
Relations

In mathematics there are endless ways that two entities can be related to each other. Consider the following mathematical statements.

$$\begin{array}{cccccccc}
 5 < 10 & 5 \leq 5 & 6 = \frac{30}{5} & 5 \mid 80 & 7 > 4 & x \neq y & 8 \nmid 3 \\
 a \equiv b \pmod{n} & 6 \in \mathbb{Z} & X \subseteq Y & \pi \approx 3.14 & 0 \geq -1 & \sqrt{2} \notin \mathbb{Z} & \mathbb{Z} \not\subseteq \mathbb{N}
 \end{array}$$

In each case two entities appear on either side of a symbol, and we interpret the symbol as expressing some relationship between the two entities. Symbols such as $<$, \leq , $=$, \mid , \neq , $>$, \in and \subset , etc., are called *relations* because they convey relationships among things.

Relations are significant. In fact, you would have to admit that there would be precious little left of mathematics if we took away all the relations. Therefore it is important to have a firm understanding of relations, and this chapter is intended to develop that understanding.

Rather than focusing on each relation individually (an impossible task anyway since there are infinitely many different relations) we will develop a general theory that encompasses *all* relations. Understanding this general theory will give us the conceptual framework and language needed to understand and discuss any specific relation.

Before stating the theoretical definition of a relation, let's look at a motivational example. This example will lead us naturally to our definition.

Consider the set $A = \{1, 2, 3, 4, 5\}$. (There's nothing special about this particular set; any set of numbers would do for this example.) Elements of A can be compared to each other by the symbol " $<$." For example, $1 < 4$, $2 < 3$, $2 < 4$, and so on. You have no trouble understanding this because the notion of numeric order is so ingrained. But imagine you had to explain it to an idiot savant, one with an obsession for detail but absolutely no understanding of the meaning of (or relationships between) integers. You might consider writing down for your student the following set:

$$R = \{(1, 2), (1, 3), (1, 4), (1, 5), (2, 3), (2, 4), (2, 5), (3, 4), (3, 5), (4, 5)\}$$

The set R encodes the meaning of the $<$ relation for elements in A . An ordered pair (a, b) appears in the set if and only if $a < b$. If asked whether or not it is true that $3 < 4$, your student could look through R until he found the ordered pair $(3, 4)$; then he would know $3 < 4$ is true. If asked about $5 < 2$, he would see that $(5, 2)$ *does not* appear in R , so $5 \not< 2$. The set R , which is a subset of $A \times A$, completely describes the relation $<$ for A .

Though it may seem simple-minded at first, this is exactly the idea we will use for our main definition. This definition is general enough to describe not just the relation $<$ for the set $A = \{1, 2, 3, 4, 5\}$, but *any* relation for *any* set A .

Definition 11.1 A **relation** on a set A is a subset $R \subseteq A \times A$. We often abbreviate the statement $(x, y) \in R$ as xRy . The statement $(x, y) \notin R$ is abbreviated as $x \not R y$.

Notice that a relation is a set, so we can use what we know about sets to understand and explore relations. But before getting deeper into the theory of relations, let's look at some examples of Definition 11.1.

Example 11.1 Let $A = \{1, 2, 3, 4\}$, and consider the following set:

$$R = \{(1, 1), (2, 1), (2, 2), (3, 3), (3, 2), (3, 1), (4, 4), (4, 3), (4, 2), (4, 1)\} \subseteq A \times A$$

The set R is a relation on A , by Definition 11.1. Since $(1, 1) \in R$, we have $1R1$. Similarly $2R1$ and $2R2$, and so on. However notice that (for example) $(3, 4) \notin R$, so $3 \not R 4$. Observe that R is the familiar relation \geq for the set A .

Chapter 1 proclaimed that all of mathematics can be described with sets. Just look at how successful this program has been! The greater-than relation is now a set R . (We might even express this in the rather cryptic form $\geq = R$.)

Example 11.2 Let $A = \{1, 2, 3, 4\}$, and consider the following set:

$$S = \{(1, 1), (1, 3), (3, 1), (3, 3), (2, 2), (2, 4), (4, 2), (4, 4)\} \subseteq A \times A$$

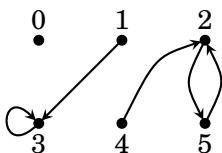
Here we have $1S1$, $1S3$, $4S2$, etc., but $3 \not S 4$ and $2 \not S 1$. What does S mean? Think of it as meaning "has the same parity as." Thus $1S1$ reads "1 has the same parity as 1," and $4S2$ reads "4 has the same parity as 2."

Example 11.3 Let $B = \{0, 1, 2, 3, 4, 5\}$, and consider the following set:

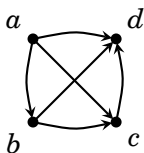
$$U = \{(1, 3), (3, 3), (5, 2), (2, 5), (4, 2)\} \subseteq B \times B$$

Then U is a relation on B because $U \subseteq B \times B$. You may be hard-pressed to invent any “meaning” for this particular relation. A relation does not have to have any meaning. Any random subset of $B \times B$ is a relation on B , whether or not it describes anything familiar.

Some relations can be described with pictures. For example, we can depict the above relation U on B by drawing points labeled by elements of B . The statement $(x, y) \in U$ is then represented by an arrow pointing from x to y , a graphic symbol meaning “ x relates to y .” Here’s a picture of U :



The next picture illustrates the relation R on the set $A = \{a, b, c, d\}$, where xRy means x comes before y in the alphabet. According to Definition 11.1, as a set this relation is $R = \{(a, b), (a, c), (a, d), (b, c), (b, d), (c, d)\}$. You may feel that the picture conveys the relation better than the set does. They are two different ways of expressing the same thing. In some instances pictures are more convenient than sets for discussing relations.



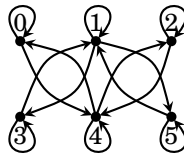
Although pictures can help us visualize relations, they do have their limitations. If A and R were infinite, then the diagram would be impossible to draw, but the set R might be easily expressed in set-builder notation. For instance here is a relation that is too big to be described by a picture.

Example 11.4 Consider the set $R = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : x - y \in \mathbb{N}\} \subseteq \mathbb{Z} \times \mathbb{Z}$. This is the $>$ relation on the set $A = \mathbb{Z}$. It is infinite because there are infinitely many ways to have $x > y$ where x and y are integers.

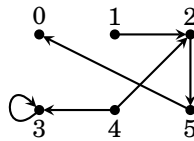
Example 11.5 The set $R = \{(x, x) : x \in \mathbb{R}\} \subseteq \mathbb{R} \times \mathbb{R}$ is the relation $=$ on the set \mathbb{R} , because xRy means the same thing as $x = y$. Thus R is a set that expresses the notion of equality of real numbers.

Exercises for Section 11.0

- Let $A = \{0, 1, 2, 3, 4, 5\}$. Write out the relation R that expresses $>$ on A . Then illustrate it with a diagram.
- Let $A = \{1, 2, 3, 4, 5, 6\}$. Write out the relation R that expresses $|$ (divides) on A . Then illustrate it with a diagram.
- Let $A = \{0, 1, 2, 3, 4, 5\}$. Write out the relation R that expresses \geq on A . Then illustrate it with a diagram.
- The following diagram represents a relation R on a set A . Write the sets A and R .



- The following diagram represents a relation R on a set A . Write the sets A and R .



- Congruence modulo 5 is a relation on the set $A = \mathbb{Z}$. In this relation xRy means $x \equiv y \pmod{5}$. Write out the set R in set-builder notation.
 - Write the relation $<$ on the set $A = \mathbb{Z}$ as a subset R of $\mathbb{Z} \times \mathbb{Z}$. This is an infinite set, so you will have to use set-builder notation.
 - Let $A = \{1, 2, 3, 4, 5, 6\}$. Observe that $\emptyset \subseteq A \times A$, so $R = \emptyset$ is a relation on A . Draw a diagram for this relation.
 - Let $A = \{1, 2, 3, 4, 5, 6\}$. How many different relations are there on the set A ?
-

11.1 Properties of Relations

Some relations have special properties that other relations don't have. For example, the relation \leq on \mathbb{Z} has the property that $x \leq x$ for every $x \in \mathbb{Z}$, but the relation $<$ on \mathbb{Z} does not have this property, for $x < x$ is never true. The next definition lays out three particularly significant properties that relations may have.

Definition 11.2 Suppose R is a relation on a set A .

1. Relation R is **reflexive** if xRx for every $x \in A$.
(That is, R is reflexive if $\forall x \in A, xRx$.)
2. Relation R is **symmetric** if xRy implies yRx for all $x, y \in A$.
(That is, R is symmetric if $\forall x, y \in A, xRy \Rightarrow yRx$.)
3. Relation R is **transitive** if whenever xRy and yRz , then also xRz .
(That is, R is transitive if $\forall x, y, z \in A, ((xRy) \wedge (yRz)) \Rightarrow xRz$.)

To illustrate this, let's consider the set $A = \mathbb{Z}$. Examples of reflexive relations on \mathbb{Z} include \leq , $=$, and $|$, for $x \leq x$, $x = x$ and $x|x$ are all true for any $x \in \mathbb{Z}$. On the other hand, $>$, $<$, \neq and \nmid are not reflexive for none of the statements $x < x$, $x > x$, $x \neq x$ and $x \nmid x$ is true.

The relation \neq is symmetric, for if $x \neq y$, then surely $y \neq x$ also. Also, the relation $=$ is symmetric because $x = y$ always implies $y = x$.

The relation \leq is **not** symmetric, as $x \leq y$ does not necessarily imply $y \leq x$. For instance $5 \leq 6$ is true but $6 \leq 5$ is false. Notice that $(x \leq y) \Rightarrow (y \leq x)$ is true for some x and y (for example, it is true when $x = 2$ and $y = 2$) but still \leq is not symmetric because it is not the case that $(x \leq y) \Rightarrow (y \leq x)$ is true for *all* integers x and y .

The relation \leq is transitive because whenever $x \leq y$ and $y \leq z$, it also is true that $x \leq z$. Likewise $<$, \geq , $>$ and $=$ are all transitive. Examine the following table and be sure you understand why it is labeled as it is.

Relations on \mathbb{Z} :	$<$	\leq	$=$	$ $	\nmid	\neq
Reflexive	no	yes	yes	yes	no	no
Symmetric	no	no	yes	no	no	yes
Transitive	yes	yes	yes	yes	no	no

Example 11.6 Here $A = \{b, c, d, e\}$ and R is the following relation on A :
 $R = \{(b, b), (b, c), (c, b), (c, c), (d, d), (b, d), (d, b), (c, d), (d, c)\}$.

Relation R is **not** reflexive, for although bRb , cRc and dRd , it is **not** true that eRe . For a relation to be reflexive, xRx must be true for *all* $x \in A$.

The relation R is symmetric, because whenever we have xRy , it follows that yRx too. Observe that bRc and cRb ; bRd and dRb ; dRc and cRd . If we took away the ordered pair (c, b) from R , then R would no longer be symmetric.

The relation R is transitive, but it takes some work to check it. We must check that the statement $(xRy \wedge yRz) \Rightarrow xRz$ is true for all $x, y, z \in A$. In other words, we must check that whenever xRy and yRz , then also xRz .

Notice that bRc and cRd and also bRd , so the statement $(bRc \wedge cRd) \Rightarrow bRd$ is true. Likewise, bRd , dRc and also bRc , so $(bRd \wedge dRc) \Rightarrow bRc$ is true, and so on. Moreover, note that $(bRc \wedge cRb) \Rightarrow bRb$ fits the pattern $(xRy \wedge yRz) \Rightarrow xRz$, where $x = b$, $y = c$ and $z = b$; and $(bRc \wedge cRb) \Rightarrow bRb$ is true because $(bRc \wedge cRb)$ and bRb are both true. We emphasize that for R to be transitive, it is necessary that $(xRy \wedge yRz) \Rightarrow xRz$ is true for **all** choices of x, y, z from A . Even if we took $x = b$, $y = e$ and $z = c$, then $(bRe \wedge eRc)$ is false and bRc is true, but the statement $(bRe \wedge eRc) \Rightarrow bRc$ is true. It's not much fun, but going through all the combinations, you can verify that $(xRy \wedge yRz) \Rightarrow xRz$ is true for all choices $x, y, z \in A$. (You should try at least a few of them.)

The relation R from Example 11.6 has a meaning. You can think of xRy as meaning that x and y are both consonants. Thus bRc because b and c are both consonants; but bRe because it's not true that b and e are both consonants. Once we look at it this way, it's immediately clear that R has to be transitive. If x and y are both consonants and y and z are both consonants, then surely x and z are both consonants. This illustrates a point that we will see again later in this section: Knowing the meaning of a relation can help us understand it and prove things about it.

Here is a picture of the relation from Example 11.6. Notice that we can immediately spot several properties of R that may not have been so clear from its set description. For instance, we see that R is not reflexive because it lacks a loop at e , hence eRe .

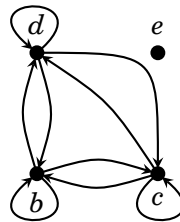




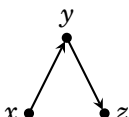





Figure 11.1. The relation R from Example 11.6

In what follows, we summarize how to spot the various properties of a relation from its diagram. Compare these with Figure 11.1.

1.	A relation is reflexive if for each point x ...		...there is a loop at x .	
2.	A relation is symmetric if whenever there is an arrow from x to y ...		...there is also an arrow from y back to x :	
3.	A relation is transitive if whenever there are arrows from x to y and y to z ...		...there is also an arrow from x to z :	
	(This also means that whenever there is an arrow from x to y and from y to x ...		...there is also a loop from x back to x .)	

Although these visual aids can be illuminating, their use is limited because many relations are too large and complex to be adequately described as diagrams. For example, it would be impossible to draw a diagram for the relation $\equiv \pmod{n}$, where $n \in \mathbb{N}$. Such a relation would best be explained in a more theoretical (and less visual) way.

In the next example we prove that $\equiv \pmod{n}$ is reflexive, symmetric and transitive. Obviously we will not glean this from a drawing. Instead we will prove it from the properties of $\equiv \pmod{n}$ and Definition 11.2. Pay special attention to this example. It illustrates how to **prove** things about relations.

Example 11.7 Prove the following proposition.

Proposition Let $n \in \mathbb{N}$. The relation $\equiv \pmod{n}$ on the set \mathbb{Z} is reflexive, symmetric and transitive.

Proof. First we will show that $\equiv \pmod{n}$ is reflexive. Take any integer $x \in \mathbb{Z}$ and observe that $n \mid 0$, so $n \mid (x - x)$. By definition of congruence modulo n , we have $x \equiv x \pmod{n}$. This shows $x \equiv x \pmod{n}$ for every $x \in \mathbb{Z}$, so $\equiv \pmod{n}$ is reflexive.

Next, we will show that $\equiv \pmod{n}$ is symmetric. For this, we must show that for all $x, y \in \mathbb{Z}$, the condition $x \equiv y \pmod{n}$ implies that $y \equiv x \pmod{n}$. We will use direct proof. Suppose $x \equiv y \pmod{n}$. Thus $n \mid (x - y)$ by definition of congruence modulo n . Then $x - y = na$ for some $a \in \mathbb{Z}$ by definition of divisibility. Multiplying both sides by -1 gives $y - x = n(-a)$. Therefore $n \mid (y - x)$, and this means $y \equiv x \pmod{n}$. We've shown that $x \equiv y \pmod{n}$ implies that $y \equiv x \pmod{n}$, and this means $\equiv \pmod{n}$ is symmetric.

Finally we will show that $\equiv \pmod{n}$ is transitive. For this we must show that if $x \equiv y \pmod{n}$ and $y \equiv z \pmod{n}$, then $x \equiv z \pmod{n}$. Again we use direct proof. Suppose $x \equiv y \pmod{n}$ and $y \equiv z \pmod{n}$. This means $n \mid (x - y)$ and $n \mid (y - z)$. Therefore there are integers a and b for which $x - y = na$ and $y - z = nb$. Adding these two equations, we obtain $x - z = na + nb$. Consequently, $x - z = n(a + b)$, so $n \mid (x - z)$, hence $x \equiv z \pmod{n}$. This completes the proof that $\equiv \pmod{n}$ is transitive.

The past three paragraphs have shown that $\equiv \pmod{n}$ is reflexive, symmetric and transitive, so the proof is complete. ■

As you continue your mathematical education, you will find that the reflexive, symmetric and transitive properties take on special significance in a variety of settings. In preparation for this, the next section explores further consequences of these relations. But first you should work some of the following exercises.

Exercises for Section 11.1

1. Consider the relation $R = \{(a, a), (b, b), (c, c), (d, d), (a, b), (b, a)\}$ on set $A = \{a, b, c, d\}$. Say whether R is reflexive, symmetric and transitive. If a property does not hold, say why.
2. Consider the relation $R = \{(a, b), (a, c), (c, c), (b, b), (c, b), (b, c)\}$ on the set $A = \{a, b, c\}$. Say whether R is reflexive, symmetric and transitive. If a property does not hold, say why.
3. Consider the relation $R = \{(a, b), (a, c), (c, b), (b, c)\}$ on the set $A = \{a, b, c\}$. Say whether R is reflexive, symmetric and transitive. If a property does not hold, say why.
4. Let $A = \{a, b, c, d\}$. Suppose R is the relation

$$R = \{(a, a), (b, b), (c, c), (d, d), (a, b), (b, a), (a, c), (c, a), \\ (a, d), (d, a), (b, c), (c, b), (b, d), (d, b), (c, d), (d, c)\}.$$

Say whether R is reflexive, symmetric and transitive. If a property does not hold, say why.

5. Consider the relation $R = \{(0,0),(\sqrt{2},0),(0,\sqrt{2}),(\sqrt{2},\sqrt{2})\}$ on \mathbb{R} . Say whether R is reflexive, symmetric and transitive. If a property does not hold, say why.
 6. Consider the relation $R = \{(x,x) : x \in \mathbb{Z}\}$ on \mathbb{Z} . Say whether R is reflexive, symmetric and transitive. If a property does not hold, say why. What familiar relation is this?
 7. There are 16 possible different relations R on the set $A = \{a,b\}$. Describe all of them. (A picture for each one will suffice, but don't forget to label the nodes.)
 8. Define a relation on \mathbb{Z} as xRy if and only if $|x-y| < 1$. Say whether R is reflexive, symmetric and transitive. If a property does not hold, say why. What familiar relation is this?
 9. Define a relation on \mathbb{Z} by declaring xRy if and only if x and y have the same parity. Say whether R is reflexive, symmetric and transitive. If a property does not hold, say why. What familiar relation is this?
 10. Suppose $A \neq \emptyset$. Since $\emptyset \subseteq A \times A$, the set $R = \emptyset$ is a relation on A . Say whether R is reflexive, symmetric and transitive. If a property does not hold, say why.
 11. Suppose $A = \{a,b,c,d\}$ and $R = \{(a,a),(b,b),(c,c),(d,d)\}$. Say whether R is reflexive, symmetric and transitive. If a property does not hold, say why.
 12. Prove that the relation $|$ (divides) on the set \mathbb{Z} is reflexive and transitive. (Use Example 11.7 as a guide if you are unsure of how to proceed.)
 13. Consider the relation $R = \{(x,y) \in \mathbb{R} \times \mathbb{R} : x - y \in \mathbb{Z}\}$ on \mathbb{R} . Prove that this relation is reflexive, symmetric and transitive.
 14. Suppose R is a symmetric and transitive relation on a set A , and there is an element $a \in A$ for which aRx for every $x \in A$. Prove that R is reflexive.
 15. Prove or disprove: If a relation is symmetric and transitive, then it is also reflexive.
 16. Define a relation R on \mathbb{Z} by declaring that xRy if and only if $x^2 \equiv y^2 \pmod{4}$. Prove that R is reflexive, symmetric and transitive.
-

11.2 Equivalence Relations

The relation $=$ on the set \mathbb{Z} (or on any set A) is reflexive, symmetric and transitive. There are many other relations that are also reflexive, symmetric and transitive. Relations which have all three of these properties occur very frequently in mathematics and often play quite significant roles. (For instance, this is certainly true of the relation $=$.) Such relations are given a special name. They are called *equivalence relations*.

Definition 11.3 A relation R on a set A is an **equivalence relation** if it is reflexive, symmetric and transitive.

As an example, Figure 11.2 illustrates four different equivalence relations R_1, R_2, R_3 and R_4 on the set $A = \{-1, 1, 2, 3, 4\}$. Each one has its own meaning, as labeled. For example, in the second row the relation R_2 literally means “has the same parity as.” So $1R_23$ means “1 has the same parity as 3,” etc.

Relation R	Diagram	Equivalence classes (see next page)
<p>“is equal to” (=)</p> <p>$R_1 = \{(-1, -1), (1, 1), (2, 2), (3, 3), (4, 4)\}$</p>		<p>$\{-1\}, \{1\},$ $\{2\}, \{3\}, \{4\}$</p>
<p>“has same parity as”</p> <p>$R_2 = \{(-1, -1), (1, 1), (2, 2), (3, 3), (4, 4),$ $(-1, 1), (1, -1), (-1, 3), (3, -1),$ $(1, 3), (3, 1), (2, 4), (4, 2)\}$</p>		<p>$\{-1, 1, 3\},$ $\{2, 4\}$</p>
<p>“has same sign as”</p> <p>$R_3 = \{(-1, -1), (1, 1), (2, 2), (3, 3), (4, 4),$ $(1, 2), (2, 1), (1, 3), (3, 1), (1, 4), (4, 1),$ $(2, 3), (3, 2), (2, 4), (4, 2), (1, 3), (3, 1)\}$</p>		<p>$\{-1\},$ $\{1, 2, 3, 4\}$</p>
<p>“has same parity and sign as”</p> <p>$R_4 = \{(-1, -1), (1, 1), (2, 2), (3, 3), (4, 4),$ $(1, 3), (3, 1), (2, 4), (4, 2)\}$</p>		<p>$\{-1\}, \{1, 3\},$ $\{2, 4\}$</p>

Figure 11.2. Examples of equivalence relations on the set $A = \{-1, 1, 2, 3, 4\}$

The diagrams in Figure 11.2 make it easy to check that each relation is reflexive, symmetric and transitive, i.e. that each is an equivalence relation. As you can see from these examples, equivalence relations on a set tend to express some measure of “sameness” among the elements of the set, whether it is true equality or something weaker (like having the same parity).

It's time to introduce an important definition. Whenever you have an equivalence relation R on a set A , it divides A into subsets called *equivalence classes*. Here is the definition.

Definition 11.4 Suppose R is an equivalence relation on a set A . Given any element $a \in A$, the **equivalence class containing a** is the subset $\{x \in A : xRa\}$ of A consisting of all the elements of A that relate to a . This set is denoted as $[a]$. Thus the equivalence class containing a is the set $[a] = \{x \in A : xRa\}$.

Example 11.8 Consider the relation R_1 in Figure 11.2. The equivalence class containing 2 is the set $[2] = \{x \in A : xR_1 2\}$. Since in this relation 2 relates to itself and nothing else, we have $[2] = \{2\}$. Other equivalence classes for R_1 are $[-1] = \{-1\}$, $[1] = \{1\}$, $[3] = \{3\}$ and $[4] = \{4\}$. Thus this relation has five separate equivalence classes.

Example 11.9 Consider the relation R_2 in Figure 11.2. The equivalence class containing 2 is the set $[2] = \{x \in A : xR_2 2\}$. Since 2 relates only to itself and 4, we have $[2] = \{2, 4\}$. Observe that we also have $[4] = \{x \in A : xR_2 4\} = \{2, 4\}$, so $[2] = [4]$. Another equivalence class for R_2 is $[1] = \{x \in A : xR_2 1\} = \{-1, 1, 3\}$. In addition, note that $[1] = [-1] = [3] = \{-1, 1, 3\}$. Thus this relation has just two equivalence classes.

Example 11.10 The relation R_4 in Figure 11.2 has three equivalence classes. They are $[-1] = \{-1\}$, and $[1] = [3] = \{1, 3\}$, and $[2] = [4] = \{2, 4\}$.

Don't be misled by Figure 11.2. It's important to realize that not every equivalence relation can be drawn as a diagram involving nodes and arrows. Even the simple relation $R = \{(x, x) : x \in \mathbb{R}\}$ which expresses equality in the set \mathbb{R} is too big to be drawn. Its picture would involve a point for every real number, and a loop at each point. Clearly that's too many points and loops to draw.

We close this section with several other examples of equivalence relations on infinite sets.

Example 11.11 Let P be the set of all polynomials. Define a relation R on P as follows. Given two polynomials $f(x), g(x) \in P$, let $f(x)Rg(x)$ mean that $f(x)$ and $g(x)$ have the same degree. Thus, for example $(x^2 + 3x - 4)R(3x^2 - 2)$, and $(x^3 + 3x^2 - 4)R(3x^2 - 2)$. It takes just a quick mental check to see that R is an equivalence relation. (Do it.) It's easy to describe the equivalence classes of R . For example $[3x^2 + 2]$ is the set of all polynomials that have the same degree as $3x^2 + 2$, that is the set of all polynomials of degree 2. We can write this as $[3x^2 + 2] = \{ax^2 + bx + c : a, b, c \in \mathbb{R}, a \neq 0\}$.

Recall that in Example 11.7 we proved that for a given $n \in \mathbb{N}$ the relation $\equiv (\text{mod } n)$ is reflexive, symmetric and transitive. Thus, in our new parlance, $\equiv (\text{mod } n)$ is an equivalence relation on \mathbb{Z} . Consider the case $n = 3$. Let's find the equivalence classes of the equivalence relation $\equiv (\text{mod } 3)$. The equivalence class containing 0 seems like a reasonable place to start. Observe that

$$\begin{aligned} [0] &= \{x \in \mathbb{Z} : x \equiv 0 (\text{mod } 3)\} \\ &= \{x \in \mathbb{Z} : 3|(x-0)\} = \{x \in \mathbb{Z} : 3|x\} = \{\dots, -3, 0, 3, 6, 9, \dots\}. \end{aligned}$$

Thus the class $[0]$ consists of all the multiples of 3. (Or, said differently, $[0]$ consists of all integers that have a remainder of 0 when divided by 3). Note that $[0] = [3] = [6] = [9]$, etc. The number 1 does not show up in the set $[0]$ so let's next look at the equivalence class $[1]$:

$$[1] = \{x \in \mathbb{Z} : x \equiv 1 (\text{mod } 3)\} = \{x \in \mathbb{Z} : 3|(x-1)\} = \{\dots, -5, -2, 1, 4, 7, 10, \dots\}$$

The equivalence class $[1]$ consists of all integers that give a remainder of 1 when divided by 3. The number 2 is in neither of the sets $[0]$ or $[1]$, so we next look at the equivalence class $[2]$.

$$[2] = \{x \in \mathbb{Z} : x \equiv 2 (\text{mod } 3)\} = \{x \in \mathbb{Z} : 3|(x-2)\} = \{\dots, -4, -1, 2, 5, 8, 11, \dots\}$$

The equivalence class $[2]$ consists of all integers that give a remainder of 2 when divided by 3. Observe that any integer is in one of the sets $[0]$, $[1]$ or $[2]$, so we have listed all of the equivalence classes. Thus $\equiv (\text{mod } 3)$ has exactly three equivalence classes, as described above.

Similarly, you can show that the equivalence relation $\equiv (\text{mod } n)$ has n equivalence classes $[0], [1], [2], \dots, [n-1]$.

Exercises for Section 11.2

1. Let $A = \{1, 2, 3, 4, 5, 6\}$, and consider the following equivalence relation on A :

$$\begin{aligned} R &= \{(1, 1), (2, 2), (3, 3), (4, 4), (5, 5), (6, 6), (2, 3), \\ &\quad (3, 2), (4, 5), (5, 4), (4, 6), (6, 4), (5, 6), (6, 5)\}. \end{aligned}$$

List the equivalence classes of R .

2. Let $A = \{a, b, c, d, e\}$. Suppose R is an equivalence relation on A . Suppose R has two equivalence classes. Also aRd , bRc and eRd . Write out R as a set.

3. Let $A = \{a, b, c, d, e\}$. Suppose R is an equivalence relation on A . Suppose R has three equivalence classes. Also aRd and bRc . Write out R as a set.
 4. Let $A = \{a, b, c, d, e\}$. Suppose R is an equivalence relation on A . Suppose also that aRd and bRc , eRa and cRe . How many equivalence classes does R have?
 5. There are two different equivalence relations on the set $A = \{a, b\}$. Describe them. Diagrams will suffice.
 6. There are five different equivalence relations on the set $A = \{a, b, c\}$. Describe them all. Diagrams will suffice.
 7. Define a relation R on \mathbb{Z} as xRy if and only if $3x - 5y$ is even. Prove R is an equivalence relation. Describe its equivalence classes.
 8. Define a relation R on \mathbb{Z} as xRy if and only if $x^2 + y^2$ is even. Prove R is an equivalence relation. Describe its equivalence classes.
 9. Define a relation R on \mathbb{Z} as xRy if and only if $4 \mid (x+3y)$. Prove R is an equivalence relation. Describe its equivalence classes.
 10. Suppose R and S are two equivalence relations on a set A . Prove that $R \cap S$ is also an equivalence relation. (For an example of this, look at Figure 11.2. Observe that for the equivalence relations R_2, R_3 and R_4 , we have $R_2 \cap R_3 = R_4$.)
 11. Prove or disprove: If R is an equivalence relation on an infinite set A , then R has infinitely many equivalence classes.
 12. Prove or disprove: If R and S are two equivalence relations on a set A , then $R \cup S$ is also an equivalence relation on A .
-

11.3 Equivalence Classes and Partitions

This section collects several properties of equivalence classes.

Our first result proves that $[a] = [b]$ if and only if aRb . This is useful because it assures us that whenever we are in a situation where $[a] = [b]$, we also have aRb , and vice versa. Being able to switch back and forth between these two pieces of information can be helpful in a variety of situations, and you may find yourself using this result a lot. Be sure to notice that the proof uses all three properties (reflexive, symmetric and transitive) of equivalence relations. Notice also that we have to use some Chapter 8 techniques in dealing with the sets $[a]$ and $[b]$.

Theorem 11.1 Suppose R is an equivalence relation on a set A . Suppose also that $a, b \in A$. Then $[a] = [b]$ if and only if aRb .

Proof. Suppose $[a] = [b]$. Note that $a \in [a]$, because $[a] = \{x \in A : xRa\}$ and aRa by the reflexive property of R . But since $[a] = [b]$, we also have

$a \in [b] = \{x \in A : xRb\}$. Then since a belongs to the set $\{x \in A : xRb\}$, it follows that aRb . This completes the first part of the if-and-only-if proof.

Conversely, suppose aRb . We need to show $[a] = [b]$. This will be accomplished by showing $[a] \subseteq [b]$ and $[b] \subseteq [a]$.

First we show $[a] \subseteq [b]$. Suppose $c \in [a]$. By definition of $[a]$ (recall $[a] = \{x \in A : xRa\}$), it follows that cRa . Now we have cRa and aRb , and since R is transitive we obtain cRb . But cRb implies $c \in \{x \in A : xRb\} = [b]$. This demonstrates that $c \in [a]$ implies $c \in [b]$, so $[a] \subseteq [b]$.

Next we show $[b] \subseteq [a]$. Suppose $c \in [b]$. By definition of $[b]$ (recall $[b] = \{x \in A : xRb\}$), it follows that cRb . Remember that we are assuming aRb , and since R is symmetric, it follows that bRa . Now we have cRb and bRa , and since R is transitive we obtain cRa . But cRa implies $c \in \{x \in A : xRa\} = [a]$. This demonstrates that $c \in [b]$ implies $c \in [a]$, so $[b] \subseteq [a]$.

The previous two paragraphs imply that $[a] = [b]$. ■

To illustrate Theorem 11.1, recall how we worked out the equivalence classes of $\equiv \pmod{3}$ at the end of Section 11.2. We observed that $[-3] = [9] = \{\dots, -3, 0, 3, 6, 9, \dots\}$. Note that $[-3] = [9]$ and $-3 \equiv 9 \pmod{3}$, just as Theorem 11.1 predicts. The theorem assures us that this will work for any equivalence relation. In this course and beyond you may find yourself using the result of Theorem 11.1 quite often. Over time it may become natural and familiar, and you will use it automatically, without even thinking of it as a theorem.

Our next topic addresses the fact that an equivalence relation on a set A divides A into various equivalence classes. There is a special word for this kind of situation. We address it now, as you are likely to encounter it in subsequent mathematics classes.

Definition 11.5 A **partition** of a set A is a set of subsets of A , such that the union of all the subsets equals A , and the intersection of any two different subsets is \emptyset .

Example 11.12 Let $A = \{a, b, c, d\}$. One partition of A is $\{\{a, b\}, \{c\}, \{d\}\}$. This is a set of three subsets $\{a, b\}$, $\{c\}$ and $\{d\}$ of A . The union of the three subsets equals A ; the intersection of any two subsets is \emptyset .

Other partitions of A are

$$\{\{a, b\}, \{c, d\}\}, \quad \{\{a, c\}, \{b\}, \{d\}\}, \quad \{\{a\}, \{b\}, \{c\}, \{d\}\}, \quad \text{and} \quad \{\{a, b, c, d\}\},$$

to name a few. Intuitively, a partition is just a dividing up of A into pieces.

Example 11.13 Consider the equivalence relations in Figure 11.2. Each of these is a relation on the set $A = \{-1, 1, 2, 3, 4\}$. The equivalence classes of each relation are listed on the right side of the figure. Observe that, in each case, the set of equivalence classes forms a partition of A . For example, the relation R_1 yields the partition $\{\{-1\}, \{1\}, \{2\}, \{3\}, \{4\}\}$ of A . Likewise the equivalence classes of R_2 form the partition $\{\{-1, 1, 3\}, \{2, 4\}\}$.

Example 11.14 Recall that we worked out the equivalence classes of the equivalence relation $\equiv \pmod{3}$ on the set \mathbb{Z} . These equivalence classes give the following partition of \mathbb{Z} : $\{\{\dots, -3, 0, 3, 6, 9, \dots\}, \{\dots, -2, 1, 4, 7, 10, \dots\}, \{\dots, -1, 2, 5, 8, 11, \dots\}\}$. We can write it more compactly as $\{[0], [1], [2]\}$.

Our examples and experience suggest that the equivalence classes of an equivalence relation on a set form a partition of that set. This is indeed the case, and we now prove it.

Theorem 11.2 Suppose R is an equivalence relation on a set A . Then the set $\{[a] : a \in A\}$ of equivalence classes of R forms a partition of A .

Proof. To show that $\{[a] : a \in A\}$ is a partition of A we need to show two things: We need to show that the union of all the sets $[a]$ equals A , and we need to show that if $[a] \neq [b]$, then $[a] \cap [b] = \emptyset$.

Notationally, the union of all the sets $[a]$ is $\bigcup_{a \in A} [a]$, so we need to prove $\bigcup_{a \in A} [a] = A$. Suppose $x \in \bigcup_{a \in A} [a]$. This means $x \in [a]$ for some $a \in A$. Since $[a] \subseteq A$, it then follows that $x \in A$. Thus $\bigcup_{a \in A} [a] \subseteq A$. On the other hand, if $x \in A$, then $x \in [x]$, so $x \in [a]$ for some $a \in A$. Therefore $x \in \bigcup_{a \in A} [a]$, and this shows $A \subseteq \bigcup_{a \in A} [a]$. Since $\bigcup_{a \in A} [a] \subseteq A$ and $A \subseteq \bigcup_{a \in A} [a]$, it follows that $\bigcup_{a \in A} [a] = A$.

Next we need to show that if $[a] \neq [b]$ then $[a] \cap [b] = \emptyset$. Let's use contrapositive proof. Suppose it's not the case that $[a] \cap [b] = \emptyset$, so there is some element c with $c \in [a] \cap [b]$. Thus $c \in [a]$ and $c \in [b]$. Now, $c \in [a]$ means cRa , and then aRc since R is symmetric. Also $c \in [b]$ means cRb . Now we have aRc and cRb , so aRb (because R is transitive). Theorem 11.1 now implies $[a] = [b]$, so $[a] \neq [b]$ is not true. ■

Theorem 11.2 says the equivalence classes of any equivalence relation on a set A form a partition of A . Conversely, any partition of A describes an equivalence relation R where xRy if and only if x and y belong to the same set in the partition. Thus equivalence relations and partitions are really just two different ways of looking at the same thing.

Exercises for Section 11.3

1. List all the partitions of the set $A = \{a, b\}$. Compare your answer to the answer to Exercise 5 of Section 11.2.
 2. List all the partitions of the set $A = \{a, b, c\}$. Compare your answer to the answer to Exercise 6 of Section 11.2.
 3. Describe the partition of \mathbb{Z} resulting from the equivalence relation $\equiv \pmod{4}$.
-

11.4 The Integers Modulo n

Example 11.7 proved that for a given $n \in \mathbb{N}$, the relation $\equiv \pmod{n}$ is reflexive, symmetric and transitive, so it is an equivalence relation. This is a particularly significant equivalence relation in mathematics, and in the present section we deduce some of its properties.

To make matters simpler, let's pick a concrete n , say $n = 5$. Let's begin by looking at the equivalence classes of the relation $\equiv \pmod{5}$. There are five equivalence classes, as follows.

$$\begin{aligned}
 [0] &= \{x \in \mathbb{Z} : x \equiv 0 \pmod{5}\} = \{x \in \mathbb{Z} : 5 \mid (x-0)\} = \{\dots, -10, -5, 0, 5, 10, 15, \dots\} \\
 [1] &= \{x \in \mathbb{Z} : x \equiv 1 \pmod{5}\} = \{x \in \mathbb{Z} : 5 \mid (x-1)\} = \{\dots, -9, -4, 1, 6, 11, 16, \dots\} \\
 [2] &= \{x \in \mathbb{Z} : x \equiv 2 \pmod{5}\} = \{x \in \mathbb{Z} : 5 \mid (x-2)\} = \{\dots, -8, -3, 2, 7, 12, 17, \dots\} \\
 [3] &= \{x \in \mathbb{Z} : x \equiv 3 \pmod{5}\} = \{x \in \mathbb{Z} : 5 \mid (x-3)\} = \{\dots, -7, -2, 3, 8, 13, 18, \dots\} \\
 [4] &= \{x \in \mathbb{Z} : x \equiv 4 \pmod{5}\} = \{x \in \mathbb{Z} : 5 \mid (x-4)\} = \{\dots, -6, -1, 4, 9, 14, 19, \dots\}
 \end{aligned}$$

Notice how these equivalence classes form a partition of the set \mathbb{Z} . We label the five equivalence classes as $[0], [1], [2], [3]$, and $[4]$, but you know of course that there are other ways to label them. For example, $[0] = [5] = [10] = [15]$, and so on; and $[1] = [6] = [-4]$, etc. Still, for this discussion we denote the five classes as $[0], [1], [2], [3]$, and $[4]$.

These five classes form a set, which we shall denote as \mathbb{Z}_5 . Thus

$$\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$$

is a set of five sets. The interesting thing about \mathbb{Z}_5 is that even though its elements are sets (and not numbers) it is possible to add and multiply them. In fact, we can define the following rules that tell how elements of

\mathbb{Z}_5 can be added and multiplied.

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

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

For example, $[2] + [1] = [2 + 1] = [3]$, and $[2] \cdot [2] = [2 \cdot 2] = [4]$. We stress that in doing this we are adding and multiplying *sets* (more precisely equivalence classes), not numbers. We added (or multiplied) two elements of \mathbb{Z}_5 and obtained another element of \mathbb{Z}_5 .

Here is a trickier example. Observe that $[2] + [3] = [5]$. This time we added elements $[2], [3] \in \mathbb{Z}_5$, and got the element $[5] \in \mathbb{Z}_5$. That was easy, except where is our answer $[5]$ in the set $\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$? Since $[5] = [0]$, it is more appropriate to write $[2] + [3] = [0]$.

In a similar vein, $[2] \cdot [3] = [6]$ would be written as $[2] \cdot [3] = [1]$ because $[6] = [1]$. Test your skill with this by verifying the following addition and multiplication tables for \mathbb{Z}_5 .

+	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]	[0]
[2]	[2]	[3]	[4]	[0]	[1]
[3]	[3]	[4]	[0]	[1]	[2]
[4]	[4]	[0]	[1]	[2]	[3]

·	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]
[2]	[0]	[2]	[4]	[1]	[3]
[3]	[0]	[3]	[1]	[4]	[2]
[4]	[0]	[4]	[3]	[2]	[1]

We call the set $\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$ the **integers modulo 5**. As our tables suggest, \mathbb{Z}_5 is more than just a set: It is a little number system with its own addition and multiplication. In this way it is like the familiar set \mathbb{Z} which also comes equipped with an addition and a multiplication.

Of course, there is nothing special about the number 5. We can also define \mathbb{Z}_n for any natural number n . Here is the definition.

Definition 11.6 Let $n \in \mathbb{N}$. The equivalence classes of the equivalence relation $\equiv \pmod{n}$ are $[0], [1], [2], \dots, [n-1]$. The **integers modulo n** is the set $\mathbb{Z}_n = \{[0], [1], [2], \dots, [n-1]\}$. Elements of \mathbb{Z}_n can be added by the rule $[a] + [b] = [a + b]$ and multiplied by the rule $[a] \cdot [b] = [ab]$.

Given a natural number n , the set \mathbb{Z}_n is a number system containing n elements. It has many of the algebraic properties that \mathbb{Z}, \mathbb{R} and \mathbb{Q} possess.

For example, it is probably obvious to you already that elements of \mathbb{Z}_n obey the commutative laws $[a] + [b] = [b] + [a]$ and $[a] \cdot [b] = [b] \cdot [a]$. You can also verify that the distributive law $[a] \cdot ([b] + [c]) = [a] \cdot [b] + [a] \cdot [c]$ holds, as follows.

$$\begin{aligned} [a] \cdot ([b] + [c]) &= [a] \cdot [b + c] \\ &= [a(b + c)] \\ &= [ab + ac] \\ &= [ab] + [ac] \\ &= [a] \cdot [b] + [a] \cdot [c] \end{aligned}$$

The integers modulo n are significant because they more closely fit certain applications than do other number systems such as \mathbb{Z} or \mathbb{R} . If you go on to take a course in abstract algebra, then you will work extensively with \mathbb{Z}_n as well as other, more exotic, number systems. (In such a course you will also use all of the proof techniques that we have discussed, as well as the ideas of equivalence relations.)

To close this section we take up an issue that may have bothered you earlier. It has to do with our definitions of addition $[a] + [b] = [a + b]$ and multiplication $[a] \cdot [b] = [ab]$. These definitions define addition and multiplication of equivalence classes in terms of representatives a and b in the equivalence classes. Since there are many different ways to choose such representatives, we may well wonder if addition and multiplication are consistently defined. For example, suppose two people, Alice and Bob, want to multiply the elements $[2]$ and $[3]$ in \mathbb{Z}_5 . Alice does the calculation as $[2] \cdot [3] = [6] = [1]$, so her final answer is $[1]$. Bob does it differently. Since $[2] = [7]$ and $[3] = [8]$, he works out $[2] \cdot [3]$ as $[7] \cdot [8] = [56]$. Since $56 \equiv 1 \pmod{5}$, Bob's answer is $[56] = [1]$, and that agrees with Alice's answer. Will their answers always agree or did they just get lucky (with the arithmetic)?

The fact is that no matter how they do the multiplication in \mathbb{Z}_n , their answers will agree. To see why, suppose Alice and Bob want to multiply the elements $[a], [b] \in \mathbb{Z}_n$, and suppose $[a] = [a']$ and $[b] = [b']$. Alice and Bob do the multiplication as follows.

$$\begin{array}{ll} \text{Alice:} & [a] \cdot [b] = [ab] \\ \text{Bob:} & [a'] \cdot [b'] = [a'b'] \end{array}$$

We need to show that their answers agree, that is we need to show $[ab] = [a'b']$. Since $[a] = [a']$, we know by Theorem 11.1 that $a \equiv a' \pmod{n}$.

Thus $n|(a - a')$, so $a - a' = nk$ for some integer k . Likewise, as $[b] = [b']$, we know $b \equiv b' \pmod{n}$, or $n|(b - b')$, so $b - b' = n\ell$ for some integer ℓ . Thus we get $a = a' + nk$ and $b = b' + n\ell$. Therefore:

$$\begin{aligned} ab &= (a' + nk)(b' + n\ell) \\ ab &= a'b' + a'n\ell + nkb' + n^2k\ell \\ ab - a'b' &= n(a'\ell + kb' + nk\ell) \end{aligned}$$

This shows $n|(ab - a'b')$, so $ab \equiv a'b' \pmod{n}$, and from that we conclude $[ab] = [a'b']$. Consequently Alice and Bob really do get the same answer, so we can be assured that the definition of multiplication in \mathbb{Z}_n is consistent.

In one of the exercises, you will be asked to show that addition in \mathbb{Z}_n is similarly consistent.

Exercises for Section 11.4

- Write the addition and multiplication tables for \mathbb{Z}_2 .
- Write the addition and multiplication tables for \mathbb{Z}_3 .
- Write the addition and multiplication tables for \mathbb{Z}_4 .
- Write the addition and multiplication tables for \mathbb{Z}_6 .
- Suppose $[a], [b] \in \mathbb{Z}_5$ and $[a] \cdot [b] = [0]$. Is it necessarily true that either $[a] = [0]$ or $[b] = [0]$?
- Suppose $[a], [b] \in \mathbb{Z}_6$ and $[a] \cdot [b] = [0]$. Is it necessarily true that either $[a] = [0]$ or $[b] = [0]$?
- Do the following calculations in \mathbb{Z}_9 , in each case expressing your answer as $[a]$ with $0 \leq a \leq 8$.

(a) $[8] + [8]$	(b) $[24] + [11]$	(c) $[21] \cdot [15]$	(d) $[8] \cdot [8]$
-----------------	-------------------	-----------------------	---------------------
- Suppose $[a], [b] \in \mathbb{Z}_n$, and $[a] = [a']$ and $[b] = [b']$. Alice adds $[a]$ and $[b]$ as $[a] + [b] = [a + b]$. Bob adds them as $[a'] + [b'] = [a' + b']$. Show that their answers $[a + b]$ and $[a' + b']$ are the same.

11.5 Relations Between Sets

In the beginning of this chapter, we defined a relation on a set A to be a subset $R \subseteq A \times A$. This created a framework that could model any situation in which elements of A are compared to themselves. In this setting, the statement xRy has elements x and y from A on either side of the R because R compares elements from A . But there are other

relational symbols that don't work this way. Consider \in . The statement $5 \in \mathbb{Z}$ expresses a relationship between 5 and \mathbb{Z} (namely that the element 5 is in the set \mathbb{Z}) but 5 and \mathbb{Z} are not in any way naturally regarded as both elements of some set A . To overcome this difficulty, we generalize the idea of a relation on A to a *relation from A to B* .

Definition 11.7 A **relation** from a set A to a set B is a subset $R \subseteq A \times B$. We often abbreviate the statement $(x, y) \in R$ as xRy . The statement $(x, y) \notin R$ is abbreviated as $x \not R y$.

Example 11.15 Suppose $A = \{1, 2\}$ and $B = \mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$. Then $R = \{(1, \{1\}), (2, \{2\}), (1, \{1, 2\}), (2, \{1, 2\})\} \subseteq A \times B$ is a relation from A to B . Notice that we have $1R\{1\}$, $2R\{2\}$, $1R\{1, 2\}$ and $2R\{1, 2\}$. The relation R is the familiar relation \in for the set A , that is xRX means exactly the same thing as $x \in X$.

Diagrams for relations from A to B differ from diagrams for relations on A . Since there are two sets A and B in a relation from A to B , we have to draw labeled nodes for each of the two sets. Then we draw arrows from x to y whenever xRy . The following figure illustrates this for Example 11.15.

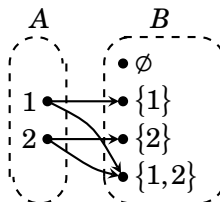


Figure 11.3. A relation from A to B

The ideas from this chapter show that any relation (whether it is a familiar one like \geq , \leq , $=$, $|$, \in or \subseteq , or a more exotic one) is really just a set. Therefore the theory of relations is a part of set theory. In the next chapter we will see that this idea touches on another important mathematical construction, namely functions. We will define a function to be a special kind of relation from one set to another, and in this context we will see that any function is really just a set.