

# Chapter 1

## Numbers

- **The Natural Numbers** are well-ordered. This allows one to use induction to define addition and multiplication of natural numbers, and to prove the basic (commutative, associative, distributive) laws. There is no subtraction or exact division, but there is division with remainders, which goes into Euclid's algorithm for finding the greatest common divisor (gcd) of two natural numbers.
- **The Integers** consist of the natural numbers, as well as 0 and the negatives. The negatives, which are the additive inverses of the natural numbers, allow one to define subtraction as addition of the additive inverse. The negation transformation, taking a number to its additive inverse, is our first example of a linear transformation.
- **The Rational Numbers** are equivalence classes of integer fractions, which include the integers themselves. All the arithmetic operations and rules hold for the rational numbers, including exact division. Such a number system is called a field. Any definition meant to apply to rational numbers, but made in terms of fractions (e.g. addition and multiplication) needs to be checked to be sure it is well-defined.
- **The Real Numbers** are the positive length numbers, together with 0, and the negative numbers. The field of real numbers contains the rational numbers as well as many irrationals. Infinite decimals represent real numbers, such as  $\sqrt{2}$  (the length of the hypotenuse of a right triangle with sides of length 1) and  $\pi$  (the circumference of a circle whose diameter has length 1). Arithmetic can be defined geometrically, or by continuity from the rational numbers.
- **The Complex Numbers** contain two square roots of  $-1$ , which are declared to be the imaginary numbers  $i$  and  $-i$ . This allows one to define the complex numbers as a vector space over the real numbers with basis  $\{1, i\}$ , which is also (miraculously) a field. All the  $n$ th roots of a nonzero complex number may then be geometrically described (there are always  $n$  of them) using polar coordinates.

## 1.1 The Natural Numbers

The elements of the set of natural numbers:

$$\mathbb{N} = \{1, 2, 3, 4, 5, \dots\}$$

are the numbers we use for counting. They come equipped with an **ordering**:

$$1 < 2 < 3 < 4 < \dots$$

and they also come equipped with the:

**Well-ordered axiom:** Every set of natural numbers except the empty set has a smallest element.

**Note:** This is an axiom, meaning we will accept it without demanding a proof. (Why do you suppose mathematicians are willing to accept this?)

From the well-ordered axiom we may deduce the:

**Principle of induction:** If  $S$  is a subset of  $\mathbb{N}$ , such that:

- (i)  $1 \in S$  and
- (ii) whenever  $n \in S$ , the next number after  $n$  is also an element of  $S$

then  $S$  is equal to  $\mathbb{N}$ , the set of all natural numbers.

**Note:** This is **not** given as an axiom, so we have to prove it!

**Proof:** Consider the complementary set  $S^c$  whose elements are the natural numbers that are **not** elements of  $S$ . This is also a set of natural numbers, to which we will apply the well-ordered axiom. In other words, either  $S^c$  has a smallest element or else it is the empty set. Let's suppose  $S^c$  has a smallest element. That element can't be 1 (because  $1 \in S$  by (i)) and it can't be anything bigger than 1 (because whenever  $S^c$  contains a number bigger than 1, then  $S^c$  also contains the number immediately **before** it by (ii)). So **no** natural number can be the smallest element of  $S^c$ , so  $S^c$  is empty, which is the same as saying that  $S$  is the set of all natural numbers.

We can do a lot with the principle of induction. Any time you might be tempted to write the abbreviation "etc." or "..." in a proof or definition, then you probably should use the principle of induction. For example, we define the addition of 1 to any natural number  $m$  as follows:

**Definition of Addition of 1:**  $m + 1$  is the next number after  $m$ .

But we'd also like to be able to define addition of anything as follows:

$m + 2$  is the next number after  $m + 1$ ,

$m + 3$  is the next number after  $m + 2$ ,

etc.

This is a job for the principle of induction.

**Strategy for making definitions by induction.**

A function  $f$  whose domain is  $\mathbb{N}$  may be defined in two steps:

- (i) Define  $f(1)$ .
- (ii) Define each  $f(n+1)$ , possibly using a previous definition of  $f(n)$ .

The domain of the function  $f$  is then a subset of  $\mathbb{N}$  that contains 1 by (i), and whenever  $n$  is in the domain, then  $n+1$  is also in the domain by (ii). Therefore the domain of  $f$  is  $\mathbb{N}$ , by the principle of induction!

**Definition of Addition:**  $m+n$  is defined for all  $m$  and  $n$  as follows:

- (i)  $m+1$  is, as above, defined to be the next number after  $m$ .
- (ii) Each  $m+(n+1)$  is defined to be the next number after  $m+n$ .

Think of  $m$  as a fixed natural number and  $n$  as a variable. Then (i) and (ii) define the function  $f(n) = m+n$  for all values of  $n$  by the strategy above for definitions by induction.

**Clarification:** Since we are regarding  $m$  as fixed while  $n$  is a variable, the two letters play quite different roles. Because of this, we need to prove annoying things like the commutativity of addition(!) If we had thought of them both as variables, we would not have been able to use the principle of induction to define addition because  $f(m,n) = m+n$  would have been a function of two variables!

Next we turn to proofs by induction. A **mathematical sentence**  $P$  is an (ordinary) sentence that is definitely either true or false. For example:

- “There are 5 days in a week” is a false mathematical sentence,
- “ $14 > 13$ ” is a true mathematical sentence, and
- “ $5 + 2 = 8$ ” is another false mathematical sentence, but
- “It was a dark and stormy night” is too vague to be mathematical.

$P(n)$  will stand for an ordinary sentence that may contain the variable  $n$  (but no other variables) and which becomes a mathematical sentence whenever  $n$  is given a (natural number) value. These are much like functions  $f(n)$ , which contain the variable  $n$  and become a number whenever  $n$  is given a natural number value. Sentences  $P(n)$  may be true for all values of  $n$ , or they may be only true for some (or no) values. For example:

- “There are  $n$  days in a week” is only true for the value  $n = 7$ . But
- “ $n + 1 > n$ ” is true for all values of  $n$ , and
- “ $n + 1 = n$ ” is never true (but it is still of the form  $P(n)$ ), while
- “ $n = m$ ” is only of the form  $P(n)$  when a value for  $m$  is chosen.

Suppose we are given  $P(n)$ , which we think should be true for all  $n$ .

**Strategy for proving  $P(n)$  is true for all  $n$  by induction.**

This may be done in two steps:

(i) Prove that the sentence  $P(1)$  is true.

(ii) Prove that each sentence  $P(n + 1)$  is true, possibly making use of the assumed truth of  $P(n)$ .

Define  $S$  to be the set of natural numbers that make  $P(n)$  true.  $1 \in S$  by (i), and whenever  $n \in S$ , then  $n + 1 \in S$ , by (ii). Thus  $S = \mathbb{N}$  by the principle of induction, so proving (i) and (ii) proves that the sentences  $P(n)$  are all true.

**Associativity Law of Addition:**

$$(l + m) + n = l + (m + n)$$

for all natural numbers  $l, m, n$ .

**Proof:** Think of  $l$  and  $m$  as fixed. We follow the strategy for a proof by induction to prove, for all  $n$ , the associativity sentences:

$$“(l + m) + n = l + (m + n)”$$

which we’ll call  $P(n)$ .

(i) By addition definition (i),  $(l + m) + 1$  is the next number after  $l + m$ , and by addition definition (ii),  $l + (m + 1)$  is also the next number after  $l + m$ . Since there is only one next number after  $l + m$ , we get:

$$(l + m) + 1 = l + (m + 1)$$

That is,  $P(1)$  is proved to be true.

**More Clarification:** In the proof of (i) above,  $l + m$  plays the role of  $m$  in addition definition (i), and  $l$  and  $m$  play the roles of  $m$  and  $n$ , respectively, in addition definition (ii). This scrambling of letters is unfortunate in these proofs, but it is also pretty much unavoidable. When you are checking these proofs and constructing your own, you might want to keep careful track of such scrambles. One way of keeping track would be with footnotes. As an example, I’ve footnoted the scrambles for you in the remainder of this proof.

(ii) We need to prove each  $P(n + 1)$ :

$$(l + m) + (n + 1) = l + (m + (n + 1))$$

allowing ourself to assume  $P(n)$ :

$$(l + m) + n = l + (m + n)$$

We will do this by taking the next numbers after each side of equation  $P(n)$  (which must then be equal to each other!). Applying addition definition (ii)<sup>1</sup> to the left side, we see that:

$$(l + m) + (n + 1) \text{ is the next number after } (l + m) + n$$

On the other hand, applying addition definition (ii)<sup>2</sup> to the right side of the equation, we see that  $l + ((m + n) + 1)$  is the next number after  $l + (m + n)$ . Moreover, using  $P(1)$  above<sup>3</sup>, which we have already proved(!) and substitution, we get  $l + ((m + n) + 1) = l + (m + (n + 1))$ , so:

$$l + (m + (n + 1)) \text{ is the next number after } l + (m + n)$$

and putting these together, we do indeed get  $(l + m) + (n + 1) = l + (m + (n + 1))$  completing part (ii) of the proof.

Thus our proof by induction strategy proves that the associativity sentence is true for every  $n$ . And since  $l$  and  $m$  could be anything, we have proved the associative law of addition!

You will prove the commutative law of addition (in the exercises).

**Definition of Multiplication:**  $m \times n$  is defined for all  $m$  and  $n$  as follows:

- (i)  $m \times 1 = m$ .
- (ii) Each  $m \times (n + 1) = m \times n + m$ .

Think of  $m$  as a fixed natural number and  $n$  as a variable. Then  $f(n) = m \times n$  (also written  $mn$ ) is defined for all  $n$  by induction.

**Note:** By writing  $m \times n + m$  or  $mn + m$ , we mean, of course,  $(m \times n) + m$ , following the standard rules for the order of arithmetic operations.

**Multiplication distributes with addition:**

$$(l + m) \times n = l \times n + m \times n$$

for all natural numbers  $l, m, n$ .

**Proof:** Think of  $l$  and  $m$  as fixed, and apply the induction strategy to prove:

$$“(l + m) \times n = l \times n + m \times n”$$

(the distributivity sentence, which we’ll call  $P(n)$ ) for all  $n$ .

- (i) Two applications of multiplication definition (i) give  $P(1)$ :

$$(l + m) \times 1 = l + m = l \times 1 + m \times 1$$

---

<sup>1</sup>Here,  $l + m$  plays the role of  $m$  in the definition.

<sup>2</sup>Here,  $l$  and  $m + n$  play the role of  $m$  and  $n$ , respectively, in the definition.

<sup>3</sup>Here,  $m$  and  $n$  play the role of  $l$  and  $m$ , respectively.

(ii) For each  $n$ , if we assume  $P(n)$  is true:  $(l + m)n = ln + mn$ , then

$$(l + m)(n + 1) = (l + m)n + (l + m) = (ln + mn) + (l + m)$$

by multiplication definition (ii) and substituting.

But now we may use the associative and commutative rules for addition to regroup and reorder the terms of the right side to get:

$$\begin{aligned} (ln + mn) + (l + m) &= ((ln + mn) + l) + m \\ &= (ln + (mn + l)) + m \\ &= (ln + (l + mn)) + m \\ &= ((ln + l) + mn) + m \\ &= (ln + l) + (mn + m) \end{aligned}$$

On the other hand:

$$l(n + 1) = ln + l \text{ and } m(n + 1) = mn + m$$

by multiplication definition (ii). So we see that  $P(n + 1)$  follows:

$$(l + m)(n + 1) = l(n + 1) + m(n + 1)$$

and we conclude that the distributivity sentence  $P(n)$  is true for **all**  $n$ .

We will leave the associative law of multiplication for the exercises, and prove instead the commutative law:

**Multiplication is commutative:**  $mn = nm$  for all  $m$  and  $n$ .

**Proof:** Think of  $m$  as fixed and use proof by induction to prove:

$$“mn = nm”$$

(the commutativity sentences, which we’ll call  $P(n)$ ) for all values of  $n$ .

(i)  $m \times 1 = m$ , so we need to prove  $1 \times m = m$ . We’ll do this by induction!

(i’)  $1 \times 1 = 1$  by multiplication definition (i)

(ii’) For each  $n$ ,  $1 \times n = n$  implies that  $1 \times (n + 1) = 1 \times n + 1 = n + 1$  by multiplication definition (ii).

(i’) and (ii’) together prove  $1 \times n = n$  for all  $n$  (including  $m$ , whatever  $m$  is), which is what we needed to prove (i). Now on to the proof of (ii).

(ii) For each  $n$ ,  $mn = nm$  implies that  $m(n + 1) = mn + m = nm + m$  by multiplication definition (ii) and substitution. But  $nm + m = (n + 1)m$  by the distributive law and (i) above, so  $m(n + 1) = (n + 1)m$ . By our proof by induction strategy we’ve proved  $P(n)$  for all  $n$ , which is the commutative law.

This completes the basic arithmetic of the natural numbers. We’ve seen how induction was an important tool for making precise definitions and proofs.

Next, we'll do a couple of easy proofs by induction as further illustration of this powerful strategy. For this, we'll use one more definition:

**Definition of subtraction of 1:** For all natural numbers  $n$  except  $n = 1$ ,  $n - 1$  is defined to be the natural number immediately before  $n$ .

**Proposition 1.1.1.** *For all  $n$ , the  $n$ th odd number is  $2n - 1$ .*

**Proof (by induction):**

(i) The first odd number is 1, which is the number immediately before  $2 \times 1$ .

(ii) For each  $n$ , if the  $n$ th odd number is  $2n - 1$ , then the  $n + 1$ st odd number is  $(2n - 1) + 2$  (odd numbers alternate with even numbers!), which is clearly(!) the number before  $2n + 2 = 2(n + 1)$ . That is, the  $n + 1$ st odd number is  $2(n + 1) - 1$ . End of proof!

**Proposition 1.1.2.** *For all  $n$ , the sum of the first  $n$  odd natural numbers is  $n^2 = n \times n$ .*

**Proof (by induction):**

(i) The sum of the first 1 odd numbers is  $1 = 1^2$ .

(ii) For each  $n$ , if the sum of the first  $n$  odd numbers is  $n^2$ , then the  $n + 1$ st odd number is  $2(n + 1) - 1 = 2n + 1$  by Proposition 1.1.1 and so the sum of the first  $n + 1$  odd numbers is:

$$n^2 + (2n + 1) = (n^2 + n) + (n + 1) = n(n + 1) + (n + 1) = (n + 1)^2$$

by the standard rules of arithmetic. End of proof.

**Remark:** One can prove many results of this type using induction. See the exercises and any elementary textbook in number theory.

Like subtraction, division of natural numbers is not usually defined. We'll fix this later with the rational numbers. However, we do have:

**Division with remainders (long division):** To each pair  $m < k$ , there is a quotient natural number  $q$  with the property that either:

(a)  $k = mq$ , and we say that  $m$  **divides**  $k$  (or  $m$  is a **factor** of  $k$ ),

or else there is a remainder natural number  $r < m$  such that:

(b)  $k = mq + r$ .

**Proof:** First of all, if  $m = 1$  then  $m$  divides every number ( $k = 1 \times k$ ) so we only need to worry about  $m$ 's that are greater than 1. Fixing  $m$ , we will use proof by induction to prove division with remainders for all  $n$  and  $k = m + n$  (the entire division with remainders sentence with  $k = m + n$  will be our  $P(n)$ ). The two cases complicate matters somewhat, but it all works out:

(i)  $m + 1 = m \times 1 + 1$  (this is case (b) with  $r = 1$ ). This proves  $P(1)$ .

(ii) For each  $n$ , if  $P(n)$  is true for  $k = m + n$ , then either:

(a)  $m + n = mq$ , or or else:

(b)  $m + n = mq + r$  and  $r < m$

In (a),  $m + (n + 1) = mq + 1$  which is case (b) of  $P(n + 1)$  with remainder 1.

In (b), there are two possibilities to consider:

(a') if  $r + 1 = m$ , then  $m + (n + 1) = mq + m = m(q + 1)$   
(This is case (a) of  $P(n + 1)$ ) or

(b') if  $r + 1 < m$ , then  $m + (n + 1) = mq + (r + 1)$   
(This is case (b) of  $P(n + 1)$  with remainder  $r + 1$ ).

Thus no matter which case occurs in division with remainders for  $k = m + n$ , we've proved that division with remainders is then true for  $k = m + (n + 1)$ . So division with remainders is true for **every**  $k > m$  by induction.

**Definition:** A natural number  $p$  (other than 1) is **prime** if the only numbers that divide  $p$  are 1 and  $p$  itself.

**The primes under 50:** 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47.

Here's a different use of the well-ordered axiom.

**Fundamental Theorem of Arithmetic:** Every natural number except 1 factors as a product of prime numbers.

**Proof:** Let  $S$  be the set of natural numbers (other than 1) that **cannot** be factored as a product of prime numbers. By the well-ordered axiom  $S$  is either empty, or else it has a smallest element, which we'll call  $k$ , and which is either prime or not prime. But:

(a) Prime numbers do not belong to  $S$ , because they are factored!

(b) Numbers that are not prime (other than 1) can be written as  $k = mq$  with both  $m$  and  $q$  smaller than  $k$ . So if  $k$  is the smallest element of  $S$ , then both  $m$  and  $q$  are not in  $S$  and therefore they can both be factored(!). But then  $k$  can be factored, too, so  $k$  couldn't have been in  $S$  in the first place!

Thus there cannot be a smallest element of  $S$ , so  $S$  is empty, which means that all natural numbers (other than 1) can be factored.

**Remarks:** The primes are the building blocks of the natural numbers much like the elements are the building blocks of the molecules. The factorization of a number into a product of primes is unique, as we shall see later in the course. If you are given a very large number, however, there is no known algorithm for factoring it quickly as a product of primes, even on a fast computer. This observation has been exploited for internet security. It is even difficult to tell quickly whether the number is prime or not, though there are some quick ways of telling "almost for sure" whether or not a given large number is prime.

We can now prove a very famous old result of Euclid:

**Theorem (Euclid):** There are infinitely many prime numbers.

**Proof:** Suppose we only know of finitely many. We could name them:

$$p_1, p_2, \dots, p_n$$

and we could then build the following number:

$$N = p_1 \times p_2 \times \dots \times p_n + 1$$

By the fundamental theorem of arithmetic,  $N$  factors as a product of primes, but none of the known primes  $p_1, \dots, p_n$  divides  $N$ . So the prime factors of  $N$  are new, and since there are always new primes, there must be infinitely many!

We finish the natural numbers with another useful result of Euclid:

**Euclid's Algorithm:** Start with natural numbers  $m < n$ . Perform long divisions according to the following algorithm whenever there is a remainder:

$$\begin{aligned} n &= mq_1 + r_1 \\ m &= r_1q_2 + r_2 \\ r_1 &= r_2q_3 + r_3 \\ r_2 &= r_3q_4 + r_4 \end{aligned}$$

Eventually the algorithm terminates with no remainder:  $r_k = r_{k+1}q_{k+2}$ , and the last of the remainders, namely  $r_{k+1}$ , is the greatest common divisor (gcd) of  $m$  and  $n$ , i.e. the largest natural number that divides both. We will prove this later in the course, but for now, let's consider an:

**Example:** Find the gcd of  $2^5 \times 3^3 \times 5^2 = 21600$  and  $2^2 \times 3^3 \times 5^5 = 337500$ .

We can do this with Euclid's algorithm:

$$\begin{aligned} 337500 &= 21600 \times 15 + 13500 \\ 21600 &= 13500 \times 1 + 8100 \\ 13500 &= 8100 \times 1 + 5400 \\ 8100 &= 5400 \times 1 + 2700 \\ 5400 &= 2700 \times 2 \end{aligned}$$

and then  $r_k = 5400$ ,  $r_{k+1} = 2700$  and  $q_{k+2} = 2$ , so 2700 is the gcd.

Of course, those of you who were paying attention in gradeschool also know:  $2^2 \times 3^3 \times 5^2 = 2700$  is the gcd, and this is certainly an easier way to find the gcd of these two particular numbers than Euclid's algorithm. But there's a catch. This way of finding gcd's requires the **factorizations** of  $m$  and  $n$ . Euclid's algorithm doesn't require any factorizations, and indeed using Euclid's algorithm to find the gcd of two large numbers is very fast and easy (for computers), even when factoring the numbers is slow and hard.

### 1.1.1 Natural Number Exercises

**1-1** Find the error in the following fake definition by induction of subtraction:

**Fake Subtraction definition:** Let  $m$  be a natural number other than 1.

- (i)  $f(1) = m - 1$  is the number before  $m$ .
- (ii)  $f(n + 1) = m - (n + 1)$  is the number before  $f(n) = m - n$ .

Therefore,  $m - n$  is defined (and a natural number!) for all  $m$  and  $n$ .

**1-2** Here's another arithmetic operation that can be defined by induction:

- (a) Define the **exponential**  $m^n$  by induction.

( $m$  is the “base” and  $n$  is the “exponent”)

- (b) Prove by induction that  $m^{l+n} = m^l m^n$ .
- (c) Prove by induction that  $(m^l)^n = m^{ln}$ .

**1-3** Define the **factorial**  $n!$  by induction.

**1-4** Prove by induction that addition of natural numbers is commutative.

**1-5** Prove by induction that multiplication of natural numbers is associative.

**1-6** (a) Prove by induction that the  $n$ th even number is  $2n$ .

- (b) Prove by induction that the sum of the first  $n$  even numbers is  $n \times (n + 1)$ .

**1-7** Find (and count) all the prime numbers:

- (a) between 1 and 100
- (b) between 101 and 200
- (c) between 201 and 300
- (d) between 301 and 400

**1-8** Factor each of the following numbers as a product of primes:

- (a) 9699690
- (b) 82861
- (c) 10001

**1-9** Find the gcd of 159477 and 241133 using Euclid's algorithm.

**1-10** Induction also is important in set theory.

- (a) Define the set  $S_n = \{1, 2, \dots, n\}$  by induction.
- (b) Prove by induction that there are exactly  $2^n$  subsets of  $S_n$ .

**Hint:** Exactly half the subsets of  $S_{n+1}$  contain the element  $n + 1$ .

## 1.2 The Integers and Rational Numbers

The elements of the set of integers:

$$\mathbb{Z} = \{\dots, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, \dots\}$$

consist of three types of numbers:

- I. The (positive) natural numbers  $\{1, 2, 3, 4, 5, \dots\}$ ,
- II. The negative integers  $\{-1, -2, -3, -4, -5, \dots\}$ , and
- III. The number 0.

The ordering on the natural numbers extends to an ordering of the integers:

$$\dots < -5 < -4 < -3 < -2 < -1 < 0 < 1 < 2 < 3 < 4 < 5 < \dots$$

but there is no well-ordered principle for the integers since many subsets of  $\mathbb{Z}$  (including  $\mathbb{Z}$  itself) have no smallest element.

Negative numbers may seem obvious today, but there was a long period of time when only positive numbers were used. The introduction of 0 is often cited as evidence of the scientific superiority of the eastern cultures during the middle ages. It is remarkable that we can easily (if tediously) extend the operations of addition and multiplication of natural numbers to include 0 and the negative integers, maintaining all the fundamental laws of arithmetic. Negative numbers are necessary today because, in our society based upon the right to the pursuit of happiness through credit card debt, we need to be able to **subtract**!

**Definition of Addition.**  $a + b$  is defined on a case by case basis:

**Case I.**  $b = n$  is positive. Then  $a + n$  is defined by induction.

- (i)  $a + 1$  is the next number after  $a$ ,
- (ii) Each  $a + (n + 1)$  is the next number after  $a + n$

**Case II.**  $b = -n$  is negative. Then  $a + (-n)$  is also defined by induction.

- (i')  $a + (-1)$  is the number immediately before  $a$ , and
- (ii') Each  $a + (-(n + 1))$  is the number immediately before  $a + (-n)$

**Case III.**  $b = 0$ . By definition,

$$a + 0 = a$$

The associative and commutative laws of addition can now be proved for this new definition of addition by the same proof-by-induction strategy we used in §1.1 (but it is tedious, involving lots of different cases, so we won't do it!) Since the first case of the definition of addition is identical to the definition of addition of natural numbers from §1.1, the two additions give the same result when applied to two natural numbers.

Before we tackle multiplication, we introduce:

**The Negation Transformation:** Negation is the function:

$$- : \mathbb{Z} \rightarrow \mathbb{Z}$$

defined by:  $-(n) = -n$ ,  $-(0) = 0$  and  $-(-n) = n$ . It is clear that

$$-(-a) = a \text{ for all integers } a$$

(double negatives cancel) and that taking negatives reverses order:

$$\text{if } a < b \text{ then } -b < -a$$

Negation has the following three important properties, too:

**Proposition 1.2.1.** *For all integers  $a$ ,*

$$a + (-a) = 0$$

(and because of this, we say that  $-a$  is an **additive inverse** of  $a$ ).

**Proof:** This is clearly true for  $a = 0$  since  $0 + (-0) = 0 + 0 = 0$ . Otherwise, either  $a$  or  $-a$  must be a natural number, so it is enough by the commutativity of addition to prove the “additive inverse” sentence  $n + (-n) = 0$  for all  $n$ , which we will now do by induction:

(i)  $1 + (-1)$  is the number before 1, by addition definition (i'), which is 0.

(ii) For each  $n$ , once we know  $n + (-n) = 0$ , then since  $-(n + 1)$  is the number before  $-n$ , we also know that:

$$(n + 1) + (-(n + 1)) = (n + 1) + (-n + (-1))$$

by addition definition (i'), and then

$$(n + 1) + (-n + (-1)) = (1 + (-1)) + (n + (-n))$$

by the commutative and associative laws of addition. But now:

$$1 + (-1) = 0, \quad n + (-n) = 0 \quad \text{and} \quad 0 + 0 = 0$$

allow us to conclude that  $(n + 1) + (-(n + 1)) = 0$ , hence the induction.

**Proposition 1.2.2.**  *$-a$  is the **only** additive inverse of  $a$ .*

**Proof:** Suppose  $b$  is another additive inverse of  $a$ . Then:

$$-a + (a + b) = -a + 0 = -a$$

but using the associative law of addition, we also have:

$$-a + (a + b) = (-a + a) + b = 0 + b = b$$

so  $-a = b$ . Thus any other additive inverse of  $a$  is equal to  $-a$ , which is the same thing as saying that  $-a$  is the only additive inverse of  $a$ .

**Proposition 1.2.3.** *Negation is a linear transformation, meaning:*

$$-(a + b) = -a + (-b)$$

**Proof:** By the laws of addition and Proposition 1.2.1:

$$(a + b) + (-a + (-b)) = (a + (-a)) + (b + (-b)) = 0$$

so  $-a + (-b)$  is an additive inverse of  $a + b$ . From Proposition 1.2.2, we know that there is only one additive inverse of  $a + b$ , so  $-a + (-b) = -(a + b)$ .

Now we are finally ready for the:

**Definition of Subtraction:** For all integers  $a$  and  $b$ :

$$a - b = a + (-b)$$

(that is, subtraction of  $b$  is defined to be addition of the additive inverse of  $b$ )

Finally (for the integers), we use negatives to define multiplication:

**Definition of Multiplication.**  $ab$  is defined on a case-by-case basis.

**Case I.**  $b = n$  is a positive. Then  $a \times n$  is defined by induction:

- (i)  $a \times 1 = a$ ,
- (ii) Each  $a \times (n + 1) = a \times n + a$ .

**Case II.**  $b = -n$  is negative. Then  $a \times (-n)$  is defined to be  $-(a \times n)$ .

**Case III.**  $b = 0$ . Then  $a \times 0 = 0$

**Remark:** The definitions in Cases II and III are forced upon us, if we want multiplication to satisfy the distributive law! (see the exercises) Notice also that

$$a \times (-1) = -a$$

so the negation transformation is the same as multiplication by  $-1$ .

Again, we will not go through the tedious exercise of proving the rest of the basic laws of arithmetic, but it can be done with only induction and these definitions, if you are willing to work through all the cases.

**Recap:** The new number 0 is the **additive identity**, meaning that:

$$a + 0 = a$$

for all integers  $a$ . Negation takes an integer to its additive inverse, allowing us to define subtraction as addition of the additive inverse. Note that 1 is the **multiplicative identity**, meaning that  $a \times 1 = a$  for all integers  $a$ , but integer multiplicative inverses only exist for the integers 1 and  $-1$ .

The rational numbers can be thought of geometrically as slopes of lines:

$$\mathbb{Q} = \{(\text{slopes of}) \text{ lines that pass through } (0, 0) \text{ and a point } (b, a)\}$$

where  $a, b \in \mathbb{Z}$  and  $b \neq 0$  (so the line isn't vertical.)

The line  $L$  passing through  $(0, 0)$  and  $(b, a)$  has equation:

$$by = ax$$

and the slope is also the  $y$ -coordinate of the intersection of  $L$  with the (vertical) line  $x = 1$ . In particular, different lines through the origin have different slopes.

Many different points with integer coordinates will lie on the same line  $L$ ! If  $(b', a')$  is another point with integer coordinates, then by the equation above for the line  $L$ , we see that  $(b', a')$  is also on  $L$  exactly when:

$$ba' = ab'$$

**Definition:** An integer fraction is a symbol of the form:

$$\frac{a}{b}$$

where  $a, b \in \mathbb{Z}$  and  $b \neq 0$ . Two integer fractions are **equivalent**, written:

$$\frac{a}{b} \sim \frac{a'}{b'}$$

if  $(b, a)$  and  $(b', a')$  are on the same line through the origin.

**Note:** The symbol “ $\sim$ ” is called a **relation**, and it is easy to see that:

(i)  $\sim$  is **reflexive**, meaning that  $\frac{a}{b} \sim \frac{a}{b}$

(ii)  $\sim$  is **symmetric** meaning that if  $\frac{a}{b} \sim \frac{a'}{b'}$  then  $\frac{a'}{b'} \sim \frac{a}{b}$

(iii)  $\sim$  is **transitive** meaning that if  $\frac{a}{b} \sim \frac{a'}{b'}$  and  $\frac{a'}{b'} \sim \frac{a''}{b''}$  then  $\frac{a}{b} \sim \frac{a''}{b''}$

(A relation satisfying (i)-(iii) is called an **equivalence relation**.)

**Definition:** The **equivalence class**

$$\left[ \frac{a}{b} \right]$$

is the set of all fractions that are equivalent to  $\frac{a}{b}$ . Notice that:

$$\left[ \frac{a}{b} \right] = \left[ \frac{a'}{b'} \right]$$

whenever  $\frac{a}{b} \sim \frac{a'}{b'}$ , that is, whenever  $(b, a)$  and  $(b', a')$  are on the same line through the origin, or, as we noticed above, whenever  $ba' = ab'$ .

Thus we can reinterpret the rational numbers as:

$$\mathbb{Q} = \{\text{equivalence classes of integer fractions}\}$$

and this reinterpretation is very useful for seeing the arithmetic of  $\mathbb{Q}$ .

Before we do this, let's notice that the rational numbers are still ordered:

$$\left[\frac{a}{b}\right] < \left[\frac{c}{d}\right]$$

if the line through  $(0, 0)$  and  $(b, a)$  intersects the vertical line  $x = 1$  at a point that is **below** the intersection of the line through  $(0, 0)$  and  $(d, c)$ .

Unlike the integers, there is no such thing as the next rational number after a rational number  $[\frac{a}{b}]$ , so there is no way to use induction to define addition. Instead, we use the rule for adding fractions that we learned in gradeschool.

**Definition of Addition:** Given rational numbers  $[\frac{a}{b}]$  and  $[\frac{c}{d}]$ , then:

$$\left[\frac{a}{b}\right] + \left[\frac{c}{d}\right] = \left[\frac{ad + bc}{bd}\right]$$

(using the arithmetic of integers to define the numerator and denominator).

But we need to check something!

**Is addition is well-defined?** Here's the problem. If

$$\left[\frac{a}{b}\right] = \left[\frac{a'}{b'}\right] \text{ and } \left[\frac{c}{d}\right] = \left[\frac{c'}{d'}\right]$$

how do we know that:

$$\left[\frac{ad + bc}{bd}\right] = \left[\frac{a'd' + b'c'}{b'd'}\right] ?$$

This isn't obvious, and it needs to be checked, because if it weren't true, then this would be **bad** definition of addition, because it would only be an addition of integer fractions, and not of rational numbers, which are equivalence classes of integer fractions. This problem will arise whenever we try to make a definition involving equivalence classes of fractions (or other things). So beware!

**Proof that addition is well-defined:** Suppose:

$$\frac{a}{b} \sim \frac{a'}{b'} \text{ and } \frac{c}{d} \sim \frac{c'}{d'}$$

This means that  $ba' = ab'$  and  $dc' = cd'$ . But then:

$$\begin{aligned} (bd)(a'd' + b'c') &= (ba')(dd') + (c'd)(bb') \\ &= (ab')(dd') + (cd')(bb') = (ad + bc)(b'd') \end{aligned}$$

(substituting, and applying the laws of arithmetic for integers). So:

$$\frac{ad + bc}{bd} \sim \frac{a'd' + b'c'}{b'd'}$$

as desired.

Now that the definition is OK, it is very useful!

**Addition is associative. Proof:**

$$\left( \left[ \frac{a}{b} \right] + \left[ \frac{c}{d} \right] \right) + \left[ \frac{e}{f} \right] = \left[ \frac{ad + bc}{bd} \right] + \left[ \frac{e}{f} \right] = \left[ \frac{((ad)f + (bc)f) + (bd)e}{(bd)f} \right]$$

and

$$\left[ \frac{a}{b} \right] + \left( \left[ \frac{c}{d} \right] + \left[ \frac{e}{f} \right] \right) = \left[ \frac{a}{b} \right] + \left[ \frac{cf + de}{df} \right] = \left[ \frac{a(df) + (b(cf) + b(de))}{b(df)} \right]$$

and these are the same because of the associative laws for integer arithmetic!

Similarly, you can prove that addition is commutative.

**Definition of Multiplication:**

$$\left[ \frac{a}{b} \right] \left[ \frac{c}{d} \right] = \left[ \frac{ac}{bd} \right]$$

**Proof that multiplication is well-defined:** If  $\frac{a}{b} \sim \frac{a'}{b'}$  and  $\frac{c}{d} \sim \frac{c'}{d'}$ , then  $ba' = ab'$  and  $dc' = cd'$ , so  $(bd)(a'c') = (ba')(dc') = (ab')(cd') = (ac)(b'd')$ . But this gives us:

$$\frac{ac}{bd} \sim \frac{a'c'}{b'd'}$$

which is just what we needed to check.

It is now easy to prove the associative and commutative laws for the multiplication of rational numbers. To see that multiplication distributes with addition, though, we need an extra:

**Proposition 1.2.4.** *Suppose  $a = a'f$  and  $b = b'f$ , in which case we say that  $f$  is a **common factor** of both  $a$  and  $b$ . Then:*

$$\left[ \frac{a}{b} \right] = \left[ \frac{a'}{b'} \right]$$

(i.e. we can cancel common factors of the numerator and denominator.)

**Proof:** We need to show that  $\frac{a}{b} \sim \frac{a'}{b'}$ . But:

$$ab' = (a'f)b'$$

by substituting, and likewise,

$$ba' = (b'f)a'$$

so indeed the two fractions are equivalent.

**Multiplication distributes with addition. Proof:**

$$\left(\left[\frac{a}{b}\right] + \left[\frac{c}{d}\right]\right) \left[\frac{e}{f}\right] = \left[\frac{ad+bc}{bd}\right] \left[\frac{e}{f}\right] = \left[\frac{(ad)e + (bc)e}{(bd)f}\right] \text{ and}$$

$$\left[\frac{a}{b}\right] \left[\frac{e}{f}\right] + \left[\frac{c}{d}\right] \left[\frac{e}{f}\right] = \left[\frac{ae}{bf}\right] + \left[\frac{ce}{df}\right] = \left[\frac{(ae)(df) + (bf)(ce)}{(bf)(df)}\right]$$

There is a common factor of  $f$  in the numerator and denominator of the second fraction. Once we cancel it (Proposition 1.2.4), we see that the two rational numbers are the same!

Now for some extra goodies:

**The additive identity is the rational number:**

$$\left[\frac{0}{d}\right]$$

(and it doesn't matter what  $d$  is, as long as it isn't 0).

**Proof:**  $\frac{0}{d} \sim \frac{0'}{d'}$  since  $0 \times d' = 0 = 0 \times d$ , so all choices of denominator give the same rational number (namely the slope of the  $x$ -axis!). Next:

$$\left[\frac{a}{b}\right] + \left[\frac{0}{d}\right] = \left[\frac{ad}{bd}\right] = \left[\frac{a}{b}\right]$$

(using Proposition 1.2.4 again) proves that  $\left[\frac{0}{d}\right]$  is the additive identity.

**Notation:** Mathematicians always denote the additive identity by:

$$0$$

so we will, too.

**Every rational number has an additive inverse. Proof:**

$$\left[\frac{a}{b}\right] + \left[\frac{-a}{b}\right] = \left[\frac{ab + (-a)b}{b^2}\right] = \left[\frac{a + (-a)}{b}\right] = \left[\frac{0}{b}\right] = 0$$

using Proposition 1.2.4. So  $\left[\frac{-a}{b}\right]$  is an additive inverse to  $\left[\frac{a}{b}\right]$ .

As in Proposition 1.2.2, this is the **only** additive inverse!

**Definition of Subtraction:**

$$\left[\frac{a}{b}\right] - \left[\frac{c}{d}\right] = \left[\frac{a}{b}\right] + \left[\frac{-c}{d}\right]$$

As always, subtraction is addition of the additive inverse

**The multiplicative identity is the rational number:**

$$\left[\frac{d}{d}\right]$$

(and it doesn't matter what  $d$  is, as long as it isn't 0)

**Proof:**  $\frac{d}{d} \sim \frac{d'}{d'}$  since  $dd' = d'd$ . So it doesn't matter what  $d$  is, and:

$$\left[\frac{a}{b}\right] \left[\frac{d}{d}\right] = \left[\frac{ad}{bd}\right] = \left[\frac{a}{b}\right]$$

by Proposition 1.2.4. This is what we needed to prove. Again, it is easy to see that this is the **only** multiplicative identity.

**Notation:** Once again, we follow mathematical custom and write:

$$1$$

for the multiplicative identity.

**Every rational (except 0) has a multiplicative inverse. Proof:** Every rational number other than 0 is of the form  $\left[\frac{a}{b}\right]$  where  $a \neq 0$ . Then:

$$\left[\frac{a}{b}\right] \left[\frac{b}{a}\right] = \left[\frac{ab}{ba}\right] = 1$$

so  $\left[\frac{b}{a}\right]$  is the one and only multiplicative inverse (or **reciprocal**) of  $\left[\frac{a}{b}\right]$ .

**Definition of Division (by anything other than 0):**

$$\left[\frac{a}{b}\right] \div \left[\frac{c}{d}\right] = \left[\frac{a}{b}\right] \left[\frac{d}{c}\right]$$

(i.e. division is multiplication by the reciprocal)

Finally, I want to talk about one last definition:

**Definition of Lowest Terms:** An integer fraction (not rational number!)

$$\frac{a}{b}$$

is in lowest terms if  $b > 0$  and  $a$  and  $b$  have no common factors other than 1 and  $-1$  (which are common factors of all integers, hence “uninteresting!”).

**Proposition 1.2.5.** *Every rational number  $\left[\frac{a}{b}\right]$  contains exactly one fraction in lowest terms (in the equivalence class).*

**Idea of Proof:** Start with the fraction  $\frac{a}{b}$ , which may not be in lowest terms. By cancelling out all the (interesting) common factors of  $a$  and  $b$  and also  $-1$  if necessary (to make  $b > 0$ ) we arrive at a fraction in lowest terms. This shows that there is **at least** one fraction in lowest terms in the equivalence class  $\left[\frac{a}{b}\right]$ . To see that there cannot be more than one, we will need to know a bit more about prime numbers, which we will work out later in the course (§2.2).

This allows us to redefine one more time:

$$\mathbb{Q} = \{\text{integer fractions } \frac{a}{b} \text{ that are in lowest terms}\}$$

In particular, we get an inclusion of sets:

$$\mathbb{Z} \subset \mathbb{Q}$$

by identifying each integer  $a$  with the fraction  $\frac{a}{1}$ , which is clearly in lowest terms. When we do this, we see something very important. Namely:

$$\left[\frac{a}{1}\right] + \left[\frac{b}{1}\right] = \left[\frac{a+b}{1}\right] \quad \text{and} \quad \left[\frac{a}{1}\right] \left[\frac{b}{1}\right] = \left[\frac{ab}{1}\right]$$

so addition and multiplication are the same regardless of whether we view  $a$  and  $b$  as integers, or as rational numbers!

Finally, as in §1.1, we finish with another gem from ancient Greece:

**Theorem (Pythagoras):** There is no square root of 2 in  $\mathbb{Q}$ .

**Proof:** If there were a rational number square root of 2, then:

$$\left[\frac{a}{b}\right]^2 = \left[\frac{a^2}{b^2}\right] = \left[\frac{2}{1}\right]$$

would tell us that:

$$2b^2 = a^2$$

so that 2 divides  $a^2$ . But then it would follow that **2 divides a** since the square of an odd number is odd. Thus  $a = 2c$  for some  $c$ , and then:

$$2b^2 = (2c)^2 = 4c^2 \quad \text{so} \quad b^2 = 2c^2$$

But then 2 divides  $b^2$  so it would follow as above that **2 divides b**. In other words, 2 would be an interesting common factor of  $a$  and  $b$ . All this would be true no matter what fraction  $a/b$  we chose to represent the rational square root of 2. In other words, **there would be no way to put such a rational number in lowest terms!** This contradicts Proposition 1.2.5, so there cannot be such a rational number.

**Recap:** Rational numbers are equivalence classes of integer fractions, and they have a very satisfactory arithmetic, with additive inverses and multiplicative inverses (of everything except 0) allowing us to define subtraction and exact division (by anything except 0). On the other hand, from the point of view of geometry, they are less satisfactory, since a perfectly reasonable length ( $\sqrt{2}$ ) cannot be represented by a rational number.

### 1.2.1 Integer and Rational Number Exercises

In the first three exercises, we consider arithmetic in an abstract setting. The idea is that many of the results of this section are not special properties of the integers or rational numbers, but rather follow from the laws of arithmetic themselves.

**2-1** Suppose  $S$  is a set and  $+$  is an addition rule for elements of  $S$  that satisfies:

- the associative law:  $(s + t) + u = s + (t + u)$  for all  $s, t, u \in S$ , and
- the commutative law:  $s + t = t + s$  for all  $s, t \in S$ .

(a) Prove that there is at most one additive identity element in  $S$ . That is, prove there is at most one element  $z \in S$  such that:

$$s + z = s \text{ for all } s \in S$$

(Mathematicians tell us to rename this element 0)

Hint: If  $y$  is another additive identity, think about  $y + z$  in two ways.

(b) Assuming that there is an additive identity element (renamed 0), prove that each  $s \in S$  has at most one additive inverse in  $S$ . That is, prove that there is at most one element  $t \in S$  so that:

$$s + t = 0$$

(Mathematicians tell us to rename this element  $-s$ )

(c) Prove that if  $s$  has an additive inverse  $-s$ , then the additive inverse of  $-s$  is  $s$ . That is, prove:  $-(-s) = s$

**Definition:** A set  $S$  with an addition rule  $+$  with a 0 and additive inverses of everything is an **Abelian group**.

**2-2** If  $S$  is an Abelian group with a multiplication rule  $\times$  satisfying:

- the associative law:  $(s \times t) \times u = s \times (t \times u)$  and
- the two-sided distributive law with addition:

$$(s + t) \times u = s \times u + t \times u \text{ and } u \times (s + t) = u \times s + u \times t$$

(we will not, for now, assume that multiplication is commutative!)

- (a) Prove that  $s \times 0 = 0$  and  $0 \times s = 0$  for all  $s \in S$ .

Hint: Consider  $s \times (0 + 0)$  and  $(0 + 0) \times s$ .

- (b) Prove that for all  $s, t \in S$

$$s \times (-t) = -(s \times t) \text{ and } -(s \times t) = (-s) \times t$$

Hint: Consider  $s \times (t + (-t))$  and  $(s + (-s)) \times t$ .

- (c) Prove that  $(-s) \times (-t) = s \times t$  for all  $s, t \in S$ .

**Definition:** An Abelian group  $S$  with an associative and two-sided distributive multiplication rule is called a **ring**.

**Examples:**  $\mathbb{Z}$  and  $\mathbb{Q}$  are rings with a commutative multiplication rule. The  $n \times n$  matrices (for  $n > 1$ ) with entries in  $\mathbb{Z}$  or  $\mathbb{Q}$  (or any ring) are themselves a ring with a non-commutative matrix multiplication!

**2-3** Suppose  $S$  is a ring with a commutative multiplication rule.

- (a) Prove that there is at most one multiplicative identity in  $S$ .

(Mathematicians tell us to rename this 1)

- (b) Prove that each element  $s \in S$  has at most one multiplicative inverse (reciprocal) element  $t \in S$ .

(Mathematicians tell us to rename this  $1/s$ .)

- (c) Prove that 0 does not have a multiplicative inverse (unless  $0 = 1$ ). Discuss what the ring would look like if  $0 = 1$ .

- (d) If  $s$  has a multiplicative inverse, prove that:

$$\frac{1}{1/s} = s$$

Hint: Exercise 2.3 is very similar to Exercise 2.1.

**Definition:** A ring  $S$  with a commutative multiplication and a multiplicative identity  $1 \in S$ , such that every element of  $S$  (except 0) has a multiplicative inverse is called a **field**.

**Our Only Example of a Field (so far):**  $\mathbb{Q}$  is a field.

**2-4** Prove the following:

- (a) If  $a, b \in \mathbb{Z}$  and  $ab = 0$ , then either  $a = 0$  or  $b = 0$  (or both).

Hint: If  $a$  and  $b$  are both natural numbers, then  $ab \neq 0$  because it is a natural number! What are the other possibilities for  $a$  and  $b$ ?

- (b) If  $a, b, c \in \mathbb{Z}$  and  $ab = cb$  and  $b \neq 0$ , then  $a = c$ .

Hint: Find a way to use (a).

**2-5** Recall that:

$$\frac{a}{b} \sim \frac{a'}{b'} \text{ exactly when } ba' = ba'$$

We'll check “algebraically” that this really is an equivalence relation.

(i) Reflexive. This is the commutative law for multiplication!

$$\frac{a}{b} \sim \frac{a}{b} \text{ because } ba = ab$$

(ii) Symmetric. This is also the commutative law for multiplication.

$$\text{If } \frac{a}{b} \sim \frac{a'}{b'} \text{ then } ba' = ab' \text{ but then } b'a = a'b \text{ so } \frac{a'}{b'} \sim \frac{a}{b}$$

(iii) Transitive. This is your exercise! You need to explain why

$$ba' = ab' \text{ and } b'a'' = a'b'' \text{ together imply that } ba'' = ab''$$

**2-6** Consider the two rational numbers:

$$\left[ \frac{1}{2} \right] = \left[ \frac{2}{4} \right] \text{ and } \left[ \frac{1}{3} \right]$$

Explain carefully why the fact that  $\left[ \frac{2}{5} \right] \neq \left[ \frac{3}{7} \right]$  shows that “dumb” addition:

$$\left[ \frac{a}{b} \right] \oplus \left[ \frac{c}{d} \right] = \left[ \frac{a+c}{b+d} \right]$$

is not well-defined on rational numbers.

**2-7** Prove **Pascal's identity**. For natural numbers  $m < n$ ,

$$\frac{n!}{m!(n-m)!} + \frac{n!}{(m-1)!(n-m+1)!} = \frac{(n+1)!}{m!(n-m+1)!}$$

**Remark (for your enjoyment):** This proves that the “binomial coefficient:”

$$\binom{n}{m} = \frac{n!}{m!(n-m)!}$$

is the  $m + 1$ st number in the  $n + 1$ st row of **Pascal's Triangle**:

$$\begin{array}{c} 1 \\ 1 \ 1 \\ 1 \ 2 \ 1 \\ 1 \ 3 \ 3 \ 1 \\ \vdots \end{array}$$

**2-8** The ancient Egyptians had some ideas about fractions, though they apparently didn't like to subtract, didn't like numerators, and didn't like repetitions. The "Egyptian fraction" expansion of a rational number between 0 and 1 is a sum of distinct fractions, all of the form:

$$\frac{1}{n}$$

Here are some examples (I'm going to drop the cumbersome brackets around rational numbers in this problem and from now on!):

$$\frac{5}{6} = \frac{1}{2} + \frac{1}{3}, \quad \frac{2}{3} = \frac{1}{2} + \frac{1}{6}$$

( $\frac{2}{3} = \frac{1}{3} + \frac{1}{3}$  is not an Egyptian fraction expansion because the  $\frac{1}{3}$  repeats)

$$\frac{5}{12} = \frac{1}{3} + \frac{1}{12} = \frac{1}{4} + \frac{1}{6}$$

(so sometimes there is more than one possible expansion).

(a) Find Egyptian fraction expansions for the numbers:

$$\frac{5}{7}, \frac{11}{27}, \frac{19}{49}, \frac{5}{61}$$

(b) Devise a strategy for finding an Egyptian fraction for any  $m/n$  (assuming that  $m < n$ ). Hint: You might find induction useful. Apply your strategy to the four numbers above (your calculator will not give you enough accuracy for the last two...you will need a computer!).

### 1.3 The Real Numbers.

The real numbers:

$$\mathbb{R} = \{\text{numbers on the number-line}\}$$

require some real analysis for a “proper” definition. We’ll sidestep the analysis, relying instead on our less precise notions of continuity from calculus. Notice that the real numbers are ordered (from left to right) and come in three types:

$$\mathbb{R} = \mathbb{R}^- \cup \{0\} \cup \mathbb{R}^+$$

where

$$\mathbb{R}^+ = \{\text{positive real numbers}\}$$

are the real numbers that measure lengths (just as the natural numbers count). Notice also that rational numbers are examples of real numbers. We didn’t define the rational numbers to be numbers on the number-line, but since the slope of a line through  $(0, 0)$  and  $(b, a)$  is the  $y$ -coordinate of its intersection with the vertical line  $x = 1$ , we may think about our number-line in that way (as the vertical line  $x = 1$ ), and then

$$\mathbb{Q} \subset \mathbb{R} = \{\text{slopes of all lines through } (0, 0) \text{ (except the } y\text{-axis)}\}$$

We want to see that the real numbers are a field (see 1.1.2) and that “most” of the real numbers are not rational (remember  $\sqrt{2}$ ). In fact, we will be able to find plenty of irrational numbers using:

**Decimals:** An **infinite decimal** is a sequence of the following form:

$$q.d_1d_2d_3\cdots$$

where  $q$  is a whole number (a natural number or zero), and each  $d_i$  is a digit (whole number between 0 and 9). All the decimals we will use will be infinite. A **terminating decimal** is a decimal

$$q.d_1d_2\cdots d_n$$

which we will make infinite by padding it with zeroes:

$$q.d_1d_2\cdots d_n00\cdots$$

A terminating decimal always represents a rational number:

$$q.d_1d_2\cdots d_n00\cdots = q + \frac{d_1}{10} + \frac{d_2}{10^2} + \cdots + \frac{d_n}{10^n}$$

(Remember, we no longer use the brackets when writing rational numbers!)

A non-terminating decimal represents a real number in the same way, except that we need the notion of **convergence** from calculus to make sense of the infinite sum:

$$q + \frac{d_1}{10} + \frac{d_2}{10^2} + \frac{d_3}{10^3} + \cdots$$

Conversely, every (positive) real number has a decimal expansion.

**Definition of Decimal Expansions:** Given a positive real number  $r \in \mathbb{R}^+$ , the (infinite) decimal expansion of  $r$  is defined as follows:

$q$  is chosen so that  $q \leq r < q + 1$ . The digits are then chosen by induction:

(i)  $d_1$  is chosen so that:

$$q + \frac{d_1}{10} \leq r < q + \frac{d_1}{10} + \frac{1}{10}$$

It is between 0 and 9 because  $q \leq r < q + 1$ .

(ii) Each  $d_{n+1}$  is chosen so that:

$$q + \frac{d_1}{10} + \cdots + \frac{d_{n+1}}{10^{n+1}} \leq r < q + \frac{d_1}{10} + \cdots + \frac{d_{n+1}}{10^{n+1}} + \frac{1}{10^{n+1}}$$

It is between 0 and 9 because:

$$q + \frac{d_1}{10} + \cdots + \frac{d_n}{10^n} \leq r < q + \frac{d_1}{10} + \cdots + \frac{d_n}{10^n} + \frac{1}{10^n}$$

This gives a **sequence** of terminating decimals (= rational numbers):

$$q, q.d_1, q.d_1d_2, q.d_1d_2d_3, \text{ etc.}$$

that converges to  $r$ . Thus,  $r = q.d_1d_2d_3 \cdots$ .

**Examples:** (a) The natural number  $m$  expands as the terminating decimal:

$$m.000000 \cdots$$

The infinite decimal:

$$(m - 1).99999 \cdots$$

also represents  $m$ , but you will never get it as the decimal expansion. All the terminating decimals (and only the terminating decimals) have this ambiguity.

(b) The decimal expansion of  $1/3$  is  $0.33333 \cdots$  because

$$0.333 \cdots 3 < \frac{1}{3} < 0.333 \cdots 4$$

no matter how many digits we take (multiply through by 3 to see this).

(c) We can decimal expand  $\sqrt{2}$  as far as we want by squaring:

$$1^2 = 1 < 2 < 4 = 2^2, \text{ so } 1 < \sqrt{2} < 2 \text{ so } q = 1.$$

$$(1.4)^2 = 1.96 < 2 < 2.25 = (1.5)^2, \text{ so } d_1 = 4.$$

$$(1.41)^2 = 1.9881 < 2 < 2.0164 = (1.42)^2, \text{ so } d_2 = 1.$$

$$(1.414)^2 = 1.999396 < 2 < 2.002225 = (1.415)^2, \text{ so } d_3 = 4.$$

**Remark:** You will frequently see:  $\sqrt{2} = 1.414\dots$ . Unlike the decimal  $0.333\dots$  above, this use of “ $\dots$ ” means only that 1.414 are the first three digits of the infinite decimal expansion of  $\sqrt{2}$ . It does **not** mean that there is a pattern!

**Expanding Rationals.** Given a positive rational number  $\frac{l}{m}$ , perform the following divisions with remainders to define the digits of a decimal:

First, set  $l = mq + r$  (this defines  $q$  and a whole number  $r < m$ )

Next, define the digits by induction:

(i) Set  $10r = md_1 + r_1$  (this defines  $d_1$ , which is a digit, and  $r_1 < m$ )

(ii) Set each  $10r_n = md_{n+1} + r_{n+1}$   
(this defines  $d_{n+1}$ , which is a digit, as well as  $r_{n+1} < m$ )

and this defines digits  $d_n$  (and remainders  $r_n < m$ ) for all  $n$  by induction.

This looks sort of like Euclid’s algorithm, except this one never ends. But if  $r_n = 0$  for some  $n$ , then  $0 = d_{n+1} = d_{n+2} = \dots$  and the decimal terminates.

You should convince yourself that this algorithm for expanding rationals is exactly how you were taught to find the decimal of a rational number as the “long division” of  $l$  by  $m$ . But now we are in a position to prove that this expansion gives the **correct** decimal expansion of  $\frac{l}{m}$ !

**Proposition 1.3.1.** *The infinite decimal in the rational expansion of  $\frac{l}{m}$  is equal to its decimal expansion.*

**Proof:** To get started, divide  $l = mq + r$  by  $m$  to get:

$$(*) \quad \frac{l}{m} = q + \frac{r}{m} \quad \text{and then} \quad q \leq \frac{l}{m} < q + 1 \quad (\text{because } 0 \leq \frac{r}{m} < 1)$$

so this is the correct  $q$ . Next, a proof by induction checks the decimals:

(i) Divide  $10r = md_1 + r_1$  by  $10m$  to get  $\frac{r}{m} = \frac{d_1}{10} + \frac{r_1}{10m}$ , and substitute into (\*) to get:

$$\frac{l}{m} = q + \frac{d_1}{10} + \frac{r_1}{10m}$$

which proves that  $d_1$  is the correct digit (because  $0 \leq \frac{r_1}{m} < 1$ )!

(ii) Once we know that  $d_1, \dots, d_n$  are the correct first  $n$  digits, and in fact that:

$$(**) \quad \frac{l}{m} = q.d_1d_2\dots d_n + \frac{r_n}{10^n m}$$

then divide  $10r_n = md_{n+1} + r_{n+1}$  by  $10^{n+1}m$  to get  $\frac{r_n}{10^n m} = \frac{d_{n+1}}{10^{n+1}} + \frac{r_{n+1}}{10^{n+1}m}$ , and substitute into (\*\*) to get:

$$\frac{l}{m} = q.d_1d_2\dots d_n + \frac{d_{n+1}}{10^{n+1}} + \frac{r_{n+1}}{10^{n+1}m} = q.d_1d_2\dots d_{n+1} + \frac{r_{n+1}}{10^{n+1}m}$$

This proves that  $d_{n+1}$  is also correct, and completes the proof by induction.

**Definition:** A **repeating decimal** is any decimal of the form:

$$q.d_1d_2\cdots d_kd_{k+1}\cdots d_nd_{k+1}\cdots d_nd_{k+1}\cdots d_n\cdots$$

for some pair of natural numbers  $k < n$ . We write this as:

$$q.d_1d_2\cdots \overline{d_kd_{k+1}\cdots d_n}$$

to avoid the “ $\cdots$ ” ambiguity remarked upon earlier.

**Example:** Your calculator’s output for  $1/35$  will convince you that:

$$\frac{1}{35} = 0.0\overline{285714} \quad (k = 1, n = 7)$$

We will prove this as we prove the following:

**Proposition 1.3.2.** *All the decimal expansions of rational numbers repeat.*

**Proof:** Consider again step (ii) in the rational expansion of  $l/m$  above:

$$(ii) \quad 10r_n = md_{n+1} + r_{n+1}$$

From this step, it follows that if  $r_k = r_n$  for some  $k < n$ , then:

$$d_{k+1} = d_{n+1} \text{ and } r_{k+1} = r_{n+1}$$

because they are the quotients and remainders when the **same** numbers  $10r_k = 10r_n$  are divided by  $m$  (with remainders). But since  $r_{k+1} = r_{n+1}$  it will then follow that

$$d_{k+2} = d_{n+2} \text{ and } r_{k+2} = r_{n+2}$$

and so on (this could be proved by induction, but I think it is clear). Thus when the remainder repeats for the first time, the decimal repeats! How do we know that the remainders eventually repeat? *Because all remainders are between 0 and  $m - 1$ .* So by the time we have done  $m$  divisions with remainders, we must have come across a repeat of the remainders!!

**Example:** The expansion of  $1/35$  really does repeat as indicated above.

$$1 = 35(0) + 1 \quad (q = 0 \text{ and } r = 1) \text{ Decimal so far: } 0$$

$$10(1) = 35(0) + 10 \quad (d_1 = 0 \text{ and } r_1 = 10) \text{ Decimal so far: } 0.0$$

$$10(10) = 35(2) + 30 \quad (d_2 = 2 \text{ and } r_2 = 30) \text{ Decimal so far: } 0.02$$

$$10(30) = 35(8) + 20 \quad (d_3 = 8 \text{ and } r_3 = 20) \text{ Decimal so far: } 0.028$$

$$10(20) = 35(5) + 25 \quad (d_4 = 5 \text{ and } r_4 = 25) \text{ Decimal so far: } 0.0285$$

$$10(25) = 35(7) + 5 \quad (d_5 = 7 \text{ and } r_5 = 5) \text{ Decimal so far: } 0.02857$$

$$10(5) = 35(1) + 15 \quad (d_6 = 1 \text{ and } r_6 = 15) \text{ Decimal so far: } 0.028571$$

$$10(15) = 35(4) + 10 \quad (d_7 = 4 \text{ and } r_7 = 10 = r_1. \text{ Repeat!}) \text{ Decimal: } 0.0\overline{285714}.$$

**Remarks:** The proposition is again telling us something we've already learned. On the other hand, now we've proved it! Also notice that the proposition tells us that any non-repeating decimal gives a real number which is not rational. My personal favorite has a simple pattern, but not a repeating one:

$$1.01001000100001000001\dots$$

There are “many more” non-repeating decimals than repeating ones! This may seem a strange statement to make since there are infinitely many of both. One good way to think about this is that if a decimal could be chosen at random, then the chances of it repeating are less than the chances of winning the biggest lottery you could imagine!

**Addition:** We could try to define the addition of real numbers as an addition of infinite decimals, but this would be messy, as such an addition will typically involve infinitely many “carries.” Instead, we'll define addition geometrically, via translations.

If  $r$  is a real number (possibly negative or 0), then **translation by  $r$**  is the slide of the number-line that is required to move 0 to  $r$ . Thus, for instance, translation by 1 slides the number-line one unit to the right, and translation by  $-1$  slides it one unit to the left.

**Translation definition of addition:** If  $s$  is a real number, then  $s + r$  is the resting place of  $s$  after translating it by  $r$ .

This sounds fancy, but I claim that it does the same thing as our earlier definitions of addition for integers. Why? Because the “next” integer after  $a$  is the translation of  $a$  by 1 unit to the right, and the “previous” integer before  $a$  is the translation of  $a$  by 1 unit to the left, while translating by 0 does nothing (induction takes care of the rest). It takes a bit more work to see:

**Proposition 1.3.3.** *The translation definition of addition does the same thing to rational numbers as the earlier definition.*

**Proof:** First of all, notice that the line of slope  $\frac{1}{n}$  meets the line  $x = 1$  at a point whose  $y$ -coordinate is “one  $n$ th of the way to 1.” That is, it takes  $n$  of the translations by  $\frac{1}{n}$  to move 0 to 1. This is seen by considering the triangle with vertices  $(0, 0)$ ,  $(n, 0)$ ,  $(n, 1)$  and the similar triangle cut out by the line  $x = 1$ . Since it takes  $n$  (horizontal) translations by 1 to move from 0 to  $n$ , similar triangles tell us that the same is true of the vertical translations. We will refer to  $\frac{1}{n}$  as a “fractional unit.”

The sum of two rational numbers was:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

and we can assume that the fractions are in lowest terms, so  $b > 0$  and  $d > 0$ . We can then put the fractions over a **common denominator**:

$$\frac{a}{b} = \frac{ad}{bd} \quad \text{and} \quad \frac{c}{d} = \frac{bc}{bd}$$

using Proposition 1.2.4. Now, translation by  $\frac{c}{d}$  is translation by  $c$  of the fractional units  $\frac{1}{d}$ , which is also translation by  $bc$  of the fractional units  $\frac{1}{bd}$ , and likewise for  $\frac{a}{b}$ . Thus, addition of these rational numbers is translation of 0 by  $ad+bc$  of the fractional units  $\frac{1}{bd}$ , which agrees with the addition definition above for rationals.

**Laws of Addition:** One could prove these with Euclidean geometry, but I would rather remind you that calculus does the job. The necessary ingredients are:

- (a) The translation definition of addition is **continuous** and
- (b) Every real number is a limit of rational numbers

because with these two ingredients, we can use the laws for addition of rational numbers to deduce the laws for the addition of real numbers. For example, real numbers  $r, s, t$  are limits of rational numbers:

$$r = \lim_{n \rightarrow \infty} \left\{ \frac{a_n}{b_n} \right\}, s = \lim_{n \rightarrow \infty} \left\{ \frac{c_n}{d_n} \right\}, t = \lim_{n \rightarrow \infty} \left\{ \frac{e_n}{f_n} \right\}$$

and because addition is continuous, we can pull out limits(!)

$$\begin{aligned} (r + s) + t &= \left( \lim_{n \rightarrow \infty} \left\{ \frac{a_n}{b_n} \right\} + \lim_{n \rightarrow \infty} \left\{ \frac{c_n}{d_n} \right\} \right) + \lim_{n \rightarrow \infty} \left\{ \frac{e_n}{f_n} \right\} \\ &= \lim_{n \rightarrow \infty} \left\{ \left( \frac{a_n}{b_n} + \frac{c_n}{d_n} \right) + \frac{e_n}{f_n} \right\} \end{aligned}$$

and because addition is associative for rationals we can substitute:

$$\left( \frac{a_n}{b_n} + \frac{c_n}{d_n} \right) + \frac{e_n}{f_n} = \frac{a_n}{b_n} + \left( \frac{c_n}{d_n} + \frac{e_n}{f_n} \right)$$

for each  $n$ , and plug back into the limits to get:

$$(r + s) + t = r + (s + t)$$

From the point of view of translations, it is obvious that:

**0 is the additive identity** and we can get mileage out of the:

**Negation Transformation:** This is defined the same way as before!

$$- : \mathbb{R} \rightarrow \mathbb{R}$$

takes a translation to the equal translation in the opposite direction. From this it is clear that  $-r$  is the additive inverse of  $r$ , and arguing as in Proposition 1.2.3, we conclude that the negation transformation is a linear transformation:  $-(r + s) = -r + (-s)$ .

**Subtraction** is defined as usual, to be addition of the additive inverse.

**Area definition of multiplication:** For positive reals  $r$  and  $s$ , define:

$rs$  is the **area** of the  $r \times s$  rectangle

and then  $r(-s) = -(rs)$ ,  $(-r)s = -(rs)$ ,  $(-r)(-s) = rs$  and  $r \cdot 0 = 0 = 0 \cdot r$ .

Again, I am appealing to your geometric intuition of the meaning of area. It can be carefully defined using limits and calculus, if you prefer.

**Proposition 1.3.4.** *The area definition for real numbers does the same thing to **rational numbers** as the earlier definition.*

**Proof:** Because the definitions incorporate negatives in the same way, it is enough to see that the definitions are the same for positive rational numbers. Of course, the area of an  $m \times 1$  rectangle is  $m$ . The area of an  $m \times (n+1)$  rectangle is  $m$  more than the area of an  $m \times n$  rectangle because an  $m \times (n+1)$  rectangle is the union of  $m \times n$  and  $m \times 1$  rectangles! Thus the area definition agrees with the earlier definition for natural numbers.

As for positive rational numbers, it again comes down to the fact that  $n$  of the fractional  $\frac{1}{n}$  units are equal to 1 unit. From this it follows that  $mn$  of the  $\frac{1}{m} \times \frac{1}{n}$  squares exactly fill a  $1 \times 1$  square, so  $\frac{1}{mn} = \frac{1}{m} \times \frac{1}{n}$  in both definitions, and again we see that  $\frac{k}{m} \times \frac{l}{n}$  is  $kl$  of the fractional squares  $\frac{1}{mn}$ , so it has the appropriate area  $\frac{kl}{mn}$ .

The rest of the laws of arithmetic have a very pretty geometric interpretation:

**The Distributive Law:**

$$r(s+t) = rs + rt$$

because an  $r \times (s+t)$  rectangle is a union of  $r \times s$  and  $r \times t$  rectangles.

**The Commutative Law:**

$$rs = sr$$

because an  $r \times s$  rectangle has the same area as an  $s \times r$  rectangle.

**The Associative Law:**

$$r(st) = (rs)t$$

because both are the **volumes** of an  $r \times s \times t$  **box**.

**1 is the multiplicative identity.** The area of an  $r \times 1$  rectangle is  $r$ .

We finally want to prove that every real number except 0 has a multiplicative inverse. This can be done either using calculus or using geometry. For the calculus approach, let  $r$  be a positive real number. Then the function:

$$f(x) = rx$$

is continuous (in fact, differentiable with derivative  $f'(x) = r$ ). Since  $f(0) = 0$  and  $\lim_{x \rightarrow +\infty} f(x) = +\infty$ , the **intermediate value theorem** tells us that there must be some positive real number  $s$  so that  $f(s) = 1$ . In other words,  $rs = 1$  so  $s = 1/r$ . And then, of course,  $-s$  is the multiplicative inverse of  $-r$ .

The calculus proof only says that the inverse exists, not how to find it. For a geometric construction of the multiplicative inverse, let  $L$  be the line through  $(0, 0)$  and  $(r, 1)$ . This has slope  $1/r$  (unless  $r = 0$ , in which case it is vertical!). In particular, the intersection of  $L$  with the vertical line  $x = 1$  is the point  $(1, 1/r)$ . That is, by drawing  $L$  and intersecting with  $x = 1$ , we have constructed the multiplicative inverse. This is more satisfying than just proving that it exists!

**So  $\mathbb{R}$  is a field.**

As we said earlier, addition and multiplication of decimals is messy. There are, however, a couple of useful exceptions to this.

**Multiplying by powers of 10:** If  $r = q.d_1d_2d_3 \dots$ , then:

$$10r = (10q + d_1).d_2d_3d_4 \dots$$

$$100r = (100q + 10d_1 + d_2).d_3d_4d_5 \dots$$

etc.

That is, multiplying by powers of 10 shifts the decimal point.

**Subtracting “matching” digits:** Suppose  $r$  and  $s$  are real numbers with matching digits. That is, suppose:

$r$  has decimal expansion  $q.d_1d_2d_3 \dots$  and

$s$  has decimal expansion  $p.d_1d_2d_3 \dots$

Then

$$r - s = q - p$$

That is, if the decimals all match, then the difference is an integer.

In Proposition 1.3.2, we proved that every rational number expands as a repeating decimal. Here we prove the *converse* statement.

**Proposition 1.3.5.** *Every repeating decimal is the decimal expansion of some rational number.*

**Proof:** Start with a repeating decimal  $r = q.d_1d_2 \dots d_k \overline{d_{k+1} \dots d_n}$ . Then:

$$10^k r = (10^k q + 10^{k-1} d_1 + \dots + d_k) \overline{d_{k+1} \dots d_n}$$

and

$$10^n r = (10^n q + 10^{n-1} d_1 + \dots + d_n) \overline{d_{k+1} \dots d_n}$$

and these are matching decimals, so we can subtract them to get:

$$10^n r - 10^k r = (10^n q + \dots + d_n) - (10^k q + \dots + d_k)$$

and dividing both sides by  $10^n - 10^k$ , we see that  $r$  is rational:

$$r = \frac{(10^n q + \dots + d_n) - (10^k q + \dots + d_k)}{10^n - 10^k}$$

**Example:** To find the rational number that expands to:

$$1.11\overline{12}$$

we take:

$$\frac{11112 - 111}{10^4 - 10^2} = \frac{11001}{9900} = \frac{3667}{3300}$$

Finally, from the irrationality of  $\sqrt{2}$  (see §1.2) we get an interesting:

**Corollary:** The decimal expansion of  $\sqrt{2}$  doesn't repeat!

### 1.3.1 Real Number Exercises

**3-1** (a) Find the first 5 decimals in the expansion of  $\sqrt{3}$  by squaring.

(b) Find the first 5 decimals in the expansion of  $\sqrt[3]{2}$  by cubing.

**3-2** Find the decimal expansions for each of the following:

(a)  $\frac{1}{13}$  (b)  $\frac{2}{13}$  (c)  $\frac{3}{13}$  (d)  $\frac{4}{13}$  (e)  $\frac{5}{13}$  (f)  $\frac{6}{13}$  (g)  $\frac{7}{13}$

Do you see a pattern?

**3-3** Convert each repeating decimal to a fraction in lowest terms.

(a)  $0.\overline{27}$  (b)  $0.0\overline{27}$  (c)  $0.2\overline{27}$  (d)  $0.\overline{027}$  (e)  $0.\overline{037}$

**3-4** Which rational numbers correspond to terminating decimals?

Infinite decimals are not the “most efficient” way to express a positive real number as a limit of rational numbers. The **continued fraction** expansion actually works much better.

**Continued Fraction Expansion:** Given a positive real number  $r$ , define its *continued fraction* by induction:

(i)  $q_1$  is chosen so that  $q_1 \leq r < q_1 + 1$  ( $q_1$  is the **integer part** of  $r$ ) and

$$s_1 = r - q_1 \quad (s_1 \text{ is the } \mathbf{fractional part} \text{ of } r, \text{ with } 0 \leq s_1 < 1).$$

(ii) Once  $s_n$  is defined, then if  $s_n = 0$ , STOP! Otherwise,

$q_{n+1}$  is defined to be the integer part of  $1/s_n$  and:

$s_{n+1}$  is defined to be the fractional part of  $1/s_n$ .

This gives a sequence of rational numbers converging to  $r$ :

$$q_1, \quad q_1 + \frac{1}{q_2}, \quad q_1 + \frac{1}{q_2 + \frac{1}{q_3}}, \quad q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \frac{1}{q_4}}}, \dots$$

**Example:** Expand  $25/17 = 1.\overline{4705882352941176}$  as a continued fraction.

$$q_1 = 1 \text{ and } s_1 = 8/17 \text{ (so } 1/s_1 = 17/8\text{),}$$

$$q_2 = 2 \text{ and } s_2 = 1/8 \text{ (so } 1/s_2 = 8\text{),}$$

$q_3 = 8$  and  $s_3 = 0$ . STOP! This gives the sequence:

$$1, 1 + \frac{1}{2} = \frac{3}{2}, 1 + \frac{1}{2 + \frac{1}{8}} = \frac{25}{17}$$

Continued fraction expansions of rational numbers always terminate. (Why?)

**3-5** Expand each of the following as continued fractions and write the sequences (as in the example above):

$$(a) \frac{56}{55} \quad (b) \frac{57}{55} \quad (c) \frac{59}{55} \quad (d) \frac{89}{55}$$

**Another Example:** Expand  $\sqrt{2} = 1.414\dots$  as a continued fraction.

$$q_1 = 1 \text{ and } s_1 = \sqrt{2} - 1$$

Next step. Simplify:

$$\frac{1}{s_1} = \frac{1}{\sqrt{2} - 1} = \frac{\sqrt{2} + 1}{(\sqrt{2} - 1)(\sqrt{2} + 1)} = \frac{\sqrt{2} + 1}{2 - 1} = \sqrt{2} + 1 = 2.414\dots$$

$$q_2 = 2 \text{ and } s_2 = \sqrt{2} + 1 - 2 = \sqrt{2} - 1 \text{ (same as } s_1\text{)}$$

$$q_3 = 2 \text{ and } s_3 = \sqrt{2} - 1 \text{ (same as } q_2 \text{ and } s_2\text{)}$$

so  $2 = q_2 = q_3 = q_4 = \dots$ , giving the sequence:

$$1, 1 + \frac{1}{2} = \frac{3}{2}, 1 + \frac{1}{2 + \frac{1}{2}} = \frac{7}{5}, 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2}}} = \frac{17}{12}, \dots$$

In particular, the continued fraction for  $\sqrt{2}$  doesn't terminate (this is another proof that  $\sqrt{2}$  isn't rational!). But the  $q$ 's do repeat. In fact, continued fraction expansions of solutions to the quadratic formula:

$$\frac{-b + \sqrt{b^2 - 4ac}}{2a} \text{ with } a, b, c \in \mathbb{Z}$$

(see §2.3) always repeat. (Why?)

**3-6** Expand the following two numbers as continued fractions, indicating where the repeat in the  $q$ 's occurs, and write out the first four terms of the sequence, as in the example.

$$(a) \sqrt{3} \quad (b) \text{ the golden mean: } \frac{1+\sqrt{5}}{2}$$

Hint: The golden mean satisfies the cool property:

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

**3-7** Calculator exercise. Use a calculator to find the first 5 values  $q_1, q_2, \dots, q_5$  in the continued fraction expansion of  $\pi$  and then find the rational number:

$$q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \frac{1}{q_4 + \frac{1}{q_5}}}}$$

which is an excellent (much better than 3.14159) approximation of  $\pi$ .

## 1.4 The Complex Numbers.

We start with an important property of the real numbers.

**Proposition 1.4.1.** *Every positive real number  $r$  has a single positive  $n$ th root for each natural number  $n$ . In other words, the equations*

$$x^n = r$$

*each have exactly one positive real solution, which is denoted  $\sqrt[n]{r}$ .*

**Proof:** The function:

$$f(x) = x^n$$

is continuous and differentiable, with derivative  $f'(x) = nx^{n-1}$ . Since  $f(0) = 0$  and  $\lim_{x \rightarrow +\infty} f(x) = +\infty$ , the intermediate value theorem tells us that the graph of  $f$  crosses the line  $y = r$  somewhere, say at the point  $(s, r)$ . This means  $f(s) = r$ , or in other words  $s^n = r$ . But now we ask: “Why doesn’t the graph of  $f$  cross  $y = r$  **more than once**? Of course, it may cross the line  $y = r$  again when  $x$  is negative (if  $n$  is even). But when  $x$  is positive, then  $f(x)$  is a strictly **increasing** function because  $f'(x) = nx^{n-1} > 0$ . And strictly increasing functions cannot take the same value more than once!

It may seem as though with the real numbers we have reached the ultimate number system. However, the fact that negative real numbers do not have real square roots leads us to one final improvement.

The “purely imaginary number”  $i$  is by definition a square root of  $-1$ :

$$i^2 = -1$$

To be honest, this doesn’t seem much more “imaginary” to me than the negative numbers, which were introduced in order to have additive inverses. Just as it made good geometric sense to place  $-1$  one unit to the left of 0 on the number-line, it turns out to make good geometric sense to place  $i$  one unit above 0 on a “number-plane”.

**The Complex Numbers:**

$$\mathbb{C} = \{\text{points on the number-plane}\}$$

A point in the plane is given by two real coordinates  $(s, t)$  or else as:

$$s + ti$$

The complex numbers are no longer ordered, since it makes no sense any more to write:  $s + ti < u + vi$ , but addition and multiplication can still be defined, so that  $\mathbb{C}$  a field, and what is more, addition and multiplication have very useful geometric interpretations.

**Definition of Addition.** Addition of complex numbers is defined to be vector addition,  $(s, t) + (u, v) = (s + u, t + v)$ , which can also be written:

$$(s + ti) + (u + vi) = (s + u) + (t + v)i$$

Vector addition takes the translation definition for addition of real numbers and promotes it to a translation definition for the addition of vectors in spaces of all dimensions. In the case of the complex numbers, the space is two-dimensional. But the rules for addition will hold in all dimensions:

**Addition is associative:**

$$((s, t) + (u, v)) + (x, y) = ((s + u) + x, (t + v) + y)$$

$$(s, t) + ((u, v) + (x, y)) = (s + (u + x), t + (v + y))$$

These are the same because addition of real numbers is associative. Similarly,

**Addition is commutative, and  $(0,0)$  is the additive identity.**

We also have a fancier:

**Negation Transformation:** This time the negation transformation

$$- : \mathbb{C} \rightarrow \mathbb{C}$$

takes  $(s, t)$  to  $(-s, -t)$ . It reflects the number-plane across the origin.

**Definition of Multiplication:** Multiplication of complex numbers is defined by  $(s, t) \cdot (u, v) = (su - tv, sv + tu)$ , which may also be written:

$$(s + ti)(u + vi) = (su - tv) + (sv + tu)i$$

Unlike addition, this is **not** something we get for free by thinking of  $\mathbb{C}$  as a vector space. Instead, this definition is forced upon us by the distributive law, and the fact that  $i^2 = -1$ .

**Multiplication is commutative:**

$$(s + ti)(u + vi) = su - tv + (sv + tu)i$$

$$(u + vi)(s + ti) = us - vt + (ut + vs)i$$

These are the same because multiplication of real numbers is commutative!

**Multiplication is associative:** Check this for yourself.

**Multiplication distributes with addition:** (Exercise.)

**$(1,0)$  is the multiplicative identity:**

$$(1 + 0i)(u + vi) = (u - 0) + (v + 0)i = u + vi$$

Finally, we want multiplicative inverses. To do this, we introduce a second:

**Conjugation Transformation:** This is the function:

$$c : \mathbb{C} \rightarrow \mathbb{C}$$

such that  $c(s + ti) = \overline{s + ti} = s - ti$ . It reflects the plane across the  $x$ -axis. Notice that only the real numbers are unchanged under conjugation, and that the “purely imaginary” numbers  $ti$  conjugate to their additive inverses  $-ti$ .

**Proposition 1.4.2.** *The conjugation transformation is both linear and multiplicative. That is:*

$$\begin{aligned} \overline{(s + ti) + (u + vi)} &= \overline{(s + ti) + (u + vi)} \text{ and} \\ \overline{(s + ti) \cdot (u + vi)} &= \overline{(s + ti)(u + vi)} \end{aligned}$$

**Proof:** Let's work them out:

$$\overline{(s + ti) + (u + vi)} = \overline{(s + u) + (t + v)i} = (s + u) - (t + v)i.$$

$$\overline{(s + ti) + (u + vi)} = (s - ti) + (u - vi) = (s + u) - (t + v)i. \text{ Check.}$$

$$\overline{(s + ti)(u + vi)} = \overline{(su - tv) + (sv + tu)i} = (su - tv) - (sv + tu)i.$$

$$\overline{(s + ti) \cdot (u + vi)} = (s - ti)(u - vi) = (su - tv) - (sv + tu)i. \text{ Check.}$$

It is somewhat surprising that conjugation is a multiplicative transformation! After all, the negation transformation certainly isn't multiplicative:

$$(-r)(-s) = rs, \text{ not } -(rs)$$

**Absolute Value:** The absolute value of a complex (or real) number is its Euclidean distance from  $0 = (0, 0)$ . That is,

$$|s + ti| = \sqrt{s^2 + t^2}$$

and it is very useful to notice that:

$$|s + ti|^2 = s^2 + t^2 = (s + ti)(s - ti) = (s + ti)\overline{(s + ti)}$$

and that whenever  $s + ti \neq 0$ , then:

$$1 = \frac{s^2 + t^2}{s^2 + t^2} = \frac{(s + ti)(s - ti)}{s^2 + t^2} = (s + ti) \left( \frac{s - ti}{s^2 + t^2} \right)$$

so that  $s + ti$  has a multiplicative inverse, namely:

$$\frac{1}{(s + ti)} = \frac{s - ti}{s^2 + t^2} = \frac{s}{s^2 + t^2} - \frac{t}{s^2 + t^2}i$$

Thus:

**$\mathbb{C}$  is a field!**

I promised a useful geometric interpretation of the multiplication of complex numbers. This is done using:

**Polar Coordinates:** If  $r$  is a positive real number (or zero) and  $\theta$  is any real number, then the “polar coordinates”:

$$(r; \theta)$$

are the coordinates of the unique point in the plane which is at the distance  $r$  from 0, and such that the line segment between 0 and  $(r; \theta)$  is at the angle  $\theta$  from the positive  $x$ -axis (measured counter-clockwise). I have put a semi-colon between  $r$  and  $\theta$  to distinguish this notation from the vector notation for a point in the plane. Also **all angles will be measured in radians**.

There is some redundancy in polar coordinates. Precisely:

$(0; \theta)$  is the origin whatever  $\theta$  may be, and

$(r; \theta)$  and  $(r; \theta + 2\pi a)$  are the same point when  $a$  is an integer.

**Proposition 1.4.3.** *In polar coordinates, the multiplication rule for complex numbers becomes:*

$$(r; \theta) \cdot (s; \psi) = (rs; \theta + \psi)$$

*which is a wonderfully simple geometric description. In English:*

**Multiplication Rule:** *To multiply two complex numbers in polar coordinates, add their angles and multiply their distances from 0.*

**Proof:** Recall that  $\cos(\theta)$  and  $\sin(\theta)$  are the  $x$  and  $y$ -coordinates of the point on the unit circle at the angle  $\theta$  from the positive real axis. Thus,

$$(1; \theta) = (\cos(\theta), \sin(\theta))$$

and replacing 1 by  $r$  multiplies through by  $r$ , so  $(r; \theta) = (r\cos(\theta), r\sin(\theta))$ .

To see the rule, we translate from polar to vector coordinates, do the multiplication, and then translate back into polar coordinates. Let  $(r; \theta)$  and  $(t; \psi)$  be our two complex numbers. Then:

$$\begin{aligned} (r; \theta) \cdot (t; \psi) &= (r\cos(\theta), r\sin(\theta)) \cdot (t\cos(\psi), t\sin(\psi)) \\ &= (r\cos(\theta)t\cos(\psi) - r\sin(\theta)t\sin(\psi), r\cos(\theta)t\sin(\psi) + r\sin(\theta)t\cos(\psi)) \\ &= (rt(\cos(\theta)\cos(\psi) - \sin(\theta)\sin(\psi)), rt(\cos(\theta)\sin(\psi) + \sin(\theta)\cos(\psi))) \end{aligned}$$

Now, remember the angle addition identities from trigonometry:

$$\cos(\theta + \psi) = \cos(\theta)\cos(\psi) - \sin(\theta)\sin(\psi)$$

and

$$\sin(\theta + \psi) = \cos(\theta)\sin(\psi) + \sin(\theta)\cos(\psi)$$

Substituting these identities into our formula for the product gives:

$$(r; \theta) \cdot (t; \psi) = (rt\cos(\theta + \psi), rt\sin(\theta + \psi))$$

and in polar coordinates, this is:  $(rt; \theta + \psi)$ . Done!

**Corollary 1.4.4.** *There are  $n$  different  $n$ th roots of any complex number except for 0, which always has only one  $n$ th root!*

**Proof:** Let  $z = (r; \theta)$  in polar coordinates. Taking an  $n$ th power is easy to do using Proposition 1.4.3. Namely:

$$z^n = (r; \theta)^n = (r^n; n\theta)$$

But then using Proposition 1.4.1, we see that conversely:

$$\left( \sqrt[n]{r}; \frac{\theta}{n} \right)$$

is an  $n$ th root of  $(r; \theta)$  (we use Proposition 1.4.1 for  $\sqrt[n]{r}$ ). But:

$$\left( \sqrt[n]{r}; \frac{\theta}{n} + \frac{2\pi}{n} \right), \left( \sqrt[n]{r}; \frac{\theta}{n} + \frac{4\pi}{n} \right), \dots, \left( \sqrt[n]{r}; \frac{\theta}{n} + \frac{(2n-2)\pi}{n} \right)$$

are also  $n$ th roots of  $r$ , and what's more, these are all **different** complex numbers because the angles between any two of them do not differ by a multiple of  $2\pi$ . We have  $n$  of these in all, so we have found as many  $n$ th roots as we wanted. But why aren't there any more? As we've seen, if  $(s; \psi)$  is an  $n$ th root of  $(r; \theta)$ , then  $s = \sqrt[n]{r}$  must be the **unique** positive  $n$ th root of  $r$  from Proposition 1.4.1. Moreover, the  $n$  angles we've listed above are the **only** angles between 0 and  $2\pi$  with the property that  $n\psi = \theta + 2\pi a$ . This tells us that if  $(s; \psi)$  is any complex number other than the  $n$  roots listed above, then either  $s^n \neq r$  or else  $n\psi \neq \theta + 2\pi a$ . Thus, there are no more  $n$ th roots than these!

**Examples:** (a) The two square roots of  $i = (1; \frac{\pi}{2})$  are:

$$\left( 1; \frac{\pi}{4} \right) \text{ and } \left( 1; \frac{\pi}{4} + \frac{2\pi}{2} \right) = \left( 1; \frac{5\pi}{4} \right)$$

In ordinary complex number notation, these are:  $\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}i$  and  $-\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}}i$ .

(b) The three cube roots of  $-8 = (8; \pi)$  are:

$$\left( 2; \frac{\pi}{3} \right), \left( 2; \frac{\pi}{3} + \frac{2\pi}{3} = \pi \right), \text{ and } \left( 2; \frac{\pi}{3} + \frac{4\pi}{3} = \frac{5\pi}{3} \right)$$

which in ordinary notation for complex numbers are:  $1 + \sqrt{3}i$ ,  $-2$  and  $1 - \sqrt{3}i$ .

**Remark:** We introduced  $i$  as an imaginary square root of  $-1$ , used it to define the complex numbers, and now we see that by doing this, we have in fact given ourselves **all** possible  $n$ th roots of **all** numbers, even the new complex numbers themselves! This is indeed a remarkable development. But it gets even better. In §2.5, we will see that all roots of all polynomials with complex number coefficients (not just the polynomials  $x^n = z$ ) are complex numbers.

I can't resist finishing by pointing out the link between:

**Exponentials and Trigonometry:** The Taylor series for  $e^z$  is given by:

$$e^z = 1 + z + \frac{z^2}{2!} + \frac{z^3}{3!} + \frac{z^4}{4!} + \dots$$

and this series, which converges for all real numbers, also converges for all **complex** numbers. Moreover, if  $z = i\theta$  is a purely imaginary complex number, then:

$$\begin{aligned} e^{i\theta} &= 1 + (i\theta) + \frac{(i\theta)^2}{2!} + \frac{(i\theta)^3}{3!} + \frac{(i\theta)^4}{4!} + \dots \\ &= 1 + i\theta - \frac{\theta^2}{2!} - i\frac{\theta^3}{3!} + \frac{\theta^4}{4!} + i\frac{\theta^5}{5!} - \dots \\ &= \left(1 - \frac{\theta^2}{2!} + \frac{\theta^4}{4!} - \dots\right) + i\left(\theta - \frac{\theta^3}{3!} + \frac{\theta^5}{5!} - \dots\right) \end{aligned}$$

and then the Taylor series for  $\cos(\theta)$  and  $\sin(\theta)$  tell us that:

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

which is even simpler in polar coordinates:

$$e^{i\theta} = (1; \theta).$$

We can multiply through by a positive real number  $r$ , to get:

$$re^{i\theta} = (r; \theta)$$

This gives a new way of looking at Proposition 1.4.3:

$$(r; \theta) \cdot (t; \psi) = (re^{i\theta}) \cdot (te^{i\psi}) = rte^{i\theta}e^{i\psi} = rte^{i(\theta+\psi)} = (rt; \theta + \psi)$$

so the angle addition is just the rule for exponents:  $e^{i\theta}e^{i\psi} = e^{i(\theta+\psi)}$ .

Since  $(1; \pi) = -1$ , this interpretation of polar coordinates gives:

$$e^{i\pi} = -1$$

which is an extraordinary relation among the special numbers:  $i, \pi, e$  and  $-1$ .

### 1.4.1 Complex Number Exercises

**4-1** For each of the following complex numbers:

$$(a) 3 + 4i, \quad (b) 3 - 4i \quad (c) -3 + 4i \quad (d) -3 - 4i$$

- (i) Square it.    (ii) Find its multiplicative inverse.
- (iii) Find (approximate) polar coordinates for it.
- (iv) Find both square roots of it, in both polar and rectangular coordinates.
- (v) Plot it, its inverses and its square roots.

**Note:** To put  $s + ti$  in polar coordinates, set:

$$r = \sqrt{s^2 + t^2} \quad \text{and} \quad \theta = \tan^{-1}(t/s)$$

There is a subtlety in determining the angle  $\theta$ , though. If, for example, you feed  $-1 - i$  into your calculator (always set for **radians!**), it will give you:

$$r \approx 1.414 \quad \text{and} \quad \theta \approx 0.7854$$

which are the approximate polar coordinates for  $1 + i$ , not for  $-1 - i$ . The problem is that the calculator always chooses  $\tan^{-1}$  so that the angle is between  $-\pi/2$  and  $\pi/2$ . In other words, it will always assume that  $s \geq 0$ . If your complex number has a negative value of  $s$ , you will need to add  $\pi$  to the value of  $\theta$  given by your calculator to get the “true”  $\theta$ . Thus:

$$r \approx 1.414 \quad \text{and} \quad \theta \approx \pi + 0.7854 \approx 3.927$$

are the true approximate polar coordinates for  $-1 - i$ .

**4-2** Find  $(1 + 2i)^5$  and  $(1 + 2i)^{10}$  in two different ways:

(a) Multiply them out cleverly (show your work!).

(b) Convert to (approximate) polar coordinates, take the power, then convert back to rectangular coordinates.

**4-3** Prove the distributive law for complex numbers.

**4-4** Prove the following:

(a)  $|(s + ti)(u + vi)| = |s + ti||u + vi|$

(b)  $|1/(s + ti)| = 1/|s + ti|$ .

(c)  $\overline{1/(s + ti)} = 1/\overline{(s + ti)}$

**4-5** Find the polar coordinates for each of the following:

(a)  $\overline{(r; \theta)}$ ,      (b)  $-(r; \theta)$       (c)  $1/(r; \theta)$       (d)  $-\overline{1/(r; \theta)}$

**4-6** (a) Find all the eighth roots of 16 in exact rectangular coordinates.

(b) Find all the twelfth roots of 16 in exact polar coordinates.

**4-7** The **Gaussian integers** are:

$$\mathbb{Z}[i] = \{a + bi \text{ such that } a, b \in \mathbb{Z}\} \subset \mathbb{C}$$

The four Gaussian integers with multiplicative inverses are  $1, -1, i, -i$ . All the other Gaussian integers are “interesting.” A Gaussian integer  $a + bi$  is **prime** if its only factors are  $1, -1, i, -i$  or one of these multiplied by  $a + bi$ , namely  $a + bi, -a - bi, b - ai$  or  $-b + ai$ .

Notice:

$$2 + 0i = (1 + i)(1 - i) = 1^2 + 1^2 \quad \text{and} \quad 5 + 0i = (1 + 2i)(1 - 2i) = 1^2 + 2^2$$

so 2 and 5 are no longer primes when thought of as Gaussian integers!

(a) Graph all the Gaussian integers on a chunk of the number plane.

(b) For each of the integer primes from 2 to 30, decide whether they can be factored or remain prime when thought of as Gaussian integers. Can you detect a pattern?

(c) Would you expect 10007 to be a prime Gaussian integer or not?

(Hint: It has a remainder of 3 when divided by 4.)

**4-8 The Eisenstein integers are:**

$$\mathbb{Z}[\omega] = \{a + b\omega \text{ such that } a, b \in \mathbb{Z}\} \subset \mathbb{C}$$

where

$$\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$$

(a) Show that the product of two Eisenstein integers is again an Eisenstein integer. (This was obvious for the Gaussian integers!)

(b) Show that

$$\bar{\omega} = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$$

is an Eisenstein integer.

(c) Graph the Eisenstein integers on a chunk of the number-plane.

(d) Which six Eisenstein integers have multiplicative inverses that are also Eisenstein integers? These are the “uninteresting” ones.

(e) Calculate  $(a + b\omega)(a + b\bar{\omega})$ .

(f) Show that 3 is not prime as an Eisenstein integer.

## Chapter 2

# Polynomials

A **polynomial** in the variable  $x$  looks like:

$$a_d x^d + a_{d-1} x^{d-1} + \dots + a_0$$

where  $a_0, \dots, a_d$  are the coefficients, which are usually elements of a field, and  $d$  is the degree (assuming the leading coefficient  $a_d$  is nonzero). The arithmetic of polynomials has a lot of the same features as the arithmetic of integers: both admit division with remainders, Euclid's algorithm and have infinitely many primes, and rational functions (polynomial fractions) play the role of rational numbers (integer fractions). This resemblance is formalized in the definition of a **Euclidean domain**, which includes both the integers and all polynomials with coefficients in a field, and where there is unique factorization into primes.

The **roots** tell us everything there is to know about a polynomial. Polynomials with rational number coefficients will be of particular interest to us. The rational roots test finds all the rational number roots of such polynomials, but there are often irrational roots. The quadratic and cubic formulas give the (possibly complex) roots of polynomials of degree 2 or 3, but things are considerably more complicated in higher degree. Even deciding whether or not a polynomial is prime can be difficult, and Eisenstein's criterion uses the finite fields produced by **clock arithmetic** to give one useful way of detecting prime polynomials. We know one thing for sure. All the roots are complex numbers. This is the **fundamental theorem of algebra** which we will prove using a few simple ideas from analysis.

## 2.1 Polynomial Basics

**Definition:** A **polynomial** in the variable  $x$  has the following form:

$$f(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_1 x + a_0$$

where the **coefficients**  $a_0, a_1, \dots, a_d$  are elements of a field.

**Note:** We have seen three fields so far:  $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ . We will see many other fields! The set of all polynomials with coefficients in a given field  $F$  will be denoted:

$$F[x]$$

so for example  $\mathbb{Q}[x]$  is the set of all polynomials with rational coefficients.

**Examples:** Some polynomials have special names:

- (a) The zero polynomial is  $f(x) = 0$ .
- (b) The constants are  $f(x) = a$  with  $a \neq 0$ .
- (c) The linear polynomials are  $f(x) = ax + b$ , with  $a \neq 0$ .
- (d) The quadratic polynomials are  $f(x) = ax^2 + bx + c$ , with  $a \neq 0$ .
- (e) The cubic polynomials are  $f(x) = ax^3 + bx^2 + cx + d$ , with  $a \neq 0$ .

**Padding polynomials:** The two polynomials:

$$f(x) \quad \text{and} \quad 0x^d + f(x)$$

will be considered to be equivalent. That is why, for example, we do not consider  $0x + b$  to be a linear polynomial. It is a constant that has been padded with the fake linear term  $0x$ , and similarly  $0x^2 + ax + b$  is a padded linear polynomial, not a quadratic polynomial. In every equivalence class of polynomials except the zero polynomial, there is exactly one “unpadded” polynomial:

$$f(x) = a_d x^d + \cdots + a_0 \quad \text{with} \quad a_d \neq 0$$

and the **degree** of this  $f(x)$  (or any padding of it) is well-defined to be  $d$ . Thus only the zero polynomial does not have a well-defined degree (after you unpad all the zero coefficients, it completely disappears!). Some texts set the degree of the zero polynomial to be  $-\infty$ . We won't do that here. We will simply leave the degree of the zero polynomial undefined.

**Examples:** The special names correspond to low degree polynomials:

- (b) The constants are the polynomials of degree 0.
- (c) The linear polynomials are the polynomials of degree 1.
- (d) The quadratic polynomials are the polynomials of degree 2.
- (e) The cubic polynomials are the polynomials of degree 3.

**Definition of Addition.** This is done coefficient by coefficient:

$$\begin{array}{cccccc}
 a_d x^d & + & \cdots & + & a_0 & \\
 + & b_d x^d & + & \cdots & + & b_0 \\
 \hline
 = & (a_d + b_d)x^d & + & \cdots & + & (a_0 + b_0)
 \end{array}$$

**More on Addition:**  $F[x]$  is a vector space with (infinite) basis:  $1, x, x^2, x^3, \dots$ . The addition is vector addition, which is associative and commutative with additive identity element 0, and additive inverses always exist. Also:

$$b(a_d x^n + \cdots + a_0) = (ba_d)x^n + \cdots + (ba_0)$$

is scalar multiplication (and  $F$  is often called the **scalar field**.)

**Note:** You may have only seen linear algebra in the case of the scalar field  $\mathbb{R}$ . In this course, it will be important to consider other scalar fields. See §3.1.

**Definition of Multiplication.** This is **not** just scalar multiplication above. It is determined by “foil” (the distributive law) and the rule for exponents  $x^d x^e = x^{d+e}$ . The bookkeeping may be done in the following way:

$$\begin{array}{cccccc}
 a_d x^d & + & \cdots & + & \cdots & + & a_1 x & + & a_0 \\
 \times & & & & b_e x^e & + & \cdots & + & b_1 x & + & b_0 \\
 \hline
 (a_d b_0)x^d & + & \cdots & + & \cdots & + & (a_1 b_0)x & + & a_0 b_0 \\
 (a_d b_1)x^{d+1} & + & (a_{d-1} b_1)x^d & + & \cdots & + & \cdots & + & (a_0 b_1)x \\
 & & & & \vdots & & & & & & 
 \end{array}$$

just as you do the bookkeeping when you multiply many-digit numbers, adding up each of the columns under the bar. Notice that in the far left column, there will only be one term to add, namely  $a_d b_e x^{d+e}$  just as on the far right there is only the constant term  $a_0 b_0$ , so the final answer looks like:

$$a_d b_e x^{d+e} + (a_d b_{e-1} + a_{d-1} b_e)x^{d+e-1} + \cdots + (a_1 b_0 + a_0 b_1)x + a_0 b_0$$

with a jumble of terms in the middle. In summation notation (from calculus) the final answer is written really simply like this:

$$\sum_{i=0}^d \sum_{j=0}^e a_i b_j x^{i+j}$$

**Example:** Calculate  $(x^2 + x + 1)(x - 1) = x^3 - 1$ :

$$\begin{array}{r}
 \begin{array}{ccccccc}
 & & x^2 & + & x & + & 1 \\
 \times & & & & & & \\
 \hline
 & & (-1)x^2 & + & (-1)x & + & (-1) \\
 x^3 & + & x^2 & + & x & & \\
 \hline
 x^3 & + & 0x^2 & + & 0x & + & (-1)
 \end{array}
 \end{array}$$

Multiplication is associative, commutative and distributes with addition. The constant 1 is the multiplicative identity element, but  $F[x]$  is not a field because not every non-zero polynomial has a multiplicative inverse. In fact, only the constants have multiplicative inverses. All but the last of these statements follow from the rules of arithmetic for  $F$ , and can be seen quite elegantly with the summation notation (see Exercise 5-7). The last statement is a corollary of the following:

**Proposition 2.1.1.** *If  $f(x)$  has degree  $d$  and  $g(x)$  has degree  $e$ , then*

$$f(x)g(x) \text{ has degree } d + e$$

**Proof:** Unpad all the zero terms from  $f(x)$  and  $g(x)$ . Then

$$f(x)g(x) = (a_dx^d + \cdots + a_0)(b_ex^e + \cdots + b_0) = a_db_ex^{d+e} + \cdots + a_0b_0$$

and  $a_d \neq 0$  and  $b_e \neq 0$  by the definition of degree. Since  $a_d \neq 0$  and  $b_e \neq 0$  and  $F$  is a field, there are multiplicative inverses  $\frac{1}{a_d}$  and  $\frac{1}{b_e}$  in  $F$ , and then  $\left(\frac{1}{a_d}\right)\left(\frac{1}{b_e}\right)$  is the multiplicative inverse of  $a_db_e$ , so  $a_db_e \neq 0$ . Thus  $d + e$  is the degree of  $f(x)g(x)$ .

**Corollary 2.1.2.** *Only the constants have multiplicative inverses in  $F[x]$ .*

**Proof:** If  $f(x)$  and  $g(x)$  have degrees  $d$  and  $e$  and are multiplicative inverses of each other, then  $f(x)g(x) = 1$ , which has degree 0, so  $d + e = 0$ . But  $d \geq 0$  and  $e \geq 0$ , so  $d + e = 0$  can only happen if both  $d = 0$  and  $e = 0$ . That is,  $f(x)$  and  $g(x)$  can only be multiplicative inverses if they are both constants.

**Corollary 2.1.3.** *If  $f(x)g(x) = 0$ , then  $f(x) = 0$  or  $g(x) = 0$ .*

**Proof:** If  $f(x)g(x) = 0$ , then its degree is undefined. By Proposition 2.1.1, this means that either the degree of  $f(x)$  or the degree of  $g(x)$  is undefined (otherwise, the degree of  $f(x)g(x)$  would be  $d + e$ ). Thus either  $f(x) = 0$  or  $g(x) = 0$  (or both).

**Corollary 2.1.4.** *If  $f(x) \neq 0$  and  $f(x)g(x) = f(x)h(x)$ , then  $g(x) = h(x)$ . (in other words,  $f(x)$  can be cancelled from both sides).*

**Proof:** After subtracting and distributing:  $f(x)(g(x) - h(x)) = 0$ , so either  $f(x) = 0$  or  $g(x) - h(x) = 0$  by Corollary 2.1.3. But  $f(x) \neq 0$  by assumption, so  $g(x) - h(x) = 0$ , and adding  $h(x)$  to both sides gives  $g(x) = h(x)$ .

No multiplicative inverses (of non-constant polynomials) means we don't have an honest division. But as in §1.1 there is a consolation prize:

**Division with Remainders:** If  $f(x)$  and  $g(x)$  have degrees  $d$  and  $e$ , with  $d \leq e$ , then:

$$g(x) = f(x)q(x) + r(x)$$

where  $r(x)$  is either 0 or else a polynomial of smaller degree than  $d$ .

I won't burden you with the proof. Suffice it to say that as with the natural numbers, you can, using induction, turn the familiar long division into a mathematical proof of division with remainders.

**Example:** In  $\mathbb{Q}[x]$ , long divide  $x^3 + 1$  by  $2x + 1$ :

$$\begin{array}{r}
 2x + 1 \quad \overline{) \begin{array}{r} x^3 + 0x^2 + 0x + 1 \\ x^3 + \frac{1}{2}x^2 \\ \hline -\frac{1}{2}x^2 + 0x \\ -\frac{1}{2}x^2 - \frac{1}{4}x \\ \hline \frac{1}{4}x + 1 \\ \frac{1}{4}x + \frac{1}{8} \\ \hline \frac{7}{8} \end{array} \\
 \end{array}$$

to get the quotient  $q(x) = \frac{1}{2}x^2 - \frac{1}{4}x + \frac{1}{8}$  and remainder  $r(x) = \frac{7}{8}$ .

**Definitions:** (a)  $f(x)$  **divides**  $g(x)$  if  $g(x) = f(x)q(x)$  (with zero remainder). In this case,  $f(x)$  is said to be a **factor** of  $g(x)$ .

(b)  $f(x)$  is a **prime** polynomial of degree  $d > 0$  if the only factors of  $f(x)$  have either degree  $d$ , or else degree 0 (in this case, the constants are all considered to be uninteresting, and in particular are not primes!).

**Examples:** (a) All linear polynomials are prime.

(b) Whether a polynomial is a prime or not may depend upon the coefficients. For example,  $x^2 + 1$  is prime in  $\mathbb{R}[x]$ , but not in  $\mathbb{C}[x]$ , where  $x^2 + 1 = (x - i)(x + i)$ .

**The Fundamental Theorem for Polynomials:** Each non-constant polynomial in  $F[x]$  factors as a product of finitely many prime polynomials.

**Proof:** Let  $S \subset \mathbb{N}$  be the set of **degrees** of all the polynomials that do not factor as a product of finitely many prime polynomials. Then  $S = \emptyset$  or else  $S$  has a smallest element  $d$ , by the well-ordered axiom. If  $f(x)$  is any polynomial of degree  $d$ , then either  $f(x)$  is prime or else  $f(x) = g(x)h(x)$  so that  $g(x)$  and  $h(x)$  have smaller degree. But then  $g(x)$  and  $h(x)$  must both be products of finitely many primes because their degrees are not elements of  $S$ , and so  $f(x)$  itself factors as a product of finitely many primes. But this tells us that every polynomial of degree  $d$  must factor as a product of primes, so there can be no such  $d$ , and therefore  $S = \emptyset$ , meaning that all polynomials factor.

**Euclid's Theorem:** There are infinitely many primes in each  $F[x]$ .

**Proof:** Same as the proof for  $\mathbb{N}$ . Given a finite number of prime polynomials:

$$p_1(x), p_2(x), \dots, p_n(x)$$

the fundamental theorem tells us we can factor the polynomial:

$$g(x) = p_1(x)p_2(x)\dots p_n(x) + 1$$

and each of the prime factors of  $g(x)$  is “new” (not one of the  $p_i(x)$ ) because none of the  $p_i(x)$  divide  $g(x)$ . So however many primes we start with, we know there are more, and this can only be true if there are infinitely many.

**Remark:** Every field  $F$  we have seen so far is already infinite, so in this case there are already infinitely many **linear** polynomials:

$$f(x) = x + a$$

and Euclid's theorem isn't really telling us much. We will, however, soon see fields with only a finite number of elements, where Euclid's theorem is definitely telling us something interesting!

**Euclid's Algorithm:** Start with  $f(x)$  and  $g(x)$  of degrees  $d \leq e$ , and apply division with remainders according to the following prescription:

$$\begin{aligned} g(x) &= f(x)q_1(x) + r_1(x) \\ f(x) &= r_1(x)q_2(x) + r_2(x) \\ r_1(x) &= r_2(x)q_3(x) + r_3(x) \\ &\vdots \end{aligned}$$

until we reach a remainder of zero. Then the last non-zero remainder  $r_{k+1}(x)$  is a common divisor of  $f(x)$  and  $g(x)$  of greatest degree.

**Remark:** If  $d(x)$  is a common divisor of  $f(x)$  and  $g(x)$ , then so is any constant multiple of  $d(x)$ . So there is no single gcd of two polynomials.

**Example:** If  $f(x) = x^6 + 1$  and  $g(x) = x^{10} + 1$  then:

$$\begin{aligned} x^{10} + 1 &= (x^6 + 1)(x^4) + (-x^4 + 1) \\ x^6 + 1 &= (-x^4 + 1)(-x^2) + (x^2 + 1) \\ -x^4 + 1 &= (x^2 + 1)(-x^2 + 1) \end{aligned}$$

so  $x^2 + 1$  is a common divisor of largest degree. But so are  $2x^2 + 2$  and  $\frac{1}{2}x^2 + \frac{1}{2}$ .

**Rational Functions:** The set of rational functions with coefficients in  $F$  is

$$F(x) = \left\{ \text{equivalence classes of fractions } \frac{f(x)}{g(x)} \right\}$$

where  $f(x)$  and  $g(x)$  are elements of  $F[x]$ , and  $g(x) \neq 0$ .

This time, we define the equivalence relation on fractions by the:

**Cross Multiplication Rule:**

$$\frac{f(x)}{g(x)} \sim \frac{a(x)}{b(x)} \text{ if } f(x)b(x) = g(x)a(x)$$

Unlike the rational numbers, there is no nice geometric way of picturing the equivalence classes as lines through the origin. But this doesn't matter! The "algebraic" cross multiplication rule is all that we need to create the field of rational functions. Recall that we have to verify three properties before we are technically allowed to talk about equivalence classes. Namely:

(i) Reflexivity:

$$\frac{f(x)}{g(x)} \sim \frac{f(x)}{g(x)} \text{ because } f(x)g(x) = g(x)f(x) \text{ Check.}$$

(ii) Symmetry:

$$\text{If } \frac{f(x)}{g(x)} \sim \frac{a(x)}{b(x)} \text{ then } \frac{a(x)}{b(x)} \sim \frac{f(x)}{g(x)}$$

because  $f(x)b(x) = g(x)a(x)$  rearranges as  $a(x)g(x) = b(x)f(x)$ . Check.

(iii) Transitivity:

$$\text{If } \frac{f(x)}{g(x)} \sim \frac{a(x)}{b(x)} \text{ and } \frac{a(x)}{b(x)} \sim \frac{c(x)}{d(x)} \text{ then } \frac{f(x)}{g(x)} \sim \frac{c(x)}{d(x)}$$

because, from  $f(x)b(x) = g(x)a(x)$  and  $a(x)d(x) = b(x)c(x)$  we conclude:

$$g(x)b(x)c(x) = g(x)a(x)d(x) = f(x)b(x)d(x)$$

and then we can cancel  $b(x)$  from both sides using Corollary 5.4 to finally get:  $f(x)d(x) = g(x)c(x)$ . Check.

Now we can finish as with rational numbers.

The formulas for addition and multiplication are the same:

$$\left[ \frac{f(x)}{g(x)} \right] + \left[ \frac{a(x)}{b(x)} \right] = \left[ \frac{f(x)b(x) + a(x)g(x)}{g(x)b(x)} \right]$$

$$\left[ \frac{f(x)}{g(x)} \right] \left[ \frac{a(x)}{b(x)} \right] = \left[ \frac{f(x)a(x)}{g(x)b(x)} \right]$$

Using the cross multiplication rule, these formulas are seen to be well-defined in precisely the same way as the formulas for addition and multiplication were seen to be well-defined in §1.2. The rules of arithmetic are also verified in the same way, showing that  $F(x)$  (like  $\mathbb{Q}$ ) is a field.

Next we turn our attention in a completely different direction, to:

**The Simplest Field.** This has just the two elements 0 and 1:

$$F_2 = \{0, 1\}$$

and the only unusual thing about the field  $F_2$  is the definition:

$$1 + 1 = 0$$

(the other additions and multiplications are the familiar ones) For polynomials with coefficients in  $F_2$ , you are allowed to make the “Freshman’s mistake:”

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

Let’s think about how some of the results we’ve been discussing play out for this field. First, we can list all the polynomials in low degrees!

**Constants in  $F_2[x]$ :** There is only 1 (0 isn’t a constant)

**Linear Polynomials in  $F_2[x]$ :** There are two:  $x$  and  $x + 1$

**Quadratic Polynomials:** There are four:  $x^2$ ,  $x^2 + 1$ ,  $x^2 + x$  and  $x^2 + x + 1$

**Cubic Polynomials:** There are 8 of them:  $x^3$ ,  $x^3 + 1$ ,

$$x^3 + x, x^3 + x + 1, x^3 + x^2, x^3 + x^2 + 1, x^3 + x^2 + x, x^3 + x^2 + x + 1$$

and there are exactly  $2^d$  polynomials of each degree  $d$ . (Can you see why?)

Now for the **prime** polynomials:

**Linear Primes:** Linear polynomials are always prime.

**Quadratic Primes:** If a quadratic polynomial is **not** prime, then it must factor as a product of two linear polynomials. That means that if we form all the products of linear polynomials, then whatever is left over is prime!! There are three products we can take:

$$x \cdot x = x^2, x \cdot (x + 1) = x^2 + x \text{ and } (x + 1)^2 = x^2 + 1$$

and this leaves  $x^2 + x + 1$  as the only quadratic prime.

**Cubic Primes:** Again, we notice that if a cubic polynomial is **not** prime, then it must factor as a product of a linear polynomial and a quadratic polynomial. If we look at our list, there are 2 linears and 4 quadratics, so it looks like we aren’t going to have any cubic polynomials left over! But we do, because some of these products turn out to be the same. Let’s see:

$$x \cdot x^2 = x^3 \text{ (1)}, x \cdot (x^2 + 1) = x^3 + x \text{ (2)}, x \cdot (x^2 + x) = x^3 + x^2 \text{ (3)}$$

$$x \cdot (x^2 + x + 1) = x^3 + x^2 + x \text{ (4)}, (x + 1) \cdot x^2 = x^3 + x^2 \text{ (5)}$$

$$(x+1)(x^2+1) = x^3 + x^2 + x + 1 \quad (6)$$

$$(x+1)(x^2+x) = x^3 + x \quad (7), \quad (x+1)(x^2+x+1) = x^3 + 1 \quad (8)$$

Indeed, (3)=(5) and (2)=(7) and there are two polynomials left out:

$$x^3 + x + 1 \text{ and } x^3 + x^2 + 1 \text{ are the cubic primes!}$$

One could go on. A quartic (degree four) polynomial that is not prime must **either** factor as a linear times a cubic or as a quadratic times a quadratic. Again, it looks like there are plenty of products to use up all 16 quartic polynomials, but in fact many of the products are the same, and several are once again left over. Thus in this setting, Euclid's theorem is very powerful indeed, since it tells us that there are infinitely many primes, and in particular there are primes of larger and larger degrees in  $F_2[x]$ .

**A Last Remark** about this field  $F_2$ . The negation transformation here is a bit of a surprise, because  $-0 = 0$  (as always) but also  $-1 = 1$  since  $1 + 1 = 0$ . That is, the negation transformation on  $F_2$  **does nothing!** The smallest field where the negation transformation does something interesting will be:

$$F_3 = \{-1, 0, 1\}$$

but that is a story for the exercises.

### 2.1.1 Polynomial Exercises

**5-1** Prove by induction that:

$$(x+c)^n = x^n + \frac{n!}{(n-1)!1!}x^{n-1}c + \frac{n!}{(n-2)!2!}x^{n-2}c^2 + \cdots + \frac{n!}{1!(n-1)!}xc^{n-1} + c^n$$

(Hint: Where have we seen something like this before?)

**5-2** Factor each of the following polynomials as a product of primes in four ways, regarding them first as elements of  $\mathbb{Q}[x]$ , then  $\mathbb{R}[x]$ ,  $\mathbb{C}[x]$  and finally  $F_2[x]$ .

(a)  $x^2 - 1$

(b)  $x^2 + 1$

(c)  $x^3 - 1$

(d)  $x^3 + 1$

(e)  $x^4 - 1$

(f)  $x^4 + 1$

(g)  $x^5 - 1$

(h)  $x^6 - 1$

**5-3** Find a common divisor of largest degree of each of the following pairs of polynomials. Does it matter whether we regard them as polynomials in  $\mathbb{Q}[x]$  or as polynomials in  $\mathbb{C}[x]$  or  $F_2[x]$ ? If so, what's the difference?

- (a)  $x^9 - 1$  and  $x^6 - 1$
- (b)  $x^9 + 1$  and  $x^6 + 1$
- (c)  $x^{10} - 1$  and  $x^8 - 1$
- (d)  $x^{10} + 1$  and  $x^8 + 1$

**5-4** Find all the prime quartic polynomials in  $F_2[x]$ .

**5-5** (a) Find the only possible definitions of addition and multiplication that will make:

$$F_3 = \{-1, 0, 1\}$$

into a field (this is the second simplest field).

- (b) Find all the prime quadratic polynomials in  $F_3[x]$ .

**5-6** Explain why:

- (a) There are no prime quadratic polynomials in  $\mathbb{C}[x]$ .
- (b) The prime quadratic polynomials  $ax^2 + bx + c$  in  $\mathbb{R}[x]$  all satisfy:

$$b^2 - 4ac < 0$$

**5-7** Let  $p(x) = \sum_{i=0}^d a_i x^i$ ,  $q(x) = \sum_{j=0}^e b_j x^j$  and  $r(x) = \sum_{k=0}^f c_k x^k$  be three polynomials (written in summation notation). Then:

$$p(x)q(x) = \sum_{i=0}^d \sum_{j=0}^e a_i b_j x^{i+j} \text{ and}$$

$$q(x)p(x) = \sum_{j=0}^e \sum_{i=0}^d b_j a_i x^{j+i}$$

It is a fact of the summation notation that (finite) sums can be reversed:

$$\sum_{j=0}^e \sum_{i=0}^d b_j a_i x^{j+i} = \sum_{i=0}^d \sum_{j=0}^e b_j a_i x^{j+i}$$

and then  $a_i b_j = b_j a_i$  and  $i + j = j + i$  (for all  $i$  and  $j$ ) explain the commutative law of multiplication for polynomials.

Using the above discussion as a model, use facts about summation notation to:

- (a) State and explain the distributive law for polynomials.
- (b) State and explain the associative law of multiplication for polynomials.

## 2.2 Euclidean Domains

The sets of integers and of polynomials (for any field of coefficients) have:

- (a) Addition that associates and commutes.
- (b) An additive identity element 0 and additive inverses of everything.
- (c) Multiplication that associates, commutes and distributes with addition.
- (d) A multiplicative identity element 1.
- (e) A cancellation rule: if  $a \neq 0$  and  $ab = ac$ , then  $b = c$ .
- (f) Division with remainders.

Any set  $D$  with addition and multiplication rules that has all the properties (a)-(e) above is called an **integral domain**. A field is one kind of integral domain, and the integers and polynomials are another. Condition (f) will be part of the definition of a **Euclidean domain**.

**Definition:** An element  $a \in D$  of an integral domain is called a **unit** if it has a multiplicative inverse element, which we denote  $a^{-1}$  or  $1/a$ . There is always at least one unit in any integral domain, namely the multiplicative identity 1.

**Note:** Units are the things we call “not interesting” when we factor.

**Examples:** (a) In a field  $F$ , all the elements except 0 are units.

(b) In  $F[x]$ , the constant polynomials are the units (Corollary 2.1.2).

(c) 1 and  $-1$  are the integer units.

**Definition:** A function:

$$\deg : D - \{0\} \rightarrow \mathbb{R}^+ \cup \{0\}$$

is called a **degree function** if it has the following properties:

- (i) deg converts multiplication to addition:

$$\deg(ab) = \deg(a) + \deg(b)$$

- (ii) deg detects the units of the integral domain:

$$\deg(a) = 0 \text{ if and only if } a \text{ is a unit}$$

**Example:** The degree of a polynomial in §2.1 is a degree function:

$$\deg(a(x)) = \text{the ordinary degree of } a(x)$$

This is what Proposition 2.1.1 and Corollary 2.1.2 tell us. Notice that the range of this degree function is the set of whole numbers.

To define the degree of an *integer*, I need to remind you of the:

**Natural Logarithm:** This is defined for all positive real numbers by:

$$\ln(x) = \int_1^x \frac{1}{t} dt$$

from which it follows immediately that  $\ln(1) = 0$  and

$$\ln(x) < \ln(y) \text{ whenever } x < y$$

(in other words,  $\ln(x)$  is an **increasing** function of  $x$ ).

If  $x$  and  $y$  are fixed positive real numbers, then:

$$\int_x^{xy} \frac{1}{t} dt = \int_1^y \frac{1}{xs} (x ds) = \int_1^y \frac{1}{s} ds = \ln(y)$$

using the substitution  $t = xs$  (and  $dt = x ds$ ). But then:

$$\ln(xy) = \int_1^{xy} \frac{1}{t} dt = \int_1^x \frac{1}{t} dt + \int_x^{xy} \frac{1}{t} dt = \ln(x) + \ln(y)$$

**Proposition 2.2.1.** *The “natural log of the absolute value:”*

$$\deg(a) = \ln(|a|)$$

*is a degree function for the integers.*

**Proof:** If  $a = 0$ , then  $\deg(a) = \ln(0)$  is undefined. Otherwise  $|a| \geq 1$ , and then  $\deg(a) = \ln(|a|) \geq 0$ , so  $\deg$  has the required domain and range.

Next,  $-1$  and  $1$  are the only integers with  $\ln(|a|) = 0$ , and these are the integer units. This gives Property (ii). And finally,

$$\ln(|ab|) = \ln(|a||b|) = \ln(|a|) + \ln(|b|)$$

is what we require for Property (i). So  $\ln(|a|)$  is a degree function.

**Remark:** The smallest range of this degree function is  $\{0 = \ln(1), \ln(2), \ln(3), \dots\}$  which is not the set of whole numbers, but like the set of natural numbers and the set of whole numbers, this set **does** satisfy the well-ordered axiom. This will be important for us later.

**Definition:** An integral domain  $D$  with degree function is called a **Euclidean domain** if it has division with remainders: For all  $a, b \in D - \{0\}$ , either:

- (a)  $a = bq$  for some  $q$ , so  $b$  **divides**  $a$  ( $b$  is a **factor** of  $a$ ), or else:
- (b)  $a = bq + r$  with  $\deg(r) < \deg(b)$ , and  $r$  is the **remainder**.

**Examples:** (a)  $F[x]$  is a Euclidean domain, with the ordinary degree function.

- (b)  $\mathbb{Z}$  is a Euclidean domain with  $\log(|a|)$  as its degree function.

**Confession:** We saw in §1.1 that  $\mathbb{N}$  (not  $\mathbb{Z}$ ) has division with remainders. This can easily be modified to incorporate the negatives, however. In fact, it works even better when we allow negative remainders, since we can make their absolute values even smaller. That is, we can arrange:

$$a = bq + r \quad \text{with} \quad |r| \leq \frac{1}{2}|b|$$

which the degree function sees as  $\deg(r) \leq \deg(b) - \log(2)$ .

**Example:** Divide 1000 by 501 with remainders:

As natural numbers:  $1000 = 501(1) + 499$  with a (large) remainder of 499.

As integers:  $1000 = 501(2) + (-2)$  with a (much smaller) remainder of  $-2$ .

**Another Example:** Divide 900 by 200 with remainders:

As natural numbers:  $900 = 200(4) + 100$ .

As integers, we could take that or equally well:  $900 = 200(5) + (-100)$

In general, when  $|r| = \frac{1}{2}|b|$ , there are two possibilities for  $r$ .

Now that we have a general definition of a Euclidean domain, we'll reexamine Euclid's algorithm and refine the fundamental theorem of arithmetic for integers and polynomials (and all Euclidean domains).

**Euclid's algorithm:** If  $D$  is a Euclidean domain and the degree function has a range set that satisfies the well-ordered axiom, then each sequence of divisions with remainders eventually stops:

$$\begin{array}{rclcl} a & = & bq_1 & + & r_1 \\ b & = & r_1q_2 & + & r_2 \\ r_1 & = & r_2q_3 & + & r_3 \\ & & \vdots & & \\ r_k & = & r_{k+1}q_{k+2} & & \text{STOP} \end{array}$$

and the last remainder  $r_{k+1}$  is a common divisor of greatest degree.

**Proof:** First, we prove that each of the sequences of divisions with remainders eventually stops. Given one of them, consider the set of all degrees of all the remainders:

$$S = \{\deg(r_1), \deg(r_2), \deg(r_3), \dots\}$$

Since  $\deg(r_1) > \deg(r_2) > \deg(r_3) > \dots$ , the well-ordered axiom says there is smallest element of  $S$ , which is the degree of the last remainder!

To see that  $r_{k+1}$  is a common divisor of  $a$  and  $b$ , we work our way back up Euclid's algorithm, starting with the last line. Namely:

$$r_k = r_{k+1}q_{k+2}$$

shows that  $r_{k+1}$  divides  $r_k$ .

Next:

$$\begin{aligned} r_{k-1} &= r_k q_{k+1} + r_{k+1} \\ &= (r_{k+1} q_{k+2}) q_{k+1} + r_{k+1} \\ &= r_{k+1} (q_{k+2} q_{k+1} + 1) \end{aligned}$$

shows that  $r_{k+1}$  divides  $r_{k-1}$ . As we work our way up and substitute, we see that  $r_{k+1}$  divides **all** the remainders, and it divides  $a$  and  $b$  as well, so that  $r_{k+1}$  is a common divisor of  $a$  and  $b$  (and all other remainders, too!).

To see that  $r_{k+1}$  has greatest degree among all the common divisors, we work our way down Euclid's algorithm. The first equation:

$$a = bq_1 + r_1$$

can be rewritten as

$$r_1 = a + (-q_1)b$$

showing that  $r_1$  is a linear combination of  $a$  and  $b$ . Then:

$$r_2 = b + (-q_2)r_1 = b + (-q_2)(a + (-q_1)b) = (-q_2)a + (1 + q_1q_2)b$$

so  $r_2$  is a linear combination of  $a$  and  $b$ , too, and as we work our way down, every remainder is a linear combination of  $a$  and  $b$ , down to:

$$r_{k+1} = ua + vb$$

for some pair of elements  $u, v \in D$ .

Now if  $d$  is any common divisor of  $a$  and  $b$ , then  $a = dq$  and  $b = dq'$ , and:

$$r_{k+1} = udq + vdq' = d(uq + vq') \text{ so } d \text{ divides } r_{k+1}$$

But then

$$\deg(d) + \deg(uq + vq') = \deg(r_{k+1})$$

so  $\deg(d) \leq \deg(r_{k+1})$ . Thus  $r_{k+1}$  has the possible greatest degree of any common divisor of  $a$  and  $b$ !

**Definition:** A common divisor of greatest degree will be called a **gcd**.

**Two Examples:** First, an integer example. Start with 750 and 144.

$$\begin{aligned} 750 &= 144(5) + 30 \\ 144 &= 30(5) + (-6) \\ 30 &= (-6)(-5) \end{aligned}$$

First we go up Euclid's algorithm and substitute:

$$\begin{aligned} 30 &= (-6)(-5) \\ 144 &= 30(5) + (-6) = (-6)(-5)(5) + (-6) = (-6)(-24) \\ 750 &= 144(5) + 30 = (-6)(-24)(5) + (-6)(-5) = (-6)(-125) \end{aligned}$$

to see that  $-6$  is a common divisor of 144 and 750.

Then we go down Euclid's algorithm:

$$\begin{aligned} 30 &= 750 + 144(-5) \\ -6 &= 144 + 30(-5) = 144 + (750 + 144(-5))(-5) \\ &= 750(-5) + 144(26) \end{aligned}$$

to see that  $-6$  is a linear combination of  $750$  and  $144$ .

Next, a polynomial example. Start with  $x^4 - 1$  and  $x^3 + x$  in  $\mathbb{Q}[x]$ .

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

First we go up Euclid's algorithm and substitute:

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

to see that  $-x^2 - 1$  is a common divisor. Then we go down:

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

to see that  $-x^2 - 1$  is a linear combination of the polynomials.

**Note:** Unlike the natural numbers, gcd's in  $\mathbb{Z}$  and  $F[x]$  are not unique. In the first example,  $6$  would have been a perfectly good gcd, and in the second,  $x^2 + 1$ , or even  $\frac{1}{2}x^2 + \frac{1}{2}$  would have been possible gcd's.

**Proposition 2.2.2.** *Every gcd of  $a$  and  $b$  is a linear combination of  $a$  and  $b$ .*

**Proof:** Start with the linear combination from Euclid's algorithm:

$$r_{k+1} = ua + vb$$

If  $d$  is any gcd, then  $d$  divides  $r_{k+1}$  (see the proof of Euclid's algorithm above). So  $r_{k+1} = dq$ . But  $\deg(r_{k+1}) = \deg(d)$  (because both of them are gcds). This tells us  $\deg(q) = 0$ , so  $q$  is a **unit**. That means  $d = r_{k+1}/q$ , and:

$$d = (u/q)a + (v/q)b$$

is a linear combination of  $a$  and  $b$ .

**Example:** We said  $6$  is a gcd of  $750$  and  $144$ . We multiply:

$$-6 = 750(-5) + 144(26)$$

from Euclid's algorithm by the unit  $-1$  to get:

$$6 = 750(5) + 144(-26)$$

**Definition:** An element  $p$  of positive degree in a Euclidean domain is **prime** if its only factors of smaller degree are units.

**Example:** In  $F[x]$ , the primes are, of course, the prime polynomials. The integer primes are  $p$  and  $-p$ , where  $p$  are the natural number primes.

**Proposition 2.2.3.** *Suppose  $p$  is a prime in a Euclidean domain  $D$  and  $a \in D$  is another element of  $D$ . If  $p$  does not divide  $a$ , then 1 is a gcd of  $p$  and  $a$ .*

**Proof:** Suppose  $d$  is a gcd of  $p$  and  $a$ . Since  $p$  is a prime and  $d$  divides  $p$ , then either  $\deg(d) = 0$  or else  $\deg(d) = \deg(p)$ .

If  $\deg(d) = \deg(p)$ , let  $p = dq$ . Then  $\deg(q) = 0$ , so  $q$  is a unit, so  $d = p/q$  and  $p$  divides  $d$ , which divides  $a$ , which is not allowed.

But if  $\deg(d) = 0$ , then 1 is also a gcd of  $p$  and  $a$  because 1 obviously divides both  $p$  and  $a$  and  $\deg(1) = \deg(d) = 0$ . In other words, if a unit is a gcd of  $p$  and  $a$ , then the special unit 1 is also a gcd of  $p$  and  $a$ .

**Proposition 2.2.4.** *In a Euclidean domain, every prime that divides  $ab$  must divide  $a$  or divide  $b$  (or it divides both  $a$  and  $b$ ).*

**Proof:** If  $p$  divides  $ab$ , then  $ab = pq$  for some  $q$ . If  $p$  doesn't divide  $a$ , then 1 is a gcd of  $p$  and  $a$  (Proposition 2.2.3), and by Proposition 2.2.2

$$1 = up + va$$

for some  $u$  and  $v$ . If we multiply through by  $b$ , we get:

$$b = bup + vab = bup + vqp = p(tu + vq)$$

so  $p$  divides  $b$ . That is, if  $p$  doesn't divide  $a$ , then it must divide  $b$ . So  $p$  must divide either  $a$  or  $b$  (or both) !!

**Definition:** Primes  $p$  and  $p'$  are **associated** if  $p' = pu$  for some unit  $u \in D$ .

**Proposition 2.2.5.** *If  $p$  divides  $p'$ , then  $p$  is associated to  $p'$ .*

**Proof:** If  $p$  divides  $p'$ , they both have positive degree, since they are primes, and so  $\deg(p) = \deg(p')$  by definition of a prime. But then  $p' = pq$ , and it follows as usual, taking degrees, that  $q$  is a unit.

**Examples:** (a) In  $\mathbb{Z}$ , the primes  $p$  and  $-p$  are associated.

(b) In  $F[x]$ , primes  $f(x)$  and  $kf(x)$  (for any constant  $k$ ) are associated.

**The Fundamental Theorem of Arithmetic Revisited:** In a Euclidean domain, every element of positive degree factors as a product of finitely many primes. Moreover, if:

$$p_1 \cdots p_n = a = p'_1 \cdots p'_m$$

are two factorizations of  $a$ , then each of the  $p$ 's is associated to one of the  $p'$ 's and vice versa (so there are the same number of  $p$ 's as  $p'$ 's)

**Proof:** The fact that factorizations exist is the well-ordered axiom. We've seen this twice already! The second part needs a proof, though.

If  $p_1 \cdots p_n = p'_1 \cdots p'_m$ , then in particular,  $p_1$  divides  $p'_1(p'_2 \cdots p'_m)$ , so by Proposition 2.2.4 either  $p_1$  divides  $p'_1$  or else  $p_1$  divides  $p'_2 \cdots p'_m$ . If  $p_1$  divides  $p'_1$ , then  $p_1$  and  $p'_1$  are associated by Proposition 2.2.5.

Otherwise  $p_1$  divides  $p'_2(p'_3 \cdots p'_m)$ , and continuing in this fashion, eventually  $p_1$  is associated to one of the  $p'$ 's. Similarly, every  $p_i$  is associated to one of the  $p'_j$ 's, and reversing the argument, every  $p'_j$  is associated to one of the  $p_i$ 's.

**Example:** There are two possible prime factorizations of 15:

$$(3)(5) = 15 = (-3)(-5)$$

and 3 is associated to  $-3$  and 5 is associated to  $-5$ .

There are many prime factorizations of  $x^2 - 1$  in  $\mathbb{Q}[x]$ . Examples:

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

and  $x-1$  is associated to  $2x-2$  and  $x+1$  is associated to  $\frac{1}{2}x + \frac{1}{2}$ .

**Finishing up the proof of Proposition 1.2.5:** We needed to show that there is only one fraction in lowest terms representing each rational number. That is, we need to know that if:

$$\frac{a}{b} \sim \frac{a'}{b'}$$

and both are in lowest terms, then  $a = a'$  and  $b = b'$ . If any of them is 1 or  $-1$ , the result is obvious. Otherwise we factorize them:

$$a = p_1 \cdots p_n, \quad a' = p'_1 \cdots p'_m, \quad b = q_1 \cdots q_l, \quad b' = q'_1 \cdots q'_k$$

and then:

$$ab' = p_1 \cdots p_n \cdot q'_1 \cdots q'_k = q_1 \cdots q_l \cdot p'_1 \cdots p'_m = ba'$$

and we can assume that all the  $q$ 's and  $q'$ 's are positive, since  $b$  and  $b'$  are positive. But remember that  $a$  and  $b$  have no common factors, so **every**  $q$  must be associated, in fact **equal** to one of the  $q'$ 's. And  $a'$  and  $b'$  have no common factors, so each  $q'$  is equal one of the  $q$ 's. But then  $b = b'$  and then  $a = a'$  (cancellation law!) and we're done.

The same argument gives another useful result:

**Proposition 2.2.6.** *If  $a/b$  is in lowest terms, and*

$$\frac{a}{b} \sim \frac{a'}{b'}$$

*then  $a$  divides  $a'$  and  $b$  divides  $b'$ .*

**Proof:** Again we factorize. And again, we conclude as above that each  $q$  is equal to one of the  $q'$ 's. This is enough to let us conclude that  $b$  divides  $b'$ . Of course there may be **more**  $q'$ 's than  $q$ 's, so it may be that  $b \neq b'$ . But anyway, let  $b' = bc$ . Then  $ba' = ab' = abc$  cancels to give  $a' = ac$ , so  $a$  divides  $a'$  as well (with the same quotient  $c$ ).

### 2.2.1 Euclidean Domain Exercises

**6-1** Suppose  $D$  is an integral domain and  $ab = 0$ . Prove that  $a = 0$  or  $b = 0$ .

**6-2** Exactly one of the following is a degree function for the integers. Figure out which it is, and explain why the others don't qualify.

(a) The “absolute value minus one” function:

$$\deg(a) = |a| - 1$$

(b) The zero function:

$$\deg(a) = 0$$

(c) The “natural log of the square” function:

$$\deg(a) = \ln(a^2)$$

**6-3** For each of the following pairs of integers:

(i) Find a gcd.

(ii) Express your gcd as a linear combination of the integers.

$$(a) 37 \text{ and } 100 \quad (b) -77 \text{ and } 91 \quad (c) 777, 777 \text{ and } 100, 100$$

**6-4** For each of the following pairs of polynomials (in  $\mathbb{Q}[x]$ ):

(i) Find a gcd.

(ii) Express your gcd as a linear combination of the polynomials.

$$(a) x^5 \text{ and } x^3 + 1 \quad (b) x^{12} - 1 \text{ and } x^8 - x^6 + x^2 - 1$$

**6-5** Consider again the Gaussian integers  $\mathbb{Z}[i] = \{a + bi\}$  from §1.4.

(a) Show that  $\log(|a + bi|) = \log(\sqrt{a^2 + b^2})$  is a degree function.

There is a long division for Gaussian integers! Given  $a + bi$  and  $c + di$ , with  $\deg(c + di) < \deg(a + bi)$ , let  $p + qi$  be the closest Gaussian integer to the complex number:

$$\frac{a + bi}{c + di} = \frac{(a + bi)(c - di)}{c^2 + d^2} = \frac{ac + bd}{c^2 + d^2} + \frac{bc - ad}{c^2 + d^2}i$$

Then  $p + qi$  is the quotient Gaussian integer.

Next, define  $r + si$  by:

$$a + bi = (c + di)(p + qi) + (r + si)$$

This is the remainder, which does satisfy  $\deg(r + si) < \deg(c + di)$ .

(b) Long divide the Gaussian integer  $10 + 5i$  by  $2 + 3i$ .

(c) Find a gcd of  $5 + 5i$  and  $4 + 2i$ .

**6-6** A **power series** in the variable  $x$  is a (usually infinite) sum:

$$f(x) = a_d x^d + a_{d+1} x^{d+1} + a_{d+2} x^{d+2} + \dots \quad (a_d \neq 0, d \geq 0)$$

where the coefficients all belong to a field  $F$ . Power series are added and multiplied as polynomials are added and multiplied, and they are easily seen to satisfy properties (a)-(d) of the beginning of this section.

The set of power series is denoted by  $F[[x]]$ . In  $\mathbb{Q}[[x]]$ :

- (a) Find the multiplicative inverse of  $1 + (a/b)x$ .
- (b) Find the multiplicative inverse of  $1 + 2x + 3x^3 + 4x^4 + \dots$ .

Hint: This power series is the derivative of  $1 + x + x^2 + \dots = 1/(1-x)$ .

(c) The units in  $F[[x]]$  are exactly the power series satisfying  $d = 0$ . Assuming this fact (which I could ask you to prove, but I won't!) show that the function:

$$\deg(a_d x^d + a_{d+1} x^{d+1} + a_{d+2} x^{d+2} + \dots) = d$$

is a degree function for the power series.

- (d) Prove that  $x$  has no multiplicative inverse in any  $F[[x]]$ .

(e) Prove that  $F[[x]]$  satisfies property (e) at the beginning of this section, so it is an integral domain.

Finally,  $F[[x]]$  satisfies a strong form of division with remainders. Namely, if  $\deg(f(x)) \leq \deg(g(x))$ , then:

$$f(x) \text{ divides } g(x)$$

(I am telling you this. If you want to prove it, go for it!)

In other words, this is division with remainders without remainders! So  $F[[x]]$  is yet another example of a Euclidean domain.

## 2.3 Roots

Roots are the key to a deeper understanding of polynomials.

**Definition:** Any value  $r \in F$  that solves:

$$f(r) = 0$$

is called a **root** of the polynomial  $f(x) \in F[x]$ .

**Examples:** (a) Every  $f(x) \in \mathbb{R}[x]$  of odd degree has at least one real root. The graph of  $y = f(x)$  crosses  $y = 0$  at least once (Intermediate Value Theorem) and if  $r$  is the  $x$ -coordinate of a crossing point, then  $f(r) = 0$ . In other words, each crossing point produces a root.

(b) Linear polynomials always have one root. We can be specific in this case. The linear polynomial  $f(x) = ax + b$  has  $r = -\frac{b}{a}$  as its one and only root.

**Proposition 2.3.1.** (a) If  $x - r$  divides  $f(x)$ , then  $r$  is a root of  $f(x)$ .

(b) Conversely, if  $x - r$  doesn't divide  $f(x)$ , then  $r$  isn't a root of  $f(x)$ .

**Proof:** If  $x - r$  divides  $f(x)$  then  $f(x) = (x - r)q(x)$  and so:

$$f(r) = (r - r)q(r) = 0 \cdot q(r) = 0$$

This gives (a). If  $x - r$  doesn't divide  $f(x)$ , division with remainders gives a **constant** remainder:  $f(x) = (x - r)q(x) + a$  so that

$$f(r) = (r - r)q(r) + a = a \neq 0$$

This gives (b).

**Corollary 2.3.2.** A polynomial of degree  $d$  has at most  $d$  different roots.

**Proof:** Let  $\{r_1, \dots, r_n\}$  be any set of distinct roots of  $f(x)$ . We need to prove that  $n \leq d$ . Since  $r_1$  is a root,  $f(x) = (x - r_1)q_1(x)$  by the Proposition. All the other roots must also be roots of  $q_1(x)$ , since  $f(r_i) = (r_i - r_1)q_1(r_i) = 0$  and  $r_i - r_1 \neq 0$ . In particular,  $q_1(x) = (x - r_2)q_2(x)$ , and we can continue the process, getting a string of equalities:

$$\begin{aligned} f(x) &= (x - r_1)q_1(x) = (x - r_1)(x - r_2)q_2(x) = \dots \\ &= (x - r_1) \cdots (x - r_n)q_n(x) \end{aligned}$$

Thus  $n \leq d$  because  $d = \deg(f(x)) = n + \deg(q_n(x))$ .

Of course a polynomial of degree  $d$  could have **fewer** than  $d$  roots. A prime polynomial of degree  $\geq 2$ , for example, has **no** roots at all.

**Proposition 2.3.3 (The Rational Roots Test).** *The only possible rational roots of a polynomial with integer coefficients:*

$$f(x) = a_d x^d + a_{d-1} x^{d-1} + \dots + a_0$$

are the rational numbers  $a/b$  (written in lowest terms) such that  $b$  divides  $a_d$  and  $a$  divides  $a_0$

**Proof:** Suppose  $a/b$  is a rational root in lowest terms. Then

$$a_d \left(\frac{a}{b}\right)^d + a_{d-1} \left(\frac{a}{b}\right)^{d-1} + \dots + a_1 \left(\frac{a}{b}\right) + a_0 = 0.$$

If we clear denominators by multiplying through by  $b^d$ , we get:

$$a_d(a^d) + a_{d-1}(a^{d-1}b) + \dots + a_1(ab^{d-1}) + a_0(b^d) = 0$$

and we can put  $a_0(b^d)$  to one side of the equation and collect an  $a$  out of each of the terms on the other side to get:

$$a_0(b^d) = a(-a_d a^{d-1} - a_{d-1} a^{d-2} b - \dots - a_1 b^{d-1})$$

and so we see that  $a$  divides  $a_0(b^d)$ . Similarly:

$$a_d a^d = b(-a_{d-1} a^{d-1} - a_{d-2} a^{d-2} b - \dots - a_0 b^{d-1})$$

so we see that  $b$  divides  $a_d(a^d)$ . But we chose  $a/b$  to be in lowest terms, so none of the prime factors of  $a$  and of  $b$  are the same. It follows that  $a$  divides  $a_0$  and  $b$  divides  $a_d$ .

This gives us the following:

**Strategy for finding all rational roots of  $f(x)$  with integer coefficients:**

**Step 1:** Assemble all  $a/b$ 's for which  $a$  divides  $a_0$  and  $b$  divides  $a_d$ .

**Step 2:** The ones that solve  $f(a/b) = 0$  are all the rational roots.

**Example:** Find the rational roots of  $2x^3 + 11x^2 + 17x + 6$ . First, assemble:

$$\frac{1}{2}, -\frac{1}{2}, 1, -1, \frac{3}{2}, -\frac{3}{2}, 2, -2, 3, -3, 6, -6$$

and then try them all!

$$\begin{array}{llll} f(\frac{1}{2}) = \frac{35}{2} & f(-\frac{1}{2}) = 0 & f(1) = 36 & f(-1) = -2 \\ f(\frac{3}{2}) = 63 & f(-\frac{3}{2}) = -\frac{3}{2} & f(2) = 100 & f(-2) = 0 \\ f(3) = 210 & f(-3) = 0 & f(6) = 936 & f(-6) = -132 \end{array}$$

Thus  $-1/2, -2$  and  $-3$  are the rational roots.

**Corollary 2.3.4.** *None of the  $n$ th roots  $\sqrt[n]{2}$  is rational (for  $n > 1$ ).*

**Proof:** An  $n$ th root of 2 is, by definition, a root of the polynomial:

$$f(x) = x^n - 2$$

But the only possible rational roots of  $f(x)$  are 1,  $-1$ , 2,  $-2$  by the test. Since none of these solve  $x^n - 2 = 0$ , we see that  $\sqrt[n]{2}$  isn't rational!

**Amusing Observation:** This is our third proof that  $\sqrt{2}$  is irrational. This one, however, proves much more.

**Definition:** Any complex number that is a root of a polynomial in  $\mathbb{Q}[x]$  is called an **algebraic number** (or just **algebraic**).

**Proposition 2.3.5.** *If  $\alpha = s + it$  is an algebraic number, then  $\bar{\alpha} = s - it$  is an algebraic number, too.*

**Proof:** If  $\alpha$  is algebraic, then by definition,  $f(\alpha) = 0$  where

$$f(x) = a_d x^d + \dots + a_0 \text{ and each } a_i \text{ is rational.}$$

But then  $0 = \bar{0} = \overline{f(\alpha)} = \bar{a}_d \bar{\alpha}^d + \dots + \bar{a}_0 = f(\bar{\alpha})$  because complex conjugation is linear and multiplicative! So  $\bar{\alpha}$  is a root of the **same** polynomial  $f(x)$ .

**Proposition 2.3.6.** *If  $f(x)$  and  $g(x) \in \mathbb{Q}[x]$  have a **complex** root in common, then “the” gcd of  $f(x)$  and  $g(x)$  has **positive** degree.*

**Proof:** Euclid's algorithm **gives the same result** for the gcd of  $f(x)$  and  $g(x)$  whether we think of them as polynomials in  $\mathbb{Q}[x]$  or as polynomials in  $\mathbb{C}[x]$  (See Exercise 5-3). As polynomials in  $\mathbb{C}[x]$ , they have a common factor, namely  $x - \alpha$ , where  $\alpha$  is the complex root they have in common (Proposition 2.3.1). So the gcd, whether thought of in  $\mathbb{C}[x]$  or in  $\mathbb{Q}[x]$ , has positive degree.

**Example:**  $x^4 + 2x^2 + 1$  and  $x^4 + 3x^2 + 2$  have no rational roots at all. They do have the complex root  $i$  in common, and  $x^2 + 1$  is a gcd.

**Proposition 2.3.7.** *If  $\alpha = s + it$  is an algebraic number, there is **exactly one** prime polynomial  $p(x) \in \mathbb{Q}[x]$  with  $\alpha$  as a root and of the form:*

$$p(x) = x^d + a_{d-1}x^{d-1} + \dots + a_0$$

**Proof:** By definition,  $\alpha$  is a root of **some** polynomial  $f(x) \in \mathbb{Q}[x]$ . If we factorize:  $f(x) = p_1(x) \cdots p_n(x)$  in  $\mathbb{Q}[x]$ , then  $0 = f(\alpha) = p_1(\alpha)p_2(\alpha) \cdots p_n(\alpha)$  so (at least) one of the  $p_i(\alpha) = 0$ . Thus  $\alpha$  is a root of **some** prime polynomial. Suppose there are two prime polynomials  $p(x)$  and  $q(x)$  with  $\alpha$  as a root. By Proposition 2.3.6, we know that their gcd has positive degree. But the gcd must have the same degree as  $p(x)$  and as  $q(x)$  since they are prime, and it follows that  $p(x)$  is a constant (rational) multiple of  $q(x)$ . There is exactly one constant multiple of any polynomial that has the form  $x^d + a_{d-1}x^{d-1} + \dots + a_0$ , so there is exactly one such prime polynomial with  $\alpha$  as a root.

**Definition:** Given an algebraic number  $\alpha$ , the prime polynomial  $p(x)$  of the Proposition is called the **characteristic polynomial** of  $\alpha$ .

**Remark:** The algebraic number  $\alpha$  “knows” its characteristic polynomial  $p(x)$ , so it also knows all the **other** roots of  $p(x)$ . These other roots are called the **(algebraic) conjugates** of  $\alpha$ .

**Examples:** (a) The golden mean  $\frac{-1+\sqrt{5}}{2}$  has characteristic polynomial:

$$x^2 + x - 1$$

and its algebraic conjugate is “little” golden mean:  $\frac{-1-\sqrt{5}}{2}$ .

(b) The characteristic polynomial of  $\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}i$  is:

$$x^4 + 1$$

and there are three algebraic conjugates, which are the other fourth roots of  $-1$ :

$$-\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}i, \quad \frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}}i \quad \text{and} \quad -\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}}i$$

Notice that the “ordinary” complex conjugate is one of the algebraic conjugates. This is always true of algebraic numbers that are not real (see Proposition 2.3.5).

**A Hard Question:** Which complex numbers are algebraic numbers?

The classical formulas for the roots of low degree polynomials give some clues.

**The Quadratic Formula:** The roots of  $ax^2 + bx + c \in \mathbb{Q}[x]$  are:

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

where  $\pm\sqrt{b^2 - 4ac}$  are the square roots of  $b^2 - 4ac$ .

**Proof:** Divide through by  $a$  and complete the square:

$$x^2 + \frac{b}{a}x + \frac{c}{a} = \left(x + \frac{b}{2a}\right)^2 + \left(\frac{c}{a} - \frac{b^2}{4a^2}\right) = 0$$

The solutions are then:

$$x + \frac{b}{2a} = \pm\sqrt{\frac{b^2}{4a^2} - \frac{c}{a}} = \frac{\pm\sqrt{b^2 - 4ac}}{2a} \quad \text{or} \quad x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

**Definition:**  $\Delta = b^2 - 4ac$  is the **discriminant** of  $ax^2 + bx + c$ .

**Corollary 2.3.8.** *If  $ax^2 + bx + c \in \mathbb{Q}[x]$  then:*

- (i) *if  $\Delta > 0$ , there are two roots, both real.*
- (ii) *if  $\Delta = 0$ , the two roots come together to one real root.*
- (iii) *if  $\Delta < 0$ , there are two roots, both complex (i.e. not real).*

**The Cubic Formula:** The roots of

$$f(x) = ax^3 + bx^2 + cx + d \in \mathbb{Q}[x]$$

may be obtained as follows:

**Preliminary Step:** Divide through by  $a$ .

**Next Step:** Complete the **cube**. This is already a little messy:

$$x^3 + \frac{b}{a}x^2 + \frac{c}{a}x + \frac{d}{a} = \left(x + \frac{b}{3a}\right)^3 + \left(\frac{c}{a} - \frac{b^2}{3a^2}\right)\left(x + \frac{b}{3a}\right) + \left(\frac{d}{a} - \frac{bc}{3a^2} + \frac{2b^3}{27a^3}\right) = 0$$

We change variables before proceeding:

$$y = x + \frac{b}{3a}, \quad p = \frac{c}{a} - \frac{b^2}{3a^2} \quad \text{and} \quad q = \frac{d}{a} - \frac{bc}{3a^2} + \frac{2b^3}{27a^3}$$

and then the roots of  $y^3 + py + q = 0$  minus  $b/3a$  are the roots of  $f(x)$ .

If we are really lucky and  $q = 0$ , then the roots are  $y = 0, \pm\sqrt{-p}$  so:

$$x = -\frac{b}{3a} \quad \text{and} \quad x = -\frac{b}{3a} \pm \sqrt{\frac{b^2}{3a^2} - \frac{c}{a}} = \frac{-b \pm \sqrt{3b^2 - 9ac}}{3a}$$

are the roots of  $f(x)$ . This looks a bit like the quadratic formula, which is no accident. The first root could have been found with the rational roots test, and then the other two by the quadratic formula.

If we are only a little lucky and  $p = 0$ , then the roots are  $y = \sqrt[3]{-q}$  for the **three** complex cube roots of  $-q$ , and then the roots of  $f(x)$  are:

$$x = \frac{-b}{3a} + \sqrt[3]{\frac{bc}{3a^2} - \frac{2b^3}{27a^3} - \frac{d}{a}} = \frac{-b + \sqrt[3]{b^3 - 27a^2d}}{3a}$$

which also looks a bit like the quadratic formula (but it produces three roots)! Otherwise  $p \neq 0$  and  $q \neq 0$ , and we turn to the:

**Second Step (an inspired guess):** Set

$$y = z - \frac{p}{3z}$$

Then:

$$y^3 + py + q = \left(z - \frac{p}{3z}\right)^3 + p\left(z - \frac{p}{3z}\right) + q = z^3 - \frac{p^3}{27z^3} + q$$

which we multiply through by  $z^3$  to get a degree 6 equation:

$$z^6 + qz^3 - \frac{p^3}{27} = 0$$

This looks like a strange thing to do, since it created a degree 6 polynomial. However, we can use the quadratic formula to find the solutions to this:

$$z^3 = \frac{-q + \sqrt{q^2 + \frac{4p^3}{27}}}{2} = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$$

so that the roots of  $z^6 + qz^3 - \frac{p^3}{27}$  are:

$$z = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

and then the roots of  $y^3 + py + q$  are:

$$y = z - \frac{p}{3z} = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} - \frac{p}{3\sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}}$$

and finally, the roots of  $f(x)$  are:

$$x = -\frac{b}{3a} + y = -\frac{b}{3a} + \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} - \frac{p}{3\sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}}$$

This looks like it gives six numbers (one for each square root and cube root). But it actually only produces 3 different numbers.

**Two “Easy” Examples** (already of the form  $y^3 + py + q$ ).

(a) Find the roots of  $y^3 - y + 1$ . Here  $p = -1, q = 1$  and so:

$$y = \sqrt[3]{-\frac{1}{2} + \sqrt{\frac{1}{4} - \frac{1}{27}}} + \frac{1}{3\sqrt[3]{-\frac{1}{2} + \sqrt{\frac{1}{4} - \frac{1}{27}}}}$$

From the positive square root:  $\sqrt{\frac{1}{4} - \frac{1}{27}} \approx 0.46148$  we get:

$$z = \sqrt[3]{-\frac{1}{2} + \sqrt{\frac{1}{4} - \frac{1}{27}}} \approx \sqrt[3]{-0.03852} \approx 0.3377\sqrt[3]{-1}$$

In polar coordinates:

$$z \approx (0.3377; \frac{\pi}{3}), (0.3377; \pi), (0.3377; \frac{5\pi}{3})$$

When we plug into the formula for  $y$  we get the roots:

$$y \approx .6624 - 0.5624i, \quad x \approx -1.325, \quad \text{and } y \approx .6624 + 0.5624i$$

(b) Find the roots of  $y^3 - 2y + 1$ . Here  $p = -2, q = 1$  and so:

$$y = \sqrt[3]{-\frac{1}{2} + \sqrt{\frac{1}{4} - \frac{8}{27}}} + \frac{2}{3\sqrt[3]{-\frac{1}{2} + \sqrt{\frac{1}{4} - \frac{8}{27}}}}$$

Right away we get complex numbers, since  $\frac{1}{4} - \frac{8}{27}$  is negative.

$$z = \sqrt[3]{-\frac{1}{2} + i\sqrt{\frac{8}{27} - \frac{1}{4}}} \approx \sqrt[3]{(0.54433; 2.73521)}$$

This looks nasty! The cube roots are (approximately):

$$(0.8165; 0.9118), (0.8165; 3.0061) \text{ and } (0.8165; 5.1005)$$

and when we plug these in to the formula for  $y$ , we get a surprise!

$$y \approx 0.9999, -1.6180, 0.6180$$

which are familiar **real** numbers. The first is 1 (within margin of error) and the others are (also within margin of error) the golden mean and its conjugate! Looking back at the polynomial, we notice that it factors.

$$y^3 - 2y + 1 = (y - 1)(y^2 + y - 1)$$

so this shouldn't have been a surprise after all.

**Note:** In the first example, only one root was real, while in the second there were three real roots. There is a discriminant to detect this:

**Definition:** The **discriminant** of  $ax^3 + bx^2 + cx + d$  is

$$\Delta = a^4 3^3 2^2 \left( \frac{q^2}{4} + \frac{p^3}{27} \right)$$

and this gets pretty complicated when we substitute for  $a, b, c, d$ :

$$\Delta = 27a^2d^2 - 18abcd + 4ac^3 + 4b^3d - b^2c^2$$

**Corollary 2.3.9.** *If  $ax^3 + bx^2 + cx + d \in \mathbb{Q}[x]$ , then:*

- (i) *if  $\Delta > 0$ , then there are three roots; one real and two complex.*
- (ii) *if  $\Delta = 0$ , then two (or three) roots come together; all are real.*
- (iii) *if  $\Delta < 0$ , then there are three roots; all real.*

**Note:** Unlike the quadratic case, this isn't obvious at all. In fact, it is pretty counterintuitive. When  $\Delta < 0$ , the square root is purely imaginary, which means

that in order to come up with three real roots, we are **forced** to go through the “nastiness” with the complex numbers!

**Proof:** Consider:

$$f(y) = y^3 + py + q$$

the polynomial we got after completing the cube in the cubic formula. Since the roots of the original polynomial are translated by  $-\frac{b}{3a}$  of the roots of  $f(y)$ , we may work with  $f(y)$  instead.

Also, forget about the factor  $a^4 3^3 2^2$ , since it is always a positive number. (This factor is only there to make discriminant look nicer!)

The idea is to study critical points of  $f(y)$ . These are the two solutions to:

$$f'(y) = 3y^2 + p = 0; \quad \text{namely } y = \pm\sqrt{-\frac{p}{3}}$$

Two roots come together when a critical point is **also** a solution of  $f(y) = 0$ . (Exercise!) Substituting  $y = \pm\sqrt{-\frac{p}{3}}$  into  $y^3 + py + q = 0$ , this gives us:

$$\left(\pm\sqrt{-\frac{p}{3}}\right)^3 + p\left(\pm\sqrt{-\frac{p}{3}}\right) + q = 0$$

so

$$q = \mp\frac{2}{3}\sqrt{-\frac{p}{3}} \quad \text{and then} \quad q^2 = -\frac{4p^3}{27}$$

(squaring both sides). But this is exactly what we get when we set  $\Delta = 0$ . It also tells us that  $p \leq 0$  at each critical point (because  $q^2 \geq 0$ ), and so the critical point is always a **real** root (either  $\sqrt{-\frac{p}{3}}$  or  $-\sqrt{-\frac{p}{3}}$ ). This only leaves one more root which has to be real, too, because if it weren't, its complex conjugate would be an additional root (see Proposition 2.3.5).

Next, notice that if  $p \geq 0$  then  $f(y)$  has zero (or one) real critical points, so it is a strictly increasing function, and therefore has only one **real** root! In fact, the only way  $f(y)$  can have three real roots is if  $p < 0$  and if the critical points  $c_1 = -\sqrt{-\frac{p}{3}}$  and  $c_2 = \sqrt{-\frac{p}{3}}$  satisfy  $f(c_1) > 0$  and  $f(c_2) < 0$ . (Think about the graph of  $f(y)$ .)

Substituting into  $f(y)$  (and remembering that  $p < 0$ ), we see that:

$$f(c_1) = -\frac{2p}{3}\sqrt{-\frac{p}{3}} + q > 0 \quad \text{and} \quad f(c_2) = \frac{2p}{3}\sqrt{-\frac{p}{3}} + q < 0$$

both happen exactly when:

$$|q| < \left|\frac{2p}{3}\right|\sqrt{-\frac{p}{3}} \quad \text{and} \quad q^2 < -\frac{4p^3}{27}$$

which is to say, exactly when  $\Delta < 0$ . This the Corollary.

**Examples:** (a)  $x^3 - 3x + 4$  has only one real root because  $\Delta = 324$ .

(b)  $x^3 - 3x + 1$  has three real roots because  $\Delta = -81$ .

(c)  $x^3 - 3x + 2$  has less than three roots because  $\Delta = 0$ .

Just to see that it is possible, here is (without proof):

**The Quartic Formula:** The four roots of:

$$ax^4 + bx^3 + cx^2 + dx + e \in \mathbb{Q}[x]$$

are obtained as follows:

**First Step:** Divide through by  $a$  and complete the **quartic**, to get:

$$y^4 + py^2 + qy + r = 0$$

with the substitutions:

$$y = x + \frac{b}{4a}$$

$$p = \frac{c}{a} - \frac{3b^2}{8a^2}$$

$$q = \frac{d}{a} - \frac{bc}{2a^2} + \frac{b^3}{8a^3}$$

$$r = \frac{e}{a} - \frac{bd}{4} + \frac{b^2c}{16a^3} - \frac{3b^4}{256a^4}$$

**Second Step (a truly inspired guess):** Solve a different cubic(!)

$$g(y) = y^3 - 2py^2 + (p^2 - 4r)y + q^2 = 0$$

with the cubic formula, and let  $s_1, s_2, s_3$  be the roots. Then it turns out that:

$$-\frac{b}{4a} + \frac{\sqrt{-s_1} + \sqrt{-s_2} + \sqrt{-s_3}}{2}, \quad -\frac{b}{4a} + \frac{\sqrt{-s_1} - \sqrt{-s_2} - \sqrt{-s_3}}{2}$$

$$-\frac{b}{4a} - \frac{\sqrt{-s_1} + \sqrt{-s_2} - \sqrt{-s_3}}{2} \quad \text{and} \quad -\frac{b}{4a} - \frac{\sqrt{-s_1} - \sqrt{-s_2} + \sqrt{-s_3}}{2}$$

are the four roots of the original quartic!

**Remark:** This inspired guess is very misleading! It seems to suggest that trickery will allow you to solve high degree polynomials by solving lower degree ones and combining the roots in clever ways. This turns out to be impossible already for degree 5 polynomials, as we will see.

### 2.3.1 Roots Exercises

**7-1** Define the **derivative transformation** on polynomials:

$$\frac{d}{dx} : F[x] \rightarrow F[x] \quad \text{by setting} \quad \frac{dx^n}{dx} = nx^{n-1}$$

By calling it a transformation, I am putting linearity into the definition:

$$\frac{d}{dx}(f + g) = \frac{df}{dx} + \frac{dg}{dx} \quad \text{and} \quad \frac{d}{dx}(kf) = k \frac{df}{dx}$$

(a) Prove Leibniz' rule:

$$\frac{d}{dx}(f \cdot g) = \frac{df}{dx} \cdot g + f \cdot \frac{dg}{dx}$$

Hint: You only need to prove it when  $f(x) = x^n$  and  $g(x) = x^m$ .

(b) Prove that if  $(x - r)^2$  divides  $f(x)$ , then  $r$  is a root of  $f(x)$  **and**  $\frac{df}{dx}(x)$ .

(c) Prove the converse of (b) (see Proposition 2.3.1 (b)).

(d) If  $f(x) \in \mathbb{Q}[x]$  is the characteristic polynomial of  $\alpha$ , prove that  $(x - \alpha)^2$  does not divide  $f(x)$ . (So an algebraic number is never a conjugate of itself.)

Hint: Think about the gcd of  $f(x)$  and of  $\frac{df}{dx}(x)$ .

(e) If  $f(x) \in \mathbb{Q}[x]$  has degree  $n$ , then prove that for each  $x_0 \in \mathbb{Q}$ :

$$f(x) = f(x_0) + \frac{1}{1!} \frac{df}{dx}(x_0)(x - x_0) + \dots + \frac{1}{n!} \frac{d^n f}{dx^n}(x_0)(x - x_0)^n$$

In other words, each polynomial has a Taylor expansion at each  $x_0$ .

Hint: Again, you only need to check it for  $f(x) = x^n$  (see Exercise 5-1).

**7-2** Find **all** of the roots (some only approximate) of:

- (a)  $x^3 + x + 2$       (b)  $x^3 + x - 3$   
 (c)  $x^3 - 3x + 1$       (d)  $x^3 - 3x + 2$   
 (e)  $x^3 + x^2 + x + 1$       (f)  $x^3 + x^2 + x + 2$

**7-3** Find the characteristic polynomials and all conjugates of:

- (a)  $\frac{1-\sqrt{7}}{2}$       (b)  $\frac{1+\sqrt{7}}{2} i$       (c)  $\sqrt[3]{2}$   
 (d)  $\frac{-1+\sqrt[3]{-26}}{3}$       (e)  $\sqrt{2} + \sqrt{3} i$       (f)  $\sqrt{\frac{3+\sqrt{2}}{2}}$

## 2.4 Clock Arithmetic and Finite Fields.

We want to think about roots of prime polynomials in  $\mathbb{Q}[x]$ . An appropriate first question is: “How do we know there are any interesting prime polynomials?” The rational roots test tells us there are lots of polynomials with no rational roots, but that doesn’t tell us the polynomials are prime! We’ll find prime polynomials using finite fields, which are constructed with “clock arithmetic.”

Fix a natural number  $n$ .

**Definition:** Integers  $a$  and  $b$  are **equivalent mod  $n$** , written:

$$a \equiv b \pmod{n}$$

if  $n$  divides  $a - b$ .

First of all, equivalence mod  $n$  is an equivalence relation (see §1.2):

(i) Reflexive:

$$a \equiv a \pmod{n} \text{ because } a - a = 0 \text{ and } n \text{ divides } 0.$$

(ii) Symmetric:

If  $a \equiv b \pmod{n}$ , then  $n$  divides  $a - b$ , which means  $a - b = dn$  for some  $d$ , and then  $b - a = (-d)n$  so  $b \equiv a \pmod{n}$ .

(iii) Transitive:

If  $a \equiv b \pmod{n}$  and  $b \equiv c \pmod{n}$  then  $a - b = dn$  and  $b - c = en$ , so  $a - c = (a - b) + (b - c) = (d + e)n$  and so  $a \equiv c \pmod{n}$ .

**Definition:** We let  $[a]$  be the equivalence class of  $a \pmod{n}$ .

**Remark:** There are  $n$  different equivalence classes:

$$\mathbb{Z}_n = \{[0], [1], [2], \dots, [n - 2], [n - 1]\}$$

since we can always divide by  $n$  to get a remainder between 0 and  $n - 1$ , and two different remainders are never equivalent.

**Definition of “clock” addition and multiplication in  $\mathbb{Z}_n$ :**

$$[a] + [b] = [a + b] \quad \text{and} \quad [a][b] = [ab]$$

**These are well-defined:** If  $a - a' = dn$  and  $b - b' = en$  then:

$$(a + b) - (a' + b') = (a - a') + (b - b') = (d + e)n$$

so addition is well-defined, and:

$$(ab) - (a'b') = (a - a')b + a'(b - b') = dnb + a'en = (db + a'e)n$$

so multiplication is well-defined!

With these definitions, it is obvious that:

- (a) Clock addition is associative and commutative.
- (b)  $[0]$  is the additive identity and  $[-a]$  is the additive inverse of  $[a]$ .
- (c) Clock multiplication is distributive, associative and commutative.
- (d)  $[1]$  is the multiplicative identity.

but there is no cancellation law unless  $n$  is a **prime**.

**Example:** If  $n = 12$  (the “usual” clock on the wall), then:

$$[3][4] = [12] = 0$$

so the cancellation law doesn’t hold! (See Exercise 6-1) In other words, 12-clock arithmetic isn’t an integral domain (see §2.2). However:

**Proposition 2.4.1.**  *$p$ -clock arithmetic is a field:*

$$\mathbb{Z}_p := \{0 = [0], 1 = [1], \dots, [p - 1]\}$$

if  $p$  is a prime number.

**Proof:** Because of (a)-(d) above, we just need to find multiplicative inverses of everything (except 0). We use Propositions 2.2.2 and 2.2.4. Namely, if  $[a] \neq [0]$ , then  $p$  does not divide  $a$  and Proposition 2.2.4 says that 1 is a gcd of  $a$  and  $p$ . Then Proposition 2.2.2 says:

$$1 = up + va$$

for some integers  $u, v$ . But  $1 - va = up$  tells us  $1 \equiv va \pmod{p}$  and so:

$$1 = [1] = [va] = [v][a]$$

That is,  $[v]$  is the multiplicative inverse of  $[a]$ !

**Examples:**

- (a)  $\mathbb{Z}_2 = \{0, 1\}$  and  $[1] + [1] = [2] = [0]$ . Just as before! (See §2.1)
- (b)  $\mathbb{Z}_3 = \{0, 1, [2]\}$  and  $[2] = -1$  in this field. (Compare with Exercise 5-5)
- (c)  $\mathbb{Z}_5 = \{0, 1, [2], [3], [4]\}$  with the following “+” and “ $\times$ ” tables:

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\times$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

So there are fields with any prime  $p$  number of elements. We will later see how to find fields with any **prime power**  $p^n$  number of elements.

Now that we know  $\mathbb{Z}_p$  is a field, we can consider  $\mathbb{Z}_p[x]$ , the set of polynomials with coefficients in  $\mathbb{Z}_p$ . Rather surprisingly, these polynomials will help us to find prime polynomials in  $\mathbb{Q}[x]$ . What's the connection? If we start with a polynomial with integer coefficients:

$$f(x) = a_d x^d + a_{d-1} x^{d-1} + \dots + a_1 x + a_0$$

we can take the equivalence classes of the coefficients to get:

$$[f(x)] = [a_d]x^d + [a_{d-1}]x^{d-1} + \dots + [a_1]x + [a_0]$$

(putting brackets around  $f(x)$  is just a device to shorten the notation). Each  $[f(x)]$  is called **the reduction mod  $p$**  of  $f(x)$ . For example:

$$[px^2 + px + p] = [p]x^2 + [p]x + [p] = [0]x^2 + [0]x + [0] = 0$$

Another example:  $[x^2 + x - 3] = x^2 + x = (x + [1])(x) \in \mathbb{Z}_3[x]$  shows that the reduced polynomial can factor when the original doesn't. On the other hand, if  $f(x)$  factors, then:

$$[f(x)] = [g(x)h(x)] = [g(x)][h(x)]$$

because it makes no difference whether we take the reduction mod  $p$  before or after multiplying the polynomials!

**Gauss's Lemma:** If  $f(x)$  is a polynomial with integer coefficients and

$$f(x) = g(x)h(x) \in \mathbb{Q}[x]$$

then there is a rational number  $\frac{a}{b}$  so that  $\frac{a}{b}g(x)$  and  $\frac{b}{a}h(x)$  both have **integer** coefficients, and of course:

$$f(x) = \left(\frac{a}{b}g(x)\right) \left(\frac{b}{a}h(x)\right)$$

**Proof:** Since the coefficients of  $g(x)$  and  $h(x)$  are rational numbers, we can clear the denominators by multiplying through by some pair of natural numbers  $m$  and  $n$  so that  $mg(x)$  and  $nh(x)$  are polynomials with **integer** coefficients. Then:

$$mnf(x) = (mg(x))(nh(x))$$

is a product of polynomials with integer coefficients. Of course, this isn't what we want. But now suppose  $p$  is a prime and  $p$  divides  $mn$ . Then  $p$  divides all the coefficients of  $mnf(x)$  and so  $mnf(x)$  reduces to the zero polynomial mod  $p$ . But that means:

$$0 = [mg(x)][nh(x)] \in \mathbb{Z}_p[x]$$

Since  $\mathbb{Z}_p[x]$  is an integral domain (see §2.2), it has a cancellation law, which tells us that **either**  $[mg(x)] = 0$  or  $[nh(x)] = 0$  (Exercise 6-1). So  $p$  divides all the

coefficients of  $mg(x)$  or of  $nh(x)$ . **Now divide through by  $p$  and continue.** That is, if  $p$  divides all the coefficients of  $mg(x)$ , change it to  $\frac{m}{p}g(x)$ , otherwise change  $h(x)$  to  $\frac{n}{p}h(x)$ . This gives us two polynomials with integer coefficients whose product is  $\frac{mn}{p}f(x)$ . We can keep doing this, dividing either  $m$  or  $n$  on the right by each of the primes that divide  $mn$  to finally get:

$$f(x) = \left( \frac{m}{p_1 \cdots p_d} g(x) \right) \left( \frac{n}{q_1 \cdots q_e} h(x) \right)$$

with  $mn = p_1 \cdots p_d \cdot q_1 \cdots q_e$  and each of the polynomials on the right side has integer coefficients!

**Example:** Starting with a “silly” factorization  $x^2 - 1 = (\frac{3}{2}x - \frac{3}{2})(\frac{2}{3}x + \frac{2}{3})$ , clear denominators taking  $m = 2$  and  $n = 3$  to get:

$$6(x^2 - 1) = (3x - 3)(2x + 2)$$

Dividing through by  $p = 2$  gives:

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

and dividing through by  $p = 3$  gives:

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

the factorization with integer coefficients.

**Proposition 2.4.2.** *Suppose*

$$f(x) = a_d x^d + \dots + a_0 \in \mathbb{Q}[x]$$

*has integer coefficients, and that  $p$  is a prime that doesn't divide  $a_d$ . Then if  $[f(x)]$  is prime in  $\mathbb{Z}_p[x]$ , it follows that  $f(x)$  is prime in  $\mathbb{Q}[x]$ .*

**Proof:** Since we assume  $p$  doesn't divide  $a_d$ , the reduced polynomial  $[f(x)]$  is a polynomial of degree  $d$  in  $\mathbb{Z}_p[x]$ . If  $f(x) = g(x)h(x)$ , then Gauss' lemma says  $g(x)$  and  $h(x)$  can be replaced by polynomials with integer coefficients (without changing their degrees) and then:  $[f(x)] = [g(x)][h(x)]$ . But if  $[f(x)]$  is prime, then  $[g(x)]$  (or  $[h(x)]$ ) must have degree  $d$ , and then  $g(x)$  (or  $h(x)$ ) must have had degree  $d$ . So  $f(x)$  is prime!

**Example:**  $x^4 + x + 1 = [x^4 + x + 1]$ , is prime in  $\mathbb{Z}_2[x]$  (Exercise 5.4). It follows that this polynomial, as well as each of the polynomials:

$$3x^4 + 2x^2 + 6x^2 + 7x + 5, \quad 5x^4 + 9x - 1, \quad 17x^4 - 2x^3 - 21x - 39$$

and indeed any polynomial with integer coefficients of the form:

$$(\text{odd})x^4 + (\text{even})x^3 + (\text{even})x^2 + (\text{odd})x + (\text{odd})$$

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

**Remark:** This gives us infinitely many prime polynomials in  $\mathbb{Q}[x]$  with integer coefficients starting with a single prime polynomial in  $\mathbb{Z}_p[x]$ . We know that there are prime polynomials of larger and larger degrees in  $\mathbb{Z}_p[x]$ , by Euclid's theorem, so we know there are prime polynomials in  $\mathbb{Q}[x]$  of larger and larger degrees. But it can be hard to use this to check whether a **given** polynomial is prime! For example, is  $x^n - 2$  prime? It certainly isn't prime in  $\mathbb{Z}_2[x]$ . Is it prime in  $\mathbb{Z}_3[x]$ ? In  $\mathbb{Z}_5[x]$ ?

**Eisenstein's Criterion:** If

$$f(x) = a_d x^d + a_{d-1} x^{d-1} + \dots + a_1 x + a_0$$

is a polynomial with integer coefficients, and  $p$  is a prime such that:

- (i)  $p$  divides each of the coefficients  $a_{d-1}, a_{d-2}, \dots, a_1, a_0$ .
- (ii)  $p$  doesn't divide  $a_d$ .
- (iii)  $p^2$  doesn't divide  $a_0$ .

Then  $f(x)$  is prime in  $\mathbb{Q}[x]$ .

**Proof:** If  $f(x) = g(x)h(x)$ , then by Gauss's Lemma we can assume  $g(x)$  and  $h(x)$  have integer coefficients. Properties (i) and (ii) above tell us that  $[f(x)] = [a_d]x^d \in \mathbb{Z}_p[x]$  since all the other coefficients are divisible by  $p$ . But then it follows from the unique factorization in the fundamental theorem of arithmetic (§2.2) that  $[g(x)] = [b_m]x^m$  and  $[h(x)] = [c_n]x^n$ . If  $m$  and  $n$  are both positive, this means in particular that  $p$  divides the constant terms of both  $g(x)$  and  $h(x)$ . But this would imply that  $p^2$  divides the constant term of  $f(x)$ , violating (iii). Thus either  $m = 0$  or  $n = 0$ , which is to say either  $n = d$  or  $m = d$ , telling us that either  $g(x)$  or  $h(x)$  has degree  $d$ , hence  $f(x)$  is prime!

**Example:**  $x^n - 2$  is always prime in  $\mathbb{Q}[x]$ .

Use the criterion for  $p = 2$ . (This also shows that every  $x^n - p$  is prime.)

**Remark:** Eisenstein's criterion was designed to prove that a certain kind of polynomial, the "cyclotomic" polynomial is prime. Namely:

**Corollary 2.4.3.** *If  $p$  is a prime number, then:*

$$f(x) = x^{p-1} + x^{p-2} + \dots + x + 1 = \frac{x^p - 1}{x - 1}$$

*is a prime polynomial.*

**Proof:** Obviously Eisenstein's criterion doesn't apply to  $f(x)$ . Instead, we will apply it to the polynomial  $f(x+1)$ . Notice that any factorization of  $f(x)$ :

$$f(x) = g(x)h(x)$$

gives a factorization of  $f(x+1)$ :

$$f(x+1) = g(x+1)h(x+1)$$

and vice versa, so that if we want to see that  $f(x)$  is prime, we may instead prove that  $f(x+1)$  is prime!

By Exercise 5-1, we know that:

$$(x+1)^p = x^p + \frac{p!}{(p-1)!1!}x^{p-1} + \frac{p!}{(p-2)!2!}x^{p-2} + \dots + \frac{p!}{1!(p-1)!}x + 1$$

from which we get:

$$f(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1} = x^{p-1} + \frac{p!}{(p-1)!1!}x^{p-2} + \dots + \frac{p!}{2!(p-2)!}x + \frac{p!}{1!(p-1)!}$$

But now Eisenstein's criterion does apply!

(i)  $p$  divides  $p!$  (of course), which we can rewrite as:

$$p! = \left( \frac{p!}{(p-n)!n!} \right) (p-n)!n!$$

and as long as  $p-n$  and  $n$  are both less than  $p$ , then  $p$  cannot divide  $(p-n)!n!$  because  $p$  is bigger than all the prime factors. So  $p$  divides:

$$\frac{p!}{(p-n)!n!}$$

which are all the coefficients of  $f(x+1)$  (except the first one).

(ii) The leading coefficient of  $f(x+1)$  is 1 and  $p$  doesn't divide 1.

(iii) The last coefficient is  $\frac{p!}{1!(p-1)!} = p$ , and  $p^2$  doesn't divide  $p$ .

So Eisenstein's criterion applies, and  $f(x+1)$  (and  $f(x)$ ) is prime.

**Examples:** (a) ( $p=3$ ):  $f(x) = x^2 + x + 1$  is prime and:

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

(b) ( $p=5$ ):  $f(x) = x^4 + x^3 + x^2 + x + 1$  is prime and:

$$f(x+1) = x^4 + 5x^3 + 10x^2 + 10x + 5$$

(c) On the other hand,  $f(x) = x^3 + x^2 + x + 1 = (x+1)(x^2 + 1)$  and:

$$f(x+1) = x^3 + 4x^2 + 6x + 4$$

(What went wrong? Well, 4 isn't a prime, so Eisenstein's criterion fails!)

In fact, one can prove that:

$$x^{n-1} + x^{n-2} + \dots + x + 1$$

is **only** a prime polynomial when  $n$  is a prime number.

### 2.4.1 Clock Arithmetic and Finite Fields Exercises

**8-1** Write addition and multiplication tables for the following fields:

- (a)  $\mathbb{Z}_7$    (b)  $\mathbb{Z}_{11}$    (c)  $\mathbb{Z}_{13}$

**8-2** (a) Prove that if  $n$  isn't prime, then  $\mathbb{Z}_n$  isn't a domain.

(b) Prove that if 1 is a gcd of  $a$  and  $n$ , then  $[a]$  has a multiplicative inverse in  $\mathbb{Z}_n$  (and we'll call  $[a]$  a unit even when  $\mathbb{Z}_n$  isn't a domain).

(c) Find every unit in  $\mathbb{Z}_{48}$  and its multiplicative inverse.

(d) Find the multiplicative inverse of  $[1027]$  in  $\mathbb{Z}_{20317}$ .

**8-3** Prove that if  $n$  isn't a prime number, then:

$$x^{n-1} + x^{n-2} + \dots + 1 \text{ isn't a prime polynomial}$$

**8-4** Decide whether the following polynomials are prime in  $\mathbb{Q}[x]$  or not. If not, factor them. If prime, explain how you came to that conclusion (Eisenstein's criterion, rational root test or Proposition 2.4.2)

- (a)  $x^3 + 2x + 4$   
 (b)  $x^4 + 3x^2 + 3$   
 (c)  $x^4 + 3x^3 + 9$   
 (d)  $x^4 + 6x^2 + 9$   
 (e)  $x^5 + 5x^4 + 10x^3 + 10x^2 + 5x + 1$   
 (f)  $x^6 + 3x^4 + 3x^2 + 1$   
 (g)  $x^6 + x^3 + 1$

**8-5** For which primes  $p$  is  $[x^2 + 1] \in \mathbb{Z}_p[x]$  prime? For example:

In  $\mathbb{Z}_2[x]$ , it isn't prime:  $[x + 1]^2 = [x^2 + 1]$ .

In  $\mathbb{Z}_3[x]$ , it is prime (Exercises 6).

In  $\mathbb{Z}_5[x]$ , it isn't prime:  $[x - 2][x - 3] = [x^2 - 5x + 6] = [x^2 + 1]$ .

What about in  $\mathbb{Z}_7[x], \mathbb{Z}_{11}[x], \mathbb{Z}_{13}[x], \mathbb{Z}_{17}[x], \mathbb{Z}_{19}[x]$ ?

Do you see a pattern?

## 2.5 The Fundamental Theorem of Algebra.

We've seen formulas for the roots of quadratic, cubic and quartic polynomials. It is then reasonable to ask: "Do all the polynomials with rational (or complex) coefficients have complex roots?", and if this is true, then: "Are there formulas for the roots of polynomials in all degrees?"

**The Fundamental Theorem of Algebra:** All the non-constant polynomials in  $\mathbb{C}[x]$  have complex roots.

So the answer to the first question is "yes." But the answer to the second question turns out to be "no:"

**Abel's Theorem:** There is no formula that will produce the complex roots of every polynomial of any degree  $\geq 5$ .

So there are no general formulas. But the word "every" in the statement of the theorem is important. Obviously **some** polynomials, like  $x^n - 2$ , **do** have roots that are given by a formula. This makes the following refinement, due to Galois, extremely interesting.

**Galois' Theorem:** There is a group of symmetries attached to each prime polynomial in  $\mathbb{Q}[x]$  that explains whether or not there is a formula for its roots.

The Theorems of Abel and Galois are not easy to prove! In this section, we will focus on the Fundamental Theorem of Algebra, and provide a proof that uses a bit of mathematical analysis:

**Proof of the Fundamental Theorem of Algebra:** Given  $f(x) \in \mathbb{C}[x]$ , let  $f(z)$  be the same polynomial thought of as a **function** of a complex variable  $z$ . The graph of:

$$f(z) : \mathbb{C} \rightarrow \mathbb{C}$$

is hard to visualize, since it lives in  $\mathbb{C}^2 = \mathbb{R}^4$ , so instead we'll look at:

$$|f(z)| : \mathbb{C} \rightarrow \mathbb{R}$$

which we **can** visualize, as its graph lives in  $\mathbb{R}^3$ . We will write  $z = s + ti$  and  $|f(z)| = u$ , so that the coordinates on  $\mathbb{R}^3$  are  $(s, t, u)$ .

**Examples:**

- (a) For constants  $f(x) = a$ , the graph is the horizontal plane  $u = |a|$ .
- (b) If  $f(x) = x$ , the graph is  $u = \sqrt{s^2 + t^2}$ , and squaring gives:

$$u^2 = s^2 + t^2$$

The graph is (the upper half of) a cone with vertex at the origin.

More generally, the graphs  $u = |az + b|$  for linear functions  $f(x) = ax + b$  are all (upper parts of) cones with vertex at  $(|-\frac{b}{a}|, 0)$  ( $-b/a$  is a complex number!).

These cones are good examples of graphs of functions that are continuous, but not differentiable (at the vertex).

(c) If  $f(x) = x^2$ , then  $|f(z)| = |(s + ti)|^2 = s^2 + t^2$ , so the graph is:

$$u = s^2 + t^2$$

which is a paraboloid meeting the  $st$ -plane at the origin.

On the other hand, the graph of

$$|z^2 - 1| = |z - 1| \cdot |z + 1|$$

is not a translated paraboloid. It has two points of intersection with the  $st$ -plane, namely the points  $(1, 0, 0)$  and  $(-1, 0, 0)$ , and very near these points, the graph looks like a cone. Thus this function, too, is not differentiable at these two points.

**Back to the Proof:** The function  $|f(z)|$  is continuous everywhere. If  $f(x)$  has a root  $\alpha$ , then  $|f(\alpha)| = 0$  is a (global) minimum for the function  $|f(z)|$ , since the absolute value is non-negative. Thus proving that there are roots of  $f(x)$  is the same thing as proving that  $|f(z)|$  has global minimum equal to 0. We will prove that such minima occur, if the polynomial is not a constant. Let's write:

$$f(x) = a_d x^d + a_{d-1} x^{d-1} + \dots + a_0$$

Then the proof follows from:

**A couple of analytic observations:**

(a) If  $f(x)$  is not constant, then on **circles**  $C \subset \mathbb{C}$  centered at 0 of big enough radius,

$$|f(z)| > |f(0)| \text{ for all } z \in C$$

We'll prove this below. But first recall that the **disc**  $D$  consisting of  $C$  together with all the interior points of  $C$  is **compact**, and that the continuous function:

$$|f(z)| : D \rightarrow \mathbb{R}$$

must therefore have maximum and minimum values somewhere in  $D$ . The maxima can (and do) live on  $C$ , which is the boundary of  $D$ , without being local maxima of  $|f(z)|$ , but for any  $C$  satisfying (a), we know that:

$$|f(0)| < |f(z)| \text{ for all points } z \in C$$

so all global minima must be in the **interior** of  $D$ , and therefore they must also be **local** minima of the function  $|f(z)|$ . But I claim:

(b) All the local minima of  $|f(z)|$  satisfy  $|f(\alpha)| = 0$ .

Putting these together, (a) says there **must** be minima in the interior of big enough circles, and (b) says that each minimum value of the function is 0, so

each  $\alpha \in \mathbb{C}$  that realizes the minimum must satisfy  $|f(\alpha)| = 0$ . That is,  $\alpha$  is a root!

So we have to prove (a) and (b). The key is to think about limits. These are “large” limits: the behavior of  $f(z)$  for large values of  $|z|$ , and “small” limits: the behavior of  $f(z)$  very close to a fixed  $z_0 \in \mathbb{C}$ .

**Large Limits:**  $f(z) = a_d z^d + \dots + a_0$  “grows like”  $a_d z^d$  for large  $z$ .

**Small Limits:**  $f(z)$  has Taylor expansions (Exercise 7-1):

$$f(z) = f(z_0) + b_1(z - z_0) + \dots + b_d(z - z_0)^d$$

where

$$b_k = \frac{f^{(k)}(z_0)}{k!}$$

and then  $f(z)$  “looks like”  $f(z_0) + b_k(z - z_0)^k$  when  $z$  is close to  $z_0$ , and  $f^{(k)}(z_0)$  is the first non-zero derivative.

To make all this precise, we need the **triangle inequality**:

$$|z + w| \leq |z| + |w| \quad \text{or (setting } v = z + w) \quad |v| \leq |v - w| + |w|$$

which it is convenient to rewrite as:

$$|w| \geq |v| - |v - w| = |v| - |w - v|$$

**Proof of (a):** By the triangle inequality:

$$|f(z)| \geq |a_d z^d| - |f(z) - a_d z^d| = |a_d| R^d - |a_{d-1} z^{d-1} + \dots + a_0|$$

and also by the triangle inequality:

$$|a_{d-1} z^{d-1} + \dots + a_0| \leq |a_{d-1} z^{d-1}| + \dots + |a_0|$$

so putting this all together, we get:

$$|f(z)| \geq |a_d| R^d - |a_{d-1}| R^{d-1} - \dots - |a_0|$$

whenever  $|z| = R$ . i.e.  $z$  is on the circle of radius  $R$  centered at 0. We conclude from this that when  $R$  is very large,  $|f(z)|$  grows like  $|a_d| R^d$ , and so can be made as large as we please. But let's be very precise about this. Take  $R > 1$  and also:

$$R > \frac{|a_{d-1}| + \dots + |a_0| + |f(0)|}{|a_d|}$$

Then:

$$\begin{aligned} |a_d| R^d &= (|a_d| R) R^{d-1} \\ &> (|a_{d-1}| + \dots + |a_0| + |f(0)|) R^{d-1} \\ &= |a_{d-1}| R^{d-1} + |a_{d-2}| R^{d-1} + \dots + |a_0| R^{d-1} + |f(0)| R^{d-1} \\ &> |a_{d-1}| R^{d-1} + |a_{d-2}| R^{d-2} + \dots + |a_0| + |f(0)| \end{aligned}$$

(because we made sure that  $R > 1$ ) so

$$|f(z)| \geq |a_d|R^d - |a_{d-1}|R^{d-1} - \dots - |a_0| > |f(0)|$$

when  $|z| = R$ .

**Example:** Consider the polynomial

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

In this case  $|f(0)| = 1$ , and the proof above tells us that if:

$$R > \frac{2 + 1 + 1}{3} = \frac{4}{3}$$

then  $|f(z)| > 1$  whenever  $|z| = R > 4/3$ . In particular, notice that this tells us that any roots of  $f(x)$  must be inside the disc of radius  $4/3$ ! Exercise 9-1 gives an even better estimate.

**Proof of (b):** Let  $b_k$  be a complex number other than zero, and consider the function (of the variable  $z$ ):

$$|f(z_0) + b_k(z - z_0)^k|$$

We can solve  $b_k(z - z_0)^k = w$  for **any** complex number  $w$  by taking

$$z = \sqrt[k]{\frac{w}{b_k}} + z_0$$

(for any of the  $k$ th roots of  $w/b_k$ ) so if  $f(z_0) \neq 0$ , we can be very clever and choose  $w = -rf(z_0)$  for some real number  $r < 1$  and solve:

$$z = \sqrt[k]{\frac{-rf(z_0)}{b_k}} + z_0$$

to conclude that:

$$|f(z_0) + b_k(z - z_0)^k| = |f(z_0) - rf(z_0)| = (1 - r)|f(z_0)| < |f(z_0)|$$

In other words, we've shown that if  $|f(z_0)| > 0$ , then  $z_0$  is **not** a minimum of the function:

$$|f(z_0) + b_k(z - z_0)^k|$$

Now we turn to the function we're really interested in:

$$|f(z)| = |f(z_0) + b_k(z - z_0)^k + \dots + b_d(z - z_0)^d|$$

(the Taylor series of  $f(z)$ , where I've deleted all the zero coefficients). The idea is that if we make  $|z - z_0|$  small enough, and  $r$  small enough, then we come to the same conclusion:  $z_0$  is not a local minimum because there are nearby values of  $z$  with smaller values of  $|f(z)|$ !

Precisely, we will choose  $r$  satisfying:

$$\sqrt[k]{\frac{r|f(z_0)|}{|b_k|}} < \frac{|b_k|}{|b_{k+1}| + \dots + |b_d|}$$

or, in other words:

$$r < \left( \frac{|b_k|}{|b_{k+1}| + \dots + |b_d|} \right)^k \frac{|b_k|}{|f(z_0)|}$$

and as in the previous page, we solve:

$$z = \sqrt[k]{\frac{-rf(z_0)}{b_k}} + z_0$$

and conclude that:

$$|z - z_0| = \left| \sqrt[k]{\frac{-rf(z_0)}{b_k}} \right| < \frac{|b_k|}{|b_{k+1}| + \dots + |b_d|}$$

and we will additionally choose the  $r$  small enough to guarantee that  $|z - z_0| < 1$ . Now we use the triangle inequality and our inequalities:

$$\begin{aligned} |f(z)| &\leq |f(z_0) + b_k(z - z_0)^k| + |b_{k+1}||z - z_0|^{k+1} + \dots + |b_d||z - z_0|^d \\ &= (1 - r)|f(z_0)| + |z - z_0|^{k+1} (|b_{k+1}| + \dots + |b_d||z - z_0|^{d-k-1}) \\ &< (1 - r)|f(z_0)| + |z - z_0|^{k+1} (|b_{k+1}| + \dots + |b_d|) \\ &= (1 - r)|f(z_0)| + \frac{r|f(z_0)|}{|b_k|} |z - z_0| (|b_{k+1}| + \dots + |b_d|) \\ &< (1 - r)|f(z_0)| + \frac{r|f(z_0)|}{|b_k|} \frac{|b_k|}{|b_{k+1}| + \dots + |b_d|} (|b_{k+1}| + \dots + |b_d|) \\ &= |f(z_0)| - r|f(z_0)| + r|f(z_0)| \\ &= |f(z_0)| \end{aligned}$$

to get exactly what we need to complete the proof of the Theorem!

With all big proofs, it is useful to play the devil's advocate and think about settings where the proof couldn't possibly work, because it would prove something false. When you construct your own proofs, this is a good way to detect errors. (If it does prove something false, there must be something wrong with the proof!) But even here, where there are no errors, playing the devil's advocate is useful for exploring the proof.

**Devil's Advocate 1:** This shouldn't prove that there are **real** roots because, for example, the polynomial  $x^2 + 1$  does not have real roots. So what happens to the proof when we replace  $\mathbb{C}$  by  $\mathbb{R}$ ? Well, (a) still works, except that in this case a "circle"  $C$  of radius  $R$  is just the pair of points  $R, -R \in \mathbb{R}$ . So there must be a global minimum of  $|x^2 + 1|$  inside each interval  $[-R, R]$  (and  $R$  large). But (b) fails (obviously) since 1 (not 0) is the global minimum for  $|x^2 + 1|$ . When we investigate the proof, we see that in (b), we assumed we could always solve:

$$z = \sqrt[k]{\frac{-r f(z_0)}{b_k}} + z_0$$

In this case, when  $x_0 = 0$ ,  $f(0) = 1$  and  $b_2 = 1$ , we are asking to solve:

$$x = \sqrt[2]{-r}$$

which **can't be done** when  $x$  is real, though of course it can be done when  $x$  is complex! This is why our proof does not (wrongly!) prove that polynomials always have real roots.

**Devil's Advocate 2:** What about the exponential function from §4?:

$$e^z = e^{x+iy} = e^x e^{iy}$$

We saw that  $e^{iy} = \cos(y) + \sin(y) i$  so:

$$|e^z| = |e^x| |e^{iy}| = e^x (\cos^2(y) + \sin^2(y)) = e^x$$

and this function has **no** "roots." In this case, part (b) of the proof still holds (it only required  $e^z$  to have a Taylor series expansion!) and  $|e^z|$  has no local (or global) minima inside the disk, but (a) doesn't hold! In fact,

$$|e^z| = e^x$$

gets very **small** on the points of large circles with "large" negative  $x$ -coordinates. So on **every** disc  $D$ , the global minima of  $|e^z|$  occur on the boundary circle  $C$ !

## 2.5.1 Fundamental Theorem of Algebra Exercises

**9-1** Prove that **every** complex root  $\alpha$  of:

$$f(x) = a_d x^d + \dots + a_0$$

satisfies

$$|\alpha| \leq \frac{|a_{d-1}| + \dots + |a_0|}{|a_d|} \text{ or } |\alpha| < 1$$

(Hint: You need to modify the proof of (a), replacing  $|f(0)|$  with 0)

**9-2** Taylor expand the following polynomials about  $x = -1$ :

- (a)  $x^2 + 2x + 2$
- (b)  $x^3 + 3x^2 + 3x + 3$
- (c)  $x^3 + 4x^2 + 5x + 4$
- (d)  $x^5 + 1$

Which of these polynomials, thought of as a function  $f : \mathbb{R} \rightarrow \mathbb{R}$ , has a global minimum at  $x = -1$ ? Which has a local minimum at  $x = -1$ ? Which has a critical point at  $x = -1$ ?

**9-3** Consider the polynomial:

$$x^2 + 1 \in F_2[x]$$

and attempt a “Taylor expansion” of it at  $x = 1$ . What happens?

**9-4** Use the fundamental theorem to prove:

(a) Every prime polynomial in  $\mathbb{Q}[x]$  of degree  $d$  has  $d$  **different** complex roots. (See also Exercise 7-1(d)). So if the characteristic polynomial of  $\alpha$  has degree  $d$ , then  $\alpha$  has  $d - 1$  conjugates.

(b) The **only** prime polynomials in  $\mathbb{C}[x]$  are the linear polynomials.

(c) The **only** prime polynomials in  $\mathbb{R}[x]$  are the linear polynomials and quadratic polynomials  $ax^2 + bx + c$  with  $b^2 - 4ac < 0$ .

**9-5** Prove the triangle inequality:

$$|z + w| \leq |z| + |w|$$

for complex numbers  $z, w$ .



## Chapter 3

# Symmetries

Symmetries are linear transformations of a vector space, so we will begin with a review of some linear algebra. In a basic linear algebra course, the scalars are real numbers, but here they might belong to any field. Each **algebraic number** (root of a polynomial with rational number coefficients) comes equipped with a multiplication transformation, which is a symmetry whose characteristic polynomial is the polynomial that gave birth to the algebraic number in the first place. The **constructible numbers** (numbers that can be constructed using only a compass and straightedge) are particular algebraic numbers that were of great interest to the ancients, and we will use linear algebra to understand them in some detail. Symmetries come in **groups**, and finite symmetry groups are always subgroups of **permutation** groups. There is a qualitative difference between permutation groups of 4 or less objects versus permutation groups of 5 or more objects, which we will explore. Finally, we will look at the **Galois group** of symmetries of the “splitting field” of an algebraic number, which is one of the most interesting objects in all of mathematics.

### 3.1 Linear Algebra

Start with a field  $F$  (this will be the field of **scalars**).

**Definition:** A **vector space over  $F$**  is a set  $V$  with a vector addition and scalar multiplication (“scalars” in  $F$  times “vectors” in  $V$ ) so that:

- (a) Vector addition is associative and commutative.
- (b) There is an additive identity vector, denoted  $0$ , or sometimes  $\vec{0}$ .
- (c) Every vector  $\vec{v}$  has an additive inverse vector  $-\vec{v}$ .
- (d) Scalar multiplication distributes with vector addition.
- (e) If  $c, k \in F$  are scalars and  $\vec{v} \in V$  is a vector, then  $c(k\vec{v}) = (ck)\vec{v}$ .
- (f) If  $1 \in F$  is the multiplicative identity, then  $1\vec{v} = \vec{v}$  for all  $\vec{v}$ .

**Examples:** (a)  $F^n$  is the standard finite-dimensional vector space of  $n$ -tuples of elements of  $F$ . Vectors  $\vec{v} \in F^n$  will be written vertically:

$$\vec{v} = \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix}, \quad \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix} + \begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{bmatrix} = \begin{bmatrix} v_1 + w_1 \\ v_2 + w_2 \\ \vdots \\ v_n + w_n \end{bmatrix}, \quad k \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix} = \begin{bmatrix} kv_1 \\ kv_2 \\ \vdots \\ kv_n \end{bmatrix}$$

(b) If  $F \subset D$  and  $D$  is a commutative ring with 1, then  $D$  is a vector space over  $F$ . The scalar multiplication is ordinary multiplication in  $D$ , and property (e) is the associative law for multiplication in  $D$ . Thus, for example, vector spaces over  $\mathbb{Q}$  include  $\mathbb{R}, \mathbb{C}, \mathbb{Q}[x]$  and  $\mathbb{Q}(x)$ .

**Definition:** A **basis** of a vector space  $V$  is a set of vectors  $\{\vec{v}_i\}$  that:

- (i) **Span.** Every vector is a linear combination of the  $\vec{v}_i$ :

$$\vec{v} = k_1\vec{v}_1 + \dots + k_n\vec{v}_n$$

and

- (ii) **Are Linearly Independent.** The only way:

$$k_1\vec{v}_1 + \dots + k_n\vec{v}_n = 0$$

is if all the scalars  $k_1, \dots, k_n$  are zero.

**Proposition 3.1.1.** *If  $\{\vec{v}_1, \dots, \vec{v}_n\}$  is a basis of  $V$ , then every vector  $\vec{v} \in V$  is a **unique** scalar linear combination of the basis vectors:*

$$\vec{v} = k_1\vec{v}_1 + \dots + k_n\vec{v}_n$$

*and any other basis  $\{\vec{w}_i\}$  of  $V$  must also consist of a set of  $n$  vectors. The number  $n$  is called the **dimension** of the vector space  $V$  over  $F$ .*

**Proof:** Since the  $\{\vec{v}_i\}$  span, each vector  $\vec{v}$  has at least one expression as a linear combination of the  $\vec{v}_i$ , and if there are two:

$$\vec{v} = k_1\vec{v}_1 + \dots + k_n\vec{v}_n \text{ and } \vec{v} = l_1\vec{v}_1 + \dots + l_n\vec{v}_n$$

then subtracting them gives:  $0 = (k_1 - l_1)\vec{v}_1 + \dots + (k_n - l_n)\vec{v}_n$ . But then each  $k_i = l_i$  because the  $\{\vec{v}_i\}$  are linearly independent, and thus the two linear combinations are the same. This gives uniqueness.

Now take another basis  $\{\vec{w}_i\}$  and solve:  $\vec{w}_1 = b_1\vec{v}_1 + \dots + b_n\vec{v}_n$ . We can assume (reordering the  $\vec{v}_i$  if necessary) that  $b_1 \neq 0$ . Then:

$$\vec{v}_1 = \frac{1}{b_1}\vec{w}_1 - \frac{b_2}{b_1}\vec{v}_2 - \dots - \frac{b_n}{b_1}\vec{v}_n$$

and then  $\{\vec{w}_1, \vec{v}_2, \dots, \vec{v}_n\}$  is another basis of  $V$  because every

$$\vec{v} = k_1\vec{v}_1 + \dots + k_n\vec{v}_n = k_1\left(\frac{1}{b_1}\vec{w}_1 - \frac{b_2}{b_1}\vec{v}_2 - \dots - \frac{b_n}{b_1}\vec{v}_n\right) + k_2\vec{v}_2 + \dots + k_n\vec{v}_n$$

so the vectors span  $V$ , and the only way:

$$0 = k_1\vec{w}_1 + \dots + k_n\vec{v}_n = k_1(b_1\vec{v}_1 + \dots + b_n\vec{v}_n) + k_2\vec{v}_2 + \dots + k_n\vec{v}_n$$

is if  $k_1b_1 = 0$  (so  $k_1 = 0$ ) and each  $k_1b_i + k_i = 0$  (so each  $k_i = 0$ , too!)

Similarly we can replace each  $\vec{v}_i$  with a  $\vec{w}_i$  to get a sequence of bases:  $\{\vec{w}_1, \vec{w}_2, \vec{v}_3, \dots, \vec{v}_n\}, \{\vec{w}_1, \vec{w}_2, \vec{w}_3, \vec{v}_4, \dots, \vec{v}_n\}$ , etc. If there were **fewer** of the  $\vec{w}_i$  basis vectors than  $\vec{v}_i$  basis vectors we would finish with a basis:

$$\{\vec{w}_1, \dots, \vec{w}_m, \vec{v}_{m+1}, \dots, \vec{v}_n\}$$

which is impossible, since  $\{\vec{w}_1, \dots, \vec{w}_m\}$  is already a basis! Similarly, reversing the roles of the  $\vec{v}_i$ 's and  $\vec{w}_i$ 's, we see that there cannot be fewer  $\vec{v}_i$ 's than  $\vec{w}_i$ 's. So there must be the same number of  $\vec{w}_i$ 's as  $\vec{v}_i$ 's!

**Examples:**

(a)  $F^n$  has  $n$  "standard" basis vectors:

$$\vec{e}_1 = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \vec{e}_2 = \begin{bmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix}, \dots, \vec{e}_n = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix}$$

(b)  $\mathbb{R}^1$  is the line,  $\mathbb{R}^2$  is the plane, and  $\mathbb{R}^3$  is space.

(c)  $\mathbb{C}$  has basis  $\{1, i\}$  as a vector space over  $\mathbb{R}$ .

(d)  $\mathbb{Q}[x]$  has infinite basis  $\{1, x, x^2, x^3, \dots\}$  as a vector space over  $\mathbb{Q}$ .

(e) It is hard to even imagine a basis for  $\mathbb{R}$  as a vector space over  $\mathbb{Q}$ .

(f) Likewise it is hard to imagine a basis for  $\mathbb{Q}(x)$  over  $\mathbb{Q}$ .

We can create vector spaces with **polynomial clock arithmetic**. Given

$$f(x) = x^d + a_{d-1}x^{d-1} + \dots + a_0 \in F[x]$$

we first define the “mod  $f(x)$ ” equivalence relation by setting

$$g(x) \equiv h(x) \pmod{f(x)}$$

if  $g(x) - h(x)$  is divisible by  $f(x)$ , and then the “polynomial clock”:

$$F[x]_{f(x)} = \{[g(x)]\}$$

is the set of “mod  $f(x)$ ” equivalence classes.

**Proposition 3.1.2.** *The polynomial clock  $F[x]_{f(x)}$  is a commutative ring with 1 and a vector space over  $F$  with basis:*

$$\{[1], [x], \dots, [x^{d-1}]\}$$

and if  $f(x)$  is a **prime** polynomial, then the polynomial clock is a field.

**Proof:** Division with remainders tells us that in every equivalence class there is a “remainder” polynomial  $r(x)$  of degree  $< d$ . This tells us that the vectors:

$$[1], [x], [x^2], \dots, [x^{d-1}] \in F[x]_{f(x)}$$

span the polynomial clock. They are linearly independent since if:

$$b_{d-1}[x^{d-1}] + \dots + b_0[1] = 0$$

then  $r(x) = b_{d-1}x^{d-1} + \dots + b_0$  is divisible by  $f(x)$ , which is impossible (unless  $r(x) = 0$ ) because  $f(x)$  has larger degree than  $r(x)$ .

The addition and multiplication are defined as in the ordinary clock arithmetic (and are shown to be well-defined in the same way, see §8). As in the ordinary (integer) clock arithmetic, if  $[r(x)]$  is a non-zero remainder polynomial and  $f(x)$  is **prime**, then 1 is a gcd of  $f(x)$  and  $r(x)$ , and we can solve:

$$1 = r(x)u(x) + f(x)v(x)$$

and then  $[u(x)]$  is the multiplicative inverse of  $[r(x)]$ .

**Example:** We saw that  $x^2 + x + 1 \in F_2[x]$  is prime. From this, we get  $\{[1], [x]\}$  as the basis of the polynomial clock defined by  $x^2 + x + 1$ , which is a vector space over  $F_2$  of dimension 2 and a field with 4 elements (removing the cumbersome brackets):

$$0, 1, x, x + 1$$

Let’s write down the multiplication and addition laws for this field. Notice that this is **not**  $\mathbb{Z}_4$  ( $\mathbb{Z}_4$  isn’t a field!). We’ll call this field  $F_4$ :

+	0	1	$x$	$x+1$
0	0	1	$x$	$x+1$
1	1	0	$x+1$	$x$
$x$	$x$	$x+1$	0	1
$x+1$	$x+1$	$x$	1	0

$\times$	0	1	$x$	$x+1$
0	0	0	0	0
1	0	1	$x$	$x+1$
$x$	0	$x$	$x+1$	1
$x+1$	0	$x+1$	1	$x$

Next recall that an algebraic number  $\alpha$  is a complex root of a prime polynomial:

$$f(x) = x^d + a_{d-1}x^{d-1} + \dots + a_d \in \mathbb{Q}[x]$$

We claim next that via  $\alpha$ , the polynomial  $f(x)$ -clock can be regarded as a **subfield** of the field  $\mathbb{C}$  of complex numbers. In fact:

**Proposition 3.1.3.** *Suppose  $F \subset \mathbb{C}$  is a subfield and  $\alpha \in \mathbb{C}$  is a root of a prime polynomial:*

$$f(x) = x^d + a_{d-1}x^{d-1} + \dots + a_0 \in F[x]$$

*Then the  $f(x)$ -clock becomes a subfield of  $\mathbb{C}$  when we set  $[x] = \alpha$ . This subfield is always denoted by  $F(\alpha)$ , and it sits between  $F$  and  $\mathbb{C}$ :*

$$F \subset F(\alpha) \subset \mathbb{C}$$

**Proof:** The  $f(x)$ -clock is set up so that:

$$[x]^d + a_{d-1}[x]^{d-1} + \dots + a_0 = 0$$

But if  $\alpha \in \mathbb{C}$  is a root of  $f(x)$ , then it is also true that

$$\alpha^d + a_{d-1}\alpha^{d-1} + \dots + a_0 = 0$$

so setting  $[x] = \alpha$  is a well-defined substitution, and because  $f(x)$  is prime, it follows that the clock becomes a subfield of  $\mathbb{C}$ .

**Examples:** We can give multiplication tables for clocks by just telling how to multiply the basis elements of the vector spaces:

(a)  $F = \mathbb{R}$  and  $f(x) = x^2 + 1$ . The  $x^2 + 1$ -clock has table:

$\times$	1	$x$
1	1	$x$
$x$	$x$	-1

On the other hand,  $\mathbb{R}(i)$  and  $\mathbb{R}(-i)$  have multiplication tables:

$\times$	1	$i$	and	$\times$	1	$-i$
1	1	$i$		1	1	$-i$
$i$	$i$	-1		$-i$	$-i$	-1

Both  $\mathbb{R}(i)$  and  $\mathbb{R}(-i)$  are, in fact, **equal** to  $\mathbb{C}$ . The only difference is in the basis as a vector space over  $\mathbb{R}$ . One basis uses  $i$  and the other uses its complex conjugate  $-i$ .

(b) If  $F = \mathbb{Q}$  and  $f(x) = x^3 - 2$ , the clock has multiplication table:

$\times$	1	$x$	$x^2$
1	1	$x$	$x^2$
$x$	$x$	$x^2$	2
$x^2$	$x^2$	2	$2x$

and  $\mathbb{Q}(\sqrt[3]{2})$  (necessarily) has the same multiplication table:

$\times$	1	$\sqrt[3]{2}$	$\sqrt[3]{4}$
1	1	$\sqrt[3]{2}$	$\sqrt[3]{4}$
$\sqrt[3]{2}$	$\sqrt[3]{2}$	$\sqrt[3]{4}$	$\sqrt[3]{8} = 2$
$\sqrt[3]{4}$	$\sqrt[3]{4}$	$\sqrt[3]{8} = 2$	$\sqrt[3]{16} = 2\sqrt[3]{2}$

To find, for example, the inverse of  $x^2 + 1$  in the clock, we solve:

$$1 = (x^2 + 1)u(x) + (x^3 - 2)v(x)$$

which we do, as usual, using Euclid's algorithm:

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

so, solving back up Euclid's algorithm:

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

giving us the inverse in the  $x^3 - 2$ -clock:

$$(x^2 + 1)^{-1} = \frac{1}{5}(-x^2 + 2x + 1)$$

which we can substitute  $x = \sqrt[3]{2}$  to get the inverse in  $\mathbb{Q}(\sqrt[3]{2})$ :

$$(\sqrt[3]{4} + 1)^{-1} = \frac{1}{5}(-\sqrt[3]{4} + 2\sqrt[3]{2} + 1)$$

**Definition:** A **linear transformation** of a vector space is a function:

$$T : V \rightarrow V$$

such that:

$$T(\vec{v} + \vec{w}) = T(\vec{v}) + T(\vec{w}) \quad \text{and} \quad T(k\vec{v}) = kT(\vec{v})$$

for all vectors  $\vec{v}, \vec{w}$  and all scalars  $k$ . The linear transformation is **invertible** if there is an inverse function  $T^{-1} : V \rightarrow V$ , which is then automatically **also** a linear transformation!

**Definition:** Given a vector space  $V$  of dimension  $n$  with a basis  $\{\vec{v}_i\}$  and a linear transformation  $T : V \rightarrow V$ , the associated  $n \times n$  **matrix**

$$A = (a_{ij}) = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ & & \vdots & \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}$$

is defined by:

$$T(\vec{v}_j) = a_{1j}\vec{v}_1 + a_{2j}\vec{v}_2 + \dots + a_{nj}\vec{v}_n = \sum_{i=1}^n a_{ij}\vec{v}_i$$

**Examples:** (a) **Rotations in the  $\mathbb{R}^2$  plane.** We start with the basis:

$$\vec{e}_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \text{ and } \vec{e}_2 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

and we want the matrix for  $T : \mathbb{R}^2 \rightarrow \mathbb{R}^2$  given by counterclockwise rotation by an angle of  $\theta$ . For the matrix, use:

$$T(\vec{e}_1) = \cos(\theta)\vec{e}_1 + \sin(\theta)\vec{e}_2$$

by the definition of sin and cos. Since  $\vec{e}_2$  can be thought of as  $\vec{e}_1$  already rotated by  $\frac{\pi}{2}$ , we can think of  $T(\vec{e}_2)$  as the rotation of  $\vec{e}_1$  by  $\frac{\pi}{2} + \theta$  so:

$$T(\vec{e}_2) = \cos\left(\frac{\pi}{2} + \theta\right)\vec{e}_1 + \sin\left(\frac{\pi}{2} + \theta\right)\vec{e}_2$$

and then the matrix for counterclockwise rotation by  $\theta$  is:

$$A = \begin{bmatrix} \cos(\theta) & \cos\left(\frac{\pi}{2} + \theta\right) \\ \sin(\theta) & \sin\left(\frac{\pi}{2} + \theta\right) \end{bmatrix} = \begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix}$$

(using the identities:  $\cos\left(\frac{\pi}{2} + \theta\right) = -\sin(\theta)$  and  $\sin\left(\frac{\pi}{2} + \theta\right) = \cos(\theta)$ )

(b) **Multiplication by a scalar.** If  $k \in F$ , let  $T(\vec{v}) = k\vec{v}$ , so:

$$T(\vec{v}_1) = k\vec{v}_1, \dots, T(\vec{v}_n) = k\vec{v}_n$$

for any basis, and then:

$$A = \begin{bmatrix} k & 0 & \cdots & 0 \\ 0 & k & \cdots & 0 \\ & & \vdots & \\ 0 & 0 & \cdots & k \end{bmatrix}$$

In particular, the negation transformation is the case  $k = -1$ .

(c) **Multiplication by  $\alpha$ .** If  $\alpha$  has characteristic polynomial:

$$x^d + a_{d-1}x^{d-1} + \dots + a_0 \in \mathbb{Q}[x]$$

then multiplication by  $\alpha$  on the vector space  $\mathbb{Q}(\alpha)$  is defined by:

$$T(1) = \alpha, T(\alpha) = \alpha^2, \dots, T(\alpha^{d-1}) = \alpha^d = -a_0 - \dots - a_{d-1}\alpha^{d-1}$$

giving us the matrix:

$$A = \begin{bmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ & & \ddots & & \\ 0 & 0 & \cdots & 1 & -a_{d-1} \end{bmatrix}$$

The fact that multiplication by  $\alpha$  is a linear transformation comes from:

**Proposition 3.1.4.** *Multiplication by any  $\beta \in \mathbb{Q}(\alpha)$  is linear.*

**Proof:** We need to show that  $\beta(\vec{v} + \vec{w}) = \beta\vec{v} + \beta\vec{w}$  and  $\beta(k\vec{v}) = k(\beta\vec{v})$ . But in this vector space, all the vectors are **complex numbers!** For convenience set  $\vec{v} = s$  and  $\vec{w} = t$  to help us remember that they are numbers. Then:

$$\beta(s + t) = \beta s + \beta t$$

is the distributive law! And:

$$\beta(ks) = (\beta k)s = (k\beta)s = k(\beta s)$$

are the associative and commutative laws for multiplication.

**Matrix multiplication** (of matrices  $A = (a_{ij})$  and  $B = (b_{jk})$ ) is given by the prescription:

$$AB = C \text{ for } c_{ik} = a_{i1}b_{1k} + a_{i2}b_{2k} + \dots + a_{in}b_{nk} = \sum_j a_{ij}b_{jk}$$

Fix a basis  $\{\vec{v}_i\}$  for  $V$ . If the matrices  $A$  and  $B$  are associated to the linear transformations  $S$  and  $T$ , respectively, and if  $U = S \circ T$ , then:

$$U(\vec{v}_k) = S(T(\vec{v}_k)) = S\left(\sum_j b_{jk}\vec{v}_j\right) = \sum_{i,j} a_{ij}b_{jk}\vec{v}_i = \sum_i c_{ik}\vec{v}_i$$

is the  $k$ th column of  $C$ . So the product of two matrices is the matrix of the composition of the linear transformations.

We see from this that **matrix multiplication is associative:**

$$(AB)C = A(BC)$$

since composition of functions is associative:

$$(R \circ S) \circ T = R \circ S \circ T = R \circ (S \circ T)$$

Composition of linear transformations often isn't commutative, so matrix multiplication often isn't commutative (but sometimes it is!).

The identity transformation corresponds to the **identity matrix**:

$$I_n = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ & & \vdots & \\ 0 & 0 & \cdots & 1 \end{bmatrix}$$

which is a (multiplicative) identity, since  $I_n A = A = A I_n$  for all  $A$ . So  $I_n$  commutes with all matrices! In fact, multiplication by any scalar commutes with all matrices, by definition of a linear transformation.

If  $T$  is an **invertible** linear transformation with matrix  $A$ , then the matrix  $A^{-1}$  associated to  $T^{-1}$  is the (two-sided) **inverse matrix** because the inverse function is always a two-sided inverse! In other words, the inverse matrix satisfies:

$$A A^{-1} = I_n = A^{-1} A$$

(so  $A$  commutes with its inverse matrix, whenever an inverse exists!)

**Examples:** (a) The matrices for rotations by  $\theta$  and  $\psi$  are:

$$A_\theta = \begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix} \text{ and } A_\psi = \begin{bmatrix} \cos(\psi) & -\sin(\psi) \\ \sin(\psi) & \cos(\psi) \end{bmatrix}$$

The product of the two matrices is:

$$A_\theta A_\psi = \begin{bmatrix} \cos(\theta)\cos(\psi) - \sin(\theta)\sin(\psi) & -\cos(\theta)\sin(\psi) - \sin(\theta)\cos(\psi) \\ \cos(\theta)\sin(\psi) + \sin(\theta)\cos(\psi) & -\sin(\theta)\sin(\psi) + \cos(\theta)\cos(\psi) \end{bmatrix}$$

and by the angle sum formula from trig (see also §4) this is  $A_{\theta+\psi}$ , which is, as it must be, the matrix associated to the rotation by  $\theta + \psi$ . Notice that here, too, the matrix multiplication **is** commutative, since  $\theta + \psi = \psi + \theta$ !

(b) We saw in an earlier example that in  $\mathbb{Q}(\sqrt[3]{2})$ , there is an equality:

$$(\sqrt[3]{4} + 1)(-\sqrt[3]{4} + 2\sqrt[3]{2} + 1) = 5$$

Let's check this out with matrix multiplication. Start with:

$$A = \begin{bmatrix} 0 & 0 & 2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \quad A^2 = \begin{bmatrix} 0 & 2 & 0 \\ 0 & 0 & 2 \\ 1 & 0 & 0 \end{bmatrix}$$

(the matrices for multiplication by  $\sqrt[3]{2}$  and  $\sqrt[3]{4}$ , respectively)

The matrices for multiplication by  $\sqrt[3]{4} + 1$  and  $-\sqrt[3]{4} + 2\sqrt[3]{2} + 1$  are:

$$A^2 + I_3 = \begin{bmatrix} 1 & 2 & 0 \\ 0 & 1 & 2 \\ 1 & 0 & 1 \end{bmatrix}, \quad -A^2 + 2A + I_3 = \begin{bmatrix} 1 & -2 & 4 \\ 2 & 1 & -2 \\ -1 & 2 & 1 \end{bmatrix}$$

and then the matrix version of the equality above is:

$$(A^2 + I_3)(-A^2 + 2A + I_3) = 5I_3$$

as you may directly check with matrix multiplication!

Recall some more basic concepts from linear algebra:

**Similarity:** Two  $n \times n$  matrices  $A$  and  $A'$  are **similar** if

$$B^{-1}AB = A'$$

for some invertible matrix  $B$ . This is an **equivalence relation**:

- (i) Reflexive:  $I_n^{-1}AI_n = A$
- (ii) Symmetric: If  $B^{-1}AB = A'$ , then  $(B^{-1})^{-1}A'B^{-1} = A$ .
- (iii) Transitive: If  $B^{-1}AB = A'$  and  $C^{-1}A'C = A''$ , then:

$$A'' = C^{-1}(B^{-1}AB)C = (BC)^{-1}A(BC)$$

**Note:** Similarity occurs when we change basis. If  $A$  is the matrix for a transformation  $T$  with basis  $\{\vec{v}_i\}$  and if  $\{\vec{w}_j\}$  is another basis with:

$$\vec{w}_j = b_{1j}\vec{v}_1 + b_{2j}\vec{v}_2 + \dots + b_{nj}\vec{v}_n$$

then  $A' = B^{-1}AB$  is the matrix for  $T$  with the basis  $\{\vec{w}_j\}$ .

**Determinant:** The determinant is the unique function:

$$\det : \text{square matrices} \rightarrow F$$

that satisfies the following properties:

- (i)  $\det(AB) = \det(A)\det(B)$  for square  $n \times n$  matrices  $A$  and  $B$ .
- (ii)  $\det(A) = 0$  if and only if  $A$  is not invertible.
- (iii) The determinants of the “basic” matrices satisfy:

- (a)  $\det(A) = -1$  when  $A$  transposes two basis vectors  $\vec{v}_i$  and  $\vec{v}_j$ :

$$T(\vec{v}_i) = \vec{v}_j, T(\vec{v}_j) = \vec{v}_i, \quad \text{otherwise } T(\vec{v}_l) = \vec{v}_l$$

- (b)  $\det(A) = 1$  when  $A$  adds a multiple of one basis vector to another:

$$T(\vec{v}_j) = \vec{v}_j + k\vec{v}_i, \quad \text{otherwise } T(\vec{v}_l) = \vec{v}_l$$

(c)  $\det(A) = k$  when  $A$  multiplies one basis vector by  $k$ :

$$T(\vec{v}_i) = k\vec{v}_i \text{ and otherwise } T(\vec{v}_l) = \vec{v}_l$$

**Example:** The basic  $2 \times 2$  matrices are:

$$\det \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = -1$$

$$\det \begin{bmatrix} 1 & 0 \\ k & 1 \end{bmatrix} = 1, \quad \det \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix} = 1$$

$$\det \begin{bmatrix} k & 0 \\ 0 & 1 \end{bmatrix} = k, \quad \det \begin{bmatrix} 1 & 0 \\ 0 & k \end{bmatrix} = k$$

Since each matrix is a product of basic matrices (Gaussian elimination!) the determinant is completely determined by property (iii).

**Note:**  $\det(B^{-1})\det(B) = \det(I_n) = 1$  when  $B$  is invertible, and

$$\det(A') = \det(B^{-1})\det(A)\det(B) = \det(B)^{-1}\det(A)\det(B) = \det(A)$$

when  $A' = B^{-1}AB$ , so the determinants of similar matrices are equal. Thus the determinant **doesn't care** about the choice of basis.

**Characteristic Polynomial:** This is the function:

$$ch : \text{square matrices} \rightarrow F[x]$$

defined by:  $ch(A) = \det(xI_n - A)$  (assuming  $A$  is an  $n \times n$  matrix). And the characteristic polynomial is the same for similar matrices, too:

$$ch(A') = \det(xI_n - B^{-1}AB) = \det(B^{-1}(xI_n - A)B) = \det(xI_n - A) = ch(A)$$

**Examples:** (a) The characteristic polynomial of rotation by  $\theta$ :

$$\det \begin{bmatrix} x - \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & x - \cos(\theta) \end{bmatrix} = x^2 - 2\cos(\theta)x + 1$$

and the roots of this polynomial are the two complex numbers:

$$e^{i\theta} = \cos(\theta) + \sin(\theta)i \quad \text{and} \quad e^{-i\theta} = \cos(\theta) - \sin(\theta)i$$

(b) The characteristic polynomial of multiplication by  $\alpha \in \mathbb{Q}(\alpha)$  is:

$$\det \begin{bmatrix} x & 0 & \cdots & 0 & a_0 \\ -1 & x & \cdots & 0 & a_1 \\ 0 & -1 & \cdots & 0 & a_2 \\ & & \vdots & & \\ 0 & 0 & \cdots & -1 & x + a_{d-1} \end{bmatrix} = x^d + a_{d-1}x^{d-1} + \cdots + a_0$$

which is exactly the **same** as the characteristic polynomial of  $\alpha$  thought of as an algebraic number! This apparent coincidence is explained by the following:

**Proposition 3.1.5.** *Each  $n \times n$  matrix  $A$  is a “root” of its characteristic polynomial. That is, if*

$$ch(A) = x^n + a_{n-1}x^{n-1} + \dots + a_0$$

then

$$A^n + a_{n-1}A^{n-1} + \dots + a_0I_n = 0$$

(this isn't a root in our usual sense, because  $A$  is a matrix, not a scalar!)

**Proof:** The sum:

$$B = A^n + a_{n-1}A^{n-1} + \dots + a_0I_n$$

is a **matrix**, so to see that it is zero, we need to see that it is the zero linear transformation, which is to say that  $B\vec{v} = 0$  for all vectors  $\vec{v} \in V$ . In fact, it is enough to see that  $B\vec{v}_i = 0$  for all basis vectors, but in this case it isn't helpful to restrict our attention to basis vectors.

So given an arbitrary vector  $\vec{v}$ , we know that eventually the vectors:

$$\vec{v}, A\vec{v}, A^2\vec{v}, \dots, A^m\vec{v}$$

are linearly dependent (though we may have to wait until  $m = n$ ). For the first such  $m$ , the vector  $A^m\vec{v}$  is a linear combination of the others (which are linearly independent):

$$b_0\vec{v} + b_1A\vec{v} + \dots + b_{m-1}A^{m-1}\vec{v} + A^m\vec{v} = 0$$

Now I claim that the polynomial  $x^m + b_{m-1}x^{m-1} + \dots + b_0$  divides  $ch(A)$ . To see this, we extend  $\vec{v}, \dots, A^{m-1}\vec{v}$  to a basis of the vector space  $V$ :

$$\vec{v}, A\vec{v}, \dots, A^{m-1}\vec{v}, \vec{w}_{m+1}, \dots, \vec{w}_n$$

with some extra vectors  $\vec{w}_{m+1}, \dots, \vec{w}_n$  that I don't care about. The characteristic polynomial doesn't care what basis we use, so let's use this one. The point is that some of this matrix we know:

$$A = \begin{bmatrix} 0 & 0 & \cdots & 0 & -b_0 & * & \cdots & * \\ 1 & 0 & \cdots & 0 & -b_1 & * & \cdots & * \\ 0 & 1 & \cdots & 0 & -b_2 & * & \cdots & * \\ & & \vdots & & & & \vdots & \\ 0 & 0 & \cdots & 1 & -b_{m-1} & * & \cdots & * \\ 0 & 0 & \cdots & 0 & 0 & * & \cdots & * \\ & & \vdots & & & & \vdots & \\ 0 & 0 & \cdots & 0 & 0 & * & \cdots & * \end{bmatrix}$$

where the “\*” denote entries that we do not know, since they involve the  $\vec{w}_i$  basis vectors. But this is enough. It follows as in Example (b) above that  $x^m + b_{m-1}x^{m-1} + \dots + b_0$  divides the determinant of  $xI_n - A$ !

But now that  $ch(A)$  factors, we can write

$$ch(A) = (x^{n-m} + c_{n-m-1}x^{n-m-1} + \dots + c_0)(x^m + b_{m-1}x^{m-1} + \dots + b_0)$$

for some other polynomial with  $c$  coefficients, and then:

$$B\vec{v} = (A^{n-m} + c_{n-m-1}A^{n-m-1} + \dots + c_0I_n)(A^m + b_{m-1}A^{m-1} + \dots + b_0I_n)\vec{v} = 0$$

because  $A^m\vec{v} = -b_0\vec{v} - \dots - b_{m-1}A^{m-1}\vec{v}$ . That's the proof!

**Final Remarks:** Given an  $n \times n$  matrix  $A$ , then any vector satisfying:

$$A\vec{v} = \lambda\vec{v}$$

is an **eigenvector** of the linear transformation and  $\lambda$  is its **eigenvalue**. If  $\vec{v}$  is a nonzero eigenvector, then

$$(\lambda I_n - A)\vec{v} = 0$$

so in particular,  $\lambda I_n - A$  is **not** an invertible matrix, and so:

$$\det(\lambda I_n - A) = 0$$

In other words, an eigenvalue is a **root** of the characteristic polynomial, and conversely, each root is an eigenvalue for some eigenvector. Notice that if the vector space happens to have a **basis**  $\{\vec{v}_i\}$  of eigenvectors with eigenvalues  $\{\lambda_i\}$ , then by changing to this basis, we get a matrix  $A'$  similar to  $A$  with:

$$A' = \begin{bmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ & & \vdots & \\ 0 & 0 & \cdots & \lambda_n \end{bmatrix}$$

In this case  $A$  is said to be **diagonalizable**.

**Example:** Rotation by  $\theta$  is not diagonalizable if  $\mathbb{R}$  is our scalar field, since the eigenvalues for rotation are the complex numbers  $e^{i\theta}$  and  $e^{-i\theta}$ . However, if we broaden our horizons and allow  $\mathbb{C}$  to be the scalar field, then:

$$\begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix} \begin{bmatrix} 1 \\ -i \end{bmatrix} = \begin{bmatrix} \cos(\theta) + i\sin(\theta) \\ \sin(\theta) - i\cos(\theta) \end{bmatrix} = e^{i\theta} \begin{bmatrix} 1 \\ -i \end{bmatrix}$$

and

$$\begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix} \begin{bmatrix} 1 \\ i \end{bmatrix} = \begin{bmatrix} \cos(\theta) - i\cos(\theta) \\ \sin(\theta) + i\cos(\theta) \end{bmatrix} = e^{-i\theta} \begin{bmatrix} 1 \\ i \end{bmatrix}$$

so we have our basis of eigenvectors and in that basis, rotation is given by the matrix:

$$\begin{bmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{bmatrix}$$

### 3.1.1 Linear Algebra Exercises

**10-1** Recall that the polynomial  $f(x) = x^3 + x + 1 \in F_2[x]$  is prime. This means that the  $f(x)$ -clock is a field with 8 elements. Complete the following addition and multiplication tables for this field:

+	0	1	$x$	$x + 1$	$x^2$	$x^2 + 1$	$x^2 + x$	$x^2 + x + 1$
0								
1								
$x$								
$x + 1$								
$x^2$								
$x^2 + 1$								
$x^2 + x$								
$x^2 + x + 1$								

$\times$	0	1	$x$	$x + 1$	$x^2$	$x^2 + 1$	$x^2 + x$	$x^2 + x + 1$
0								
1								
$x$								
$x + 1$								
$x^2$								
$x^2 + 1$								
$x^2 + x$								
$x^2 + x + 1$								

**10-2** Repeat 10-1 for the prime polynomial  $f(x) = x^2 + 1 \in F_3[x]$ . Hint: This time you'll get a field with 9 elements!

**10-3** In the field  $\mathbb{Q}(\sqrt{2})$  do the following:

- Find the multiplicative inverse of  $1 + \sqrt{2}$  in  $\mathbb{Q}(\sqrt{2})$ .
- Write the  $2 \times 2$  matrix for multiplication by  $1 + \sqrt{2}$  in  $\mathbb{Q}(\sqrt{2})$ .
- Find the characteristic polynomial for the matrix in (b).
- Find the (complex!) eigenvalues of the matrix in (b).
- Find the  $2 \times 2$  matrix for multiplication by  $(1 + \sqrt{2})^{-1}$  in  $\mathbb{Q}(\sqrt{2})$ .
- Multiply the matrices (for  $1 + \sqrt{2}$  and for  $(1 + \sqrt{2})^{-1}$ ) to see that they are really inverses of each other.

**10-4** Let  $\alpha = \cos(\frac{2\pi}{5}) + i \sin(\frac{2\pi}{5})$ . In the field  $\mathbb{Q}(\alpha)$  do the following:

- Find the characteristic polynomial of the algebraic number  $\alpha$ . (Hint: It is a polynomial of degree 4).

(b) Fill out the following multiplication table for  $\mathbb{Q}(\alpha)$ :

$\times$	1	$\alpha$	$\alpha^2$	$\alpha^3$
1				
$\alpha$				
$\alpha^2$				
$\alpha^3$				

(c) Find the multiplicative inverse of  $\alpha^2$  in  $\mathbb{Q}(\alpha)$ .

(d) Write the  $4 \times 4$  matrix for multiplication by  $\alpha^2$ .

**10-5** Find the characteristic polynomials and eigenvalues of the following:

(a)

$$\begin{bmatrix} \cos(\theta) & \sin(\theta) \\ \sin(\theta) & -\cos(\theta) \end{bmatrix}$$

(b)

$$\begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

(c)

$$\begin{bmatrix} 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & -1 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & -1 \end{bmatrix}$$

## 3.2 Constructible Numbers

Armed with a straightedge, a compass and two points 0 and 1 marked on an otherwise blank “number-plane,” the game is to see which complex numbers you can construct, and which complex numbers you **cannot** construct!

**Definition:** A complex number  $\alpha$  can be constructed if  $\alpha = 0$  or  $\alpha = 1$  or else  $\alpha$  is an intersection point of a pair of lines, a line and a circle, or a pair of circles that you can draw with your straightedge and compass.

**The Rules:** With your straightedge and compass, you are allowed to:

(i) Draw the line  $L(p, q)$  (with the straightedge) through any two points  $p$  and  $q$  that you have already constructed.

(ii) Open the compass to span the distance  $|q - p|$  between any two points  $p$  and  $q$  that you have already constructed, place the base at a third point  $o$  (already constructed), and draw the circle  $C(o; |q - p|)$ .

**Example:** Your first move is one of the following:

(i) Drawing the  $x$ -axis, which is the line  $L(0, 1)$ , or

(ii) Drawing the circle  $C(0; 1)$  (of radius 1 about 0) or else  $C(1; 1)$ .

When you draw all three of these, you’ve constructed 4 numbers:

(a)  $L(0, 1)$  and  $C(0; 1)$  intersect at 1 and the new number  $-1$ ,

(b)  $L(0, 1)$  and  $C(1; 1)$  intersect at 0 and the new number 2,

(c)  $C(0; 1)$  and  $C(1; 1)$  intersect at the two new numbers  $\frac{1}{2} \pm \frac{\sqrt{3}}{2}i$ .

**Proposition 3.2.1.** *All the integers can be constructed.*

**Proof:** By induction. 0 was given to us.

(i) 1 was given to us, and we’ve seen above how to construct  $-1$ .

(ii) Once you’ve constructed  $n$  and  $-n$ , draw  $C(n; 1)$  and  $C(-n; 1)$  to construct  $n + 1$  (as one point of the intersection  $L(0, 1) \cap C(n; 1)$ ) and  $-(n + 1)$  (as one point of the intersection  $L(0, 1) \cap C(-n; 1)$ ).

By induction, then, all integers can be constructed!

**Construction 3.2.2.** *If  $L$  is a line that has already been drawn and  $p$  is a point that has already been constructed (which may or may not be on  $L$ ), then we can draw*

$$p \in L^\perp \quad \text{and} \quad p \in L^\parallel$$

*the unique lines containing  $p$  that are perpendicular and parallel to  $L$ .*

**The Construction:** Since  $L$  has already been drawn, there are at least two points on it that have been constructed, so in particular at least one of them is different from  $p$ . Let  $q \neq p$  be one of these points. Now draw  $C(p; |q - p|)$ . If this circle only intersects  $L$  at  $q$ , then it is tangent to  $L$ , and  $L(p, q)$  is  $p \in L^\perp$ . Otherwise let  $q' \in L$  be the second point of  $L \cap C(p; |q - p|)$ . Now draw  $C(q; |q - q'|)$  and  $C(q'; |q - q'|)$ . These intersect in two points  $r, r'$  and the line  $L(r, r')$  is  $p \in L^\perp$ .

To draw the parallel line  $p \in L^\parallel$ , just draw two perpendiculars. Namely, first draw  $p \in L^\perp$ , and then draw  $p \in (p \in L^\perp)^\perp$ .

**Proposition 3.2.3.** *All Gaussian integers can be constructed*

**Proof:** To construct  $a + bi$ , first construct the integer  $a$ , then draw  $a \in L(0, 1)^\perp$ , which is the vertical line  $x = a$ . Then construct any  $a + bi$  on that line by induction, as in Proposition 3.2.1.

**Proposition 3.2.4.** *Once a complex number  $\alpha$  has been constructed,*

$$-\alpha, \quad i\alpha, \quad \text{and} \quad \bar{\alpha}$$

*can also be constructed.*

**Proof:** Using  $\alpha$ , construct the line  $L(0, \alpha)$  and the circle  $C(0; |\alpha|)$ . These intersect at the two points  $\alpha$  and  $-\alpha$ .

Next, recall that  $i\alpha$  is the rotation of  $\alpha$  by  $\frac{\pi}{2}$ . Draw  $0 \in L(0, \alpha)^\perp$ . This line intersects  $C(0; |\alpha|)$  at the two points  $i\alpha$  and  $-i\alpha$ .

If we write  $\alpha = s + ti$ , then  $\alpha \in L(0, 1)^\perp$  is the line  $x = s$ , which meets  $L(0, 1)$  at the real point  $s + 0i$ . Similarly,  $\alpha \in L(0, 1)^\parallel$  is the line  $y = t$ , which meets the  $y$ -axis  $L(0, i)$  at the purely imaginary point  $0 + ti$ . Now draw the circle  $C(s + 0i; |t|)$ . Its intersections with  $x = s$  are the two numbers  $\alpha$  and  $\bar{\alpha} = s - it$ .

**Proposition 3.2.5.** *Once  $\alpha$  and  $\beta$  have been constructed, then*

$$\alpha + \beta$$

*can be constructed.*

**Proof:** If  $\alpha = 0$  or  $\beta = 0$ , there is nothing to do! Otherwise draw  $L(0, \beta)$ , the parallel line  $\alpha \in L(0, \beta)^\parallel$  through  $\alpha$ , and then draw  $C(\alpha; |\beta|)$ . Then  $\alpha \in L(0, \beta)^\parallel$  and  $C(\alpha, |\beta|)$  intersect at  $\alpha \pm \beta$ .

**Construction 3.2.6.** *If you can construct a length  $r$ , then you can construct  $1/r$ .*

*If you can construct a second length  $s$ , then you can construct  $rs$ .*

**The Construction:** First, draw the vertical “slope recorder” line:

$$1 \in L(0, 1)^\perp \text{ (which is just the line } x = 1)$$

then draw the vertical line  $r \in L(0, 1)^\perp$  (which is  $x = r$ ), and construct  $r + i$  by intersecting  $x = r$  with  $C(r; 1)$ . Now draw  $L(0, r + i)$ . The intersection of this line with  $x = 1$  is the point  $1 + \frac{1}{r}i$ , which gives  $1/r$  (as the intersection of  $C(0; |(1 + \frac{1}{r}i) - 1|)$  with the  $x$ -axis  $L(0, 1)$ ).

Draw the vertical line  $x = s$ , and construct  $1 + ir$  as the intersection of the slope recorder with  $C(1; r)$ . Then the intersection of  $L(0, 1 + ir)$  (the line of slope  $r$ ) with the line  $x = s$  is  $s + irs$ , which gives  $rs$ .

**Proposition 3.2.7.** *Every element of the field  $\mathbb{Q}(i)$  can be constructed.*

**Proof:** By Construction 3.2.6 and Proposition 3.2.5, we can construct every rational number, since we take any integers  $a$  and  $b \neq 0$  and construct  $a \times 1/b = a/b$ . But the elements of  $\mathbb{Q}(i)$  are all of the form  $a/b + c/di$ , which can then be constructed by constructing  $a/b$  and  $c/d$ , and then intersecting the line  $x = a/b$  with the circle  $C(a/b; |c/d|)$ .

If  $p \in L$  is a line passing through a point  $p$ , then we will write:

$$p \in L^\theta$$

for the line passing through  $p$  and making an angle  $\theta$  with  $L$ , measured counterclockwise. For example,  $p \in L^\perp$  and  $p \in L^{\pi/2}$  are the same line.

**Construction 3.2.8.** *If  $p \in L$  and  $p \in L^\theta$  can be constructed (and drawn), then:*

- (a) *The “opposite” line  $p \in L^{-\theta}$  can be drawn.*
- (b) *If  $q \in M$  is a point on another line, then  $q \in M^\theta$  can be drawn.*
- (c) *The “angle bisector”  $p \in L^{\theta/2}$  can be drawn.*

**The Construction:** Exercise!

**Proposition 3.2.9.** *If you can construct  $\alpha, \beta$ , you can also construct*

$$1/\alpha \text{ (if } \alpha \neq 0) \text{ and } \alpha \cdot \beta$$

**Proof:** In polar coordinates,  $\alpha = (r; \theta)$  and  $\beta = (s; \psi)$ . Thus  $L(0, \alpha)$  is the line  $0 \in L(0, 1)^\theta$  and  $L(0, \beta)$  is the line  $0 \in L(0, 1)^\psi$ . Then:

$$1/\alpha = (1/r; -\theta)$$

is an intersection of  $0 \in L(0, 1)^{-\theta}$  (drawn with Construction 3.2.8) and the circle  $C(0; 1/r)$  (drawn with Construction 3.2.6). Similarly,

$$\alpha\beta = (rs; \theta + \psi)$$

is an intersection of  $0 \in L(0, \alpha)^\psi$  (drawn with Construction 3.2.8) with  $C(0; rs)$  (drawn with Construction 3.2.6).

**Proposition 3.2.10.** *The constructible complex numbers are a field:*

$$\mathbb{Q}(i) \subset F_{\text{const}} \subset \mathbb{C}$$

**Proof:** Additive inverses exist in  $F_{\text{const}}$ , by Proposition 3.2.6,  $F_{\text{const}}$  is closed under addition by Proposition 3.2.5, multiplicative inverses exist and  $F_{\text{const}}$  is closed under multiplication by Proposition 3.2.9, and finally  $F_{\text{const}}$  contains  $\mathbb{Q}(i)$  by Proposition 3.2.7. (The associative, distributive, commutative laws are automatic since  $F_{\text{const}} \subset \mathbb{C}$ ).

**The Question:** Which numbers are in  $F_{\text{const}}$  and which are not?

(This is a paraphrase of the question we asked to start this chapter)

**Construction 3.2.11.** *If you can construct a positive real number  $r$ , you can also construct  $\sqrt{r}$ .*

**Remark:** Pythagoras knew how to construct  $\sqrt{2}$  as the hypotenuse of a right triangle. For example,  $\sqrt{2} = |1+i|$ , which is therefore the (positive) intersection of the circle  $C(0; |1+i|)$  with the  $x$ -axis. It was apparently difficult for some of his contemporaries to accept the fact that this number was constructible but at the same time **not** rational.

**The Construction:** As in the Pythagorean theorem:

$$\sqrt{1+r^2} = |r+i|$$

is constructible, if  $r$  is constructible. Now consider the intersection of the circle  $C(0; 1+r)$  with the vertical line  $x = \sqrt{1+r^2}$ , which constructs the complex number:

$$\alpha = \sqrt{1+r^2} + it$$

that therefore satisfies:  $|\alpha|^2 = 1+r^2+t^2 = (1+r)^2$ , or, simplifying:

$$t^2 = 2r$$

so that  $t = \sqrt{2r}$  is constructible. We can divide by any constructed length (Construction 3.2.6), and so giving thanks to Pythagoras, we construct  $\sqrt{r} = t \times 1/\sqrt{2}$ .

**Proposition 3.2.12.**  *$F_{\text{const}}$  is closed under taking square roots.*

**Proof:** We need to show that if  $\alpha$  is constructible, then  $\pm\sqrt{\alpha}$  are also constructible. Again, go polar. If  $\alpha = (r; \theta)$ , we can bisect  $\theta$  by Construction 3.2.8 to get  $0 \in L(0, 1)^{\theta/2}$  and we can construct the square root of  $r$  by Construction 3.2.11, and these allow us to construct

$$\pm\sqrt{\alpha} = \pm(\sqrt{r}; \frac{1}{2}\theta)$$

as the two points of the intersection of  $C(0; \sqrt{r})$  with  $0 \in L(0, 1)^{\theta/2}$ .

**Remark:** So far, we've concentrated on what we **can** construct. Now it is time to turn our attention to what **cannot** be constructed. This was a problem that puzzled the ancients for centuries!

In fact, with the vector space technology from §10, we will prove:

**The Constructible Number Theorem:** Every number  $\alpha$  that you can construct has the following properties:

- (i)  $\alpha$  is an algebraic number.
- (ii) The degree of the characteristic polynomial of  $\alpha$  is a power of 2.

Before we prove this, we note a couple of significant corollaries:

**Corollary 3.2.13.** *You cannot construct  $\sqrt[3]{2}$ .*

**Proof:**  $x^3 - 2$  has degree 3, which is not a power of 2!

**Corollary 3.2.14.** *There is no general construction for trisecting angles. (Compare with Construction 3.2.8, which bisects angles)*

**Proof:** Way back at the beginning, we saw how to construct  $\frac{1}{2} + \frac{\sqrt{3}}{2}i$ . We can subtract 1 from this to get  $-\frac{1}{2} + \frac{\sqrt{3}}{2}i$ , and hence  $L(0, -\frac{1}{2} + \frac{\sqrt{3}}{2}i)$ , which is the same thing as the line:

$$0 \in L(0, 1)^{2\pi/3}$$

If there were a general trisecting construction, we could use it to draw:

$$0 \in L(0, 1)^{2\pi/9}$$

and then by intersecting with  $C(0; 1)$ , we would have constructed:

$$\alpha = (1; \frac{2\pi}{9}) = \cos(\frac{2\pi}{9}) + \sin(\frac{2\pi}{9})i$$

But this number **cannot** be constructed. To see this, we find the characteristic polynomial of  $\alpha$ :

$$\alpha^3 = (1; \frac{2\pi}{3}) = -\frac{1}{2} + i\frac{\sqrt{3}}{2} \text{ and } \alpha^6 = (1; \frac{4\pi}{3}) = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$$

so  $\alpha^6 + \alpha^3 = -1$  and  $\alpha$  is a root of  $f(x) = x^6 + x^3 + 1 = 0$ . Is this prime? Yes! (Exercise 8.4(g)). So  $f(x)$  is the characteristic polynomial of  $\alpha$ , and 6 isn't a power of 2, so the theorem tells us  $\alpha$  isn't constructible! So  $0 \in L(0, 1)^{2\pi/9}$  cannot be drawn! So there is no way to trisect angles!!

**Remark:** In case you thought "of course  $(1; \frac{2\pi}{9})$  isn't constructible" let me point out that  $(1; \frac{2\pi}{5}) = \cos(\frac{2\pi}{5}) + \sin(\frac{2\pi}{5})i$ , another unlikely-looking number, **can** be constructed. You are invited to check that:

$$(1; \frac{2\pi}{5}) = \frac{-1 + \sqrt{5}}{4} + i\sqrt{\frac{5 + \sqrt{5}}{8}}$$

and then to construct this with a straightedge and compass.

To prove the theorem, we will need to think about “towers” of fields.

**Definition:** If  $E \subset F$  are fields, then  $[F : E]$  is the **dimension** of  $F$ , thought of as a vector space over  $E$ .

**Examples:** (a)  $[\mathbb{C} : \mathbb{R}] = 2$ , and  $[\mathbb{C} : \mathbb{Q}] = \infty$

(b) In the setting of Proposition 10.3, where  $F \subset \mathbb{C}$  is a subfield and  $\alpha \in \mathbb{C}$  is a root of a prime polynomial  $x^d + a_{d-1}x^{d-1} + \dots + a_0 \in F[x]$  then  $[F(\alpha) : F] = d$ , since  $\{1, \alpha, \alpha^2, \dots, \alpha^{d-1}\}$  is a basis of  $F(\alpha)$ .

**Proposition 3.2.15.** *If  $E \subset F \subset G$  are all fields, then:*

$$[G : E] = [F : E] \cdot [G : F]$$

**Proof:** Let  $\{f_1, \dots, f_m\}$  be a basis for  $F$  as a vector space over  $E$ , and  $\{g_1, \dots, g_n\}$  be a basis for  $G$  as a vector space over  $F$ , and consider the set:  $\{f_1g_1, \dots, f_ig_j, \dots, f_mg_n\}$  of elements of  $G$  consisting of all products of pairs of basis vectors. We are done if we show that this set of  $mn$  elements is a basis of  $G$  as a vector space over  $E$ .

To see this, notice first of all that any  $g \in G$  is a linear combination:

$$g = k_1g_1 + \dots + k_n g_n \text{ for “scalars” } k_j \in F$$

because  $\{g_1, \dots, g_n\}$  span  $G$  as a vector space over  $F$ . But we can also regard the scalars  $k_1, \dots, k_n \in F$  as **vectors** when we think of  $F$  as a vector space over  $E$ . Thus each  $k_j$  is a linear combination:

$$k_j = c_{1,j}f_1 + \dots + c_{m,j}f_m \text{ for “scalars” } c_{i,j} \in E$$

Substituting for the  $k_j$  now gives us:

$$\begin{aligned} g &= (c_{1,1}f_1 + \dots + c_{m,1}f_m)g_1 + \dots + (c_{1,n}f_1 + \dots + c_{m,n}f_m)g_n \\ &= c_{1,1}f_1g_1 + \dots + c_{i,j}f_ig_j + \dots + c_{m,n}f_mg_n \end{aligned}$$

showing that  $\{f_ig_j\}$  span  $G$  as a vector space over  $E$ . And if:

$$0 = (c_{1,1}f_1 + \dots + c_{m,1}f_m)g_1 + \dots + (c_{1,n}f_1 + \dots + c_{m,n}f_m)g_n$$

then all of the  $k_j = c_{1,j}f_1 + \dots + c_{m,j}f_m$  must be 0 because the  $\{g_j\}$  are linearly independent, and then all of the  $c_{i,j}$  must be 0 because the  $\{f_i\}$  are linearly independent! Thus it follows that the  $\{f_ig_j\}$  are linearly independent. So the  $\{f_ig_j\}$  are a basis.

**Example:** Start with the field

$$F = \mathbb{Q}(\sqrt{2})$$

which is a vector space over  $\mathbb{Q}$  with basis  $\{1, \sqrt{2}\}$ . I claim that:

$$F(\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$$

is a vector space over  $F$  with basis  $\{1, \sqrt{3}\}$ . To see this, we need to check that  $x^2 - 3$  is prime in  $F[x]$ . To see this it is enough to show that  $x^2 - 3$  has no root in  $F$ . So try to solve  $3 = (a + b\sqrt{2})^2 = a^2 + 2ab\sqrt{2} + 2b^2$  with  $a, b \in \mathbb{Q}$ . Since  $\sqrt{2}$  is irrational, this would mean  $2ab = 0$ , so  $a = 0$  or  $b = 0$ , but then we'd either have  $a^2 = 3$  or  $b^2 = \frac{3}{2}$  which is impossible since both square roots are irrational. So indeed  $x^2 - 3 \in F[x]$  is prime. By the Proposition, then,  $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$  and:

$$\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$$

is a basis of  $F(\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$  as a vector space over  $\mathbb{Q}$ .

**Proposition 3.2.16.** *If  $F$  is a field with  $\mathbb{Q} \subset F \subset \mathbb{C}$  and  $[F : \mathbb{Q}] = n$ , then every element  $\alpha \in F$  is an algebraic number, and the degree of the characteristic polynomial of  $\alpha$  divides  $n$ .*

**Proof:** The field  $\mathbb{Q}(\alpha)$  sits between  $\mathbb{Q}$  and  $F$ .

$$\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset F$$

By Proposition 3.2.15,  $[F : \mathbb{Q}] = [F : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}]$ . But  $[\mathbb{Q}(\alpha) : \mathbb{Q}]$  is the degree of the characteristic polynomial of  $\alpha$ .

**Example (cont):** (i) Let  $\alpha = \sqrt{6} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$ . The characteristic polynomial of  $\alpha$  is  $x^2 - 6$ , which has degree 2 (and 2 divides 4).

(ii) Let  $\alpha = \sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$ . The characteristic polynomial of  $\alpha$  is  $x^4 - 10x^2 + 1$ , which has degree 4.

**Proof of the Constructible Number Theorem:** Get a notebook to go with your straightedge and compass. At the top, write:

$$F = \mathbb{Q}(i)$$

This is the field you start with, which will be updated with each new complex number that you construct. Each time you draw a line or a circle, you are constructing a finite set of new complex numbers, which are the intersection points of the line (or circle) with all the lines and circles that were drawn before. You consider these numbers one at a time and ask of each: "Is the intersection in  $F$ ?" If not, update  $F$ , replacing it with a carefully chosen new field that contains the intersection point, which you enter below  $F$  in your notebook.

After going through all the lines and circles of the construction, you get a list of fields, ending with:

$$F = \mathbb{Q}(i, \alpha_1, \alpha_2, \dots, \alpha_n)$$

which contains every complex number of your construction. I claim that we can choose the  $\alpha_1, \dots, \alpha_n$  so that:

$$[F : \mathbb{Q}] = 2^{n+1}$$

Once we prove this, we are done! If  $\alpha \in F_{\text{const}}$ , then by definition there is a construction so that  $\alpha \in F$ , the last field in your notebook, and then Proposition 3.2.16 tells us that  $\alpha$  is an algebraic number and that the degree of its characteristic polynomial divides  $[F : \mathbb{Q}]$ . So once we know that each  $[F : \mathbb{Q}] = 2^{n+1}$ , then we know that the characteristic polynomial of each constructible number divides a power of 2. But the only numbers that divide powers of 2 are smaller powers of 2!

To prove  $[F : \mathbb{Q}] = 2^{n+1}$ , we'll use Proposition 3.2.15, showing that each new field we enter into our notebook is  $F(\alpha_{k+1})$ , where  $\alpha_{k+1}$  a root of a **quadratic** polynomial in  $F[x] = \mathbb{Q}(i, \alpha_1, \dots, \alpha_k)[x]$ . That's enough, because it shows that the dimensions of:

$$\mathbb{Q}(i) \subset \mathbb{Q}(i, \alpha_1) \subset \mathbb{Q}(i, \alpha_1, \alpha_2) \subset \dots \subset \mathbb{Q}(i, \alpha_1, \dots, \alpha_n)$$

are  $2, 2^2, 2^3, \dots, 2^{n+1}$  as vector spaces over  $\mathbb{Q}$ . We will also see that each new  $\alpha_{k+1}$  can be chosen to be a **real** number, from which it follows that each of the fields  $\mathbb{Q}(i, \alpha_1, \dots, \alpha_n)$  is closed under complex conjugation.

So let's find these quadratic polynomials. Suppose you have just drawn a line or a circle, and the field so far is  $F = \mathbb{Q}(i, \alpha_1, \dots, \alpha_k)$  and  $F$  is closed under complex conjugation. Then you are looking at an intersection point  $\alpha$ , and trying to see whether it is in  $F$  or whether the new field  $F(\alpha_{k+1})$  is required. One thing to notice is that since **every** number that was constructed earlier belongs to  $F$ , it follows that every line passes through two points of  $F$  and every circle has its center and a radius vector in  $F$ , **including** whatever line or circle you just drew. This means that each line is *parametrized* by:

- $\beta + \gamma x$  for some pair  $\beta, \gamma \in F$  ( $x$  is a real parameter)

and the *equation* of each circle is:

- $|z - \beta|^2 = |\gamma|^2$  for some pair  $\beta, \gamma \in F$  ( $z$  is a complex variable)

Also, since  $F$  is closed under conjugation, if  $\beta = s + it \in F$ , then:

$$\bar{\beta}, \beta\bar{\beta} = s^2 + t^2, \frac{1}{2}(\beta + \bar{\beta}) = s \quad \text{and} \quad \frac{1}{2i}(\beta - \bar{\beta}) = t$$

are also all in  $F$ , and similarly for  $\gamma$ .

Now let's consider the three possibilities for  $\alpha$ :

1)  $\alpha$  is an intersection of two lines  $L_1$  and  $L_2$ :

$$\beta_1 + \gamma_1 x = \alpha = \beta_2 + \gamma_2 x_2$$

Let  $\beta_1 = s_1 + it_1$ ,  $\beta_2 = s_2 + it_2$ ,  $\gamma_1 = u_1 + iv_1$  and  $\gamma_2 = u_2 + iv_2$ . Then  $\alpha$  is obtained by solving the pair of linear equations:

$$s_1 + u_1x_1 = s_2 + u_2x_2$$

$$t_1 + v_1x_1 = t_2 + v_2x_2$$

which can easily be done. Namely:

$$x = \frac{v_2(s_2 - s_1) + u_2(t_1 - t_2)}{u_1v_2 - v_1u_2}$$

(if  $u_1v_2 - v_1u_2 = 0$ , the lines are parallel). This is an element of  $F$ ! And this means that  $\alpha$  is also in  $F$ :

$$\alpha = \beta + \gamma \frac{v_2(s_2 - s_1) + u_2(t_1 - t_2)}{u_1v_2 - v_1u_2}$$

so in this case we don't add a new entry to our notebook.

**2)  $\alpha$  is an intersection of a line and a circle  $L_1$  and  $C_2$ :**

$$\alpha = \beta_1 + \gamma_1x \quad \text{and} \quad |\alpha - \beta_2|^2 = |\gamma_2|^2$$

Write out  $\beta_1, \beta_2, \gamma_1$  and  $\gamma_2$  as in 1). Then substitute:

$$|(\beta_1 + \gamma_1x) - \beta_2|^2 = |\gamma_2|^2$$

$$(s_1 + u_1x - s_2)^2 + (t_1 + v_1x - t_2)^2 = u_2^2 + v_2^2$$

and expand, to get a quadratic polynomial:

$$ax^2 + bx + c = 0, \quad \text{where}$$

$$a = (u_1^2 + v_1^2)$$

$$b = 2(u_1(s_1 - s_2) + v_1(t_1 - t_2))$$

$$c = (s_1 - s_2)^2 + (t_1 - t_2)^2 - (u_2^2 + v_2^2)$$

The roots of this polynomial are the values of  $x$  so that  $\alpha = \beta + \gamma x$  is a point of intersection of the line and circle. This is a quadratic polynomial with real coefficients, and its roots have to be real numbers (if the roots weren't real, then the line would not intersect the circle!!) It is possible that the roots of this polynomial are already in  $F$ , in which case, as before, we don't make a new entry in the notebook, because then  $\alpha \in F$ . If the roots aren't in  $F$ , let  $\alpha_{k+1}$  be one of them and then  $\alpha = \beta + \gamma\alpha_{k+1} \in F(\alpha_{k+1})$  as we wanted. So we make  $F(\alpha_{k+1})$  the new entry in the notebook.

**3)**  $\alpha$  is an intersection of two circles  $C_1$  and  $C_2$ :

$$|\alpha - \beta_1|^2 = |\gamma_1|^2 \text{ and } |\alpha - \beta_2|^2 = |\gamma_2|^2$$

Let  $\alpha = x + iy$  and write out  $\beta_1, \beta_2, \gamma_1, \gamma_2$  as in 1). Then we solve:

$$(x - s_1)^2 + (y - t_1)^2 = u_1^2 + v_1^2 \text{ and } (x - s_2)^2 + (y - t_2)^2 = u_2^2 + v_2^2$$

and subtracting the first from the second, we get:

$$(*) \ 2(s_1 - s_2)x + 2(t_1 - t_2)y = (u_2^2 + v_2^2 + s_1^2 + t_1^2) - (u_1^2 + v_1^2 + s_2^2 + t_2^2)$$

Solve for  $y$  in  $(*)$  and substitute back into the first equation to get a quadratic polynomial (which I won't write in all the gory details!)

$$ax^2 + bx + c = 0 \text{ with } a, b, c \in F$$

As before, the roots have to be real, or else the circles don't intersect. The roots might be in  $F$ , in which case the intersections are all in  $F$ . Otherwise we get out our notebook and add  $F(\alpha_{k+1})$  where  $\alpha_{k+1}$  is a root of  $ax^2 + bx + c$ . In this case,  $\alpha_{k+1}$  is the  $x$ -coordinate of the intersection, and we can use  $(*)$  to solve for the  $y$ -coordinate, which is then also in  $F(\alpha_{k+1})$ . Thus  $\alpha \in F(\alpha_{k+1})$ , and this finishes the proof!

### 3.2.1 Constructible Number Exercises

**11-1** Explain how to do the three constructions of Construction 3.2.8.

**11-2** Construct the following lengths from scratch:

- (a)  $\sqrt{7}$
- (b)  $\sqrt{2 - \sqrt{2}}$
- (c)  $\sqrt{\frac{5 + \sqrt{5}}{8}}$

**11-3** Construct the following complex numbers:

- (a)  $(1; \frac{\pi}{6}) = \cos(\frac{\pi}{6}) + \sin(\frac{\pi}{6})i$
- (b)  $(1; \frac{2\pi}{5}) = \cos(\frac{2\pi}{5}) + \sin(\frac{2\pi}{5})i$
- (c)  $(1; \frac{\pi}{12}) = \cos(\frac{\pi}{12}) + \sin(\frac{\pi}{12})i$

**11-4** Find the characteristic polynomial of  $(1; \frac{2\pi}{7}) = \cos(\frac{2\pi}{7}) + \sin(\frac{2\pi}{7})i$ . Conclude from the constructible number theorem that this cannot be constructed, so general angles cannot be "heptasected" (divided by 7).

**11-5** Find the characteristic polynomial of  $(1; \frac{2\pi}{25}) = \cos(\frac{2\pi}{25}) + \sin(\frac{2\pi}{25})i$ . Conclude that this cannot be constructed, so general angles cannot be "pentasected" (divided by 5).

**11-6** For which  $n$  can  $\sqrt[n]{2}$  be constructed? What about  $\sqrt[n]{3}$ ?