P55 #20.

$U(n)$, $n \geq 2$.

$1^2 = 1$

$n-1 \in U(n)$

$(n-1)(n-1) = \underbrace{n^2 - 2n}_{n(n-2)} + 1 = 1 \bmod n$

P55 #6(c) $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$

$$\begin{pmatrix} 6 & 3 \\ 8 & 2 \end{pmatrix}^{-1} = \frac{1}{-12}\begin{pmatrix} 2 & -3 \\ -8 & 6 \end{pmatrix} = \begin{pmatrix} -1/6 & 1/4 \\ 2/3 & -1/2 \end{pmatrix}$$

G group, $a \in G$, $a^0 = e$

$S = \{ a^i \mid i \in \mathbb{Z} \}$ $\quad a^{-2} = (a^{-1})^2$

$e \in S$

$a^i \cdot a^j = a^{i+j} \in S$, $(a^i)^{-1} = (a^{-1})^i \in S$

$\Rightarrow$ S subgroup of G. Notation: $S = \langle a \rangle$

Suppose $o(a) = m \Rightarrow a^m = e$

$\langle a \rangle = \{ a, a^2, \dots, a^{m-1}, e \}$

$|\langle a \rangle| = m$.

$a \in G$

$\langle a \rangle$ is the subgroup generated by a is called the cyclic subgroup generated by a.

A group G is called cyclic if

$G = \langle a \rangle$ for some $a \in G$.

Ex(1) $(\mathbb{Z}, +)$ $e = 0$

$\langle 1 \rangle = \{0, \pm 1, \pm 2, \pm 3, \text{---} \} = \mathbb{Z}$

$\Rightarrow$ $\mathbb{Z}$ is a cyclic group.

$\langle 2 \rangle = \{0, \pm 2, \pm 4, \pm 6, \pm 8, \text{----} \} = 2\mathbb{Z}$

a cyclic subgroup.

H be any subgroup of $\mathbb{Z}$.

$|H| = 1 \Rightarrow H = \{0\} = \langle 0 \rangle$

$|H| > 1 \Rightarrow 0 \neq a \in H \Rightarrow -a \in H$

$\Rightarrow$ H contains positive integers.

Choose $m \in H$ to be the smallest positive integer in H.

Claim: $H = \langle m \rangle = m\mathbb{Z}$

$\langle m \rangle \subseteq H$ by definition.

$0 \neq n \in H$

By Division algorithm

$n = mq + r, \quad 0 \leq r < m$

$\Rightarrow r = n - mq \in H$ since $n \in H, m \in H$.

$\Rightarrow r = 0$ since m is smallest

$\Rightarrow n = mq \in \langle m \rangle$

$\Rightarrow H = \langle m \rangle$.

$\therefore$ Every subgroup of $\mathbb{Z}$ is a cyclic subgroup of $\mathbb{Z}$.

G group

A nonempty subset H of G is a subgroup if for all $a, b \in H$, $ab^{-1} \in H$.

(1) Suppose H and K subgroups of G,

$H \cap K \neq \phi$

$a, b \in H \cap K \Rightarrow a, b \in H$ and $a, b \in K$

H subgroup $\Rightarrow ab^{-1} \in H$

K subgroup $\Rightarrow ab^{-1} \in K$

$\Rightarrow ab^{-1} \in H \cap K$

$\Rightarrow H \cap K$ subgroup of G.

Warning: $H \cup K$ not necessarily a subgroup.

Ex(1) $H = 2\mathbb{Z}$, $K = 3\mathbb{Z}$, $G = \mathbb{Z}$

$H \cup K$ subgroup? No.

$3 \in 3\mathbb{Z} = K$, $-2 \in H$

$3, -2 \in H \cup K$

$3 + (-2) = 1 \notin H \cup K$

(2) G group

$$Z(G)=\{a\in G \mid ax=xa \ \forall x\in G\}$$

$$e\in Z(G) \Rightarrow Z(G)\neq\phi$$

$$a,b\in Z(G) \Rightarrow ax=xa,\ bx=xb \quad \forall x\in G$$

$$\begin{aligned}(ab)x &= a(bx)\\ &= a(xb)\\ &= (ax)b = (xa)b\\ &= x(ab)\end{aligned}$$

$$\Rightarrow ab\in Z(G)$$

$$bxb^{-1}=x \Rightarrow xb^{-1}=b^{-1}x \Rightarrow b^{-1}\in Z(G)$$

$\Rightarrow Z(G)$ is a subgroup of G called the <u>center of G</u>.

<u>Note</u>: G abelian $\Rightarrow Z(G)=G$.

(3) G group, $x\in G$

$$C(x)=\{a\in G \mid ax=xa\}\neq\phi$$

$$a,b\in C(x) \Rightarrow ax=xa \ \&\ bx=xb$$

$(ab)x = x(ab)$ as above.

$$xb^{-1}=b^{-1}x$$

$\Rightarrow C(x)$ is a subgroup of G called the centralizer of x.

Thm: $\bigcap_{x \in G} C(x) = Z(G)$

Ex(1) $D_4 = \{I, R, R^2, R^3, H, HR, HR^2, HR^3\}$

$C(I) = D_4$, $C(R) = \{I, R, R^2, R^3\}$

$C(R^2) = \{I, R, R^2, R^3, H, HR, HR^2, HR^3\} = D_4$

$C(R^3) = C(R)$

$C(H) = \{I, H, R^2, HR^2\}$

$C(HR) = \{I, HR, R^2, HR^3\} = C(HR^3)$

$C(HR^2) = \{I, HR^2, R^2, H\}$

$\Rightarrow Z(D_4) = \{I, R^2\}$

Cyclic group

$G = \langle a \rangle = \{a^i \mid i \in \mathbb{Z}\} = \langle a^{-1} \rangle$

$o(a) = m \Rightarrow \langle a \rangle = \{a, a^2, \dots, a^{m-1}, e\}$

$\Rightarrow o(a) = |G|$.

Ex (2) $U(10)$ cyclic?

$U(10) = \{1, 3, 7, 9\}$

$\langle 1 \rangle = \{1\}$

$\langle 3 \rangle = \{3, 9, 7, 1\} = U(10)$

$\Rightarrow$ $U(10)$ is cyclic.

$\langle 7 \rangle = \{7, 9, 3, 1\} = U(10)$

$\overset{\shortparallel}{\langle 3^{-1} \rangle}$

$\langle 9 \rangle = \{9, 1\}$.

P68 # 1, 2, 4, 5, 6, 10, 12, 18, 20, 22, 23, 27, 29, 34, 37, 42, 49, 52, 53, 57, 58, 60, 65, 67, 71, 79.