CHAPTER 6: RATIONAL NUMBERS AND ORDERED FIELDS

LECTURE NOTES FOR MATH 378 (CSUSM, SPRING 2009). WAYNE AITKEN

1. Introduction

In this chapter we construct the set of rational numbers $\mathbb{Q}$ using equivalence classes of pairs of elements of $\mathbb{Z}$. Informally, the coordinates of such a pair denote the numerator and denominators of a fraction, but formally we treat them simply as ordered pairs. The first main result of this chapter is that $\mathbb{Q}$ is a field. We use a canonical embedding to view $\mathbb{Z}$ as a subset of $\mathbb{Q}$.

Although the definitions for addition and multiplication for $\mathbb{Q}$ are inspired by our prior experience with fractions, we do not use this knowledge in our proofs in the formal development. Instead the proofs are based on previous results developed for $\mathbb{Z}$ in earlier chapters. Later we do formally develop division and fractional notation for fields in general, not just $\mathbb{Q}$, and prove the main laws that govern the use of fractions. After this we can and will use fractions in our formal development.

Next we investigate the inequality relation on $\mathbb{Q}$ centered around the concept of *positive*. Many of the results discussed here hold for the field $\mathbb{R}$, developed in the next chapter. For the sake of efficiency, we develop the general notation of an *ordered field* in order to formulate and prove results that hold for both $\mathbb{Q}$ and $\mathbb{R}$.

2. Basic Definitions

We need to define $\mathbb{Q}$ and the operations of addition and multiplication on this set. Before defining $\mathbb{Q}$ we define a related set Q which informally represents quotients of integers. The difference between Q and $\mathbb{Q}$ is that the latter consists of equivalence classes of the former.

Definition 1. Let $Q = \big\{(x, y) \mid x, y \in \mathbb{Z} \text{ and } y \neq 0\big\}$. The first element x of a pair in Q is called the *numerator*, and the second element y is called the *denominator*. Elements of Q are called *numerator-denominator pairs*.

Remark 1. It might be tempting to write (x, y) symbolically as x/y. We do not do so because we will define x/y later when considering division in any field, so using x/y now could create confusion. Also, using the notation x/y might lead one to unintentionally use properties about fractions that have not yet been formally proved.

Date: May 19, 2009.

Informal Exercise 1. Using your prior informal knowledge of fractions as inspiration, how would you add and multiply (x, y) and (w, z)? How would you decide if (x, y) and (w, z) are equivalent?

We now formalize the concepts in the above exercise. First we define rational equivalence.

Definition 2. We say that two elements (x, y) and (z, w) of Q are *rationally equivalent* if $xw = yz$. In this case, we write $(x, y) \sim (z, w)$.

Theorem 1. *The relation $\sim$ is an equivalence relation on the set Q.*

Exercise 2. Prove the above theorem. Hint: the reflexive and symmetry laws involve using the commutative law for $\mathbb{Z}$. The transitivity law requires multiplying an equation by a constant, performing basic manipulations, and using the cancellation law (for a non-zero element of $\mathbb{Z}$).

Definition 3. If $(x, y) \in Q$ then $[(x, y)]$, or just $[x, y]$, denotes the equivalence class containing (x, y) under the above equivalence relation.

Definition 4. Define $\mathbb{Q}$ as follows

$$\mathbb{Q} \stackrel{\text{def}}{=} \big\{[x, y] \mid (x, y) \in Q\big\}.$$

In other words,

$$\mathbb{Q} = \big\{[x, y] \mid x, y \in \mathbb{Z} \text{ with non-zero } y\big\}.$$

Exercise 3. Prove the following two theorems.

Theorem 2. *Let $(x, y) \in Q$. Then $[x, y] = [0, 1]$ if and only if $x = 0$.*

Theorem 3. *Let $(x, y) \in Q$. Then $[x, y] = [1, 1]$ if and only if $x = y$.*

Definition 5. Define two binary operations, *addition* and *multiplication*, for $\mathbb{Q}$ as follows. Let $[x, y]$ and $[z, w]$ be elements of $\mathbb{Q}$. Then

$$[x, y] + [z, w] \stackrel{\text{def}}{=} [xw + yz,\ yw]$$

and

$$[x, y] \cdot [z, w] \stackrel{\text{def}}{=} [xz,\ yw].$$

Since these definitions involve equivalence classes, we must show that they are well-defined. This is the purpose of the following lemmas.

Lemma 4. *Addition on $\mathbb{Q}$ is well-defined.*

Proof. We want to show that if $[x, y] = [x', y']$ and $[z, w] = [z', w']$ then

$$[xw + yz,\ yw] = [x'w' + y'z',\ y'w'].$$

In other words, suppose $(x, y) \sim (x', y')$ and $(z, w) \sim (z', w')$. We must show $(xw + yz, yw) \sim (x'w' + y'z', y'w')$. By definition of $\sim$, we need to show that

$$(xw + yz)(y'w') = (x'w' + y'z')(yw).$$

This can be shown as follows:

$$
\begin{aligned}
(xw+yz)(y'w') &= (xw)(y'w')+(yz)(y'w') && \text{(Distr. Law of Ch. 3)}\\
&= (xy')(ww')+(zw')(yy') && \text{(Laws of Ch. 3)}\\
&= (yx')(ww')+(zw')(yy') && \text{(Since } (x,y)\sim(x',y')\text{)}\\
&= (yx')(ww')+(wz')(yy') && \text{(Since } (z,w)\sim(z',w')\text{)}\\
&= (x'w')(yw)+(y'z')(yw) && \text{(Laws of Ch. 3)}\\
&= (x'w'+y'z')(yw) && \text{(Distr. Law of Ch. 3).}
\end{aligned}
$$

□

Lemma 5. *Multiplication on $\mathbb{Q}$ is well-defined.*

Exercise 4. Prove the above lemma.

Exercise 5. Prove the following two theorems.

Theorem 6. *For any $[x,y]\in\mathbb{Q}$,*

$$[x,y]+[0,1]=[x,y]$$

and

$$[x,y]\cdot[1,1]=[x,y]$$

Theorem 7. *Suppose $x,y,c\in\mathbb{Z}$ where $y\neq 0$ and $c\neq 0$. Then $(cx,cy)\in Q$ and*

$$[cx,cy]=[x,y].$$

Exercise 6. Prove the following three theorems.

Theorem 8. *Addition in $\mathbb{Q}$ is commutative.*

Theorem 9. *Multiplication in $\mathbb{Q}$ is commutative.*

Theorem 10. *Suppose x,y are non-zero integers. Then*

$$[x,y]\cdot[y,x]=[1,1].$$

3. Main Theorem

Theorem 11. *The set $\mathbb{Q}$ is a field. The additive identity is $[0,1]$ and the multiplicative identity is $[1,1]$. Suppose $x,y\in\mathbb{Z}$ with $y\neq 0$. Then the additive inverse of $[x,y]$ is $[-x,y]$. If $x\neq 0$ and $y\neq 0$ then the multiplicative inverse of $[x,y]$ is $[y,x]$.*

Exercise 7. Prove the above theorem. Hint: several parts have been proved above.

4. The Canonical Embedding

Definition 6. The *canonical embedding* $\mathbb{Z} \to \mathbb{Q}$ is the function defined by the rule

$$a \mapsto [a, 1].$$

Theorem 12. *The canonical embedding $\mathbb{Z} \to \mathbb{Q}$ is injective.*

Exercise 8. Prove the above theorem.

Exercise 9. Show that $[2, 2]$ is in the image of the canonical embedding, but $[1, 2]$ is not in the image of the canonical embedding. Conclude that the canonical embedding is not surjective. Hint: suppose $[1, 2] = [a, 1]$. Derive a contradiction from $(1, 2) \sim (a, 1)$.

If we identify $a \in \mathbb{Z}$ with its image in $\mathbb{Q}$, then we can think of $\mathbb{Z}$ as a subset of $\mathbb{Q}$. So from now on, if $a \in \mathbb{Z}$, we will think of a and $[a, 1]$ as being the same element of $\mathbb{Q}$. By Theorem 7 we have that $[ca, c]$ and a are considered as the same element of $\mathbb{Q}$ (if c is non-zero), so a pair does not have to end in 1 to be an integer.

By this convention, $0 \in \mathbb{Z}$ is identified with $[0, 1]$, and $1 \in \mathbb{Z}$ is identified with its image $[1, 1]$. By Theorem 11, $0 = [0, 1]$ is the additive identity and $1 = [1, 1]$ is the multiplicative identity as expected.

Since we now think of $\mathbb{Z}$ as a subset of $\mathbb{Q}$ we have to be careful with $+$ and $\cdot$ in $\mathbb{Z}$. We defined these operations for $\mathbb{Z}$ in one way in Chapter 3, and then defined them for $\mathbb{Q}$ in the current chapter. Do we get the same answer for integers $a, b \in \mathbb{Z}$ as for the corresponding elements $[a, 1]$ and $[b, 1]$ in $\mathbb{Q}$? The answer is yes since

$$[a, 1] + [b, 1] = [a + b,\ 1] \qquad \textit{and} \qquad [a, 1] \cdot [b, 1] = [a \cdot b, 1 \cdot 1] = [ab, 1].$$

Likewise for additive inverse: by Theorem 11

$$-[a, 1] = [-a, 1].$$

This equality shows that if a is identified with $[a, 1]$, then the definitions of additive inverse, either as an integer or as a fraction, gives the same result. We summarize the above observations as follows.

Theorem 13. *Consider $\mathbb{Z}$ as a subset of $\mathbb{Q}$. Then the addition, multiplication, and additive inverse operators on $\mathbb{Q}$ extend the corresponding operators on $\mathbb{Z}$.*

Remark 2. Since subtraction (in any ring) is defined in terms of addition and additive inverse, the above theorem tells us that the subtraction of $\mathbb{Q}$ extends that of $\mathbb{Z}$.

Remark 3. In this chapter we have constructed $\mathbb{Q}$ from $\mathbb{Z}$ using equivalence classes. Everything we have done works if $\mathbb{Z}$ is replaced with an arbitrary integral domain. In other words, if R is an integral domain, the above techniques can be used to construct a field F and a canonical embedding of R into F. The field F is called the *field of fractions of R*. Thus $\mathbb{Q}$ is the field of fractions of $\mathbb{Z}$. The field F is called the field of fractions since every element of F can be written as a/b where $a, b \in R$ with $b \neq 0$ (see next section for the definition of a/b).

If R is already a field, then the canonical embedding can be shown to be a bijection.

5. Division and Fractional Notation

Before studying the field $\mathbb{Q}$ in more detail, it is helpful to have the concept of division and to set up fractional notation. These concepts are valid in any field F, not just $\mathbb{Q}$.

Definition 7. Suppose $x, y \in F$ where F is a field and where $y \neq 0$. Then x/y is defined to be $x \cdot y^{-1}$. We also write this as $\frac{x}{y}$.

Remark 4. The rule $(x, y) \mapsto x/y$ defines a function $F \times F^\times \to F$. This is almost, but not quite, a binary operation. If fails to be a binary operation due to the fact that its domain is not all of $F \times F$. We call this "almost binary" operation the *division operation.*

Observe that a field has all four traditional arithmetic operations: addition, subtraction, multiplication, and division.

Most of the familiar identities and laws concerning fractions and division are valid for general fields, and can be easily proved using the identity $(xy)^{-1} = x^{-1}y^{-1}$, an identity that is valid in any field. Here are some examples,

Theorem 14. *Suppose that $x \in F$ and $y, z \in F^\times$ where F is a field. Then*

$$\frac{zx}{zy} = \frac{x}{y}.$$

Proof. Observe that

$$\begin{aligned}
(zx)/(zy) &= (zx)(zy)^{-1} && \text{(Def. 7)} \\
&= (zx)\left(z^{-1}y^{-1}\right) && \text{(Inverse Law for fields)} \\
&= \left(xy^{-1}\right)\left(zz^{-1}\right) && \text{(Comm/Assoc. Laws for fields)} \\
&= \left(xy^{-1}\right) \cdot 1 = x/y && \text{(Def. of inverse, Def. 7).}
\end{aligned}$$

□

Theorem 15. *Suppose that $x, y, z \in F$ where F is a field and $y \neq 0$. Then*

$$\frac{x}{y} + \frac{z}{y} = \frac{x+z}{y}.$$

Proof. Observe that

$$\begin{aligned}
x/y + z/y &= xy^{-1} + zy^{-1} && \text{(Def. 7)} \\
&= (x+z)y^{-1} && \text{(Distr. Law for rings)} \\
&= (x+z)/y && \text{(Def. 7)}
\end{aligned}$$

□

Theorem 16. *Suppose $x, z \in F$ and $y, w \in F^\times$ where F is a field. Then*

$$\frac{x}{y} + \frac{z}{w} = \frac{xw + yz}{yw}.$$

Proof. Observe that

$$\begin{aligned}
(xw + yz)/(yw) &= (xw + yz)(yw)^{-1} && \text{(Def. 7)}\\
&= (xw)(yw)^{-1} + (yz)(yw)^{-1} && \text{(Distr. Law for rings)}\\
&= (xw)/(yw) + (yz)/(yw) && \text{(Def. 7)}\\
&= x/y + z/w && \text{(Thm. 14)}
\end{aligned}$$

□

Exercise 10. Let $x, z \in F$ and $y, w \in F^\times$ where F is a field. Prove the following

$$\frac{x}{y} \cdot \frac{z}{w} = \frac{xz}{yw}, \qquad \frac{0}{y} = 0, \qquad \frac{y}{y} = 1,$$

$$\frac{x}{1} = x, \qquad x\frac{z}{y} = \frac{xz}{y}, \qquad y\frac{x}{y} = x.$$

Exercise 11. Let $x, y \in F$ where F is a field and y is not zero. Then show that x/y and $(-x)/y$ are additive inverses. Conclude that

$$-\frac{x}{y} = \frac{-x}{y} \qquad \text{and} \qquad -\frac{-x}{y} = \frac{x}{y}.$$

Exercise 12. Let $x, y \in F^\times$ where F is a field. Then show that x/y and y/x are multiplicative inverses. Conclude that

$$\frac{1}{x/y} = \frac{y}{x}.$$

Theorem 17. *Let $x, z \in F$ and $y, w \in F^\times$ where F is a field. Then*

$$\frac{x}{y} = \frac{z}{w} \iff xw = yz,$$

and

$$\frac{x}{y} = \frac{z}{y} \iff x = z.$$

Proof. Multiply both sides of each equation by the appropriate constant. □

6. Further properties of $\mathbb{Q}$

The above concepts and properties apply to any field. Now we use these concepts and properties in the context of $\mathbb{Q}$. First we see that $[x, y]$ can be thought of as the fraction x/y.

Theorem 18. *Let $x, y \in \mathbb{Z}$ where $y \neq 0$. Think of $\mathbb{Z}$ as a subset of $\mathbb{Q}$ via the canonical embedding. Then*

$$[x, y] = \frac{x}{y}.$$

Proof. By definition of multiplication in $\mathbb{Q}$, we have $[x, y] = [x, 1] \cdot [1, y]$. However, $[1, y] = [y, 1]^{-1}$. Thus

$$[x, y] \;=\; [x, 1] \cdot [y, 1]^{-1}.$$

We identify x with $[x, 1]$ and y with $[y, 1]$. Therefore,

$$[x, y] \;=\; x \cdot y^{-1} = x/y.$$

□

Corollary 19. *Think of $\mathbb{Z}$ as a subset of $\mathbb{Q}$ via the canonical embedding. Then*

$$\mathbb{Q} = \left\{ \frac{a}{b} \;\middle|\; a, b \in \mathbb{Z} \text{ and } b \neq 0 \right\}.$$

Remark 5. Another consequence of the above theorem is that the canonical embedding is given by the law $a \mapsto a/1$.

In $\mathbb{Q}$ we can be picky and insist that the denominator be positive:

Theorem 20. *If $r \in \mathbb{Q}$ then there are integers a, b such that*

$$r = \frac{a}{b}$$

and such that b is positive. In particular,

$$\mathbb{Q} = \left\{ \frac{a}{b} \;\middle|\; a, b \in \mathbb{Z} \text{ and } b > 0 \right\}.$$

Exercise 13. Prove the above theorem. Hint: use Theorem 14 if necessary.

Lemma 21. *If $r \in \mathbb{Q}$ then there are relatively prime integers $a, b \in \mathbb{Z}$ such that $b > 0$ and such that $r = a/b$.*

Proof. By Theorem 20 there are $a', b' \in \mathbb{Z}$ such that $b' > 0$ and $r = a'/b'$. This theorem does not guarantee that a', b' are relatively prime, so let g be the GCD of a' and b'. Thus a' and b' are multiples of g, so we can find $a, b \in \mathbb{Z}$ such that $a' = ga$ and $b' = gb$. Since g and b' are postive, b must also be positive. By Theorem 14, $r = a/b$.

Are a and b relatively prime? Let d be the GCD of a and b. We must show $d = 1$. Since $d \mid a$ we have $dg \mid ag$. In other words, $dg \mid a'$. Likewise, $dg \mid b'$. Thus dg is a common divisor of a' and b', but g is the greatest such common divisor. So $d = 1$. Thus a and b are relatively prime. □

Theorem 22. *If $r \in \mathbb{Q}$ then there is a unique pair a, b of relatively prime integers such that $b > 0$ and*

$$r = \frac{a}{b}.$$

Proof. The existence is established by the previous lemma. If $r = 0$, then $a = 0$ and $b = 1$ is the unique pair that works (if $b > 0$ and $a = 0$ then the GCD of b and a is just b). So assume $a \neq 0$, and suppose c, d is another such pair. Since $a/b = c/d$ we get $ad = bc$. Thus $b \mid ad$. Of course, $a \mid ad$. By a theorem of Chapter 4, $ab \mid ad$ since a and b are relatively prime. Thus $b \mid d$. A similar argument shows that $d \mid b$. By a result of Chapter 4, $|b| = |d|$. Since b and d are positive, $b = d$. This, in turn, implies that $a = c$. □

If we do not insist on the relatively prime condition, we can always find a common denominator for any two elements of $\mathbb{Q}$:

Theorem 23. *If $u, v \in \mathbb{Q}$ then we can find integers a, b, d with $d > 0$ such that*

$$u = \frac{a}{d} \quad \textit{and} \quad v = \frac{b}{d}.$$

Exercise 14. Prove the above theorem.

Division is related to divisibility:

Theorem 24. *Let $a, b \in \mathbb{Z}$ with $b \neq 0$. Then $a/b \in \mathbb{Z}$ if and only if $b \mid a$.*

Proof. If $a/b \in \mathbb{Z}$ then $ab^{-1} = c$ for some $c \in \mathbb{Z}$. Multiply both sides by b. Thus $a = bc$. In other words, $b \mid a$.

If $b \mid a$ then $a = bc$ for some $c \in \mathbb{Z}$. Multiply both sides by b^{-1}. $\square$

Remark 6. If $a, b \in \mathbb{Z}$ are such that $b \mid a$ and $b \neq 0$, then a/b was defined in Chapter 4 as the unique integer c such that $bc = a$. By multiplying $bc = a$ by b^{-1} we see that $c = ab^{-1}$. Thus the current (Chapter 6) definition of division is equivalent to the definition of Chapter 4.

7. Positive and Negative Rational Numbers

The set $\mathbb{Q}$ is not just a field, but is an *ordered field*. We will define the notion of ordered field later, but a key part of the definition is the idea of a positive subset. In this section we define the subset of positive rational numbers.

Definition 8 (Positive and Negative)**.** A number $r \in \mathbb{Q}$ is said to be a *positive* rational number if it can be written as a/b where a and b are positive integers. An number $r \in \mathbb{Q}$ is a said to be a *negative* rational number if $-r$ is positive.

Remark 7. We already know, from Chapter 3, what positive and negative integers are. The above extends the definitions to rational numbers. Lemma 28 below shows that the new definitions truly extend the old definitions.

Theorem 25. *The set of positive rational numbers is closed under addition and multiplication: if $u, v \in \mathbb{Q}$ are positive, then so are $u + v$ and uv.*

Exercise 15. Prove the above. Hint: write $u = a/b$ and $v = c/d$ where a, b, c, d are positive integers. Use properties of positive integers from Ch. 3.

Theorem 26. *Let $a/b \in \mathbb{Q}$ where $a, b \in \mathbb{Z}$ with $b \neq 0$. Then a/b is a positive rational number if and only if either (i) both a and b are positive integers or (ii) both a and b are negative integers.*

Proof. First suppose that a/b is a positive rational number. By Definition 8, $a/b = c/d$ for some positive integers c and d. Thus $ad = bc$. Now we consider cases. First suppose that b is a positive integer. Then bc is a positive integer (Chapter 3). Thus ad is a positive integer. Since d is a positive integer, we must also have that a is a positive integer.

In the second case, suppose that b is a negative integer. Then bc is a negative integer (Chapter 3). Thus ad is a negative integer. Since d is a positive integer, we must also have that a is a negative integer.

Now we prove the converse. If a and b are positive integers, the result follows from Definition 8. If a and b are negative integers, then $a/b = (-a)/(-b)$ by Theorem 14. Now use Definition 8 with $-a$ and $-b$. $\square$

Theorem 27. *Let $a/b \in \mathbb{Q}$ where $a, b \in \mathbb{Z}$ with $b \neq 0$. Then a/b is a negative rational number if and only if either (i) a is a positive integer and b is a negative integer, or (ii) a is a negative integer and b is a positive integer.*

Proof. First suppose that a/b is a negative rational number. By Definition 8, $-(a/b)$ is positive, but $-(a/b) = (-a)/b$ by Exercise 11. So, by the previous theorem, $-a$ and b are either both positive or both negative. The result follows from results of Chapter 3.

Conversely, suppose (i) or (ii) holds. This implies that $-a$ and b are either both positive or both negative. Thus, by definition, $(-a)/b$ is positive. But $-(a/b) = (-a)/b$ by Exercise 11. So $-(a/b)$ is a positive rational number. Thus a/b is a negative rational number by Definition 8. $\square$

We now show that the definitions of positive and negative numbers really do extend the definitions of positive and negative integer.

Lemma 28. *Let $a \in \mathbb{Z}$. Then $a/1$ is a positive rational number if and only if a is a positive integer. Likewise, $a/1$ is a negative rational number if and only if a is a negative integer.*

Proof. If $a/1$ is a positive rational number then, since 1 is a positive integer, it follows that a is a positive integer (Theorem 26). Conversely, if a is a positive integer, then $a/1$ is a positive rational number since 1 is a positive integer (Theorem 26).

If $a/1$ is a negative rational number then, since 1 is a positive integer, it follows that a is a negative integer (Theorem 27). Conversely, if a is a negative integer, then $a/1$ is a negative rational number since 1 is a positive integer (Theorem 27). $\square$

Theorem 29 (Trichotomy version 1)**.** *If $r \in \mathbb{Q}$ then exactly one of the following occurs: (i) $r = 0$, (ii) r is positive, (iii) r is negative.*

Exercise 16. Prove the above theorem. Hint: you can use Theorem 20 to simplify your proof.

8. Ordered fields

Definition 9. An *ordered field* F is a field with a designated subset P such that (i) P is closed under addition and multiplication, and (ii) for any element $u \in F$ exactly one of the following occurs: $u = 0, u \in P, -u \in P$.

Remark 8. When we say that P is *closed under addition and multiplication*, we mean that if $x, y \in P$ then $x + y$ and $x \cdot y$ are in P.

Definition 10. Let F be an ordered field with designated subset P. The elements in P are called the *positive elements*.

Here is the second important theorem in this chapter.

Theorem 30. *The field $\mathbb{Q}$ is an ordered field.*

Exercise 17 (Easy). Prove the above theorem using earlier theorems.

Exercise 18. Show that the field $\mathbb{F}_5$ cannot qualify as an ordered field. Hint: try all possible subsets for P, and show that none work.

Remark 9. This extends: no $\mathbb{F}_p$ can be an ordered field. In fact, ordered fields must be infinite. Later we will study the complex numbers $\mathbb{C}$ which is an example of an infinite field that is not an ordered field.

Definition 11. Let F be an ordered field with designated subset P. As in the case of $F = \mathbb{Q}$, if $u \in F$ is such that $-u \in P$ then u is said to be *negative*. We often write the designated subset P as $F_{>0}$.

For most of the rest of the chapter we will consider theorems about a general ordered field F. The only ordered field we have constructed so far is $\mathbb{Q}$, so you can think of F as being something like $\mathbb{Q}$. You can freely use all the standard laws of algebra of $\mathbb{Q}$ that are true in a general field. Later we will construct the real numbers $\mathbb{R}$, another ordered field, and everything we prove about ordered fields will apply to $\mathbb{R}$. There are other ordered fields in mathematics, but we will not need to discuss them in this course.

As the name suggests, an ordered field is ordered: it has a natural order relation on it. This order is defined as follows.

Definition 12. Let F be an ordered field, and let $x, y \in F$. If $y - x$ is positive then we write $x < y$. We also write $y > x$ in this case.

Exercise 19. Show that $y - x$ is negative if and only if $y < x$. Here x and y are in an ordered field.

Exercise 20. Prove the two following theorems.

Theorem 31. *Suppose $u \in F$ where F is an ordered field. Then u is positive if and only if $u > 0$. Similarly, u is negative if and only if $u < 0$.*

Theorem 32 (Transitivity)**.** *Suppose $x, y, z \in F$ where F is an ordered field. If $x < y$ and $y < z$ then $x < z$.*

Theorem 33. *Suppose $x, y, z \in F$ where F is an ordered field. If $x < y$ then $x + z < y + z$.*

Exercise 21. Prove the above theorem. Hint: simplify $(y + z) - (x + z)$.

Theorem 34. *Let $x, y, x', y' \in F$. If $x < y$ and $x' < y'$ then $x + x' < y + y'$.*

Proof. By Theorem 33, transitivity, and the commutative law for fields, we have

$$x + x' < y + x' < y' + y'.$$

□

Theorem 35 (Trichotomy version 2)**.** *Suppose $x, y \in F$ where F is an ordered field. Then exactly one of the following occurs: (i) $x = y$, (ii) $y < x$, or (iii) $x < y$.*

Exercise 22. Prove the above. Hint: Use the second part of the definition of ordered field. (i) occurs if and only if $x - y = 0$, (ii) occurs if and only if $x - y$ is positive, and (iii) occurs if and only if $-(x - y)$ is positive.

Theorem 36. *Suppose $x, y \in F$ where F is an ordered field. If x and y are positive, then xy is positive. If x is positive, but y is negative, then xy is negative. If x and y are negative, then xy is positive.*

Proof. The first statement follows from the definition of ordered field: the positive elements are closed under multiplication.

In the second statement, $-y$ is positive by definition of negative. Thus $x(-y)$ is positive by closure. But $x(-y) = -(xy)$ since F is a field (this is true in any ring). Thus $-(xy)$ is positive, so xy is negative.

In the third statement, $-x$ and $-y$ are positive. So $(-x)(-y)$ is positive by closure. But, since F is a field,

$$(-x)(-y) = -\big(x(-y)\big) = -\big(-(xy)\big) = xy.$$

Thus xy is positive. □

Theorem 37. *Suppose $x, y, z \in F$ where F is an ordered field. If $x < y$, and if z is positive, then $xz < yz$. If $x < y$, and if z is negative, then $xz > yz$.*

Exercise 23. Prove the above theorem. Hint: multiply $y - x$ and z.

The follow statement is already known for $F = \mathbb{Q}$. The point of proving it here is to show that it is true of any other possible ordered field F.

Theorem 38. *The element $1 \in F$ is positive, and -1 is negative.*

Proof. Since $0 \neq 1$ in any field, we have that 1 is either positive or negative (by definition of ordered field). Suppose 1 is negative. Then $1 \cdot 1$ is positive by Theorem 36. But $1 \cdot 1 = 1$, so 1 is positive, a contradiction.

Since 1 is positive, -1 is negative by definition of negative. □

Theorem 39. *Suppose x is a positive element of an ordered field F. Then x^{-1} is also positive. Suppose x is a negative element of F. Then x^{-1} is also negative.*

Proof. Suppose x is positive. Observe that x^{-1} cannot be 0: otherwise $1 = xx^{-1} = 0$ which is not allowed in a field. Observe that x^{-1} cannot be negative: otherwise $xx^{-1} = 1$ must be negative (Theorem 36) contradicting Theorem 38. Thus, by trichotomy, x^{-1} is positive.

The proof of the second claim is similar. □

Theorem 40. *Suppose x, y are positive elements of an ordered field F. If $x < y$ then $y^{-1} < x^{-1}$.*

Proof. Multiply both sides of $x < y$ by $x^{-1}y^{-1}$. □

Now we consider the special case where $F = \mathbb{Q}$. Recall that $\mathbb{Z}$ is regarded as a subset of $\mathbb{Q}$. We have an order for $\mathbb{Z}$ from Chapter 3, and an order for $F = \mathbb{Q}$ defined in the current section. We now show that the new order extends the old order.

Lemma 41. *The order relation $<$ on $\mathbb{Q}$ extends the order relation $<$ on $\mathbb{Z}$. In other words, if $a, b \in \mathbb{Z}$, then $a < b$ (as defined in Chapter 3) if and only $a/1 < b/1$ (as defined in this section).*

Proof. Suppose that $a < b$ in the sense of Chapter 3. Then $b - a$ is a positive integer. Thus $(b - a)/1$ is positive (Lemma 28). Since

$$b/1 - a/1 = b/1 + (-a)/1 = (b - a)/1,$$

we have that $b/1 - a/1$ is positive. Thus, by Definition 12, $a/1 < b/1$ in the sense of the current section. The converse is similar. □

Theorem 42. *Suppose a and b are integers, and d is a positive integer. Then $a/d > b/d$ if and only if $a > b$.*

Proof. If $a/d > b/d$, then multiply both sides by d to show $a > b$. Conversely, suppose that $a > b$. Multiply both sides by d^{-1}. Now $d^{-1} > 0$ by Theorem 39. Thus $a/d > b/d$. □

9. Less than or equal

Let F be an ordered field.

Definition 13. If $x, y \in F$ then $x \le y$ means $(x < y) \vee (x = y)$. We also write $y \ge x$ in this case.

Theorem 43. *Let $x, y \in F$. Then the negation of $x < y$ is $y \le x$. The negation of $y \le x$ is $x < y$.*

Proof. By trichotomy (Theorem 35),

$$\neg(x < y) \iff y \le x.$$

The contrapositive of the above gives

$$\neg(y \le x) \iff x < y.$$

□

Theorem 44 (Mixed transitivity)**.** *Let $x, y, z \in F$. If $x < y$ and $y \le z$ then $x < z$. Likewise, if $x \le y$ and $y < z$ then $x < z$.*

Proof. Suppose that $x < y$ and $y \le z$. By definition of $y \le z$, we have either $y < z$ or $y = z$. In the first case, use transitivity of $<$ (Theorem 32). In the second case, use substitution. In either case $x < z$. This proves the first statement. The proof of the second is similar. □

Theorem 45 (Transitivity)**.** *Let $x, y, z \in F$. If $x \le y$ and $y \le z$ then $x \le z$.*

Proof. Suppose that $x \le y$ and $y \le z$. By definition of $x \le y$, we have either $x < y$ or $x = y$. In the first case, use mixed transitivity (Theorem 44). In the second case, use substitution. In either case $x \le z$ as desired. □

Theorem 46. *Let $x, y, z \in F$. If $x \le y$ then $x + z \le y + z$.*

Proof. By definition of $x \le y$, we have either $x < y$ or $x = y$. In the first case, $x + z < y + z$ by an earlier result (Theorem 33). In the second case, $x + z = y + z$. In either case $x + z \le y + z$ as desired. □

Theorem 47. *Let $x, y, z \in F$ where $x \le y$. If $z \ge 0$ then $xz \le yz$. If $z \le 0$ then $yz \le xz$.*

Proof. If $z = 0$ or $x = y$ then $xz = yz$, and both statements are true (both $xz \le yz$ and $yz \le xz$ hold). So we can assume that $z \ne 0$ and $x < y$. Now use Theorem 37. □

Theorem 48. *Let $x, y, x', y' \in F$. If $x \le y$ and $x' \le y'$ then $x + x' \le y + y'$.*

Proof. By Theorem 46, transitivity, and the commutative law for fields, we have

$$x + x' \le y + x' \le y' + y'.$$

□

Here is an easy result that will be useful in Chapter 6.

Theorem 49. *For all $r \in \mathbb{Q}$, then there is an $n \in \mathbb{Z}$ such that $r \le n$.*

Proof. If $r \le 0$ then let $n = 0$. So we can assume r is positive. By definition there are positive $a, b \in \mathbb{Z}$ with $r = a/b$. Since $1 \le b$ we have $a \le ab$. By Theorem 39, $b^{-1} > 0$. So $ab^{-1} \le (ab)b^{-1}$. Thus $a/b \le a$. Let $n = a$. □

10. Absolute Value

Let F be an ordered field.

Definition 14. The *absolute value* $|x|$ of $x \in F$ is defined as follows.

$$|x| \stackrel{\text{def}}{=} \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0 \end{cases}$$

Theorem 50. *If $x \in F$ then $|x| \geq 0$.*

Proof. If $x \geq 0$ then $|x| = x$, so $|x| \geq 0$. If $x < 0$ then $|x| = -x$. Adding $-x$ to both sides of $x < 0$ gives $0 < -x$. Thus $|x| = -x > 0$ in this case. □

Remark 10. The above theorem shows that the absolute value defines a function $F \to F_{\geq 0}$ where $F_{\geq 0}$ is the set $\{x \in F \,|\, x \geq 0\}$.

Informal Exercise 24. Is the function $F \to F_{\geq 0}$ defined by $x \mapsto |x|$ injective? Is it surjective?

The following is an easy consequence of the definition.

Theorem 51. *Let $x \in F$. Then*

$$|x| = 0 \iff x = 0.$$

Theorem 52. *Let $x \in F$. Then*

$$|x| > 0 \iff x \neq 0.$$

Proof. Use the contrapositive of the above, and the fact that $|x| \geq 0$. □

Theorem 53. *Let $x \in F$. Then $|x| = |-x|$.*

Proof. We use trichotomy to divide the proof into three cases.

If $x > 0$ then $|x| = x$ and $|-x| = -(-x) = x$ (since $-x < 0$).

If $x = 0$ then $|x| = x = 0$ and $|-x| = -x = 0$ (since $-x = 0$).

If $x < 0$ then $|x| = -x$ and $|-x| = -x$ (since $-x > 0$). □

Absolute value is compatible with multiplication.

Theorem 54. *Let $x, y \in F$. Then*

$$|xy| = |x| \cdot |y|.$$

Proof. We divide the proof into cases using trichotomy.

If both x and y are positive then so is xy (Theorem 36). Thus $|xy| = xy$ and $|x||y| = xy$.

If both x and y are negative, then xy is positive (Theorem 36). Thus $|xy| = xy$ and

$$|x||y| = (-x)(-y) = -\big(x(-y)\big) = -\big(-(xy)\big) = xy.$$

If either $x = 0$ or $y = 0$ then $|xy| = 0$ and $|x||y| = 0$.

If x is positive and y is negative, then xy is negative (Theorem 36). Thus $|xy| = -xy$ and $|x||y| = x(-y) = -xy$.

The case where x is negative and y is positive is similar. □

Lemma 55. *If $x \in F$ then $x \leq |x|$ and $-x \leq |x|$.*

Proof. We use trichotomy to divide into cases.

If $x = 0$ then $|x| = 0$ and $-x = 0$. So obviously $x \leq |x|$ and $-x \leq |x|$.

If $x > 0$ then $x = |x|$, so $x \leq |x|$. Also $-x < 0$ and $0 < |x|$, so $-x \leq |x|$.

If $x < 0$ then $-x = |x|$, so $-x \leq |x|$. Since $x < 0$ and $0 \leq |x|$ (Theorem 50), we have $x \leq |x|$. □

Theorem 56. *Suppose $x, y \in F$ where $y \geq 0$. Then*
(i) $|x| < y$ if and only if $-y < x < y$,
(ii) $|x| > y$ if and only if $x > y$ or $x < -y$, and
(iii) $|x| = y$ if and only if $x = y$ or $x = -y$.

Proof. (ia) Suppose that $|x| < y$. Now $x \leq |x|$ (by Lemma 55). So $x < y$ by transitivity (Theorem 44). Also $-x \leq |-x|$ (Lemma 55) and $|-x| = |x|$ (Theorem 53), so $-x \leq |x|$. Thus $-x < y$ by transitivity (Theorem 44). Adding $x - y$ to both sides gives $-y < x$ (Theorem 33). We have both $x < y$ and $-y < x$, so $-y < x < y$.

(ib) Suppose $-y < x < y$. If $x \geq 0$ then $|x| = x$, so $|x| < y$. Otherwise, $x < 0$. Adding $y - x$ to both sides of $-y < x$ gives $-x < y$ (see Theorem 33). Since $|x| = -x$, we have $|x| < y$.

We leave the proofs of (ii) and (iii) to the reader. □

Exercise 25. Prove (ii) and (iii) of the above theorem.

Corollary 57. *Suppose $x, y \in F$ where $y \geq 0$. Then*
(i) $|x| \leq y$ if and only if $-y \leq x \leq y$,
(ii) $|x| \geq y$ if and only if $x \geq y$ or $x \leq -y$, and

The following is sometimes called the "triangle inequality" since the analogous vector version says that the third side of a triangle can be no larger than the sum of the lengths of the other two sides.

Theorem 58. *If $x, y \in F$ then*

$$|x + y| \leq |x| + |y|.$$

Proof. We have $x \leq |x|$ and $y \leq |y|$ (Lemma 55). Thus $x + y \leq |x| + |y|$ (Theorem 48).

We have $-x \leq |x|$ and $-y \leq |y|$ (Lemma 55). Adding $x - |x|$ to both sides of $-x \leq |x|$ gives $-|x| \leq x$ (see Theorem 46). Likewise, $-|y| \leq y$. So $-(|x| + |y|) \leq x + y$ (Theorem 48). Thus

$$-(|x| + |y|) \leq x + y \leq |x| + |y|.$$

By Corollary 57 (i),

$$|x + y| \leq |x| + |y|.$$

□

11. Density

In this section, we will show that any ordered field F, including $\mathbb{Q}$, is dense. In other words, for all $x, y \in F$ with $x < y$ there is a $z \in F$ with $x < z < y$. So you can always find new elements between two given elements.

The proof is simple: show that the average $(x+y)/2$ is between x and y. One question: is $2 \in F$? Of course, in the case of $\mathbb{Q}$ the answer is clearly yes: $\mathbb{Q}$ contains $\mathbb{Z}$. In general, it can be shown that $\mathbb{Z}$ can be embedding into any ordered field. Instead of showing this now, we make an *ad hoc* definition of the number two. This makes 2 a member of any ordered field.

Definition 15. Let 1 be the multiplicative identity of an ordered field F. Define 2 to be $1+1$.

Remark 11. If we needed to, we could define 3 to be $1+1+1$, and so on. This works not just for ordered fields, but for any ring whatsoever. However, in some rings, including the ring $\mathbb{Z}_3$, we would have $3 = 0$.

Remark 12. Observe that 2 is positive in any ordered field F since $1 \in F$ and the set of positive elements is closed under addition. Thus, in an ordered field, 2^{-1} exists and is positive.

Theorem 59. *Let F be an ordered field. Let $x, y \in F$ be such that $x < y$. Then we can find an element $z \in F$ with $x < z < y$. In other words, F is dense.*

Proof. Let $z = (x+y)/2$.

Since $x < y$ we have $x+x < x+y$. Now $x+x = 1\cdot x+1\cdot x = (1+1)x = 2x$. So $2x < x+y$. Since 2 is positive, 2^{-1} is positive. Thus $x < (x+y)/2$.

Since $x < y$ we have $x+y < y+y$. Now $y+y = 1\cdot y+1\cdot y = (1+1)y = 2y$. So $x+y < 2y$. Since 2 is positive, 2^{-1} is positive. Thus $(x+y)/2 < y$. $\square$

12. Appendix: Remarks and corrections

In a future draft of this appendix, I will include show how to embed $\mathbb{Q}$ into any ordered field. Thus we can regard any ordered field F as an extension of $\mathbb{Q}$. This shows that $\mathbb{Z}$ can be embedding into F as mentioned in Remark 11.