Subgroups (For convenience, we omit the operation.)

Defn. If $H \subseteq G$, G is a group and H is a group itself, then H is a subgroup of G, denoted by $H \leq G$. $H < G$ denotes that $H \leq G$ and $H \neq G$, and H is called a proper subgroup of G.

Defn. $\{e\}$ is the trivial subgroup of G and G is an improper subgroup of G.

Example Groups of order 4

$\mathbb{Z}_4$:

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

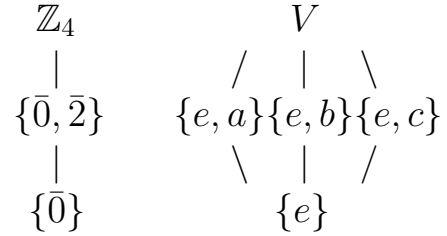
Klein 4-group $V(Vier)$:

0	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

$\mathbb{Z}_2 \times \mathbb{Z}_2 \quad (x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$

$+$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,1)$	$(0,1)$	$(0,0)$	$(1,1)$	$(1,0)$
$(1,0)$	$(1,0)$	$(1,1)$	$(0,0)$	$(0,1)$
$(1,1)$	$(1,1)$	$(1,0)$	$(0,1)$	$(0,0)$

Subgroup Diagram



(*) Use a^{-1} for the inverse element of a.

Theorem A subset H of a group G is a subgroup of G iff

1. H is closed under the binary operation of G.
2. The identity element e of G is in H.
3. $\forall\ a \in H,\ a^{-1} \in H$.

Theorem A subset H of a group G is a subgroup of G iff $\forall\ a, b \in H,\ ab^{-1} \in H$ (b^{-1} is defined in G).

Proof.

($\Leftarrow$) Since $aa^{-1} \in H,\ e \in H$. By $ea^{-1} \in H$, we have $a^{-1} \in H$ for each $a \in H$. Therefore $ab = a(b^{-1})^{-1} \in H$. These conclude that $H \leq G$.

($\Leftarrow$) is trivial.

Example

G : {Invertible $n \times n$ matrices}.

T : {Invertible $n \times n$ matrices A with determinant $det(A) = 1$}.

$T \leq G$. (Multiplicative group)

Theorem If $H \leq G$ and $K \leq G$, then $H \cap K \leq G$.

Theorem If G is an abelian group, $H \leq G$ and $K \leq G$, then
$$HK = \{hk | h \in H \ and \ k \in K\} \leq G.$$

Theorem Let G be a group and S be a nonempty subset of G. Then
$$H_S = \{x | xs = sx\ \forall\ s \in S\} \text{ is a subgroup of } G.$$

Theorem The **center** of G, H_G, is an abelian group.

Proof. $\forall\ a, b \in H_G,\ ab = ba$. ($a$ is in center and b is from G.)

$$a^n = \underbrace{a \cdot a \cdots a}_{n\text{-tuple}} \qquad a^{-m} = \underbrace{a^{-1} \cdot a^{-1} \cdots a^{-1}}_{m\text{-tuple}}$$

Observation If G is a group and $a \in G$, then $\forall\ n \in \mathbb{Z},\ a^n \in G$.

(*)Theorem Let G be a group and $a \in G$. Then $< a >_G = \{a^n | n \in \mathbb{Z}\}$ is a subgroup of G and is the smallest subgroup of G which contains a, that is, every subgroup of G containing a contains $< a >_G$.

Proof. Note that a^{-n} is the inverse element of a^n. ■

Defn. A group G is a cyclic group if $G =< a >$ (generated by a) for some $a \in G$.

Defn. Let a be an element of a group G. Then $< a >$ is a cyclic subgroup of G.

Example $\mathbb{Z}_4$ is cyclic but not V.

Theorem Every cyclic group is abelian.

Theorem An (infinite) cyclic group is isomorphic to $< \mathbb{Z}, + >$.

Defn. If $G =< a >$, then G is generated by a and a is a generator of G. (G may have many different generators.)

Defn. Let a be an element of G. Then the number of elements in $< a >$ is the order of a. If $| < a > | < +\infty$, then the order is finite and the order is infinite otherwise.

$$\forall\ n, m \in \mathbb{Z}\ where\ m \in \mathbb{Z}^+$$
$$\Rightarrow\ n = mq(quotient) + r(remainder),\ 0 \leq r < m.$$

(Division Algorithm)

Theorem A subgroup of a cyclic group is cyclic.

Proof. $H \leq G$(cyclic), let $G =< a >$. ($H \subseteq \{a^n | n \in \mathbb{Z}\}$)

(i) $H = \{e\},\ H =< e >$.

(ii) $H \neq \{e\}$, $\exists$ a smallest positive integer $m \in \mathbb{Z}^+$ such that $a^m \in H$.
Claim $H =< a^m >$ by using division algorithm. ■

$n\mathbb{Z} =< n >$ (in $\mathbb{Z}$)
$\downarrow \quad \downarrow$
cyclic subgroups of $\mathbb{Z}$.

Example Let r and s be two positive integers and

$$H = \{mr + ns | m, n \in \mathbb{Z}\}. \text{ Then } H \leq \mathbb{Z} \text{ and } H =< d >.$$

$$\Rightarrow d = g.c.d.(r, s).$$

Proof. Since $r \in H$ and $s \in H$, $d|r$ and $d|s$. Now, if d' is a common divisor of r and s, then $d'|m_0 r + n_0 s = d$. ■

Theorem A finite cyclic group of order n is isomorphic to $< \mathbb{Z}_n, +_n >$.

Proof. Let $G =< a >$ where $a^n = e$ (n is the smallest positive integer.)

Claim: $e = a^0, a, a^2, \cdots, a^{n-1}$ are distinct elements.
($a^{h-k} = e$, where $0 < h - k < n$) $\rightarrow\leftarrow$

Claim: $\psi : G \rightarrow \mathbb{Z}_n$ defined by $\psi(a^i) = i$ for $i = 0, 1, \cdots, n-1$ is an isomorphism.

$$\psi(a^i a^j) = \psi(a^{i+j}) = i +_n j = \psi(a^i) +_n \psi(a^j).$$ ■

Important fact $\mathbb{Z}_9$ is not a subgroup of $\mathbb{Z}_{18}$!

In $\mathbb{Z}_{18}$, $< \bar{2} >_{18} = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \bar{10}, \bar{12}, \bar{14}, \bar{16}\}$
$< \bar{3} >_{18} = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}, \bar{12}, \bar{15}\}$
$(*)$ $< \bar{5} >_{18} = \mathbb{Z}_{18}$

Theorem $(**)$ Let G be a cyclic group of order n generated by a and $b = a^s$ where $s \in \mathbb{Z}^+ \cup \{0\}$ and $d = gcd(n, s)$. Then $< b >$ is a cyclic subgroup of G of order n/d. Also, $< a^s >=< a^t >$ iff

$gcd(s,n) = gcd(t,n)$.

Proof. Claim: n/d is the smallest positive power of b such that $b^{n/d} = e$. If $n \in \mathbb{Z}^+$ satisfies $b^m = e$, then $a^{sm} = e$ and hence $n|sm$. Since $d = gcd(s,n)$, $\frac{n}{d}|\frac{s}{d} \cdot m$, now, $gcd(\frac{n}{d}, \frac{s}{d}) = 1$, $\frac{n}{d}|m$. Therefore, it suffices to show $b^{n/d} = e$, it follows from $b^{n/d} = (a^s)^{n/d} = a^{sn/d} = a^{(s/d)n} = e$. The second part can be obtained following the fact they have the same number of elements.

Corollary The number of generators of $\mathbb{Z}_n$ is equal to $\phi(n)$.

Proof. If $gcd(s,n) = 1$, then $< a^s >$ has n elements and thus $< a^s >= \mathbb{Z}_n$.

Theorem $\sum_{d|n} \phi(d) = n$.

Proof. $\phi(d)$ is the number of elements which generate $\mathbb{Z}_d$.

Let $n = sd$, then $< a^s > \cong \mathbb{Z}_d$ where $< a^s > \leq \mathbb{Z}_n$. As long as $gcd(s', n) = s$, $< a^{s'} > \cong \mathbb{Z}_d$, since $n = sd$, $s' = s \cdot d'$ where $gcd(d', d) = 1$. Furthermore, $s' \leq n$ implies that $d' \leq d$. Therefore, there are exactly $\psi(d)$ s''s which gives $< a^{s'} > \cong \mathbb{Z}_d$. Since $\forall\ 0 \leq x \leq n-1$, $< a^x > \cong \mathbb{Z}_d$ for some $d|n$, thus

$$n = \sum_{d|n} \psi(d).$$