The Rational Numbers

Fields

The system $\mathbb{Z}$ of integers that we formally defined is an improvement algebraically on ω (we can subtract in $\mathbb{Z}$). But $\mathbb{Z}$ still has some serious deficiencies: for example, a simple equation like $3x+4=2$ has no solution in $\mathbb{Z}$. We want to build a larger number system, the rational numbers, to improve the situation.

In Chapter 3, we introduced the idea of an algebraic structure called a field and we proved, for example, that $\mathbb{Z}_p$ is a field iff p is a prime number.

The fields axioms, as we stated them in Chapter 3, are repeated here for convenience.

Definition Suppose F is a set with two operations (called addition and multiplication) defined inside F. F is called a field if the following "field axioms" are true.

1) There are elements $0 \in F$ and $1 \in F$ (and $0 \neq 1$)

2) $\forall x \forall y \forall z \ (x+y)+z = x+(y+z)$ 2$'$) $\forall x \forall y \ \forall z \ (x \cdot y) \cdot z = x \cdot (y \cdot z)$
(addition and multiplication are associative)

3) $\forall x \forall y \ x+y=y+x$ 3$'$) $\forall x \forall y \ x \cdot y = y \cdot x$
(addition and multiplication are commutative)

4) $\forall x \forall y \forall z \ x \cdot (y+z) = x \cdot y + x \cdot z$
(the distributive law connects addition and multiplication)

5) $\forall x \ x+0=x$ 5$'$) $\forall x \ (x \neq 0 \Rightarrow \ x \cdot 1 = x)$
(0 and 1 are "neutral" elements for addition and multiplication. 0 is called the additive identity element and 1 is called the multiplicative identity element in F)

6) $\forall x \exists y \ x+y=0$
(y is called an additive inverse of x)

6$'$) $\forall x \ (x \neq 0 \Rightarrow \ (\exists y) \ x \cdot y = 1)$
(for each $x \neq 0$, such a y is called a multiplicative inverse of x)

In any field F, multiplication "$x \cdot y$" is often written as just "xy".

The (still informal) systems $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are other examples of fields. So is the collection $\{a+b\sqrt{2} \ : \ a, b \in \mathbb{Q}\}$, as you proved in a homework assignment.

Much of the material about fields in the next few pages is material you've seen before. It's just collected in a systematic way here, partly for review.

Any particular field such as $\mathbb{Z}_p$, $\mathbb{Q}$ and $\mathbb{R}$ is called a model for the field axioms. There are significant differences between these models. For example,

- $\mathbb{Z}_3$ has only 3 elements, while $\mathbb{Z}_5$ has 5 elements and $\mathbb{Q}$ and $\mathbb{R}$ are infinite fields.
- In $\mathbb{Z}_3$, $1+1+1=0$; in $\mathbb{Z}_5$, $1+1+1+1+1=0$; in $\mathbb{Q}$ and $\mathbb{R}$, no finite sum of 1's has 0 for a sum. .

In other words, we cannot say that "all fields look alike." In that respect, the field axioms are quite different from the axioms P1-P5) for a Peano system: there, we were able to argue that "all Peano systems look alike" – or, in more formal language, that any two Peano systems are isomorphic.

> *An axiom system for which "all models are isomorphic" is called a categorical axiom system. The field axioms are not categorical.*

Some useful theorems can be proved just using the field axioms: these theorems therefore apply in all fields. Proving them in the abstract is efficient; it saves the effort of proving them over and over each time a new field comes up. For example, the statements in the following theorem are true in every field – $\mathbb{Z}_p$ (p a prime), $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, ...

Theorem 1 Suppose x, u, v are a members of a field F.

a) (Cancellation for addition) If $x+u=x+v$, then $u=v$.
b) (Cancellation for multiplication) If $x \neq 0$ and $xu=xv$, then $u=v$.
c) The additive inverse of x is unique.
d) If $x \neq 0$, then the multiplicative inverse of x is unique.
e) The additive identity, 0, is unique and the multiplicative identity, 1, are unique.
f) $\forall x \in F,\ x \cdot 0 = 0$
g) If $uv=0$, then $u=0$ or $v=0$.

Proof

a) Suppose $x+u=x+v$. By Axiom 5), x has an additive inverse y. Then

$y+(x+u)=y+(x+v)$
$(y+x)+u=(y+x)+v$ (using Axiom 2)
$(x+y)+u=(x+y)+v$ (using Axiom 3)
$0+u=0+v$ (since y is an additive inverse for x)
$u+0=v+0$ (using Axiom 3)
$u=v.$ (using Axiom 5)

b) If $x \neq 0$, then x has a multiplicative inverse y (Axiom $6'$). So if $xu = xv$, then

$$\begin{aligned}
&y(xu) = y(xv) && \\
&(yx)u = (yx)v && \text{(using Axiom } 2'\text{)} \\
&(xy)u = (xy)v && \text{(using Axiom } 3'\text{)} \\
&1 \cdot u = 1 \cdot v && \text{(since } y \text{ is a multiplicative inverse for } x\text{)} \\
&u \cdot 1 = v \cdot 1 && \text{(using Axiom } 3'\text{)} \\
&u = v && \text{(using Axiom } 5'\text{)}
\end{aligned}$$

c) Suppose $y,\ y' \in F$. If $x + y = 0$ and $x + y' = 0$ both are true, then $x + y = x + y'$. Adding y to both sides, we get

$$\begin{aligned}
&y + (x + y) = y + (x + y') && \\
&(y + x) + y = (y + x) + y' && \text{(using Axiom 2)} \\
&(x + y) + y = (x + y) + y' && \text{(using Axiom 3)} \\
&0 + y = 0 + y' && \text{(because } y \text{ is an additive inverse for } x\text{)} \\
&y + 0 = y' + 0 && \text{(using Axiom 3)} \\
&y = y' && \text{(using Axiom 5).}
\end{aligned}$$

Since x has a unique additive inverse, we can talk about the additive inverse of x and give it a name: $(-x)$. Then $x + (-x) = 0$ and (using Axiom 3) $(-x) + x = 0$.

The last equation says that x is the additive inverse for $-x$: that is $-(-x) = x$. This is not some profound fact; it's just a consequence of the notation we chose for the additive inverse.

d) Suppose $x \neq 0$, that $y, y' \in F$. If $xy = 1$ and $xy' = 1$ both are true, then $xy = xy'$. Multiplying both sides by y, we get

$$\begin{aligned}
&y(xy) = y(xy') && \\
&(yx)y = (yx)y' && \text{(using Axiom } 2'\text{)} \\
&(xy)y = (xy)y' && \text{(using Axiom 23)} \\
&1 \cdot y = 1 \cdot y' && \text{(since } y \text{ is a multiplicative inverse for } x\text{)} \\
&y \cdot 1 = y' \cdot 1 && \text{(using Axiom } 3'\text{)} \\
&y = y' && \text{(using Axiom } 5'\text{)}
\end{aligned}$$

If $x \neq 0$, then x has a unique multiplicative inverse, so we can talk about the multiplicative inverse of x and give it a name: x^{-1}. Then $x \cdot x^{-1} = 1$ and (using Axiom $3'$) $x^{-1} \cdot x = 1$.

The latter equation says that x is the multiplicative inverse for x^{-1} : that is $(x^{-1})^{-1} = x$.

e) Suppose $z \in F$ and that z is an additive identity, that is, $\forall x$ $x + z = x = x + 0$. Using part a) to cancel the x's, we get $z = 0$.

.

Suppose $w \in F$ and that w is a multiplicative identity, that is, $\forall x \neq 0,\ \ xw = x = x \cdot 1$. Using part b) to cancel the x's, we get $w = 1$.

f) Suppose $x \in F$. 0 is the additive identity in F, so $0 + 0 = 0$. Therefore

$$\begin{aligned} x \cdot (0+0) &= x \cdot 0 \\ x \cdot 0 + x \cdot 0 &= x \cdot 0 \qquad\qquad \text{(using Axiom 4)} \end{aligned}$$

Let y be the additive inverse of $x \cdot 0$, that is $y = \,-\,(0 \cdot x)$

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

Part g) is left as an exercise. ●

In a field, we can also define subtraction and division.

Definition Suppose x and y are members of a field F.

a) We define the difference $x - y = x + (\,-\,y)$.
So subtraction is defined in terms of addition (adding the additive inverse).

b) If $x \neq 0$, we define the quotient $y \div x = yx^{-1}$.
So division is defined in terms of multiplication (multiplying by the multiplicative inverse).

Example Consider the field $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ (*where* $1, 2, ..., 6$ *are abbreviations for the equivalence classes* [1], [2], ..., [6])

a) The additive inverse of 4 is 3 because $4 + 3 = 0$ (and only 3 has this property). Therefore we write $-\,4 = 3$.

b) Subtraction: $2 - 4 = 2 + (\,-\,4) = 2 + 3 = 5$.

c) The multiplicative inverse of 3 is 5 because $3 \cdot 5 = 1$ (and only 5 has this property). Therefore we write $3^{-1} = 5$ (and $5^{-1} = 3$).

d) Division: $2 \div 3 = 2 \cdot 3^{-1} = 2 \cdot 5 = 3.$
$1 \div 3 = 1 \cdot 3^{-1} = 1 \cdot 5 = 5.$

Example If a, b, c are members of <u>any</u> field F and $a \neq 0$, then the equation $ax + b = c$ has a unique solution in F. We can simply use the "algebra of fields" contained in the axioms and theorems to solve the equation (some detailed justifications $-$ like references to the repeated use of associativity and commutativity in $\mathbb{Z}$ $-$ are omitted).

$ax + b = c$
$ax + b + (-b) = c + (-b)$ Using the additive inverse of b
$ax + 0 = c + (-b)$
$ax = c - b$
$a^{-1}(ax) = a^{-1}(c - b)$ $a \neq 0$ so a has a multiplicative inverse
$1 \cdot x = a^{-1}(c - b)$
$x = a^{-1}(c - b)$

For a more specific example, we solve the equation $3x + 4 = 2$ in $\mathbb{Z}_7$. (*See the preceding example.*)

$$
\begin{aligned}
&3x + 4 = 2 \\
&3x + 4 - 4 = 2 - 4 \\
&3x + 4 + 3 = 2 + 3 \\
&3x = 5 \\
&5 \cdot 3x = 5 \cdot 5 \\
&1 \cdot x = 4 \\
&x = 4.
\end{aligned}
$$

Constructing $\mathbb{Q}$

The preceding example shows that if we can enlarge the numbers system $\mathbb{Z}$ to a field, there will no longer be an issue about solving linear equations like $3x+4=2$. We will try to enlarge $\mathbb{Z}$ in the most economical way we can. (Of course, what we are after is to formally construct a field that acts just like the informal, familiar field of rational numbers.)

In the work that follows, we can use all the properties of the integers that we have already proven $-$ for example, that addition and multiplication are commutative and associative, the distributive law, that every integer has a unique additive inverse, that there are cancellation rules for addition and multiplication (by a nonzero integer) in $\mathbb{Z}$, etc. We will often use these facts about integer arithmetic without actually citing the "chapter and verse" reasons.

Think of a rational number $\frac{a}{b}$ $(b \neq 0)$. To name a rational number we need two integers a, b where $b \neq 0$. So, starting with $\mathbb{Z}$, we could try to create $\mathbb{Q}$ by defining a rational number to be a pair of integers (a,b) in which $b \neq 0$.

However, that attempt would give us "too many" different rationals. After all, we think of $\frac{1}{2}, \frac{2}{4}, \frac{-3}{-6}$ as being the same rational number. In the informal system of rationals, $\frac{a}{b} = \frac{c}{d}$ iff $ad = bc$. So $-$ if rational numbers are to be represented using pairs of integers, we would want the pairs (a,b) and (c,d) to represent the same rational number iff $ad = bc$. We can accomplish this by using an equivalence relation.

Definition For (a,b) and $(c,d) \in \mathbb{Z} \times (\mathbb{Z} - \{0\})$, let

$$(a,b) \simeq (c,d) \quad \text{iff} \quad ad = bc$$

Theorem 2 $\simeq$ is an equivalence relation on $\mathbb{Z} \times (\mathbb{Z} - \{0\})$.

Proof i) $(a,b) \simeq (a,b)$ because $ab = ba$ in (the formal system) $\mathbb{Z}$. Therefore $\simeq$ is reflexive.

ii) If $(a,b) \simeq (c,d)$, then $ad = bc$, so $cb = da$ in $\mathbb{Z}$. But that means $(c,d) \simeq (a,b)$, so $\simeq$ is symmetric.

iii) Suppose $\begin{cases} (a,b) \simeq (c,d) \\ (c,d) \simeq (e,f) \end{cases}$ so that $\begin{cases} ad = bc & (1) \\ cf = de & (2) \end{cases}$

We want to show that $(a,b) \simeq (e,f)$.

Since $(c, d) \in \mathbb{Z} \times (\mathbb{Z} - \{0\})$, we know $d \neq 0$

Case i) If $c = 0$, then $ad = bc = b(0) = 0 = (0)d$, and canceling the nonzero d gives $a = 0$.

Similarly, $de = cf = (0)f = 0 = d(0)$, and canceling the nonzero d gives $e = 0$.

Then $(a, b) = (0, b) \simeq (0, f) = (e, f)$.

Case ii) If $c \neq 0$, then multiplying equations (1), (2) and using commutativity and associativity gives $(af)(cd) = (be)(cd)$.
Since $cd \neq 0$ (a theorem we proved in $\mathbb{Z}$), we can cancel (cd) from both sides leaving $af = be$. Therefore $(a, b) \simeq (e, f)$.

Therefore $\simeq$ is transitive. ●

Definition $\mathbb{Q} = \mathbb{Z} \times (\mathbb{Z} - \{0\}) / \simeq$. A member of $\mathbb{Q}$ is called a rational number.

According to the definition, a rational number is an equivalence class containing certain pairs of integers. What do some of the equivalence classes look like?

$$... = [(- 2 - 2)] = [(- 1, - 1)] = [(1,1)] = [(2,2)] = ...$$

Going back to the intuitive motivation, we think of this equivalence class as the rational number 1.

Similarly, in the intuitive motivation, we think of the equivalence class

$$... = [(- 2,4)] = [(- 1,2)] = [(- 1,2)] = [(- 2,4)] = ... = [(- 17,34)] = ...$$
$$... = [(2, - 4)] = [(1, - 2)] = [(1, - 2)] = [(2, - 4)] = ... = [(17, - 34)] = ...$$

as the rational number $-\frac{1}{2}$.

Arithmetic in $\mathbb{Q}$

We want to define addition and multiplication in $\mathbb{Q}$: that is, we want to define addition and multiplication of these equivalence classes. The definitions make use of representatives of the equivalence classes – so, as always, we will have to check that the addition and multiplication are well-defined.

Definition Suppose $[(a,b)]$ and $[(c,d)]$ are in $\mathbb{Q}$. Let

i) $[(a,b)]+[(c,d)]=[(ad+bc,bd)]$
Of course, the definition of addition is motivated by the way, informally, that we think addition in the rationals should behave: $\frac{a}{b}+\frac{c}{d}=\frac{(ad+bc)}{bd}$

ii) $[(a,b)]\cdot[(c,d)]=[(ac,bd)]$
Again, the definition is motivated by the fact that in the informal system of rationals, $\frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd}$.

Notice that since $[(a,b)]$ and $[(c,d)]\in\mathbb{Q}$, we know that neither b nor d is 0, and therefore $bd\neq 0$. Therefore $[(ad+bc,bd)]$ and $[(ad+bc,bd)]$ are also in $\mathbb{Q}$. Adding or multiplying two rational numbers gives another rational number.

Since $[(1,-2)]=[(-2,4)]$ and $[(2,3)]=[(-4,-6)]$, applying the definitions to

$[(1,-2)]+[(2,3)]$ and $[(1,-2)]\cdot[(2,3)]$ should produce the same answers as applying them to
$[(-2,4)]+[(-4,-6)]$ and $[(-2,4)]\cdot[(-4,-6)]$

The next theorem guarantees that this is true.

Theorem 3 Addition and multiplication in $\mathbb{Q}$ are well-defined.

Proof Suppose $\begin{cases}(a,b)\simeq(c,d) \text{ and}\\ (e,f)\simeq(g,h)\end{cases}$ that is, suppose $\begin{cases}ad=bc & (1)\ \text{and}\\ eh=fg & (2)\end{cases}$

1) Addition We need to show that

$[(a,b)]+[(e,f)]=[(c,d)]+[(g,h)]$. This is true iff
$(af+be,bf)\simeq(ch+dg,dh)$ iff
$dh(af+be)=bf(ch+dg)$ iff
$adhf+bdeh=bcfh+bdfg$ (*)

But $ad=bc$ and $eh=fg$, so the equation (*) just says

$bchf+bdfg=bcfh+bdfg$, which is true.

2) <u>Multiplication</u> We need to show that

$[(a,b)]\cdot[(e,f)] = [(c,d)]\cdot[(g,h)]$ This is true iff
$[(ae,bf)] = [(cg,dh)]$ iff
$aedh = bfcg$ (**)

But equation (**) is true: it is just the result of multiplying together the equations (1) and (2) in the hypothesis. ●

Theorem 4 With addition and multiplication so defined, $\mathbb{Q}$ is a field.

Proof We will prove that some of the field axioms are true for $\mathbb{Q}$. The others (all just as easy) are left as exercises. Suppose $[(a,b)]$ and $[(c,d)]$ are in $\mathbb{Q}$

Axiom 3) <u>Addition is commutative</u>:

$$\begin{aligned}[(a,b)]+[(c,d)] &= [(ad+bc,bd)]\\ &= [(cb+da,db)] \quad \text{(because addition and multiplication in } \mathbb{Z} \text{ are commutative)}\\ &= [(c,d)]+[(a,b)]\end{aligned}$$

Axioms 5 and 5$'$) <u>Existence of identity elements</u>

The equivalence classes $[(0,1)]$ and $[(1,1)]$ are the identity elements for addition and multiplication in $\mathbb{Q}$. For any $[(a,b)]\in\mathbb{Q}$:

$[(a,b)]+[(0,1)] = [(a\cdot 1+b\cdot 0, b\cdot 1)] = [(a,b)]$ and

$[(a,b)]\cdot[(1,1)] = [(a\cdot 1, b\cdot 1)] = [(a,b)]$

6 and 6$'$) <u>Existence of inverses</u> For any $[(a,b)]\in\mathbb{Q}$:

$$\begin{aligned}[(a,b)]+[(-a,b)] &= [(a\cdot b+b\cdot(-a),\ b\cdot b)]\\ &= [(0,b\cdot b)] = [(0,0)]\end{aligned}$$
so $[(a,b)]$ has an additive inverse in $\mathbb{Q}$: $[(-a,b)]$.

If $[(a,b)] \neq [(0,0)]$, then $a\neq 0$ so $(b,a)\in\mathbb{Z}\times(\mathbb{Z}-\{0\})$ and $[(b,a)]\in\mathbb{Q}$. Then $[(a,b)]\cdot[(b,a)] = [(ab,ab)] = [(1,1)]$. Therefore $[(a,b)]$ has a multiplicative inverse in $\mathbb{Q}$: $[(b,a)]$.

Just for convenience, we now assign some handy (and suggestive) names to the equivalence classes.

Definition For any integers a, b (with $b \neq 0$), the rational number $[(a, b)]$ is denoted using fraction notation $\frac{a}{b}$. In addition, we will also write an equivalence class $\frac{a}{1} = [(a, 1)]$ simply as a.

Thus, a fractional notation like, say, $\frac{3}{7}$ is nothing but a convenient, handy definition of a name for an equivalence class. It is a single, one-piece symbol standing for the equivalence class $[(3, 7)]$. The definition here of the symbol "$\frac{3}{7}$" has nothing to do with division.

> *However: As in any field,* $3 \div 7$ *means* $3 \cdot 7^{-1} = [(3,1)] \cdot [(7,1)]^{-1}$ $= [(3,1)] \cdot [(1,7)] = [(3 \cdot 1, 1 \cdot 7)] = [(3,7)] = \frac{3}{7}$. *So it then turns out that the symbol "*$\frac{3}{7}$*" is the answer, in our formal system* $\mathbb{Q}$*, to the problem "*$3 \div 7 =$ *?".*
>
> *This is good; if it didn't turn out that way, then the formal system* $\mathbb{Q}$ *that we've constructed wouldn't "act just like" the informal system of rationals after all.*

Examples

$[(1,1)] = \frac{1}{1}$. The equivalence class $\frac{1}{1}$ is also just written as the rational number 1.

The "1*" 's in the pair* $(1,1)$ *are the integer* 1 *: this integer, constructed earlier, is used to construct a new object – the rational number* 1*. Strictly speaking, the rational number* 1 *is different from the integer* 1*.*

We saw a similar phenomenon earlier: when we constructed $\mathbb{Z}$*, we saw that the integer* 1 *was not the same as the whole number 1 (they are quite literally defined by different sets). There are some additional comments about this at the conclusion of these notes.*

$[(0,1)] = \frac{0}{1}$. The equivalence class $\frac{0}{1}$ is also just written as the rational number 0. Since $[(0,1)] = [(0,b)]$ for any nonzero integer b, we have $\frac{0}{b} = 0$.

Since $[(2,1)] = [(4,2)] = [(-10, -5)]$, we have $\frac{2}{1} = \frac{4}{2} = \frac{-10}{-5}$: because these fractions are all just names agreed upon names for the same equivalence class. An equivalence class like $\frac{2}{1}$ is also written more simply as the rational number 2.

$\frac{1}{2} = \{ ..., (-3, -6), (-2, -4), (-1, -2), (1,2), (2,4), (3,6), ...\}$ and
$\frac{2}{4} = \{ ..., (-3, -6), (-2, -4), (-1, -2), (1,2), (2,4), (3,6), ...\}$ and
$\frac{-3}{-6} = \{ ..., (-3, -6), (-2, -4), (-1, -2), (1,2), (2,4), (3,6), ...\}$
etc.

$\frac{1}{2}$, $\frac{2}{4}$, and $\frac{-3}{-6}$ are names for the same equivalence class: $\frac{1}{2} = \frac{2}{4} = \frac{-3}{-6}$.

Notice that, in fraction notation, $\frac{a}{b} = \frac{c}{d}$ iff $[(a,b)] = [(c,d)]$
iff $(a,b) \simeq (c,d)$ iff $ad = bc$.

Examples Here once again are the definitions of addition and multiplication in $\mathbb{Q}$ $-$ but this time restated in terms of fractions. There is nothing to prove here. We are just rewriting the definitions in a different notation. :

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

$$[(3,4)] + [(2,4)] = [(20,16)] = [(5,4)]$$

In fraction notation,

$$\frac{3}{4} + \frac{2}{4} = \frac{3 \cdot 4 + 2 \cdot 4}{16} = \frac{20}{16} = \frac{5}{4}$$

$$[(3,4)] + [(-1,5)] = [(15-4,20)] = [(11,20)]$$

In fraction notation,

$$\frac{3}{4} + \frac{-1}{5} = \frac{15-4}{20} = \frac{11}{20}$$

2) $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$

$$[(-3,4)] \cdot [(1,60)] = [(-3,240)] = [(-1,80)]$$

In fraction notation,

$$\frac{-3}{4} \cdot \frac{1}{60} = \frac{-3}{240} = \frac{-1}{80}.$$

Examples

1) $\frac{ab}{ac} = \frac{b}{c}$ because $[(ab,ac)] = [(b,c)]$ because $(ab,ac) \simeq (b,c)$
because $abc = acb$

So, in fraction notation, a common factor can be "canceled" from numerator and denominator

2) $\frac{a}{b} + \frac{c}{b} = \frac{ab+bc}{b \cdot b} = \frac{b(a+c)}{b \cdot b} = \frac{a+c}{b}$ (*canceling a common factor*)

3) We proved that an object (in any field) has a unique additive inverse. As in any field, we write the additive inverse of $\frac{a}{b}$ as $-\frac{a}{b}$, so $\frac{a}{b} + (-\frac{a}{b}) = 0$.

Since $\frac{a}{b} + (\frac{-a}{b}) = \frac{ab+(-a)b}{b^2} = \frac{b(a+(-a))}{b^2} = \frac{0}{b^2} = 0$, we see that

$\frac{-a}{b}$ is an additive inverse for $\frac{a}{b}$. But $-\frac{a}{b}$ is the one and only element in $\mathbb{Q}$ which added to $\frac{a}{b}$ produces 0. Therefore it must be that $-\frac{a}{b} = \frac{-a}{b}$ in $\mathbb{Q}$.

Moreover, $\frac{a}{-b} = \frac{-a}{b}$ (because we proved, in $\mathbb{Z}$, that $ab = (-a)(-b)$).

Therefore $-\frac{a}{b} = \frac{-a}{b} = \frac{a}{-b}$ for any $\frac{a}{b} \in \mathbb{Q}$

4) $\frac{a}{b} = \frac{-a}{-b}$ since $(a,b) \simeq (-a, -b)$.

5) Subtraction: $\frac{a}{b} - \frac{c}{d} \underset{\uparrow}{=} \frac{a}{b} + (-\frac{c}{d}) = \frac{a}{b} + \frac{-c}{d} = \frac{ad-bc}{bd}$

subtraction is defined in any field by
“add the additive inverse”

6) We proved that a nonzero object (in any field) has a unique multiplication inverse. If $0 \neq \frac{a}{b} \in \mathbb{Q}$, then the multiplicative inverse of $\frac{a}{b}$ is denoted (as in any field) by $(\frac{a}{b})^{-1}$.

Since $\frac{a}{b} \cdot \frac{b}{a} = 1$, $\frac{b}{a}$ is a multiplicative inverse for $\frac{a}{b}$ in $\mathbb{Q}$. Since $(\frac{a}{b})^{-1}$ is the one and only rational which multiplied times $\frac{a}{b}$ produces 1, it must be that $\frac{b}{a} = (\frac{a}{b})^{-1}$ in $\mathbb{Q}$.

For example: $(\frac{2}{3})^{-1} = \frac{3}{2}$, $2^{-1} = (\frac{2}{1})^{-1} = \frac{1}{2}$ and

If $b \neq 0$, $b^{-1} = (\frac{b}{1})^{-1} = \frac{1}{b}$

7) Division: If $\frac{c}{d} \neq 0$, then $\frac{a}{b} \div \frac{c}{d} = \frac{a}{b} \cdot (\frac{c}{d})^{-1} = \frac{a}{b} \cdot \frac{d}{c} = \frac{ad}{bc}$
(*the old “invert and multiply" rule”*).

Since we already observed that a rational number, in fractional form, can be thought of as a division, we can also write this computation as

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

As illustrated earlier: $3 \div 7 = \frac{3}{1} \div \frac{7}{1} = \frac{3}{1} \cdot \frac{1}{7} = \frac{3}{7}$.

$$\frac{\frac{2}{3}}{\frac{4}{7}} = \frac{2}{3} \div \frac{4}{7} = \frac{2}{3} \cdot \frac{7}{4} = \frac{14}{12} = \frac{7}{6}$$

All the familiar manipulations involving addition, subtraction, multiplication and division from the informal system of rationals can be shown to be true in the formal system $\mathbb{Q}$.

At this point, we will assume that all such rules have been proven and we will use them freely, without further comment. However, rules for manipulating inequalities in $\mathbb{Q}$ still need to be explored and justified.

Inequalities in $\mathbb{Q}$

Of course, we have an idea in the informal system of rationals what "positive" and "negative" mean, and how relations like $<$ and $\leq$ work. But in the formal system $\mathbb{Q}$ that we have defined, we need to give definitions for positive, negative, $<$, and $\leq$ show see what properties they have (hopefully, they will "act just like" our informal notions).

Definition A nonzero rational number $\frac{a}{b}$ is called positive if it is possible to write $\frac{a}{b} = \frac{c}{d}$ where c and d are both in $\mathbb{N}$.

Equivalently, we can say that $\frac{a}{b}$ is positive if it is possible to write $\frac{a}{b} = \frac{c}{d}$ where the integers c, d are both not in $\mathbb{N}$ – because, in that case, we have $\frac{a}{b} = \frac{-c}{-d}$ where $-c$, $-d$ are both in $\mathbb{N}$,

Definition A nonzero rational number $\frac{a}{b}$ is called negative if it is possible to write $\frac{a}{b} = \frac{c}{d}$ where exactly one of the two integers c, d is in $\mathbb{N}$.

The rational 0 is by definition, neither positive nor negative.

Theorem 5 For every $\frac{a}{b} \in \mathbb{Q}$, exactly one of the following statements is true:

$\frac{a}{b} = 0$
$\frac{a}{b}$ is positive
$\frac{a}{b}$ is negative

Proof If $\frac{a}{b} \neq 0$ and $\frac{a}{b}$ is not positive, then it must be that exactly one of a or b is in $\mathbb{N}$ so $\frac{a}{b}$ is negative. Therefore one of the three statements must be true.

By definition, if $\frac{a}{b} = 0$, then $\frac{a}{b}$ is neither positive nor negative. So we only need to consider whether it is possible for $\frac{a}{b}$ to be both positive and negative.

> Suppose $\frac{a}{b}$ is positive, where $a, b \in \mathbb{N}$. Suppose $\frac{a}{b} = \frac{c}{d}$. It cannot be that exactly one of c, d is in $\mathbb{N}$ because then the equation $ad = bc$ would have member of $\mathbb{N}$

on

> one side but not the other. Therefore $\frac{a}{b}$ is not also negative.
> $cf = de$ holds in $\mathbb{Z}$. This is impossible since one side of the equation is in $\mathbb{N}$ but the other isn't. ●

Example $2 = \frac{2}{1} = \frac{-2}{-1}$, $\frac{1}{2}$, and $\frac{-3}{-4}$, are all positive, and
$\frac{-1}{2} = \frac{1}{-2}$, $-\frac{3}{7} = \frac{-3}{7} = \frac{3}{-7}$, and $\frac{-2}{1} = -2$ are all negative.

Theorem 6 Suppose $x = \frac{a}{b} \in \mathbb{Q}$. Then x is positive iff $-x$ is negative.

Proof If x is positive, then we can write $x = \frac{a}{b} = \frac{c}{d}$ where both $c, d \in \mathbb{N}$. Then $-x = -\frac{c}{d} = \frac{-c}{d}$ where $d \in \mathbb{N}$ and $-c \notin \mathbb{N}$. Therefore $-x$ is negative.

The proof of the converse is left as an exercise. ●

Theorem 7 If x and y are positive rationals, then $x + y$ and xy are positive.

Proof We can write $x = \frac{a}{b}$ and $y = \frac{c}{d}$ where all of $a, b, c, d \in \mathbb{N}$. Then

$$x + y = \frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}\text{, and}$$
$$xy = \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Since $ad + bc$, bd, and $ac \in \mathbb{N}$, the sum and product are positive. ●

In the discussion that follows, the notation is cleaner if we simply refer to rationals as $x, y, z, ... \in \mathbb{Q}$. We don't need the "fractional forms" $x = \frac{a}{b}$, ...

We can use the term "positive" to define order relations $<$ and $\leq$ in $\mathbb{Q}$.

Definition For $x, y \in \mathbb{Q}$, we say

$$\begin{array}{lll} x < y & \text{iff} & y - x \text{ is positive} \\ x \leq y & \text{iff} & y - x \text{ is positive or } x = y \end{array}$$

(We also write $x < y$ and $x \leq y$ as $y > x$ and $y \geq x$.)

In particular, this means (*fortunately for our intuition*) that

$$0 > x \quad \text{iff} \quad x - 0 = x \text{ is positive}$$

$$\begin{array}{llll} \text{and} & x < 0 & \text{iff} & 0 - x \text{ is positive} \\ & & & \text{iff } -x \text{ is positive} \\ & & & \text{iff } -(-x) \text{ is negative} \\ & & & \text{iff } x \text{ is negative} \end{array}$$

Example Using $<$, we can rewrite some of our previous observations (*which ones?*) in a new way:

1) Since 0 is not positive, $0 < 0$ is false.

2) $\forall x \in \mathbb{Q}$, exactly one of the following is true:

$x < 0, \ x = 0, \ x > 0$

3) $\forall x \in \mathbb{Q} \quad x > 0$ iff $-x < 0$.

Note, just for emphasis: this statement implies that $-x > 0$ *iff* $-(-x) = x < 0$.)

4) $\forall x \forall y \in \mathbb{Q}$, if $x > 0$ and $y > 0$, then $x + y > 0$ and $xy > 0$.

Some of the most important facts about $<$ are listed in the following theorem. You can also formulate an analogous theorem for $\leq$.

Theorem 8 For all $x, y, z, w \in \mathbb{Q}$,

a) If $x < y$ and $y < z$, then $x < z$ (the relation " $<$ " is transitive)
b) If $x < y$, then $x + z < y + z$
c) If $x < y$ and $z > 0$, then $xz < yz$
d) If $x < y$ and $z < 0$, then $xz > yz$
e) If $x \neq 0$, then $x^2 > 0$
f) If $x < y$, then $-x > -y$.
g) If $xy > 0$, then both x, y are positive or both are negative
h) If $x < y$ and $z < w$, then $x + z < y + w$.

Proof We will prove a few of the statements to indicate how the arguments go.

a) Suppose $x < y$ and $y < z$.
Then $y - x$ and $z - y$ are both positive. (*Definition of* " $<$ ")
So $(y - x) + (z - y) = z - x$ is positive. (*Theorem 7*)
Therefore $x < z$. (*Definition of* " $<$ ")

d) If $x < y$, then $y - x$ is positive (*Definition of* " $<$ ")
If $z < 0$, then $0 - z = -z$ is positive (*Definition of* " $<$ ")
Therefore $-z(y - x)$ is positive (*Theorem* 7)
$z(x - y)$ is positive
$xz - xy$ is positive
$xz > yz$ (*Definition of* " $<$ ")

e) If x is positive, then $x \cdot x = x^2$ is positive,
that is, $x^2 > 0$. (*Theorem* 7)
If x is negative, then $-x$ is positive (*Theorem* 6)

so $(-x)\cdot(-x) = x^2$ is positive. $\quad$ $(\textit{Theorem } 7)$

g) The proof is by contraposition.

If x is positive and y is negative, then x and $-y$ are both positive, $\quad$ $(\textit{Theorem } 6)$
so $-xy$ is positive $\quad$ $(\textit{Theorem } 7)$
Then $-(-xy) = xy$ is negative $\quad$ $(\textit{Theorem } 6)$
so $xy \not> 0$. $\quad$ (*Definition of* "$<$")

In a similar way, you can also show that it is impossible to have x negative and y positive.

The remaining parts of the theorem are left as exercises. $\bullet$

Definition A relation R on a set X is called antisymmetric iff

$$\forall x \, \forall y \in X \ \ (xRy \wedge yRx) \Rightarrow x = y$$

"Antisymmetry" for a relation R means more than "not symmetric." It is the extreme opposite of "symmetry" in the following sense: :

"symmetric" $\quad$ $\forall x \, \forall y \in X \ \ (xRy \Rightarrow yRx)$

"not symmetric" $\quad$ $\sim (\forall x \, \forall y \in X \ \ (xRy \Rightarrow yRx))$
which is equivalent to $\quad$ $\exists x \, \exists y \in X \ \ (xRy \wedge y \not{R} x)$

"antisymmetric" $\quad$ $\forall x \, \forall y \in X \ \ (xRy \Rightarrow y \not{R} x)$

Definition A relation R on X is called a linear ordering (or total ordering) iff R is

i) reflexive, transitive, and antisymmetric, and
ii) $\forall x \, \forall y \in X \ (xRy \vee yRx)$

The pair (X, R) is then called a linearly ordered set.

It is easy to show that $\leq$ is a linear ordering on $\mathbb{Q}$. (*What about* $<$ *?*)

Theorem 9 $\leq$ is a linear ordering on $\mathbb{Q}$.

Proof Exercise.

Concluding Comments

1) We constructed the rationals from the integers, the integers from the whole numbers, and whole numbers from sets. If everything is "unpacked," each rational number is a (complicated) set. For example, what is the rational number "2" ?

The rational number $2 = [(2,1)]$

$$= \{..., (-4, -2), (-2, -1), (2,1), (4,2), ...\}$$

$$(\textit{the } 2\textit{'s in the ordered pairs are } \underline{\textit{integer}}\ 2\textit{'s})$$

Each member of this equivalence class is an ordered pair of integers, and each ordered pair (a,b) is a set $\{\{a\},\{a,b\}\}$. We will "unpack" just one of those ordered pairs, say $(2,1)$:

$(2,1) = \{\{2\},\{2,1\}\}$, where 2 and 1 here represent the integers 2 and 1.

Descending deeper (*see the similar comments in the notes "Constructing the Integers"*): the integer*s* 2 and 1 are certain equivalence classes of pairs of whole numbers:

The integer 2 is the set (equivalence class) $[(2,0)] = \{(2,0),\ (3,1),\ (4,2),\ ...\}$
The integer 1 is the set (equivalence class) $[(1,0)] = \{(1,0),\ (2,1),\ (3,2),\ ...\}$

So the ordered pair of integers

$$(2,1) = \{\{2\},\{2,1\}\} = \{\{[(2,0)]\},\{[(2,0)],[(1,0)]\}\}$$

$$= \{\{\{(2,0),\ (3,1),\ (4,2),\ ...\}\},\{\{(2,0),\ (3,1),\ (4,2),\ ...\},\{(1,0),\ (2,1),\ (3,2),\ ...\}\}\} \quad (*)$$

(*where on the preceding line, the numbers in the ordered pairs are whole numbers.*

So each one of the ordered pairs of integers in the rational number 2 is really a set like (*)

But to go further, each one of the ordered pairs in each set like (*) can be further unpacked: for example, consider the single ordered pair $(2,1)$ of whole numbers that occurs in (*). Each whole number was defined earlier as a set, so

whole number pair $(2,1) = \{\{2\},\{2,1\}\} = \{\{\{\emptyset,\{\emptyset\}\}\},\ \{\{\emptyset,\{\emptyset\}\},\{\emptyset\}\}\}$

"What is 2?" can rapidly become mind-boggling. The thing to remember in years to come is not the details of how each rational number is constructed but that

i) each rational can be built up from sets – so sets, as far as we have gone, are proving to be an adequate set of building blocks for mathematics, and

ii) beyond that, all we need to know about "2" to do mathematics is "how does 2 behave?"

2) As we constructed them, the integers are not members of $\mathbb{Q}$. However, it is not hard to see that

the system of rational numbers $\{..., -2, -1, 0, 1, 2, ...\}$

"acts just like"

the system of integers $\{..., -2, -1, 0, 1, 2, ...\}$

(*the more technical language is that the two systems are isomorphic*).

So we can think of the system of rationals $\{..., -2, -1, 0, 1, 2, ...\}$ inside $\mathbb{Q}$ as being an "exact photocopy" of the system of integers $\{..., -2, -1, 0, 1, 2, ...\}$. If we agree to ignore the difference between the photocopy and the real thing, then we can write $\mathbb{Z} \subseteq \mathbb{Q}$.

3) Of course the number system $\mathbb{Q}$ is for many purposes a big improvement over $\mathbb{Z}$. For example, it's a field and $\mathbb{Z}$ isn't, and linear equations in $\mathbb{Q}$, but not in $\mathbb{Z}$, can always be solved. But $\mathbb{Q}$ still has some major algebraic shortcomings. For example, such a simple equation as $x^2 = 2$ cannot be solved in $\mathbb{Q}$. (*Why not?*)

To deal with this difficulty requires enlarging the number system again to include new number(s) with square 2. The informal number system $\mathbb{R}$ has such numbers: $\pm\sqrt{2}$.

> *Unfortunately won't have time in this course to formally construct* $\mathbb{R}$. *It turns out, in that construction, that a real number is an ordered pair* (A, B), *where* A *and* B *are two special subsets of* $\mathbb{Q}$ *that form a "cut" in* $\mathbb{Q}$. *For example,* $\sqrt{2} = (A, B)$ *where* $A = \{q \in \mathbb{Q} : q^2 < 2\}$ *and* $B = \{q \in \mathbb{Q} : q^2 > 2\}$.

Informally, $\mathbb{R}$ is a field – just as $\mathbb{Q}$ is – but, in $\mathbb{R}$, there is a solution for $x^2 = 2$. $\mathbb{R}$ must have some additional property(s) making it a "more special" field than $\mathbb{Q}$: some property that guarantees that there are also "irrational" numbers.

The number system $\mathbb{R}$ is a very powerful system: it's all you needed to be able to do calculus. But even $\mathbb{R}$ is not completely satisfactory algebraically. Such as simple equation as $x^2 + 1 = 0$ has no solution in $\mathbb{R}$.

For a very substantial part of mathematics, one more enlargement finally does the trick: the field $\mathbb{R}$ is enlarged to the set of complex numbers $\mathbb{C}$. Each element of $\mathbb{C}$ is an ordered pair of real numbers (a, b), and addition and multiplication are defined in $\mathbb{C}$ in such a way as to make $\mathbb{C}$ into a field.

> *In high school, you probably learned to write complex number in a form like* $a + bi$ *and* $c + di$, *and you probably we told to compute*

$$\begin{aligned}(a+bi)(c+di) &= ac+bci+adi+bdi^2 \\ &= (ac-bd)\ +(bc+ad)i \ \textit{ because } i^2 =\ -1\end{aligned}$$

This is the informal motivation for the definition of multiplication in a formal construction of $\mathbb{C}$:

$$(a,b)\cdot(c,d) = (ac-bd, bc+ad)$$

In $\mathbb{C}$, it turns out (and it's <u>not</u> easy to prove) that
<u>every polynomial equation</u>

$$a_n z^n + ... + a_1 z + a_0 = 0$$

has a solution.

This result is called the <u>Fundamental Theorem of Algebra.</u>