The impediment to action advances action.
What stands in the way becomes the way.

Marcus Aurelius, Roman emperor

Chapter 7

Relations and Partitions

While there is no agreed upon universal definition of mathematics, one could argue that mathematics focuses on the study of patterns and relationships. Certain types of relationships occur over and over in mathematics. One way of formalizing the abstract nature and structure of these relationships is with the notion of relations. In Chapter 8, we will see that a function is a special type of relation.

7.1 Relations

Recall from Section 3.5 that the Cartesian product of two sets A and B, written $A \times B$, is the set of all ordered pairs (a, b), where $a \in A$ and $b \in B$. That is, $A \times B = \{(a, b) \mid a \in A, b \in B\}$.

Definition 7.1. Let A and B be sets. A **relation** R **from** A **to** B is a subset of $A \times B$. If R is a relation from A to B and $(a, b) \in R$, then we say that a **is related to** b and we may write $\boxed{aRb}$ in place of $(a, b) \in R$. If R is a relation from A to the same set A, then we say that R is a **relation on** A.

Example 7.2. The set $\mathbb{N} \times \mathbb{R}$ from Problem 3.55 is an example of a relation on $\mathbb{R}$ since $\mathbb{N} \times \mathbb{R}$ is a subset of $\mathbb{R} \times \mathbb{R}$.

It is important to notice that the order in which we write things for relations matters. In particular, if R is a relation from A to B and aRb, then it may or may not be the case that bRa.

Example 7.3. If $A = \{a, b, c, d, e\}$ and $B = \{1, 2, 3, 4\}$, then the set of ordered pairs

$$R = \{(a, 1), (a, 2), (a, 4), (c, 2), (d, 2), (e, 2), (e, 4)\}$$

is an example of a relation from A to B. In this case, we could write $(c, 2) \in R$ or $cR2$. We could also say that a is related to 1, 2, and 4.

Example 7.4. As in the previous example, let $A = \{a, b, c, d, e\}$. One possible relation on A is given by

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

Example 7.5. Consider the set of accounts A on the social media platform Twitter. On Twitter, each account has a set of accounts that they follow. We can model this situation mathematically using a relation on A. Define T on A via xTy if x follows y on Twitter. As a set

$$T = \{(x, y) \in A \times A \mid x \text{ follows } y \text{ on Twitter}\}.$$

Example 7.6. You are already familiar with many relations. For example, $=$, $\leq$, and $<$ are each examples of relations on the real numbers. We could say that $(3, \pi)$ is in the relation $\leq$ and the relation $<$ since $3 \leq \pi$ and $3 < \pi$. However, $(3, \pi)$ is not in the relation $=$ since $3 \neq \pi$. Also, notice that order matters for the relations $\leq$ and $<$ yet does not for $=$. For example, $(-\sqrt{2}, 4)$ is in the relation $\leq$ while $(4, -\sqrt{2})$ is not.

Example 7.7. Define the relation S from $\{-1, 1\}$ to $\mathbb{Z}$ via $1Sx$ if x is even and $-1Sx$ if x is odd. That is, 1 is related to all even integers and -1 is related to all odd integers.

Example 7.8. Let A be any set. Since $\emptyset \subseteq A \times A$, the empty set forms a relation on A. This relation is called the **empty relation** on A.

Relations can be represented using digraphs. A **digraph** (short for **directed graph**) is a discrete graph that consists of a set of vertices connected by edges, where the edges have a direction associated with them. If R is a relation from A to B, then the elements of A and B are the vertices of the digraph and there is a directed edge from $a \in A$ to $b \in B$ if (a, b) is in the relation R (i.e., aRb). We can visually represent digraphs by using dots to represent the vertices and arrows to represent directed edges. We will not make a distinction between a digraph and its visual representation. Utilizing a digraph to represent a relation may be impractical if there is a large number of vertices or directed edges.

Example 7.9. Consider the relation given in Example 7.3. The corresponding digraph is depicted in Figure 7.1. Notice that we have placed the vertices corresponding to elements of A on the left and the elements of B on the right. This is standard practice, but what really matters is the edge connections not how the vertices are placed on the page.

Problem 7.10. Let $A = \{1, 2, 3, 4, 5, 6\}$ and $B = \{1, 2, 3, 4\}$ and define D from A to B via $(a, b) \in D$ if $a - b$ is divisible by 2. List the ordered pairs in D and draw the corresponding digraph.

If R is a relation on A (i.e., a relation from A to A), then we can simplify the structure of the digraph by only utilizing one copy of A for the vertices. In this case, we may have directed edges that point from a vertex to itself. When drawing digraphs for a relation on a set, we will default to this simplified digraph (like the one depicted in Figure 7.2(b)).

Example 7.11. Figure 7.2(a) represents the relation of Example 7.4 as a digraph from A to A while the digraph in Figure 7.2(b) provides a streamlined representation of the same relation that uses the elements in A only once instead of twice.

Problem 7.12. Let $A = \{1, 2, 3, 4, 5, 6\}$ and define $|$ on A via $x|y$ if x divides y. List the ordered pairs in $|$ and draw the corresponding digraph.

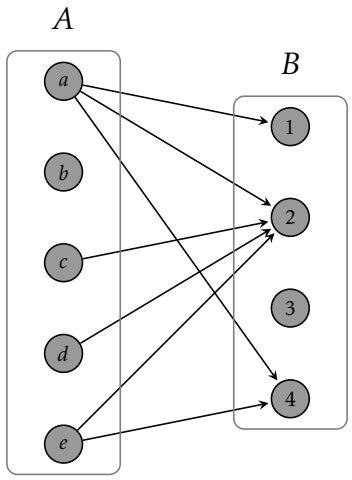

Figure 7.1: Digraph for a relation from $A = \{a, b, c, d, e\}$ to $B = \{1, 2, 3, 4\}$.

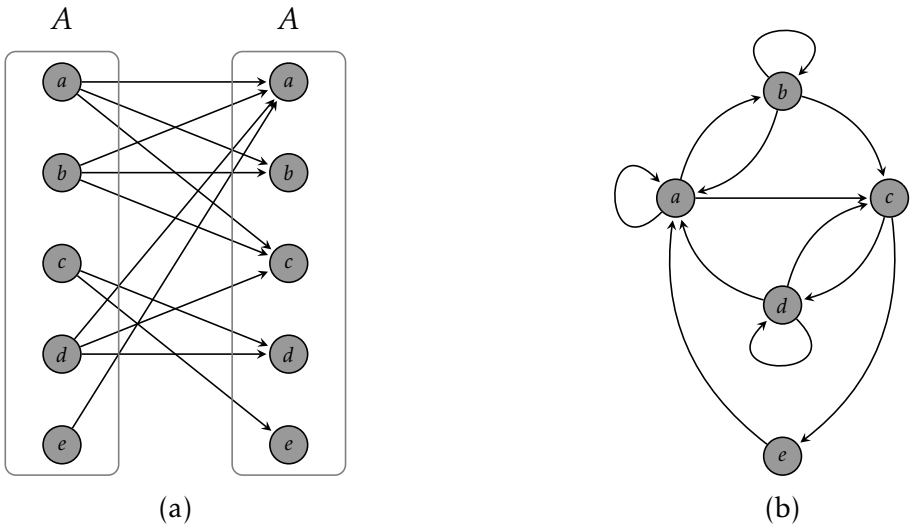

Figure 7.2: Two variations of digraphs for a relation on $A = \{a, b, c, d, e\}$.

Problem 7.13. Let $A = \{a, b, c, d\}$ and define R on A via

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

(a) Draw the digraph for R.

(b) Draw the digraph for the empty relation on A.

We can also visually represent a relation by plotting the points in the relation. In particular, if R is a relation from A to B and aRb, we can plot all points (a, b) that satisfy aRb in two dimensions, where we interpret the set A to be the horizontal axis and B to be the vertical axis. We will refer to this visual representation of a relation as the **graph** of the relation.

Example 7.14. When we write $x^2 + y^2 = 1$, we are implicitly defining a relation. In particular, the relation is the set of ordered pairs (x, y) satisfying $x^2 + y^2 = 1$, namely $\{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$. The graph of this relation in $\mathbb{R}^2$ is the unit circle centered at the origin in the plane as shown in Figure 7.3.

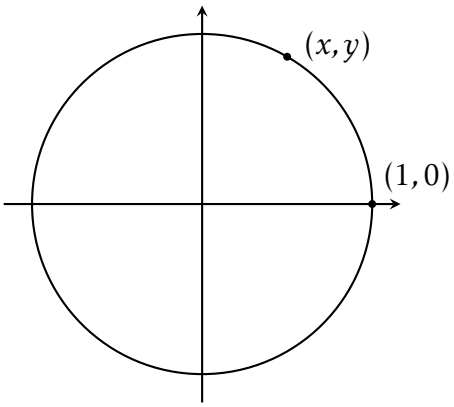

Figure 7.3: Graph of the relation determined by $x^2 + y^2 = 1$.

Problem 7.15. For each of the following, draw a portion of the graph that represents the relation as a subset of $\mathbb{R}^2$.

(a) $\{(x, y) \in \mathbb{R}^2 \mid y = x^2\}$

(b) $\{(x, y) \in \mathbb{Z}^2 \mid y = x^2\}$

(c) $\{(x, y) \in \mathbb{R}^2 \mid y^2 = x\}$

(d) $\{(x, y) \in \mathbb{N} \times \mathbb{R} \mid y^2 = x\}$

Problem 7.16. Draw a portion of the graph that represents the relation $\leq$ on $\mathbb{R}$.

For a relation on a set, it is natural to consider the collection of elements that a given element is related to. For example, a user's "Following List" on Twitter is the set of accounts on Twitter that the user is following.

Definition 7.17. Let R be a relation on a set A. For each $a \in A$, we define the **set of relatives of a with respect to** R via

$$\boxed{\text{rel}(a, R) := \{b \in A \mid aRb\}}.$$

We also define the **collection of the sets of relatives with respect to** R by

$$\boxed{\text{Rel}(R) := \{\text{rel}(a) \mid a \in A\}}.$$

If R is clear from the context, we will usually write $\boxed{\text{rel}(a)}$ in place of $\text{rel}(a, R)$. In terms of digraphs, $\text{rel}(a)$ is the collection of vertices that have a directed edge pointing towards them from the vertex labeled by a. In graph theory, this collection of vertices is called the **out neighborhood** of a and each such vertex is called an **out neighbor**. Notice that $\text{Rel}(R)$ is a set of sets. In particular, an element in $\text{Rel}(R)$ is a subset of A—equivalently, an element of $\mathcal{P}(A)$.

Example 7.18. Consider the relation given in Example 7.4. By inspecting the ordered pairs in R or by looking at the digraph in Figure 7.2(b), we see that

$$\text{rel}(a) = \{a, b, c\},\ \text{rel}(b) = \{a, b, c\},\ \text{rel}(c) = \{d, e\},\ \text{rel}(d) = \{a, c, d\},\ \text{rel}(e) = \{a\},$$

so that $\text{Rel}(R) = \{\{a, b, c\}, \{d, e\}, \{a, c, d\}, \{a\}\}$.

Problem 7.19. Consider the relation given in Problem 7.13(a). Find $\text{Rel}(R)$ by determining $\text{rel}(x)$ for each $x \in A$.

Problem 7.20. Describe the collection of the sets of relatives with respect to the empty relation from Problem 7.13(b).

Problem 7.21. Let P denote the set of all people with accounts on Facebook and define the relation F on P via xFy if x is friends with y. Describe rel(Maria), where Maria is the name of a specific Facebook user. What is $\text{Rel}(F)$?

Problem 7.22. Define the relation $\equiv_5$ on $\mathbb{Z}$ via $a \equiv_5 b$ if $a - b$ is divisible by 5. Find rel(1), rel(2), and rel(6). How many distinct sets are in $\text{Rel}(\equiv_5)$? List the distinct sets in $\text{Rel}(\equiv_5)$.

Problem 7.23. Consider the relation $\leq$ on $\mathbb{R}$. If $x \in \mathbb{R}$, what is $\text{rel}(x)$?

Problem 7.24. Suppose R is a relation on $A = \{1, 2, 3, 4, 5\}$ such that $\text{rel}(1) = \{1, 3, 4\}$, $\text{rel}(2) = \{4\}$, $\text{rel}(3) = \{3, 4, 5\}$, $\text{rel}(4) = \{1, 2\}$, and $\text{rel}(5) = \emptyset$. List the ordered pairs in R and draw the corresponding digraph.

We will now examine three important properties that a relation on a set may or may not possess.

Definition 7.25. Let R be a relation on a set A.

(a) The relation R is **reflexive** if for all $a \in A$, aRa.

(b) The relation R is **symmetric** if for all $a, b \in A$, if aRb, then bRa.

(c) The relation R is **transitive** if for all $a, b, c \in A$, if aRb and bRc, then aRc.

Example 7.26. Here are a few examples that illustrate the concepts in the previous definition.

(a) The relation $=$ on $\mathbb{R}$ is reflexive, symmetric, and transitive.

(b) The relation $\leq$ is reflexive and transitive on $\mathbb{R}$, but not symmetric. However, notice that $<$ is transitive on $\mathbb{R}$, but neither symmetric nor reflexive.

(c) If S is a set, then $\subseteq$ on $\mathcal{P}(S)$ is reflexive and transitive, but not symmetric.

Problem 7.27. Determine whether the relations given in each of the following is reflexive, symmetric, or transitive.

(a) Example 7.4

(b) Problem 7.13

Problem 7.28. Suppose R is a relation on a set A.

(a) Explain what it means for R to *not* be reflexive.

(b) Explain what it means for R to *not* be symmetric.

(c) Explain what it means for R to *not* be transitive.

Problem 7.29. Let $A = \{a, b, c, d, e\}$.

(a) Define a relation R on A that is reflexive, but not symmetric or transitive.

(b) Define a relation S on A that is symmetric, but not reflexive or transitive.

(c) Define a relation T on A that is transitive, but not reflexive or symmetric.

Problem 7.30. Given a relation R on a finite set A, describe what each of reflexive, symmetric, and transitive look like in terms of a digraph. That is, draw pictures that represent each of reflexive, symmetric, and transitive. One thing to keep in mind is that the elements used in the definitions of symmetric and transitive do not have to be distinct. So, you might need to consider multiple cases.

Below, we provide skeleton proofs for proving that a relation is reflexive, symmetric, or transitive. Notice that the skeleton proof for proving that a relation is reflexive is a special case of Skeleton Proof 2.81. Similarly, the skeleton proofs involving symmetric and transitive are both special cases of Skeleton Proof 2.82. It is important to point out that every relation on the empty set is vacuously reflexive, symmetric, and transitive. In the skeleton proofs below, we are implicitly assuming that the set in question is nonempty. In some circumstances, it may be necessary to mention the possibility of the empty set.

Skeleton Proof 7.31 (Proof that a relation is reflexive)**.** Here is the general structure for proving that a relation is reflexive.

Proof. Assume R is a relation on A defined by (or satisfying)... *[Use the given definition (or describe the given property) of R].* Let $a \in A$.

... *[Use the definition (or property) of R to verify that aRa]* ...

Therefore, the relation R is reflexive on A. □

Skeleton Proof 7.32 (Proof that a relation is symmetric)**.** Here is the general structure for proving that a relation is symmetric.

Proof. Assume R is a relation on A defined by (or satisfying)... *[Use the given definition (or describe the given property) of R].* Let $a, b \in A$ and suppose aRb.

... [Use assumption that aRb with definition (or property) of R to verify that bRa] ...

Therefore, the relation R is symmetric on A. □

Skeleton Proof 7.33 (Proof that a relation is transitive)**.** Here is the general structure for proving that a relation is transitive.

Proof. Assume R is a relation on A defined by (or satisfying)... *[Use the given definition (or describe the given property) of R].* Let $a, b, c \in A$ and suppose aRb and bRc.

... [Use assumption that aRb and bRc with definition (or property) of R to verify that aRc] ...

Therefore, the relation R is transitive on A. □

Problem 7.34. Determine whether each of the following relations is reflexive, symmetric, or transitive. In each case, you should either provide a specific counterexample or a proof.

(a) Consider the relation T described in Example 7.5.

(b) Consider the relation F described in Problem 7.21.

(c) Consider the relation $\equiv_5$ described in Problem 7.22.

(d) Let P be the set of all people and define H via xHy if x and y have the same height.

(e) Let P be the set of all people and define T via xTy if x is taller than y.

(f) Consider the relation "divides" on $\mathbb{N}$.

(g) Let L be the set of lines and define $\|$ via $l_1 \| l_2$ if l_1 is parallel to l_2.

(h) Let $C[0,1]$ be the set of continuous functions on $[0,1]$. Define $f \sim g$ if

$$\int_0^1 |f(x)|\,dx = \int_0^1 |g(x)|\,dx.$$

(i) Define R on $\mathbb{N}$ via nRm if $n+m$ is even.

(j) Define D on $\mathbb{R}$ via $(x,y) \in D$ if $x = 2y$.

(k) Define F on $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ via $(a,b)F(c,d)$ if $ad = bc$. Do you recognize this relation? Think about fractions.

(l) Define $\sim$ on $\mathbb{R}^2$ via $(x_1, y_1) \sim (x_2, y_2)$ if $x_1^2 + y_1^2 = x_2^2 + y_2^2$.

(m) Define S on $\mathbb{R}$ via xSy if $\lfloor x \rfloor = \lfloor y \rfloor$, where $\lfloor x \rfloor$ is the greatest integer less than or equal to x (e.g., $\lfloor \pi \rfloor = 3$, $\lfloor -1.5 \rfloor = -2$, and $\lfloor 4 \rfloor = 4$).

(n) Define C on $\mathbb{R}$ via xCy if $|x - y| < 1$.

> Most of what we believe, we believe because it was told to us by someone we trusted. What I would like to suggest, however, is that if we rely too much on that kind of education, we could find in the end that we have never really learned anything.
>
> Paul Wallace, physicist & theologian

7.2 Equivalence Relations

As we have seen in the previous section, the notions of reflexive, symmetric, and transitive are independent of each other. That is, a relation may have some combination of these properties, possibly none of them and possibly all of them. However, we have a special name for when a relation satisfies all three properties.

Definition 7.35. Let $\sim$ be a relation on a set A. Then $\sim$ is called an **equivalence relation** on A if $\sim$ is reflexive, symmetric, and transitive.

The symbol "$\sim$" is usually pronounced as "twiddle" or "tilde" and the phrase "$a \sim b$" could be read as "a is related to b" or "a twiddles b".

Problem 7.36. Let $A = \{1, 2, 3, 4, 5, 6\}$ and define

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

Using R, complete each of the following.

(a) Draw the digraph for R.

(b) Determine whether R is an equivalence relation on A.

(c) Find Rel(R) by determining rel(x) for each $x \in A$.

Problem 7.37. Let $A = \{a, b, c, d, e\}$.

(a) Make up an equivalence relation $\sim$ on A by drawing a digraph such that a is not related to b and c is not related to b.

(b) Using your digraph, find Rel($\sim$) by determining rel(x) for each $x \in A$.

Problem 7.38. Given a finite set A and an equivalence relation $\sim$ on A, describe what the corresponding digraph would have to look like.

Problem 7.39. Determine which relations given in Problem 7.34 are equivalence relations.

Problem 7.40. Let $\mathcal{T}$ be the set of all triangles and define $\sim$ on $\mathcal{T}$ via $T_1 \sim T_2$ if T_1 is similar to T_2. Determine whether $\sim$ is an equivalence relation on $\mathcal{T}$.

Problem 7.41. If possible, construct an equivalence relation on the empty set. If this is not possible, explain why.

Theorem 7.42. Suppose $\sim$ is an equivalence relation on a set A and let $a, b \in A$. Then $\text{rel}(a) = \text{rel}(b)$ if and only if $a \sim b$.

Theorem 7.43. Suppose $\sim$ is an equivalence relation on a set A. Then

(a) $\bigcup_{a \in A} \text{rel}(a) = A$, and

(b) For all $a, b \in A$, either $\text{rel}(a) = \text{rel}(b)$ or $\text{rel}(a) \cap \text{rel}(b) = \emptyset$.

In light of Theorem 7.43, we have the following definition.

Definition 7.44. If $\sim$ is an equivalence relation on a set A, then for each $a \in A$, we refer to $\text{rel}(a)$ as the **equivalence class** of a.

When $\sim$ is an equivalence relation on a set A, it is common to write each equivalence class $\text{rel}(a)$ as $\boxed{[a]}$ (or sometimes $\overline{a}$). The element a inside the square brackets is called the **representative of the equivalence class** $[a]$. Theorem 7.42 implies that an equivalence class can be represented by any element of the equivalence class. For example, in Problem 7.36, we have $[1] = [6]$ since 1 and 6 are in the same equivalence class. The collection of equivalence classes $\text{Rel}(\sim)$ is often denoted by $\boxed{A/\sim}$, which is read as "A modulo $\sim$" or "A mod $\sim$". The collection $A/\sim$ is sometimes referred to as the **quotient of** A **by** $\sim$.

Example 7.45. Let P denote the residents of a particular town and define $\sim$ on P via $a \sim b$ if a and b have the same last name. It is easily seen that this relation is reflexive, symmetric, and transitive, and hence $\sim$ is an equivalence relation on P. The equivalence classes correspond to collections of individuals with the same last name. For example, Maria Garcia, Anthony Garcia, and Ariana Garcia all belong to the same equivalence class. Any Garcia can be used as a representative for the corresponding equivalence class, so we can denote it as [Maria Garcia], for example. The collection $P/\sim$ consists of the various sets of people with the same last name. In particular, [Maria Garcia] $\in P/\sim$.

Example 7.46. The five distinct sets of relatives that you identified in Problem 7.22 are the equivalence classes for $\equiv_5$ on $\mathbb{Z}$. These equivalence classes are often called the **congruence classes modulo 5**.

The upshot of Theorem 7.43 is that given an equivalence relation, every element lives in exactly one equivalence class. In the next section, we will see that we can run this in reverse. That is, if we separate out the elements of a set so that every element is an element of exactly one subset, then this determines an equivalence relation.

Problem 7.47. If $\sim$ is an equivalence relation on a finite set A, describe $A/\sim$ in terms of the digraph corresponding to $\sim$.

Problem 7.48. For each of the equivalence relations you identified in Problem 7.39, succinctly describe the corresponding equivalence classes.

Problem 7.49. Suppose R and S are both equivalence relations on a set A. Is $R \cap S$ an equivalence relation on A? If so, prove it. Otherwise, provide a counterexample.

Problem 7.50. Suppose R and S are both equivalence relations on a set A. Is $R \cup S$ an equivalence relation on A? If so, prove it. Otherwise, provide a counterexample.

> Mathematics has beauty and romance. It's not a boring place to be, the mathematical world. It's an extraordinary place; it's worth spending time there.
>
> Marcus du Sautoy, mathematician

7.3 Partitions

Theorems 7.42 and 7.43 imply that if $\sim$ is an equivalence relation on a set A, then $\sim$ breaks A up into pairwise disjoint "chunks", where each chunk is some $[a]$ for $a \in A$. As you have probably already noticed, equivalence relations are intimately related to the following concept.

Definition 7.51. A collection Ω of subsets of a set A is said to be a **partition** of A if the elements of Ω satisfy:

(a) Each $X \in \Omega$ is nonempty,

(b) For all $X, Y \in \Omega$, $X \cap Y = \emptyset$ when $X \neq Y$, and

(c) $\bigcup_{X \in \Omega} X = A$.

That is, the elements of Ω are pairwise disjoint nonempty sets and their union is all of A. Each $X \in \Omega$ is called a **block** of the partition.

Example 7.52. Consider the equivalence relation $\sim$ on the set P described in Example 7.45. Recall that the equivalence classes correspond to collections of individuals with the same last name. Since each equivalence class is nonempty and each resident of the town belongs to exactly one equivalence class, the collection of equivalence classes forms a partition of P. That is, $P/\sim$ is a partition of P, where the blocks of the partition correspond to sets of residents with the same last name.

Example 7.53. Each of the following is an example of a partition of the set given in parentheses.

(a) Democrat, Republican, Independent, Green Party, Libertarian, etc. (set of registered voters)

(b) Freshman, sophomore, junior, senior (set of high school students)

(c) Evens, odds (set of integers)

(d) Rationals, irrationals (set of real numbers)

Example 7.54. Let $A = \{a, b, c, d, e, f\}$ and $\Omega = \{\{a\}, \{b, c, d\}, \{e, f\}\}$. Since the elements of Ω are pairwise disjoint nonempty subsets of A such that their union is all of A, Ω is a partition of A consisting of three blocks.

Problem 7.55. Consider the set A from Example 7.54.

(a) Find a partition of A consisting of four blocks.

(b) Find a collection of subsets of A that does *not* form a partition. See how many ways you can prevent your collection from being a partition.

Problem 7.56. For each of the following, find a partition of $\mathbb{Z}$ with the given properties.

(a) A partition of $\mathbb{Z}$ that consists of finitely many blocks, where each of the blocks is infinite.

(b) A partition of $\mathbb{Z}$ that consists of infinitely many blocks, where each of the blocks is finite.

(c) A partition of $\mathbb{Z}$ that consists of infinitely many blocks, where each of the blocks is infinite.

Problem 7.57. For each relation in Problem 7.34, determine whether the corresponding collection of the sets of relatives forms a partition of the given set.

Problem 7.58. Can we partition the empty set? If so, describe a partition. If not, explain why.

The next theorem spells out half of the close connection between partitions and equivalence relations. Theorem 7.73 yields the other half.

Theorem 7.59. If $\sim$ is an equivalence relation on a nonempty set A, then $A/\sim$ forms a partition of A.

Problem 7.60. In the previous theorem, why did we require A to be nonempty?

Problem 7.61. Consider the equivalence relation

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

on the set $A = \{1, 2, 3, 4, 5, 6\}$. Find the partition determined by Rel($\sim$).

It turns out that we can reverse the situation, as well. That is, given a partition, we can form an equivalence relation such that the equivalence classes correspond to the blocks of the partition. Before proving this, we need a definition.

Definition 7.62. Let A be a set and Ω any collection of subsets of A (not necessarily a partition). Define the relation R_Ω on A via $aR_\Omega b$ if there exists $X \in \Omega$ that contains both a and b. This relation is called the **relation on** A **associated to** Ω.

In other words, two elements are related exactly when they are in the same subset.

Problem 7.63. Let $A = \{a, b, c, d, e, f\}$ and let $\Omega = \{\{a, c\}, \{b, c\}, \{d, f\}\}$. List the ordered pairs in R_Ω and draw the corresponding digraph.

Problem 7.64. Let A and Ω be as in Example 7.54. List the ordered pairs in R_Ω and draw the corresponding digraph.

Problem 7.65. Consider Problem 7.24. Find the relation on A associated to $\mathrm{Rel}(\sim)$ and compare with what you obtained for R in Problem 7.24.

Problem 7.66. Give an example of a set A and a collection Ω from $\mathcal{P}(A)$ such that the relation R_Ω is not reflexive.

Problem 7.67. Let $A = \{1, 2, 3, 4, 5, 6\}$ and $\Omega = \{\{1, 3, 4\}, \{2, 4\}, \{3, 4\}, \{6\}\}$.

1. Is Ω a partition of A?
2. Find R_Ω by listing ordered pairs or drawing a digraph.
3. Is R_Ω an equivalence relation?
4. Find $\mathrm{Rel}(R_\Omega)$ (i.e., the collection of subsets of A determined by R_Ω). How are Ω and $\mathrm{Rel}(R_\Omega)$ related?

Theorem 7.68. If Ω is a collection of subsets of a nonempty set A (not necessarily a partition) such that

$$\bigcup_{X \in \Omega} X = A,$$

then R_Ω is reflexive.

Problem 7.69. Is it necessary to require A to be nonempty in Theorem 7.68?

Theorem 7.70. If Ω is a collection of subsets of a set A (not necessarily a partition), then R_Ω is symmetric.

Theorem 7.71. If Ω is a collection of subsets of a set A (not necessarily a partition) such that the elements of Ω are pairwise disjoint, then R_Ω is transitive.

Problem 7.72. Why didn't we require A to be nonempty in Theorems 7.70 and 7.71?

Recall that Theorem 7.59 says that the equivalence classes for a relation on a nonempty set A determines a partition of A. The following theorem tells us that every partition of a set yields an equivalence relation where the equivalence classes correspond to the blocks of the partition. This result is a consequence of Theorems 7.68, 7.70, and 7.71.

Theorem 7.73. If Ω is a partition of a set A, then R_Ω is an equivalence relation.

Together, Theorems 7.59 and 7.73 tell us that equivalence relations and partitions are two different ways of viewing the same thing.

Corollary 7.74. If R is a relation on a nonempty set A such that the collection of the set of relatives with respect to R is a partition of A, then R is an equivalence relation.

Problem 7.75. Let $A = \{\circ, \triangle, \blacktriangle, \square, \blacksquare, \bigstar, \odot, \circledcirc\}$. Make up a partition Ω on A and then draw the digraph corresponding to R_Ω.

> In the broad light of day mathematicians check their equations and their proofs, leaving no stone unturned in their search for rigour. But, at night, under the full moon, they dream, they float among the stars and wonder at the miracle of the heavens. They are inspired. Without dreams there is no art, no mathematics, no life.
>
> Michael Atiyah, mathematician

7.4 Modular Arithmetic

In this section, we look at a particular family of equivalence relations on the integers and explore the way in which arithmetic interacts with them.

Definition 7.76. For each $n \in \mathbb{N}$, define $n\mathbb{Z}$ to be the set of all integers that are divisible by n. In set-builder notation, we have

$$\boxed{n\mathbb{Z} := \{m \in \mathbb{Z} \mid m = nk \text{ for some } k \in \mathbb{Z}\}}.$$

For example, $5\mathbb{Z} = \{\ldots, -10, -5, 0, 5, 10, \ldots\}$ and $2\mathbb{Z}$ is the set of even integers.

Problem 7.77. Consider the sets $3\mathbb{Z}$, $5\mathbb{Z}$, $15\mathbb{Z}$, and $20\mathbb{Z}$.

(a) List at least five elements in each of the above sets.

(b) Notice that $3\mathbb{Z} \cap 5\mathbb{Z} = n\mathbb{Z}$ for some $n \in \mathbb{N}$. What is n? Describe $15\mathbb{Z} \cap 20\mathbb{Z}$ in a similar way.

(c) Draw a Venn diagram illustrating how the sets $3\mathbb{Z}$, $5\mathbb{Z}$, and $15\mathbb{Z}$ intersect.

(d) Draw a Venn diagram illustrating how the sets $5\mathbb{Z}$, $15\mathbb{Z}$, and $20\mathbb{Z}$ intersect.

Theorem 7.78. Let $n \in \mathbb{N}$. If $a, b \in n\mathbb{Z}$, then $-a$, $a+b$, and ab are also in $n\mathbb{Z}$.

Definition 7.79. For each $n \in \mathbb{N}$, define the relation $\boxed{\equiv_n}$ on $\mathbb{Z}$ via $a \equiv_n b$ if $a - b \in n\mathbb{Z}$. We read $a \equiv_n b$ as "a is congruent to b modulo n."

Note that $a - b \in n\mathbb{Z}$ if and only if n divides $a - b$, which implies that $a \equiv_n b$ if and only if n divides $a - b$.

Example 7.80. We encountered $\equiv_5$ in Problem 7.22 and discovered that there were five distinct sets of relatives. In particular, we have

$$\begin{aligned}
\text{rel}(0) &= \{\ldots, -10, -5, 0, 5, 10, \ldots\} \\
\text{rel}(1) &= \{\ldots, -9, -4, 1, 6, 11, \ldots\} \\
\text{rel}(2) &= \{\ldots, -8, -3, 2, 7, 12, \ldots\} \\
\text{rel}(3) &= \{\ldots, -7, -2, 3, 8, 13, \ldots\} \\
\text{rel}(4) &= \{\ldots, -6, -1, 4, 9, 14, \ldots\}.
\end{aligned}$$

Notice that this collection forms a partition of $\mathbb{Z}$. By Corollary 7.74, the relation $\equiv_5$ must be an equivalence relation.

The previous example generalizes as expected. You can prove the following theorem by either proving that $\equiv_n$ is reflexive, symmetric, and transitive or by utilizing Corollary 7.74.

Theorem 7.81. For $n \in \mathbb{N}$, the relation $\equiv_n$ is an equivalence relation on $\mathbb{Z}$.

We have have special notation and terminology for the equivalence classes that correspond to $\equiv_n$.

Definition 7.82. For $n \in \mathbb{N}$, let $\boxed{[a]_n}$ denote the equivalence class of a with respect to $\equiv_n$ (see Definitions 7.17 and 7.44). The equivalence class $[a]_n$ is called the **congruence** (or **residue**) **class of** a **modulo** n. The collection of all equivalence classes determined by $\equiv_n$ is denoted $\boxed{\mathbb{Z}/n\mathbb{Z}}$, which is read "$\mathbb{Z}$ modulo $n\mathbb{Z}$".

Example 7.83. Let's compute $[2]_7$. Tracing back through the definitions, we see that

$$\begin{aligned}
m \in [2]_7 &\iff m \equiv_7 2 \\
&\iff m - 2 \in 7\mathbb{Z} \\
&\iff m - 2 = 7k \text{ for some } k \in \mathbb{Z} \\
&\iff m = 7k + 2 \text{ for some } k \in \mathbb{Z}.
\end{aligned}$$

Since the multiples of 7 are $7\mathbb{Z} = \{\ldots, -14, -7, 0, 7, 14, \ldots\}$, we can find $[2]_7$ by adding 2 to each element of $7\mathbb{Z}$ to get $[2]_7 = \{\ldots, -12, -5, 2, 9, 16, \ldots\}$.

Problem 7.84. For each of the following congruence classes, find five elements in the set such that at least one is greater than 70 and one is less than 70.

(a) $[4]_7$

(b) $[-3]_7$

(c) $[7]_7$

Problem 7.85. Describe $[0]_3$, $[1]_3$, $[2]_3$, $[4]_3$, and $[-2]_3$ as lists of elements as in Example 7.83. How many distinct congruence classes are in $\mathbb{Z}/3\mathbb{Z}$? Theorem 7.43 might be helpful.

Consider using Theorem 7.42 to prove the next theorem.

Theorem 7.86. For $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$, $[a]_n = [b]_n$ if and only if n divides $a - b$.

Corollary 7.87. For $n \in \mathbb{N}$ and $a \in \mathbb{Z}$, $[a]_n = [0]_n$ if and only if n divides a.

The next result provides a useful characterization for when two congruence classes are equal. The Division Algorithm will be useful when proving this theorem.

Theorem 7.88. For $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$, $[a]_n = [b]_n$ if and only if a and b have the same remainder when divided by n.

When proving Part (a) of the next theorem, make use of Theorem 7.86. For Part (b), note that $a_1 b_1 - a_2 b_2 = a_1 b_1 - a_2 b_1 + a_2 b_1 - a_2 b_2$.

Theorem 7.89. Let $n \in \mathbb{N}$ and let $a_1, a_2, b_1, b_2 \in \mathbb{Z}$. If $[a_1]_n = [a_2]_n$ and $[b_1]_n = [b_2]_n$, then

(a) $[a_1 + b_1]_n = [a_2 + b_2]_n$, and

(b) $[a_1 \cdot b_1]_n = [a_2 \cdot b_2]_n$.

The previous theorem allows us to define addition and multiplication in $\mathbb{Z}/n\mathbb{Z}$.

Definition 7.90. Let $n \in \mathbb{N}$. We define the sum and product of congruence classes in $\mathbb{Z}/n\mathbb{Z}$ via

$$[a]_n + [b]_n := [a + b]_n \quad \text{and} \quad [a]_n \cdot [b]_n := [a \cdot b]_n.$$

Example 7.91. By Definition 7.90, $[2]_7 + [6]_7 = [2+6]_7 = [8]_7$. By Theorem 7.86, $[8]_7 = [1]_7$, and so $[2]_7 + [6]_7 = [1]_7$. Similarly, $[2]_7 \cdot [6]_7 = [2 \cdot 6]_7 = [12]_7 = [5]_7$.

Addition and multiplication for $\mathbb{Z}/n\mathbb{Z}$ has many familiar—and some not so familiar—properties. For example, addition and multiplication of congruence classes are both associative and commutative. However, it is possible for $[a]_n \cdot [b]_n = [0]_n$ even when $[a]_n \neq [0]_n$ and $[b]_n \neq [0]_n$.

Theorem 7.92. If $n \in \mathbb{N}$, then addition in $\mathbb{Z}/n\mathbb{Z}$ is commutative and associative. That is, for all $[a]_n, [b]_n, [c]_n \in \mathbb{Z}/n\mathbb{Z}$, we have

(a) $[a]_n + [b]_n = [b]_n + [a]_n$, and

(b) $([a]_n + [b]_n) + [c]_n = [a]_n + ([b]_n + [c]_n)$.

Theorem 7.93. If $n \in \mathbb{N}$, then multiplication in $\mathbb{Z}/n\mathbb{Z}$ is commutative and associative. That is, for all $[a]_n, [b]_n, [c]_n \in \mathbb{Z}/n\mathbb{Z}$, we have

(a) $[a]_n \cdot [b]_n = [b]_n \cdot [a]_n$, and

(b) $([a]_n \cdot [b]_n) \cdot [c]_n = [a]_n \cdot ([b]_n \cdot [c]_n)$.

One consequence of Theorems 7.92(b) and 7.93(b) is that parentheses are not needed when adding or multiplying congruence classes. The next theorem follows from Definition 7.90 together with Theorems 7.92(b) and 7.93(b) and induction on k.

Theorem 7.94. Let $n \in \mathbb{N}$. For all $k \in \mathbb{N}$, if $[a_1]_n, [a_2]_n, \ldots, [a_k]_n \in \mathbb{Z}/n\mathbb{Z}$, then

(a) $[a_1]_n + [a_2]_n + \cdots + [a_k]_n = [a_1 + a_2 + \cdots + a_k]_n$, and

(b) $[a_1]_n [a_2]_n \cdots [a_k]_n = [a_1 a_2 \cdots a_k]_n$.

The next result is a special case of Theorem 7.94(b).

Corollary 7.95. Let $n \in \mathbb{N}$. If $a \in \mathbb{Z}$ and $k \in \mathbb{N}$, then $([a]_n)^k = [a^k]_n$

Example 7.96. Let's compute $[8^{179}]_7$. We see that

$$\begin{aligned} [8^{179}]_7 &= ([8]_7)^{179} && \text{(Corollary 7.95)} \\ &= ([1]_7)^{179} && \text{(Theorem 7.86)} \\ &= [1^{179}]_7 && \text{(Corollary 7.95)} \\ &= [1]_7. \end{aligned}$$

For Part (a) in the next problem, use the fact that $[6]_7 = [-1]_7$. For Part (b), use the fact that $[2^3]_7 = [1]_7$.

Problem 7.97. For each of the following, find a number a with $0 \leq a \leq 6$ such that the given quantity is equal to $[a]_7$.

(a) $[6^{179}]_7$

(b) $[2^{300}]_7$

(c) $[2^{301} + 5]_7$

Problem 7.98. Find a and b such that $[a]_6 \cdot [b]_6 = [0]_6$ but $[a]_6 \neq [0]_6$ and $[b]_6 \neq [0]_6$.

Theorem 7.99. If $n \in \mathbb{N}$ such that n is not prime, then there exists $[a]_n, [b]_n \in \mathbb{Z}/n\mathbb{Z}$ such that $[a]_n \cdot [b]_n = [0]_n$ while $[a]_n \neq [0]_n$ and $[b]_n \neq [0]_n$.

Problem 7.100. Notice that $2x = 1$ has no solution in $\mathbb{Z}$. Show that $[2]_7 [x]_7 = [1]_7$ does have a solution with x in $\mathbb{Z}$. What about $[14]_7 [x]_7 = [1]_7$?

Make use of Theorem 7.94, Corollary 7.95, and Theorem 7.86 to prove the following theorem.

Theorem 7.101. If $m \in \mathbb{N}$ such that

$$m = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0,$$

where $a_k, a_{k-1}, \ldots, a_1, a_0 \in \{0, 1, \ldots, 9\}$ (i.e., $a_k, a_{k-1}, \ldots, a_1, a_0$ are the digits of m), then

$$[m]_3 = [a_k + a_{k-1} + \cdots + a_1 + a_0]_3.$$

You likely recognize the next result. Its proof follows quickly from Corollary 7.87 together with the previous theorem.

Theorem 7.102. An integer is divisible by 3 if and only if the sum of its digits is divisible by 3.

Let's revisit Theorem 4.21, which we originally proved by induction.

Problem 7.103. Use Corollary 7.87 to prove that for all integers $n \geq 0$, $3^{2n} - 1$ is divisible by 8. You will need to handle the case involving $n = 0$ separately.

We close this chapter with a fun problem.

Problem 7.104. Prove or provide a counterexample: No integer n exists such that $4n + 3$ is a perfect square.

> Without change something sleeps inside us, and seldom awakens. The sleeper must awaken.
>
> *Dune* by Frank Herbert