Section 11: Binary operations (continued)

Let $S$ be a set.
Recall that a binary operation $\ast$ on $S$ is a function

$$\ast : S \times S \to S.$$ 

For convenience we write $a \ast b$ instead of $\ast(a, b)$.

**Remark:**
If $\ast$ is associative, then we can write $a \ast b \ast c$, meaning $(a \ast b) \ast c$ and $a \ast (b \ast c)$.
We may also define longer expressions $a_1 \ast \cdots \ast a_n$.
Hence for $n \in \mathbb{N}$ and $a \in S$, we may define

$$a^n = \underbrace{a \ast \cdots \ast a}_n.$$ 

**Examples:** On board (Continued from last lecture).
Identity elements

Let \( * \) be a binary operation on a set \( S \).
We say \( e \in S \) is an identity element for \( S \) (with respect to \( * \)) if

\[
\forall a \in S, \ e * a = a * e = a.
\]

If there is an identity element, then it’s unique:

Proposition

Let \( * \) be a binary operation on a set \( S \). Let \( e, f \in S \) be identity elements for \( S \) with respect to \( * \). Then \( e = f \).

Proof.

Since \( e \) is an identity element and \( f \in S \), we have \( e * f = f \).
Since \( f \) is an identity element and \( e \in S \), we have \( e * f = e \).
Hence \( e = e * f = f \).
(i) 0 is the identity element for $S = \mathbb{R}$ when $* = +$.

(ii) 1 is the identity element for $S = \mathbb{R}$ when $* = \times$.

(iii) Let $S = \mathbb{Q} \setminus \{0\}$ and $a * b = \frac{a}{b}$. Then there is no identity element.

On board

(iv) $S = \{a, b, c, d\}$, and define a binary operation $*$ on $S$ by the multiplication table

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

In this case $c$ is an (the) identity element.
Groups

Let $G$ be a non-empty set and $\ast$ a binary operation on $G$. We call $(G, \ast)$ a group if the following hold:

(G1) $\ast$ is associative

(G2) $G$ has an identity element $e$ with respect to $\ast$

(G3) $\forall g \in G, \exists h \in G$ such that $g \ast h = h \ast g = e$.

[We sometimes say $G$ forms a group under $\ast$.]

Remark:

In (G3), the element $h$ is called an inverse to $g$. It is unique, since suppose $h_1, h_2 \in G$ with

$$g \ast h_1 = h_1 \ast g = e, \quad g \ast h_2 = h_2 \ast g = e.$$

Then $h_1 \ast (g \ast h_2) = h_1 \ast e = h_1$ and $h_1 \ast (g \ast h_2) = (h_1 \ast g) \ast h_2 = e \ast h_2 = h_2$, since $\ast$ is associative.

Hence $h_1 = h_2$.

Hence we may refer to the (unique) inverse to $g$, and write $g^{-1}$. 
Examples

(i) $G = \mathbb{Z}$, $\ast = +$. The identity element is 0, and $\ast$ is associative.

Let $a \in \mathbb{Z}$. Then $(-a) + a = a + (-a) = 0$, so $-a$ is the inverse of $a$ (i.e., $a^{-1} = -a$).

Hence $(\mathbb{Z}, +)$ forms a group.

(ii) Let $G = \mathbb{R} \setminus \{0\}$, with $\ast = \times$.

1 is the identity element, since $\forall a \in \mathbb{R}$, $a \times 1 = 1 \times a = a$.

Multiplication is associative.

Let $a \in \mathbb{R} \setminus \{0\}$. Then $\left(\frac{1}{a}\right)a = a\left(\frac{1}{a}\right) = 1$. So $a^{-1} = \frac{1}{a}$.

Hence $(\mathbb{R} \setminus \{0\}, \times)$ forms a group.

(iii) Let $G = \{-1, 1, -i, i\} \subseteq \mathbb{C}$, with $\ast$ multiplication of complex numbers.

On board
Cancellation in groups

Let \((G, \ast)\) be a group. Let \(g, h_1, h_2 \in G\).

Suppose that \(g \ast h_1 = g \ast h_2\). Then

\[ g^{-1} \ast (g \ast h_1) = g^{-1} \ast (g \ast h_2). \]

Since \(\ast\) is associative, this means

\[ (g^{-1} \ast g) \ast h_1 = (g^{-1} \ast g) \ast h_2. \]

\[ g^{-1} \ast g = e, \text{ so } \]

\[ h_1 = e \ast h_1 = e \ast h_2 = h_2. \]

We have shown that \(g \ast h_1 = g \ast h_2 \Rightarrow h_1 = h_2\). Hence in any given row of the multiplication table for \((G, \ast)\) we cannot have any repetitions (i.e., each row must contain every element of \(G\), in some order).

Similarly \(h_1 \ast g = h_2 \ast g \Rightarrow h_1 = h_2\), so each column of the multiplication table must contain every element of \(G\), with no repetition.
A group \((G, \ast)\) is called *commutative* if \(\ast\) is commutative, i.e.,

\[
\forall g, h \in G, g \ast h = h \ast g.
\]

All the groups in the above set of examples are commutative.

A group is commutative iff its multiplication table is symmetrical about the leading diagonal.
Let \( n \in \mathbb{N} \), and write \( G = \mathbb{Z}_n = \{0, \ldots, n - 1\} \).

Let * = \( \oplus \) (addition modulo \( n \)).

Note that \( |G| = n \).

The identity element is 0.

Let \( a \in \mathbb{Z}_n \). If \( a \neq 0 \), then \((n - a) + a = a + (n - a) = n \equiv 0 \mod n\), so \( a^{-1} = n - a \).

We also have \( 0^{-1} = 0 \). Hence every element has an inverse.

Addition is associative and commutative, so \((\mathbb{Z}_n, \oplus)\) forms a commutative group.

**Example:** \( G = (\mathbb{Z}_5, \oplus) \). *On board*
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 $\odot$, multiplication modulo $p$.

The identity element is 1.

$\odot$ is associative since multiplication is associative.

$\odot$ 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 $ab \equiv 1 \pmod{p}$ (and $ba \equiv 1 \pmod{p}$).

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

Hence $a$ has inverse $r$, i.e., $a^{-1} = r$.

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

**Example**: $(\mathbb{Z}_5^*, \odot)$. On board