MATH 321 – EQUIVALENCE RELATIONS, WELL-DEFINEDNESS, MODULAR ARITHMETIC, AND THE RATIONAL NUMBERS

ALLAN YASHINSKI

Abstract. We explore the notion of well-definedness when defining functions whose domain is the set of all equivalence classes of an equivalence relation. Then we apply this to define modular arithmetic and the set $\mathbb{Q}$ of rational numbers.

1. Equivalence Classes

We shall slightly adapt our notation for relations in this document. Let $\sim$ be a relation on a set X. Formally, $\sim$ is a subset of $X \times X$. Given two elements $x, y \in X$, we shall write $x \sim y$ to mean $(x, y) \in \sim$. From now on, we shall just use the notation $x \sim y$, and not explicitly reference $\sim$ as a subset of $X \times X$.

Recall that a relation $\sim$ on a set X is an *equivalence relation* if $\sim$ is

(i) *reflexive*: $(\forall x \in X)(x \sim x)$,
(ii) *symmetric*: $(\forall x, y \in X)(x \sim y \Rightarrow y \sim x)$, and
(iii) *transitive*: $(\forall x, y, z \in X)\big((x \sim y \ \wedge \ y \sim z) \Rightarrow (x \sim z)\big)$.

Suppose $\sim$ is an equivalence relation on X. When two elements are related via $\sim$, it is common usage of language to say they are *equivalent*. Given $x \in X$, the *equivalence class* of x is the set

$$[x] = \{y \in X \ : \ x \sim y\}.$$

In other words, the equivalence class $[x]$ of x is the set of all elements of X that are equivalent to x. Be mindful that $[x]$ is a subset of X, it is not an element of X. Typically, the set $[x]$ contains much more than just x. The element x is called a *representative* of the equivalence class $[x]$. Any element of an equivalence class can serve as a representative.

Exercise A. Given an equivalence relation $\sim$ on a set X, show that for any two elements $x, y \in X$,

$$x \sim y \quad \text{if and only if} \quad [x] = [y].$$

We shall use the notation $X/\!\sim$ to mean the set of all equivalence classes with respect to $\sim$. That is,

$$X/\!\sim = \big\{[x] \ : \ x \in X\big\}.$$

Notice that $X/\!\sim$ is a set whose elements are subsets of X. We've often referred to such a thing as a *family* of subsets of X. As shown in Theorem 6.2.10 (i), $X/\!\sim$ is actually a partition of X.

Example 1. Fix $n \in \mathbb{N}$. Recall that we say two integers $a, b \in \mathbb{Z}$ are *congruent modulo* n when $n \mid (a - b)$. As discussed in class, conguence modulo n is an equivalence relation. We shall write

$$a \equiv b \mod n$$

to mean a is conguent to b modulo n. The set of equivalence classes of integers with respect to this equivalence relation is traditionally denoted $\mathbb{Z}/n\mathbb{Z}$. This is less cumbersome notationally than writing something like $\mathbb{Z}/(\equiv \mod n)$.

Exercise B. Consider the relation of congruence modulo 5. Explicitly describe the equivalence classes [0] and [7] from $\mathbb{Z}/5\mathbb{Z}$.

2. Functions whose domain is $X/\sim$

It is common in mathematics (more common than you might guess) to work with the set $X/\sim$ of equivalence classes of an equivalence relation. Issues arise when one attempts to define functions

$$f : X/\sim \to Y$$

whose domain is $X/\sim$. When defining any function, one usually describes what the function does to a typical element of the domain. In this case, a typical element of the domain is an equivalence class $[x]$, which is represented by some element $x \in X$. One typically wants to define what $f([x])$ is in terms of the representative x. This is where one can get into trouble. Consider the following example.

Example 2. Let us attempt to define a function

$$f : \mathbb{Z}/5\mathbb{Z} \to \mathbb{Z}$$

by the formula $f([m]) = m$. Then we have

$$f([0]) = 0, \quad f([2]) = 2, \quad f([3]) = 3, \quad f([7]) = 7,$$

and so on. But there is a major problem here. Since $2 \equiv 7 \mod 5$, it follows that $[2] = [7]$. That is, [2] and [7] are the exact same element of the set $\mathbb{Z}/5\mathbb{Z}$. However, the "function" we've defined above has the property that $f([2]) \neq f([7])$. This is a clear violation of the definition of a function, and so f is not really a function at all. Mathematicians would say that the "function" f is not *well-defined*, which really just means that f is not a function. The issue is that the "rule" for f maps different representatives of the same equivalence class to different elements of the codomain.

Example 3. Let us attempt to define another function with domain $\mathbb{Z}/5\mathbb{Z}$. Given an integer $m \in \mathbb{Z}$, let $r_5(m)$ denote the remainder, as in the Division Algorithm, after m is divided by 5. So $r_5(m) \in \{0, 1, 2, 3, 4\}$. For example,

$$r_5(13) = 3, \quad \text{because} \quad 13 = 2 \cdot 5 + 3.$$

Let's define a function

$$f : Z/5\mathbb{Z} \to \{0, 1, 2, 3, 4\}, \quad \text{by} \quad f([m]) = r_5(m).$$

In this case, this function is *well-defined* (we'll explain how one checks this below.) At first glance, the definition of $f([m])$ appears to depend on the choice of the representative m of the equivalence class, but it actually does not.

We shall now explore how to ensure that we are defining actual functions out of $X/\sim$. In what follows, let

$$\pi : X \to X/\sim$$

be the function defined by $\pi(x) = [x]$. Notice this is an honest function. It is surjective, but in general is not injective, because any two equivalent elements will have the same image.

Exercise C. Suppose that $f : X/\sim \to Y$ is a function, that is an honest well-defined function. Let $g : X \to Y$ be the function $g = f \circ \pi$. Prove that

$$g(x) = g(x') \quad \text{whenever} \quad x \sim x'.$$

The point of this exercise is that in order to have a well-defined function

$$f : X/\sim \to Y,$$

then it must be the case that $f([x]) = f([x'])$ whenever $x \sim x'$. If not, then our attempt at making a function is not really a function at all. The following theorem says that this is the *only* issue we need to confront.

Theorem 1. *Let $\sim$ be an equivalence relation on X and let $g : X \to Y$ be a function with the property that*

$$g(x) = g(x') \quad \textit{whenever} \quad x \sim x'.$$

Then there exists a (well-defined) function

$$f : X/\sim \to Y$$

given by the formula $f([x]) = g(x)$.

Before we prove this theorem, let us return to Example 3. We started with the function

$$r_5 : \mathbb{Z} \to \{0, 1, 2, 3, 4\}.$$

Here, r_5 is going to play the role of g in the statement of the theorem. To use the theorem to verify that $f([m]) = r_5(m)$ is well-defined, we must show that

$$r_5(m) = r_5(m') \quad \text{whenever} \quad m \equiv m' \mod 5.$$

Assume $m \equiv m' \mod 5$. Then there is some $k \in \mathbb{Z}$ such that

$$m = m' + 5k.$$

Applying the Division Algorithm to m' gives us integers q and r such that

$$m' = 5q + r.$$

Now $r \in \{0, 1, 2, 3, 4\}$ and $r_5(m') = r$ by definition of r_5. Combining the above equations shows that

$$m = m' + 5k = (5q + r) + 5k = 5(q + k) + r.$$

From this, it follows that $r_5(m) = r$. Thus we have shown that

$$r_5(m) = r_5(m') \quad \text{whenever} \quad m \equiv m' \mod 5.$$

By the above theorem, the function

$$f : \mathbb{Z}/5\mathbb{Z} \to \{0, 1, 2, 3, 4\}, \quad f([m]) = r_5(m)$$

is well-defined.

This argument is typical of how one verifies that a function

$$f : X/\sim \to Y$$

is well-defined. One takes arbitrary elements $x, x' \in X$ for which $x \sim x'$, and then one shows that the proposed expressions for $f([x])$ and $f([x'])$ give the same element of Y. In this case we would say that the expression $f([x])$ depends only on the equivalence class of x, not on the representative x itself.

To prove the theorem, we must take a slight digression into the foundations of what a function actually is.

3. The Definition of a Function

We have been dealing with functions for quite some time now, but we never actually gave them a proper definition. According to the text:

"A function f from X to Y, written $f : X \to Y$, is a rule that pairs an element $x \in X$ with an element $y \in Y$, written $f(x) = y$, such that the following property holds.

$$(\forall x \in X)(\exists! y \in Y)[f(x) = y].$$

The central issue here is that the term "rule" is undefined. This makes for an ambiguous definition. This is really unacceptable in mathematics. Everything must always have a precise, unambiguous definition. This deficiency (hopefully) did not impede our understanding of functions. Instead, it is making it quite awkward to prove the above theorem. In order to prove that something *is* a function, we must be clear about *what* a function is.

Modern mathematics is built upon the foundations of set theory. What this means, is that *everything* in mathematics is really a set. This includes numbers, ordered pairs, relations (as we saw in class), and functions. We often don't think of these objects as sets, but they must be defined as sets so that we can be clear about what they are when we need to be. Here is the definition of a function:

Definition. A *function f from a set X to a set Y*, is a subset of $X \times Y$ with the following property:

$$(\forall x \in X)(\exists! y \in Y)\big[(x, y) \in f\big].$$

The set X is the *domain* of f and the set Y is the *codomain* of f. For each $x \in X$, the unique value $y \in Y$ such that $(x, y) \in f$ is denoted by $f(x)$ and is called the *image* of x.

Notice that f is a set. By definition, the statement $(x, y) \in f$ is equivalent to the statement $f(x) = y$. So whenever we say $f(x) = y$, we really mean $(x, y) \in f$. The collection of ordered pairs in f completely encode the "rule" of f. On your exam, the set f was called the *graph of f*.

Let us now define function composition.

Definition. Suppose $f \subseteq X \times Y$ and $g \subseteq Y \times Z$ are functions. The composition of g with f is the set

$$g \circ f = \big\{(x, z) \in X \times Z \ : \ (\exists y \in Y)\big[(x, y) \in f \ \wedge \ (y, z) \in g\big]\big\}.$$

Exercise D. Prove that $g \circ f$, as defined above, is a function. (Hint: for each $x \in X$, prove existence and uniqueness of $z \in Z$ for which $(x, z) \in g \circ f$ separately. To prove uniqueness, suppose $(x, z_1), (x, z_2) \in g \circ f$, and show that $z_1 = z_2$.)

We can translate the definitions of injectivity and surjectivity in terms of the set f.

Definition. Let $f \subseteq X \times Y$ be a function.

(i) We say f is *injective* if

$$(\forall y \in Y)(\forall x_1, x_2 \in X)\left(\big[(x_1, y) \in f \ \wedge \ (x_2, y) \in f\big] \Rightarrow (x_1 = x_2)\right).$$

(ii) We say f is *surjective* if

$$(\forall y \in Y)(\exists x \in X)\big[(x, y) \in f\big].$$

Exercise E. Suppose that $f \subseteq X \times Y$ is a function. Define $f^{-1} \subseteq Y \times X$ by

$$f^{-1} = \{(y, x) \in Y \times X \ : \ (x, y) \in f\}.$$

Prove that if f is both injective and surjective, then f^{-1} is a function.

Now we shall prove Theorem 1.

Proof. (Theorem 1) Suppose $\sim$ is an equivalence relation on X and $g : X \to Y$ is a function such that

$$g(x) = g(x') \quad \text{whenever} \quad x \sim x'.$$

Define $f \subseteq (X/\!\sim) \times Y$ by

$$f = \left\{\big([x], g(x)\big) \ : \ x \in X\right\}.$$

We shall prove that f is a function. Notice that every element of $X/\!\sim$ is of the form $[x]$ for some $x \in X$. So let $[x] \in X/\!\sim$ be an arbitrary equivalence class, one of whose elements is $x \in X$. Let $y = g(x)$. Then

$$\big([x], y\big) = \big([x], g(x)\big) \in f.$$

This shows that for every $[x] \in X/\!\sim$, there is $y \in Y$ such that $\big([x], y\big) \in f$. For the uniqueness assertion, suppose that $\big([x], g(x)\big) \in f$ and $\big([x'], g(x')\big) \in f$ are such that $[x] = [x']$. Then $x' \in [x]$, which implies $x \sim x'$ by definition of equivalence class. So $g(x) = g(x')$, by the assumed properties of g. We conclude that for every $[x] \in X/\!\sim$, there is a unique $y \in Y$ such that $\big([x], y\big) \in f$. By definition, f is a function. $\square$

From now on, we shall no longer explicitly think of a function $f : X \to Y$ as a subset of $X \times Y$, unless we need to. In fact, other people may look strangely at you if you say things like $(x, y) \in f$, rather than $f(x) = y$ (remember, they are equivalent statements, by definition.) So now we can go about our lives treating functions as we used to, secretly knowing that we've built a rigorous foundation of what a function really is.

Example 4. Another situation in which we have been a little lax is in defining ordered pairs properly (and consequently Cartesian products). In light of the definition of a function, this is a loose end we should tie up. Everything must be a set, so we need to encode an ordered pair (x, y) into some set. Since sets are unordered, we cannot use $\{x, y\}$ to represent (x, y), because $\{x, y\} = \{y, x\}$ would then represent (y, x) as well. This is a problem because we want to distinguish between (x, y) and (y, x). Someone clever (Kazimierz Kuratowski) came up with

the following definition. Given $x \in X$ and $y \in Y$, define the *ordered pair* (x, y) to be the set

$$(x, y) = \big\{\{x\}, \{x, y\}\big\}.$$

Notice that $(x, y) \in \mathscr{P}(\mathscr{P}(X \cup Y))$. This turns out to be a good definition, because it satisfies what we want to be true about ordered pairs, namely that

$$(x_1, y_1) = (x_2, y_2) \quad \text{if and only if} \quad (x_1 = x_2) \ \wedge \ (y_1 = y_2).$$

Notice here that $(x_1, y_1) = (x_2, y_2)$ is an equality of *sets*. The *Cartesian Product of* X *and* Y is defined to be the subset $X \times Y \subseteq \mathscr{P}(\mathscr{P}(X \cup Y))$ given by

$$X \times Y = \big\{(x, y) \ : \ x \in X \ \wedge \ y \in Y\big\}.$$

Exercise F. Using Kuratowski's definition of an ordered pair, prove that

$$(x_1, y_1) = (x_2, y_2) \quad \text{if and only if} \quad (x_1 = x_2) \ \wedge \ (y_1 = y_2).$$

(Hint: The forward ($\Rightarrow$) direction is the nontrivial part. You may want to deal with the case where $x_1 = y_1$ first, and then you can assume $x_1 \neq y_1$ for the rest of the proof. The reason for doing this is that

$$(x, x) = \big\{\{x\}, \{x, x\}\big\} = \big\{\{x\}, \{x\}\big\} = \big\{\{x\}\big\}$$

reduces to something much simpler when the two coordinates are the same.)

Similarly to the case of functions, no one ever really explicitly thinks of (x, y) as the set $\big\{\{x\}, \{x, y\}\big\}$. For example, people will look strangely at you if you write things like $\{x\} \in (x, y)$ or $\big\{\{x, y\}\big\} \subseteq (x, y)$, even if they are technically true. What's most important here is that we've rigorously defined the object (x, y) in such a way that

$$(x_1, y_1) = (x_2, y_2) \quad \text{if and only if} \quad (x_1 = x_2) \ \wedge \ (y_1 = y_2).$$

Now, we can treat an ordered pair as a "black box" that satisfies the above property. If you think about it, that's what we've been doing all along.

4. A Canonical Bijection

Given a function $f : X \to Y$, let $\sim_f$ be the relation on X defined by

$$x \sim_f x' \quad \text{if and only if} \quad f(x) = f(x').$$

Exercise G. Prove that $\sim_f$ is an equivalence relation on X.

Theorem 2. *If $f : X \to Y$ is a surjection, then there is a bijection*

$$\tilde{f} : X/{\sim_f} \to Y,$$

defined by

$$\tilde{f}\big([x]\big) = f(x).$$

Proof. By definition of $\sim_f$, we know that

$$f(x) = f(x') \quad \text{whenever} \quad x \sim_f x'.$$

So by Theorem 1, the function

$$\tilde{f} : X/{\sim_f} \to Y, \qquad \tilde{f}\big([x]\big) = f(x)$$

is well-defined. We shall prove $\tilde{f}$ is a bijection. To see it is surjective, let $y \in Y$ be arbitrary. Since f is surjective, there is some $x \in X$ for which $f(x) = y$. Thus, the element $[x] \in X/\!\sim_f$ satisfies

$$\tilde{f}\big([x]\big) = f(x) = y.$$

Thus, $\tilde{f}$ is surjective. To see it is injective, suppose $[x], [x'] \in X/\!\sim_f$ are arbitrary classes for which $\tilde{f}\big([x]\big) = \tilde{f}\big([x']\big)$. Then $f(x) = f(x')$ by definition of $\tilde{f}$. It follows that $x \sim_f x'$ by definition of $\sim_f$. As $\sim_f$ is an equivalence relation, this implies $[x] = [x']$. Thus, $\tilde{f}$ is surjective. □

As an example of this theorem, consider for $n \in \mathbb{N}$ the surjection

$$r_n : \mathbb{Z} \to \{0, 1, 2, \ldots, n-1\}$$

which associates to an integer its remainder after division by n. Notice that the equivalence relation $\sim_{r_n}$ on $\mathbb{Z}$ is exactly congruence modulo n. By Theorem 2, the map

$$\tilde{r}_n : \mathbb{Z}/n\mathbb{Z} \to \{0, 1, 2, \ldots, n-1\}, \qquad \tilde{r}_n\big([m]\big) = r_n(m)$$

is a bijection. We conclude that $\mathbb{Z}/n\mathbb{Z}$ contains exactly n distinct equivalence classes, and more explicitly,

$$\mathbb{Z}/n\mathbb{Z} = \big\{[0], [1], [2], \ldots, [n-1]\big\}.$$

5. Modular Arithmetic

The familiar arithmetical operations of addition and multiplication can actually be carried out on the elements of

$$\mathbb{Z}/n\mathbb{Z} = \big\{[0], [1], [2], \ldots, [n-1]\big\}.$$

5.1. **Addition.** Notice that the operation of addition of integers can be thought of as a function

$$+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}.$$

The element $+(a, b) \in \mathbb{Z}$ is usually written as $a + b$.

To define addition on $\mathbb{Z}/n\mathbb{Z}$, we will define a function

$$+ : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}.$$

We shall write $[a] + [b]$ to mean the element $+\big([a], [b]\big)$ of $\mathbb{Z}/n\mathbb{Z}$.

Definition. Define $+ : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ by

$$[a] + [b] = [a + b].$$

Notice that the $a + b$ on the right hand side is the sum of two integers, which is already defined. The sum $[a] + [b]$ is defined the be the equivalence class of the sum $a + b$. Here, we run into the potential problem that this operation is not well-defined. The sum $[a] + [b]$ is actually defined in terms of the representatives of the equivalence classes. We must make sure that if we choose different representatives, we still get the same result. Here's how a typical proof of well-definedness of this operation looks:

Suppose $a \equiv c \mod n$ and $b \equiv d \mod n$. Then

$$a = c + nk, \qquad b = d + n\ell,$$

for some $k, \ell \in \mathbb{Z}$. Then

$$c + d = a - nk + b - n\ell = (a + b) - (k + \ell)n,$$

which shows that

$$c + d \equiv a + b \mod n.$$

Thus, $[c + d] = [a + b]$. We conclude that when $[a] = [c]$ and $[b] = [d]$, we have

$$[a] + [b] = [a + b] = [c + d] = [c] + [d].$$

So our formula for addition on $\mathbb{Z}/n\mathbb{Z}$ is well-defined.

Example 5. When $n = 2$, $\mathbb{Z}/2\mathbb{Z} = \big\{[0], [1]\big\}$. We have

$$[0] + [0] = [0], \quad [0] + [1] = [1], \quad [1] + [0] = [1], \quad [1] + [1] = [2] = [0].$$

Example 6. In $\mathbb{Z}/8\mathbb{Z} = \big\{[0], [1], [2], [3], [4], [5], [6], [7]\big\}$,

$$[1] + [4] = [5], \quad [3] + [5] = [8] = [0], \quad [4] + [6] = [10] = [2], \quad \text{etc.}$$

Once we know that the operation $+$ is well-defined on $\mathbb{Z}/n\mathbb{Z}$, in inherits many of the properties of $+$ on the integers $\mathbb{Z}$, such as associativity and commutativity.

Proposition 3. *For all $[a], [b], [c] \in \mathbb{Z}/n\mathbb{Z}$,*

(i) (Associativity) $\big([a] + [b]\big) + [c] = [a] + \big([b] + [c]\big)$.
(ii) (Commutativity) $[a] + [b] = [b] + [a]$.
(iii) (Additive identity) $[0] + [a] = [a] = [a] + [0]$.
(iv) (Additive inverses) $[a] + [-a] = [0] = [-a] + [a]$.

Proof. For arbitrary $[a], [b], [c] \in \mathbb{Z}/n\mathbb{Z}$,

$$\big([a] + [b]\big) + [c] = [a + b] + [c] = [(a + b) + c].$$

By associativity of addition on $\mathbb{Z}$,

$$[(a + b) + c] = [a + (b + c)] = [a] + [b + c] = [a] + \big([b] + [c]\big).$$

This proves (i). For (ii),

$$[a] \cdot [b] = [ab] = [ba] = [b] \cdot [a],$$

where in the middle we used commutativity of multiplication on $\mathbb{Z}$. Similarly, we prove (iii) and (iv):

$$[0] + [a] = [0 + a] = [a] = [a + 0] = [a] + [0],$$

$$[a] + [-a] = [a + (-a)] = [0] = [(-a) + a] = [-a] + [a].$$

□

In the language of abstract algebra, this proposition says that the addition operation we've defined makes $\mathbb{Z}/n\mathbb{Z}$ into an *abelian group*. We won't define this term, and I won't expect you to know it, this is just for your information (you'll see it again if you take abstract algebra.)

5.2. **Multiplication.** We can also define a multiplication operation

$$\cdot : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}.$$

We shall write $[a] \cdot [b]$ to mean the image of $\big([a], [b]\big)$ under this function.

Definition. Define $\cdot : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ by

$$[a] \cdot [b] = [ab].$$

Again, we must check that this is well-defined. Suppose

$$a \equiv c \mod n, \qquad b \equiv d \mod n.$$

Then

$$a = c + nk, \qquad b = d + n\ell$$

for some integers $k, \ell \in \mathbb{Z}$. We see that

$$cd = (a - nk)(b - n\ell) = ab - na\ell - nbk + n^2 k\ell = ab - n(a\ell + bk - nk\ell).$$

This calculation shows that $cd \equiv ab \mod n$, and consequently, $[ab] = [cd]$. Thus, if $[a] = [c]$ and $[b] = [d]$, we have

$$[a] \cdot [b] = [ab] = [cd] = [c] \cdot [d].$$

We conclude that the element $[a] \cdot [b] \in \mathbb{Z}/n\mathbb{Z}$ does not depend on the choice of representatives a and b. Our operation of multiplication is well-defined.

Example 7. In $\mathbb{Z}/8\mathbb{Z} = \big\{[0], [1], [2], [3], [4], [5], [6], [7]\big\}$,

$[2] \cdot [3] = [6], \quad [4] \cdot [6] = [24] = [0], \quad [3] \cdot [7] = [21] = [5], \quad [5] \cdot [5] = [25] = [1], \quad$ etc.

Multiplication on $\mathbb{Z}/n\mathbb{Z}$ inherits several properties from multiplication on $\mathbb{Z}$, as the next proposition shows.

Proposition 4. *For all* $[a], [b], [c] \in \mathbb{Z}/n\mathbb{Z}$,

(i) (Associativity) $\big([a] \cdot [b]\big) \cdot [c] = [a] \cdot \big([b] \cdot [c]\big)$.
(ii) (Commutativity) $[a] \cdot [b] = [b] \cdot [a]$.
(iii) (Distributive Property) $[a] \cdot \big([b] + [c]\big) = \big([a] \cdot [b]\big) + \big([a] \cdot [c]\big)$.
(iv) (Multiplicative Identity) $[1] \cdot [a] = [a] = [a] \cdot [1]$.

Proof. The proof is similar to that of Proposition 3. For example, to prove *(iii)*,

$$[a] \cdot \big([b] + [c]\big) = [a] \cdot [b + c] = [a(b + c)] = [ab + ac],$$

by the distributive property of $\mathbb{Z}$. Continuing the calculation,

$$[ab + ac] = [ab] + [ac] = \big([a] \cdot [b]\big) + \big([a] \cdot [c]\big).$$

□

All these properties mean that the set $\mathbb{Z}/n\mathbb{Z}$ with its two operations of addition and multiplication is a *commutative ring*. Again, you don't need to know this terminology, but you would see it in an abstract algebra course.

Definition. The *multiplicative inverse* of an element $[a] \in \mathbb{Z}/n\mathbb{Z}$ is an element $[b] \in \mathbb{Z}/n\mathbb{Z}$ for which $[a] \cdot [b] = [1]$.

Multiplicative inverses do not always exist. For example, $[0] \in \mathbb{Z}/n\mathbb{Z}$ never has a multiplicative inverse (assuming $n > 1$).

Example 8. In $\mathbb{Z}/5\mathbb{Z}$, the following are true:

$$[1] \cdot [1] = [1], \quad [2] \cdot [3] = [1], \quad [4] \cdot [4] = [1].$$

Thus, [3] is the inverse of [2] (and vice-versa), [4] is its own inverse, and [1] is its own inverse.

Example 9. In $\mathbb{Z}/4\mathbb{Z}$, the element [2] has no multiplicative inverse. We can prove this by exhaustion (checking its product with all possibilities):

$$[2] \cdot [0] = [0], \quad [2] \cdot [1] = [2], \quad [2] \cdot [2] = [0], \quad [2] \cdot [3] = [2].$$

Thus, there is no element $[a]$ such that $[2] \cdot [a] = [1]$.

Exercise H. (a) It is a fact that in

$$\mathbb{Z}/7\mathbb{Z} = \big\{[0], [1], [2], [3], [4], [5], [6]\big\},$$

every element except for [0] has a multiplicative inverse. Find the inverse of each nonzero class.

(b) Determine which elements of

$$\mathbb{Z}/9\mathbb{Z} = \big\{[0], [1], [2], [3], [4], [5], [6], [7], [8]\big\}$$

have a multiplicative inverse, and find the inverses.

A commutative ring for which each nonzero element has a multiplicative inverse is called a *field*. Once again, this is more abstract algebra terminology that you don't have to know for this class. It is a fact, which we shall neither prove nor use, that

$$\mathbb{Z}/n\mathbb{Z} \text{ is a field if and only if } n \text{ is prime.}$$

6. Building the Rational Numbers

As discussed above, everything in mathematics must be defined, typically as a set, and this includes numbers. Defining our number systems $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$ is an issue we have largely avoided, and is one which may be more complicated than you would think. Notice that

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}.$$

This chain of subset inclusions also represents how one constructs these number systems:

- $\mathbb{Z}$ is defined in terms of $\mathbb{N}$.
- $\mathbb{Q}$ is defined in terms of $\mathbb{Z}$.
- $\mathbb{R}$ is defined in terms of $\mathbb{Q}$.
- $\mathbb{C}$ is defined in terms of $\mathbb{R}$.

This begs the question: "How does one define $\mathbb{N}$?" The answer is that $\mathbb{N}$ must be defined using sets, and sets alone. We shall not explore the construction of $\mathbb{N}$, but it is a fact that once we have defined the set $\mathbb{N}$, we can build the other number systems as indicated above. Each of the four constructions differs from the others. Some are simpler than others: Defining the complex numbers $\mathbb{C}$ in terms of the reals $\mathbb{R}$ is one of the simplest, whereas defining $\mathbb{R}$ in terms of $\mathbb{Q}$ is much more difficult. Here, we shall explore only one of them: constructing the set $\mathbb{Q}$ of rational numbers from the set $\mathbb{Z}$ of integers.

Here is the main idea in defining $\mathbb{Q}$. We think of a rational number as a quotient $\frac{a}{b}$ of two integers a and b. We could attempt to represent this quotient as an ordered

pair $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ (remember we are supposed to be using $\mathbb{Z}$ to define $\mathbb{Q}$.) The central issue is this: several pairs of integers can be used to represent the same rational number. For example, we all know that

$$\frac{1}{2} = \frac{2}{4} = \frac{5}{10} = \frac{150}{300}.$$

However, none of the ordered pairs

$$(1, 2), \quad (2, 4), \quad (5, 10), \quad (150, 300)$$

are equal, as elements on $\mathbb{Z} \times \mathbb{Z}$. We shall want to *think* of these ordered pairs as being the same. The mathematical solution to this problem is to put an equivalence relation on the set of ordered pairs of integers in such a way that the above pairs are *equivalent*. This is the idea that will guide the construction.

Not every ordered pair of integers should represent a fraction, because we want to prohibit the situation in which the denominator is 0. Thus, the set we shall work with will be

$$\mathbb{Z} \times \big(\mathbb{Z} \setminus \{0\}\big).$$

An element $(a, b) \in \mathbb{Z} \times \big(\mathbb{Z} \setminus \{0\}\big)$ will ultimately represent the number $\frac{a}{b}$. We need to figure out when two such pairs (a, b) and (c, d) represent the *same* fraction. We've known since grade school that the statement

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

needs to be true. Teachers usually call this "cross-multiplying." This motivates the following definition.

Definition. Define a relation $\sim$ on $\mathbb{Z} \times \big(\mathbb{Z} \setminus \{0\}\big)$ so that

$$(a, b) \sim (c, d) \quad \text{whenever} \quad ad = bc.$$

Exercise I. Prove that $\sim$ is an equivalence relation on $\mathbb{Z} \times \big(\mathbb{Z} \setminus \{0\}\big)$.

(Hint: To prove transitivity, assume $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$. Then show that this implies that $d(af - be) = 0$. Then use the fact that if a product of integers is zero, then one of the factors must be zero.

Definition. The set $\mathbb{Q}$ of *rational numbers* is defined the be the set of equivalence classes of elements of the set $\mathbb{Z} \times \big(\mathbb{Z} \setminus \{0\}\big)$ with respect to the relation $\sim$.

Given $a, b \in \mathbb{Z}$ with $b \neq 0$, se shall use the notation $\frac{a}{b}$ to mean $\big[(a, b)\big] \in \mathbb{Q}$. That is,

$$\frac{a}{b} = \big[(a, b)\big],$$

is a *definition*, where we are defining the left hand side to be the right hand side.

Exercise J. Prove that

$$\frac{1}{2} = \frac{2}{4} \quad \text{and} \quad \frac{-2}{5} = \frac{6}{-15}.$$

Exercise K. Define a function $f : \mathbb{Z} \to \mathbb{Q}$ by $f(n) = \big[(n, 1)\big]$. Prove that this function is injective. (Be careful about what it means when two elements of $\mathbb{Q}$ are equal.) This allows us to identify $\mathbb{Z}$ as a subset of $\mathbb{Q}$, namely its image $\overline{f}(\mathbb{Z}) \subseteq \mathbb{Q}$, under the function f.

A discussion of $\mathbb{Q}$ would not be complete without discussing its algebraic operations of addition and multiplication. Since $\mathbb{Q}$ is a set of equivalence classes, this will cause issues of well-definedness as it did in the discussion of $\mathbb{Z}/n\mathbb{Z}$.

Knowing what we know about adding fractions, we define addition $+ : \mathbb{Q}\times\mathbb{Q} \to \mathbb{Q}$ by

$$[(a,b)] + [(c,d)] = [(ad+bc, bd)].$$

Exercise L. Prove that addition on $\mathbb{Q}$ is well-defined. That is, show that the result of addition $[(a,b)] + [(c,d)]$ does not depend on the choice of representatives (a,b) and (c,d). It is important to understand what needs to be done here: Given ordered pairs $(a,b),(c,d),(e,f),(g,h)$ such that $(a,b) \sim (e,f)$ and $(c,d) \sim (g,h)$, you must show that

$$(ad+bc, bd) \sim (eh+fg, fh),$$

so that

$$\big[(ad+bc,bd)\big] = \big[(eh+fg,fh)\big].$$

From this it follows that if $\big[(a,b)\big] = \big[(e,f)\big]$ and $\big[(c,d)\big] = \big[(g,h)\big]$, then

$$\big[(a,b)\big] + \big[(c,d)\big] = \big[(ad+bc,bd)\big] = \big[(eh+fg,fh)\big] = \big[(e,f)\big] + \big[(g,h)\big],$$

This shows that the result of addition does not depend on the chosen representatives of the equivalence classes.

We can also define multiplication $\cdot : \mathbb{Q}\times\mathbb{Q} \to \mathbb{Q}$ by

$$\big[(a,b)\big] \cdot \big[(c,d)\big] = \big[(ac,bd)\big].$$

Exercise M. Similarly to the last exercise, show that multiplication on $\mathbb{Q}$ is well-defined.

We shall denote the element $\big[(0,1)\big] \in \mathbb{Q}$ by 0, and denote the element $\big[(1,1)\big]$ by 1. Given an element $r = \big[(a,b)\big] \in \mathbb{Q}$, we define $-r$ to be the element

$$-r = \big[(-a,b)\big] \in \mathbb{Q}.$$

Proposition 5. *Let $r,s,t \in \mathbb{Q}$. Then*

(i) $(r+s)+t = r+(s+t)$.
(ii) $r+s = s+r$.
(iii) $r+0 = r = 0+r$.
(iv) $r+(-r) = 0 = (-r)+r$.
(v) $(r\cdot s)\cdot t = r\cdot(s\cdot t)$.
(vi) $r\cdot s = s\cdot r$.
(vii) $r\cdot(s+t) = (r\cdot s)+(r\cdot t)$.
(viii) $r\cdot 1 = r = 1\cdot r$.

Proof. We'll prove $(i),(iv),(vi)$, and $(viii)$. Let's denote $r = \big[(a,b)\big], s = \big[(c,d)\big]$, and $t = \big[(e,f)\big]$. For (i),

$$\begin{aligned}(r+s)+t &= \big(\big[(a,b)\big] + \big[(c,d)\big]\big) + \big[(e,f)\big] \\ &= \big[(ad+bc,bd)\big] + \big[(e,f)\big] \\ &= \big[((ad+bc)f + bde, bdf)\big] \\ &= \big[(adf+bcf+bde, bdf)\big],\end{aligned}$$

whereas

$$\begin{aligned} r + (s + t) &= \big[(a, b)\big] + \big(\big[(c, d)\big] + \big[(e, f)\big]\big) \\ &= \big[(a, b)\big] + \big[(cf + de, df)\big] \\ &= \big[(adf + b(cf + de), bdf)\big] \\ &= \big[(adf + bcf + bde, bdf)\big]. \end{aligned}$$

Thus, we see that

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

For (iv),

$$r + (-r) = \big[(a, b)\big] + \big[(-a, b)\big] = \big[(ab + (-ab), b^2)\big] = \big[(0, b^2)\big].$$

Notice that for any $m \in \mathbb{Z} \setminus \{0\}$, we have $(0, m) \sim (0, 1)$. Indeed, it is true that $0 \cdot 1 = 0 \cdot m$. Thus, for any such m, $\big[(0, m)\big] = 0 \in \mathbb{Q}$. Thus,

$$r + (-r) = \big[(0, b^2)\big] = 0,$$

as desired. Similarly (or by part (ii)), we have $(-r) + r = 0$.

For (vi),

$$r \cdot s = \big[(a, b)\big] \cdot \big[(c, d)\big] = \big[(ac, bd)\big] = \big[(ca, db)\big] = \big[(c, d)\big] \cdot \big[(a, b)\big] = s \cdot r.$$

For $(viii)$,

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

By part (vi) and the previous calculation, $1 \cdot r = r \cdot 1 = r$. □

Exercise N. Prove parts $(ii), (iii), (v), (vii)$ of Proposition 5.

Using the notation $\dfrac{a}{b} = \big[(a, b)\big] \in \mathbb{Q}$, our operations satisfy

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

Thus, we have defined the arithmetic of $\mathbb{Q}$ and proved its familiar properties.

Lastly, let's address the issue of multiplicative inverses. Given $r = \big[(a, b)\big] \in \mathbb{Q}$ such that $r \neq 0$, define $r^{-1} = \big[(b, a)\big]$. Notice that $a \neq 0$ here (Why?).

Exercise O. Show that for any $r \in \mathbb{Q}$ such that $r \neq 0$,

$$r \cdot r^{-1} = 1 = r^{-1} \cdot r.$$

In the language of abstract algebra, $\mathbb{Q}$ is a field, because it is a commutative ring (by Proposition 5), in which every nonzero element has a multiplicative inverse.

People don't outwardly treat rational numbers as equivalence classes of ordered pairs of integers. Once again, you will earn strange looks if you write things like

$$(4, 8) \in \frac{1}{2},$$

even though it is a true statement. The point is that we have rigorously defined $\mathbb{Q}$ and its operations in such a way that it behaves in the way that we've always treated rational numbers. Now we can go back to our old habits, confidently knowing that everything has been put on a firm foundation.