EQUIVALENCE CLASSES

ROHAN RAMCHAND, MICHAEL MIYAGI

Let X be a set. Then for some $x \in X$, the **equivalence class of** x is defined for some equivalence relation $\sim \in X \times X$ as

$$C(x) = \{y \in X \mid x \sim y\}.$$

For an equivalence class $C(x)$, x is referred to as the **representative of** C.

Theorem 1. *Let $C(x)$ and $C(y)$ be equivalence classes for some $x, y \in X$. Then either*

$$C(x) = C(y)$$

or

$$C(x) \cap C(y) = \varnothing.$$

Proof. Assume $z \in C(x) \cap C(y)$, where we assume by contradiction that $C(x) \cap C(y) \neq \varnothing$. Then

$$z \in C(x) \to z \sim x$$

and

$$z \in C(y) \to z \sim y.$$

Then for some $a \in C(x)$,

$$\begin{aligned} & a \sim x && \wedge x \sim z \\ \to\ & a \sim z && \wedge y \sim z \\ \to\ & a \sim y && \\ \to\ & a \in C(y) && \end{aligned}$$

Then $C(x) \subseteq C(y)$. The proof of $C(y) \subseteq C(x)$ follows from a similar argument and is left as an exercise. Then $C(x) = C(y)$ if $C(x) \cap C(y) \neq \varnothing$ and the proof is complete. $\square$

Continuing from above, for some set X and equivalence relation $\sim$ on X, we define a partition on X as

$$X/_{\sim} = P_{\sim} = \{C(x) \mid x \in X\}.$$

By definition of equivalence classes, this is a valid partitioning of X, and therefore no proof is provided.

Continuing in the opposite direction, let P be a partition of X. Then

$$\sim_P\colon x \sim_P y \Leftrightarrow x, y \text{ are in the same class in } P.$$

Example. *Let* $X = \{1, 2, 3\}$ *and let* $\sim = \{(1, 1), (2, 2), (3, 3)\}$. *Then*
$$P_\sim = \{\{1\}, \{2\}, \{3\}\}$$
and
$$C(1) = \{1\}, C(2) = \{2\}, C(3) = \{3\}.$$

Example. *Let* $X = \{1, 2, 3\}$ *and let* $\sim = \{(1, 1), (2, 2), (3, 3), (1, 2), (2, 1)\}$. *Then*
$$C(1) = \{1, 2\}, C(2) = \{2, 1\}, C(3) = \{3\}$$
and
$$P_\sim = \{C(1), C(2), C(3)\} = \{\{1, 2\}, \{3\}\}.$$

Properties of $\sim_N$

We will now revisit the partitioning of $\mathbb{Z}$ from above. Recall that $a \sim_n b \Leftrightarrow n|(b - a)$. Then
$$\mathbb{Z}/_{\sim_n} = \{C(a) \,|\, a \in \mathbb{Z}\}$$
where $C(a)$ is denoted $\overline{a}$. Note that $b \sim_n a \Leftrightarrow b = a+kn$ for some $k \in \mathbb{Z}$ and therefore
$$\mathbb{Z}/_{\sim_n} = \{C(0), C(1), ..., C(n - 1)\}$$
since $C(n) = C(0)$. Finally, for $i, j : 0 \leq i \leq j \leq n - 1$,
$$C(i) \cap C(j) = \varnothing \Leftrightarrow i \sim_n j.$$

Operations on $\mathbb{Z}/_{\sim_n}$. Let C_1 and C_2 be equivalence classes. Then if $a \in C_1$ and $b \in C_2$, then
$$C_1 + C_2 = C(a + b).$$
Note that this sum doesn't depend on the choice of a and b. This is proven below.

Proof. Let $C_1, C_2 \in \mathbb{Z}/_{\sim_n}$ such that $C_1 = C(a)$ and $C_2 = C(b)$. Furthermore, let $C_1 = C(a')$ and $C_2 = C(b')$. Then
$$\begin{aligned}
C(a) = C(a') \to a \sim_n a' && \to a' = a + kn \\
C(b) = C(b') \to b \sim_n b' && \to b' = b + jn \\
&& \to a' + b' = a + b + (j + k)n \\
&& \to a' + b' \sim_n a + b \\
&& \to C(a' + b') = C(a + b)
\end{aligned}$$

Then the operation of addition on equivalence classes does not depend on the choice of representatives a, b. □

An operation on equivalence classes that does not depend on the choice of representative is called **well-defined**; by the proof above, addition of equivalence classes is well-defined.

Like addition, multiplication can also be defined on equivalence classes. As above, let $C_1, C_2 \in \mathbb{Z}/_{\sim_n}$ such that $C_1 = C(a)$ and $C_2 = C(b)$. Then

$$C_1C_2 = C(ab).$$

Multiplication is well-defined; this is proven below.

Proof. Let $C_1, C_2 \in \mathbb{Z}/_{\sim_n}$ such that $C_1 = C(a)$ and $C_2 = C(b)$. Furthermore, let $C_1 = C(a')$ and $C_2 = C(b')$. Then

$$\begin{aligned} C(a) = C(a') \to a \sim_n a' & \qquad \to a' = a + kn \\ C(b) = C(b') \to b \sim_n b' & \qquad \to b' = b + jn \\ & \qquad \to a'b' = ab + (aj + bk)n + jkn^2 \\ & \qquad \qquad = ab + (aj + bk + jkn)n \\ & \qquad \to a'b' \sim_n ab \\ & \qquad \to C(a'b') = C(ab) \end{aligned}$$

Then the operation of multiplication on equivalence classes does not depend on the choice of representatives a, b. $\square$

For sufficiently small n, it is possible to calculate all possible results of addition and multiplication, since no product or sum of equivalence classes in $\mathbb{Z}/_{\sim_n}$ can exceed n itself. This is usually represented as a table; an example, using $\mathbb{Z}/_{\sim_4}$, is shown below.

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Note that under multiplication, $\overline{2}$ does not admit an inverse – that is, since $\overline{1}$ is the multiplicative identity, there is no $\overline{n}$ such that $\overline{2} \times \overline{n} = \overline{1}$. This is a result of an important theorem, given here without proof. (This theorem is proven in many number-theoretic books.)

Theorem 2. *Let $\mathbb{Z}/n\mathbb{Z}$ be the set of equivalence classes of $\mathbb{Z}$ under $\sim_n$. Then every $\overline{x} \neq 0 \in \mathbb{Z}/n\mathbb{Z}$ admits an inverse under multiplication if and only if n is prime.*

Properties of $+$ and $\times$ on $\mathbb{Z}/n\mathbb{Z}$

We will now prove several properties of the operations defined in the previous section. The relevance of these properties will become apparent in the next section.

Theorem 3 (Associativity of Addition)**.** *Let $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}/n\mathbb{Z}$. Then*

$$\overline{a} + (\overline{b} + \overline{c}) = (\overline{a} + \overline{b}) + \overline{c}.$$

Proof.

$$\begin{aligned} \overline{a} + (\overline{b} + \overline{c}) &= \overline{a} + \overline{b + c} \\ &= \overline{a + b + c} \\ &= \overline{a + b} + \overline{c} \\ &= (\overline{a} + \overline{b}) + \overline{c} \end{aligned}$$

□

Theorem 4 (Identity and Inverse of Addition)**.** *For any element $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$,*

$$\overline{a} + \overline{0} = \overline{0} + \overline{a} = \overline{a}.$$

Then $\overline{0}$ is the identity element of $\mathbb{Z}/n\mathbb{Z}$ under addition. Furthermore,

$$\overline{-a} + \overline{a} = \overline{a} + \overline{-a} = \overline{0}$$

and therefore $+$ is closed under inversion.

Proof.

$$\begin{aligned} \overline{a} + \overline{0} &= \overline{a + 0} \\ &= \overline{a} \\ \overline{0} + \overline{a} &= \overline{0 + a} \\ &= \overline{a} \end{aligned}$$

Then $\mathrm{Id}_{\mathbb{Z}/n\mathbb{Z}} = \overline{0}$.

$$\begin{aligned} \overline{a} + \overline{-a} &= \overline{a + (-a)} \\ &= \overline{0} \\ \overline{-a} + \overline{a} &= \overline{(-a) + a} \\ &= \overline{0} \end{aligned}$$

Then for any $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$, there exists an inverse element in $\mathbb{Z}/n\mathbb{Z}$. Then $+$ is closed under inversion. □

Theorem 5 (Commutativity of Addition)**.** *Let* $\overline{a}, \overline{b} \in \mathbb{Z}/n\mathbb{Z}$*. Then*

$$\overline{a} + \overline{b} = \overline{b} + \overline{a}.$$

Proof.

$$\begin{aligned} \overline{a} + \overline{b} &= \overline{a+b} \\ &= \overline{b+a} \\ &= \overline{b} + \overline{a} \end{aligned}$$

Therefore, $+$ is commutative. □

The following theorems on multiplication are stated without proof, which is left to the reader as an exercise. (The proofs all follow the same structure as those for addition.)

Theorem 6 (Associativity of Multiplication)**.** *Let* $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}/n\mathbb{Z}$*. Then*

$$\overline{a} * (\overline{b} * \overline{c}) = (\overline{a} * \overline{b}) * \overline{c}.$$

Theorem 7 (Identity and Inverse of Multiplication)**.** *For any element* $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$*,*

$$\overline{a} * \overline{1} = \overline{1} * \overline{a} = \overline{a}.$$

Then $\overline{1}$ *is the identity element of* $\mathbb{Z}/n\mathbb{Z}$ *under addition. Furthermore, if* n *is prime,*

$$\exists \overline{b} \in \mathbb{Z}/n\mathbb{Z} : \overline{a} * \overline{b} = \overline{1}.$$

(Note that the second part of the above theorem holds if and only if n is prime, by the theorem stated above.)

Theorem 8 (Commutativity of Multiplication)**.** *Let* $\overline{a}, \overline{b} \in \mathbb{Z}/n\mathbb{Z}$*. Then*

$$\overline{a} * \overline{b} = \overline{b} * \overline{a}.$$

Theorem 9 (Distributivity of Multiplication over Addition)**.** *Let* $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}/n\mathbb{Z}$*. Then*

$$\overline{a} \times (\overline{b} + \overline{c}) = \overline{a} \times \overline{b} + \overline{a} \times \overline{c}.$$

Finally, let

$$\left(\mathbb{Z}/n\mathbb{Z}, +, \times, \overline{0}, \overline{1}\right)$$

be the 5-tuple consisting of the set $\mathbb{Z}/n\mathbb{Z}$, the operations $+, \times : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, and the identities $\overline{0}$ under addition and $\overline{1}$ under multiplication. This is referred to as the **ring of integers** $\pmod n$, and if n is prime (and therefore multiplication admits an inverse), it is called the **field of integers** $\pmod n$. (We shall delve more deeply into the definitions of rings and fields later on.)