Math 546
Set 8
Binary Operations
Groups
Semigroups
Binary Operations

Defn. A binary operation on a set $S$ is a function $*: S \times S \to U$.

Note: This means $\forall a, b \in S \quad *(a, b) \in U$.

Ex: $S = U = \mathbb{Z}$. $+$ is addition.
This is a bin. op.
$+(3, 4) = 7$.
$+(i, j) \in U = \mathbb{Z}$.
$\forall i, j \in S = \mathbb{Z}$. etc.
Ex. \[ S = \mathbb{Z}^+ \quad U = \mathbb{R} \]

Let \[ * (a, b) = \frac{a}{b} \]

\[ \forall a, b \in \mathbb{Z}^+ \quad * (a, b) \in \mathbb{R} \]

This is a binary op.

Notice that there is not \[ * (a, b) \] in \( S = \mathbb{Z}^+ \) in general.

Ex. \[ * (1, 2) = \frac{1}{2} \notin \mathbb{Z}^+ \]

**Defn.** The binary operation \( * \) is closed (on \( S \)), if \( \forall a, b \in S \quad * (a, b) \in S \).

Ex. \[ + \] is closed on \( \mathbb{Z}^+ \).

\[ * \] is not closed on \( \mathbb{Z}^+ \).
Alert: "Closure" is sometimes included in the defn. of binary operation. This is the case in our text! Use my defn.
Defn. An operation \( \star : S \times S \to U \) is commutative if
\[
\forall a, b \in S \quad \star(a, b) = \star(b, a)
\]
Ex. + and \( \cdot \) are commutative on \( \mathbb{Z}, \mathbb{R} \)
+ is commutative on the set of \( n \times n \) matrices over \( \mathbb{R} \).
Multiplication is not commutative for \( n \times n \) matrices over \( \mathbb{R} \) for all \( n \geq 2 \).
Ex. \[
\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \neq \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}
\]
Operator Notation

Instead of functional notation \( \ast (a, b) \)
we write \( a \ast b \)
(as with +, \( \cdot \), \( \div \), \( \circ \), etc.,

Ex. + on \( \mathbb{Z} \)
we write
\[
((3 + 4) + (-2)) + 5
\]
instead of
\[
+(+(3,4), -2), 5)
\]
If we know what \( \ast \)
it, we may omit it.
Ex. \( \ast \) on \( \mathbb{R} \)
\[
(3 \cdot 4) \cdot \pi
\]
(3 \cdot 4) \pi
\[(x \cdot y) \cdot z = (xy)z = xyz\]

of fns., say perms.

\[\sigma \circ (\pi \circ \rho) \]

\[\sigma (\pi \circ \rho) \]

\[\sigma \pi \rho \]
Defn. An operation $*$ on a set $S$ is associative if $\forall a, b, c \in S$:

$$(a * b) * c = a * (b * c)$$

when $*$ is associative, one can show by induction that $\forall a_1, a_2, \ldots, a_n \in S$:

$$a_1 * a_2 * a_3 * \ldots * a_n$$

is the same no matter how it is parenthesized.

Ex. $\frac{n}{n = 4}$

$$a_1 * (a_2 * a_3) * a_4, a_1 * (a_2 * (a_3 * a_4)) = (a_1 * a_2) * (a_3 * a_4)$$

Bonus How many different ways can one parenthesize $a_1 * a_2 * \ldots * a_n$?
Ex: \((\mathbb{Z}, +)\) (commutative)\n
\((\mathbb{Z}, \times)\) (associative and commutative)

\(M_n(\mathbb{R}) = \{\text{n x n real matrices}\}\)

\((M_n(\mathbb{R}), +)\) (associative)\n
\((M_n(\mathbb{R}), \times)\) (not commutative for \(n \neq 2\))

\(S = \mathcal{F}_n\)

\(* = \text{multiplication (composition)}\)

\(\text{not associative, but not commutative.}\)

More generally, function composition is associative (but not commutative).

\[f \circ (g \circ h)(x) = (f \circ g) \circ h(x)\]

\[f(g(h(x))) = f(g(h(x)))\]
Defn: A group \((S, *)\) is a set \(S \neq \emptyset\) together with a binary operation \(*\) that is:

1. closed on \(S\), i.e., \(\forall a, b \in S\):
   \[
   a * b \in S
   \]

2. associative:
   \[
   \forall a, b, c \in S :
   (a * b) * c = a * (b * c)
   \]

3. with an identity elt.:
   \[
   \exists e \in S : \forall a \in S
   e * a = a * e = a
   \]

4. with inverses:
   \[
   \forall a \in S
   \exists a' \in S
   a * a' = a' * a = e
   \]

We need to justify the uniqueness of the identity elt.
Exs. 1. \((\mathbb{Z}, +)\)

- **Closure:** \(a, b \in \mathbb{Z} \Rightarrow a + b \in \mathbb{Z}\)
- **Assoc.:** \((a + b) + c = a + (b + c)\)
- **Identity:** 0 is the identity, \(0 + a = a + 0 = a \quad \forall a\)
- **Inverses:** \(a \in \mathbb{Z}, a' = -a\), since \(a + (-a) = (-a) + a = 0\).

\(\therefore (\mathbb{Z}, +)\) is a group!

2. \((\mathbb{Z}, \times)\)

- **Closure:** \(a, b \in \mathbb{Z} \Rightarrow a \times b \in \mathbb{Z}\)
- **Assoc.:** \((a \times b) \times c = a \times (b \times c)\)
- **Identity:** 1 is the identity, \(1 \times a = a \times 1 = a \quad \forall a\)
- **Inverses:** No, \(\forall a = 2\)

\(\text{Ex: } a \times 2 \text{ not } a = 1\), \(b \in \mathbb{Z}, b \neq 0\).

\(\frac{1}{b} \in \mathbb{Z}\), \(2 \times b = \frac{1}{b}\), \(\frac{1}{b} \in \mathbb{Z}\).

\(\therefore (\mathbb{Z}, \times)\) is not a group.
3. \((\mathbb{Q}, \times)\) closure, assoc., + identity invertible.

_if \(a \in \mathbb{Q}\) then \(a = \frac{p}{q} \Rightarrow q \neq 0\)

\[a' = \frac{1}{a} = \frac{q}{p}\]

Oops! if \(a = 0\) \(\Rightarrow\) \(a' = 0\).

\[\Rightarrow \frac{1}{a} \text{ is undefined}\]

Problem is that \(0 \times b = 1\)

has no soln. \(b \in \mathbb{Q}\).

\(\therefore (\mathbb{Q}, \times)\) is NOT a group.

4. \((\mathbb{Q}^+, \times)\) is a group by these arguments.

\((\mathbb{Z}^+, \times)\) is not a group.

\[\text{Note: we see that division} \quad \frac{p}{q} \quad \text{means} \quad p \times q^{-1}\]

\[\frac{1}{a} \quad \text{means} \quad a \times a^{-1}\]
5. An operation $S = \{1, 2\}$

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

closure: yes, by table

assoc.: $1 \times (1 \times 1) = ? (1 \times 1) \times 1 = 1$

$1 \times 2 = 2$

$2 \neq 1$ (8 cases)

No!

identity elt.:?

$1 \times 1 = 1 \neq e$

$1 \times 2 = 2 = e$ $e = 2$

$\therefore$ no inverses

6. $(\text{M}_n(\mathbb{R}), +)$

Closure: $A, B \in \text{M}_n(\mathbb{R}) \Rightarrow A + B \in \text{M}_n(\mathbb{R})$

Assoc.: prop of matrices

Identity: $e = \text{all zeros matrix}$

$A + 0_{n \times n} + A = A$
inverses?

\[ A' = -A \]

ex. \[ \begin{bmatrix} 1 & 2 \\ -1 & 5 \end{bmatrix} = \begin{bmatrix} 1 & -2 \\ -1 & 5 \end{bmatrix} \]

\[ A + (-A) = (-A) + A = O_n \]

\[ (\text{M}_n(\mathbb{R}), +) \text{ is a group.} \]

7. \((\text{M}_n(\mathbb{R}), \times)\)

- closure: \checkmark
- assoc.: \checkmark
- identity: yes, the order \(n\)
- identity matrix: \(I_n = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \)

\[ A \times I_n = I_n \times A = A \]

The inverse of a matrix is inverse:

\[ A' = A^{-1} \]
opt: it has an inverse only if it's invertible
\[ \iff \det A \neq 0 \]

example: \( \text{On} \) has no inverse.

\( (M_n(C(R)), \times) \) is NOT a group.

---

8. Let \( S = \{ A \in M_n(C(R)): \det A \neq 0 \} \)

Then \((S, \times)\) is a group:

- closure
  \[ \forall A, B \in M_n(C(R)) \quad \det A, \ \det B \neq 0, \quad \text{then} \quad AB \in M_n(C(R)) \]

- associativity: yes, as before

- identity: \( \text{In} \in S \) since \( \det \text{In} = 1 \neq 0 \)

- \( GL(n, C(R)) \) ("General Linear Group")
\text{Inverses}

If \( A \in S \), then \( A^{-1} = A^{-1} \in S \).

Note: \( \det A^{-1} = \frac{1}{\det A} \neq 0 \).

\( (S, \ast) \) is a group \( \text{GL}(n, \mathbb{R}) \).

Prop. If \( (S, \ast) \) has an identity, the identity is unique.

Proof. Suppose \( (S, \ast) \) has identity elts. \( e, f \in S \).

[Means that:
\[
\forall a \in S, \quad a \ast e = e \ast a = a \\
\ast f = f \ast a = a
\]
]

To show: \( e = f \).

Since \( f \) is an identity elt.

Since \( e \) is an identity elt.

\[ e = e \ast f \\
= f \\
\Rightarrow e = f. \]
Notation \((G, \ast)\) \(a, b \in G\)

\[
\ast(a, b) \iff a \ast b \iff ab
\]

**Prop.** Every elt. \(a\) of a group \(G\) has a unique inverse.

**Pf.** \(G\) group, \(a \in G\)

\(\Rightarrow\) by defn. \(\exists a'\) : 

\[
a' a = aa' = e.
\]

Suppose \(a'\) and \(a''\) an inverses : 

\[
a'' a = a a'' = e.
\]

to show: \(a' = a''\).

\[
\text{try:} \quad a' a
\]

\[
\text{try:} \quad a' aa'
\]

\[
\text{try:} \quad a'(aa'') = a'e = a' = e a'' = a''
\]

\[
(a' a) a'' = e a'' = a''
\]

By associativity, \(a' = a''\) is unique.
Defn. \((S, \ast)\) is a semigroup if \(\ast\) is closed and associative.

Ex. \((\mathbb{M}_n(\mathbb{C}), \ast)\) is a semigroup with identity.

Defn. A group \(G = (S, \ast)\) is abelian if it is commutative, i.e. \(\forall a, b \in S\)
\[ a \ast b = b \ast a.\]

Named after Abel

Exs. \(\mathbb{Z}, +\)
\(\mathbb{Q}^+, \times\)
\(\mathbb{M}_n(\mathbb{C}), +\)

Ex. \(\text{GL}(n, \mathbb{C})\) is non-abelian \((n \geq 2)\).

One can find matrices (invertible) \(A, B \in \text{GL}(n, \mathbb{C})\) such that \(AB \neq BA\).
(exercise)
Ex. 9 from syllabus

\[
\begin{array}{c|ccc}
& i & j & k \\
\hline
i & 1 & j & -k \\
j & -j & 1 & -i \\
k & k & i & 1 \\
\end{array}
\]

\[i^2 = j^2 = k^2 = -1\]

closure, yet (from table) -

asso.

identity 1

inverses \(i(-i) = j(-j) = k(-k) = 1 = (1)(1)\)

It is a group, but
it is non-abelian

\[ij = k, \quad ji = -k \neq k\]

quaternion group.
Ex. 10  \[ A = \{ a, b, c, \ldots, z \} \]

"letters"

"words on A":

\[ W_A = \{ \alpha_1 \alpha_2 \ldots \alpha_r \mid \alpha_i \in A \ \forall i, \ r \geq 0 \} \]

empty word is denoted \( \Lambda \).

\[ W_A = \{ \Lambda, a, b, c, \ldots, z, \]
\[ aa, ab, ac, \ldots, \]
\[ aaa, aab, \ldots \} \]

The order of the letters matters, e.g., \( ab \neq ba \).

Define \( * \) on \( W_A \) to be concatenation:

\[ \alpha_1 \alpha_2 \ldots \alpha_r * \beta_1 \beta_2 \ldots \beta_s \]
\[ = \alpha_1 \alpha_2 \ldots \alpha_r \beta_1 \beta_2 \ldots \beta_s \]

Ex: \( abc * a\bar{z} = abcaz \)
\( \neg \) * \( abc = a\bar{z} a\neg abc \)
Consider \((W_A, \ast)\)

**closure**

The concatenation of two words in \(W_A\) is a word in \(W_A\):

**associative**

\[(\alpha_1 \ldots \alpha_r * \beta_1 \ldots \beta_s) \ast \ldots \ast \]

\[= (\alpha_1 \cdots \alpha_r \beta_1 \cdots \beta_s) * \ldots * \]

\[= \alpha_1 \cdots \alpha_r \beta_1 \cdots \beta_s \ast \ldots \ast \]

Similarly,

\[\alpha_1 \ldots \alpha_r * (\beta_1 \ldots \beta_s * \ldots *)\]

\[= \alpha_1 \cdots \alpha_r \beta_1 \cdots \beta_s \ast \ldots \ast \]

**identity**

\[e = \Lambda\]

\[\Lambda * \alpha_1 \ldots \alpha_r = \alpha_1 \ldots \alpha_r * \Lambda = \alpha_1 \ldots \alpha_r\]

**inverse**

\[
\text{No!} \quad \text{Jacking \(\beta_1 \ldots \beta_s\) onto}
\]

\[
\text{never shortens it!}
\]

\[
\alpha_1 \ldots \alpha_r \text{ has an inverse}
\]

\[
\text{so only } \Lambda \text{ is a semigroup identity.}
\]
\[ (\mathbb{Z}^+, -) \]

\[ \mathbb{Z}^+ \] is not closed under -

e.g. \[ 3 - 5 = -2 \notin \mathbb{Z}^+ \]

Not a group
or a semigroup
(Not abelian either)

Ex.
\[ S = \{ 0, 1, 2, 3, 4 \} \]
\[ \ast = \text{subtraction mod 5} \]

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>4</td>
<td>2</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>4</td>
<td>2</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

\[ (0-1)-4 \]
\[ = -1 - 4 = 0 \]
\[ 0 - (1 - 4) \]
\[ = -1 + 4 = 3 \]
identity? NO
For $a - e = a$
forces $e = 0$
but $0 - 1 = -1 = 4 \neq 1$
so $0$ does not work.

commut. NO
\[ e.g. \quad 1 - 2 = -1 = 4 \]
\[ 2 - 1 = 1 \neq 4 \]
Ex. \( T = \{0, 1, 2, 3\} \)

\[ * = \text{mult. mod 4} \]

\[
\begin{array}{cccc}
0 & 1 & 2 & 3 \\
\hline
0 & 0 & 0 & 0 \\
1 & 1 & 2 & 3 \\
2 & 2 & 0 & 2 \\
3 & 3 & 2 & 1 \\
\end{array}
\]

Not a group
(0 has no inverse)
Is closed, assoc., has identity. Is semigroup
Is commutative.

Ex. \( T' = \{1, 2, 3\} \)

\[ * = \text{mult. mod 4} \]

Not even closed:
\[ 2 \times 2 = 0 \notin T' \]
Ex. \( U = \{0, 1, 2, 3, 4\} \)
\(* = \text{mult. mod 5}\)

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>3</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>4</td>
<td>3</td>
<td>2</td>
</tr>
</tbody>
</table>

Again \((U, \ast)\) is a semigroup with identity, but has no inverses for 0.

Ex. \( U' = \{3, 1, 2, 3, 4\}\)
\(*\) is now closed!

In fact, we have a group:\n- closed
- associative
- identity
- inverses

Abelian Group of "order 4".