CHAPTER 6: THE RATIONAL NUMBERS $\mathbb{Q}$

MATH 378, CSUSM. SPRING 2016.

1. Introduction

In this chapter we study the field of rational numbers $\mathbb{Q}$. We construct the set of rational numbers $\mathbb{Q}$ using equivalence classes $[(x, y)]$ of pairs of elements $x, y, \in \mathbb{Z}$, and we usually write $[x, y]$ for the class $[(x, y)]$. Informally, the coordinates x and y can be thought of as the numerator and denominators of a fraction. We define an addition and a multiplication operation. The first main result of this chapter is that this construction results in a field. We use a canonical embedding $\mathbb{Z} \to \mathbb{Q}$ to view $\mathbb{Z}$ as a subset of the field $\mathbb{Q}$. After this we prove some basic facts about rational numbers.

Although the definitions for addition and multiplication for $\mathbb{Q}$ are inspired by our prior experience with fractions, we do not use such experience with fractions in our proofs. Instead the proofs are based on previous results developed for $\mathbb{Z}$ in earlier chapters. At first we write $[x, y]$ for elements of $\mathbb{Q}$. Later in the chapter we develop thel notation x/y 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 the notation of fractions in our formal development.

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: March 14, 2016. Author: Professor W. Aitken (2009-2016) with updates by Professor L. Holt (2013-2016).

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:

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

□

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. *Using the above addition and multiplication, 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 have the second number 1 to be thought of as an integer. For example, $[3, 3]$ is 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. We can think of F as a field containing R. The field F is called the *field of fractions of* R. Thus $\mathbb{Q}$ is the field of fractions of $\mathbb{Z}$.

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

Optional Exercise. Verify that the construction and the main results concerning the construction can really be extended from $\mathbb{Z}$ to a general integral domain R. Why does R have to be an integral domain? In other words, what goes wrong if R is a more general ring?

Optional Exercise. Show that if R is a field, then the canonical embedding $R \to F$ is a bijection where F is the field of fractions of F. In other words, if R is already a field then its field of fractions is, in some sense, just itself.

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. In fact, we proved this identity for units in any commutative ring (see Chapter 5). 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

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

□

When you have a common denominator, the formula for addition is very simple. This is just a special case of the distributive law.

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 notation and properties from the previous section apply to any field. We will now return to the study of $\mathbb{Q}$, but will use the fractional notation whenever possible. Of course, $[x, y]$ can be written 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.

Now we show that we can be even pickier and insist that a and b have no factor in common greater than one:

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 $dg \leq g$. This implies that $d \leq 1$, which implies that $d = 1$, since d and g are both positive. 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}. □

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 in the following chapter, 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. A number $r \in \mathbb{Q}$ is 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.

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. We will show that either both a and b are positive integers, or that a and b are both negative integers. 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 $-b$. □

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 the previous theorem, $(-a)/b$ 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. □

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). □

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. The Incompleteness of $\mathbb{Q}$

In geometry we learn the Pythagorean Theorem which allows us to compute one side of a right triangle assuming we know the lengths of the other two sides. As an application, one easily shows that the diagonal of the unit square has length $\sqrt{2}$. In other words, the length d of the diagonal has the property that $d^2 = 2$. There is a problem: there is no such d in the field $\mathbb{Q}$. This elementary observation shows that $\mathbb{Q}$ does not have all the numbers required to do even basic geometry. So in some sense (to be made precise in Chapter 8) the rational numbers $\mathbb{Q}$ are "incomplete". This compels us to construct a richer number system $\mathbb{R}$ called the *real numbers* to fill in all the gaps in $\mathbb{Q}$. Any real number that is not in $\mathbb{Q}$ is called an *irrational real number*. The number $\pi \in \mathbb{R}$ is another important number missing from $\mathbb{Q}$.

We now formally show that there is indeed no $r \in \mathbb{Q}$ such that $r^2 = 2$. There are several proofs of this fact, and you may have seen a proof in another course. The proof given here is designed to build on our familiarity with modular arithmetic.

Theorem 30. *There is no $r \in \mathbb{Q}$ with the property that $r^2 = 2$.*

Proof. Suppose such an r exists. By Theorem 22 we can write $r = a/b$ where a and b are relatively prime integers. This implies that a and b cannot both be even. From the assumption $r^2 = 2$ we get the equation $a^2 = 2b^2$. This, in turn, implies that

$$a^2 \equiv 2b^2 \mod 4$$

CASE 1: a and b are both odd. In this case, $a^2 \equiv b^2 \equiv 1 \bmod 4$ by the following lemma. Substituting into $a^2 \equiv 2b^2$ gives $1 \equiv 2$ modulo 4. This is a contradiction.

CASE 2: a is odd, b is even. In this case, $a^2 \equiv 1 \bmod 4$ as before, but $b^2 \equiv 0 \bmod 4$ (see the following lemma). Substituting into $a^2 \equiv 2b^2$ gives $1 \equiv 0$ modulo 4. This is a contradiction.

CASE 3: a is even, b is odd. This case is similar to the previous case: $a^2 \equiv 0 \bmod 4$ but $b^2 \equiv 1 \bmod 4$. Substituting into $a^2 \equiv 2b^2$ gives us $0 \equiv 2$ modulo 4. This is a contradiction.

So in any case, we get a contradiction. So no such $r \in \mathbb{Q}$ exists. □

Lemma 31. *If $c \in \mathbb{Z}$ is odd then $c^2 \equiv 1$ modulo 4. If $c \in \mathbb{Z}$ is even then $c^2 \equiv 0$ modulo 4.*

Proof. Suppose $c \in \mathbb{Z}$ is odd. By the Quotient-Remainder Theorem and the definition of odd integer, $c = 2q + 1$. Thus

$$c^2 = (2q+1)^2 = 4q^2 + 4q + 1,$$

but

$$4q^2 + 4q + 1 \equiv 0 + 0 + 1 \equiv 1 \bmod 4.$$

Now suppose $c \in \mathbb{Z}$ is even. Then $c = 2d$ for some $d \in \mathbb{Z}$. So $c^2 = 4d^2$. Since $4 \mid c^2$ the result follows. □

Exercise 17. Adapt the proof of Theorem 30 to show that if $n \equiv 2 \bmod 4$ then there is no $r \in \mathbb{Q}$ such that $r^2 = n$. This shows, for example, that $\sqrt{10}$ is irrational.

Remark 8. One can generalize the above theorem to show that if $n \in \mathbb{Z}$ is not equal to some m^2 (with $m \in \mathbb{N}$) then there is no $r \in \mathbb{Q}$ with $r^2 = n$. Informally we say that if n is not a perfect square then n is irrational. This result can, in turn, be generalized to other powers beyond 2. We will not prove such results here.