Cyclic Groups

Theorem

$\langle a \rangle = \{a^n \mid n \in Z\}$ is a group.

Proof

Associativity

$$
\begin{aligned}
&\text{Assume } x, y, z \in \langle a \rangle \\
&\exists\, r, s, t \in \mathbb{Z}, x = a^r, y = a^2, z = a^t \\
&(xy)z = (a^r a^s)a^t = a^{r+s}a^t = a^{r+s+t} \\
&x(yz) = a^r(a^s a^t) = a^r a^{s+t} = a^{r+s+t} \\
&\therefore \langle a \rangle \text{ is associative.}
\end{aligned}
$$

Identity

$$
\begin{aligned}
&a^0 \in \langle a \rangle \\
&\text{Assume } a^n \in \langle a \rangle \\
&a^0 a^n = a^{0+n} = a^n \\
&a^n a^0 = a^{n+0} = a^n \\
&\therefore a^0 = e \in \langle a \rangle
\end{aligned}
$$

Inverses

$$
\begin{aligned}
&\text{Assume } a^n \in \langle a \rangle \\
&a^{-n} \in \langle a \rangle \\
&a^{-n} a^n = a^{-n+n} = a^0 = e \\
&a^n a^{-n} = a^{n+(-n)} = a^0 = e
\end{aligned}
$$

$\therefore \langle a \rangle$ is a group.

Definition

To say that a group G is *cyclic* means $\exists\, a \in G, \langle a \rangle = G$. The element a is said to *generate* G and a is called a *generator* for G. G is said to be *generated* by a.

Theorem

$$\left\langle a^{-1} \right\rangle = \langle a \rangle$$

Proof

$\implies$ Assume $(a^{-1})^n \in \langle a^{-1} \rangle$

$$
\begin{aligned}
&(a^{-1})^n = a^{-n} \in \langle a \rangle \\
&\therefore \langle a^{-1} \rangle \subseteq \langle a^n \rangle
\end{aligned}
$$

$\Longleftarrow$ Assume $a^n \in \langle a \rangle$

$a^n = (a^{-1})^{-n} \in \langle a^{-1} \rangle$
$\therefore \langle a^n \rangle \subseteq \langle a^{-1} \rangle$

$\therefore \langle a^{-1} \rangle = \langle a \rangle$

Example

$Z_4 = \{0, 1, 2, 3\}$

$1 + 3 = 3 + 1 = 0$
$-1 = 3$ and $-3 = 1$

$\langle 1 \rangle = \{1, 2, 3, 0\} = \mathbb{Z}_4$
$\langle 3 \rangle = \{3, 2, 1, 0\} = \mathbb{Z}_4$

$\langle 1 \rangle = \langle 3 \rangle = \mathbb{Z}_4$

Theorem

Let G be a group:

$$G \text{ cyclic} \implies G \text{ abelian}$$

Proof

Assume G is cyclic
$\exists\, a \in G, \langle a \rangle = G$
Assume $x, y \in G$
$\exists\, n, m \in G, x = a^n$ and $y = a^m$
$xy = a^n a^m = a^{n+m} = a^{m+n} = a^m a^n = yx$
$\therefore G$ is abelian.

Note that the inverse is not true: consider K_4:

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

$$\begin{aligned} \langle e \rangle &= \{e\} \\ \langle a \rangle &= \{e, a\} \\ \langle b \rangle &= \{e, b\} \\ \langle c \rangle &= \{e, c\} \end{aligned}$$

It is abelian; however, it has no generator and is thus not cyclic.

Theorem

Let G and G' be groups and $\phi : G \to G'$ be an isomorphism:

$$\forall\, a \in G, \forall\, n \in \mathbb{Z}, \phi(a^n) = \phi(a)^n$$

Proof

Assume $a \in G$ Assume $n \in \mathbb{Z}$

Case 1: $n > 0$

Proof by induction on n

Base: $n = 1$

$$\phi(a^1) = \phi(a) = \phi(a)^1$$

Assume $\phi(a^n) = \phi(a)^n$

Consider $\phi(a^{n+1})$

$$\phi(a^{n+1}) = \phi(a^n a) = \phi(a^n)\phi(a) = \phi(a)^n \phi(a) = \phi(a)^{n+1}$$

Case 2: $n = 0$

$$\phi(a^0) = \phi(e) = e' = \phi(a)^0$$

Case 3: $n < 0$

Let $m = -n$
$n > 0$
$\phi(a^n) = \phi(a^{-m}) = \phi[(a^m)^{-1}] = \phi(a^m)^{-1} = [\phi(a)^m]^{-1} = \phi(a)^{-m} = \phi(a)^{-(-n)} = \phi(a)^n$

Theorem

Let G and G' be groups and $\phi : G \to G'$ be an isomorphism:

1). G cyclic $\implies$ G' cyclic

2). ϕ maps generators in G to generators in G'

Proof

Assume G is cyclic
$\exists\, a \in G, \langle a \rangle = G$
Assume $b' \in G'$
ϕ is onto
$\exists\, b \in G, \phi(b) = b'$
$\exists\, n \in \mathbb{Z}, b = a^n$
$b' = \phi(b) = \phi(a^n) = \phi(a)^n$
$\therefore\, \phi(a)$ is a generator for G' and G' is cyclic.

Definition

Let G be a group. An *automorphism* of G is an isomorphism between G and itself: $\phi : G \to G$.

To determine the number of possible automorphisms for a cyclic group, determine the number of generators.

Theorem

Let $\langle a \rangle = G$ and $|G| = n$:

- G finite $\implies n \in \mathbb{Z}^+$ is the smallest positive number such that $a^n = e$.
- G infinite $\implies n = \aleph_0$

Proof

Assume G is finite

$a \in G$, so $n > 0$
$n \in \mathbb{Z}^+$
$\exists\, m \in \mathbb{Z}^+, a^m = e$
Let $m \in \mathbb{Z}^+$ be the smallest positive number such that $a^m = e$
Let $G' = \{a^k \mid 0 \leq k < m\}$
ABC: G' contains duplicates
$\exists\, h, k \in \mathbb{Z}^+, 0 \leq h < k < m$ and $a^h = a^k$
$a^{k-h} = e$
But $1 \leq h - k < m$
CONTRADICTION! (on the minimality of m)
So G' contains m distinct elements, and all $a^k, k \geq m$ are duplicates
$\therefore |G| = m = n$

Assume G is infinite

$\forall\, n \in \mathbb{Z}^+, a^n \neq e$
ABC: $\exists\, h, k \in \mathbb{Z}^+, 1 \leq h < k$ and $a^k = a^k$
$a^{k-h} = e$
CONTRADITION!
So $\forall\, n \in \mathbb{Z}^+, a^n$ is distinct
So G is countably infinite
$\therefore |G| = \aleph_0$

Theorem

Let G be a cyclic group and $|G| = n$:

- G finite $\implies G \simeq \mathbb{Z}_n$
- G infinite $\implies G \simeq \mathbb{Z}$

Proof

Assume G is finite

$n \in \mathbb{Z}+$
Let a be a generator for G
$G = \{a^k \mid k \in \mathbb{Z}^+ \cup \{0\}$ and $0 \leq k < n\}$
All of the $a^k \in G$ are distinct

Let $\phi : G \to \mathbb{Z}_n$ such that $\phi(a^k) = k$
Clearly, ϕ is bijective
Assume $a^k \in G$
Per the division algorithm, $k = qn + r$ where $q, r \in \mathbb{Z}$ and $0 \leq r < n$
$a^k = a^{qn+r} = (a^n)^q a^r = e^q a^r = a^r$
$k \equiv r \pmod{n}$
Assume $a^h, a^k \in G$
$\phi(a^h a^k) = \phi(a^{h+_n k}) = h +_n k = \phi(a^h) +_n \phi(a^k)$
So ϕ is bijective and a homomorphism, and thus an isomorphism
$\therefore G \simeq \mathbb{Z}_n$

Assume G is infinite

$n \in \aleph_0$
Let $G = \{a^k \mid k \in \mathbb{Z}^+ \cup \{0\}\}$
All of the $a^k \in G$ are distinct
Let $\phi : G \to \mathbb{Z}$ such that $\phi(a^k) = k$
Clearly, ϕ is bijective
Assume $a^h, a^k \in G$
$\phi(a^h a^k) = \phi(a^{h+k}) = h + k = \phi(a^h) + \phi(a^k)$
So ϕ is bijective and a homomorphism, and thus an isomorphism
$\therefore G \simeq \mathbb{Z}$

Thus, all finite cyclic groups are isomorphic to each other (via $\mathbb{Z}_n$) and all infinite cyclic groups are isomorphic to each other (via $\mathbb{Z}$).

Furthermore, all structural proofs on cyclic groups can be performed more easily in terms of Z_n or Z.