Integers modulo a prime under multiplication

Let \( p \) be a prime.

Define \( \mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\} = \{1, 2, \ldots, p - 1\} \).

Consider \( \circ \), multiplication modulo \( p \).

The identity element is 1.

\( \circ \) is associative since multiplication is associative.

\( \circ \) is commutative since multiplication is commutative.

Let \( a \in \mathbb{Z}_p^* \). Then \( \gcd(a, p) = 1 \).

So there is \( b \in \mathbb{Z} \) such that \( ab \equiv 1 \mod p \) (and \( ba \equiv 1 \mod p \)).

Now \( b \equiv r \mod p \) for some \( r \in \mathbb{Z}_p^* \) and \( ar \equiv ra \equiv 1 \).

Hence \( a \) has inverse \( r \), i.e., \( a^{-1} = r \).

Hence \( (\mathbb{Z}_p^*, \circ) \) is a commutative group.

**Example**: \( (\mathbb{Z}_5^*, \circ) \). *On board*
The symmetric group

Fix \( n \in \mathbb{N} \). Write \( \mathbb{N}_n = \{1, \ldots, n\} \).

Write \( S_n \) for the set of permutations \( f : \mathbb{N}_n \rightarrow \mathbb{N}_n \).

Recall from Section 6 that we have \( |S_n| = n! \).

Consider the binary operation \( \circ \) given by composition of permutations.

The identity map \( i_{\mathbb{N}_n} : \mathbb{N}_n \rightarrow \mathbb{N}_n \) is the identity element. Write \( e = i_{\mathbb{N}_n} \).

Composition of functions is associative, so the binary operation is associative.

We saw (Section 5) that every permutation has an inverse.

Hence \( S_n \) forms a group under \( \circ \). Called the \textit{symmetric group}.

When \( f, g \in S_n \), we often write \( fg \) instead of \( f \circ g \).
More on inverses in groups

Let \((G, \ast)\) be a group. Let \(g, h \in G\).

What is \((g \ast h)^{-1}\)?

\[
(g \ast h) \ast (h^{-1} \ast g^{-1}) = g \ast (h \ast h^{-1}) \ast g^{-1} = g \ast e \ast g^{-1} = g \ast g^{-1} = e
\]

and

\[
(h^{-1} \ast g^{-1}) \ast (g \ast h) = h^{-1} \ast (g^{-1} \ast g) \ast h = h^{-1} \ast e \ast h = h^{-1} \ast h = e,
\]

so \(h^{-1} \ast g^{-1} = (g \ast h)^{-1}\).

By induction, if \(g_1, g_2, \ldots, g_n \in G\), then

\[
(g_1 \ast g_2 \ast \ldots \ast g_n)^{-1} = g_n^{-1} \ast \ldots \ast g_1^{-1}.
\]

Example:

Let \((G, \ast) = (S_6, \circ)\).

We have \(((1234)(2346))^{-1} = (12463)^{-1} = (13642)\) and

\[
(2346)^{-1}(1234)^{-1} = (2643)(1432) = (13642).
\]
Another example

Let $G = \{e, (12)(34), (13)(24), (14)(23)\} \subseteq S_4$, with composition as the binary operation.

$((12)(34))^{-1} = (12)(34), ((13)(24))^{-1} = (13)(24)$ and $((14)(23))^{-1} = (14)(23)$.

Write $a = (12)(34), b = (13)(24)$ and $c = (14)(23)$. Then the multiplication table is

<table>
<thead>
<tr>
<th></th>
<th>$e$</th>
<th>$a$</th>
<th>$b$</th>
<th>$c$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$e$</td>
<td>$e$</td>
<td>$a$</td>
<td>$b$</td>
<td>$c$</td>
</tr>
<tr>
<td>$a$</td>
<td>$a$</td>
<td>$e$</td>
<td>$c$</td>
<td>$b$</td>
</tr>
<tr>
<td>$b$</td>
<td>$b$</td>
<td>$c$</td>
<td>$e$</td>
<td>$a$</td>
</tr>
<tr>
<td>$c$</td>
<td>$c$</td>
<td>$b$</td>
<td>$a$</td>
<td>$e$</td>
</tr>
</tbody>
</table>

Hence $\circ$ is a binary operation, and $G$ forms a group.

Note that $G$ is commutative.
We are interested in sets with two compatible binary operations.

**Definition**

Let $F$ be a non-empty set and let $+, \ast$ be binary operations on $F$ (they need not be addition and multiplication).

We say $(F, +, \ast)$ is a *field* if the following are satisfied:

1. **(F1)** $(F, +)$ is a commutative group. Write 0 for the identity.
2. **(F2)** $(F \setminus \{0\}, \ast)$ is a commutative group. Write 1 for the identity.
3. **(F3)** $\forall a, b, c \in F$, $a \ast (b + c) = (a \ast b) + (a \ast c)$. ($\ast$ is *distributive* over $+$).

$F$ will have an identity element with respect to $+$ (the additive identity) and an identity element with respect to $\ast$ (the multiplicative identity).

Each $a \in F$ has an inverse with respect to $+$, written $-a$.

Each $a \in F \setminus \{0\}$ has an inverse with respect to $\ast$, written $a^{-1}$.

$\mathbb{R}$, $\mathbb{C}$ and $\mathbb{Q}$ are fields when $+$ is addition and $\ast$ is multiplication.
Some finite fields

Let $p \in \mathbb{N}$ be a prime. Let $F = \mathbb{Z}_p$.

Write $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$.

Consider $\oplus$ and $\odot$ as the binary operations on $F$.

$(\mathbb{Z}_p, \oplus)$ forms a commutative group (with identity element 0). So (F1) is satisfied.

$(\mathbb{Z}_p^*, \odot)$ is a commutative group (with identity element 1). So (F2) is satisfied.

$\forall a, b, c \in \mathbb{Z}_p, a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$.

Hence $(F, \oplus, \odot)$ is a field. Note that $F$ is finite.

$\mathbb{Q}$ and $\mathbb{Z}_p$ are the fundamental examples of fields - in a sense every field ‘contains’ a copy of one of these.