

so that $\gcd(a,b) = \gcd(b,r) = \cdots = \gcd(r^{(k)},0)$. But $\gcd(r^{(k)},0) = r^{(k)}$. □

Thus we have an efficient algorithm for computing greatest common divisors. But this algorithm throws out useful information. Surely the sequence of quotients $q, q', q'', \ldots$ must tell us something useful. In this course I gave the fancy definition of greatest common divisors. Namely, the gcd of two elements a, b in a domain R, if it exists, is the unique (up to units) element $\gcd(a,b) \in R$ satisfying

$$aR + bR = \gcd(a,b)R.$$

Since $\gcd(a,b)$ is an element of the set $\gcd(a,b)R$ it is also an element of the set $aR + bR$, hence there exist $x, y \in R$ such that

$$ax + by = \gcd(a,b).$$

Note that these elements are not unique. Indeed suppose that $ax + by = \gcd(a,b)$ and let k be any integer. Then the elements $x', y' \in R$ defined by $x' = x - bk$ and $y' = y + ak$ also satisfy $ax' + by' = \gcd(a,b)$.[31]

The Extended Euclidean Algorithm will allow us to find one such pair x, y. Before giving the formal statement, we illustrate the ideas using the previous example $(a,b) = (2513, 3094)$. We used the Euclidean Algorithm to show that $\gcd(2513, 3094) = 7$. Now we will use the Extended Euclidean Algorithm to find some $x, y \in \mathbb{Z}$ satisfying $2513x + 3094y = 7$. The key is to consider the set of triples of integers $(x,y,z) \in \mathbb{Z}^3$ satisfying $2513x + 3094y = z$:

$$V = \{(x,y,z) \in \mathbb{Z}^3 : 2513x + 3094y = z\}.$$

Why did I choose the letter V? This set behaves like a vector space because it is closed under addition and scalar multiplication by integers.[32] Indeed, let $\mathbf{x} = (x,y,z)$ and $\mathbf{x}' = (x',y',z')$

[31] Given one solution $ax + by = \gcd(a,b)$, the **complete** solution is given by $x' = x - b'k$ and $y' = y + a'k$ where $a' = a/\gcd(a,b)$ and $b' = b/\gcd(a,b)$. We won't bother to prove this.

[32] Technically, a vector space is only defined over a field. A vector space over a more general ring such as $\mathbb{Z}$ is called a *module*. But the name doesn't matter.

be elements of V and let k be any integer. Then the triple $\mathbf{x}'' = (x'', y'', z'') = (x + kx', y + ky', z + kz') = \mathbf{x} + k\mathbf{x}'$ is also in V because

$$\begin{aligned}
2513x'' + 3094y'' &= 2513(x + kx') + 3094(y + ky') \\
&= (2513x + 3094y) + k(2513x' + 3094y') \\
&= z + kz' \\
&= z''.
\end{aligned}$$

The idea is to start with the two obvious triples $\mathbf{x} = (0, 1, 3094) \in V$ and $\mathbf{x}' = (1, 0, 2513) \in V$, then to combine these via linear combinations until we obtain a triple of the form $(x, y, 7) \in V$. The steps from the Euclidean Algorithm tells us exactly how to do this. It is convenient to organize all of the data in a table:

x	y	z	operation
0	1	3094	$\mathbf{x}$
1	0	2513	$\mathbf{x}'$
-1	1	538	$\mathbf{x}'' = \mathbf{x}' - 1 \cdot \mathbf{x}$
5	-4	189	$\mathbf{x}^{(3)} = \mathbf{x}'' - 4 \cdot \mathbf{x}'$
-16	13	14	$\mathbf{x}^{(4)} = \mathbf{x}^{(3)} - 3 \cdot \mathbf{x}''$
213	-173	7	$\mathbf{x}^{(5)} = \mathbf{x}^{(4)} - 13 \cdot \mathbf{x}^{(3)}$
-442	359	0	$\mathbf{x}^{(6)} = \mathbf{x}^{(5)} - 2 \cdot \mathbf{x}^{(4)}$

Note that the sequence of row operations correspond to the sequence of quotients from our original example: $1, 4, 3, 13, 2$. By the above remarks, each row operation produces a new solution to the equation $2513x + 3094y = z$. Thus the second-to-last row is the desired solution:[33]

$$2513(213) + 3094(-173) = 7.$$

It would be very difficult to find this solution by trial and error.

Now here is the formal statement.

The Extended Euclidean Algorithm

Consider two elements a, b of a Euclidean domain R and consider the set of triples $\mathbf{x} = (x, y, z)$ satisfying $ax + by = z$:

$$V = \{(x, y, z) \in R^3 : ax + by = z\}.$$

This set is closed under addition and multiplication by scalars from R. That is, for any

[33]Remark: The complete solution is given by combining the last two rows:

$$(x, y) = (213 - 442k, -173 + 359k) \quad \text{for any integer } k \in \mathbb{Z}.$$

$\mathbf{x}, \mathbf{x}' \in V$ and $r \in R$ we have $\mathbf{x} + r\mathbf{x}' \in V$. Note that there are two obvious triples in V:

$$\mathbf{x} = (1, 0, a) \in V \quad \text{ and } \quad \mathbf{x}' = (0, 1, b) \in V.$$

Our goal is to combine these using linear combinations until we obtain a triple of the form (x, y, z) where $z = \gcd(a, b)$. The Euclidean Algorithm tells us which steps to use.

To be precise, let $q, q', q'', \ldots$ and $r, r', r'', \ldots$ be the quotients and remainders produced by the Euclidean Algorithm (as defined previously). Then we recursively define the sequence of triples $\mathbf{x}, \mathbf{x}', \mathbf{x}'', \ldots$ by

$$\mathbf{x}^{(i)} = \mathbf{x}^{(i-1)} - q^{(i)}\mathbf{x}^{(i)}.$$

By construction, the third entry of the triple $\mathbf{x}^{(i)}$ is the remainder $r^{(i-2)}$.[34] But recall that $r^{(k)} = \gcd(a, b)$ for some k. Hence the vector $\mathbf{x}^{(k+2)}$ has the form $(x, y, \gcd(a, b))$ for some $x, y \in R$, which gives us the desired solution:

$$ax + by = \gcd(a, b).$$

It is convenient to organize these computations in a table, as follows:

x	y	z	operation
1	0	a	$\mathbf{x}$
0	1	b	$\mathbf{x}'$
1	$-q$	r	$\mathbf{x}'' = \mathbf{x} - q\mathbf{x}'$
$-q'$	$1 + qq'$	r'	$\mathbf{x}^{(3)} = \mathbf{x}'' - q'\mathbf{x}'$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
something	something	$\gcd(a, b)$	$\mathbf{x}^{(k+2)} = \mathbf{x}^{(k+1)} - q^{(k)}\mathbf{x}^{(k)}$

Remarks.

- It is not strictly necessary to use the sequence of row operations determined by the quotients. As long as you perform row operations that shrink the z-coordinate (with respect to the given size function), you will eventually arrive at a solution. However, the solution is not unique; different sequences of row operations may lead to different solutions.
- It is not clear right now why we **want** to solve the equation $ax + by = \gcd(a, b)$. Later we will see that this computation underlies all of modern cryptography.

We gave an example from the ring $\mathbb{Z}$, but the Euclidean Algorithm applies to any Euclidean domain. Here is an example involving polynomials. Consider the polynomials $x^2 + 1$ and

[34] I apologize for the discrepancy in the indices. There isn't really a clean way to do this.

$x+1$.[35] By applying the algorithm we will see that

$$\gcd(x^2+1, x+1) = 1,$$

and we will find specific polynomials $A(x), B(x)$ such that

$$(x^2+1)A(x) + (x+1)B(x) = 1.$$

We could jump right to the Extended algorithm but for teaching purposes it makes sense to begin with the basic Euclidean Algorithm. First we divide x^2+1 by $x+1$:

$$\begin{array}{r|l} & \quad\; x - 1 \\ \hline x+1 & x^2 \qquad +1 \\ & -x^2 - x \\ \hline & \qquad -x + 1 \\ & \qquad\;\; x + 1 \\ \hline & \qquad\qquad 2 \end{array}$$

Then we divide $x+1$ by 2:

$$\begin{array}{r|l} & \tfrac{1}{2}x + \tfrac{1}{2} \\ \hline 2 & \; x + 1 \\ & -x \\ \hline & \qquad 1 \\ & \quad\; -1 \\ \hline & \qquad 0 \end{array}$$

Note that we are already done after two steps. Since the last nonzero remainder was 2, we conclude that

$$\gcd(x^2+1, x+1) = 2.$$

Wait a minute! Didn't I tell you that $\gcd(x^2+1, x+1) = 1$? Recall that the greatest divisor is only unique up to multiplication by units. But the units of the polynomial ring $\mathbb{F}[x]$ are the nonzero constants. Hence 1 and 2 are associate polynomials. By convention, when we talk about "the" greatest common divisor of polynomials we always multiply by a nonzero constant so that the leading coefficient becomes 1. That is, we assume that "the" gcd of two polynomials is a *monic polynomial*.

Now we will apply the Extended algorithm to find polynomials $A(x)$ and $B(x)$ satisfying $(x^2+1)A(x) + (x+1)B(x) = 1$. The idea is to consider the set V of triples[36] of polynomials $(A(x), B(x), C(x))$ satisfying

$$(x^2+1)A(x) + (x+1)B(x) = C(x).$$

[35] The field of coefficients can be $\mathbb{Q}$ or $\mathbb{R}$ or $\mathbb{C}$, or any field that contains $\mathbb{Z}$.

[36] Here it does not make sense to use the letters (x, y, z) because x is already used for the variable.

Note that there are two obvious triples:

$$(1, 0, x^2 + 1) \text{ and } (0, 1, x + 1).$$

We combine the obvious triples using the "same steps" as the basic Euclidean Algorithm:

x	y	z	operation
1	0	x^2+1	(row 1)
0	1	$x+1$	(row 2)
1	$-x+1$	2	(row 3) = (row 1) − $(x-1)$(row 2)
$-x/2-1/2$	$x^2/2+1/2$	0	(row 4) = (row 2) − $(x/2+1/2)$(row 3)

The second-to-last row tells us that

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

And we scale this by 1/2 to obtain

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

I used this method to illustrate the general theory. However, I believe that you already know a faster method to solve the equation $(x^2 + 1)A(x) + (x + 1)B(x) = 1$. To jog your memory, we divide both sides of the previous equation by the polynomial $(x^2 + 1)(x + 1)$ to obtain

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

This is called a *partial fraction expansion*, which you probably learned in calculus class. Partial fractions are used to compute integrals of rational expressions. In our case we have

$$\begin{aligned}
\int \frac{1}{(x+1)(x^2+1)}\,dx &= \frac{1}{2}\left(\int \frac{1}{x+1}\,dx - \int \frac{x}{x^2+1}\,dx - \int \frac{1}{x^2+1}\,dx\right) \\
&= \frac{1}{2}\left(\ln(x+1) - \frac{1}{2}\ln(x^2+1) - \arctan(x)\right).
\end{aligned}$$

4.7 Unique Prime Factorization

In this section we will finish our discussion of Euclidean domains by proving that every Euclidean domain satisfies "unique prime factorization". As is the case for this whole chapter, the basic ideas of this section go back to Euclid's *Elements*, Book VII ($\sim$ 300 BC). Gauss revived these ideas in his *Disquisitiones Arithmeticae* (1801), where he proved that integers has unique prime factorization, and he called this the "fundamental theorem of arithmetic".

You are certainly familiar with unique factorization of integers. For example, we can factor the integer $12 \in \mathbb{Z}$ in various ways:

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

But these factorizations are essentially the same. The only important information is that 12 contains "two copies of the prime 2" and "one copy of the prime 3". The following details are not important:

- We can reorder the factors.
- We can multiply an even number of factors by -1.
- We can include the factor 1 an arbitrary number of times.

For general Euclidean domains we must replace "multiplication by ± 1" with "multiplication by units". For example, consider the polynomial $x^3 - x^2 - 2x + 2$ in the ring $\mathbb{Q}[x]$. Here are several factorizations:

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

This time we observe that **multiplication by constants is not interesting**. Indeed, the nonzero constants are the units of the ring $\mathbb{Q}[x]$. The only important information is that $x^3 - x^2 - 2x + 2$ contains "one copy of the prime $x - 1$" and "one copy of the prime $x^2 - 1$".[37]

But how do we know that the polynomial $x^2 - 2$ is prime? This depends on the fact that $\sqrt{2}$ is not a rational number, which we will prove at the end of this section.[38] Over the real numbers, the polynomial $x^2 - 2$ does factor, and we obtain

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

Thus the unique prime factors of a polynomial depend on the field of coefficients.

[37] Since we can always scale the leading coefficient, we will only discuss monic factors (i.e., factors with leading coefficient 1).

[38] More generally, we will use the Fundamental Theorem of Arithmetic to prove that the polynomial $x^2 - d$ is prime over $\mathbb{Q}$ whenever $d \in \mathbb{Z}$ is not a perfect square.

In order to discuss prime factorization, we must first define the word "prime". **This is trickier than you might think!** In a general ring there are several different kinds of elements that we might want to call "prime". So as not to confuse you with extra terminology I will use the word "prime" for all of these elements. For example, the next definition is usually called "irreducibility", but I will just call it "primality".

The school definition a "prime number" is "an integer greater than 1 that is only divisible by 1 and itself". Here is the translation of this concept into the language of domains.[39]

Prime Element of a Domain

Let R be a domain. An element $p \in R$ is called *prime* when:

- $p \neq 0$,
- p is not a unit,
- $a|p$ implies that $a \sim p$ or $a \sim 1$.

Thus we have made the transition from equality to associatedness:

$$\text{“if } a|p \text{ then } a = p \text{ or } a = 1\text{”} \quad \rightsquigarrow \quad \text{“if } a|p \text{ then } a \sim p \text{ or } a \sim 1\text{”}.$$

Here we are officially stating that units do not matter in the theory of factorization. It is more elegant to express this in the language of ideals.

Prime Elements in Terms of Ideals

Let a, b be elements of a domain R. We we recall that

$$\begin{aligned} aR \subseteq bR &\iff b|a, \\ aR = bR &\iff a \sim b, \\ aR = 1R &\iff a \sim 1 \\ aR = 0R &\iff a = 0. \end{aligned}$$

Thus an element $p \in R$ is prime when

- $pR \neq 0R$,
- $pR \neq 1R$,

[39] In practice, we will only discuss prime elements of domains. Factorization is non-domains is more exotic.

- $pR \subseteq aR$ implies that $aR = pR$ or $aR = 1R$.

Now we are ready to state and prove the Fundamental Theorem of Arithmetic. Note that this theorem applies to **Euclidean** domains.

The Fundamental Theorem of Arithmetic

Let R be a Euclidean domain. Suppose that we have

$$p_1 p_2 \cdots p_k \sim q_1 q_2 \cdots q_\ell$$

for some prime elements $p_1, \ldots, p_k, q_1, \ldots, q_\ell \in R$. Then we must have $k = \ell$ and we can relabel the factors so that $p_i \sim q_i$ for all i.

The key step of the proof is a famous lemma, which appears as proposition 30 in Book VII of Euclid's *Elements*. This lemma is so important that it has its own name.

Euclid's Lemma

Let R be a Euclidean domain and let $p \in R$ be prime. Then for all $a, b \in R$ we have

$$p|ab \quad \Longrightarrow \quad p|a \quad \text{or} \quad p|b.$$

Assuming this lemma, we will prove the theorem. Then we will prove the lemma.

Proof of the Fundamental Theorem. Let R be a Euclidean domain and consider any prime elements $p_1, \ldots, p_k, q_1, \ldots, q_\ell \in R$ satisfying

$$(*) \qquad p_1 p_2 \cdots p_k \sim q_1 q_2 \cdots q_\ell.$$

Since p_1 divides the left hand side it must also divide the right hand side, so

$$p_1 | q_1 q_2 \cdots q_\ell.$$

Since p_1 is prime, it follows from Euclid's Lemma that $p_1 | q_i$ for some i. After relabeling if necessary, we can assume that $p_1 | q_1$. Since q_1 is prime this implies that $p_1 \sim 1$ or $p_1 \sim q_1$. But $p_1 \sim 1$ is impossible because units are not prime, so we must have $p_1 \sim q_1$. Canceling this factor from both sides of $(*)$ gives

$$p_2 \cdots p_k \sim q_2 \cdots q_\ell.$$

And now we are done by induction. □

You might worry that I skipped some details in this proof. In particular, I didn't tell you it was going to be a proof by induction until the very end. I could certainly make the proof more explicit but I believe you would understand it less if I did that. The proof is a bit subtle so I prefered to emphasize the important steps and de-emphasize the routine steps. You might also worry that I used the symbol "$\sim$" instead of "$=$". This is because units don't matter; including them would just waste letters of the alphabet.

Proof of Euclid's Lemma. Let R be a Euclidean domain and let $p \in R$ be prime. For any elements $a, b \in R$ we will prove that

$$p|ab \quad \text{and} \quad p \nmid a \quad \Longrightarrow \quad p|b,$$

which is equivalent to the desired result.

So suppose that $p|ab$ (say $pk = ab$) and $p \nmid a$. Since p is prime and $p \nmid a$, I claim that $aR + pR = R$. Indeed, **since R is Euclidean** we know that $aR + pR = dR$ for some $d \in R$, which implies that $pR \subseteq dR$ because $pR \subseteq aR + pR$. Since p is prime, the inclusion $pR \subseteq dR$ implies that $pR = dR$ or $dR = R$. But if $pR = dR$ then $aR + pR = pR$ implies $aR \subseteq pR$, which contradicts our assumption that $p \nmid a$.

Thus we have shown that $aR + pR = R$. Since $1 \in R$ this implies that $1 \in aR + pR$, hence there exist some elements $x, y \in R$ satisfying $ax + py = 1$.[40] Finally, we multiply both sides of this equation by b to obtain

$$\begin{aligned} ax + py &= 1 \\ b(ax + py) &= b \\ abx + pby &= b \\ pkx + pby &= b \\ p(kx + by) &= b. \end{aligned}$$

It follows that $p|b$ as desired. □

To end this chapter I will apply the theory of unique factorization to give a slick proof of the following theorem.

Irrationality of Square Roots

Let n be a positive integer and let $\sqrt{n}$ be the unique positive real square root. Then

$$\sqrt{n} \in \mathbb{Q} \quad \Longrightarrow \quad \sqrt{n} \in \mathbb{Z}.$$

[40] We could find some specific x, y by using the Extended Euclidean Algorithm.

In other words, if n is not a perfect square then $\sqrt{n}$ is irrational.

In order to make the proof as clean as possible, we use the concept of "prime multipliciticy".

Prime Multiplicity

Let R be a Euclidean domain and let $p \in R$ be prime. According to the Fundamental Theorem of Arithmetic, there exists a function[41]

$$\mu_p : R \to \mathbb{N},$$

where $\mu_p(a)$ is the "multiplicity of the prime p" in the prime factorization of a. It is easy to check that this function behaves like a logarithm:

$$\mu_p(ab) = \mu_p(a) + \mu_p(b) \text{ for all } a, b \in R.$$

For example, the prime factorizations

$$\begin{aligned} 15 &= 2^0 \cdot 3^1 \cdot 5^1 \cdot 7^0, \\ 42 &= 2^1 \cdot 3^1 \cdot 5^0 \cdot 7^1, \\ 630 = 15 \cdot 42 &= 2^1 \cdot 3^2 \cdot 5^1 \cdot 7^1, \end{aligned}$$

correspond to the information

$$\begin{array}{ccccccc} \mu_2(15) + \mu_2(42) & = & 0+1 & = & 1 & = & \mu_2(630), \\ \mu_3(15) + \mu_3(42) & = & 1+1 & = & 2 & = & \mu_3(630), \\ \mu_5(15) + \mu_5(42) & = & 1+0 & = & 1 & = & \mu_5(630), \\ \mu_7(15) + \mu_7(42) & = & 0+1 & = & 1 & = & \mu_7(630). \end{array}$$

Now we can prove the theorem.

Proof. Suppose that $\sqrt{n}$ is not an integer. I claim that there exists a prime $p \in \mathbb{Z}$ such that $\mu_p(n)$ is odd. Indeed, if this were not the case then for every prime p we would have $\mu_p(n) = 2k_p$ for some integer $k_p \geqslant 0$, and hence

$$\left(\prod_p p^{k_p}\right)^2 = \prod_p p^{2k_p} = \prod_p p^{\mu_p(n)} = n.$$

[41] I use the letter μ for "multiplicity". The most common notation is ν_p, and I'm not sure why. There is a more general concept called a *discrete valuation* $\nu : R \to \mathbb{N}$. Maybe the notation ν is based on the coincidence that the Greek letter ν looks like the English letter v. I hope that's not the case.

But this contradicts the fact that n is not the square of an integer.

Now assume for contradiction that $\sqrt{n} = a/b$ for some integers $a, b \in \mathbb{Z}$, i.e., that

$$a^2 = nb^2 \quad \text{for some integers } a, b \in \mathbb{Z}.$$

Now let p be any prime such that $\mu_p(n)$ is odd, and apply μ_p to both sides of the previous equation to obtain a contradiction:

$$\begin{aligned}
\mu_p(a^2) &= \mu_p(nb^2) \\
\mu_p(a) + \mu_p(a) &= \mu_p(n) + \mu_p(b) + \mu_p(b) \\
2\mu_p(a) &= \mu_p(n) + 2\mu_p(b) \\
\text{(even)} &= \text{(odd)} + \text{(even)}.
\end{aligned}$$

□

4.8 Epilogue: Gauss' Lemma

After the basic ideas appeared in Euclid's *Elements*, it is interesting that the uniqueness of prime factorization was not studied again until Gauss' *Disquisitiones Arithmeticae* in 1800. This book launched the modern era of number theory and established a lot of notation that we still use today.[42]

Actually, Gauss' main interest was not factorization of integers, but factorization of polynomials with integer coefficients. To be specific, in his study of regular polygons (such as the 17-gon) he needed to know that for any prime $p \in \mathbb{Z}$ the polynomial

$$1 + x + x^2 + \cdots + x^{p-1}$$

cannot be factored as a product of two polynomials with integer coefficients. This is true but not at all easy to prove. The important step is to show that this polynomial cannot be factored in the ring $\mathbb{Q}[x]$ and then use this to show that it cannot be factored in $\mathbb{Z}[x]$.

We know that the ring $\mathbb{Q}[x]$ has unique prime factorization because $\mathbb{Q}$ is a field, hence $\mathbb{Q}[x]$ is a Euclidean domain. However, we remarked above that the ring $\mathbb{Z}[x]$ is **not Euclidean**. Indeed, we showed that the set

$$\begin{aligned}
2\mathbb{Z}[x] + x\mathbb{Z}[x] &= \{2f(x) + xg(x) : f(x), g(x) \in \mathbb{Z}[x]\} \\
&= \{\text{integer polynomials whose constant term is even}\}
\end{aligned}$$

cannot be expressed as $f(x)\mathbb{Z}[x]$ for any polynomial $f(x) \in \mathbb{Z}[x]$. This means that our proof of unique prime factorization does not apply to $\mathbb{Z}[x]$.

Nevertheless, it is still true that the ring $\mathbb{Z}[x]$ has unique prime factorization. More generally, we have the following abstract theorem, which is based on Article 42 of the *Disquisitiones*.

[42]For example, Gauss introduced the notation $a \equiv b \pmod{n}$, which we will discuss in our chapter on modular arithmetic.

Gauss' Lemma

Let R be a domain and consider the ring of polyonomials $R[x]$. We say that R is a *unique factorization domain* (UFD) if it satisfies the conclusion of the Fundamental Theorem of Arithmetic. Then

$$R \text{ is a UFD} \quad \Longrightarrow \quad R[x] \text{ is a UFD.}$$

The proof requires a few new ideas, so we omit it for lack of time.

In particular, since $\mathbb{Z}$ is Euclidean it is a UFD, and it follows from Gauss' Lemma that $\mathbb{Z}[x]$ is a UFD. Furthermore, if $\mathbb{F}$ is a field then since $\mathbb{F}[x]$ is Euclidean it is a UFD, and we conclude from Gauss' Lemma that $\mathbb{F}[x][y] = \mathbb{F}[x, y]$ is a UFD. By induction, the ring of polynomials in any number of variables over $\mathbb{Z}$ or a field $\mathbb{F}$ has unique prime factorization.

In general, it is difficult to prove that a given polynomial is prime. We will return to this topic when we discuss field extensions.

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:

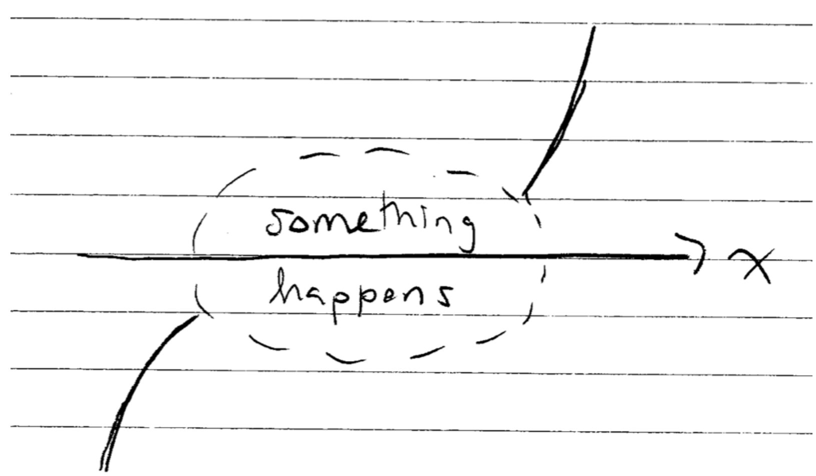
- Prove that a solution exists.
- Find an approximate solution.
- Find an exact formula for a solution.

The first two questions can be answered with calculus.

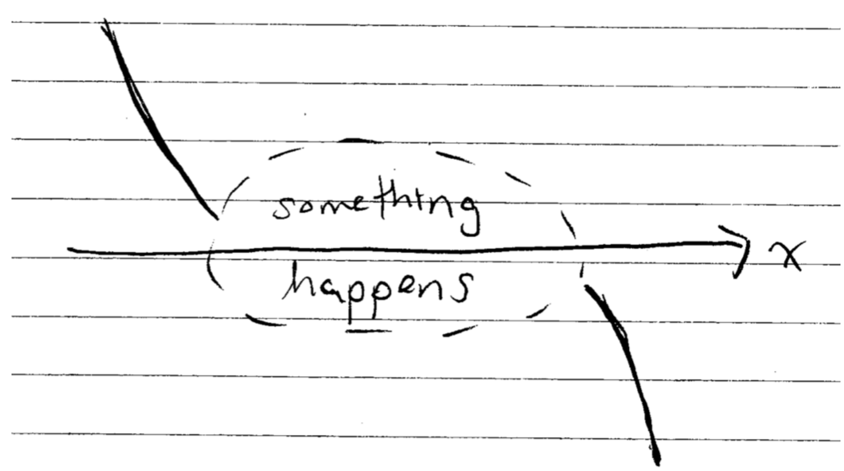
Every Odd Polynomial Has a Real Root

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. $\square$

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",[43] which is the opposite of "algebra". Nevertheless, I will give you a quick taste.

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 $c \in \mathbb{R}$,[44] 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 $f(c) = 0$. $\square$

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

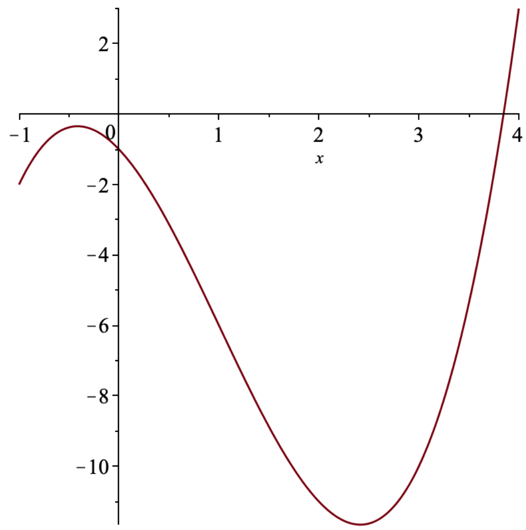
[44] Today we would take this as part of the **definition** of the real numbers.

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:



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.[45] 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.

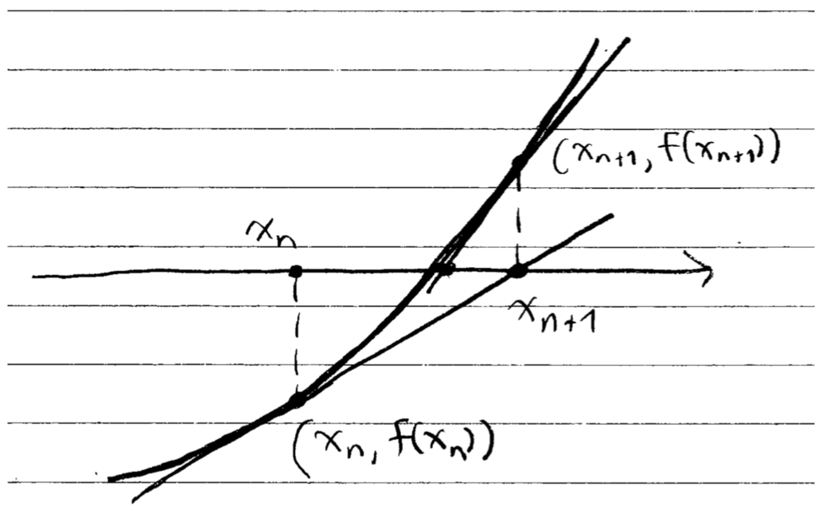
Newton's Method

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:

[45]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

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

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

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

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

$$\begin{cases} uv &= 2,\\ u^3 + v^3 &= 6.\end{cases}$$

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

$$\begin{cases} u^3v^3 &= 8,\\ u^3 + v^3 &= 6.\end{cases}$$

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

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

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

$$x = y + \alpha$$

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

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. $\square$

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:[46]

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

[46] 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.

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 $-i$.[47] 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:

$$\begin{array}{cr}
i \cdot i = -1 & \textit{più di meno via più di meno fa meno} \\
i(-i) = 1 & \textit{più di meno via meno di meno fa più} \\
(-i)i = 1 & \textit{meno di meno via più di meno fa più} \\
(-i)(-i) = -1. & \textit{meno di meno via meno di meno fa meno}
\end{array}$$

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[48]

$$\begin{aligned}
(a + bi)^3 &= a^3 + 3a^3bi + 3ab^2i^2 + b^3i^3 \\
&= a^3 + 3a^3bi - 3ab^2 - b^3i \\
&= (a^3 - 3ab^2) + (3a^2b - b^3)i.
\end{aligned}$$

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

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

[47] 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.

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

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

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)

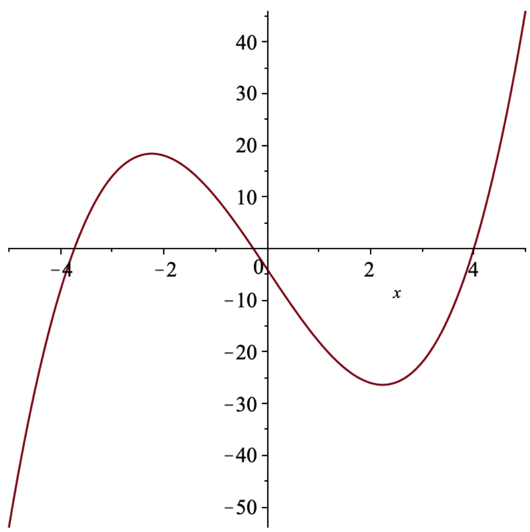
Unfortunately, Bombelli still could not answer the question of multiple real roots. Since $x = 4$ is a root of $x^3 - 15x - 4$, we can use long division to factor out $x - 4$:

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

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 $\Delta \neq 0$. $\square$

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[49] 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. Take $s = 11i$, which is 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:

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

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

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

[49] 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.

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

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.[50] 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 $i^2 = -1$:

$$\begin{aligned}(a+bi) + (c+di) &:= (a+c) + (b+d)i,\\ (a+bi)(c+di) &:= (ac - bd) + (ad + bc)i.\end{aligned}$$

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" $1 + 0i$.[51] 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**.

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

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

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

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

$\square$

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.[52] 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.

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:

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

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

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.[53] You will verify them on the homework.

(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

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

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

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.[54] 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.[55] 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.

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.[56] 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.

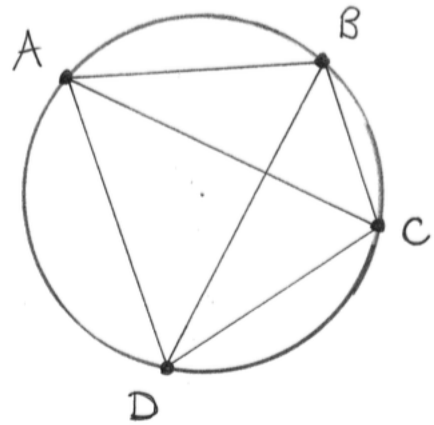
Ptolemy's Theorem

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

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

[55] *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).

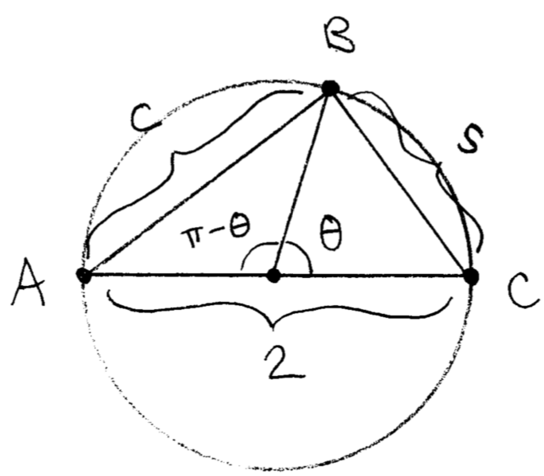
[56] This is why we still use the Babylonian "base 60" numerical system to measure angles.



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:



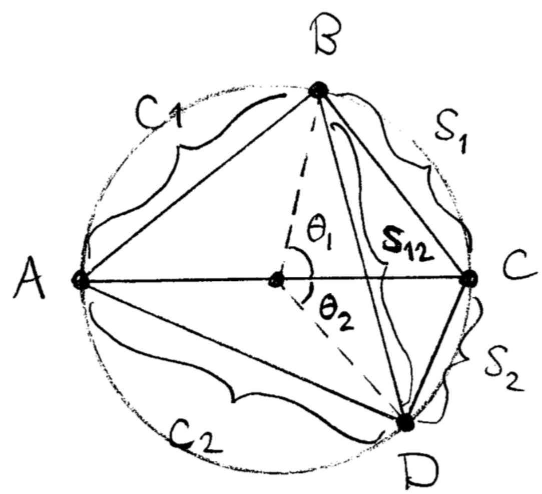
Here we have a right triangle inscribed in a circle of radius 1. In modern language, one can check that the chord lengths s and c satisfy

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

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":

$$\cos(2\theta) = 2\cos\theta\cos(1\theta) - \cos(0\theta)$$

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

And after that the "triple angle formula":

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

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:

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

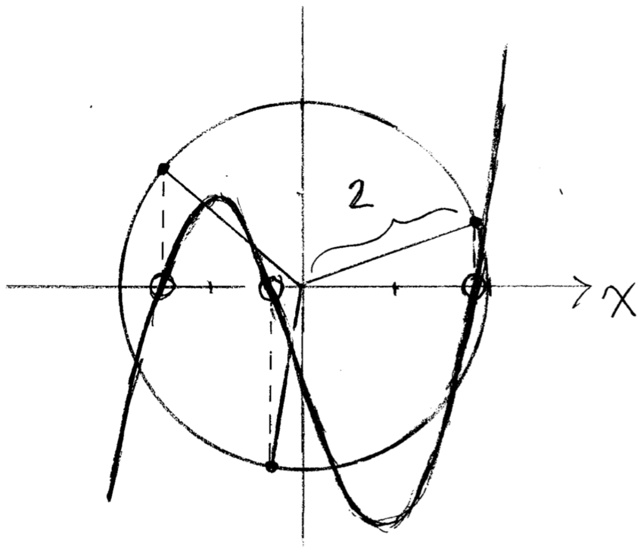
Observe that this equation becomes $x^3 - 3x - 1 = 0$ when we substitute $x = 2\cos\theta$ and $\cos(3\theta) = 1/2$. The second condition has **exactly three solutions**:

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

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.[57]

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

[57] 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.

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

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

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:

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

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

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

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:

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

□

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.[58] 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.

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 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*:[59]

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

For all $\alpha \in \mathbb{C}$ and integers $n \geqslant 0$ we apply the triangle inequality and the multiplicative

[58] 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.*

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

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:

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

□

Euler was not 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[60] 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 $\mathbb{C}$:

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

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

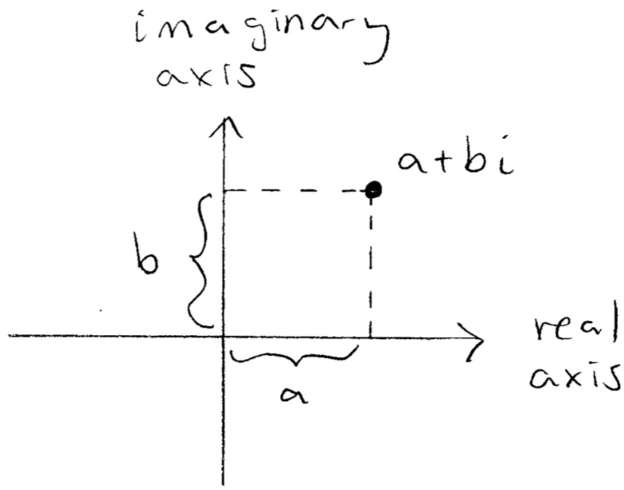
$$x^3 - 1 = (x-1)\left(x - \frac{1+i\sqrt{3}}{2}\right)\left(x - \frac{1-i\sqrt{3}}{2}\right).$$

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.

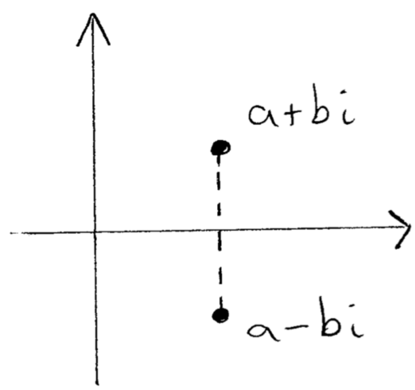
Definition of the Complex Plane

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:

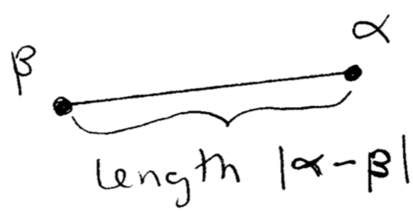
[60] Or clockwise. The choice is arbitrary.



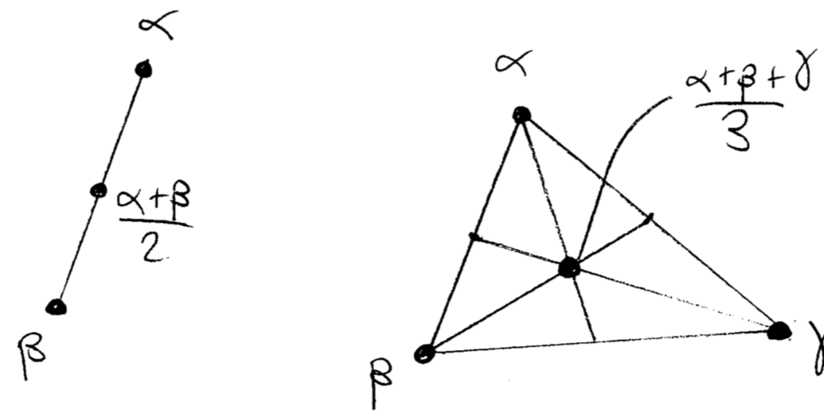
In this language, we observe that conjugate pairs of complex numbers correspond to "mirror images" across the real axis:



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:



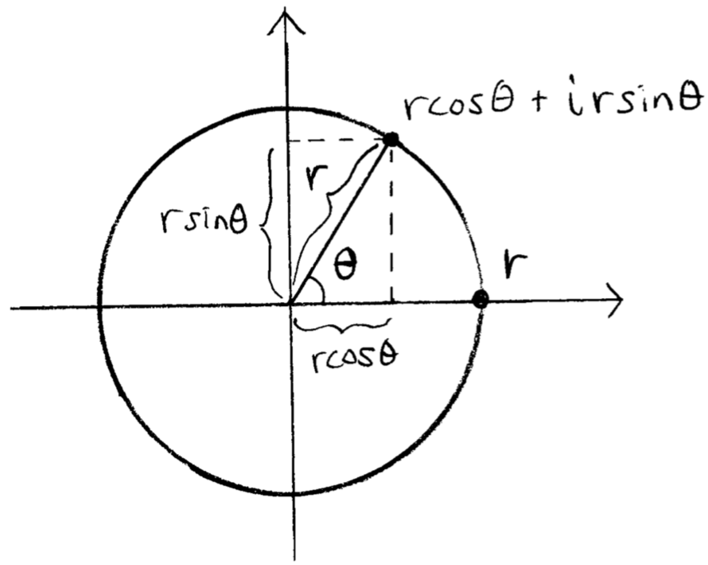
Finally, we observe that the "numerical average" of any collection of complex numbes is the "center of mass" (or "centroid") of the corresponding points:



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:

$$(r_1e^{i\theta_1})(r_2e^{i\theta_2}) = (r_1r_2)e^{i(\theta_1+\theta_2)}.$$

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

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

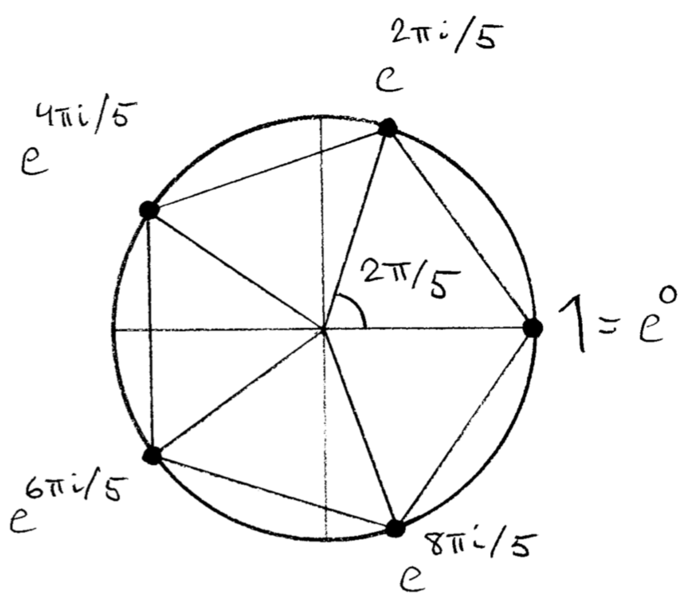
Then since $r \geqslant 0$ we must have $r = 1$. It follows that $e^{i5\theta} = 1$, and hence

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

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.

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

$$\begin{aligned} \omega^k = \omega^\ell &\Leftrightarrow e^{2\pi i k/n} = e^{2\pi i \ell/n} \\ &\Leftrightarrow 2\pi k/n - 2\pi\ell/n = 2\pi q \text{ for some } q \in \mathbb{Z} \\ &\Leftrightarrow k - \ell = nq \text{ for some } q \in \mathbb{Z} \\ &\Leftrightarrow n|(k - \ell). \end{aligned}$$

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 $r_1 = r_2$. □

Remark: Actually, the theorem still holds as stated if we replace $\omega = e^{2\pi i/n}$ by $\omega = e^{2\pi i m/n}$ 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 us observe how complex conjugation interacts with the polar form.

Complex Conjugation and Polar Form

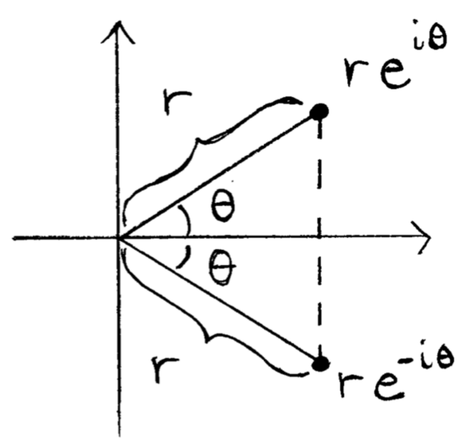
For any real number $\theta \in \mathbb{R}$ we recall that $\cos(-\theta) = \cos\theta$ and $\sin(-\theta) = -\sin\theta$. It follows from this that $e^{-i\theta}$ is the complex conjugate of $e^{i\theta}$:

$$e^{-i\theta} = \cos(-\theta) + i\sin(-\theta) = \cos\theta - i\sin\theta = (\cos\theta + i\sin\theta)^* = (e^{i\theta})^*.$$

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

$$(x-\alpha)(x-\alpha^*) = x^2 - (\alpha+\alpha^*)x + \alpha\alpha^* = x^2 - 2ax + (a^2+b^2) \in \mathbb{R}[x].$$

$\square$

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.

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 $\mathbb{Q}[x]$.[61] Thus we have obtained the prime factorization of $x^n - 1 \in \mathbb{Q}[x]$.

We postpone the proof for now. Instead we will look at an example. 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

$$x^6 - 1 = (x - 1)(x - \omega_6^1)(x - \omega_6^2)(x - \omega_6^3)(x - \omega_6^4)(x - \omega_6^5)$$

[61] According to Gauss' Lemma, a polynomial $f(x) \in \mathbb{Z}[x]$ is prime in $\mathbb{Z}[x]$ if and only if it is prime in $\mathbb{Q}[x]$.

$$
\begin{aligned}
&= (x-1)(x-\omega_6^1)(x-\omega_3^1)(x-\omega_2^1)(x-\omega_3^2)(x-\omega_6^5) \\
&= (x-1)(x-\omega_2^1)\left[(x-\omega_3^1)(x-\omega_3^2)\right]\left[(x-\omega_6^1)(x-\omega_6^5)\right] \\
&= \Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_6(x).
\end{aligned}
$$

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*,[62] 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.

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 $\mathbb{C}$.[63] 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

$$f(x) = (x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n)c \quad \text{for some } \alpha_1, \ldots, \alpha_n, c \in \mathbb{C}.$$

[62] He only proved this when n is prime.

[63] 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.

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:

$$f(x) = c \prod_{i=1}^{k} (x - a_i) \prod_{j=1}^{\ell} (x^2 - (\alpha_j + \alpha_j^*)x + \alpha_j \alpha_j^*).$$

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.[64] Gauss gave a proof along these lines, which was generally accepted as the first correct proof of the FTA.

[64] By this I mean that two curves in the plane that seem to cross based on their pictures, do indeed cross at some point.

- 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.

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 differentiation is much easier than integration/anti-differentiation. 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.[65]

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".

[65] 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.*

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:

$$\mathbb{R}(x) := \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in \mathbb{R}[x] \text{ and } g(x) \neq 0(x) \right\}.$$

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 $1/x$.[66] Leibniz

[66]The modern notation of exponential and logarithmic functions was developed by Euler.

also discovered that 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 two forms. The following result was proved by Leibniz in 1702 paper, using the method of "partial fractions".

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 $1 = 5x + 3y$. We can use the Extended Euclidean Algorithm (or just trial and error) to see that $1 = 5(2) + 3(-3)$. Then we divide both sides by 15 to obtain

$$\frac{1}{15} = \frac{5(2) + 3(-3)}{15} = \frac{5(2)}{15} + \frac{3(-3)}{15} = \frac{2}{3} + \frac{-3}{5}.$$

To get an expression for $7/15$ 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 $1 = 4x + 3y$. In this case it is easy: $1 = 4(1) + 3(-1)$. 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 $5/12$:

$$\frac{5}{12} = \frac{5}{3} + \frac{-5}{4}$$

$$
\begin{aligned}
&= \left(1+\frac{2}{3}\right)+\frac{-5}{4} \\
&= 1+\frac{2}{3}+\left(\frac{-3}{2}+\frac{1}{4}\right) \\
&= 1+\frac{2}{3}-2+\frac{1}{2}+\frac{1}{4} \\
&= -1+\frac{1}{2}+\frac{1}{4}+\frac{2}{3}.
\end{aligned}
$$

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.

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 4 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[67] 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 $N(r_{ij}) < N(p_i)$.

[67]In the case of $R = \mathbb{F}[x]$, the polynomials $c, r_{ij} \in \mathbb{F}[x]$ are unique. In the case of $R = \mathbb{Z}$ the integers $c, r_{ij} \in \mathbb{Z}$ are not unique, but they become unique if we also require $0 \leqslant r_{ij} < p_j$, as in the examples above. We won't prove either of these statements.

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

$$\frac{a}{b} = \frac{ac_1 p_2^{e_2} p_3^{e_3} \cdots p_k^{e_k}}{b} + \frac{acp_1^{e_1}}{b}.$$

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

$$\frac{a}{p^e} = \frac{q_e p + r_e}{p^e} = \frac{q_e}{p^{e-1}} + \frac{r_e}{p^e} \qquad \text{with } r_e = 0 \text{ or } N(r_e) < N(p).$$

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 the fastest way to compute partial fraction 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 is 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:[68]

> *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 $\gcd(a, b) = 1$.

[68]See *Galois' Theory of Algebraic Equations* (2001), by Jean-Pierre Tignol, pages 74–75.

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:

$$\begin{aligned} f(a/b) &= 0 \\ c_n(a/b)^n + \cdots + c_1(a/b) + c_0 &= 0 \\ b^n\left[c_n(a/b)^n + \cdots + c_1(a/b) + c_0\right] &= 0 \\ c_n a^n + c_{n-1}a^{n-1}b + \cdots + c_1 ab^{n-1} + c_0 b^n &= 0. \end{aligned}$$

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 $\mathbb{F}$. $\square$

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.[69] 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.

[69] In fact, this difficulty is the foundation of the RSA Cryptosystem, which allows us to safely transmit our credit card information to Amazon.

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 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. $\square$

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:

$$\begin{aligned} ae^{i\pi/4} &= a\omega \\ ae^{i3\pi/4} &= a\omega^3 \\ ae^{i5\pi/4} &= a\omega^5 = a\omega^{-3} \end{aligned}$$

$$ae^{i7\pi/4} = a\omega^7 = a\omega^{-1}.$$

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[70]

$$\begin{aligned} &\int \frac{1}{x^4 + a^4}\,dx \\ &= \int \frac{1}{\left(x^2 - a\sqrt{2}\,x + a^2\right)\left(x^2 + a\sqrt{2}\,x + a^2\right)}\,dx \\ &= \text{ some work} \\ &= \frac{\sqrt{2}}{4a^3}\left[\arctan\left(\frac{\sqrt{2}}{a}\,x + 1\right) + \arctan\left(\frac{\sqrt{2}}{a}\,x - 1\right) + \frac{1}{2}\ln\left|\frac{x^2 + a\sqrt{2}\,x + a^2}{x^2 - a\sqrt{2}\,x + a^2}\right|\right]. \end{aligned}$$

7.4 Equivalent Statements of the FTA

Before moving on, we should clarify the statement of the FTA.

Equivalent Statements of the FTA

I claim that the following four statements are equivalent:

(1$\mathbb{C}$) Every non-constant polynomial $f(x)\mathbb{C}[x]$ has a root in $\mathbb{C}$.

(2$\mathbb{C}$) For any $f(x) \in \mathbb{C}[x]$ of degree $n \geqslant 1$ there exist $c, \alpha_1, \ldots, \alpha_n \in \mathbb{C}$ such that

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

(1$\mathbb{R}$) Every non-constant polynomial $f(x) \in \mathbb{R}[x]$ has a root in $\mathbb{C}$.

(2$\mathbb{R}$) For any $f(x) \in \mathbb{R}[x]$ of degree $\geqslant 1$ there exist polynomials $p_1(x), \ldots, p_k(x) \in \mathbb{R}[x]$

[70] Actually, I let my computer do it. There is no need for humans to perform these kinds of computations.

of degrees 1 and 2 such that

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

This last statement was the original statement of the theorem, which together with the method of partial fractions guarantees that the antiderivative of any rational function can be expressed in terms of log and arctan.

In this section we will prove that the four statements are equivalent. The easy implications are (2ℂ)⇒(1ℂ) and (2ℝ)⇒(1ℝ). Indeed, if

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

then we have $f(\alpha_i) = 0$ for all i, hence $f(x)$ has a complex root. Next, suppose that

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

for some polynomials $p_1(x), \ldots, p_k(x) \in \mathbb{R}[x]$ of degrees 1 and 2. If some $p_i(x)$ has degree 1 then we have $p_i(x) = ax + b$ with $a \neq 0$, and hence $f(x)$ has a real root $-b/a \in \mathbb{R}$. Otherwise, all of the factors $p_i(x)$ have degree 2. But this is still okay because any degree 2 polynomial with real coefficients has a complex root by the quadratic formula.

The implication (1ℂ)⇒(2ℂ) is not much more difficult.

Proof that (1ℂ)⇒(2ℂ). Assume that (1ℂ) is true and consider any polynomial $f(x) \in \mathbb{C}[x]$ of degree $n \geqslant 1$. By (1ℂ) there exists some $\alpha_1 \in \mathbb{C}$ such that $f(\alpha_1) = 0$. Then Descartes' Theorem gives

$$f(x) = (x - \alpha_1)f_1(x)$$

for some $f_1(x) \in \mathbb{C}[x]$ of degree $n - 1$. If $n - 1 \geqslant 1$ then from (1ℂ) there exists some $\alpha_2 \in \mathbb{C}$ such that $f_1(\alpha_2) = 0$. Then Descartes' Theorem gives $f_1(x) = (x - \alpha_2)f_2(x)$ and hence

$$f(x) = (x - \alpha_1)(x - \alpha_2)f_2(x)$$

for some $f_2(x) \in \mathbb{C}[x]$ of degree $n - 2$. Continuing in this way we obtain complex numbers $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ such that

$$f(x) = (x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n)f_n(x),$$

where $f_n(x) \in \mathbb{C}[x]$ has degree 0, i.e., $f_n(x)$ is constant. □

The implication (1ℝ)⇒(2ℝ) requires two pieces of technology.

Complex Roots of Real Polynomials

For any real polynomial $f(x) \in \mathbb{R}[x]$ and complex number $\alpha \in \mathbb{C}$ we have

$$f(\alpha)^* = f(\alpha^*).$$

It follows from this that

$$f(\alpha) = 0 \quad \Longleftrightarrow \quad f(\alpha^*) = 0,$$

which says that the non-real complex roots of real polynomials come in conjugate pairs.

Proof. We recall some properties of complex conjugation. For all $\alpha, \beta \in \mathbb{C}$ we have

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

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

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

Thus for any real polynomial $f(x) = \sum a_k x^k \in \mathbb{R}[x]$ and any complex number $\alpha \in \mathbb{C}$ we have

$$\begin{aligned}
[f(\alpha)]^* &= \left(\sum a_k \alpha^k\right)^* \\
&= \sum (a_k \alpha^k)^* && \text{(i)} \\
&= \sum a_k^* (\alpha^*)^k && \text{(ii)} \\
&= \sum a_k (\alpha^*)^k && \text{(iii)} \\
&= f(\alpha^*).
\end{aligned}$$

It follows that

$$f(\alpha) = 0 \quad \Longleftrightarrow \quad [f(\alpha)]^* = 0 \quad \Longleftrightarrow \quad f(\alpha^*) = 0.$$

□

Real vs Complex Quotient and Remainder

Consider real polynomials $f(x), g(x) \in \mathbb{R}[x]$ with $g(x) \neq 0$ and suppose we have complex polynomials $q(x), r(x) \in \mathbb{C}[x]$ satisfying

$$\begin{cases} f(x) = g(x)q(x) + r(x), \\ r(x) = 0 \text{ or } \deg(r) < \deg(g). \end{cases}$$

Then actually $q(x)$ and $r(x)$ have real coefficients.

Proof. Homework.

Proof that (1ℝ)⇒(2ℝ). Assume that (1ℝ) is true and consider any non-constant polynomial $f(x) \in \mathbb{R}[x]$ with real coefficients. We will use induction on the degree of $f(x)$ to show that $f(x)$ can be expressed as

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

where $p_1(x), \ldots, p_k(x)$ are real polynomials of degrees 1 and 2. By (1ℝ) there exists a complex number $\alpha \in \mathbb{C}$ such that $f(\alpha) = 0$. There are two cases:

- Suppose α is real and consider the real polynomial $p_1(x) = x - \alpha \in \mathbb{R}[x]$ of degree 1. By Descartes' Theorem we have
$$f(x) = p_1(x)g(x)$$
for some real polynomial $g(x) \in \mathbb{R}[x]$ with $\deg(g) = \deg(f) - 1$. Then by induction the polynomial $g(x)$ can be factored as a product of real polynomials of degrees 1 and 2.

- Suppose that α is not real, so that $\alpha \neq \alpha^*$. Since $f(\alpha) = 0$ and since $f(x)$ has real coefficients, the lemma on complex roots of real polynomials tells us that $f(\alpha^*) = 0$. Applying Descartes once gives
$$f(x) = (x - \alpha)g(x)$$
for some complex polynomial $g(x)$ with $\deg(g) = \deg(f) - 1$. Since $\alpha \neq \alpha^*$ we may substitute $x = \alpha^*$ to obtain
$$\begin{aligned} (\alpha^* - \alpha)g(\alpha^*) &= f(\alpha^*) \\ (\alpha^* - \alpha)g(\alpha^*) &= 0 \\ g(\alpha^*) &= 0. \end{aligned}$$
Then applying Descartes' Theorem again gives
$$g(x) = f(x) = (x - \alpha)(x - \alpha^*)h(x)$$
for some complex polynomial $h(x) \in \mathbb{C}[x]$ with $\deg(h) = \deg(g) - 1 = \deg(f) - 2$. Observe that the polynomial
$$p_1(x) = (x - \alpha)(x - \alpha^*) = x^2 - (\alpha + \alpha^*)x + \alpha\alpha^*$$
actually has **real coefficients**. Then since $f(x) = p_1(x)h(x)$ with $f(x) \in \mathbb{R}[x]$ and $p_1(x) \in \mathbb{R}[x]$, it follows from the lemma on real vs complex quotients that $h(x)$ actually has **real coefficients**. Finally, since $\deg(h) < \deg(f)$ it follows by induction that $h(x)$ can factored as a product of real polynomials of degrees 1 and 2.

$\square$

For example, suppose that a real polynomial $f(x) \in \mathbb{R}[x]$ satisfies $f(i) = 0$. Then we must also have $f(-i) = 0$ and hence

$$f(x) = (x-i)g(x) = (x-i)(x+i)h(x) = (x^2+1)h(x)$$

for some polynomial $h(x) \in \mathbb{C}[x]$. But since $f(x)$ and x^2+1 are real and $f(x) = (x^2+1)h(x)$, then $h(x)$ must also have real coefficients.

So far we have proved that (1$\mathbb{C}$)$\Leftrightarrow$(2$\mathbb{C}$) and (1$\mathbb{R}$)$\Leftrightarrow$(2$\mathbb{R}$). Our final goal is to prove that (1$\mathbb{C}$)$\Leftrightarrow$(1$\mathbb{R}$). The direction (1$\mathbb{C}$)$\Rightarrow$(1$\mathbb{R}$) is easy. The proof is really just the observation that $\mathbb{R} \subseteq \mathbb{C}$, but I'll add a few extra words.

Proof that (1$\mathbb{C}$)$\Rightarrow$(1$\mathbb{R}$). Assume that (1$\mathbb{C}$) is true and consider any non-constant polynomial $f(x) \in \mathbb{R}[x]$. Since $\mathbb{R}[x] \subseteq \mathbb{C}[x]$ we also have $f(x) \in \mathbb{C}[x]$, so it follows from (1$\mathbb{C}$) that $f(x)$ has a root in $\mathbb{C}$. $\square$

Finally, we must prove that (1$\mathbb{R}$)$\Rightarrow$(1$\mathbb{C}$). In other words, if every non-constant real polynomial has a root in $\mathbb{C}$ then every non-constant complex polynomial has a root in $\mathbb{C}$. This sounds like it might not even be true, but there is a clever trick that makes it work.

Conjugation of Complex Polynomials

For any polynomial $f(x) = \sum \alpha_k x^k \in \mathbb{C}[x]$ we define the *conjugate polynomial* $f^*(x) \in \mathbb{C}[x]$ by conjugating each of the coefficients:

$$f^*(x) = \sum \alpha_k^* x^k.$$

Then the following properties hold:

- For all $f(x) \in \mathbb{C}[x]$ and $\alpha \in \mathbb{C}$ we have $[f(\alpha)]^* = f^*(\alpha^*)$.
- For all $f(x) \in \mathbb{C}[x]$ we have $f(x) \in \mathbb{R}[x]$ if and only if $f^*(x) = f(x)$.
- For all $f(x), g(x) \in \mathbb{C}[x]$ we have

$$(f+g)^*(x) = f^*(x) + g^*(x) \quad \text{and} \quad (fg)^*(x) = f^*(x)g^*(x).$$

- For all $f(x) \in \mathbb{C}[x]$ we have

$$f(x) + f^*(x) \in \mathbb{R}[x] \quad \text{and} \quad f(x)f^*(x) \in \mathbb{R}[x].$$

Proof. Homework.

Proof that (1ℝ)⇒(1ℂ). Homework.

7.5 Euler's Attempt

In the previous section we saw four equivalent statements of the FTA, but we have still not proved that any of these statements is true. In 1702, Leibniz doubted that the polynomial $x^4 + a^4$ could be factored over the real numbers. However, with the aid of complex numbers, we have seen that

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

Then grouping the four factors into complex conjugate pairs gives

$$x^4 + a^4 = (x^2 - a\sqrt{2}x + a^2)(x^2 + a\sqrt{2}x + a^2).$$

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 asserted that the following polynomial cannot be factored over the real numbers:

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

Euler responded with a general method to factor any real quartic as a product of two real quadratics. In this special case, we first replace x with $x + 1$ to remove the x^3 term:[71]

$$g(x) = f(x + 1) = x^4 - 4x^2 + 7.$$

We are looking for real numbers $p, q, r, s \in \mathbb{R}$ such that

$$\begin{aligned} x^4 + 0x^3 - 4x^2 + 0x + 7 &= (x^2 + px + q)(x^2 + rx + s) \\ &= x^4 + (p + r)x^3 + (pr + q + s)x^2 + p(r + s)x + qs. \end{aligned}$$

Comparing coefficients gives

$$\begin{cases} p + r &= 0, \\ pr + q + s &= -4, \\ ps + qr &= 0, \\ qs &= 7. \end{cases}$$

If $p = 0$ then we obtain the equations $q + s = -4$ and $qs = 7$, which have no real solution. So let us assume that $p \neq 0$. Then the first equation gives $r = -p$ and the third equation gives $ps = -qr = pq$, hence $s = q$. The remaining equations are

$$\begin{cases} -p^2 + 2q &= -4, \\ q^2 &= 7. \end{cases}$$

[71] In fact, the polynomial $g(x)$ has no x^3 term and no x^1 term, so it is called *biquadratic*. You will prove on the homework that every biquadratic real polynomial has real quadratic factors. Euler's method in this section is more explicit because it actually finds the factors.

This has the solution $q = \sqrt{7}$ and $p = \sqrt{4+2\sqrt{7}}$, hence we obtain

$$g(x) = x^4 - 4x^2 + 7 = \left(x^2 + \sqrt{4+2\sqrt{7}} \cdot x + \sqrt{7}\right)\left(x^2 - \sqrt{4+2\sqrt{7}} \cdot x + \sqrt{7}\right).$$

Replacing x with $x-1$ gives the desired factorization of $f(x) = g(x-1)$.

Since the polynomial $g(x)$ was biquadratic, the coefficients of the factors can be expressed in terms of square roots. In general this will not be the case, but Euler showed that the coefficients still exist.

FTA for Quartic Polynomials

Every real quartic polynomial factors as a product of two real quadratic polynomials.

I will copy Euler's proof directly from *Recherches sur les racines imaginaires des équations* (1751), § 27, with just a few small notational changes.

Euler's Proof. For any real $a, b, c, d \in \mathbb{R}$ we consider the quartic polynomial

$$f(x) = x^4 + ax^3 + bx^2 + cx + d.$$

Replace x with $x - a/4$ to obtain

$$g(x) = f(x - a/4) = x^4 + Bx^2 + Cx + D$$

for some real numbers $B, C, D \in \mathbb{R}$. We are looking for real numbers $u, \alpha, \beta\mathbb{R}$ such that

$$x^4 + Bx^2 + Cx + D = (x^2 + ux + \alpha)(x^2 - ux + \beta).$$

Expand the right hand side and compare coefficients to obtain

$$\left\{\begin{array}{lcl} B &=& \alpha + \beta - u^2, \\ C &=& (\beta - \alpha)u, \\ D &=& \alpha\beta. \end{array}\right.$$

We can rewrite the first two equations as $\alpha + \beta = B + u^2$ and $\alpha - \beta = C/u$. Then we can add and subtract these equations to obtain

$$2\alpha = B + u^2 + C/u \quad \text{and } 2\beta = B + u^2 - C/u.$$

Then the third equation gives

$$4D = 4\alpha\beta$$

$$
\begin{aligned}
&= 2\alpha 2\beta \\
&= (B + u^2 + C/u)(B + u^2 - C/u) \\
&= u^4 + 2Bu^2 + B^2 - C^2/u^2,
\end{aligned}
$$

and multiplying both sides of this equation by u^2 gives

$$h(u) := u^6 + 2Bu^4 + (B^2 - 4D)u^2 - C^2 = 0.$$

We are looking for a real solution $u \in \mathbb{R}$ to the equation $h(u) = 0$. The polynomial $h(u)$ has even degree so we normally cannot conclude that it has a real root. However, since $h(u) \to +\infty$ as $u \to \pm\infty$, and since the value $h(0) = -C^2$ is **negative**, we conclude[72] that $h(u) = 0$ has at least two real solutions, one negative and one positive. Choosing either of these solutions gives real values for $\alpha = [B + u^2 + C/u]/2$ and $\beta = [B + u^2 - C/u]/2$, hence we obtain the desired factorization of $g(x)$. Finally, we obtain a factorization of $f(x)$:

$$f(x) = g(x + a/4) = \left((x + a/4)^2 + u(x + a/4) + \alpha\right)\left((x + a/4)^2 - u(x + a/4) + \beta\right).$$

□

Euler's proof for degree 8 (article 34). Corollary: Degree 6 (article 38).

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.

[72] The Intermediate Value Theorem was not proved rigorously until much later. In Euler's time it was not regarded as needing a proof.

8 Other Rings and Fields

8.1 Modular Arithmetic

8.2 Quotient Rings in General

Maybe not.

8.3 Cauchy's Construction of Complex Numbers

8.4 Kronecker's Construction of Splitting Fields

8.5 Galois' Finite Fields

Freshman's Dream.

9 Groups

9.1 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.

9.2 Congruence Modulo a Subgroup

Subgroups of $(\mathbb{Z}, +, 0)$. The set of congruence classes. The quotient group.

9.3 Isomorphism of Groups

Examples $\Omega_n \cong \mathbb{Z}/n\mathbb{Z}$, $U(1) \cong SO(2)$.

9.4 Order of an Element

9.5 The Fermat-Euler-Lagrange-Cauchy Theorem

Order of an element. Order of a power.

9.6 Existence of Primitive Roots

If we want to prove Gauss-Wantzel then some hard Gaussian stuff is unavoidable.

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 Permuting the Roots

This section is for my own benefit. Do not read.

Let $p(x) \in \mathbb{F}[x]$ be irreducible and consider the field $\mathbb{E} = \mathbb{F}[x]_p$ of polynomials modulo $p(x)$. Note that $x \in \mathbb{E}$ is a root of $p(x)$. Suppose that $r(x) \in \mathbb{E}$ is another root of p. Note that any element of $\mathbb{E}$ has the form $f(x) \in \mathbb{E}$ for some $f(x) \in \mathbb{F}[x]$. I claim that the rule $f(x) \mapsto f(r(x))$ is a well-defined field automorphism of $\mathbb{E}$. Since evaluation is a homomorphism we only need to check that it is well-defined and bijective.

Proof: We assume that $p(r(x)) \sim 0$ so that $p(x)|p(r(x))$ in $\mathbb{F}[x]$. Well-Defined: $f(x) \sim g(x)$ implies $p(x)|[f(x) - g(x)]$ implies $p(r(x))|[f(r(x)) - g(r(x))]$ implies $p(x)|[f(r(x)) - g(r(x))]$ implies $f(r(x)) \sim g(r(x))$. Injective: Suppose $f(r(x)) \sim g(r(x))$ for some $\deg(f), \deg(g) < \deg(p)$.

For the proofs of Injective and Surjective we will first show that there exists $s(x) \in \mathbb{F}[x]$ with $r(s(x)) \sim 0$ and $s(r(x)) \sim 0$. Since $p(r(x)) \sim 0$ we have $p(x)|p(r(x))$. Then evaluating at $r(x)$ gives $p(x)|p(r(x))|p(r(r(x))$, and hence $p(r^{(k)}(x)) \sim 0$ for any compositional power of $r(x)$. Since $p(x)$ has finitely many roots in the field $\mathbb{E}$ this implies that $r^{(k)}(x) \sim r^{(\ell)}(x)$ for some $k < \ell$. But then I claim that $r^{(\ell-k)}(x) \sim r^{(0)}(x) = x$. Indeed, if $k \neq 0$ then we observe that $(r^{(k-1)} - r^{(\ell-1)})(x) \in \mathbb{F}[x]$ has the root $r(x) \in \mathbb{E}$. Since $p(x) \in \mathbb{F}[x]$ is the minimal polynomial of $r(x) \in \mathbb{E}$ this implies that $p|(r^{(k-1)} - r^{(\ell-1)})$ and hence $r^{(k-1)}(x) \sim r^{(\ell-1)}(x)$. Repeating the argument give the result. Then by defining $s(x) := r^{(\ell-k-1)}(x) \in \mathbb{F}[x]$ we have $r(s(x)) \sim x$ and $s(r(x)) \sim x$.

Injective: $f(r(x)) \sim g(r(x))$ implies $f(r(x)) - g(r(x)) = p(x)q(x)$ implies $f(r(s(x))) - g(r(s(x))) = p(s(x))q(s(x))$. Then since $p(x)|p(s(x))$ we have

$$f(x) \sim f(r(s(x)) \sim g(r(s(x))) \sim g(x).$$

Surjective: For any $f(x) \in \mathbb{E}$ we have

$$f(x) \sim f(s(r(x)) = (f \circ s)(r(x)).$$

□

10.5 The Gauss-Wantzel Theorem

Maybe this section is also for my own benefit.

The 5-gon and 17-gon are constructible. Why? Because cyclotomic polynomials are irreducible. We won't prove in general but maybe we should prove that $\Phi_p(x)$ is irreducible.

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 $(\omega^r)^* = \omega^{-r} = (\omega^{-1})^r = (\omega^*)^r$. □

Remark: An alternate—more elementary—proof appears in the previous section.

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.

Philosophy: If Gauss couldn't do it then it doesn't belong in this book.

11 Unsolvability of the Quintic

What happens when we don't have a primitive root?