5 Partitioning Sets, Equivalence Relations and Congruences

5.1 Partitioning Sets and Equivalence Relations

We have the following definition of a partition.

Definition 5.1. *A **partition** of a non-empty set X is a collection $\{A_i : i \in I\}$ of non-empty subsets of X such that*

(i) $\forall\, x \in X$, $\exists\, i \in I$ *such that* $x \in A_i$, *and*

(ii) $\forall\, x \in X$ *and* $\forall\, i, j \in I$, *if* $x \in A_i \cap A_j$, *then* $A_i = A_j$.

Example. *Let* $X = \{1, 2, 3, 4, 5, 6\}$. *Then*

$$\{\{1\},\ \{2, 3\},\ \{4, 5, 6\}\}$$

is a partition of X. *Another partition of* X *is*

$$\{\{1, 2, 3\},\ \{4, 6\},\ \{5\}\}.$$

There is a direct link between partitions of sets and equivalence relations. We have the following definitions.

Definition 5.2. *A **relation** $\sim$ on a nonempty set X is a subset $R \subseteq X \times X$. We say x is related (or equivalent) to y, denoted by $x \sim y$, when $(x, y) \in R$.*

Definition 5.3. *A relation $\sim$ on a nonempty set X is an **equivalence relation** if it satisfies the following properties.*

(i) Reflexive: $\forall\, x \in X$, $x \sim x$.

(ii) Symmetric: $\forall\, x, y \in X$, *if* $x \sim y$ *then* $y \sim x$.

(iii) Transitive: $\forall\ x, y, z \in X$, *if* $x \sim y$ *and* $y \sim z$ *then* $x \sim z$.

Example. *Let T be the set of all triangles in $\mathbb{R} \times \mathbb{R}$. For $t_1, t_2 \in T$, consider the following relation: $t_1 \sim t_2$ if t_1 is similar to t_2. Then $\sim$ is an equivalence relation (check!).*

Example. *Let $X = \mathbb{Z}$, and let $R = \{(x, x) :\ x \in \mathbb{Z}\ \}$.*

(i) Let $x \in \mathbb{Z}$. Then $(x, x) \in R$, so $x \sim x$. Hence, $\sim$ is reflexive.

(ii) Suppose that $x, y \in \mathbb{Z}$ are such that $x \sim y$. Then $(x, y) \in R$, but then $x = y$. Hence $(y, x) = (x, x) \in R$. It follows that $y \sim x$. Hence, $\sim$ is symmetric.

(iii) Suppose that $x, y, z \in \mathbb{Z}$ are such that $x \sim y$ and $y \sim z$. Then $x = y$ and $y = z$, so $x = y = z$. Hence, $(x, z) = (x, x) \in R$. It follows that $x \sim z$. Hence, $\sim$ is transitive.

Since $\sim$ is reflexive, symmetric and transitive, we have that $\sim$ is an equivalence relation.

Example. *Define a relation $\sim$ on $\mathbb{Z}$ by $x \sim y$ if $x < y$.*

(i) We have that $\sim$ is not reflexive since, for example, $1 \in \mathbb{Z}$ but $1 < 1$ is not a true statement.

(ii) We have that $\sim$ is not symmetric since, for example, $2, 3 \in \mathbb{Z}$ and $2 < 3$ but $3 < 2$ is not a true statement.

(iii) Suppose that $x, y, z \in \mathbb{Z}$ such that $x \sim y$ and $y \sim z$. Then $x < y$ and $y < z$, so $x < y < z$. Hence $x < z$, so $x \sim z$. Therefore, $\sim$ is transitive.

Since $\sim$ is not reflexive and symmetric, we have that $\sim$ is not an equivalence relation.

Definition 5.4. *Suppose $\sim$ is an equivalence relation on a (nonempty) set X. For $x \in X$, we define the **equivalence class** of x, denoted by $[x]_\sim$, to be*

$$[x]_\sim = \{y \in X : \ y \sim x\}.$$

Example. *Let $X = \{a, b, c, d\}$ and let*

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

Then $\sim$ is an equivalence relation (check!). We have the following equivalence classes:

$$\begin{aligned}
[a] &= \{y \in X : y \sim a\} = \{a, c\} \\
[b] &= \{y \in X : y \sim b\} = \{b, d\} \\
[c] &= \{y \in X : y \sim c\} = \{a, c\} = [a] \\
[d] &= \{y \in X : y \sim d\} = \{b, d\} = [b]
\end{aligned}$$

Hence, we have two distinct equivalence classes, namely $[a]$ and $[b]$.

We have the following proposition.

Proposition 5.5. *Suppose $\sim$ is an equivalence relation on a (nonempty) set X. Then for any $x, y \in X$, $[x]_\sim \neq [y]_\sim$ if and only if $[x]_\sim \cap [y]_\sim = \emptyset$.*

Proof. Take $x, y \in X$.

($\Rightarrow$) First, we will show that if $[x]_\sim \neq [y]_\sim$ then $[x]_\sim \cap [y]_\sim = \emptyset$ by giving a proof by contrapositive. So we will prove that if $[x]_\sim \cap [y]_\sim \neq \emptyset$, then $[x]_\sim = [y]_\sim$.

So suppose that $[x]_\sim \cap [y]_\sim \neq \emptyset$. Then there exists some $z \in [x]_\sim \cap [y]_\sim$. Hence, $z \in [x]_\sim$, so $z \sim x$. Similarly, $z \in [y]_\sim$, so $z \sim y$. Since $\sim$ is symmetric, we have that $x \sim z$. Since $\sim$ is transitive, we have that $x \sim y$. Now ,choose $w \in [x]_\sim$. Then $w \sim x$, and since $x \sim y$ and $\sim$ is transitive, we have that $w \sim y$. Hence, $w \in [y]_\sim$. Since $w \in [x]_\sim$ is arbitrary, we have that $[x]_\sim \subseteq [y]_\sim$. Similarly, we can show that, for any $w \in [y]_\sim$, we have $w \in [x]_\sim$, so $[y]_\sim \subseteq [x]_\sim$. Hence $[x]_\sim = [y]_\sim$.

($\Leftarrow$) Second, we will show that if $[x]_\sim \cap [y]_\sim = \emptyset$ then $[x]_\sim \neq [y]_\sim$ by giving a proof by contrapositive. So we will show that if $[x]_\sim = [y]_\sim$, then $[x]_\sim \cap [y]_\sim \neq \emptyset$.

So suppose that $[x]_\sim = [y]_\sim$. Since $\sim$ is reflexive, we know that $x \in [x]_\sim$, so $x \sim x$. Hence, $x \in [x]_\sim = [x]_\sim \cap [y]_\sim$, so $[x]_\sim \cap [y]_\sim \neq \emptyset$.

Summarising, we have that $[x]_\sim \neq [y]_\sim$ if and only if $[x]_\sim \cap [y]_\sim = \emptyset$. □

We have the following theorem.

Theorem 5.6. *Suppose $\sim$ is an equivalence relation on a (non-empty) set X. Then*

$$\Pi = \{[x]_\sim : \ x \in X\}$$

is a partition of X.

Proof. Take $a \in X$. Then $[a]_\sim \in \Pi$. Hence, every element of X is in one of the equivalence classes in Π. Now, suppose that for $a \in X$, we have $a \in [x]_\sim$ and $a \in [y]_\sim$ where $x, y \in X$. Then $[x]_\sim \cap [y]_\sim \neq \emptyset$, and we must have that $[x]_\sim = [y]_\sim$ by the proof of Proposition 5.5. It follows that Π is a partition of X. □

We have the following theorem.

Theorem 5.7. *Suppose $\Pi = \{A_i : i \in I\}$ is a partition of a (nonempty) set X, for some indexing set I. For $x, y \in X$, define $x \sim y$ if there exists an $i \in I$ such that $x, y \in A_i$. Then $\sim$ is an equivalence relation on X.*

Proof.

(i) Take $x \in X$. Since Π is a partition of X, there exists some $i \in I$ such that $x \in A_i$. Hence, $x \sim x$, so $\sim$ is reflexive.

(ii) Suppose $x, y \in X$ such that $x \sim y$. Then there exists some $i \in I$ such that $x, y \in A_i$. It follows that $y, x \in A_i$, so $y \sim x$. Hence, $\sim$ is symmetric.

(iii) Suppose that $x, y, z \in X$ are such that $x \sim y$ and $y \sim z$. Then there exists some $i \in I$ such that $x, y \in A_i$ and there exists some $j \in I$ such that $y, z \in A_j$. Hence, we have that $y \in A_i$ and $y \in A_j$. Since Π is a partition, we must have that $i = j$. It follows that $x, z \in A_i$, so $x \sim z$. Hence, $\sim$ is transitive.

Summarising, we have that $\sim$ is an equivalence relation on X. □

5.2 Congruences

We now present a fundamental example of an equivalence relation on $\mathbb{Z}$. We begin with a familiar definition.

Definition 5.8. *For $a, b \in \mathbb{Z}$, we say that a **divides** b, denoted by $a \mid b$, if $\exists\, z \in \mathbb{Z}$ such that $b = az$. Similarly, we say that a **does not divide** b, denoted by $a \nmid b$, if $\forall\, z \in \mathbb{Z}$ we have $b \neq az$.*

Definition 5.9. *Let $n \in \mathbb{N}$. For, $a, b \in \mathbb{Z}$, we say that a is **congruent** to b modulo n, denoted by $a \equiv b \pmod{n}$, if $n|(a - b)$. We say that a and b are in the same **congruence class** modulo n.*

Theorem 5.10. *Let $n \in \mathbb{N}$. For $a, b \in \mathbb{Z}$, define a relation on $\mathbb{Z}$ by $a \sim b$ if $a \equiv b \pmod{n}$. Then $\sim$ is an equivalence relation.*

Proof. Exercise 4.1. □

The following result helps to simplify many computations modulo a positive integer n.

Theorem 5.11. *Fix $n \in \mathbb{N}$. Suppose that $a, b, c, d \in \mathbb{Z}$ are such that $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$. Then*

$$a + b \equiv c + d \pmod{n} \qquad \text{and} \qquad ab \equiv cd \pmod{n}.$$

Proof. By assumption, we have that $n|a-c$ and $n|b-d$. Hence, for some $x, y \in \mathbb{Z}$, we have that $a-c=nx$ and $b-d=ny$. It follows that

$$(a+b)-(c+d)=(a-c)+(b-d)=nx+ny=n(x+y).$$

Since $x+y \in \mathbb{Z}$, this means that $n|((a+b)-(c+d))$, so $a+b \equiv c+d \pmod{n}$. Further, since $a=c+nx$ and $b=d+ny$, we have that

$$ab=(c+nx)(d+ny)=cd+n(cy+dx+nxy)$$

so $ab-cd=n(cy+dx+nxy)$. Since $cy+dx+nxy$ is an integer, we have that $n|ab-cd$, so $ab \equiv cd \pmod{n}$. □

Example. *We want to compute* $3^5+2^8 \ (mod\ 7)$. *We have* $3^2 \equiv 9 \equiv 2 \ (mod\ 7)$. *So* $3^4=3^2 \cdot 3^2 \equiv 2 \cdot 2 \equiv 4 \ (mod\ 7)$. *Hence*

$$3^5 \equiv 3^4 \cdot 3 \equiv 12 \equiv 5 \ (mod\ 7).$$

Further, we have $2^3 \equiv 8 \equiv 1 \ (mod\ 7)$, *so* $2^6 \equiv 2^3 \cdot 2^3 \equiv 1 \cdot 1 \equiv 1 \ (mod\ 7)$. *Hence, we have that*

$$2^8 \equiv 2^6 \cdot 2^2 \equiv 1 \cdot 4 \equiv 4 \ (mod\ 7).$$

It follows that

$$3^5+2^8 \equiv 5+4 \equiv 9 \equiv 2 \ (mod\ 7).$$