

MATH 304: CONSTRUCTING THE REAL NUMBERS[†]

Peter Kahn

Spring 2007

Contents

3	The Rational Numbers	1
3.1	The set \mathbb{Q}	1
3.2	Addition and multiplication of rational numbers	5
3.2.1	Definitions and properties.	5
3.2.2	Connections with \mathbb{Z}	10
3.2.3	Better notation.	11
3.2.4	Solving the equations $E_{a,b}$ and $M_{a,b}$	13
3.3	Ordering the rational numbers	14
3.4	Extending \mathbb{Q}	19
3.4.1	Adjoining roots of polynomials to \mathbb{Q}	20
3.4.2	Holes in \mathbb{Q}	21
3.4.3	Optional: Defining some sequences of rationals by induction	26

3 The Rational Numbers

3.1 The set \mathbb{Q}

As discussed at the end of the last section, we begin our construction of the rational numbers with the same kind of motivation that led to our construction of \mathbb{Z} . Namely, we begin with the equations

$$M_{a,b} : ax = b. \tag{1}$$

These are defined for any integers a and b , but, for the reasons already discussed, *we restrict exclusively to the cases in which $a \neq 0$* . We have seen that not all these

[†]©May 21, 2007

equations have integer solutions. So, we seek to enlarge the system of integers so that unique solutions to these equations always exist in the enlarged system and so that the enlarged system obeys algebraic rules similar to those described for the integers. Therefore, in this effort, we may use only the properties of the integers that we developed in the previous sections, together with the assumption that our enlarged system must obey similar rules.

We again postulate the existence of hypothetical solutions to the equations and conduct mental experiments to determine what requirements there may be, if any, for such solutions to be unique or for two equations to have the same solution.

Just as before, we can show that hypothetical solutions to the equations (1) are unique without any conditions other than what we have already stipulated: namely that $a \neq 0$. For example, if both $ar = b$ and $as = b$, then $ar = as$, and multiplicative cancellation (Theorem 5 (h)) would imply that $r = s$. (Here is where the condition $a \neq 0$ is critical, since this is required by Theorem 5 (h).) Therefore, equation $M_{a,b}$ determines its hypothetical solution uniquely.

Hypothetical solutions are unique

Next, if both $ar = b$ and $cr = d$ are valid, then there are then two possibilities: (i) $r = 0$, or (ii) $r \neq 0$. In case (i), the given equations, together with Exercise 20 in the *Integers* notes, imply that $b = 0$ and $d = 0$, which immediately imply that $ad = bc$. In case (ii), we multiply the first equation by d and the second by b , obtaining $adr = bd = bcr$, and then we cancel r from the expressions on the left and right, again obtaining $ad = bc$. Consequently, in either case, if $M_{a,b}$ and $M_{c,d}$ have the same solution, then

Condition for two equations to have same solution

$$ad = bc. \tag{2}$$

The following exercise asks you to prove the converse of this implication.

Exercise 1. Suppose that condition (2) holds and that r is a hypothetical solution to $M_{a,b}$ and s is a hypothetical solution to $M_{c,d}$. Prove that $r = s$. (Remember that we are assuming $a \neq 0$ and $c \neq 0$.)

It follows that condition (2) is *equivalent* to the fact that $M_{a,b}$ and $M_{c,d}$ have the same solution.

We may now proceed by analogy with what we did to construct \mathbb{Z} .

First, we consider the set of all ordered pairs (b, a) , where b ranges over all of \mathbb{Z} and a ranges over all integers except zero. This last set may be denoted as the set-difference $\mathbb{Z} \setminus \{0\}$. Therefore, the set of ordered pairs that we consider is none other than the Cartesian product $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$, which we temporarily call \mathcal{Q} for short. We think of the pair (b, a) as a symbol corresponding to the equation $M_{a,b}$ (or rather, corresponding to a hypothetical solution to $M_{a,b}$), analogously to what we did when we constructed the integers. And, just as then, we have to use an equivalence relation to relate two pairs that should correspond to the same hypothetical solution (which, in this case, means that they satisfy condition (2)).

The reader will notice that we have “reversed” the order of a and b in this pair: a precedes b in the notation $M_{a,b}$, and it follows b in (b, a) . *There is no mathematical reason for this. Rather, it is for later notational ease.* We are going to want the solution to $M_{a,b}$ to correspond to the so-called fraction b/a , in which convention has the so-called “denominator” a following the so-called “numerator” b . It is easier to visualize b/a as corresponding to the pair (b, a) than as corresponding to the pair (a, b) .

We now define the desired relation \approx on \mathcal{Q} as follows: for any integers a, b, c, d

**Construct-
ing**
 \mathbb{Q}

such that $a \neq 0$ and $c \neq 0$,

$$(b, a) \approx (d, c) \iff ad = bc. \tag{3}$$

**Multi-
plicative
solution
equivalence**

We'd like to call this relation "solution-equivalence," just as we did before. But since we don't want to risk any confusion with the earlier usage, we'll use the awkward name "multiplicative-solution-equivalence" when we wish to call \approx something. Mostly, we'll use the symbol \approx when discussing the relation.

The similarity between the condition for the earlier-defined relation of solution-equivalence and the condition for \approx should be obvious: the former is just the additive version of the latter.

Exercise 2. Prove that \approx is an equivalence relation on \mathcal{Q} .

Definition 1. The quotient set \mathcal{Q}/\approx is denoted \mathbb{Q} and is called the set of *rationals* or the set of *rational numbers*. An element of \mathbb{Q} , by definition, is a \approx -equivalence class of ordered pairs of integers (b, a) , with $a \neq 0$. We would usually denote the \approx -equivalence class of (b, a) by $[(b, a)]$, but, for now, we'll use the more efficient notation $\langle b, a \rangle$. Such a class is called a *rational number*.

Since, as we have confirmed, each equation $M_{a,b}$ determines a unique hypothetical solution, and two equations $M_{a,b}$ and $M_{c,d}$ determine the same solution if and only if $(b, a) \approx (d, c)$, it makes sense to consider using \mathbb{Q} as a candidate for the set of solutions to the equations (1). Just as we did in the case of constructing \mathbb{Z} as an extension of \mathbb{N} , however, we face a number of tasks before we can use \mathbb{Q} as the appropriate extension of \mathbb{Z} . We begin these tasks by defining addition and multiplication of rationals.

3.2 Addition and multiplication of rational numbers

3.2.1 Definitions and properties.

The definitions of addition and multiplication of rational numbers are motivated by the same kind of considerations that led to the definitions of these operations for integers.

Thus, let r and s be hypothetical solutions to equations $M_{a,b}$ and $M_{c,d}$:

$$ar = b$$

$$cs = d.$$

Multiplying the first of these by c and the second by a and adding yields

$$ac(r + s) = ad + bc, \tag{4}$$

**Adding
hypo-
thetical
solutions**

whereas multiplying both equations together yields

$$acrs = bd. \tag{5}$$

**Multi-
plying
hypo-
thetical
solutions**

Equation (4) suggests how we should define addition of rationals, whereas equation (5) suggests the definition of multiplication of rationals. We now give the formal definitions.

Definition 2. Let $\langle b, a \rangle$ and $\langle d, c \rangle$ be any rational numbers. We define binary

operations $+$ and \cdot for rational numbers by the following equations:

$$\langle b, a \rangle + \langle d, c \rangle = \langle ad + bc, ac \rangle$$

$$\langle b, a \rangle \cdot \langle d, c \rangle = \langle bd, ac \rangle .$$

Notice that the “ $+$ ” symbol on the left-hand side of the first equation represents the new addition operation being defined, whereas the same symbol on the right-hand side represents the addition of integers. Similarly, “ \cdot ” on the left-hand side of the second equation represents the new multiplication, whereas the products on the right-hand side have already been defined. This time we have not used alternative symbols, such as \otimes for the new operations, as we did when first defining multiplication of integers, trusting that the reader will have no trouble understanding from the context which are the new operations and which are not. As usual, we often leave out the \cdot symbol when convenient, using simple juxtaposition to denote multiplication.

Clearly the definition conforms to our usual notions of adding and multiplying fractions.

Of course, just as before, one must verify that the operations presented in Definition 2 are truly well-defined.

Exercise 3. Prove that $+$ and \cdot are well-defined for rational numbers.

Using the result of this exercise, we may now take the two operations as being well-defined. The facts in the following exercise can be proved directly from the definitions of the operations.

Exercise 4. Verify the following: (a) For any integer $a \neq 0$, $\langle 0, a \rangle = \langle 0, 1 \rangle$, and $\langle a, a \rangle = \langle 1, 1 \rangle$. (b) For any $\langle b, a \rangle$, $\langle 0, 1 \rangle \cdot \langle b, a \rangle = \langle 0, 1 \rangle$. (c) For any

$\langle b, a \rangle$, $\langle b, -a \rangle$ is defined, and $\langle -b, a \rangle = \langle b, -a \rangle$. (d) For any $\langle b, a \rangle$, $\langle -b, -a \rangle$ is defined, and $\langle b, a \rangle = \langle -b, -a \rangle$. (e) For any integers a, b, c , such that $a \neq 0$ and $c \neq 0$, the rational number $\langle bc, ac \rangle$ is defined, and it equals $\langle b, a \rangle$. (f) For any $\langle b, a \rangle$ and $\langle d, a \rangle$, we have $\langle b, a \rangle + \langle d, a \rangle = \langle b + d, a \rangle$.

The following theorem lists the basic algebraic properties of the rational numbers. These follow directly from the definitions, and verification is left to exercises below.

Theorem 1. *Let $\langle b, a \rangle, \langle d, c \rangle, \langle f, e \rangle$ be any rational numbers. Then:*

a. $\langle b, a \rangle + (\langle d, c \rangle + \langle f, e \rangle) = (\langle b, a \rangle + \langle d, c \rangle) + \langle f, e \rangle$. (*additive associative law*)

b. $\langle b, a \rangle + \langle 0, 1 \rangle = \langle 0, 1 \rangle + \langle b, a \rangle = \langle b, a \rangle$. (*additive identity law*)

c. $\langle b, a \rangle + \langle -b, a \rangle = \langle 0, 1 \rangle = \langle -b, a \rangle + \langle b, a \rangle$. (*additive inverse law*)

d. $\langle b, a \rangle + \langle d, c \rangle = \langle d, c \rangle + \langle b, a \rangle$. (*additive commutative law*)

e. $\langle b, a \rangle \cdot (\langle d, c \rangle \cdot \langle f, e \rangle) = (\langle b, a \rangle \cdot \langle d, c \rangle) \cdot \langle f, e \rangle$. (*multiplicative associative law*)

f. $\langle b, a \rangle \cdot \langle 1, 1 \rangle = \langle 1, 1 \rangle \cdot \langle b, a \rangle = \langle b, a \rangle$. (*multiplicative identity law*)

g. If $\langle b, a \rangle \neq \langle 0, 1 \rangle$, then $\langle a, b \rangle$ is defined, and $\langle b, a \rangle \cdot \langle a, b \rangle = \langle 1, 1 \rangle$.

h. $\langle b, a \rangle \cdot \langle d, c \rangle = \langle d, c \rangle \cdot \langle b, a \rangle$. (*multiplicative commutativity law*)

i. $\langle b, a \rangle \cdot (\langle d, c \rangle + \langle f, e \rangle) = (\langle b, a \rangle \cdot \langle d, c \rangle) + (\langle b, a \rangle \cdot \langle f, e \rangle)$. (*distributive law*)

**Basic
properties
of the
rationals**

Comments:

1. The reader will easily recognize that properties (a)–(f), (h), (i) show that $\langle \mathbb{Q}, +, \cdot \rangle$ is a commutative ring. The additive identity in this ring is $\langle 0, 1 \rangle$, and the multiplicative identity is $\langle 1, 1 \rangle$. We shall refer to these as *zero* and *one*, respectively, in anticipation of their later identification with the integers 0 and 1.
2. Property (g) is a multiplicative inverse law but restricted to *non-zero* rationals. It asserts that, for a non-zero rational number $\langle b, a \rangle$, a multiplicative inverse exists and equals $\langle a, b \rangle$.

Exercise 5. Verify that a rational number $\langle b, a \rangle$ is non-zero if and only if $b \neq 0$. Conclude that in that case, $\langle a, b \rangle$ is a well-defined, non-zero rational number and that $\langle b, a \rangle \langle a, b \rangle = \langle 1, 1 \rangle$, i.e., verify property (g) of the theorem.

3. Let \mathbb{Q}^* denote the set of non-zero rational numbers.

Exercise 6. (a) Show that if $\langle b, a \rangle$ and $\langle d, c \rangle$ are non-zero, then $\langle b, a \rangle \langle d, c \rangle$ is non-zero. Therefore, \mathbb{Q}^* is closed with respect to the operation of multiplication. That is, we can consider multiplication of non-zero rationals to be a binary operation on \mathbb{Q}^* .

- (b) Verify that $\langle \mathbb{Q}^*, \cdot \rangle$ is a commutative group.
- (c) Using only the properties listed in Theorem 1, prove that \mathbb{Q} satisfies a multiplicative cancellation law: i.e., if $\langle b, a \rangle \langle d, c \rangle = \langle b, a \rangle \langle f, e \rangle$ and if $\langle b, a \rangle \neq \langle 0, 1 \rangle$, then $\langle d, c \rangle = \langle f, e \rangle$.

Therefore, the commutative ring \mathbb{Q} cannot have zero-divisors (cf. the comments after Definition 8 in the *Integers* notes for a short discussion of zero-divisors).

4. A commutative ring without zero-divisors is called an *integral domain* in the mathematical literature. Therefore, both the ring \mathbb{Z} and the ring \mathbb{Q} are integral domains.

But \mathbb{Q} is more than a mere integral domain because of the multiplicative inverse law for non-zero elements.

Definition 3. A commutative ring $\langle R, +, \cdot \rangle$ that satisfies a multiplicative inverse law for its non-zero elements is called a *field*.

**Concept
of a
field**

Therefore, the commutative ring $\langle \mathbb{Q}, +, \cdot \rangle$ is a field. Other examples of fields are the real numbers \mathbb{R} and the complex numbers \mathbb{C} , both with respect to their usual addition and multiplication operations. Another example is provided by the set $\{0, 1\}$, together with the operations of mod 2 addition and multiplication. The reader should verify this last example for himself/herself.

Using the same argument that works for Exercise 6 (c), it is easy to show that a field satisfies a multiplicative cancellation law (for multiplication by non-zero elements). So, a field is an integral domain. However, \mathbb{Z} is an example of an integral domain that is not a field.

Exercise 7. Verify properties (a)–(f), (h), (i), listed in Theorem 1.

5. We usually denote additive inverses by prefixing a $-$ sign. Property (c) above can then be phrased as: $-(\langle b, a \rangle) = \langle -b, a \rangle$. By Exercise 4, this also equals $\langle b, -a \rangle$.

6. We sometimes denote multiplicative inverses by adjoining an exponent -1 .

Property (g) above can then be phrased as $\langle b, a \rangle^{-1} = \langle a, b \rangle$. Of course, as stated in property (g), this is only asserted when $\langle b, a \rangle \neq \langle 0, 1 \rangle$.

Exercise 8. Let r and s be any rational numbers, with $s \neq 0$. Verify each of the following. a) $-(-r) = r$. b) $(s^{-1})^{-1} = s$. c) $(-s)^{-1}$ is defined and equals $-(s^{-1})$.

Because of this last equality, we may write the expression as $-s^{-1}$ —i.e., with no parentheses—without fear of ambiguity.

3.2.2 Connections with \mathbb{Z} .

At this point, we have an algebraic object, namely \mathbb{Q} , with properties that resemble those that we are familiar with from our earlier experience with rational numbers. However, we have not yet connected this construction with the integers. The facts in the following exercise allow us to do this.

Exercise 9. Let a and b be any integers. (a) Prove that $\langle a, 1 \rangle = \langle b, 1 \rangle \Leftrightarrow a = b$. (b) Prove that $\langle a + b, 1 \rangle = \langle a, 1 \rangle + \langle b, 1 \rangle$. (c) Prove that $\langle ab, 1 \rangle = \langle a, 1 \rangle \cdot \langle b, 1 \rangle$. (d) Verify that $\langle b, a \rangle = \langle b, 1 \rangle \cdot \langle 1, a \rangle = \langle b, 1 \rangle \cdot \langle a, 1 \rangle^{-1}$.

This exercise can be used to show that \mathbb{Q} contains a copy of \mathbb{Z} , with the operations of \mathbb{Q} restricting to the analogous operations of \mathbb{Z} . To make this more precise, define a function $j : \mathbb{Z} \rightarrow \mathbb{Q}$ by the rule

$$j(a) = \langle a, 1 \rangle,$$

for any $a \in \mathbb{Z}$. Assertion (a) of Exercise 9 implies that j is injective. It maps the set \mathbb{Z} injectively onto the subset of \mathbb{Q} consisting of all rationals of the form $\langle n, 1 \rangle$,

where n ranges over \mathbb{Z} . Assertions (b) and (c) of the exercise can be rephrased as:

$$j(a + b) = j(a) + j(b) \quad \text{and} \quad j(ab) = j(a) \cdot j(b).$$

\mathbb{Q}
extends
 \mathbb{Z}

That is, the function j preserves the two operations.

Therefore, we may use j to identify \mathbb{Z} with this subset of \mathbb{Q} , i.e., \mathbb{Q} is an extension of \mathbb{Z} and the operations of \mathbb{Q} extend those of \mathbb{Z} . Shortly, we'll show that the order relation in \mathbb{Z} may be extended to an order relation in \mathbb{Q} .

3.2.3 Better notation.

As in our earlier construction of the integers, we now modify and simplify our notation to reflect this identification of \mathbb{Z} with a subset of \mathbb{Q} . Specifically, we do the following:

1. We identify any integer b with the rational number $j(b) = \langle b, 1 \rangle$, writing b instead of $\langle b, 1 \rangle$. Among other things, this means that the additive identity of \mathbb{Q} is now written as 0 and the multiplicative identity of \mathbb{Q} is written as 1.

Using Exercise 9 (d), we see that an arbitrary rational number $\langle b, a \rangle$ can be written as

$$\langle b, a \rangle = b \cdot a^{-1}. \tag{6}$$

2. We now introduce the operation of *division* and the usual fraction notation.

**Division,
at last**

Definition 4. For any rational numbers r and s such that $r \neq 0$, we define s divided by r to be $s \cdot r^{-1}$, and we denote this by s/r . Clearly, then $1/r = r^{-1}$, so this gives the usual reciprocal notation for the multiplicative inverse. It follows,

using equation (6), that any rational number $\langle b, a \rangle$ can be written in the familiar fraction form b/a .

From now on, we shall use the new notation, except when it is necessary to use the old notation to prove a point.

3. The foregoing is analogous to what we did when we introduced the $-$ symbol in order to write $m + (-n)$ more efficiently as $m - n$ and then regarded this as defining the operation of subtraction of integers. Incidentally, we now apply the same considerations to extend this $-$ notation further: We let $s - r$ stand for $s + (-r)$, for any rational numbers r and s .
4. Therefore, we have arrived at the situation in which we can legitimately regard \mathbb{Q} , together with its operations of addition and multiplication, as an extension of \mathbb{Z} , with corresponding operations and corresponding notational conventions. In short, we now have our standard picture of the rationals. We conclude by restating Theorem 1 in the new (of course, well-known) notation:

Theorem 2. *Let $b/a, d/c, f/e$ be any rational numbers. Then:*

$$(i) \quad b/a + (d/c + f/e) = (b/a + d/c) + f/e. \quad (\text{additive associative law})$$

$$(ii) \quad b/a + 0 = 0 + b/a = b/a. \quad (\text{additive identity law})$$

$$(iii) \quad b/a + (-b)/a = 0 = (-b)/a + b/a. \quad (\text{additive inverse law})$$

$$(iv) \quad b/a + d/c = d/c + b/a. \quad (\text{additive commutative law})$$

$$(v) \quad b/a \cdot (d/c \cdot f/e) = (b/a \cdot d/c) \cdot f/e. \quad (\text{multiplicative associative law})$$

$$(vi) \quad b/a \cdot 1 = 1 \cdot b/a = b/a. \quad (\text{multiplicative identity law})$$

(vii) If $b/a \neq 0$, then a/b is defined, and $b/a \cdot a/b = 1$.

(viii) $b/a \cdot d/c = d/c \cdot b/a$. (multiplicative commutativity law)

(ix) $b/a \cdot (d/c + f/e) = (b/a \cdot d/c) + (b/a \cdot f/e)$. (distributive law)

3.2.4 Solving the equations $E_{a,b}$ and $M_{a,b}$.

We are now in a position to attain the main goal of this construction:

Exercise 10. Let a, b, c, d be any *rational numbers*, with $c \neq 0$. Verify that each of the following two equations has a *unique* solution in \mathbb{Q} :

$$E_{a,b} : a + x = b$$

$$M_{c,d} : cy = d.$$

**Solving
equations
in \mathbb{Q}**

Specifically, verify that $E_{a,b}$ has the unique solution $x = b - a$ and $M_{c,d}$ has the unique solution $y = d/c$. (Be sure you prove this for all $a, b, c \neq 0, d$ ranging over the rationals, not just over the integers.)

Comments:

- One benefit of this construction of \mathbb{Q} is that it can be extended well beyond this context. In general, we can start with any integral domain R and construct an extension of R that essentially consists of all “fractions” of elements in R (allowing only non-zero denominators, of course). These fractions form the so-called *field of fractions* of R . Readers of these notes have encountered this process in calculus courses when they start with polynomials (which form an integral domain) and then consider rational functions (which are fractions with

a polynomial in the numerator and a non-zero polynomial in the denominator). These rational functions form a field which is the field of fractions corresponding to the ring of polynomials.

- Exercise 10 shows that if we are interested in first-order equations involving one unknown and rational coefficients, we do not have to look beyond the rationals for solutions. This is also true when there are more unknowns. Such first-order equations are often called *linear equations*. Hence, all the results and techniques of linear algebra (except those involving eigenvalues) are valid using any scalar field, in particular, the field of rationals.

The story changes, however, when we want to solve higher order equations, as we'll shortly discuss. First, however, we want to show how to introduce the standard order relation into \mathbb{Q} .

3.3 Ordering the rational numbers

To define an order relation on \mathbb{Q} extending that of \mathbb{Z} and having the standard properties, we begin by defining \mathbb{Q}^+ , the set of *positive* rationals, and \mathbb{Q}^- , the set of *negative* rationals.

Definition 5. Let a and b be any integers, with $a \neq 0$. We say that the rational number b/a is *positive* $\iff ab > 0$. Let \mathbb{Q}^+ denote the set of all positive rationals. We say that b/a is *negative* $\iff ab < 0$, and we denote the set of negative rationals by \mathbb{Q}^- .

**Positive
and
negative
rationals**

Exercise 11. Verify that if the rational number r is neither positive nor negative, then $r = 0$.

Note that we have not yet defined an order relation on \mathbb{Q} . We have only proposed a definition of certain subsets \mathbb{Q}^+ and \mathbb{Q}^- of \mathbb{Q} .

Exercise 12. Prove the following:

- a. The sets \mathbb{Q}^+ and \mathbb{Q}^- are well-defined. (This means that you have to show that the definitions of positive and negative rational numbers are well-posed.)
- b. Prove that $b/a \in \mathbb{Q}^+ \iff -(b/a) \in \mathbb{Q}^-$.
- c. Prove that \mathbb{Q}^+ is closed with respect to addition, multiplication, and the operation of multiplicative inversion.
- d. Prove that \mathbb{Q}^- is closed with respect to addition and multiplicative inversion.
- e. Prove that the product of two negative rationals is positive and the product of a negative rational and a positive rational is negative.

This exercise shows that the concepts of positive and negative as defined above are compatible with the standard meaning of these terms.

Definition 6. We define a relation \prec on \mathbb{Q} as follows: Given any two rational numbers r and s , we say that r is less than s , written $r \prec s$ provided that $s - r$ is positive. In this case, we may also say that s is strictly greater than r and write $s \succ r$.

Ordering
 \mathbb{Q}

The definition is designed to be compatible with our normal use of the words “positive” and “negative.” Thus, the assertions “ r is positive” and “ $r \succ 0$ ” are equivalent, according to our definitions, as are “ r is negative and “ $r \prec 0$.” We use these interchangeably from now on.

Exercise 13. Prove that if m and n are integers, then $m < n \iff m \prec n$. (Note: $<$ is the order relation on \mathbb{Z} defined in the previous section. Since, now, we are regarding \mathbb{Z} as a subset of \mathbb{Q} , it makes sense to apply the relation \prec to integers. This exercise asserts that, for integers, the two relations are the same.)

Since this exercise tells us that the new order relation \prec on \mathbb{Q} is an extension of the standard order on the integers, it is no longer necessary to use a separate symbol for it. So, we dispense with the symbol \prec , and, from now on, we use the symbol $<$ for the defined ordering of the rationals.

The following theorem summarizes the main features of the ordering.

Theorem 3. *Let r, s , and t be any rational numbers. Then, we have the following:*

- a. *Exactly one of the following holds: $r < s$, $r = s$, or $r > s$.*
- b. $r < s \iff -s < -r$.
- c. $r < s \wedge s < t \implies r < t$. *(transitivity of $<$).*
- d. $\neg(r < r)$. *(irreflexivity of $<$)*
- e. $r < s \iff r + t < s + t$.
- f. *If $r > 0$ and $s < t$, then $rs < rt$.*
- g. *If $r < 0$ and $s < t$, then $rs > rt$.*
- h. *If $r, s \in \mathbb{Q}^+$ and $r < s$, we have $s^{-1} < r^{-1}$. The same holds when $r, s \in \mathbb{Q}^-$.*
- i. *There exist non-empty subsets of \mathbb{Q} that are bounded below but contain no smallest element.*

We shall prove properties (c), (e), and (f) to illustrate how these proofs go.

Proof. (c) The hypothesis states that $r < s$ and $s < t$, so the rational numbers $s - r$ and $t - s$ are positive. Since \mathbb{Q}^+ is closed under addition, the sum $(t - s) + (s - r)$ is positive. Since this quantity equals $t - r$, it follows that $r < t$.

(e) Since $s - r = (s + t) - (r + t)$, one side of the equation is positive if and only if the other is. By definition, this means that $r < s$ if and only if $r + t < s + t$.

(f) The hypothesis tells us that both r and $t - s$ are positive. Since \mathbb{Q}^+ is closed under multiplication, it follows that $r(t - s)$ is positive. But, the distributive law implies that this quantity equals $rt - rs$, hence $rs < rt$, as desired.

□

Exercise 14. Prove the remaining properties listed in Theorem 3.

- Properties (a), (c), and (d) together imply that $<$ is a strict linear order on \mathbb{Q} .
- Properties (b)—(h) are closely analogous to properties already stated for the order relation on \mathbb{Z} .
- However, property (i) is different from what we have encountered earlier. It is worth giving an explicit example to illustrate this. Choose any rational number s and hold it fixed. Define the set S to consist of all rational numbers $r > s$. Clearly S is bounded below by s . Moreover, $s + 1 \in S$, so S is not empty. However, for any $r \in S$, there is a strictly smaller element in S , for example $(r + s)/2$. So, S has no smallest element. A closely similar construction shows that there are non-empty subsets of \mathbb{Q} that are bounded above but have no largest element.

Exercise 15. Verify that $r > (r + s)/2 > s$.

Exercise 16. Prove: For any positive, rational numbers r and s , $r < s \iff r^2 < s^2$.

(**Caveat:** Only use the results proved so far. In particular, you may not use the usual properties of the square-root function that you learned in calculus...this has not been defined and the properties have not been established.)

Exercise 15 illustrates what is called the *density* property of \mathbb{Q} : namely, *strictly between any two rationals, say r and s , with $r > s$, there exists another rational t : $r > t > s$* . In the exercise above, we chose t to be the average of r and s , but clearly there are many other rationals that can be constructed strictly between r and s . Notice that the natural numbers do not have this property (cf., Exercise 11 in the *Natural Numbers* notes); consequently, nor do the integers.

**Density
property
of the
rationals**

The following theorem states two more properties of the rationals that are important:

Theorem 4. *Let r and s be any positive rational numbers. Then: (a) There exists a natural number n such that $1/n < r < n$. (b) There exists a natural number m such that $s < mr$.*

Proof. We prove only part (b), leaving (a) to the reader.

Let us write $r = b/a$ and $s = d/c$, where a, b, c, d are integers. Since r is assumed to be positive, it follows easily from the definition of positivity that either both a and b are positive or both are negative (see Exercise 21 of the *Integers* notes). We can assume that they are both positive, since, if not, we just use $-a$ and $-b$, which would then be positive and have the same quotient. Similarly, we may assume that c and d are both positive. The rest is now a calculation, which follows.

Since bc is a positive natural number, we have $bc \geq 1$. Therefore, $(ad + 1)bc = ad(bc) + bc > ad(bc) \geq ad$. Now, divide both sides by ac (i.e., multiply by $1/ac$, which is positive), obtaining

$$(ad + 1)bc/ac > ad/ac.$$

It remains only to set $m = ad + 1$ and to recognize that $bc/ac = b/a$ and $ad/ac = d/c$. The inequality then becomes

$$m(b/a) > d/c,$$

as desired. (We shall discuss this proof further in class.) □

Exercise 17. Prove part (a) of the theorem. (You may use part (b), if you like, since its proof did not depend on part (a).)

To illustrate this theorem, say $r = 17/256$ and $s = 83/11$. Then, for part (a), we could choose $n = 20$, and for part (b), we could choose $m = 200$. These properties seem obvious for the integers and rationals, but the reader should be told that there are examples of linearly ordered fields that extend \mathbb{Z} for which neither property holds: so-called non-archimedean fields. These play a significant role in some parts of algebra.

3.4 Extending \mathbb{Q}

According to Exercise 10, both equations

$$a + x = b$$

$$cy = d.$$

have unique solutions in \mathbb{Q} for any rationals a, b, c, d such that $c \neq 0$. So, as already remarked, we do not need to extend \mathbb{Q} further in order to solve linear equations. However, quadratic and higher order equations are another matter. For example, as already seen earlier in the course, the equation

$$x^2 = 2 \tag{7}$$

does not have a solution in \mathbb{Q} because 2 is not a perfect square. Since quantities like $\sqrt{2}$ have geometric meaning and are useful in various formulas, we would like to include them in a number system extending \mathbb{Q} . But, how shall we do this?

In fact, there are (at least) two very different approaches to this issue. One is purely algebraic. We'll give a brief description but will then focus almost entirely on the other approach.

3.4.1 Adjoining roots of polynomials to \mathbb{Q}

We could introduce a number system that extends \mathbb{Q} and contains a solution to the above equation by proceeding purely algebraically: We consider the set \mathbb{F} of all expressions $r + s\sqrt{2}$, where r and s are rational numbers and $\sqrt{2}$ is simply a symbol. Define addition and multiplication by the rules: $(a+b\sqrt{2})+(c+d\sqrt{2}) = a+b+(c+d)\sqrt{2}$ and $(a + b\sqrt{2}) \cdot (c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}$.

Exercise 18. (a) Verify that \mathbb{F} is closed under the operations of addition and multiplication just defined. (b) Verify that, with respect to these operations, \mathbb{F} is a commutative ring. (c) Verify that every non-zero member of \mathbb{F} has a multiplicative inverse in \mathbb{F} . (Hint: Rationalize the denominator.)

The rationals \mathbb{Q} are contained in \mathbb{F} , since any rational a can be written as $a + 0\sqrt{2}$. So, the exercise shows that \mathbb{F} is a field extending \mathbb{Q} . Further, the order relation of \mathbb{Q} extends to \mathbb{F} . (We'll omit the details for this.) Finally, the multiplication operation in \mathbb{F} can be shown to satisfy $(\sqrt{2})^2 = 2$, so equation (7) has a solution in \mathbb{F} . (It won't be a unique solution, because $-\sqrt{2}$ also satisfies it, but there is no way of avoiding this.) So, in a nutshell, one can enlarge \mathbb{Q} to accommodate solutions to equation (7); similarly for solutions to any polynomial equation with rational coefficients. In fact, in an advanced algebra course, one shows how to do this all at once, enlarging \mathbb{Q} so that the result contains all possible roots of polynomials with rational coefficients. (If one wishes to extend the order relation as well, then there are certain restrictions one must place on the polynomials, but this is a technicality beyond the purview of this course.)

**Extending
 \mathbb{Q} via
equations**

This procedure is sufficient for most of what is needed in algebra, but it is not sufficient for other parts of mathematics, such as analysis (i.e., calculus). Indeed, the familiar numbers π and e cannot be constructed by this method: they are not roots of any polynomial with rational coefficients. This fact is hard to prove for each of these numbers. Indeed, it was not until 1873 that e was shown to have this property and not until 1882 that it was also demonstrated for π .

3.4.2 Holes in \mathbb{Q}

Even leaving aside the question of whether certain particularly interesting quantities can be constructed by the algebraic method mentioned above, there is another reason to look for a different way to enlarge \mathbb{Q} : namely, for the purposes of doing calculus, we must consider, in one form or another, limits of sequences. For this to work smoothly,

we need our number system to have the property that a sequence of numbers in the system that get “closer and closer together” will converge to a limiting value in the system. That is, after all, the intuitive idea of what a convergent sequence should look like. We don’t want such sequences to look as though they are converging to a limit but not have the limit exist in our system. This would represent a kind of “hole” in the system that would contradict our intuition about the continuity of space and time, which are ultimately what these basic number systems are supposed to represent. But, in fact, such holes in \mathbb{Q} , do exist, as we shall shortly demonstrate. We’ll construct a sequence of rational numbers that looks as though it’s going to converge—that is, its terms get closer and closer together—but the hypothetical limiting value would have to have square equal to two. Since, as we have just mentioned, no rational number has this property, the hypothetical limit cannot be rational, i.e., it’s a hole in \mathbb{Q} .

\mathbb{Q}
has
“holes”

In the result that follows and the subsequent discussion, we use the properties of the rational numbers developed so far in these notes and in class, but, for illustrative purposes, we also mention some of the concepts from calculus, such as sequences, limits and the like. This discussion should not be regarded as part of the constructive process we have been following, but rather it is intended as motivation for the development that follows in later sections.

Notation: We shall find it helpful to make use of the usual absolute-value notation. That is, given any rational number r , we remind the reader that $|r|$ is defined as follows:

$$|r| = \begin{cases} r & \text{if } r \geq 0, \\ -r & \text{if } r < 0. \end{cases} \quad (8)$$

We assume some familiarity with this notation.

Theorem 5. *There exists an infinite sequence of rational numbers a_0, a_1, a_2, \dots such that, for all natural numbers n and k ,*

**Example
of a
hole
in \mathbb{Q}**

$$|a_n - a_{n+k}| < \frac{1}{2^n}, \text{ and}$$

$$|a_n^2 - 2| < \frac{3}{2^n}. \quad (9)$$

The first inequality in the theorem shows that the terms of the sequence $\{a_n\}$ get closer and closer together as n gets larger and larger (and so, the sequence “should” converge). But inequality (9) implies that any hypothetical limit L of this sequence must satisfy $L^2 = 2$, so that L cannot be rational. Thus, we might say that the sequence $\{a_n\}$ converges to a “hole” in \mathbb{Q} .

Let us describe how a_n is constructed.

Construction: We shall give an inductive definition of the rational numbers a_n . The proof that this is a valid inductive definition, in the sense of Section 1.4 of the *Natural Numbers* notes, is given in the subsection below. The definition goes as follows: First, set $a_0 = 1$ and $a_1 = 3/2$. Notice that $a_0^2 = 1 < 2$, whereas $a_1^2 = 9/4 > 2$. Now, suppose that we have defined the positive rational numbers a_0, a_1, \dots, a_n , for $n \geq 1$. Since each of these is a rational number, none has square equal to 2, i.e., the square is either < 2 or > 2 . We use these to define sets \mathcal{L}_n (the “lower” set) and \mathcal{U}_n (the “upper” set) as follows, for each $n \geq 1$:

$$\mathcal{L}_n = \{a_i : 0 \leq i \leq n \text{ and } a_i^2 < 2\}, \text{ and}$$

$$\mathcal{U}_n = \{a_i : 0 \leq i \leq n \text{ and } a_i^2 > 2\}.$$

Notice that $a_0 \in \mathcal{L}_n$, whereas $a_1 \in \mathcal{U}_n$, so each set is non-empty and, of course, finite. So, each of the sets has a maximum and a minimum. Notice also that \mathcal{L}_i and \mathcal{U}_i “grow” as i increases: that is,

$$\mathcal{L}_1 \subseteq \mathcal{L}_2 \subseteq \mathcal{L}_3 \subseteq \dots \subseteq \mathcal{L}_n.$$

$$\mathcal{U}_1 \subseteq \mathcal{U}_2 \subseteq \mathcal{U}_3 \subseteq \dots \subseteq \mathcal{U}_n.$$

Now, let ℓ_n be the *maximal* member of \mathcal{L}_n , and let u_n be the *minimal* element of \mathcal{U}_n . Because the sets \mathcal{L}_i and \mathcal{U}_i grow as i gets larger, the maximal elements ℓ_i of \mathcal{L}_i get larger as i gets larger, and the minimal elements u_i of \mathcal{U}_i get smaller as i gets larger. Furthermore, Since $\ell_n^2 < 2 < u_n^2$, it follows that $\ell_n < u_n$ (cf., Exercise 16). Therefore, these numbers are ordered as follows:

$$1 = \ell_1 \leq \ell_2 \leq \dots \leq \ell_n < u_n \leq \dots \leq u_2 \leq u_1 = 3/2.$$

We now define a_{n+1} to be the average of the two closest quantities: that is,

$$a_{n+1} = \frac{\ell_n + u_n}{2}.$$

Clearly, a_{n+1} is a positive, rational number, and

$$\ell_n < a_{n+1} < u_n.$$

This concludes the construction. The next exercise spells out further properties of the construction, which, taken together, give a proof of Theorem 5.

Exercise 19. a. Prove that, for any $n \geq 1$, either $a_n = \ell_n$ or $a_n = u_n$. For $n \geq 2$, show further that in the former case, $u_n = u_{n-1}$, whereas in the latter case, $\ell_n = \ell_{n-1}$. (Hint: Calculate a few terms a_n of the sequence—say about four—according to the inductive rule given. Then calculate the corresponding sets \mathcal{L}_n and \mathcal{U}_n , and the numbers ℓ_n and u_n . Try to detect the general pattern in what is happening.)

b. Prove that, for any $n \geq 2$, $u_n - \ell_n = (u_{n-1} - \ell_{n-1})/2$. Conclude that $u_n - \ell_n = 1/2^n$.

c. (i) Assume that both n and k are natural numbers with $n \geq 1$. Show that

$$\ell_n \leq a_{n+k} \leq u_n.$$

(ii) Assume that both n and k are any natural numbers. Show that

$$|a_n - a_{n+k}| < 1/2^n.$$

(Treat the case $n = 0$ separately. Use part (i) to treat the case $n \geq 1$.)

d. Use the identity $x^2 - y^2 = (x - y)(x + y)$ to conclude that $u_n^2 - \ell_n^2 < 3/2^n$. Then conclude that $|a_n^2 - 2| < 3/2^n$. (Hint: For the first part, first prove that $u_n + \ell_n < 3$. For the second part, verify that both a_n^2 and 2 are sandwiched between u_n^2 and ℓ_n^2 .)

An alternative way of looking at this construction is useful. We can think of it as starting with the closed interval $[1, 3/2]$ and dividing that in half (i.e., choosing the mid-point, or average, of the two endpoints). Then we test the mid-point. If its

square is less than 2, choose the second half-interval, $[5/4, 3/2]$. If its square is greater than 2, choose the first half-interval $[1, 5/4]$. Then, repeat the process, starting with the new sub-half-interval. And continue inductively. The sequence of mid-points of these intervals is what was constructed above.

Notice that in order to obtain a sequence of mid-points that gets “closer and closer together,” it is not necessary to use the particular test that we did. We can use any other test, or no test at all (i.e., just choose the sub-half-intervals randomly in succession). The sequence of mid-points will always have this shrinking-together property. The particular sequence we construct for the theorem above is designed so that if it converged to a limit in some hypothetical extension of \mathbb{Q} , that limit must be a square root of 2. However, the sequences just described, with random selection of sub-half-intervals, could converge in an extended system to rational numbers or irrational numbers, to roots of polynomials (with rational coefficients) or to numbers that may not be roots of polynomials. There’s no way of knowing in general. What we would like is a field that extends \mathbb{Q} and in which *any* such sequence does converge to a definite limit.

3.4.3 Optional: Defining some sequences of rationals by induction

Some students may have noticed that our construction above of the sequence of rational numbers a_n claims to proceed via an inductive definition, but it is not obvious how the inductive definition follows from Theorem 1 of Section 1.4 in the *Natural Numbers* notes—the section on inductive definition.

The following discussion will show how the given construction, as well as any of the other constructions mentioned above, does indeed follow from said Theorem 1. We did

not include this discussion in the construction in order to focus on the end-product, which is the sequence itself.

First, we make precise what we mean by a “test” of a rational number: it is simply a function $t : \mathbb{Q} \rightarrow \{0, 1\}$. If $t(r) = 0$, we say r gets a 0 score on the test; otherwise, r gets a 1 score. For example, the test t could be random. Or the test could assign r a score 0 if $r^2 < 2$ and a score of 1 if $r^2 > 2$. Or t can be any other test you can think of.

Next, corresponding to any selected test function t , we define a function $h : \mathbb{Q}^2 \rightarrow \mathbb{Q}^2$ as follows:

$$h(r, s) = \begin{cases} ((r + s)/2, s), & \text{if } t((r+s)/2)=0, \\ (r, (r + s)/2), & \text{if } t((r+s)/2)=1. \end{cases}$$

Then, we choose any pair of “initial” rational numbers, and call them ℓ_1 and u_1 . (Note that we do not care here whether or not $\ell_1 < u_1$, although that inequality did hold in our construction.)

By Theorem 1 of the *Natural Numbers* notes, there is a function $f : \mathbb{N} \rightarrow \mathbb{Q}^2$ such that $f(0) = (\ell_1, u_1)$, and $f(n + 1) = h(f(n))$. Let us write the ordered pair $f(n)$ as (ℓ_{n+1}, u_{n+1}) .

Finally, define

$$\begin{aligned} a_0 &= \ell_1, \\ a_1 &= u_1, \\ a_{n+1} &= (\ell_n + u_n)/2, \text{ for } n \geq 1. \end{aligned}$$

All this is almost exactly what we did in the construction described earlier. The only differences here are that (i) we are choosing arbitrary initial values for the sequence, (ii) we are allowing the test t to be completely general, and (iii) we are showing explicitly how the earlier Theorem 1 on inductive definition fits into the picture.

The following exercise repeats the basic idea of the arguments already given in the construction, but some details are different because the test t may be different from the test used in the construction and because in this more general setting each ℓ_n could be $\geq u_n$

Exercise 20. Prove the following: a) For every integer $n \geq 1$, $|\ell_{n+1} - u_{n+1}| = |\ell_n - u_n|/2$. b) For every integer $n \geq 1$, $|\ell_n - u_n| = |a_0 - a_1|/2^{n-1}$. c) For every integer $n \geq 1$, $a_n = \ell_n$ or $a_n = u_n$. d) For any integer $n \geq 1$, let $m_n = \min(\ell_n, u_n)$, and let $M_n = \max(\ell_n, u_n)$. Clearly, $M_n - m_n = |\ell_n - u_n|$. Prove by induction on k that, for every natural number k , $m_n \leq \ell_{n+k} \leq M_n$ and $m_n \leq u_{n+k} \leq M_n$. e) Conclude from c) and d) that, for all natural numbers k , $m_n \leq a_{n+k} \leq M_n$ and, thus, that $|a_n - a_{n+k}| \leq |\ell_n - u_n| = |a_0 - a_1|/2^{n-1}$.

Since $|a_0 - a_1|$ does not depend on n or k , this last inequality shows that we can make the expressions $|a_n - a_{n+k}|$ as small as we want by choosing n sufficiently large (with k free to range over all natural numbers).

Some of these sequences $\{a_n\}$ will converge to rational numbers. In general, however, we'll see that "most" of them will not. When our construction of the reals is complete, it will be fairly easy to see that every real number can be obtained as the limit of some sequence of rationals of the type described in this exercise.

One final comment: Although the initial values, a_0 and a_1 , as well as the test t , are perfectly general in the foregoing construction, one aspect of the construction is

very special: namely, we proceed by taking *averages*. This is not a feature of our construction that is forced upon us, it is just a computationally convenient way of producing examples. However, for the general theory and constructions which follow in the next section, it will be much easier to consider more general sequences.