A SHORT NOTE DISSCUSING THE SET $\mathbb{Z}_n$ UNDER ADDITION AND MULTIPLICATION $mod\, n$

by Dr.Jehan Alawi Al-bar

1. We prove here that $(\mathbb{Z}_n, \oplus)$ is an abelian(a commutative) group.

2. When considering the multiplication $mod\, n$, the elements in Z_n fail to have inverses. We study $\mathbb{Z}_4$ as an example . However, we still have $(\mathbb{Z}_n, \otimes)$ is an abelian semigroup with identity as we will prove later.

3. We know that an integer a has a multiplicative inverse $mod\, n$ if and only if a and n are relatively prim ($gcd(a, n) = 1$). So for each $n > 1$, we define $U(n)$ to be the set of all positive integers less than n and relatively prim to n. Then $(U(n), \otimes)$ is an abelian group where the multiplication is taken $mod\, n$.

Let $\mathbb{Z}_n = \{0, 1, 2, 3, ...n-1\}$, we show that $(\mathbb{Z}_n, \oplus)$ is an abelian group where $\oplus$ is the addition $mod\, n$. Typical element in $\mathbb{Z}_n$ is denoted by $\overline{x}$ and $\overline{x} \oplus \overline{y} = \overline{x+y}$.

- First we show that $\oplus$ is well defined on $\mathbb{Z}_n$. Let $\overline{x}_1 = \overline{x}_2$ and $\overline{y}_1 = \overline{y}_2$, then $x_1 - x_2 = q_1 n$ and $y_1 - y_2 = q_2 n$. Therefor $x_1 - x_2 + y_1 - y_2 = q_1 n + q_2 n = (q_1 + q_2)n$. and $(x_1+y_1) - (x_2+y_2) = qn$, so $x_1 + y_1 \equiv x_2 + y_2$ $mod\, n$. Therefor $\overline{x_1 + y_1} = \overline{x_2 + y_2} \Leftrightarrow \overline{x}_1 \oplus \overline{y}_1 = \overline{x}_1 \oplus \overline{y}_2$.

- We know that Z is closed under ordinary addition. For integers x, y we have $x + y \in \overline{R}$ for some equivalence class $\overline{R}$ in $\mathbb{Z}_n$ for some n. So $\overline{x} \oplus \overline{y} = \overline{x+y} = \overline{R}$ and so $\mathbb{Z}_n$ is closed under $\oplus$.

- Let $\overline{x}, \overline{y}$, and $\overline{z} \in \mathbb{Z}_n$. Then

  $$(\overline{x} \oplus \overline{y}) \oplus \overline{z} = \overline{x+y} \oplus \overline{z} = \overline{(x+y)+z} = \overline{x+(y+z)} = \overline{x} \oplus \overline{y+z} = \overline{x} \oplus (\overline{y} \oplus \overline{z}).$$

  Therefor $\oplus$ is an associative operation on $\mathbb{Z}_n$.

- The class $\overline{0}$ is the identity in $\mathbb{Z}_n$ because

  $$\overline{x} \oplus \overline{0} = \overline{x+0} = \overline{x}.$$

  In a similar way we can show that $\overline{0} \oplus \overline{x} = \overline{0}$.

- We see that $-\overline{x} = \overline{-x}$ because

  $$\overline{x} \oplus \overline{-x} = \overline{x + (-x)} = \overline{x - x} = \overline{0}.$$

  Similarly we can show that $\overline{-x} \oplus \overline{x} = \overline{0}$. Notice that $\overline{-x} = \overline{n-x}$.

- For $\overline{x}$ and $\overline{y} \in \mathbb{Z}_n$, we see that

  $$\overline{x} \oplus \overline{y} = \overline{x+y} = \overline{y+x} = \overline{y} \oplus \overline{x}.$$

  Therefor $(\mathbb{Z}_\mathbf{n}, \oplus)$ is a commutative group.

We now study the multiplication *mod* n on the set $\mathbb{Z}_n$. Let $\overline{x} \otimes \overline{y} = \overline{xy}$

- we show that $\otimes$ is well defined. Let $\overline{x_1 y_1} = \overline{x_2 y_2}$ therefor $x_1 y_1 - x_2 y_2 = q_n$. If $\overline{x_1} = \overline{x_2}$ and $\overline{y_1} = \overline{y_2}$ then $x_1 - x_2 = q_1 n$ and $y_1 - y_2 = q_2 n$, therefor $(x_1 - x_2)(y_1 - y_2) = q_1 q_2 n^2$ implies that $x_1 y_1 + x_2 y_2 - x_2 y_1 - x_1 y_2 = q_1 q_2 n^2$ so $x_1 y_1 + x_2 y_2 = x_2 y_1 + x_1 y_2 + q_1 q_2 n^2$ implies that $x_1 y_1 + x_2 y_2 - 2x_2 y_2 = x_2 y_1 - x_2 y_2 + x_1 y_2 - x_2 y_2 + q_1 q_2 n^2$ implies that $x_1 y_1 - x_2 y_2 = x_2(y_1 - y_2) + y_2(x_1 - x_2) + q_1 q_2 n^2 = q_2 x_2 n + q_1 y_2 n + q_1 q_2 n^2 = (q_2 x_2 + q_1 y_2 + q_1 q_2 n)n$ is some multiple of n. Therefor $\overline{x_1 y_1} = \overline{x_2 y_2}$ and the multiplication is well defined.

- The set of integers Z is closed under the ordinary multiplication, so for integers x and y we have that $xy \in \overline{R}$ for some class $\overline{R} \in \mathbb{Z}_n$. Therefor $\overline{xy} = \overline{R}$ and so $\overline{xy} \in \mathbb{Z}_n$. Therefor $\mathbb{Z}_n$ is closed under multiplication *mod* n.

- Let $\overline{x}, \overline{y}$ and $\overline{z} \in \mathbb{Z}_n$. Then $(\overline{x} \otimes \overline{y}) \otimes \overline{z} = \overline{xy} \otimes \overline{z} = \overline{(xy)z} = \overline{x(yz)} = \overline{x} \otimes \overline{yz} = \overline{x}(\overline{y} \otimes \overline{z})$ and so the multiplication is associative.

- Denote the identity in $\mathbb{Z}_n$ be $\overline{e}$. Then $\overline{xe} = \overline{x}$ implies that $\overline{xe} = \overline{x}$ therefor $xe - x = qn$ for $q \in Z$. And $x(e-1) = qn$. For $q = 0$, then $x(e-1) = 0$ therefor either $x = 0$ or $e - 1 = 0$ so $e = 1$ and $\overline{e} = \overline{1}$ for all $x \neq 0$. If $\overline{e} = \overline{1}$ and $\overline{x} = \overline{0}$ then $\overline{01} = \overline{01} = \overline{0}$ and $\overline{10} = \overline{10} = \overline{0}$. Hence $\overline{e} = \overline{1}$ for all x.

- $\overline{xy} = \overline{xy} = \overline{yx} = \overline{yx}$ and so the multiplication is commutative.

Hence we have shown that $(\mathbb{Z}_n, \otimes)$ is a commutative semigroup with identity.

This semigroup fails to be a group since the inverse of the elements does not always exist as we see in the following example.
Consider $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ with the multiplication table

$*$ *mod* n	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

From this table we see that $3^{-1} = 3, 1^{-1} = 1$, but 0^{-1} and 2^{-1} are not exist.

An integer x has a multiplicative inverse $mod\, n$ if and only if x and n are relatively prime. So define for all $n > 1$ the set $U(n)$ to be the set of all positive integers less than n and relatively prime to n. **Then $(\mathbf{U}(\mathbf{n}), \otimes)$ is a group.**

Note that If n is a prime integer then $U(n) = \{1, 2, 3, ...n - 1\} = {\mathbb{Z}_n}^*$ or we write $U(p) = \mathbb{Z}_p^*$.