Chapter VI

Relations

Assumptions are the termites of relationships. Henry Winkler

Studying *relationships* between objects can yield important information about the objects themselves. For the real numbers, we study inequalities; for sets, we study inclusion; for the integers, we study divisibility and congruences. All of these relationships, whether between real numbers, sets, or integers, will be seen to be special cases of the concept of a *relation* introduced in this chapter.

Because it encompasses so many different examples, the concept of a relation has very broad applicability, but this level of generality limits what we can prove. Any theorems proved about relations must be true for a wide variety of relationships. For this reason, mathematicians have singled out several types of relations for special study. Among these special relations are equivalence relations, which we will study later in this chapter, and functions, which we will study in the next chapter.

By studying special types of relations, the theorems that we can prove will be much more interesting. The relations that we study have been chosen to be widely applicable, while simultaneously providing us with a rich collection of theorems.

20 Properties of relations

20.A What is a relation?

There are many relations that occur in mathematics. For instance, $<$ on the real numbers is a relation. Inclusion, $\subseteq$, is a relation on sets. Divisibility on the natural numbers is a relation. The following definition of a relation encompasses all of these examples and others.

Definition 20.1. A *relation* is a set R of ordered pairs. Given sets A and B, we say that R is a relation from A to B, when $R \subseteq A \times B$. For arbitrary elements $a \in A$ and $b \in B$ we will write aRb to mean $(a, b) \in R$.

In the case when $A = B$, we say R is a relation on A.

This definition is very general; in fact, it is so general that many examples of relations may have no mathematical significance. Nevertheless, some relations are very important. We give a number of examples.

Example 20.2. Fix $A = \{1, 2, 3\}$ and $B = \{x, y, z\}$. Set $R = \{(1, y), (3, x)\}$. Then we have $1Ry$ and $3Rx$, but not $1Rz$ (so we write $1\not Rz$). In fact, besides 1 relating to y and 3 relating to x, no element of A relates to any element of B (under the relation R given in this example). △

Example 20.3. Fix $A = B = \mathbb{N}$, and fix $R = \{(a, b) \in \mathbb{N} \times \mathbb{N} : a - b = 2\}$. Then $3R1$ and $5R3$, but $1\not R3$ and $5\not R1$. △

Example 20.4. We can define relations on sets of words. Indeed, fix W to be the set of all words in the English language. Fix

$$R = \{(\alpha, \beta) \in W \times W : \alpha \text{ and } \beta \text{ have the same length}\}.$$

Under this relation, two words are related to each other exactly when they have the same length. Thus "tree" is related to "yaks," but "awesome" is not related to "gum." We might name this relation the "have the same length" relation. △

Sometimes we can define relations using symbols other than R. For instance:

Example 20.5. Fix $A = \{1, 2, 3, 4, 5\}$, and fix $B = \mathscr{P}(A)$. We define a relation from A to B using the following set of ordered pairs:

$$R = \{(a, X) \in A \times B : a \in X\}.$$

Since X is a set, it makes sense to ask whether a is an element of X.

In this case, if we take $a = 2$ and $X = \{1, 2, 3\}$ we see that aRX. However, with $a = 2$ and $X = \{1, 4, 5\}$, we have $a\not RX$.

Given $a \in A$ and $X \in B$, we see that aRX if and only if $a \in X$. Thus, we could have used the symbol "$\in$" instead of "R." △

The following example exhibits a construction of a relation in a way that will be important to us in later sections.

Example 20.6. Fix $A = \{1, 2, 3, 4, 5\}$. We break A up into pieces by fixing the set $S = \{\{1, 2\}, \{3, 4\}, \{5\}\}$. (There were many different ways we could have broken A into pieces; this is just one of them.) We now define a relation R on A by

$$R = \{(a, b) \in A \times A : \text{for some } X \in S, \text{ both } a \in X \text{ and } b \in X\}.$$

Let's test whether or not 1 is related to 2. Take $a = 1$ and $b = 2$. Note that a and b are both in $\{1, 2\} \in S$. Hence, there is some X (namely $X = \{1, 2\}$) that is an element of S such that $a \in X$ and $b \in X$, so we see that $1R2$.

If we take $a = 1$ and $b = 4$, there is no element $X \in S$ such that $a \in X$ and $b \in X$, so $(1, 4) \notin R$. If we work through all the possible elements of $A \times A$, we find that

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

There are many different ways to define a relation. One option is to simply list all the possible ordered pairs in R. Another option we have seen is to write R using set-builder notation. For instance, we defined the "have the same length" relation this way. Sometimes set-builder notation is too clunky, and so we express the definition of the relation in words. The following example shows how this is commonly done.

Example 20.7. Recall the relation defined in Example 20.3,

$$R = \{(a, b) \in \mathbb{N} \times \mathbb{N} : a - b = 2\}.$$

To define the same relation, we could have instead said the following:

> Fix R to be a relation on $\mathbb{N}$, defined by aRb if $a - b = 2$.

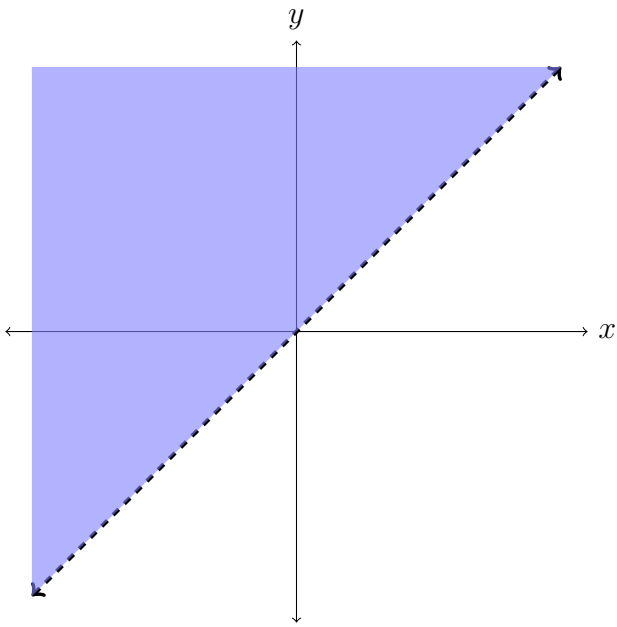
This is shorthand for the more complete sentence: "Fix R to be the relation on the natural numbers, $\mathbb{N}$, defined as the set of ordered pairs $(a, b) \in \mathbb{N} \times \mathbb{N}$ satisfying $a - b = 2$." When we define a relation R by a condition (such as $a - b = 2$) that condition tells us exactly when we should expect a to relate to b. $\triangle$

Warning 20.8. As with any definition, when we define a relation R with the word "if," the proper interpretation is "if and only if." For instance, in the previous example, the definition really means "aRb if and only if $a - b = 2$." This is a standard convention of mathematical language that can take some getting used to.

Example 20.9. Fix $A = \mathbb{R}$, and define a relation on A by xRy if $x - y$ is negative. If we wish to express R in set-builder notation, we could write

$$R = \{(x, y) \in \mathbb{R} \times \mathbb{R} : x - y \text{ is negative}\}.$$

Because $\mathbb{R} \times \mathbb{R}$ is just $\mathbb{R}^2$ we can graph the set R in the coordinate plane, as follows.



Notice that xRy means the same thing as $x < y$. In fact, this is the mathematical relation "less than," and it is usually just denoted by the symbol "$<$" rather than being called R. △

Often, for commonly used relations, we will find that there is a standard symbol. If there is not, we might use a nonstandard symbol, in which case we must be careful to define what the symbol means.

Some other standard symbols for relations on the real numbers are

$$\leq, \quad \geq, \quad >, \quad =, \quad \neq .$$

In Exercise 20.2, for each of these relations you will be asked to graph the corresponding subset of $\mathbb{R} \times \mathbb{R}$.

We end with one more example of a relation that is denoted by a standard symbol.

Example 20.10. Fix A to be the set of all logical formulas formed from P and Q. Define a relation R on A by xRy if x is logically equivalent to y. This relation R is usually written $\equiv$. △

20.B Properties of relations on a set A

We now study different properties that relations on a set A can have. These properties (especially the first three) have proven to be very useful; relations that satisfy these properties tend to be more mathematically interesting than other relations.

Definition 20.11. Let R be a relation on a set A.
(1) We say that R is *reflexive* if: $\forall a \in A,\ aRa$.
(2) We say that R is *symmetric* if: $\forall a, b \in A,\ aRb \Rightarrow bRa$.
(3) We say that R is *transitive* if: $\forall a, b, c \in A,\ ((aRb) \wedge (bRc)) \Rightarrow (aRc)$.
(4) We say that R is *antisymmetric* if: $\forall a, b \in A,\ ((aRb) \wedge (bRa)) \Rightarrow a = b$.

Example 20.12. Consider the "equality" relation on $\mathbb{C}$. Which of the four properties above hold for this relation?

It is reflexive, since given any $a \in \mathbb{C}$ we know $a = a$. It is also symmetric, since given $a, b \in \mathbb{C}$ if $a = b$ then $b = a$. It is transitive; for given $a, b, c \in \mathbb{C}$ if we assume $a = b$ and $b = c$, then $a = c$. Finally, it is antisymmetric. (Can you fill in the proof? Let $a, b \in A$. Assume $a = b$ and $b = a$. Conclude $a = b$.) △

Example 20.13. Consider the relation $<$ on $\mathbb{R}$. Using well-known facts about $<$, we will show that $<$ is not reflexive, is not symmetric, is transitive, and is antisymmetric.

(Not reflexive): Fix $0 \in \mathbb{R}$. We have $0 \not< 0$.

(Not symmetric): Fix $0, 1 \in \mathbb{R}$. We have $0 < 1$ but $1 \not< 0$.

(Transitive): Let $a, b, c \in \mathbb{R}$. Assume $a < b$ and $b < c$. It follows that $a < c$.

(Antisymmetric): Let $a, b \in \mathbb{R}$. Assume $a < b$ and $b < a$. This is impossible, so the implication is vacuously true. △

Example 20.14. Fix $A = \{1, 2, 3, 4\}$. Define a relation R on A by

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

We will prove that R is reflexive, symmetric, and transitive, but not antisymmetric. We can do this by just checking every possibility.

(Reflexive): To see that R is reflexive, we note that each of the four elements of A relates to itself; this is because $(1, 1)$, $(2, 2)$, $(3, 3)$, and $(4, 4)$ are in R.

(Symmetric): To see that R is symmetric, we note that for any pair in R, reversing the order of the elements in the pair yields another pair in R; for example, $(1, 2) \in R$, and reversing the elements, $(2, 1)$ is also in R. (What if $a = 1$ and $b = 4$? In that case the implication is vacuously true, since the premise is false.)

(Transitive): Transitivity is harder to see. Technically, we have 4 options for each of a, b, and c, giving a total of 64 cases. Most of those cases involve a false premise (hence are vacuously true). Let's do a case that is not vacuous. Notice that $(1, 2) \in R$. In addition, there are three elements c such that $(2, c) \in R$, namely $c = 1, 2, 3$. Since each of $(1, 1)$, $(1, 2)$, and $(1, 3)$ are in R, we see that whenever $(1, 2) \in R$ and $(2, c) \in R$, we have $(1, c) \in R$. Repeating this process with each element of R in place of $(1, 2)$, we see that R is transitive.

(Not antisymmetric): Fix $a = 1$ and fix $b = 2$. Both are in A. We find $1R2$ and $2R1$, but $1 \neq 2$. △

Remark 20.15. Notice that when a relation R is given explicitly by a set, it can be difficult to check transitivity. ▲

Transitivity is often easier to check when R is defined by a standard symbol, as we saw in previous examples. It is also easier to prove when R is defined by a rule, as we'll also see in the next example.

Example 20.16. Fix $A = \mathbb{N}$, and for any $a, b \in \mathbb{N}$, define aRb to mean that $b = ak$ for some $k \in \mathbb{N}$. Note that saying that aRb is the same as saying that $a \mid b$; this relation is just divisibility, so we will write $a \mid b$ instead of aRb. Before reading further, try to decide which of the four properties hold for this relation.

(Reflexive): Let $a \in \mathbb{N}$. We find $a \mid a$, because $a = a \cdot 1$.

(Not symmetric): Fix $a = 1$ and $b = 2$. These are elements of $\mathbb{N}$. Note that $a \mid b$ but $b \nmid a$.

(Transitive): Let $a, b, c \in \mathbb{N}$. Assume that $a \mid b$ and $b \mid c$. Proposition 7.13 shows that $a \mid c$.

(Antisymmetric): Let $a, b \in \mathbb{N}$. Assume that $a \mid b$ and $b \mid a$. Then $a = b$ by Corollary 17.2. Note that the relation in this example is defined on $\mathbb{N}$, not $\mathbb{Z}$. The divisibility relation on $\mathbb{Z}$ is *not* antisymmetric; take $a = 1$ and $b = -1$.) △

In the examples above we either proved that a property holds or proved that it fails. Thus, we have been using the negations of each of the properties. The following table lists all of the negations. (We leave it as an easy exercise to identify which row corresponds to which property.)

Definition	Negation
$\forall x \in A,\ xRx$	$\exists x \in A,\ x \not R x$
$\forall x, y \in A,\ xRy \Rightarrow yRx$	$\exists x, y \in A,\ xRy \wedge y \not R x$
$\forall x, y, z \in A,\ xRy \wedge yRz \Rightarrow xRz$	$\exists x, y, z \in A,\ xRy \wedge yRz \wedge x \not R z$
$\forall x, y \in A,\ (xRy \wedge yRx) \Rightarrow x = y$	$\exists x, y \in A,\ xRy \wedge yRx \wedge x \neq y$

We end this section with a few more examples of relations on sets. In some cases we will leave the proofs (and disproofs) of properties to the motivated student.

Example 20.17. Let U be a nonempty set, and fix $S = \mathscr{P}(U)$. We can define a relation R on S by ARB if $A \subseteq B$ (where $A, B \in S$ are subsets of U). Then R is easily seen to be reflexive (since every set is a subset of itself), transitive (since $A \subseteq B$ and $B \subseteq C$ implies $A \subseteq C$), and antisymmetric (since $A \subseteq B$ and $B \subseteq A$ implies $A = B$), but not symmetric. (Can you prove this last statement?) △

Example 20.18. Let A be any nonempty set, and fix $R = \emptyset$ to be the empty relation on A. We note that R is not reflexive (since, for each $a \in A$, we have $a \not R a$). On the other hand, R is symmetric, transitive, and antisymmetric, since the implications defining these properties are vacuously true for R (since no elements of A are related by R). △

Example 20.19. Let A be any nonempty set, and fix $R = A \times A$. Then, for any $a, b \in A$, we have aRb. The relation R is easily seen to be reflexive, symmetric, and transitive. It is antisymmetric if and only if $|A| = 1$. △

The reflexive, symmetric, and transitive properties are very important, and will be studied together in the next section.

20.C Exercises

Exercise 20.1. Fix $A = \{1, 2, 3, 4, 5, 6\}$ and fix

$$R = \{(1,1), (1,2), (1,3), (1,4), (2,3), (2,5), (2,6), (3,5), (4,5), (4,6)\}.$$

(a) Give an example of elements $a, b \in A$ such that aRb.
(b) Give an example of elements $a, b \in A$ such that $a \not R b$.
(c) For each $a \in A$, fix $S_a = \{x \in A : aRx\}$. Thus, S_a is the set of elements to which a relates. Write down the six sets $S_1, \ldots, S_6$ by listing their elements. For example, $S_1 = \{1, 2, 3, 4\}$.
(d) For each $a \in A$, fix $T_a = \{x \in A : xRa\}$. Thus, T_a is the set of elements that relate to a. Write down the six sets $T_1, \ldots, T_6$ by listing their elements.

Exercise 20.2. For each of the relations R from $\mathbb{R}$ to $\mathbb{R}$ defined below, write R as a set using set-builder notation, and graph R as a subset of $\mathbb{R}^2$.
(a) Define R by xRy if $x \leq y$.
(b) Define R by xRy if $x \geq y$.
(c) Define R by xRy if $x > y$.
(d) Define R by xRy if $x = y$.
(e) Define R by xRy if $x \neq y$.

Exercise 20.3. Define a relation R on $\mathbb{R}$ by xRy if $xy < 0$.
(a) Describe R as a set using set-builder notation.
(b) Graph R as a subset of $\mathbb{R} \times \mathbb{R}$.
(c) Determine whether R is reflexive, symmetric, transitive, and/or antisymmetric. (Give complete proofs.)

Exercise 20.4. Define a relation R on $\mathbb{R}$ by xRy if $x - y \in \mathbb{Z}$.
(a) Describe R as a set using set-builder notation.
(b) Graph R as a subset of $\mathbb{R} \times \mathbb{R}$.
(c) Determine whether R is reflexive, symmetric, transitive, and/or antisymmetric. (Give complete proofs.)

Exercise 20.5. Define a relation R on $\mathbb{Z}$ by aRb if $a - b$ is even.
(a) Describe R as a set using set-builder notation.
(b) Prove that R is reflexive, symmetric, and transitive.
(c) Prove that R is not antisymmetric.
(d) For which integers b is it the case that $1Rb$?

Exercise 20.6. For each part, give an example of a relation R on the set $A = \{1, 2, 3\}$ with the specified properties. Write R as a set of ordered pairs.
(a) R is reflexive, symmetric, and transitive.
(b) R is reflexive and symmetric, but not transitive.
(c) R is reflexive and transitive, but not symmetric.
(d) R is reflexive, not symmetric, and not transitive.
(e) R is not reflexive, but is symmetric and transitive.

(f) R is not reflexive and not transitive, but is symmetric.
(g) R is not reflexive and not symmetric, but is transitive.
(h) R is not reflexive, not symmetric, and not transitive.

Exercise 20.7. Fix $A = \{1, 2, 3, 4, 5\}$ and fix $S = \{\{1, 2, 3\}, \{3, 4\}, \{5\}\}$. Define

$$R = \{(a, b) \in A \times A : \text{for some } X \in S, \text{ both } a \in X \text{ and } b \in X\}.$$

(See Example 20.6 for a similar construction.)
(a) Write out the elements of R.
(b) Is R reflexive? Symmetric? Transitive? (Give complete proofs.)

Exercise 20.8. Fix $A = \{1, 2, 3, 4, 5\}$ and fix $S = \{\{1, 2\}, \{4, 5\}\}$. Define

$$R = \{(a, b) \in A \times A : \text{for some } X \in S, \text{ both } a \in X \text{ and } b \in X\}.$$

(See Example 20.6 for a similar construction.)
(a) Write out the elements of R.
(b) Is R reflexive? Symmetric? Transitive? (Give complete proofs.)

21 Equivalence relations

Knowing that we have a relation R on a set A tells us very little about either R or A. We can find many examples of relations on A, but without further information there is very little that we can say about a relation.

Placing conditions (such as "reflexive", "symmetric", and so forth) on a relation reduces the number of examples that we can find, but increases the amount that we know and can prove about each example.

One class of relations that has proven useful to mathematicians is the class of equivalence relations. Equivalence relations have enough conditions that we can prove useful theorems about them, but they are general enough that there are many examples of them in all areas of mathematics.

21.A Definition and examples

The definition of an equivalence relation is as follows:

Definition 21.1. Let R be a relation on a set A. We say that R is an *equivalence relation* if R is reflexive, symmetric, and transitive.

Equality is the prototypical example of an equivalence relation, but there are many more examples.

Example 21.2. Fix $A = \{1, 2, 3, 4\}$. Define a relation R on A by

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

as in Example 20.14. We have seen that R is reflexive, symmetric, and transitive. Hence, R is an equivalence relation. △

Example 21.3. Fix $A = \mathbb{Z}$ and for any $a, b \in A$, require aRb if a and b have the same parity. One easily checks that this relation is reflexive (an integer has the same parity as itself), symmetric (if a and b have the same parity, then so do b and a), and transitive (if a and b have the same parity, and b and c have the same parity, then a and c have the same parity). Hence, R is an equivalence relation. △

Example 21.4. Fix $A = \mathbb{R}$ and for any $a, b \in A$, require aRb if $|a| = |b|$. Again, one checks easily that this is reflexive ($|a| = |a|$), symmetric ($|a| = |b|$ clearly implies that $|b| = |a|$), and transitive (if $|a| = |b|$ and $|b| = |c|$, then $|a| = |c|$). Hence R is an equivalence relation. △

Example 21.5. Fix A to be the set of all triangles. For any $a, b \in A$, require aRb if a is similar to b. (Recall from geometry that two triangles are similar if they have the same interior angles.). One sees easily that this is an equivalence relation. △

In many cases, equivalence relations are written using symbols other than R to indicate that two elements are related. A common symbol to use for a generic equivalence relation is $\sim$, which can be read "is equivalent to." Other symbols that might be used to represent equivalence relations include $\equiv$, $\cong$, $\approx$, $\cong$, $\simeq$, $\doteq$. Using these symbols for a relation that is not an equivalence relation can cause confusion. Note that these symbols can have many different meanings, so if you use them it is important to say what they mean. For instance, $\equiv$ could mean congruence modulo n or it could mean logical equivalence (or it could have another meaning) depending on where it occurs.

Example 21.6. Fix $A = \mathbb{R} \times \mathbb{R}$. Define a relation $\sim$ on A by $(a, b) \sim (c, d)$ if $a^2 + b^2 = c^2 + d^2$. We check that $\sim$ is an equivalence relation.

Note that for $(a, b) \in \mathbb{R} \times \mathbb{R}$, we have $a^2 + b^2 = a^2 + b^2$. Hence, $(a, b) \sim (a, b)$, so the relation $\sim$ is reflexive.

Suppose that $(a, b) \sim (c, d)$. Then $a^2 + b^2 = c^2 + d^2$, so $c^2 + d^2 = a^2 + b^2$, and $(c, d) \sim (a, b)$. Hence, $\sim$ is symmetric.

Finally, assume that $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$. Then $a^2 + b^2 = c^2 + d^2$ and $c^2 + d^2 = e^2 + f^2$, so $a^2 + b^2 = e^2 + f^2$, and we see that $(a, b) \sim (e, f)$. Hence $\sim$ is transitive.

Therefore, $\sim$ is an equivalence relation. △

Example 21.7. Let P, Q, R be variables, and fix A be the set of all logical formulas formed from P, Q, and R. For any $a, b \in A$, write $a \equiv b$ if a is logically equivalent to b. One may check that $\equiv$ is an equivalence relation. △

Example 21.8. Fix $A = \{1, 2, 3, 4, 5\}$ and fix $S = \{\{1, 2\}, \{3, 4\}, \{5\}\}$.

Define a relation R on A by

$$R = \{(a, b) \in A \times A : \text{for some } X \in S, \text{ both } a \in X \text{ and } b \in X\}. \tag{21.9}$$

This is the same relation that we constructed in Example 20.6, where we saw that

$$R = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3), (3, 4), (4, 3), (4, 4), (5, 5)\}. \tag{21.10}$$

We will now prove that R is an equivalence relation. We begin by noting two facts about S that will be important: (1) every element of A is a member of some element of S, and (2) the elements of S are disjoint sets; no two of them share a common element of A. We will prove that R is an equivalence relation using (21.9), rather than using the explicit list (21.10).

(Reflexive): Let $a \in A$. There is some $X \in S$ such that $a \in X$. Hence, $(a, a) \in R$, so aRa. Therefore, R is reflexive.

(Symmetric): Let $a, b \in A$ and assume aRb. Then $(a, b) \in R$, so for some $X \in S$ we have $a, b \in X$. Hence, $b, a \in X$, so $(b, a) \in R$, and we see that bRa. Therefore R is symmetric.

(Transitive): Let $a, b, c \in A$ and assume aRb and bRc. Then there is some $X \in S$ such that $a, b \in X$, and there is some $Y \in S$ such that $b, c \in Y$. Since the elements of S are disjoint, $b \in X$ and $b \in Y$ implies that $X = Y$. Therefore, both a and c are in X, and aRc. Therefore R is transitive. △

21.B Equivalence classes

The properties of equivalence relations are chosen to mimic properties of equality. Often when we have an equivalence relation it is useful to gather together elements that are related under the equivalence relation and to treat them as if they were equal. Forming equivalence classes is the tool that performs this gathering.

Definition 21.11. Let A be a set and let $\sim$ be an equivalence relation on A. For any element $a \in A$, we define the *equivalence class of* a by

$$[a] = \{x \in A : a \sim x\}.$$

The element a is called a *representative* of the class $[a]$.

Other common notations for the equivalence class of a are $\overline{a}$, $\hat{a}$, or $\tilde{a}$. These symbols are used to represent the equivalence classes for many different equivalence relations; thus, if you use one of these notations, you must define it. Similarly, if you see such symbols in mathematical writing, you should look to see how they are defined.

Example 21.12. Fix $A = \{1, 2, 3, 4\}$ and define a relation R on A by

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

We saw in Example 20.14 that R is an equivalence relation. We now determine its equivalence classes.

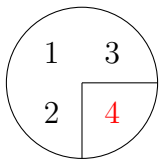
First, $[1]$ consists of all elements $x \in A$ such that $1Rx$. Examining R, we find that $1R1$, $1R2$, $1R3$, and $1\not R4$. Hence, $[1] = \{1, 2, 3\}$.

Now $[2]$ consists of all elements $x \in A$ such that $2Rx$. Examining R, we find that $2R1$, $2R2$, $2R3$, and $2\not R4$. Hence, $[2] = \{1, 2, 3\}$.

Similarly, $[3] = \{1, 2, 3\}$.

Finally, $[4] = \{4\}$, since the only $x \in A$ with $4Rx$ is $x = 4$.

We note that there are two equivalence classes in A. The first equivalence class is $[1] = [2] = [3] = \{1, 2, 3\}$ and the second is $[4] = \{4\}$. These classes divide the set A into two subsets, as in the diagram below.



△

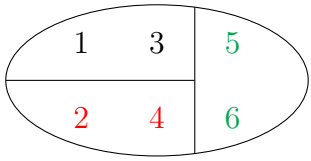
Example 21.13. Fix $A = \{1, 2, 3, 4, 5, 6\}$, and define a relation $\sim$ on A by

$$R = \left\{ \begin{array}{l} (1,1), (1,3), (2,2), (2,4), (3,1), (3,3), \\ (4,2), (4,4), (5,5), (5,6), (6,5), (6,6) \end{array} \right\}.$$

Then R is an equivalence relation. We will determine the equivalence classes of R.

To determine [1], we look for all of the ordered pairs $(1, x) \in R$. The only x's that work are 1 and 3. Hence, $[1] = \{1, 3\}$.

Similarly, $[2] = \{2, 4\}$, $[3] = \{1, 3\}$, $[4] = \{2, 4\}$, $[5] = \{5, 6\}$, and $[6] = \{5, 6\}$. We note that there are three equivalence classes, since $[1] = [3]$, $[2] = [4]$ and $[5] = [6]$. Because A is finite, we can easily draw a picture illustrating how the equivalence classes divide A into three pieces.



△

Example 21.14. Fix $A = \mathbb{Z}$, and fix $\sim$ to be the relation defined on A by $a \sim b$ if a and b have the same parity. We saw in Example 21.3 that $\sim$ is an equivalence relation. We will compute the equivalence classes.

The equivalence class [0] consists of all numbers having the same parity as 0. Hence, $[0] = 2\mathbb{Z}$, the set of even integers. The equivalence class [1] consists of all numbers having the same parity as 1. Hence, [1] is the set of odd integers.

Notice that if a is any even integer, $[a] = 2\mathbb{Z} = [0]$. Similarly, if a is any odd integer, $[a] = [1]$. Hence, in this case, there are exactly two equivalence classes, each containing infinitely many elements. Each class also has infinitely many representatives. For instance, $\cdots = [-2] = [0] = [2] = [4] = \cdots$. △

Example 21.15. Fix $A = \mathbb{R}$, and for any $a, b \in A$, define $a \doteq b$ by the rule $|a| = |b|$. We saw in Example 21.4 that $\doteq$ is an equivalence relation. For each $a \in A$, we will denote the equivalence class of a by $[a]$.

We see that $[0] = \{x \in \mathbb{R} : 0 \doteq x\} = \{x \in \mathbb{R} : |0| = |x|\}$. There is only one such value of x, namely $x = 0$. Hence, $[0] = \{0\}$.

Now, $[1] = \{x \in \mathbb{R} : 1 \doteq x\} = \{x \in \mathbb{R} : |1| = |x|\}$, or in other words the real numbers with absolute value 1. There are two such numbers: 1 and -1. Hence, $[1] = \{1, -1\}$.

Moving to negative numbers, $[-2] = \{x \in \mathbb{R} : -2 \doteq x\} = \{x \in \mathbb{R} : |-2| = |x|\}$, or in other words, the real numbers with absolute value 2. There are two such numbers: 2 and -2. Hence, $[-2] = \{2, -2\}$.

In general, if $a \in \mathbb{R}$ and $a \neq 0$, we see that $[a] = \{a, -a\}$.

We see that there are infinitely many different equivalence classes in R, each having one or two elements. △

We conclude this section by proving a very simple theorem, which is really just a restatement of the definition of an equivalence class. Nevertheless, this restatement will be quite useful to us, in telling us whether or not an element belongs to an equivalence class.

Theorem 21.16. *Let $\sim$ be an equivalence relation on a set A and let $a, b \in A$. Then $a \sim b$ if and only if $b \in [a]$.*

Proof. First, assume that $a \sim b$. Then, by the definition of $[a]$, we have $b \in [a]$. Conversely, assume that $b \in [a]$. Then, by the definition of $[a]$, we have $a \sim b$. □

21.C Exercises

Exercise 21.1. Fix $A = \{1, 2, 3\}$ and fix R to be the relation on A given by

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

Is R reflexive? Symmetric? Transitive? Antisymmetric? Is R an equivalence relation? (Give proofs.)

Exercise 21.2. Fix $A = \{1, 2, 3, 4, 5\}$. Give an example of an equivalence relation R on the set A that has exactly two equivalence classes. Explicitly write out the relation R as a set of ordered pairs.

Exercise 21.3. Let R be an equivalence relation on the set $A = \{1, 2, 3, 4, 5\}$. Assume that $1R3$ and $3R4$. Given these conditions, which ordered pairs must belong to R? (Hint: There are at least 11 such elements.)

Exercise 21.4. Fix $A = \{1, 2, 3, 4, 5\}$ and fix $S = \{\{1, 2\}, \{3, 4\}, \{5\}\}$. Define

$$R = \{(a, b) \in A \times A : \text{for some } X \in S, \text{ both } a \in X \text{ and } b \in X\}$$

as in Example 21.8. We have seen that R is an equivalence relation. What are the equivalence classes of R?

Exercise 21.5. Fix $A = \mathbb{R} - \{0\}$. Define a relation $\sim$ on A by $a \sim b$ if $ab > 0$.

(a) Prove that $\sim$ is an equivalence relation on A.
(b) Determine the equivalence classes of $\sim$.

Exercise 21.6. Fix A to be the set of humans with English names. Define a relation $\approx$ on A by $\alpha \approx \beta$ if α and β have the same first letter in their first names. (For instance, anyone named "Eugene" is related by $\approx$ to anyone named "Elizabeth".)

(a) Prove that $\approx$ is an equivalence relation on A.
(b) Determine the equivalence classes of $\approx$.

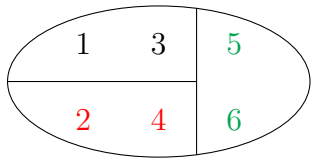
Exercise 21.7. Let A be a set. Let R be a reflexive, symmetric, and antisymmetric relation on A. Prove that R is the equality relation on A. (In other words, prove that for any $x, y \in A$, we have xRy if and only if $x = y$.)

22 Equivalence classes and partitions

In this section we prove that an equivalence relation allows us to break up a set into jigsaw-like pieces that one can fit together to give the entire set. Conversely, we will prove that if you break a set into jigsaw pieces, then one can define a corresponding equivalence relation. We saw an example of this earlier, with the set $A = \{1, 2, 3, 4, 5, 6\}$. The equivalence relation

$$R = \left\{ \begin{array}{l} (1,1), (1,3), (2,2), (2,4), (3,1), (3,3), \\ (4,2), (4,4), (5,5), (5,6), (6,5), (6,6) \end{array} \right\}$$

corresponded to breaking A into the equivalence classes pictured below.



This correspondence holds for arbitrary equivalence relations, as we will prove in this section.

22.A Properties of equivalence classes

The following theorem provides some useful criteria for determining whether two equivalence classes are equal.

Theorem 22.1. *Let $\sim$ be an equivalence relation on a set A, and for any $x \in A$ denote the equivalence class of x by $[x]$. For any $x, y \in A$, the following are equivalent:*

(1) $x \sim y$ *(the elements are related).*
(2) $[x] \cap [y] \neq \emptyset$ *(the classes intersect nontrivially).*
(3) $[x] = [y]$ *(the classes are equal).*

Proof. We prove the equivalence by proving three implications: (1) $\Rightarrow$ (3), (3) $\Rightarrow$ (2), and (2) $\Rightarrow$ (1). This will prove that we can move from any one condition to any other.

(1) $\Rightarrow$ (3): Assume $x \sim y$. By symmetry we also have $y \sim x$. We wish to show $[x] = [y]$. We will prove this equality by showing both inclusions.

First we will show $[x] \subseteq [y]$. Let $z \in [x]$. We then know $x \sim z$. Since $y \sim x$ and $x \sim z$, by transitivity we obtain $y \sim z$. Hence $z \in [y]$, and we have shown $[x] \subseteq [y]$.

The other inclusion, $[y] \subseteq [x]$, is proved similarly.

(3) $\Rightarrow$ (2): Now assume that $[x] = [y]$. By the reflexive property, $x \sim x$. Therefore $x \in [x] = [y]$. Hence $[x] \cap [y] \neq \emptyset$ since x is in the intersection.

(2) $\Rightarrow$ (1): Finally, assume $[x] \cap [y] \neq \emptyset$. Thus, there is some element $z \in [x] \cap [y]$. We then have $x \sim z$ and $y \sim z$. By symmetry and transitivity, $x \sim y$. $\square$

This theorem, along with Theorem 21.16 from the previous section, allows us to prove three central properties for equivalence classes. Let A be a set and let $\sim$ be an equivalence relation on A. The following all hold:

- **(Nonempty pieces)** No equivalence class is empty.

  Proof. Let $[x]$ be an equivalence class. Since $x \sim x$ by the reflexive property, we then have $x \in [x]$. □

- **(Covering)** Every element of A is an element of some equivalence class.

  Proof. An arbitrary element $a \in A$ belongs to the equivalence class $[a]$ (again, by the reflexive property). □

- **(Disjoint pieces)** Any two classes are either disjoint or equal.

  Proof. Since (2) implies (3) in Theorem 22.1, two classes that are not disjoint are equal. □

We can think of these three conditions as describing how to break a set into jigsaw pieces. First, none of the pieces should be empty. (Empty jigsaw pieces would just fall out of the box, and they wouldn't be missed anyway!) Second, when you put all of the pieces together, you should get the entire puzzle (in this case, the entire set A). Third, none of the pieces should overlap (else they don't fit together into a jigsaw puzzle).

We have proved that these three facts about equivalence classes are necessary. In the next subsection, we will show that they are sufficient to describe a (unique) equivalence relation with the same equivalence classes.

22.B Partitions and equivalence classes

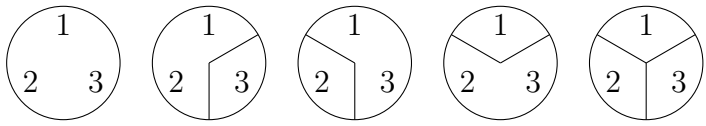
The three facts mentioned at the end of the previous subsection help us to define the concept of a partition, as follows:

Definition 22.2. Let A be a set. A collection P of subsets of A is called a *partition* of A if the following three conditions hold:
(Nonempty pieces) No set in P is empty.
(Covering) Every element of A is a member of some element of P.
(Disjoint pieces) Any two distinct elements of P are disjoint.
An element of P is called a *part* (or *piece*) of the partition.

Example 22.3. Fix $A = \{1, 2, 3\}$. Then the following are partitions of A:

$$P_1 = \{\{1, 2, 3\}\},$$
$$P_2 = \{\{1, 2\}, \{3\}\},$$
$$P_3 = \{\{1, 3\}, \{2\}\},$$
$$P_4 = \{\{2, 3\}, \{1\}\},$$
$$P_5 = \{\{1\}, \{2\}, \{3\}\}.$$

If we wish to represent these five partitions graphically, we can do so as below, where the set $A = \{1, 2, 3\}$ is represented as a circle. The parts of the partition are separated by line segments.



Careful examination shows that there are no other partitions of A.

Each of the following collections is *not* a partition of A. Try to figure out what is wrong in each case before reading the answers below.

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

Here are the reasons each of the sets above is not a partition of A:

(1) This collection fails the "nonempty pieces" condition, since one of the pieces is empty.
(2) This collection fails the "covering" condition, since we are missing 2.
(3) This collection fails the "disjoint pieces" condition, since the two distinct pieces overlap.
(4) This collection does not consist of subsets of A. (It would be a partition for the new set $B = \{1, 2, 3, 4\}$.)
(5) This collection is not a set of sets. (It would be a partition with an extra pair of set braces around it, and would then equal P_1 above.)

△

Example 22.4. Let's partition $\mathbb{N}$ into four parts. One such partition would be the following:

$$P = \{\{1\}, \{2\}, \{3\}, \{x \in \mathbb{N} : x \geq 4\}\}.$$

Three of the pieces are very small, and the other piece is infinite.

Another possibility would be the following, somewhat more natural, example. Given $n \in \mathbb{N}$ fix $S_n = \{x \in \mathbb{N} : x \equiv n \pmod 4\}$. Our new partition is

$$P' = \{S_1, S_2, S_3, S_4\}.$$

This is a partition because every natural number is congruent to exactly one of the four numbers $1, 2, 3, 4$. △

Example 22.5. There are fifteen different partitions of the set $A = \{1, 2, 3, 4\}$. We do not list them all, but mention that there is one partition with one part, seven partitions with two parts, six partitions with three parts, and one partition with four parts. As an example, $\{\{1, 2\}, \{3, 4\}\}$ is a partition of A with two parts, and $\{\{1\}, \{2\}, \{3, 4\}\}$ is a partition of A with three parts. △

The following theorem asserts that from an equivalence relation we can build a partition.

Theorem 22.6. *Let $\sim$ be an equivalence relation on a set A. For any $a \in A$, denote its equivalence class by $[a]$. Then the set*

$$P = \{[a] : a \in A\}$$

is a partition of A.

Proof. We already proved above that the set of equivalence classes satisfies all three of the defining conditions for a partition. □

The next two examples will demonstrate how we pass from an equivalence relation to a partition.

Example 22.7. Fix $A = \{1, 2, 3\}$ and fix R to be the relation defined by

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

We can easily confirm that R is an equivalence relation. The equivalence classes are $[1] = \{1\}$ and $[2] = \{2, 3\} = [3]$. Hence, the set of equivalence classes is $\{\{1\}, \{2, 3\}\}$, which is the partition P_4 from Example 22.3. △

Example 22.8. Consider the "same parity" relation on $\mathbb{Z}$. The two equivalence classes are the sets of even integers and odd integers. This partitions $\mathbb{Z}$ into two disjoint sets. △

The next theorem allows us to pass from a partition to an equivalence relation, thereby reversing the direction of the previous theorem.

Theorem 22.9. *Let P be a partition of a set A. There is an equivalence relation $\sim$ on A such that the equivalence classes of $\sim$ are precisely the parts of P.*

Proof. Let P be a partition of A. Define the relation $\sim$ on A by $a \sim b$ if a and b are both in a common part of P. We will show that $\sim$ is an equivalence relation.

First note that if A is empty (so that P is also empty), then symmetry and transitivity hold vacuously, while reflexivity holds since there is nothing to check. So, hereafter we assume A is nonempty.

(Reflexive): Let $a \in A$. By the covering property, a is an element of some part of P. Hence, $a \sim a$, so $\sim$ is reflexive.

(Symmetric): Let $a, b \in A$ and assume $a \sim b$. Thus, there is some part $X \in P$, such that $a \in X$ and $b \in X$. Hence, $b, a \in X$, so $b \sim a$. Thus, $\sim$ is symmetric.

(Transitive): Let $a, b, c \in A$ and assume $a \sim b$ and $b \sim c$. So $a, b \in X$ and $b, c \in Y$, where X and Y are parts of P. Since b is an element of both X and Y, we

must have $X = Y$ (by the disjoint pieces property), so $a, c \in X$, and hence $a \sim c$. Thus, $\sim$ is transitive, and this finishes the proof that $\sim$ is an equivalence relation.

Finally, we prove that the equivalence classes of $\sim$ are exactly the parts of P. For any $a \in A$ there is exactly one part $X \in P$ with $a \in X$ (by the covering and disjoint pieces conditions). By the definition of $\sim$, the elements of $[a]$ are exactly the elements of X, so $[a] = X$. Hence, the equivalence classes of $\sim$ are parts of P. Conversely, we show that the parts of P are equivalence classes. Given a part $X \in P$, it is nonempty. So there is some element $a \in X$. By the same argument above we obtain $[a] = X$, so it is an equivalence class. □

Together, Theorems 22.6 and 22.9 tell us that partitions of a set A and equivalence relations on A correspond to each other; every partition gives an equivalence relation and every equivalence relation gives a partition. The following example demonstrates this fact concretely.

Example 22.10. We partition $\mathbb{Z}$ into three pieces, in the following way:

$$P = \{\{0\}, \{x \in \mathbb{Z} : x < 0\}, \{x \in \mathbb{Z} : x > 0\}\}.$$

In other words, we partition $\mathbb{Z}$ into its zero, negative, and positive pieces.

What is the corresponding equivalence relation? It is the "two elements are related if they are both positive, both zero, or both negative" relation. More formally,

$$R = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : x, y \in \mathbb{Z}_{>0} \text{ or } x = y = 0 \text{ or } x, y \in \mathbb{Z}_{<0}\}.$$ △

22.C Transversals of equivalence relations

On occasion it is important to be able to refer to representatives of equivalence classes. When we pick one representative for each class, the collection of those representatives has a special name.

Definition 22.11. Let $\sim$ be an equivalence relation on a set A. A *transversal* of $\sim$ is a set $S \subseteq A$, such that S consists of exactly one representative of every equivalence class of $\sim$.

Example 22.12. Fix $A = \{1, 2, 3, 4, 5\}$ and fix

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

Then R is an equivalence relation on A. The equivalence classes of R are

$$[1] = [2] = \{1, 2\}, \quad [3] = \{3\}, \quad [4] = [5] = \{4, 5\}.$$

Then the set $\{1, 3, 5\}$ is a transversal, since it consists of a single element from each equivalence class. Other transversals are $\{1, 3, 4\}$, $\{2, 3, 4\}$, and $\{2, 3, 5\}$. △

Example 22.13. Define a relation $\sim$ on $\mathbb{R}$ by $a \sim b$ if $a - b \in \mathbb{Z}$. Thus, two real numbers are related by $\sim$ if they are an integer apart from one another. So, for instance, π is related to $\pi - 3$. We will show that $\sim$ is an equivalence relation, and that the set $[0, 1)$ is a transversal of $\sim$.

(Reflexive): Let $a \in \mathbb{R}$. We have $a - a = 0 \in \mathbb{Z}$, and so $a \sim a$.

(Symmetric): Let $a, b \in \mathbb{R}$, and assume $a \sim b$. Thus, $a - b \in \mathbb{Z}$, and so we have $b - a = -(a - b) \in \mathbb{Z}$. Therefore $b \sim a$.

(Transitive): Let $a, b, c \in \mathbb{R}$. Assuming $a \sim b$ and $b \sim c$, then we know that $a - b, b - c \in \mathbb{Z}$. Adding, we find that $a - c = (a - b) + (b - c) \in \mathbb{Z}$, so $a \sim c$.

Hence, $\sim$ is an equivalence relation.

We now proceed to show that $[0, 1)$ is a transversal of $\sim$. Define the *floor* of x, written $\lfloor x \rfloor$, to be the unique integer such that $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$. Thus, $\lfloor x \rfloor$ is obtained by "rounding down," even when x is negative. (So $\lfloor 5.6893 \rfloor = 5$, $\lfloor -3.49583 \rfloor = -4$, and $\lfloor \pi \rfloor = 3$.) The quantity $x - \lfloor x \rfloor$ is called the *fractional part* of x and is in $[0, 1)$.

First, every element of $\mathbb{R}$ is related to its fractional part, since x minus its fractional part $x - \lfloor x \rfloor$ is the integer $\lfloor x \rfloor$. This shows that some element from each equivalence class is a member of $[0, 1)$. Finally, if $a, b \in [0, 1)$ with $a \neq b$, then $a \not\sim b$, since $0 < |a - b| < 1$, so $a - b \notin \mathbb{Z}$. Thus, no more than one element from any equivalence class belongs to $[0, 1)$. △

Advice 22.14. There are typically two steps to proving that a given set T is a transversal of an equivalence relation $\sim$ on a set A.

First, you need to prove that every element of A is related to at least one element of T. Often this can be done by giving an explicit construction; for any element $a \in A$, construct an element $t \in T$ such that $a \sim t$.

Second, you need to prove that every element of A is related to at most one element of T. In other words, T cannot contain two representatives from the same class. So, it suffices to prove that $t_1 \sim t_2$ implies $t_1 = t_2$, for any $t_1, t_2 \in T$.

Example 22.15. Fix $\sim$ to be the relation on $\mathbb{R} \times \mathbb{R}$ defined by $(a, b) \sim (c, d)$ if $a + d = b + c$. We will show that $\sim$ is an equivalence relation and give a transversal of $\sim$.

(Reflexive): Let $(a, b) \in \mathbb{R} \times \mathbb{R}$. Then $(a, b) \sim (a, b)$ since $a + b = a + b$.

(Symmetric): Let $(a, b), (c, d) \in \mathbb{R} \times \mathbb{R}$. Assume that $(a, b) \sim (c, d)$. Then $a + d = b + c$. It follows that $c + b = a + d$, and we see that $(c, d) \sim (a, b)$.

(Transitive): Let $(a, b), (c, d), (e, f) \in \mathbb{R} \times \mathbb{R}$. Assume that $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$. Then $a + d = b + c$ and $c + f = d + e$. Adding these equations, we see that $a + d + c + f = b + c + d + e$. Subtracting $c + d$ from both sides of this equality, we see that $a + f = b + e$, so $(a, b) \sim (e, f)$.

Hence, $\sim$ is reflexive, symmetric, and transitive, so it is an equivalence relation.

Fix $T = \{(0, d) : d \in \mathbb{R}\}$. We will show that T is a transversal for $\sim$.

Let $(a, b) \in \mathbb{R} \times \mathbb{R}$. Then $(0, b-a) \in T$, and $(a, b) \sim (0, b-a)$, since $a+(b-a) = b+0$. Hence, every element of $\mathbb{R} \times \mathbb{R}$ is related to at least one element of T.

Now, suppose that $(0, d_1) \sim (0, d_2)$. Then $0 + d_2 = d_1 + 0$, hence $d_1 = d_2$. So $(0, d_1) = (0, d_2)$. This shows that no element of $\mathbb{R} \times \mathbb{R}$ is related to more than one element of T. Therefore T is a transversal. △

22.D Exercises

Exercise 22.1. Fix $A = \{1, 2, 3, 4\}$. List one partition of A with one part, seven partitions of A with two parts, six partitions of A with three parts, and one partition of A with four parts. This gives a total of fifteen partitions of A. (There are no more, but you do not need to prove this.)

Exercise 22.2. Let A be a set with $|A| = 10$, and let $\sim$ be an equivalence relation on A. Denote the equivalence classes of $\sim$ by $[x]$, for each $x \in A$. Suppose that we have elements $a, b, c \in A$ with $|[a]| = 3$, $|[b]| = 5$, and $|[c]| = 1$.

(a) Are any of a, b, and c related to each other by $\sim$?
(b) How many equivalence classes for $\sim$ are there?

Exercise 22.3. Define a relation $\sim$ on $\mathbb{R}^2$ by $(a, b) \sim (c, d)$ if $a^2 + b^2 = c^2 + d^2$. We saw in Example 21.6 that $\sim$ is an equivalence relation.

(a) Describe the equivalence class $[(3, 4)]$, both as a set and geometrically.
(b) For an arbitrary element $(a, b) \in \mathbb{R}^2$, describe $[(a, b)]$.
(c) Prove that the set $[0, \infty) \times \{0\}$ is a transversal of $\sim$.

Exercise 22.4. Fix W to be the set of all words in the English language. Define a relation on W by $\alpha \approx \beta$ if α and β have the same first letter.

(a) Prove that $\approx$ is an equivalence relation.
(b) Denote the equivalence class of $\alpha \in W$ using the notation $[\alpha]$. Taking $\alpha =$ "cat", list six elements of the equivalence class $[\alpha]$.
(c) How many equivalence classes are there for $\approx$?
(d) Describe a transversal of $\approx$. (You do not need to write it down in full.)

Exercise 22.5. Let A be a set with n elements. Define a relation $\sim$ on $\mathscr{P}(A)$ by $X \sim Y$ if $|X| = |Y|$, for any $X, Y \in \mathscr{P}(A)$.

(a) Prove that $\sim$ is an equivalence relation.
(b) Describe the equivalence classes for $\sim$.
(c) How many equivalence classes are there for $\sim$?
(d) One way to write down the set A is as $A = \{a_1, a_2, \ldots, a_n\}$. Using this description of A, write down a transversal of $\sim$.
(e) How many elements of $\mathscr{P}(A)$ are in each equivalence class?

Exercise 22.6. Fix $A = \{1, 2, \ldots, 10\}$. For each $i \in A$, define

$$S_i = \{X \in \mathscr{P}(A) \,:\, i \text{ is the least element of } X\}.$$

Fix $P = \{\{\emptyset\}, S_1, \ldots, S_{10}\}$.

(a) Prove that P is a partition of $\mathscr{P}(A)$. (Hint: Are the parts of P empty? Disjoint? Is every element of $\mathscr{P}(A)$ in some part?)

(b) Fix $\sim$ to be the equivalence relation on $\mathscr{P}(A)$ corresponding to P. How many equivalence classes does $\sim$ have?
(c) Write down a transversal of $\sim$.
(d) Determine the equivalence class $[\{8, 9, 10\}]$ by listing its elements.
(e) How large is the equivalence class $[\{2, 3, 4\}]$? (Do not write down all of its elements.)

Exercise 22.7. Give another proof of Theorem 22.1, by proving that (1) implies (2), that (2) implies (3), and that (3) implies (1). Note that your proof should not use any theorems after or including Theorem 22.1; it should only use basic properties of equivalence relations and equivalence classes.

Exercise 22.8. In this exercise we will show that an equivalence relation is uniquely determined by its equivalence classes, as follows: Let A be any set. Let $\sim$ and $\approx$ be two equivalence relations on A. Show that if their equivalence classes are the same, then the relations are the same. (In other words, conclude that for any $a, b \in A$, we have $a \sim b$ if and only if $a \approx b$.)

(Hint: For ease of notation, write the equivalence class of $a \in A$ under the relation $\sim$ using the notation $[a]$, and write the equivalence class under the relation $\approx$ using the notation $\overline{a}$.)

23 Integers modulo n

In this section we will study integer congruence and prove it is an equivalence relation.

23.A Review of integer congruence

Recall the definition of congruence modulo n (Definition 8.11).

Definition 23.1. Let $a, b, n \in \mathbb{Z}$. We say that $a \equiv b \pmod{n}$ when $a = b + nk$ for some $k \in \mathbb{N}$.

We read $a \equiv b \pmod{n}$ as "a is congruent to b modulo n" or "a is congruent to b mod n." This defines a relation on $\mathbb{Z}$. (Two elements are related if they are congruent modulo n.) We refer to the relation as "congruence modulo n."

Theorem 23.2. *Congruence modulo n is an equivalence relation on $\mathbb{Z}$.*

Proof. **(Reflexive):** Let $a \in \mathbb{Z}$. We have $a = a + n \cdot 0$. Hence, $a \equiv a \pmod{n}$, and so congruence modulo n is reflexive.

(Symmetric): Let $a, b \in \mathbb{Z}$, and assume $a \equiv b \pmod{n}$. Then $a = b + nk$ for some $k \in \mathbb{Z}$. This implies that $b = a + n(-k)$, so $b \equiv a \pmod{n}$. Hence, congruence modulo n is symmetric.

(Transitive): Let $a, b, c \in \mathbb{Z}$, and assume both that $a \equiv b \pmod{n}$ and that $b \equiv c \pmod{n}$. Then $a = b + nk$ and $b = c + n\ell$ for some $k, \ell \in \mathbb{Z}$. Then

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

so $a \equiv c \pmod{n}$. Hence, congruence modulo n is transitive. □

23.B Congruence classes modulo n

Having verified that congruence modulo n is an equivalence relation, we can utilize our knowledge of equivalence relations from the previous sections. In particular, we can talk about equivalence classes under the relation of congruence modulo n.

For instance, congruence modulo 3 is an equivalence relation. The set of integers that are congruent to 0 modulo 3 is

$$\{\ldots, -6, -3, 0, 3, 6, 9, \ldots\}.$$

This is the equivalence class of 0, under the relation "congruence modulo 3," which is also the equivalence class of 3, 6, -3, and so forth. We will see in a moment that there are only two other equivalence classes, which are

$$\{\ldots, -5, -2, 1, 4, 7, \ldots\}$$

and

$$\{\ldots, -4, -1, 2, 5, 8, \ldots\}.$$

We will now set up the notation to prove this in much greater generality.

Definition 23.3. An equivalence class in $\mathbb{Z}$ under the relation congruence modulo n is called a *congruence class modulo* n. The congruence class of $a \in \mathbb{Z}$ will be denoted by $\overline{a}$.

Given $a, b \in \mathbb{Z}$, we see by Theorem 22.1 that $\overline{a} = \overline{b}$ if and only if $a \equiv b \pmod{n}$.

We know by Theorem 22.6 that the equivalence classes for an equivalence relation on $\mathbb{Z}$ form a partition of $\mathbb{Z}$. We will now proceed to determine the congruence classes for "congruence modulo n" and determine the number of distinct classes. To do this we will make use of the division algorithm. In the following theorem we restrict to the case $n > 0$, since allowing n to be 0 would make the theorem false (why?) and allowing n to be negative would require absolute values in the statement.

Theorem 23.4. *Let $n \in \mathbb{N}$. There are n congruence classes modulo n, namely the classes*

$$\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}.$$

For any $a \in \mathbb{Z}$, we have

$$\overline{a} = \{a + kn : k \in \mathbb{Z}\}.$$

Proof. We first prove that the only congruence classes are the ones listed in the theorem. Let $a \in \mathbb{Z}$. By the division algorithm $a = qn + r$ for some $q, r \in \mathbb{Z}$ and $0 \leq r < n$. Thus $a = r + nq$, so $a \equiv r \pmod{n}$. Hence, $\overline{a} = \overline{r}$ is one of the n congruence classes listed in the theorem.

It remains to show that no two congruence classes listed in the theorem are equal. This follows from the uniqueness of the remainder in the division algorithm, which was proved in Lemma 17.14.

Finally, we note that for any $a \in \mathbb{Z}$,

$$\begin{aligned}\overline{a} &= \{x \in \mathbb{Z} : x \equiv a \pmod{n}\} \\ &= \{x \in \mathbb{Z} : x = a + kn \text{ for some } k \in \mathbb{Z}\} \\ &= \{a + kn : k \in \mathbb{Z}\}\end{aligned}$$

as claimed. □

The set of congruence classes modulo n is so important that we write it using a special notation.

Definition 23.5. Let $n \in \mathbb{N}$. We define $\mathbb{Z}_n$ to be the set

$$\{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$$

of congruence classes modulo n.

We note the following facts about $\mathbb{Z}_n$:

(a) $|\mathbb{Z}_n| = n$.
(b) Every element of $\mathbb{Z}$ is a member of exactly one element of $\mathbb{Z}_n$.
(c) Every element of $\mathbb{Z}_n$ is an infinite subset of $\mathbb{Z}$.

Example 23.6. The set $\mathbb{Z}_4$ has four elements. They are written $\overline{0}, \overline{1}, \overline{2}, \overline{3}$. Each of these elements, even though it looks like a number, is really an infinite set. For instance,

$$\overline{1} = \{\ldots, -7, -3, 1, 5, 9, \ldots\}. \qquad \triangle$$

Remark 23.7. We have said that the n elements $\overline{0}, \ldots, \overline{n-1}$ are the only elements in $\mathbb{Z}_n$. There are many other integers, in fact infinitely many, that are not elements of the set $\{0, 1, \ldots, n-1\}$. What happens to their congruence classes?

The proof of Theorem 23.4 shows that for *every* integer $a \in \mathbb{Z}$, the congruence class $\overline{a}$ is the same as one of the classes $\overline{r}$ with $0 \leq r < n$. We can think of $\overline{a}$ and $\overline{r}$ as different names for the same congruence class. For instance, in $\mathbb{Z}_6$ the congruence class $\overline{1}$ has many different representatives:

$$\cdots = \overline{-11} = \overline{-5} = \overline{1} = \overline{7} = \overline{13} = \overline{19} = \cdots . \qquad \blacktriangle$$

23.C Operations on $\mathbb{Z}_n$

Even though the elements of $\mathbb{Z}_n$ are sets (not numbers), we still want to treat these elements as if they *were* numbers. In fact, you have probably already done this without realizing it. For instance, when you add clock times together you are doing arithmetic in $\mathbb{Z}_{12}$. When you use the fact that "odd plus even equals odd" you are doing arithmetic in $\mathbb{Z}_2$.

The following theorem will help us make a sensible definition of addition and multiplication on the set $\mathbb{Z}_n$.

Theorem 23.8. *For any $a, b, c, d, n \in \mathbb{Z}$, if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then*
(1) *$a + c \equiv b + d \pmod{n}$ and*
(2) *$ac \equiv bd \pmod{n}$.*

Proof. Suppose that $a \equiv b \pmod{n}$ and that $c \equiv d \pmod{n}$. Then $a = b + nk$ and $c = d + n\ell$ for some $k, \ell \in \mathbb{Z}$.

We find that

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

so $a + c \equiv b + d \pmod{n}$. Hence, (1) is true.

We next find that

$$ac = (b + nk)(d + n\ell) = bd + bn\ell + nkd + n^2k\ell = bd + n(b\ell + kd + nk\ell).$$

Thus, $ac \equiv bd \pmod{n}$. Hence, (2) is true. $\square$

The next example demonstrates how using this theorem can help simplify computations modulo n.

Example 23.9. We have that $28 \equiv 2 \pmod{26}$ and $29 \equiv 3 \pmod{26}$. Hence, according to the theorem, $28 \cdot 29 \equiv 2 \cdot 3 \pmod{26}$. Indeed, computation shows that

$$28 \cdot 29 = 812 = 6 + 806 = 2 \cdot 3 + 26 \cdot 31.$$

Multiplying 2 and 3 is much easier than multiplying 28 and 29. Thus, finding $28 \cdot 29$ modulo 26 is very easy. You just multiply $2 \cdot 3$ to get 6. △

The upshot of this theorem is that when adding and multiplying, if we are only interested in what the result is modulo n, then we only need to worry about what the inputs are modulo n. Motivated by this, we make a definition of what it means to add and multiply congruence classes mod n. (The following definition may be strange at first. If so, work through the examples that follow.)

Definition 23.10. Let $n \in \mathbb{N}$. Given $X, Y \in \mathbb{Z}_n$, then $X = \overline{a}$ and $Y = \overline{b}$ for some $a, b \in \mathbb{Z}$. We define

$$X + Y = \overline{a + b},$$

and

$$X \cdot Y = \overline{a \cdot b},$$

where the $+$ and $\cdot$ on the right denote addition and multiplication of integers.

Warning 23.11. It is important to notice that on the left-hand side of the equations in Definition 23.10, the $+$ and $\cdot$ symbols are *not* the usual addition and multiplication of integers. They are telling us how to add and multiply elements of $\mathbb{Z}_n$, which are sets rather than just numbers. The definition shows that these operations are closely related to addition and multiplication on the integers, but they are not the same!

We will illustrate this definition by working modulo 7 and modulo 11. In these examples, when we work in $\mathbb{Z}_n$ we will always write our results as $\overline{r}$ with $0 \leq r < n$, even though we may use numbers larger than n during the computations.

Example 23.12. We perform the following computations in $\mathbb{Z}_7$:

$$\begin{aligned}
\overline{5} + \overline{6} &= \overline{5 + 6} = \overline{11} = \overline{4}, \\
\overline{1} + \overline{6} &= \overline{1 + 6} = \overline{7} = \overline{0}, \\
\overline{5} \cdot \overline{6} &= \overline{5 \cdot 6} = \overline{30} = \overline{2}, \text{ and} \\
\overline{3} \cdot \overline{5} &= \overline{3 \cdot 5} = \overline{15} = \overline{1}.
\end{aligned}$$

If we want to add two equivalence classes, we choose representatives, add the representatives, and then simplify (in this case modulo 7). △

Example 23.13. We perform the following calculations in $\mathbb{Z}_{11}$:

$$\begin{aligned}\overline{5}+\overline{6}&=\overline{5+6}=\overline{11}=\overline{0},\\ \overline{1}+\overline{6}&=\overline{1+6}=\overline{7},\\ \overline{5}\cdot\overline{6}&=\overline{5\cdot 6}=\overline{30}=\overline{8},\text{ and}\\ \overline{3}\cdot\overline{5}&=\overline{3\cdot 5}=\overline{15}=\overline{4}.\end{aligned}$$

If we want to add two equivalence classes, we choose representatives, add the representatives, and then simplify (in this case modulo 11). △

Warning 23.14. It is not obvious that the definition of addition (or of multiplication) in $\mathbb{Z}_n$ makes sense. Given any $X, Y \in \mathbb{Z}_n$, we have defined $X+Y$ by *choosing* integers a and b with $X=\overline{a}$ and $Y=\overline{b}$, and then taking $X+Y=\overline{a+b}$. However, other choices of integer representatives for these classes would be possible. Does the value of $X+Y$ depend on our choices?

Fortunately, no. Suppose that we had picked other integers c and d with $X=\overline{c}$ and $Y=\overline{d}$. Then $a\equiv c \pmod n$ and $b\equiv d \pmod n$. Hence, by Theorem 23.8 we know that $a+b\equiv c+d \pmod n$, so $\overline{a+b}=\overline{c+d}$. Hence, our choices make no difference in the value of $X+Y$.

When we have a definition that appears to depend on choices, but for which those choices can be shown to make no difference after all, we say that the operation being defined is *well-defined*. We have thus shown that addition on $\mathbb{Z}_n$ is well-defined.

Example 23.15. We write the complete addition and multiplication tables for $\mathbb{Z}_6$.

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

In these tables we wrote every entry using $\overline{0}, \overline{1}, \ldots, \overline{5}$. We can do this because the set $\{0,1,\ldots,5\}$ is a transversal for the equivalence classes. We could have used any other transversal such as $\{1,2,3,4,5,6\}$, $\{-2,-1,0,1,2,3\}$, or even $\{-10,-5,0,5,10,15\}$ (but it is best to keep things simple).

We notice some interesting facts about multiplication and addition in $\mathbb{Z}_n$ that are different from addition and multiplication in $\mathbb{Z}$.

If a is an integer and $a+a=0$, then a must equal 0. However, in $\mathbb{Z}_6$ we have $\overline{3}+\overline{3}=\overline{0}$ even though $\overline{3}\neq\overline{0}$.

If $a, b \in \mathbb{Z}$ with $a\cdot b=0$, then either $a=0$ or $b=0$ (or both). However, in $\mathbb{Z}_6$ we have $\overline{2}\cdot\overline{3}=\overline{0}$ even though neither $\overline{2}$ nor $\overline{3}$ is equal to $\overline{0}$. △

This example shows that we cannot take facts about addition or multiplication in $\mathbb{Z}_n$ for granted. We must prove those facts about addition and multiplication that we wish to use in $\mathbb{Z}_n$, rather than just assuming they hold. In the exercises you will prove some basic facts about operations in $\mathbb{Z}_n$ that do match our intuition from $\mathbb{Z}$. We demonstrate with an example.

Example 23.16. Let $n \in \mathbb{N}$. We will prove that for each $X \in \mathbb{Z}_n$, we have $X + \overline{0} = X$.

Let $X \in \mathbb{Z}_n$. Then for some $a \in \mathbb{Z}$, we have $X = \overline{a}$. (Note that we could take $0 \leq a < n$, but we do not need this extra information.) We find

$$X + \overline{0} = \overline{a} + \overline{0} = \overline{a + 0} = \overline{a} = X. \qquad \triangle$$

23.D Exercises

Exercise 23.1. Let $n \in \mathbb{N}$ and let $a \in \mathbb{Z}$. Write the class of a in $\mathbb{Z}_n$ as $\overline{a}$. Prove that $0 \in \overline{a}$ if and only if $n \mid a$.

Exercise 23.2. Compute the following. Write the results as $\overline{r}$, with $r \in \mathbb{Z}$ nonnegative and as small as possible.

(a) $\overline{6} + \overline{7}$ in $\mathbb{Z}_9$.
(b) $\overline{6} \cdot \overline{7}$ in $\mathbb{Z}_9$.
(c) $\overline{59} \cdot \overline{119}$ in $\mathbb{Z}_{30}$.
(d) $\overline{6} \cdot \overline{5} + \overline{85}$ in $\mathbb{Z}_7$.
(e) $\overline{2}^{10}$ in $\mathbb{Z}_5$. (By $\overline{a}^k$ we mean $\underbrace{\overline{a} \cdot \overline{a} \cdots \overline{a}}_{k \text{ times}}$, for each $k \in \mathbb{N}$.)

Exercise 23.3. Create addition and multiplication tables for $\mathbb{Z}_5$. Be sure to write each entry of the tables as one of $\overline{0}$, $\overline{1}$, $\overline{2}$, $\overline{3}$, or $\overline{4}$.

Exercise 23.4. Let $n \in \mathbb{N}$. Prove the following facts about addition and multiplication in $\mathbb{Z}_n$.

(a) For any $X, Y \in \mathbb{Z}_n$, $X + Y = Y + X$.
(b) For any $X, Y \in \mathbb{Z}_n$, $X \cdot Y = Y \cdot X$.
(c) For any $X \in \mathbb{Z}_n$, $X \cdot \overline{0} = \overline{0}$.
(d) For any $X \in \mathbb{Z}_n$, $X \cdot \overline{1} = X$.
(e) For any $X \in \mathbb{Z}_n$, $X \cdot \overline{2} = X + X$.
(f) For any $X \in \mathbb{Z}_n$, there is some $Y \in \mathbb{Z}_n$ such that $X + Y = \overline{0}$.
(g) For any $X, Y, Z \in \mathbb{Z}_n$, $(X + Y) \cdot Z = (X \cdot Z) + (Y \cdot Z)$.

Exercise 23.5. Demonstrate that for each $X \neq \overline{0}$ in $\mathbb{Z}_5$, there is some $Y \in \mathbb{Z}_5$ such that $X \cdot Y = \overline{1}$. (Hint: Use the multiplication table that you created in Exercise 23.3.)

Exercise 23.6. Is it true that for each $X \neq \overline{0}$ in $\mathbb{Z}_6$, there is some $Y \in \mathbb{Z}_6$ such that $X \cdot Y = \overline{1}$?

Exercise 23.7. In this exercise we generalize what was done in the previous two exercises.

(a) If $n \in \mathbb{N}$ is composite, prove that there are elements $\overline{a}, \overline{b} \in \mathbb{Z}_n$ with $\overline{a} \cdot \overline{b} = \overline{0}$ even though $\overline{a}, \overline{b} \neq \overline{0}$.

(b) If $n \in \mathbb{N}$ is prime, prove that given $\overline{a}, \overline{b} \in \mathbb{Z}_n$, if $\overline{a} \cdot \overline{b} = \overline{0}$, then $\overline{a} = \overline{0}$ or $\overline{b} = \overline{0}$. (Hint: Use Euclid's Lemma, Theorem 19.5.)

(c) If $n \in \mathbb{N}$ is prime, prove that for any nonzero $\overline{a} \in \mathbb{Z}_n$, there exists $\overline{b} \in \mathbb{Z}_n$ with $\overline{a} \cdot \overline{b} = \overline{1}$. (Hint: First prove that if $\overline{a} \neq \overline{0}$ then $\text{GCD}(a, n) = 1$. Then write 1 as a linear combination of a and n.)