Subgroups § 5 Fraleigh.

Read "notation + terminology" pg 49.

Switch from $a*b$ to ab. multiplicative notation

For G commutative we sometimes use $a+b$ additive notation

$a*b \Rightarrow$ ab multiplicative
$a+b$ additive

$a' \Rightarrow$ a^{-1} multiplicative
$-a$ additive

$e \Rightarrow$ 1 multiplicative
0 additive

Def 5.4 A subset H of a group $(G,*)$ is a subgroup if it is itself a group under $*$.

Recall Group axioms:

To check a subgroup:

G0 $(H,*)$ is a binary structure.

G1 $*$ is associative

G2 $e \in H$ identity

G3 $\forall\, a \in H$ $\exists$ inverse $a^{-1} \in H$.

Thm 5.14 A subset H of $(G,*)$ is a subgroup if and only if

1) H is closed under $*$

2) the identity e of G is in H

3) $\forall\, a \in H$, $a^{-1} \in H$.

Examples 1) $(n\mathbb{Z},+) < (\mathbb{Z},+) \leq (\mathbb{Q},+) \leq (\mathbb{R},+) \leq (\mathbb{C},+)$.

2) $(U,\cdot) \leq (\mathbb{C}^\times,\cdot)$.

3) $* = +$ $\quad H_2 = \underset{\text{differentiable}}{\{f:\mathbb{R}\to\mathbb{R}\}} \leq H_1 = \underset{\text{continuous}}{\{f:\mathbb{R}\to\mathbb{R}\}} \leq G = \{f:\mathbb{R}\to\mathbb{R}\}$

4) $* = \cdot$ $\quad GL_n(\mathbb{R}) \geq SL_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) \mid \det A = 1\}$.

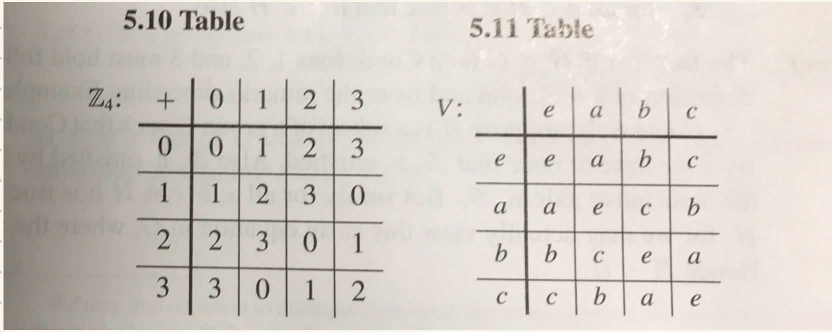
Ex 5.16.

Def 5.5 • The **improper subgroup** is $G \leq G$.

• The **trivial subgroup** is $\{e\} \leq G$

• All other subgroups are called **non-trivial**

Subgroup diagrams

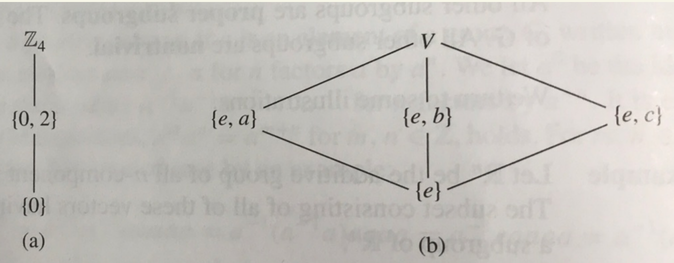


5.10 Table

$\mathbb{Z}_4$: $+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

5.11 Table

V:	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e



5.12 Figure (a) Subgroup diagram for $\mathbb{Z}_4$. (b) Subgroup diagram for V.

Cyclic Subgroups

Def 5.18 Let G be a group. then $H = \{a^n \mid n \in \mathbb{Z}\}$ is the cyclic subgroup generated by a. Write $H = \langle a \rangle$.
The element a is a generator of H

Thm 5.17 $H = \{a^n \mid n \in \mathbb{Z}\}$ is a group.

Proof. • H is closed $a^n a^m = a^{n+m} \in \mathbb{Z}$

• $e \in H$ since $a^0 = e$.

• if $b = a^n \in H$ then $b^{-1} = a^{-n} \in H$ □.

Cyclic Groups   § 6 Fraleigh

Def A group G is cyclic if $G = \{a^n \mid n \in \mathbb{Z}\}$ for some $a \in G$.

The element a is a generator of G

Ex • $(\mathbb{Z}, +)$ is cyclic ⚠ mult → additive $a^n := \underbrace{a + \cdots + a}_{n \text{ times}}$

generators $a = 1$ or -1.

• $(\mathbb{Z}_n, +_n)$ modular arithmetic

$\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$

$$a +_n b = \begin{cases} a+b & \text{if } < n \\ a+b-n & \text{if } \geq n. \end{cases}$$

Thm 6.1 Every cyclic group is abelian

Proof Let $G = \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$. and $g_1, g_2 \in G$.

Then $g_1 = a^r$ and $g_2 = a^s$ for some $r, s \in \mathbb{Z}$.

$$g_1 g_2 = a^r a^s = a^{r+s} = a^s a^r = g_2 g_1 \quad \square.$$

Division algorithm $\mathbb{Z}$ 6.3 If $m \in \mathbb{Z}^+$ and n any integer $\exists$ a unique q and r with $0 \leq r < m$ and $n = qm + r$.

Proof see text.

Thm 6.6 A subgroup of a cyclic group is cyclic.

Proof Let $G=\langle a\rangle$ and $H\le G$. If $H=\{e\}$ it is cyclic. Otherwise let $m\in\mathbb{Z}^+$ be smallest such that $\underset{\substack{\parallel \\ c}}{a^m}\in H$. Claim: $H=\langle \underset{\substack{\parallel \\ c}}{a^m}\rangle$

Let $b\in H$ will show $b=c^r$ for some $r\in\mathbb{Z}$

Since $b\in G$ $b=a^n$ for $n\in\mathbb{Z}$.

By division alg. $n=mq+r$ for $q\in\mathbb{Z}$ $0\le r<m$

Then $\underbrace{a^n}_{\in H}=a^{mq+r}=\underbrace{(a^m)^q}_{\in H}a^r \Rightarrow a^r=\underset{\in H}{a^n(a^m)^{-q}}$

However $0 \leq r < m$ and m was supposed to be smallest integer. $\Rightarrow r = 0$.

$b = a^n = (a^m)^q = c^q \Rightarrow b$ is a power of c.

So H is cyclic. $\square$.

Corollary 6.7 The subgroups of $\mathbb{Z}$ under addition are precisely the groups $n\mathbb{Z}$ for $n \in \mathbb{Z}$.

Ex. Let $H = \{nr + ms \mid n, m \in \mathbb{Z}\}$. Exercise Show H is a subgp of $(\mathbb{Z}, +)$

$H = \langle d \rangle$ where $d = \gcd(r, s)$.

See Def 6.8

Structure of cyclic groups

Thm 6.10 Let $G = \langle a \rangle$ be a cyclic group

If $|G| = \infty$ then $G \cong (\mathbb{Z}, +)$

if $|G| = n$ then $G \cong (\mathbb{Z}_n, +_n)$

Proof Case 1. Suppose $a^m \neq e$ for $m \neq 0$.

If $h \neq k$, then $a^h \neq a^k$. Otherwise $a^k (a^h)^{-1} = a^{k-h} = e$.
$\Rightarrow\Leftarrow$

Hence $\varphi : G \to \mathbb{Z}$ $\varphi(a^i) = i$ is a bijection

Also $\phi(a^i a^j) = i + j = \phi(a^i) + \phi(a^j)$

Case 2 $\quad a^m = e$ for some $m \neq 0$. Let $n \in \mathbb{Z}^+$ be smallest such that $a^n = e$. Then

$$G = \{ a^0, a^1, \dots, a^{n-1} \} \text{ since } a^s \underset{\text{division alg.}}{=} a^{qn+r} = (a^n)^q a^r = a^r$$

$$0 \leq r < n$$

$$\varphi : G \to \mathbb{Z}_n \text{ is a bijection and}$$
$$a^i \mapsto i$$

Thm 6.14 Let $G = \langle a \rangle$ with $|G| = n$, and $b = a^s \in G$. Then $H = \langle b \rangle$ is a cyclic subgroup with $|H| = \frac{n}{d}$ where $d = \gcd(n, s)$. Also

$$\langle a^s \rangle = \langle a^t \rangle \iff \gcd(s,n) = \gcd(t,n).$$

Proof $|H| = m$ where $m \in \mathbb{Z}^+$ is smallest s.t $b^m = e$.

Now, $b^m = e \iff (a^s)^m = e \iff n \mid sm$.

The smallest m s.t. $n \mid sm$ is precisely $m = \dfrac{n}{\gcd(n,s)}$. See Pg 64. $\square$

Generators of cyclic groups.

Corollary 6.16 If $G = \langle a \rangle$ and $|G| = n$, then the other generators of G are the elements of the form a^r where $\gcd(r,n) = 1$.

Proof Let $H = \langle a^r \rangle \leq G = \langle a \rangle$. By thm 6.14

$$|H| = \frac{n}{\gcd(n,r)} = \frac{n}{1} = n \quad \text{so} \quad |H| = |G|$$

Hence $H = G$. $\square$

Ex. The only generators of $(\mathbb{Z},+)$ are $+1$ and -1.