Relations – Chapter 11 of Hammack

Dr. Doreen De Leon
Math 111, Fall 2014

11.0 Relations

Symbols such as $<$, $\leq$, $=$, $|$, $\nmid$, $>$, $\geq$, $\in$, $\subseteq$, etc. are called **relations** because they describe relationships among things.

The goal of this chapter is to give you a good understanding of relations by discussing a general theory of relations.

Definition. A **relation** on a set A is a subset $R \subseteq A \times A$. The statement $(x, y) \in R$ is often written $x \, R \, y$, and the statement $(x, y) \notin R$ is often written $x \not\!R \; y$.

Note: Take special note of the fact that a relation is defined on a set.

Example: Let $A = \{1, 2, 3, 4\}$. The following sets are relations on A.

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

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

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

Note that:

1. The set R is a relation on A. Since $(2, 1) \in R$, we can write $2 \, R \, 1$. Since $(3, 4) \notin R$, we say $3 \not\!R \; 4$. What relation does R represent? We see that $y \leq x$ for all $(x, y) \in R$, and all such pairs of elements in A are in R, so R represents $x \geq y$.

2. The set S contains pairs of numbers having the same parity, and all such pairs of elements in A are in S, so S is the relation on A for which both numbers have the same parity. So, $2 \, S \, 4$ means that 2 has the same parity as 4.

3. Finally, $R \cap S$ is a relation because $R \cap S \subseteq A \times A$ and so it satisfies the definition of a relation. What relation does this represent? Relation $R \cap S$ represents: $x \geq y$, where x and y have the same parity. To write $(x, y) \in R \cap S$, we write $x \, (R \cap S) \, y$.

Relations can be infinite. For example, the set $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} : x \neq y\} \subseteq \mathbb{R} \times \mathbb{R}$ is an infinite relation, because there are infinitely many real numbers x and y that satisfy it.

11.1 Properties of Relations

For a relation defined on a set A, there are properties that a relation may have and which are of particular interest to us.

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

1. Relation R is **reflexive** if $x\,R\,x$ for every $x \in A$.
2. Relation R is **symmetric** if $x\,R\,y$ implies $y\,R\,x$ for all $x, y \in A$.
3. Relation R is **transitive** if whenver $x\,R\,y$ and $y\,R\,z$, then also $x\,R\,z$. In other words, R is transitive if $\forall x, y, z \in A, ((x\,R\,y) \wedge (y\,R\,z)) \implies x\,R\,z$.

Notes:

1. Showing that a relation R on a set A is reflexive requires proving a statement of the form $\forall a \in A,\ a\,R\,a$.
2. Showing that a relation on a set is symmetric requires proving a conditional statement of the form $P \implies Q$ for all $x, y \in A$, where $P : x\,R\,y$ and $Q : y\,R\,x$.
3. Showing that a relation on a set is transitive requires proving a conditional statement of the form $P \implies Q$ for all $x, y, z \in A$, where $P : (x\,R\,y) \wedge (y\,R\,z)$ and $Q : x\,R\,z$.

Notes:

1. To show that a relation is not reflexive, we need to show that $\sim (\forall a \in A,\ a\,R\,a)$, or $\exists a \in A,\ a \not R\ a$.
2. To show that a relation is not symmetric or is not transitive means that we need to prove $\sim (P \implies Q)$, or $P \wedge \sim Q$, where P and Q are as given above.

We will look at the examples of R, S, and $R \cap S$ defined previously.

1. Relation R is reflexive: for each $a \in A$, $a\,R\,a$. Relation R is not symmetric ($2\,R\,1$, but $1 \not R\ 2$), but it is transitive. Why? Let $a, b, c \in A$. If $a\,R\,b$ and $b\,R\,c$, we have that $a \geq b$ and $b \geq c$, which implies $a \geq c$, or $a\,R\,c$.
2. Relation S is reflexive, symmetric, and transitive. For each $a \in A$, $a\,S\,a$, so S is reflexive. Relation S is symmetric because: if $a, b \in A$ and $a\,S\,b$, then a and b have the same parity, so it follows that $b\,S\,a$. Finally, let $a, b, c \in A$. If $a\,S\,b$ and $b\,S\,c$, then we have that a and b have the same parity, and b and c has the same parity, so since a has the same parity as b, which is the same parity as c, a has the same parity as c, or $a\,S\,c$.

3. Relation $R \cap S$ is reflexive and transitive, but not symmetric. Why? It is reflexive because for all $a \in A$, we have $a\,(R \cap S)\,a$. It is transitive because of the following. Let $a, b, c \in A$. If $a\,(R \cap S)\,b$ and $b\,(R \cap S)\,c$, then $a \geq b$ and $b \geq c$ and both a and b and b and c have the same parity. It therefore follows that $a \geq c$ and a and c have the same parity, so $a\,(R \cap S)\,c$. Relation $R \cap S$ is not symmetric because although $3\,(R \cap S)\,1$, it is not true that $1\,(R \cap S)\,3$.

Examples: Let $S = \{a, b, c\}$. Determine which of these properties (if any) are possessed by the following sets.

(1) $R_1 = \{(a, b), (b, a), (c, a)\}$

(2) $R_2 = \{(a, b), (b, b), (b, c), (c, b), (c, c)\}$

(3) $R_3 = \{(a, a), (a, c), (b, b), (c, a), (c, c)\}$

(4) $R_4 = \{(a, a), (a, b), (b, b), (b, c), (a, c)\}$

(5) $R_5 = \{(a, a), (a, b)\}$

(6) $R_6 = \{(a, b), (a, c)\}$

Solution:

(1) Relation R_1 possesses none of these properties. It is not reflexive since $(a, a) \notin R_1$. It is not symmetric since $(c, a) \in R_1$ but $(a, c) \notin R_1$. It is not transitive because $(a, b) \in R_1$ and $(b, a) \in R_1$, but $(a, a) \notin R_1$.

(2) Relation R_2 also possesses none of these properties. It is not reflexive since $(a, a) \notin R_2$. It is not symmetric since $(a, b) \in R_2$ but $(b, a) \notin R_2$. And it is not transitive because $(a, b), (b, c) \in R_2$, but $(a, c) \notin R_2$.

(3) Relation R_3 is reflexive, symmetric, and transitive.

(4) Relation R_4 is transitive.

(5) Relation R_5 is transitive. Why? To be transitive, $\forall x, y, z \in S$, we must have $(x\,R_5\,y) \wedge (y\,R_5\,z) \implies x\,R_5\,z$. Since the only two pairs in R_5 are (a, a) and (a, b), $(x, y) \in R_5 \implies x = a$ and $y = a$ or $x = a$ and $y = b$. If $(x, y) = (a, a)$, then either $(y, z) = (a, a)$ or $(y, z) = (a, b)$. In the first case, we have $a\,R_5\,a$ and $a\,R_5\,a$, and $(x, z) = (a, a) \in R_5$. In the second case, $a\,R_5\,a$ and $a\,R_5\,b$, and $(x, z) = (a, b) \in R_5$. If $(x, y) = (a, b)$, there is no ordered pair in $(y, z) \in R_5$ such that $y = b$. For R_5, there are only two possibilities for two ordered pairs of the type (x, y) and (y, z), and in each case $(x, z) \in R_5$. Therefore, R_5 is transitive.

(6) Relation R_6 does not contain any ordered pairs of the form (x, y) and (y, z). Therefore, R_6 is transitive.

As another example, consider the infinite set $R = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} : a \neq b\}$. We see that R is not reflexive since $x \not R\, x$ for any $x \in \mathbb{Z}$. We do have that R is symmetric. Why? Finally, R is not transitive. Why? Let $x = 1$, $y = 2$, and $z = 1$. Then $x\,R\,y$ and $y\,R\,z$, but $x \not R\, z$.

Example (from text): Prove the following proposition.

Proposition 1. Let $n \in \mathbb{N}$. The relation $\equiv \pmod{n}$ is reflexive, symmetric, and transitive on $\mathbb{Z}$.

Proof. First, we show that $\equiv \pmod{n}$ is reflexive. Let $x \in \mathbb{Z}$. Then, since $n \mid 0$, $n \mid (x - x)$. Therefore, we have $x \equiv x \pmod{n}$, and since this is true for every $x \in \mathbb{Z}$, $\equiv \pmod{n}$ is reflexive.

Next, we will show that $\equiv \pmod{n}$ is symmetric. Let $x, y \in \mathbb{Z}$. Then if $x \equiv y \pmod{n}$, we have that $n \mid (x - y)$ and thus, $x - y = nr$ for some integer r. Multiplying both sides by -1 gives $y - x = -nr = n(-r)$. Since $-r \in \mathbb{Z}$, $n \mid (y - x)$, or $y \equiv x \mod n$. Since this is true for all $x, y \in \mathbb{Z}$, $\equiv \pmod{n}$ is symmetric.

Finally, we show that $\equiv \pmod{n}$ is transitive. Let $x, y, z \in \mathbb{Z}$ be integers such that $x \equiv y \pmod{n}$ and $y \equiv z \pmod{n}$. Then $n \mid (x - y)$ and $n \mid (y - z)$. Therefore, $x - y = nr$ and $y - z = ns$ for some integers r and s. Adding these equations together gives

$$x - z = nr + ns = n(r + s).$$

Since $r + s \in \mathbb{Z}$, $n \mid (x - z)$, or $x \equiv z \pmod{n}$. Therefore, $\equiv \pmod{n}$ is transitive. □

Exercise: Determine if the relation $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} : x - y \in \mathbb{Z}\}$ is reflexive, symmetric, and/or transitive on $\mathbb{R}$.

Solution: Relation R is reflexive, since $x - x = 0 \in \mathbb{Z}$, $x\,R\,x$.

Relation R is symmetric. Suppose $x\,R\,y$. Then $x - y = r$ for some integer r. So, $y - x = -r$, and $-r$ is an integer. Therefore, $y\,R\,x$.

Relation R is transitive, as well. Suppose $x\,R\,y$ and $y\,R\,z$. Then $x - y = r$ and $y - z = s$ for some integers r and s. Then

$$\begin{aligned} x - z &= x - y + y - z \\ &= r + s. \end{aligned}$$

Since $r + s \in \mathbb{Z}$, $x\,R\,z$.

11.2 Equivalence Relations

The relation $=$ on any set A is reflexive, symmetric, and transitive. There are many other relations that are also reflexive, symmetric, and transitive. Such relations appear frequently in mathemaitcs and often play important roles, a notable example being $=$.

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

Example: Consider the set $A = \{1, 2, 3, 4, 5, 6\}$ and the relation

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

defined on A. We may verify that this relation is reflexive, symmetric, and transitive and is, therefore, an equivalence relation.

Suppose that R is an equivalence relation on some set A. If $a \in A$, then a is related to a since R is reflexive. Other elements of A may also be related to a. The set of elements that are all related to a given element of A is importnat (as will later be seen), and it is given a special name.

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

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

Example: Consider the relation R on the set $A = \{1, 2, 3, 4, 5, 6\}$ defined in (1). The equivalence classes are

$$\begin{array}{lll} [1] = \{1, 3, 6\} & [2] = \{2, 4\} & [3] = \{1, 3, 6\} \\ [4] = \{2, 4\} & [5] = \{5\} & [6] = \{1, 3, 6\}. \end{array}$$

Note that $[1] = [3] = [6]$ and $[2] = [4]$. Therefore, there are three distinct equivalence classes for R.

Example: Consider the equivalence relation defined on $\mathbb{Z}$ by $a\,R\,b$ if $a = b$ and determine the distinct equivalence classes for this relation.

Solution: For $a \in \mathbb{Z}$,

$$[a] = \{x \in \mathbb{Z} : x\,R\,a\} = \{x \in \mathbb{Z} : x = a\} = \{a\}.$$

Therefore, every integer is in an equivalence class by itself.

Example: Define a relation R on the set L of straight lines in a plane by $l_1\,R\,l_2$ if either $l_1 = l_2$ (i.e., the lines coincide) or if l_1 is parallel to l_2. Prove that R is an equivalence relation and determine the equivalence classes of R.

Solution: First, we need to show that R is an equivalence relation. Relation R is an equivalence relation if it is reflexive, symmetric, and transitive.

- Show R is reflexive. Every line is coincident to itself, so R is reflexive.

- Show R is symmetric. If a line l_1 is parallel to a line l_2, then l_2 is also parallel to l_1. This is also true if they coincide. Therefore, R is symmetric.

- Show R is transitive. Suppose that l_1 is parallel to (or coincides with) l_2 and that l_2 is parallel to (or coincides with) l_3. Then l_1 and l_3 are parallel or they coincide, so R is transitive.

Next, we determine the equivalence classes of R. Let $l \in L$. Then the equivalence class

$$[l] = \{x \in L : x\,R\,l\} = \{x \in L : x = l \text{ or } x \text{ is parallel to } l\}.$$

In other words, the equivalence class $[l]$ consists of l and all lines in the plane parallel to l. There is an equivalence class for each line $l \in L$.

Eample: Define the relation R on $\mathbb{Z}$ by $x\,R\,y$ if $x + 3y$ is even. Prove that R is an equivalence relation and determine the equivalence classes of R.

Solution: First, we show that R is an equivalence relation. Relation R is an equivalence relation if it is reflexive, symmetric, and transitive.

- Show R is reflexive. Let $a \in \mathbb{Z}$. Then $a+3a = 4a = 2(2a)$ is even since $2a \in \mathbb{Z}$. Therefore, R is reflexive.

- Show R is symmetric. Let $a, b \in \mathbb{Z}$ such that $a\,R\,b$. Then $a + 3b$ is even, so $a + 3b = 2k$ for some integer k. Therefore, $a = 2k - 3b$ and

  $$b + 3a = b + 3(2k - 3b) = b + 6k - 9b = 6k - 8b = 2(3k - 4b).$$

  Since $3k - 4b \in \mathbb{Z}$, we have $b\,R\,a$. Therefore, R is symmetric.

- Show R is transitive. Let $a, b, c \in \mathbb{Z}$ such that $a\,R\,b$ and $b\,R\,c$. Then $a + 3b$ is even, so $a + 3b = 2k$ for some integer k, and $b + 3c$ is even, so $b + 3c = 2l$ for some integer l. Adding the two equations gives $(a + 3b) + (b + 3c) = 2k + 2l$, or $a + 4b + 3c = 2k + 2l$. So, we have

  $$a + 3c = 2k + 2l - 4b = 2(k + l - 2b).$$

  Since $k + l - 2b \in \mathbb{Z}$, $a + 3c$ is even. Therefore, $a\,R\,c$ and so R is transitive.

Since R is an equivalence relation, there are equivalence classes for each $a \in \mathbb{Z}$. For example, if $a = 0$, then

$$[0] = \{x \in \mathbb{Z} : x\,R\,0\} = \{x \in \mathbb{Z} : x + 3 \cdot 0 \text{ is even}\} = \{x \in \mathbb{Z} : x \text{ is even}\} = \{0, \pm 2, \pm 4, \dots\}.$$

In other words, $[0]$ is the set of even integers. Suppose $a \in \mathbb{Z}$ is even, so $a = 2k$, where $k \in \mathbb{Z}$. Then

$$[a] = \{x \in \mathbb{Z} : x\,R\,a\} = \{x \in \mathbb{Z} : x + 3 \cdot a \text{ is even}\} = \{x \in \mathbb{Z} : x + 6k \text{ is even}\}.$$

But, this is just the set of even integers. Now, let's determine [1].

$$[1] = \{x \in \mathbb{Z} : x\,R\,1\} = \{x \in \mathbb{Z} : x+3\cdot 1 \text{ is even}\} = \{x \in \mathbb{Z} : x+3 \text{ is even}\} = \{\pm 1, \pm 3, \pm 5, \dots\}.$$

In other words, [1] is the set of odd integers. In fact, if b is an odd integer, then $b = 2l + 1$ for some integer l. We therefore see that

$$[b] = \{x \in \mathbb{Z} : x\,R\,b\} = \{x \in \mathbb{Z} : x+3b \text{ is even}\} = \{x \in \mathbb{Z} : x+3(2l+1) \text{ is even}\} = \{x \in \mathbb{Z} : x+6l+3 \text{ is even}\}.$$

But this is just the set of odd integers.

We see that if m and n are two even integers, then $[m] = [n]$, and if m and n are both odd integers, then $[m] = [n]$. Therefore, there are only two distinct equivalence classes, [0] and [1].

11.3 Equivalence Classes and Partitions

In this section, we will discuss some properties of equivalence classes.

Theorem 1. Suppose R is an equivalence relation on a set A. Suppose also that $a, b \in A$. Then $[a] = [b]$ if and only if $a\,R\,b$.

Proof. Suppose that $[a] = [b]$. Since R is reflexive, $a \in \{x \in A : x\,R\,a\} = [a] = [b] = \{x \in A : x\,R\,b\}$. Since $a \in \{x \in A : x\,R\,b\}$, we have that $a\,R\,b$.

Conversely, suppose that $a\,R\,b$. We need to show that $[a] = [b]$. We will do this by showing $[a] \subseteq [b]$ and $[b] \subseteq [a]$. Suppose $c \in [a] = \{x \in A : x\,R\,a\}$. Then $c\,R\,a$. Since R is transitive and we have that $c\,R\,a$ and $a\,R\,b$, it follows that $c\,R\,b$, so $c \in \{x \in A : x\,R\,b\} = [b]$. Therefore, $[a] \subseteq [b]$. Now suppose $c \in [b] = \{x \in A : x\,R\,b\}$. Then, $c\,R\,b$. Since $a\,R\,b$ and R is symmetric, we have that $b\,R\,a$. By the transitivity of R, we have $c\,R\,a$, so $c \in \{x \in A : x\,R\,a\} = [a]$. Therefore, $[b] \subseteq [a]$. Since $[a] \subseteq [b]$ and $[b] \subseteq [a]$, $[a] = [b]$. $\square$

Note that the last example we did for Section 11.2 actually illustrates this theorem.

Note: The theorem also tells us that if $a \not R\ b$, then $[a] \neq [b]$.

Definition. A **partition** of a set A is a set of non-empty subsets of A such that the union of all of the subsets equals A and the intersection of any two different subsets is $\varnothing$.

Example: Consider the set $A = \{1, 2, 3, 4, 5, 6\}$. Then one partition of A is $\{\{1, 2\}, \{3, 4\}, \{5, 6\}\}$. There are other partitions of A. Three other partitions of A are $\{\{1, 3, 5\}, \{2, 4, 6\}\}$, $\{\{1, 2, 3, 5\}, \{4, 6\}\}$, and $\{\{1\}, \{2\}, \{3\}, \{4\}, \{5\}, \{6\}\}$.

Theorem 2. Suppose R is an equivalence relation on a set A. Then the set $\{[a] : a \in A\}$ of equivalence classes of R forms a partition of A.

Proof. First, note that each equivalence class is nonempty, since $a \in [a]$ and so each element of A belongs to at least one equivalence class. We must show that every element of A belongs to exactly one equivalence class. Assume that some element $x \in A$ belongs to two equivalence classes, say $[a]$ and $[b]$. Since $x \in [a]$ and $x \in [b]$, it follows that $x\,R\,a$ and $x\,R\,b$. Because R is symmetric, $x\,R\,a = a\,R\,x$, so $a\,R\,x$. Thus, $a\,R\,x$ and $x\,R\,b$. Since R is transitive, $a\,R\,b$. Since $a\,R\,b$, by Theorem 1, $[a] = [b]$. So, any two equivalence classes to which x belongs are equal, so x belongs to a unique equivalence class. $\square$

It turns out that the coverse is also true, although the proof of the converse is more complicated.

Theorem 3. Let $P = \{A_\alpha : \alpha \in I\}$ be a partition of a non-empty set A. Then there exists an equivalence relation R on A such that $P = \{[a] : a \in A\}$.

Proof. Define a relation R on A by $x\,R\,y$ if x and y belong to the same subset in P; i.e., $x\,R\,y$ if $x, y \in A_\alpha$ for some $\alpha \in I$. We will show that R so defined is an equivalence relation. First, let $a \in A$. Since P is a partition of A, $a \in A_\beta$ for some $\beta \in I$. Then $a\,R\,a$ and R is reflexive.

Next, let $a, b \in A$ and assume that $a\,R\,b$. Then $a, b \in A_\gamma$ for some $\gamma \in I$. Therefore, b and a are elements of A_γ, and $b\,R\,a$ and R is symmetric.

Finally, let $a, b, c \in A$ and suppose that $a\,R\,b$ and $b\,R\,c$. So, $a, b \in A_\beta$ and $b, c \in A_\gamma$ for some $\beta, \gamma \in I$. Since P is a partition of A, b can only belong to one set in P. Therefore, $A_\beta = A_\gamma$ and so $a, c \in A_\beta$, or $a\,R\,c$. and R is transitive.

We now consider the equivalence classes resulting from R. Let $a \in A$. Then $a \in A_\alpha$ for some $\alpha \in I$. The equivalence class $[a]$ consists of all elements of A related to a. From our definition of R, the only elements related to a are those that belong to the same subset of P to which a belongs; i.e., $[a] = A_\alpha$. Therefore,

$$\{[a] : a \in A\} = \{A_\alpha : \alpha \in I\} = P.$$

$\square$

Example: Consider the partition $P = \{\{\ldots, -4, -2, 0, 2, 4, \ldots\}, \{\ldots, -5, 3, -1, 1, 3, 5, \ldots\}\}$ of $\mathbb{Z}$. Let R be the equivalence relation whose equivalence classes are the two elements of P. What equivalence relation is R?

Solution: If $x \in \{\ldots, -4, -2, 0, 2, 4, \ldots\}$, then x is an even number. If $y \in \{\ldots, -5, 3, -1, 1, 3, 5, \ldots\}$, then y is an odd number. So, $x = 2k$ and $y = 2l + 1$ for some integers k and l. This suggests that $[x] = [0]$ and $[y] = [1]$, so R is the relation $\equiv \pmod 2$ (or same parity).

11.4 The Integers Modulo n

Let's first consider the following theorem, which we have proved previously. We repeat the proof here.

Theorem 4. Let $n \in \mathbb{Z}$, where $n \geq 2$. Then congruence modulo n (i.e., the relation R defined on $\mathbb{Z}$ by $a\,R\,b$ if $a \equiv b \pmod{n}$) is an equivalence relation on $\mathbb{Z}$.

Proof. We need to show that R is reflexive, symmetric, and transitive.

Let $a \in \mathbb{Z}$. Since $n \mid 0$, it follows that $n \mid (a - a)$ and so $a \equiv a \pmod{n}$. Therefore, $a\,R\,a$ and R is reflexive.

Next, suppose that $a\,R\,b$, where $a, b \in \mathbb{Z}$. Then $a \equiv b \pmod{n}$, so $n \mid (a-b)$. Then $a - b = kn$ for some integer k. Multiplying both sides of this equation by -1 gives $b - a = (-k)n$. Since $-k \in \mathbb{Z}$, $n|(b-a)$ and so $b \equiv a \pmod{n}$. Therefore, $b\,R\,a$ and R is symmetric.

Finally, suppose that $a\,R\,b$ and $b\,R\,c$ for some $a, b, c \in \mathbb{Z}$. Then $n \mid (a-b)$ and $n \mid (b-c)$, and so $a - b = kn$ and $b - c = ln$ for some integers k and l. Adding these two equations gives

$$(a-b) + (b-c) = kn + ln, \text{ or } a - c = (k+l)n.$$

Since $k + l \in \mathbb{Z}$, $n \mid (a-c)$. Therefore, $a \equiv c \pmod{n}$, or $a\,R\,c$, and so R is transitive. $\square$

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

Let us consider, for example, $\mathbb{Z}_6$. Then $\mathbb{Z}_6 = \{[0], [1], [2], [3], [4], [5]\}$. From the definitions of addition and multiplication given in the definition, we have

$$[1] + [3] = [1+3] = [4] \text{ and } [1] \cdot [3] = [1 \cdot 3] = [3].$$

However, consider the following:

- $[2] + [4] = [6]$. But, what equivalence class is $[6]$ equivalent to? We know that $6 \equiv 0 \pmod{6}$, so $[6] = [0]$, and we have $[2] + [4] = [0]$.
- $[2] \cdot [4] = [8]$. Again, we need to determine to what equivalence class $[8]$ corresponds. Since $8 \equiv 2 \pmod{6}$, we have $[8] = [2]$, so $[2] \cdot [4] = [2]$.

Using these definitions, we can write addition and multiplication tables for Z_6.

Addition and multiplication tables for Z_6.

+	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	[0]	[1]
[3]	[3]	[4]	[5]	[0]	[1]	[2]
[4]	[4]	[5]	[0]	[1]	[2]	[3]
[5]	[5]	[0]	[1]	[2]	[3]	[4]

·	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]
[2]	[0]	[2]	[4]	[0]	[2]	[4]
[3]	[0]	[3]	[0]	[3]	[0]	[3]
[4]	[0]	[4]	[2]	[0]	[4]	[2]
[5]	[0]	[5]	[4]	[3]	[2]	[1]

It turns out that the sum (or product) of equivalence classes is well-defined (meaning that each sum (or product) is uniquely defined). Why? Let $[a], [b], [c], [d] \in \mathbb{Z}_n$, where $[a] = [b]$ and $[c] = [d]$. We want to show that $[a] \cdot [c] = [b] \cdot [d]$. Since $[a] = [b]$, it follows by Theorem 1 that $a\,R\,b$ and that $c\,R\,d$. Therefore, $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, and so $n \mid (a-b)$ and $n \mid (c-d)$. So there exist integers k and l such that

$$a - b = nk \text{ and } c - d = nl.$$

Adding the equations gives

$$(a-b) + (c-d) = nk + nl = n(k+l).$$

In other words, $(a+c)-(b+d) = n(k+l)$. Since $k+l \in \mathbb{Z}$, $n \mid ((a+c)-(b+d))$, or $a+c \equiv b+d \pmod{n}$, or $(a+c)\,R\,(b+d)$. Therefore, we conclude that $[a+c] = [b+d]$.

Addition and multiplicaiton on $\mathbb{Z}_n$ follow many of the expected properties. For all $a, b, c \in \mathbb{Z}$, we have the following.

- Commutative properties

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

- Associative properties

$$\begin{gathered}([a] + [b]) + [c] = [a] + ([b] + [c]) \text{ and} \\ ([a] \cdot [b]) \cdot [c] = [a] \cdot ([b] \cdot [c]).\end{gathered}$$

- Distributive property

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