Previously.

- Binary Operations
- Monoids

This Section.

- Groups

Definition. Suppose that

1. G is a set and $*$ is a binary operation on G,

2. $*$ is associative,

3. there is some $e \in G$ such that
$$g * e = e * g = g,$$
for all $g \in G$, and

4. for all $g \in G$, there is an $h \in G$ such that $g * h = e = h * g$.

Then $(G, *)$ is a `GROUP`.

Note. A group is a monoid where every element has an inverse!

Exercise 1. Group or not?

(a) $(\mathbb{Z}, +)$

(b) $(\mathbb{R}, +)$

(c) $(\mathbb{N}, +)$

(d) $(\mathbb{Z}_n, +)$

(e) $(M_n(\mathbb{R}), +)$

(f) $(M_n(\mathbb{R}), \cdot)$

(g) $(\mathbb{R}, \cdot)$

(h) $(\mathbb{Z}, \cdot)$

(i) $(\mathbb{Z}_4, \cdot)$

(j) $(\mathbb{Z}_n, \cdot)$

(k) $(\mathbb{Z}_p, \cdot)$

(l) $(S_3, \circ)$

Definition. The `nth roots of unity` are the complex numbers that are the roots of
$$x^n - 1.$$
Denote the set of roots as $\mathcal{U}_n$

Definition. If the operation of a group G is commutative, we call G an `abelian group`.

Theorem 2.1.4. If $(G, *)$ is a group and $g \in G$, then the inverse of g is unique.

Theorem 2.2.1. If $(M, \cdot)$ is a monoid, then the set of all units M^* is a group using the operation $\cdot$, called the `unit group`.

Exercise 2. Consider the following monoids. Determine their group of units.

- $(\mathbb{R}, \cdot)$ has units $\mathbb{R}^* =$

- $(\mathbb{Z}, \cdot)$ has units $\mathbb{Z}^* =$

- $(\mathbb{Z}_4, \cdot)$ has units $\mathbb{Z}_4^* =$

Theorem 2.2.2. If $G_1, G_2, \ldots, G_n$ are groups with respective operations $*_1, *_2, \ldots, *_n$, then

$$G_1 \times G_2 \times \cdots \times G_n$$

is a group under component-wise operation

$$(g_1, g_2, \ldots, g_n) * (h_1, h_2, \ldots, h_n) = (g_1 *_1 h_1, g_2 *_2 h_2, \ldots, g_n *_n h_n).$$

Theorem 2.2.3. Let $g, h, g_1, g_2, \ldots, g_{n-1}, g_n$ be elements of a group G ($n \in \mathbb{Z}_{\geq 1}$).

1. $e^{-1} =$

2. $(g^{-1})^{-1} =$

3. $(gh)^{-1} =$

4. $(g_1 g_2 \cdots g_n)^{-1} =$

5. $(g^m)^{-1} =$ for all $m \geq 0$.

Theorem 2.2.4 (Exponent Laws). Let G be a group and $g, h \in G$. Then for all $m, n \in \mathbb{Z}$, the following hold,

1. $g^n g^m =$

2. $(g^n)^m =$

3. If $gh = hg$, then $(gh)^n =$

Theorem 2.2.5 (Cancellation Laws). Let G be a group and $g, h, f \in G$.

1. If $gh = gf$ then $h = f$ (`left cancellation`)
2. If $hg = fg$ then $h = f$ (`right cancellation`)

Theorem 2.2.6. Let G be a group and $g, h \in G$.

1. The equation $gx = h$ has a unique solution $x = g^{-1}h$ in G.
2. The equation $xg = h$ has a unique solution $x = hg^{-1}$ in G.

Definition. A `Cayley table` is essentially a multiplication table for a given binary operation.

Example.

$*$	e	a	b
e	e	a	b
a	a	a^2	$a * b$
b	b	$b * a$	b^2

Exercise 3. Complete the Table for $(\mathbb{Z}_3, +)$

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

Exercise 4. Consider operation $*$ with the Cayley table

$*$	e	a	b	c
e	e	a	b	c
a	a	a	b	e
b	b	b	c	c
c	c	e	c	e

(a) Is $*$ commutative? Why?

(b) Is there an identity?

(c) Determine $a * (b * c)$ and $(a * b) * c$. Is $*$ associative?

(d) Is it a monoid?!

Question 5. How many groups are there with 1 element?

Question 6. How many groups are there with 2 elements?

Let $G = \{e, g\}$ be a group with 2 elements. Complete the Cayley table.

$*$	e	g
e	e	g
a	g	

(Recall that in a group, every element must have an inverse!)

Note. Note that if $(G, *)$ is a group, every element appears exactly 1 time in every row and every column.

Exercise 7. If $G = \{e, g, h\}$ is a group, complete the Cayley table,

$*$	e	g	h
e	e	g	h
g	g		
h	h		

Note. We will say *up to isomorphism* there is only one group of order 3.

That is all of the following have the same group structure, even though they're different objects.

(a) $(\mathbb{Z}_3, +)$ - equivalences modulo 3

(b) $(A_3, \circ)$ - the alternating group on 3 elements

(c) $(\{1, \frac{-1+i\sqrt{3}}{2}, \frac{-1-i\sqrt{3}}{2}\}, \cdot)$ - the third roots of unity

Exercise 8. What about a group with 4 elements, is there 1 or are there more? (I leave two tables for exploration purposes.)

$*$	e	g	h	k
e	e	g	h	k
g	g			
h	h			
k	k			

$*$	e	g	h	k
e	e	g	h	k
g	g			
h	h			
k	k			