§3.2 Equivalence Relations

Theorem

Let A be a non-empty set and R be an equivalence relation on A. For all $x, y \in A$, we have

(a) $x \in \bar{x}$ *and* $\bar{x} \subseteq A$.

(b) xRy *if and only if* $\bar{x} = \bar{y}$.

(c) $x \not R y$ *if and only if* $\bar{x} \cap \bar{y} = \varnothing$.

Proof.

It is clear that (a) holds. To see (b) and (c), it suffices to show that "$xRy \Rightarrow \bar{x} = \bar{y}$" and "$x \not R y \Rightarrow \bar{x} \cap \bar{y} = \varnothing$".

Assume that xRy. Then if $z \in \bar{x}$, we have xRz. The symmetry and transitivity of R then implies that yRz; thus $z \in \bar{y}$ which implies that $\bar{x} \subseteq \bar{y}$. Similarly, $\bar{y} \subseteq \bar{x}$; hence we conclude that "$xRy \Rightarrow \bar{x} = \bar{y}$".

Now assume that $\bar{x} \cap \bar{y} \neq \varnothing$. Then for for some $z \in A$ we have $z \in \bar{x} \cap \bar{y}$. Therefore, xRz and yRz. Since R is symmetric and transitive, then xRy which implies that "$x \not R y \Rightarrow \bar{x} \cap \bar{y} = \varnothing$". □

§3.2 Equivalence Relations

Definition

Let m be a fixed positive integer. For $x, y \in \mathbb{Z}$, we say x ***is congruent to*** y ***modulo*** m（以 m 為除數時 x 同餘 y）and write $x = y$ (***mod*** m) if m divides $(x - y)$. The number m is called the ***modulus*** of the congruence.

Example

Using 4 as the modulus, we have

$$\begin{aligned} 3 &= 3 \pmod 4 \text{ because } 4 \text{ divides } 3-3=0\,,\\ 9 &= 5 \pmod 4 \text{ because } 4 \text{ divides } 9-5=4\,,\\ -27 &= 1 \pmod 4 \text{ because } 4 \text{ divides } -27-1=-28\,,\\ 20 &= 8 \pmod 4 \text{ because } 4 \text{ divides } 20-8=12\,,\\ 100 &= 0 \pmod 4 \text{ because } 4 \text{ divides } 100-0=100\,. \end{aligned}$$

§3.2 Equivalence Relations

Theorem

For every fixed positive integer m, the relation "congruence modulo m" is an equivalence relation on $\mathbb{Z}$.

Proof.

1. **(Reflexivity)** It is easy to see that $x = x \pmod{m}$ for all $x \in \mathbb{Z}$. Therefore, congruence modulo m is reflexive on $\mathbb{Z}$.
2. **(Symmetry)** Assume that $x = y \pmod{m}$. Then m divides $x - y$; that is, $x - y = mk$ for some $k \in \mathbb{Z}$. Therefore, $y - x = m(-k)$ which implies that m divides $y - x$; thus $y = x \pmod{m}$.
3. **(Transitivity)** Assume that $x = y \pmod{m}$ and $y = z \pmod{m}$. Then $x - y = mk$ and $y - z = m\ell$ for some $k, \ell \in \mathbb{Z}$. Therefore, $x - z = m(k + \ell)$ which implies that m divides $x - z$; thus $x = z \pmod{m}$. □

§3.2 Equivalence Relations

Definition

The set of equivalence classes for the relation congruence modulo m is denoted by $\mathbb{Z}_m$.

Remark: The elements of $\mathbb{Z}_m$ are sometimes called the ***residue*** (or ***remainder***) classes modulo m.

Example

For congruence modulo 4, there are four equivalence classes:

$$\bar{0} = \{\cdots, -16, -12, -8, -4, 0, 4, 8, 12, 16, \cdots\} = \{4k \mid k \in \mathbb{Z}\},$$

$$\bar{1} = \{\cdots, -15, -11, -7, -3, 1, 5, 9, 13, 17, \cdots\} = \{4k+1 \mid k \in \mathbb{Z}\},$$

$$\bar{2} = \{\cdots, -14, -10, -6, -2, 2, 6, 10, 14, 18, \cdots\} = \{4k+2 \mid k \in \mathbb{Z}\},$$

$$\bar{3} = \{\cdots, -13, -9, -5, -1, 3, 7, 11, 15, 19, \cdots\} = \{4k+3 \mid k \in \mathbb{Z}\}.$$

§3.2 Equivalence Relations

In general, we will prove that the equivalence relation "congruence modulo m" produces m equivalence classes

$$\bar{j} = \{mk + j \,|\, k \in \mathbb{Z}\}, \qquad j = 0, 1, \cdots, m-1.$$

The collection of these equivalence classes, by definition $\mathbb{Z}/(\text{mod } m)$, is usually denoted by $\mathbb{Z}_m$.

Theorem

Let m be a fixed positive integer. Then

1. *For integers x and y, $x = y \pmod m$ if and only if the remainder when x is divided by m equals the remainder when y divided by m.*
2. *$\mathbb{Z}_m$ consists of m distinct equivalence classes:*

$$\mathbb{Z}_m = \{\bar{0}, \bar{1}, \cdots, \overline{m-1}\}.$$

§3.2 Equivalence Relations

Proof.

1. For a given $x \in \mathbb{Z}$, let $\big(q(x), r(x)\big)$ denote the unique pair in $\mathbb{Z} \times \mathbb{Z}$ obtained by the division algorithm satisfying
$$x = mq(x) + r(x) \quad \text{and} \quad 0 \leqslant r(x) < m\,.$$
Then
$$\begin{aligned} x = y \pmod{m} &\Leftrightarrow m \text{ divides } x - y \\ &\Leftrightarrow m \text{ divides } m\big(q(x) - q(y)\big) + r(x) - r(y) \\ &\Leftrightarrow m \text{ divides } r(x) - r(y) \\ &\Leftrightarrow r(x) - r(y) = 0\,. \end{aligned}$$
where the last equivalence following from the fact that $0 \leqslant r(x), r(y) < m$. □

§3.2 Equivalence Relations

Proof. (Cont'd).

2. Using ①, x and y are in the same equivalence classes (produced by the equivalence relation "congruence modulo m") if and only if x and y has the same remainder when they are divided by m. Therefore, we find that

$$\bar{x} = \{mk + r(x) \mid k \in \mathbb{Z}\} = \overline{r(x)} \qquad \forall\, x \in \mathbb{Z}\,.$$

Since $r(x)$ has values from $\{0, 1, \cdots, m-1\}$, we find that $\mathbb{Z}_m = \{\bar{0}, \bar{1}, \cdots, \overline{m-1}\}$. The proof is completed if we show that $\bar{k} \cap \bar{j} = \varnothing$ if $k \neq j$ and $k, j \in \{0, 1, \cdots, m-1\}$. However, if $x \in \bar{k} \cap \bar{j}$, then

$$x = mq_1 + k = mq_2 + j$$

which is impossible since $k \neq j$ and $k, j \in \{0, 1, \cdots, m-1\}$. Therefore, there are exactly m equivalence classes. □

§3.3 Partitions

Definition

Let A be a non-empty set. $\mathcal{P}$ is a ***partition*** of A if $\mathcal{P}$ is a collection of subsets of A such that

1. if $X \in \mathcal{P}$, then $X \neq \varnothing$.
2. if $X \in \mathcal{P}$ and $Y \in \mathcal{P}$, then $X = Y$ or $X \cap Y = \varnothing$.
3. $\bigcup_{X \in \mathcal{P}} X = A$.

In other words, a partition of a set A is a pairwise disjoint collection of non-empty subsets of A whose union is A.

§3.3 Partitions

Example

The family $\mathcal{G} = \big\{[n, n+1) \,\big|\, n \in \mathbb{Z}\big\}$ is a partition of $\mathbb{R}$.

Example

Each of the following is a partition of $\mathbb{Z}$:

1. $\mathcal{P} = \{E, D\}$, where E is the collection of even integers and D is the collection of odd integers.
2. $\mathcal{X} = \{\mathbb{N}, \{0\}, \mathbb{Z}^-\}$, where $\mathbb{Z}^-$ is the collection of negative integers.
3. $\mathcal{H} = \{A_k \,|\, k \in \mathbb{Z}\}$, where $A_k = \{3k, 3k+1, 3k+2\}$.

§3.3 Partitions

Theorem

If R is an equivalent relation on a non-empty set A, then A/R is a partition of A.

Proof.

First of all, each equivalence class $\bar{x} \in A/R$ must be non-empty since it contains x. Let $\bar{x}$ and $\bar{y}$ be two equivalence classes in A/R. If $\bar{x} \cap \bar{y} \neq \varnothing$, then there exists $z \in \bar{x} \cap \bar{y}$ which implies that xRz and yRz. By the symmetry and the transitivity of R we have xRy which implies that $\bar{x} = \bar{y}$.

Finally, it is clear that $\bigcup_{\bar{x} \in A/R} \bar{x} \subseteq A$ since each $\bar{x} \subseteq A$. On the other hand, since each $y \in A$ belongs to the equivalence class $\bar{y}$, we must have $A \subseteq \bigcup_{\bar{x} \in A/R} \bar{x}$. Therefore, $A = \bigcup_{\bar{x} \in A/R} \bar{x}$. □

§3.3 Partitions

Theorem

Let $\mathcal{P}$ be a partition of a non-empty set A. For $x, y \in A$, define xQy if and only if there exists $C \in \mathcal{P}$ such that $x, y \in C$. Then

1. *Q is an equivalence relation on A.*
2. *$A/Q = \mathcal{P}$.*

Proof.

It is clear that Q is reflexive and symmetric on A, so it suffices to show the transitivity of Q to complete ①. Suppose that xQy and yQz. By the definition of the relation Q there exists C_1 and C_2 in $\mathcal{P}$ such that $x, y \in C_1$ and $y, z \in C_2$; hence $C_1 \cap C_2 \neq \varnothing$. Then $C_1 = C_2$ by the fact that $\mathcal{P}$ is a partition and $C_1, C_2 \in \mathcal{P}$. Therefore, $x, z \in C_1$ which implies that xQz. □

§3.3 Partitions

Proof. (Cont'd).

Next, we claim that if $C \in \mathcal{P}$, then $x \in C$ if and only if $\bar{x} = C$. It suffices to show the direction "$\Rightarrow$" since $x \in \bar{x}$.

Suppose that $C \in \mathcal{P}$ and $x \in C$.

1. "$C \subseteq \bar{x}$": Let $y \in C$ be given. By the fact that $x \in C$ we must have yQx. Therefore, $y \in \bar{x}$ which shows $C \subseteq \bar{x}$.
2. "$\bar{x} \subseteq C$": Let $y \in \bar{x}$ be given. Then there exists $\widetilde{C} \in \mathcal{P}$ such that $x, y \in \widetilde{C}$. By the fact that $x \in C$, we find that $C \cap \widetilde{C} \neq \varnothing$. Since $\mathcal{P}$ is a partition of A and $C, \widetilde{C} \in \mathcal{P}$, we must have $C = \widetilde{C}$; thus $y \in C$. Therefore, $\bar{x} \subseteq C$.

□

§3.3 Partitions

Proof. (Cont'd).

Now we show that $A/Q = \mathcal{P}$. If $C \in \mathcal{P}$, then $C \neq \varnothing$; thus there exists $x \in C$ for some $x \in A$. Then the claim above shows that $C = \overline{x} \in A/Q$. Therefore, $\mathcal{P} \subseteq A/Q$. On the other hand, if $\overline{x} \in A/Q$, by the fact that $\mathcal{P}$ is a partition of A, there exists $C \in \mathcal{P}$ such that $x \in C$. Then the claim above shows that $\overline{x} = C$. Therefore, $A/Q \subseteq \mathcal{P}$. □

Remark: The relation Q defined in the theorem proved above is called ***the equivalence relation associated with the partition*** $\mathcal{P}$.