# Lecture 10

# Quotient rings and ring isomorphisms

## 10.1 Goals

1. Recall the definitions of equivalence relation, equivalence class, and quotient sets
2. Understand why the set of algebraic functions on an algebraic set $X$ is naturally in bijection with a quotient set
3. Become familiar with some common quotient rings
4. See how to make ring homomorphisms out of quotient rings
5. See the notion of ring isomorphism

## 10.2 The set of algebraic functions on $X$

Fix an algebraic set $X \subset \mathbb{R}$. We have seen that a given algebraic function $f : X \to \mathbb{R}$ can have many different polynomial extensions $g : \mathbb{R}^n \to \mathbb{R}$. For example, if $f$ is the zero function, we have seen that the set of extensions to $\mathbb{R}^n$ forms an ideal of $\mathbb{R}[x_1, \ldots, x_n]$.

Here is a beautiful insight: The ring of all algebraic functions on $X$, then, is like the set of all polynomial functions on $\mathbb{R}^n$, but where we consider (or declare) two polynomials $g$ and $h$ to be "equivalent" when $g|_X = h|_X$.

More precisely, there seems to be a bijection between the set

$$\{\text{Algebraic functions on } X\}$$

and the set

$$\{\text{Polynomial functions on } \mathbb{R}^n, \text{ where we pretend "} g = h \text{" if } g|_X = h|_X\} \tag{10.2.0.1}$$

Put yet another way: From the perspective of $X$, a polynomial on $\mathbb{R}^n$ is only as good as its restriction to $X$, so $X$ will treat any two polynomials the same so long as they both agree along $X$.

### 10.2.1 Equivalence relations

The issue now is to try to make the vague description (10.2.0.1) precise. What does it mean to "declare" or to "pretend" that two things that are not equal, to be equal? This brings us to the notion of quotient sets, which are most naturally described by using the auxiliary ideas of equivalence relations and equivalence classes.

**Remark 10.2.1.** It is a *good* sign in math if we have a feeling about what something ought to be, but we don't know how to express our feelings precisely. Being able to give a precise description of the thing we're feeling is the hardest part of math; and if it's hard, it's typically worth doing. (This way, when you need to use the feeling again in the future, you know *exactly* how to articulate it mathematically. It's best not to put things like this off.) This is one sense in which mathematics is like poetry. They're both about finding the truest ways to express something that seems to exist in a realm outside language.

So let's recall some ideas you may have seen in another course:

**Definition 10.2.2.** Fix a set $R$. An *equivalence relation* on $R$ is a subset $E \subset R \times R$, satisfying the following properties:

1. (Reflexivity.) For every $g \in R$, $(g, g) \in E$.
2. (Symmetry.) If $(g, h) \in E$ then $(h, g) \in E$.
3. (Transitivity.) If $(g, h) \in E$ and $(h, j) \in E$, then $(g, j) \in E$.

**Notation 10.2.3.** If $E \subset R \times R$ is an equivalence relation on $R$, we will write the notation

$$g \sim h$$

to mean that $(g, h) \in E$. Using this notation, the above properties of an equivalence relation may be written as

1. (Reflexivity.) For every $g \in R$, $g \sim g$.
2. (Symmetry.) If $g \sim h$ then $h \sim g$.
3. (Transitivity.) If $g \sim h$ and $h \sim j$, then $g \sim j$.

**Example 10.2.4.** Let $R = \mathbb{R}[x, y]$ be the set of polynomials in two variables, and fix an algebraic set $X \subset \mathbb{R}^2$. Then we declare an equivalence relation on $R$ by declaring:

$$g \sim h \iff g|_X = h|_X.$$

(Or, in other words, if and only if $(g - h)|_X = 0$.) This is fun! Note that this relation describes exactly the way in which we wanted to declare two polynomials to be "the same" from the perspective of $X$ (10.2.0.1).

And yes, this is indeed an equivalence relation:

1. (Reflexivity.) Of course, if $g$ is any polynomial, then $g|_X = g|_X$. So $g \sim g$.
2. (Symmetry.) Suppose $g$ and $h$ are two polynomials for which $g \sim h$, so $g|_X = h|_X$. Then, of course, $h|_X = g|_X$ (because equality of functions is symmetric), so $h \sim g$ as well.
3. (Transitivity.) If $g \sim h$ and $h \sim j$, then we see that $g|_X = h|_X$ and $h|_X = j|_X$. Then, because equalities of functions is transitive, we see that $g|_X = j|_X$. In other words, $g \sim j$.

**Example 10.2.5** (Informal)**.** This is probably the most useful non-mathematical example. Let $R$ be some collection of people. Then we can declare $E$ to be the set of pairs of people $(g, h)$ for which person $g$ is related to person $h$. Then of course, every person is related to themselves, if $g$ is related to $h$, then $h$ is related to $g$, and finally, if $g$ is related to $h$ and $h$ is related to $j$, then of course $g$ is related to $j$.

Thus the word relation in "equivalence relation" has a different, somewhat literal, intuition about it.

### 10.2.2 Equivalence classes

"Equivalence relation" is a pretty good name for the above idea—it turns out an equivalence relation is the right amount of scaffolding one needs to create a new set for which if $g \sim h$, then in fact, "$g$ becomes equal to $h$" in the new set. We begin the construction of this new set by describing its elements: Equivalence classes.

**Definition 10.2.6.** Let $R$ be a set and $E \subset R \times R$ an equivalence relation on $R$. Then an *equivalence class* of $E$ is a subset $C \subset R$ satisfying the following three properties:

1. $C$ is non-empty. (So there is at least one element $g \in R$ that is in $C$.)
2. $C$ is closed under the relation $E$. (This means that if $g \in C$, and if $h \sim g$, then $h \in C$.)
3. Every element of $C$ is related. (This means that if $g, h \in C$, then $g \sim h$.)

**Example 10.2.7.** In the setting of Example 10.2.5, if $R$ is a collection of people, and $E$ is the "related" equivalence relation, then an equivalence class of $R$ is precisely one family of people: A family has at least one person in it, every person related to a family member is obviously a family member, and if two people are in the same family, then they are related.

(Of course, notion of "family" and "related" can be given many different meanings—I personally do not take family/related to involve blood lines or any concrete genetic link, but you should construe these terms in a way that makes this example valid. This example is being used only to build intuition.)

**Example 10.2.8.** Let $R = \mathbb{R}[x, y]$ be the set of polynomials in two variables, and fix an algebraic set $X \subset \mathbb{R}^2$. Then we declare an equivalence relation on $R$ by declaring:

$$g \sim h \iff g|_X = h|_X.$$

We saw in Example 10.2.4 that this is indeed an equivalence relation.

Then what is an equivalence class in this example? An equivalence class $C$ is some collection of polynomial functions $C \subset \mathbb{R}[x, y]$, satisfying the following properties:

1. There is at least one polynomial function $g \in C$.

2. If $g \in C$, and if some polynomial function $h \in \mathbb{R}[x, y]$ satisfies $h|_X = g|_X$, then $h$ is also in $C$.

3. Finally, if two functions $g$ and $h$ are both in $C$, then their restrictions to $X$ agree.

In other words, an equivalence class is precisely a collection of polynomials on $\mathbb{R}^2$ that take on the exact same values on $X$.

Using the language from our familial example, it's as though we declare two polynomials to be in the same family if, from the perspective of $X$, they define the same function.

**Notation 10.2.9.** Let $R$ be a set and $E \subset R \times R$ an equivalence relation. If $x \in R$, then we let

$$[x]$$

denote the equivalence class containing $x$.

### 10.2.3 Quotient sets

**Definition 10.2.10.** Let $R$ be a set and $E \subset R \times R$ an equivalence relation on $R$. Then the *quotient* of $R$ by $E$, also known as the *quotient set*, is the set of all equivalence classes. We write this set as

$$R/_\sim.$$

(We will see some other notation for it later in the course.)

**Remark 10.2.11.** Note that $R/_\sim$ is a set of sets—an element of $R/_\sim$ is a set itself.

If you've ever heard that a set is like a bag of things (where the contents of the bag are the elements of the set) then a set of sets is like a bag containing bags. That's how you can think of $R/_\sim$ if you like.

**Example 10.2.12.** Let's follow Example 10.2.5, so that $R$ is a set of people and $E \subset R \times R$ is the equivalence relation where $g \sim h$ exactly when $g$ is related to $h$. Then $R/_\sim$ is the set of families.

**Example 10.2.13.** As a further example, suppose that $R$ is the set of five names as follows:

$$\{\text{John Dille, Ralph Dille, John Lew, Erica Lew, Peter Lew.}\}$$

Let's declare a relation $E$ for which a person is related to another if and only if they have the same last name. Then the set $R/_\sim$ would consist of two elements—the Dilles and the Lews.

**Remark 10.2.14.** By definition, $[x] \in R/_\sim$. (See Notation **??**.)

We note that $x \sim y$ if and only if

$$[x] = [y].$$

So $[x]$ and $[y]$ are the *same* element of $R/_\sim$. The lesson is that the notation $[x]$ is rather biased—it privileges the representative $x$ of the equivalence class, even though there may be many other possible representatives.

### 10.2.4 The quotient map

**Definition 10.2.15** (Quotient map)**.** Let $R$ be a set and $E \subset R \times R$ an equivalence relation. Then there is a function

$$R \to R/_\sim, \qquad g \mapsto [g]$$

sending an element $x \in R$ to its equivalence class. This is called the *quotient map*.

### 10.2.5 The ring of algebraic functions on $X$ as a quotient set

The proceeding sections were a crash course in equivalence relations. Our main use of equivalence relations is the following:

**Proposition 10.2.16.** Let $X \subset \mathbb{R}^n$ be an algebraic set. Then the set of all algebraic functions on $X$ is in bijection with the quotient set

$$\mathbb{R}[x_1, \ldots, x_n]/_\sim$$

where $\sim$ is the equivalence relation declaring two polynomials $g$ and $h$ to be equivalent if $(g - h)|_X$ is zero.

The above proposition says that we can think of the set of all algebraic functions on $X \subset \mathbb{R}^n$ as a *quotient* of the set of all polynomial functions on $\mathbb{R}^n$. We will defer its proof until we state a more useful version in Proposition 10.6.2.

## 10.3 Using ideals to define quotient rings

So, we have seen that the set of all algebraic functions on an algebraic set $X \subset \mathbb{R}^n$ can be written as a quotient of the polynomial ring $\mathbb{R}[x_1, \ldots, x_n]$. But we know more: The set of algebraic functions is itself a commutative ring (because we can add and multiply functions). There are two special things going on at once: We witness a quotient set, and a ring structure on that quotient set. It turns out that there is a general setting under which quotient sets of rings can be given ring structures—when we "mod out by an ideal."

**Notation 10.3.1.** Let $R$ be a commutative ring and $I \subset R$ an ideal (Definition 9.6.1). Then the set

$$R/I$$

is defined to be the quotient set of $R$ with respect to the following equivalence relation:

$$r \sim s \iff \text{there exists some } k \in I \text{ for which } r = k + s.$$

Equivalently,

$$r \sim s \iff r - s \in I.$$

**Example 10.3.2.** Let's take the example of $R = \mathbb{R}[x_1, \ldots, x_n]$, and $I = I(X)$ for some algebraic subset $X \subset \mathbb{R}^n$. Then the equivalence relation defining $R/I$ says that we identify two functions $g, h \in \mathbb{R}[x_1, \ldots, x_n]$ precisely when $g = k + h$ for some $k \in I(X)$. In other words, $g \sim h$ precisely when $g - h = k$, where $k$ is a function that vanishes on $X$. Equivalently, $g \sim h$ precisely when they restrict to the same function on $X$.

So in this example that we care about, $R/I$ is precisely the set of algebraic functions on $X$ (Proposition 10.2.16).

The following theorem is one explanation—without using the notion of "functions"—that we witness a ring structure on this quotient set.

**Theorem 10.3.3** ($R/I$ is a ring)**.** Let $R$ be a commutative ring and $I$ an ideal of $R$. Then the operations

$$[r] + [s] := [r + s]$$

and

$$[r] \cdot [s] := [r \cdot s]$$

are well-defined, and define a ring structure on $R/I$.

**Remark 10.3.4** (What it means to be well-defined)**.** Let's remember what it means for something to be "well-defined." This is a term that is often used when is trying to define a function $h : X/_\sim \to Y$ where the domain is a quotient set.

Typically, when people define functions from $X/_\sim$ to some codomain, they will write a formula like $h([x]) = \ldots$. In particular, while $h$ is supposed to depend only on elements of $X/_\sim$ (i.e., on equivalence classes) often, the formula/description of $h$ will involve elements of $X$ instead (i.e., representatives of equivalence classes). As we have discussed, an equivalence class $[x] \in X/_\sim$ may have many representatives aside from $x$. So if one writes a formula for $h([x])$ that depends on the particular representative $x$, then one must verify that $h([x]) = h([y])$ whenever $[x] = [y]$ (that is, whenever $y$ is related to $x$).

*Proof.* Suppose that $r \sim r'$ and $s \sim s'$. We must show that $[r+s] = [r'+s']$—that is, we must show that $r+s \sim r'+s'$. To do so, observe that $r \sim r' \iff r - r' \in I$. Likewise, we see $s - s' \in I$. Then $(r-r') + (s-s')$ is a sum of two elements in $I$. Because $I$ is an ideal, we conclude that $(r-r') + (s-s') \in I$. Rearranging this sum, we see that

$$(r+s) - (r'+s') \in I$$

showing that indeed $[r+s] = [r'+s']$.

Now let us show that multiplication is also well-defined. We note that

$$rs - r's' = rs - rs' + rs' - r's' = r(s-s') + (r-r')s'.$$

Because $s \sim s'$, we know that $s - s' \in I$; and because $I$ is an ideal (hence closed under scaling) we observe that $r(s-s') \in I$ as well. Similar reasoning shows that $(r-r')s' \in I$. Again using that $I$ is an ideal (hence closed under addition) we conclude that $r(s-s') + (r-r')s' \in I$. This shows $rs - r's' \in I$, so that $rs \sim r's'$. This proves that $[rs] = [r's']$, hence that the multiplication operation $[r][s] = [rrs]$ is well-defined.

We leave the verification of the ring axioms to the reader. For the record, we will point out that [1] is the multiplicative identity, [0] is the additive identity, and $[-x] = -[x]$. □

## 10.4 Summary of algebraic geometry so far

Let us recap what all of this algebra is for.

First, we saw that every algebraic subset $X \subset \mathbb{R}^n$ defines an ideal $I(X) \subset \mathbb{R}[x_1, \ldots, x_n]$. Concretely, every $X$ gives an ideal called "the set of all polynomials that vanish along $X$."

Then, we just saw an even stronger connection: "The set of all algebraic functions on $X$" is in bijection with "the quotient of $\mathbb{R}[x_1, \ldots, x_n]$ by $I(X)$."

Thus, the idea of "ideal" and of "quotient ring" were instrumental in elevating the first correspondence to the second—where we not only have some vague back-and-forth between sets and ideals, but where this back-and-forth allows us to completely recover all algebraic functions on algebraic subsets.

As it turns out, there is a deep philosophy in math: "Understanding all functions on a space" is the same thing as understanding the space itself. So, while a deep exploration of this requires coursework typically done in a Ph.D. program, let me just tease your curiosities and say that we have reduced the study of algebraic sets to the study of ideals and quotients by ideals.

As a spectacular application of the idea that "understanding functions on a space" is enough to understand a space, it turns out that *if two rings are equivalent, then the spaces they describe are equivalent.* The technical statement is that if $X$ and $Y$ have *isomorphic* rings of algebraic functions, then they are isomorphic as algebraic sets, meaning that their geometries are indistinguishable from the perspective of polynomial functions. We will see the notion of ring isomorphism soon enough.

## 10.5 $\mathbb{Z}/n\mathbb{Z}$

Matrix rings and polynomial rings are interesting. The ring $\mathbb{Z}/n\mathbb{Z}$ is interesting in a completely different way.

**Proposition 10.5.1.** Let $n$ be any integer, and let $n\mathbb{Z} \subset \mathbb{Z}$ be the ideal of all integers divisible by $n$. Then the quotient ring

$$\mathbb{Z}/n\mathbb{Z}$$

is a ring with $n$ elements. Moreover, addition and multiplication are computed in this ring using modular arithmetic:

$$[a] + [b] = [a + b \text{ modulo } n], \qquad [a][b] = [ab \text{ modulo } n],$$

*Proof.* Let $a$ be an integer. Then, by the division algorithm, we know that $a$ may be written as

$$a = a'n + r \tag{10.5.0.1}$$

where $a'$ is an integer and $r$ is some integer between 0 and $n-1$, inclusive. Indeed, $r$ is the remainder one obtains when computing the division $a \div n$. Moreover, by demanding that $0 \leq r \leq n-1$, the number $a'$ is unique given $a$. (For example, if $n = 7$, we have:

$$\begin{aligned} 13 &= 1 \cdot 7 + 6 \\ 52 &= 7 \cdot 7 + 3 \\ 14 &= 2 \cdot 7 + 0 \\ -36 &= -6 \cdot 7 + 6 \\ -1 &= -1 \cdot 7 + 6 \end{aligned}$$

and so forth.) By definition of the ideal $n\mathbb{Z}$, we see then that for any integer $a$, there is some integer $r$ with $0 \leq r \leq n-1$ for which $a - r \in n\mathbb{Z}$. In other words, any element of $\mathbb{Z}$ is related (by the equivalence relation defined by $n\mathbb{Z}$) to an integer between 0 and n-1. On the other hand, if two distinct numbers are between 0 and n-1, their difference cannot be a multiple of $n$ for size reasons; so the map

$$\mathbb{Z}/n\mathbb{Z} \to \{0, 1, \ldots, n-1\}, \qquad [a] \mapsto r$$

(where $r$ is the number appearing in (10.5.0.1)) gives a bijection between $\mathbb{Z}/n\mathbb{Z}$ and the set $\{0, \ldots, n-1\}$. (An inverse is given by $r \mapsto [r]$.) This proves the first claim.

By definition of addition in a quotient ring, we know that $[a]+[b] = [a+b]$. On the other hand, by the above bijection, we know that $[a+b]$ is equivalent to the remainder $r$ one obtains when computing $(a+b) \div n$; this is the definition of $a+b$ modulo $r$, so the claim follows.

Likewise for the claim about multiplication. □

**Example 10.5.2.** Let $n = 5$ and consider the ring $\mathbb{Z}/5\mathbb{Z}$. Then, as usual, let 1 denote the multiplicative identity. (This is given by the element [1], confusingly enough.) Likewise, we let 0 denote the additive identity (given by [0]). Then you can check that

$$1 + 1 + 1 + 1 + 1 = 0.$$

Isn't that strange? From this, you can conclude that $-1 = 4$, and that $1 = -4$.

Likewise, in $\mathbb{Z}/2\mathbb{Z}$, we have the wonderful formula $1 + 1 = 0$. In other words, $1 = -1$.

If you have not seen this before, this is probably the first time in your life that you have encountered a setting in which "add 1 to itself a bunch of times" is an operation that can result in 0. Indeed, you have to add 1 to itself the correct number of times to output 0. (For example, in $\mathbb{Z}/2\mathbb{Z}$, you must add an even number of 1's to obtain 0.)

**Remark 10.5.3.** By extending the analogies from Section 10.4, one might wonder if there is some "geometry" to $\mathbb{Z}$, and the fact that $\mathbb{Z}$ has ideals.

Amazingly, there is indeed a way in which one can think of the ring $\mathbb{Z}$ as a ring of functions on some mysterious space. This space goes by the uninformative name of $\mathrm{Spec}(\mathbb{Z})$, otherwise known as the *Zariski spectrum* of $\mathbb{Z}$. Moreover, there is a way to think of prime numbers as "points" of this space, and of arbitrary ideals as unions of points in this space.

In truth, much of this thinking is purely by analogy, but the fact that we can begin to think of integers as a ring of functions on some space has guided a huge amount of modern number theory. (How powerful would it be if we don't only think of $\mathbb{Z}$ as a bunch of numbers, but as encoding some *geometry*?)

## 10.6 Homomorphisms out of quotient rings

For various reasons, we'll want to construct ring homomorphisms. And it turns out that quotient rings have a very nice "universal property"–i.e., a very nice way to construction functions.

**Theorem 10.6.1** (Universal property of quotient rings)**.** Suppose that $f : R \to S$ is a ring homomorphism. Then the formula

$$f'([r]) = f(r)$$

defines a ring homomorphism $f' : R/I \to S$ if and only if $x \in I \implies f(x) = 0$.

More is true: The set of ring homomoprhisms from $R/I$ to $S$ is in bijection with the set of ring homomorphisms $R \to S$ sending elements of $I$ to zero.

Fix an algebraic set $X \subset \mathbb{R}^n$. Recall that, by definition, $I(X)$ is the set of all functions in $\mathbb{R}[x_1, \ldots, x_n]$ which are sent to 0 under the restriction map (Remark 9.5.3). Thus, we have the following, more useful, reformulation of Proposition 10.2.16:

**Proposition 10.6.2.** The restriction map

$$\mathbb{R}[x_1, \ldots, x_n] \to \mathcal{O}_X(X)$$

induces a bijection

$$\mathbb{R}[x_1, \ldots, x_n]/I \to \mathcal{O}_X(X)$$

**Remark 10.6.3.** Why do I say that Proposition 10.6.2 is more useful than Proposition 10.2.16? It is because Proposition 10.6.2 actually tells us where the bijection comes from. Indeed, it is far more useful to know *what bijections* we may construct between two sets, rather than just the fact that two sets may be abstractly in bijection.

## 10.7 Ring isomorphisms

In general, "isomorphism" is a term that now refers to a function that exhibit when two things are equivalent in an appropriate sense. For sets, a set isomorphism is the same thing as a bijection. This is because for sets, the most important property is just the size of a set, and bijections exhibit a way in which two sets have the same size.

For rings, we have the following:

**Definition 10.7.1.** Let $R$ and $S$ be rings. A *ring isomorphism* is a function $R \to S$ which is (i) a ring homomorphism, and (ii) a bijection.

**Remark 10.7.2.** Let $f : R \to S$ be a ring isomorphism. Because $f$ is a bijection, $f$ admits an inverse $g : S \to R$. One can prove that $g$ is also a ring isomorphism. (This shows that the relation $R \sim S$ of rings being isomorphic is symmetric.)

Further, suppose $f : R \to S$ and $h : S \to T$ are two ring isomorphisms. Then $h \circ f$ is also a ring isomorphism. (This shows that the relation of rings being isomorphic is transitive.)

### 10.7.1 A useful criterion for when a ring homomorphism is an injection

We'll practice showing that certain ring homomorphisms are isomorphisms. For this, we'll want a tool for showing that ring homomorphisms are injections.

**Proposition 10.7.3.** Let $f : R \to S$ be a ring homomorphism. Then $f$ is an injection if and only if $0 \in R$ is the only element sent to $0 \in S$ under $f$.

*Proof.* Assume $f$ is an injection. Then if $f(x)$ and $f(y)$ both equal 0, we conclude $x = y$ by definition of injection.

In the other direction: Suppose that whenever $f(x) = 0$, then $x = 0$. We must show that $f$ is an injection. So suppose $f(x) = f(y)$—meaning $f(x) - f(y) = 0 \in S$. Because $f$ is a ring homomorphism, we conclude that $f(x - y) = 0$. By assumption, we conclude that $x - y = 0 \in R$. Therefore $x = y$. This shows $f$ is an injection. □

## 10.8 Exercises

**Exercise 10.8.1.** An ideal $I \subset R$ is called *prime* if: When $xy \in I$, at least one of $x$ or $y$ is in $I$.

Let $n$ be a positive integer. Show that the ideal $n\mathbb{Z} \subset \mathbb{Z}$ is prime if and only if $n$ is a prime number.

**Exercise 10.8.2.** Compute the following in $\mathbb{Z}/22\mathbb{Z}$. Write your answer in the form $[r]$, where $r$ is a number between 0 and 21, inclusive.

(a) $[7] + [56]$.

(b) $[56] + [56]$.

(c) $[2] \cdot [56]$.

(d) $[7] \cdot [56]$.

(e) $[56]^4$.

**Exercise 10.8.3.** Compute the following in $\mathbb{Z}/5\mathbb{Z}$. Write your answer in the form $[r]$, where $r$ is a number between 0 and 4, inclusive.

(a) $[1] \cdot [1]$.

(b) $[2] \cdot [2]$.

(c) $[56]^4$.

(d) $[-1] + [1]$.

(e) $[2] + [3]$.

(f) $[-3] + [-2]$.

**Exercise 10.8.4.** Answer the following questions about the ring $\mathbb{Z}/5\mathbb{Z}$:

(a) Does $-1$ (that is, the additive inverse of the multiplicative identity) have a square root? In other words, is there an element $x$ of $\mathbb{Z}/7\mathbb{Z}$ so that $x^2 = -1$?

(b) Does 2 have a square root?

(c) Suppose that $x \in \mathbb{Z}/7\mathbb{Z}$ is non-zero. Does $x$ have a multiplicative inverse?

**Exercise 10.8.5.** A commutative ring is called a *field* if $0 \neq 1$, and if every non-zero element admits a multiplicative inverse.

(a) Show that every field is an integral domain.

(b) Let $p$ be a prime number. Show that $\mathbb{Z}/p\mathbb{Z}$ is a field. (Hint: Euclidean algorithm—see Exercise 9.9.2.)

(c) Let $n$ be an integer for which $\mathbb{Z}/n\mathbb{Z}$ is an integral domain. (Definition 7.3.23.) Prove that $n$ must be prime, and in particular, $\mathbb{Z}/n\mathbb{Z}$ must be a field.

## 10.9 Extra Credit

**Definition 10.9.1.** Let $R$ and $S$ be commutative rings. Then the *direct product* of $R$ and $S$ is the set $R \times S$ with the following addition and multiplication:

$$(r, s) + (r', s') = (r + r', s + s'), \qquad (r, s) \cdot (r', s') = (rr', ss').$$

You do not need to prove that $R \times S$ is a ring, but note that the multiplicative identity is the element $(1_R, 1_S)$.

Suppose that $X \subset \mathbb{R}^n$ and $Y \subset \mathbb{R}^n$ are disjoint subsets, meaning that $X \cap Y = \emptyset$. We let $X \coprod Y$ denote their union. Exhibit a bijection

$$\mathcal{O}_{X \coprod Y}(X \coprod Y) \cong \mathcal{O}_X(X) \times \mathcal{O}_Y(Y).$$

**Remark 10.9.2.** This is part of building up our dictionary for passing between geometry (of algebraic subsets $X \subset \mathbb{R}^n$) and algebra:

$$\begin{aligned} \text{Algebraic subsets } X &\leftrightarrow \text{Rings } \mathcal{O}_X(X) \\ \text{Disjoint unions of sets} &\leftrightarrow \text{Direct products of rings} \\ \text{Subsets} &\leftrightarrow \text{Quotient rings} \end{aligned}$$