Equivalence Relations

Consider the following relations on the set of people in this room

- \{(a, b) \mid a \text{ and } b \text{ were born in the same month}\},
- \{(a, b) \mid a \text{ and } b \text{ are the same sex}\},
- \{(a, b) \mid a \text{ and } b \text{ are from the the same state}\}.

Observe that these relations are all reflexive, symmetric and transitive. Because of this they are all equivalent in some way.

A relation on a set \( A \) is an equivalence relation if it is reflexive, symmetric and transitive.

Suppose that \( R \) is a relation on the positive integers such that \((a, b) \in R\) if and only if \( a < 5 \) and \( b < 5 \). Is \( R \) and equivalence relation?

Since \( a = a \) it follows that if \( a < 5 \) then \((a, a) \in R\) so we know that \( R \) is reflexive.

Suppose \((a, b) \in R\) so both \( a < 5 \) and \( b < 5 \). In this case certainly \((b, a) \in R\) so that \( R \) is symmetric.

Finally, if \((a, b) \in R\) and \((b, c) \in R\) then both \( a \) and \( c \) are less than 5 so \((a, c) \in R\) showing that \( R \) is transitive.

Thus \( R \) is an equivalence relation.

Let \( R \) be an equivalence relation on a set \( A \). The set of all elements that are related to an element \( a \) of \( A \) is called the equivalence class of \( a \). This is denoted \([a]\) or just \([a]\) if it is clear what \( R \) is.

- Suppose \( R \) is \{\((a, b) \mid a \text{ and } b \text{ were born in the same month}\)\} and is defined on the set of people in this room. Then
  \[ [a] = \{ b \mid b \text{ was born in the same month as } a \}. \]

- Suppose \( A = \{1, 2, 3, 4\} \) and
  \[ R = \{(1,1), (1,2), (2,1), (2,2), (3,3), (3,4), (4,3), (4,4)\} \]

  We can list the equivalence class for each element of \( A \):
  \[ [1] = \{1, 2\}, \quad [2] = \{1, 2\}, \quad [3] = \{3, 4\}, \quad [4] = \{3, 4\} \]
**Equivalence Relations**

A **partition** of a set \( S \) is a collection of disjoint, nonempty subsets of \( S \) that have \( S \) as their union.

If \( S = \{1, 2, 3, 4, 5, 6, 7, 8\} \) then one partition of \( S \) is  
\[
\{ \{1, 2\}, \{3\}, \{4, 5, 6\}, \{7, 8\} \}
\]

Notice that every element of \( S \) is in exactly one of the subsets.

The equivalence classes of a relation on a set \( A \) form a partition of \( A \).

- The union of all the \([a]\) is equal to \( A \).
- \([a] \cap [b] = \emptyset\) when \([a] \neq [b] \).

---

**Equivalence Relations**

**Theorem**

Let \( R \) be an equivalence relation on \( A \). The following statements are equivalent.

1. \( a \ R \ b \)
2. \([a] = [b] \)
3. \([a] \cap [b] \neq \emptyset \)

We’ll prove this using a standard approach. First we’ll show that statement 1 \( \implies \) statement 2. Next we’ll show that statement 2 \( \implies \) statement 3. Finally we’ll show that statement 3 \( \implies \) statement 1.

---

**Proof: Statement 1 \( \implies \) Statement 2**

Assume \( c \in [a] \) so that \( a \ R c \). Because equivalence relations are symmetric we know that \( c \ R a \). Since \( a \ R b \) by the transitive property we can conclude that \( c \ R b \) so that \( c \in [b] \).

This argument shows that \([a] \subseteq [b] \).

We can reverse the argument above to show that \([b] \subseteq [a] \).

Taken together this shows that \( a \ R b \implies [a] = [b] \).

---

**Proof: Statement 2 \( \implies \) Statement 3**

Because \([a] = [b] \) we know that \( a \in [a] \) and \( a \in [b] \).

Since we know at least one element common to both sets \([a]\) and \([b]\) we can conclude that \([a] \cap [b] \neq \emptyset \).

This shows that \([a] = [b] \implies [a] \cap [b] \neq \emptyset \).
Equivalence Relations

Proof: Statement 3 $\Rightarrow$ Statement 1

Suppose $c \in [a] \cap [b]$ so that $c$ is in both sets $[a]$ and $[b]$. This means that $cRa$ and $cRb$.

By the symmetric and transitive properties we can conclude that $aRb$.

This shows that $[a] \cap [b] \neq \emptyset \Rightarrow aRb$.

The proof is now completed.

Equivalence Relations

Extended Example: Congruence Classes

The integer division algorithm is $p = mq + r$. Here $r$ is the remainder that results when $p$ is divided by $m$.

The modulo function is a function $m: \mathbb{Z} \times \mathbb{Z}^+ \rightarrow \mathbb{Z}^+$ that returns the remainder when one integer is divided by another. The set $\mathbb{Z}$ is the set of integers, and the set $\mathbb{Z}^+$ is the set of positive integers.

We say that $a$ is congruent to $b$ modulo $m$ if

$$m \mid (a - b)$$

which means $m$ divides $(a - b)$. Another way to express this is that

$$a \mod m = b \mod m$$

Equivalence Relations

We use the notation

$$a \equiv b \pmod m$$

to indicate that $a$ is congruent to $b$ modulo $m$.

Example: Think of a clock: in some sense 15 minutes and 75 minutes are the same, since in both cases the minute hand is at the three-o’clock position. In fact 15$\equiv$75 (mod 60). This is easy to see because 75-15 = 60.

Example: 53$\equiv$89 (mod 12). To see this observe that 89-53=36 and 12 $\mid$ 36.

Equivalence Relations

Theorem

Let $m$ be a positive integer greater than 1. The relation

$$R = \{(a, b) \mid a \equiv b \pmod m\}$$

is an equivalence relation on the set of integers.

Proof

We need to show that $R$ is reflexive, symmetric and transitive. To see that $R$ is reflexive we need to show that $(a, a) \in R$ for all integers $a$.

We know that $a \equiv a \pmod m$ if $m \mid (a - a)$. Since $a - a = 0$ and we know that $m \mid 0$ we can conclude that $R$ is reflexive.
Equivalence Relations

Proof (continued)

To see that \( R \) is symmetric we assume that \( (a, b) \in R \) so that

\[ a - b = km \]

for some integer \( k \). In this case

\[ b - a = -km \]

which is also divisible by \( m \), but this means that

\[ b \equiv a \pmod{m} \]

so \( (b, a) \in R \). Thus \( R \) is symmetric.

\[ \text{Example: } \begin{align*}
[2] &= \{\ldots, -7, -4, -1, 2, 5, 8, 11, \ldots\} \\
[0] &= \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\} \\
[1] &= \{\ldots, -8, -5, -2, 1, 4, 7, 10, \ldots\} \\
[2] &= \{\ldots, -7, -4, -1, 2, 5, 8, 11, \ldots\}
\end{align*} \]

Equivalence Relations

Proof (continued)

Finally, we need to show that \( R \) is transitive. Assume that \( (a, b) \in R \) and \( (b, c) \in R \). This means that

\[ a \equiv b \pmod{m} \quad \text{which means that } \ a - b = km \text{ for some integer } k \]

\[ b \equiv c \pmod{m} \quad \text{which means that } \ b - c = jm \text{ for some integer } j \]

Adding the equations on the right gives

\[ (a - b) + (b - c) = km + jm \]

\[ a - c = (k + j)m \]

In the second form we see that \( a - c \) is a multiple of \( m \) so that \( a \) is

congruent to \( c \) modulo \( m \). This means that \( (a, c) \in R \), and so \( R \) is

transitive.

Equivalence Relations

Since the congruence modulo \( m \) relation is an equivalence relation it must partition the set of integers. Consider all the numbers that satisfy

\[ a \equiv 1 \pmod{3} \]

Any integer which has a remainder of 1 when divided by 3 will satisfy this expression; examples are numbers like 4 and 7.

We denote the \textbf{congruence class of} \( a \) \textbf{modulo} \( m \) with \([a]_m\).

Example:

\[ [0]_3 = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\} \]

\[ [1]_3 = \{\ldots, -8, -5, -2, 1, 4, 7, 10, \ldots\} \]

\[ [2]_3 = \{\ldots, -7, -4, -1, 2, 5, 8, 11, \ldots\} \]