Content:

Definition	binary operation, group, abelian group
Properties	groups
Theorem	If G is finite, has an associative binary operation and cancellation holds, then is G a group.
Definition	Cayley Table, mod n
Examples	groups
Definition	Complex Numbers
Theorem	DeMoivre's $(\cos\theta + i\sin\theta)^n = (\cos n\theta + i\sin n\theta)$
Theorem	Euler's $e^{i\theta} = \cos\theta + i\sin\theta$
Definition	nth root of unity, primitive root of unity
Defintiion	order of a group element
Theorem	Let G be a group with $a \in G$ such that $\circ(a) = n$. Then $a^m = 1 \Leftrightarrow n \mid m$.

2.3 Groups

Definition A *binary operation* is a function $* : G \times G \to G$.

Well-defined binary operation
Closed binary operation
} redundant

Definition Let G be a set with a binary operation. Then G is a *group* if the following holds:

1) The operation is associative.
2) There is an identity element.
(i.e. $\exists\ e \in G$ such that $e * x = x * e = x$, $\forall\ x \in G$.
3) Every element has an inverse.
(i.e. If $g \in G$, then $\exists\ g' \in G$ such that $g * g' = e = g' * g$.)

Examples $\langle \mathbb{Z}, + \rangle, \langle \mathbb{Q}^*, \bullet \rangle, \langle S_n, \circ \rangle$.

Non-examples $\langle \mathbb{Z}, - \rangle, \langle \mathbb{Z}, \bullet \rangle$.

Definition A group is *abelian* if $g * h = h * g$ for all $h, g \in G$.

In an arbitrary group, we write
ab to mean $a * b$
a^{-1} to mean the inverse of a
1_G or e to mean the identity of group, G

Properties of groups:

Let G be a group.
1) Cancellation Law holds
i.e. If $ab = ac$ in G, or $ba = ca$ then $b = c$ (assume $a \neq 0$).
2) The identity of G is unique.
3) Each inverse is a unique inverse.
4) $(a^{-1})^{-1} = a$ (This follows from uniqueness)
5) $ax = b$ and $ya = b$ have unique solutions in G.

Question Suppose G has an associative binary operation and cancellation holds, is G a group? Not necessarily.
Counterexample: $\langle \mathbb{Z}^*, \bullet \rangle$

Question Suppose G is finite, has an associative binary operation and cancellation holds, is G a group? Yes.

Proof:
$G = \{a_1, a_2, \ldots, a_n\}$.
$\forall$ integer $m \geq 1$, $a_i^m \in$ G by closure.
Fix i such that $1 \leq i \leq n$, then $a_i^j = a_i^k$, where $j < k$.
Thus, $a_i^j = a_i a_i^{j+(k-j)} = a_i^j a_i^{k-j}$.
We will show that a_i^{k-j} is the **identity** for G.
Let $b \in G$, the $b\ a_i^j = b\,(a_i^j a_i^{k-j})$
$= b\,(a_i^{k-j} a_i^j)$
$= (b\, a_i^{k-j})\, a_i^j$
By the cancellation property, we have $b = b\, a_i^{k-j}$.
Similarly, we can show that $b = a_i^{k-j}\, b$.
$\therefore$ a_i^{k-j} is the identity, e, for G.

We now show that $\forall\ b \in G$, b has an **inverse**.
As noted above, $b^p = b^q$, for some integers $p \geq 1$ and $q \geq 1$.
Assume, without loss of generality that $p < q$, hence $q - p \geq 1$.
We know that $b^p\, e = b^q = b^p\, b^{q-p}$.
By the cancellation property, we have $e = b^{q-p}$.
Suppose $q - p = 1$, then $e = b^1$. Since $e^{-1} = e$, then $b^{-1} = b$.
Suppose $q - p > 1$, then $e = b\, b^{q-p-1} = b^{q-p-1}\, b$. This gives us $b^{-1} = b^{q-p-1}$.
$\therefore$ G is a group.

Recall Cayley Tables.

Let $G = \{e, a, b\}$ be a group.

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

← This cannot be a because $ab = a \Rightarrow ab = ae \Rightarrow b = e$.
Similarly, it cannot be b, so it must be e.

So, every group of order 3 looks like this Cayley Table.

Recall mod n integers.

$\mathbb{Z}_n = \{[b] | b \in \mathbb{Z}\}$

$a \sim b$ iff $a \equiv b \pmod{n}$

$\langle \mathbb{Z}_n, + \rangle$ is a group.

[a] +[b] = [a + b]

new addition that need to be defined

regular addition

Examples of Groups

1. **General Linear Group:** GL $(n, \mathbb{R})$ = {invertible $n \times n$ matrices with real entries}

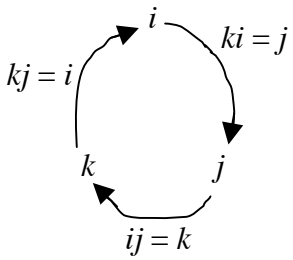
This is a group with respect to multiplication.

Not addition because $\begin{vmatrix} 0 & 0 \\ 0 & 0 \end{vmatrix}$ is not invertible.

2. **Special Linear Group**: SL $(n, \mathbb{R}) = \{A \in \text{GL}(n, \mathbb{R}) : \det A = 1\}$.

3. **Quaternions** $= \{\pm 1, \pm i, \pm j, \pm k\}$.

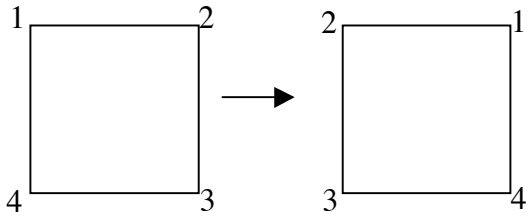
$i^2 = j^2 = k^2 = -1$. $\quad ijk = -1$.



4. **Dihedral Group**: Group of symmetris of a regular n-gon, denoted D_{2n}. There are $2n$ elements in D_{2n}.

$D_8 = \{r_0, r_{90}, r_{180}, r_{270}, h, v, d_1, d_2\}$

There are 8 elements in D_8. (It is sometimes called D_4 as you are looking at a 4-sided figure.)



Vertical flip, "v" produces (12)(34)

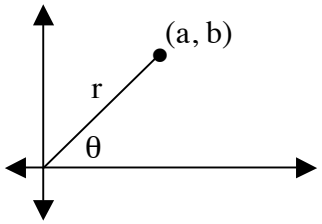
A quick review of Complex numbers:

$\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$.

$z = a + bi$. The modulus of z is $|z| = \sqrt{a^2 + b^2}$.

Polar decomposition: $z = r(\cos\theta + i \sin\theta)$.

$|z| = r$.



$z = r(\cos\theta + i \sin\theta)$

$w = s(\cos\phi + i \sin\phi)$

$z \bullet w = rs(\cos\theta + i \sin\theta)(\cos\phi + i \sin\phi)$

$= rs[(\cos\theta)(\cos\phi) + i(\sin\theta)(\cos\phi) + (\cos\theta)(i\sin\phi) + (i\sin\theta)(i\sin\phi)]$

$= rs[(\cos\theta)(\cos\phi) - (\sin\theta)(\sin\phi) + i[(\sin\theta)(\cos\phi) + (\cos\theta)(i\sin\phi)]]$

$= rs(\cos(\theta + \phi) + i \sin(\theta + \phi))$.

DeMoivre's Theorem

$(\cos\theta + i \sin\theta)^n = (\cos n\theta + i \sin n\theta)$

Proof by induction is in text, p. 17

Euler's Theorem

$e^{i\theta} = \cos\theta + i \sin\theta$

Proof by power series expansion is in text, p. 18

So, we have 3 ways to represent complex numbers.

1) $z = a + bi$
2) $z = r(\cos\theta + i \sin\theta)$
3) $z = r\, e^{i\theta}$

Circle Group: $S = \{z \in \mathbb{C} \mid |z| = 1\}$ is a group.

Proof:

We have closure as $\forall\, z, w, \in S$, $z \bullet w = rs(\cos(\theta + \phi) + i \sin(\theta + \phi))$

$= (\cos(\theta + \phi) + i \sin(\theta + \phi))$.

We have an identity: $z = 1$.

Each element has an inverse: If $z = a + bi$, then $z^{-1} = 1/(a + bi)$

$= (a - bi)/(a^2 + b^2)$

$= a - bi$

Definition If $n \geq 1$, then z is an *nth root of unity*.

(Every nth root of unity is equal to $e^{\frac{2\pi ik}{n}} = \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}$, for some $k = 0, 1, \ldots$)

Examples

n	Roots of Unity
1	$\{1\}$
2	$\{\pm 1\}$
3	$\{1, e^{\frac{2\pi i}{3}}, e^{\frac{4\pi i}{3}}\}$ $=\{1, \cos(2\pi/3) + i\sin(2\pi/3), \cos(4\pi/3) + i\sin(4\pi/3)\}$ $=\{1, -1/2 + (\sqrt{3}/2)i, -1/2 - (\sqrt{3}/2)i\}$
4	$\{\pm 1, \pm i\}$

If μ_n = the set of nth roots of unity, then μ_n is a group with respect to multiplication.

Powers

Let G be a group, $a \in G$, $n \in \mathbb{Z}$.

Multiplicatively	Additively
1) For $n \geq 1$, $a^1 = a$, $a^n = a \bullet a^{n-1}$.	1) For $n \geq 1$, $1a = a$, $na = a + (n-1)a$.
2) Define $a^0 = 1_G$.	2) Define $0a = 0_G$.
3) For $n \geq 1$, $a^{-n} = (a^{-1})^n$.	3) For $n \geq 1$, $-na = n(-a)$

Properties

1) $a^n a^m = a^{n+m}$.
2) $(a^n)^m = a^{nm}$.
3) If a, b commute, then $(ab)^n = a^n b^n$.

Definition Let G be a group and $a \in G$. The *order* of a, $\circ(a)$, is the smallest positive power, n, such that $a^n = 1_G$. If no such n exists, we say a has infinite order.

Examples 1) $z = e^{\frac{2\pi i}{3}} \in \mu_3$. $\circ(z) = 3$

(Since $\left(e^{\frac{2\pi i}{3}}\right)^3 = e^{2\pi i} = \cos 2\pi + i\sin 2\pi = 1 + 0 \bullet i = 1$ and $e^{\frac{2\pi i}{3}} \neq 1$, $\left(e^{\frac{2\pi i}{3}}\right)^2 \neq 1$)

2) $-1 \in \mu_4$ where $\mu_4 = \{\pm 1, \pm i\}$. $\circ(-1) = 2$.

Definition z is a *primitive* nth root of unity if $\circ(z) = n$.

Example In μ_4, i and $-i$ are the primitive roots of unity.

$z \in \mu_4$	Powers of z	$\circ(z)$
1	$1^1 = 1$	1
-1	$(-1)^1 = -1, (-1)^2 = 1$	2
i	$i^1 = i, i^2 = -1, i^3 = -i, i^4 = 1$	4
$-i$	$(-i)^1 = -i, (-i)^2 = -1, (-i)^3 = i, (-i)^4 = 1$	4

Theorem Let G be a group with $a \in G$ such that $\circ(a) = n$. Then $a^m = 1 \Leftrightarrow n \mid m$.

Proof:
$\Leftarrow$: Assume $n \mid m$, then $n = mk$ for some $k \in \mathbb{Z}$.
$a^m = a^{nk} = (a^n)^k = 1_G^k = 1_G$.
$\Rightarrow$: Assume $a^m = 1$. Then $\exists\ q, r \in \mathbb{Z}$ such that $m = nq + r$ and $0 \le r < n$.
$1_G = a^m = a^{nq+r} = a^{nq}\, a^r\ 1_G\, a^r = a^r$. Since $\circ(a) = n$, then n is the smallest natural number for which $a^n = 1_G$. Hence, if $r \neq 0$, $n \le r$. But $r < n$. $\therefore$ r = 0.
This gives us that $m = nq + 0$, or $n \mid m$.

Examples Let G be a group. $a \in G$ such that $\circ(a) = 3$.
$\circ(a^5) = ?$
Since $(a^5)^3 = (a^3)^5 = 1^5 = 1$, then $\circ(a^5) \le 3$.
Let's check: $(a^5)^1 = a^5 = a^3 \bullet a^2 \neq 1$. $(a^5)^2 = a^{10} = a^3 \bullet a^3 \bullet a^3 \bullet a^1 \neq 1$.