Chapter 3

<u>Defn</u>: • The <u>order</u> of a group G, denoted $|G|$, is the number of elements in the group (the cardinality of the set G).

• The <u>order</u> of an element g of a group G is the least positive integer n satisfying $g^n = e$. If no such n exists, g has <u>infinite order</u>

<u>Ex</u>:
- $|D_4| = 8$
- $|\mathbb{Z}_{12}| = 12$
- $|U(10)| = 4$ $\qquad U(10) = \{1, 3, 7, 9\}$
- $R_{90} \in D_4$ has order 4
- $R_{180}, H \in D_4$ each have order 2
- $1 \in \mathbb{Z}$ has infinite order
- $1 \in \mathbb{Z}_{28}$ has order 28
- $14 \in \mathbb{Z}_{28}$ has order 2
- $4 \in \mathbb{Z}_6$ has order 3
- $2 \in U(7)$ has order 3 $\quad (2^1 = 2, 2^2 = 4, 2^3 = 1$ in $U(7))$
- $3 \in U(7)$ has order 6 $\quad (3^1 = 3, 3^2 = 2, 3^3 = 6, 3^4 = 4, 3^5 = 5, 3^6 = 1$ in $U(7))$

<u>Note</u>: Usually we use multiplicative notation. But for abelian groups we sometimes use additive notation (such as for $\mathbb{Z}$ and $\mathbb{Z}_n$).

Multiplication	$a \cdot b$	a^n	a^{-1}
Addition	$a + b$	$n \cdot a$	$-a$

Warning: $g^n = e$ does not imply g has order n.
The order of g is the least positive n with this property.

Defn: • Let G be a group and let $H \subseteq G$. If H is itself a group with respect to the binary operation on G, then H is called a subgroup of G and we write $H \leq G$.

• H is a proper subgroup if $H \neq G$. We write $H < G$ when H is a proper subgroup of G.

• $\{e\}$ is the trivial subgroup.

Thm 3.1 (One-Step Subgroup Test):
Let G be a group and $H \subseteq G$. If $ab^{-1} \in H$ whenever $a, b \in H$ and $H \neq \emptyset$ then H is a subgroup of G

Pf: (Associative) Holds in H since it holds in G.
(Identity) Since $H \neq \emptyset$, we can pick some $a \in H$. Set $b = a$. Then $a, b \in H$ so $ab^{-1} \in H$. But $ab^{-1} = aa^{-1} = e$, so $e \in H$.
(Inverses) If $b \in H$ then $b^{-1} = eb^{-1} \in H$ since $e, b \in H$.
Finally, we must check H is closed under the binary operation. If $x, y \in H$ then $a = x$ and $b = y^{-1}$ belong to H, so $xy = ab^{-1}$ belongs to H $\square$

Ex: • $\{1, -1, i, -i\}$ is a subgroup of the multiplicative group $\mathbb{C} \setminus \{0\}$

• $\{0, 2, 4\}$ is a subgroup of $\mathbb{Z}_6$

• $\{0, 3\}$ is a subgroup of $\mathbb{Z}_6$

• $\mathbb{Z}_n \subseteq \mathbb{Z}$ but $\mathbb{Z}_n$ is not a subgroup of $\mathbb{Z}$
($\mathbb{Z}_n$ uses a different binary operation)

• $\{R_0, R_{90}, R_{180}, R_{270}\}$ is a subgroup of D_4

Ex: $H = \{n \in \mathbb{Z} : 3 \mid n\}$ is a subgroup of $\mathbb{Z}$

$3 \mid 0$ so $0 \in H$ and $H \neq \emptyset$.
Now suppose $a, b \in H$, meaning $3 \mid a$ and $3 \mid b$.
Say $a = 3p$, $b = 3q$. Then $a - b = 3p - 3q = 3(p-q)$
so $3 \mid (b-a)$ and $b - a \in H$. Thus H is a subgroup by the One-Step Subgroup Test.

Ex: Let G be an abelian group. Then $H = \{x \in G : x^2 = e\}$ is a subgroup

$e^2 = e$ so $e \in H$ and $H \neq \emptyset$. Now suppose $a, b \in H$, meaning $a^2 = e = b^2$. Since G is abelian, we have

$$(ab^{-1})^2 = ab^{-1}ab^{-1} = aab^{-1}b^{-1} = a^2(b^2)^{-1} = ee^{-1} = e$$

thus $ab^{-1} \in H$. So H is a subgroup by the One-Step Subgroup Test.

Thm 3.2 (Two-Step Subgroup Test):

Let G be a group and let $H \subseteq G$. If

① $H \neq \emptyset$,

② $ab \in H$ whenever $a, b \in H$, and

③ $a^{-1} \in H$ whenever $a \in H$

Then H is a subgroup of G

Pf: Suppose $x, y \in H$. By ③, $y^{-1} \in H$. So $x, y^{-1} \in H$ and therefore ② implies $xy^{-1} \in H$. Thus $xy^{-1} \in H$ whenever $x, y \in H$ and $H \neq \emptyset$ by ①. So H is a subgroup by the One-Step Subgroup Test. $\square$

Ex: Let G be an abelian group and let $H = \{x \in G : x \text{ has finite order}\}$. Then H is a subgroup of G

e has order 1 $(e^1 = e)$ so $e \in H$ and $H \neq \emptyset$.

Suppose $a, b \in H$. Say a has order n, b has order m.

Then $(ab)^{nm} = a^{nm} b^{nm} = (a^n)^m (b^m)^n = e^m e^n = e$

$\uparrow$ G is abelian

so $ab \in H$ (the order of ab is at most nm, so is finite).

Lastly, if $a \in H$ and n is the order of a then $(a^{-1})^n = a^{-1} a^{-1} \cdots a^{-1} = (aa \cdots a)^{-1} = (a^n)^{-1} = e^{-1} = e$

n factors

so a^{-1} has order at most n and $a \in H$. Thus H is a subgroup by the Two-Step Subgroup Test

Ex: Let G be an abelian group and $H, K \leq G$ (subgroups). Then $HK = \{hk : h \in H, k \in K\}$ is a subgroup of G

Since e belongs to H and K, $ee = e$ belongs to HK. Thus $HK \neq \emptyset$.
Next suppose $a, b \in HK$, meaning there are $h_1, h_2 \in H$ and $k_1, k_2 \in K$ with $a = h_1 k_1$ and $b = h_2 k_2$.
Since G is abelian

$$ab = h_1 k_1 h_2 k_2 = h_1 h_2 k_1 k_2$$

Also $h_1 h_2 \in H$ since $h_1, h_2 \in H$ and H is a subgroup. Similarly $k_1 k_2 \in K$. Therefore $ab = (h_1 h_2)(k_1 k_2)$ belongs to HK.
Lastly, consider any $a \in H$. Say $a = hk$ with $h \in H$, $k \in K$. Then $a^{-1} = k^{-1} h^{-1}$ and since G is abelian

$$a^{-1} = k^{-1} h^{-1} = h^{-1} k^{-1}$$

Also $h^{-1} \in H$, $k^{-1} \in K$ since H, K are subgroups. So $a^{-1} = h^{-1} k^{-1} \in HK$. By the Two-Step Subgroup Test HK is a subgroup.

How to check $H \subseteq G$ is <u>not</u> a subgroup:

- show $e \notin H$,
- find $a \in H$ with $a^{-1} \notin H$, or
- find $a, b \in H$ with $ab \notin H$.

Ex: • $\{r \in \mathbb{R} : r < 0\}$ is not a subgroup of $\mathbb{R} \setminus \{0\}$ since it does not contain 1 (and it is not closed under multiplication).

• $\{n \in \mathbb{Z} : n \geq 0\}$ is not a subgroup of $\mathbb{Z}$ since it is not closed under taking inverses

Thm 3.3 (Finite Subgroup Test):
Let G be a finite group and let $H \subseteq G$ be nonempty. If H is closed under the operation of G then H is a subgroup.

Pf: To apply Two-Step Subgroup Test, we only need to check that $a^{-1} \in H$ when $a \in H$.
Consider any $a \in H$. If $a = e$ then $a^{-1} = e = a \in H$ and we are done. So assume $a \neq e$. By closure of H,

$$a, a^2, a^3, a^4, \dots \in H$$

Since G is finite there must be $0 < i < j$ with $a^i = a^j$. Then, multiplying both sides by a^{-i} we get $e = a^{j-i}$. In particular, $a \cdot a^{j-i-1} = a^{j-i} = e$ so $a^{j-i-1} = a^{-1}$. Since $j > i$, $a^1 = a \neq e$, and $a^{j-i} = e$, we must have $j - i \geq 2$. Therefore $j-i-1 \geq 1$ and $a^{j-i-1} \in H$. So $a^{-1} = a^{j-i-1} \in H$, which is what we wanted to show.

Defn: For a group G and $a \in G$, set

$$\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$$

Note this includes negative exponents of a as well as $a^0 = e$

Thm 3.4: For any group G and $a \in G$,
$\langle a \rangle$ is a subgroup of G

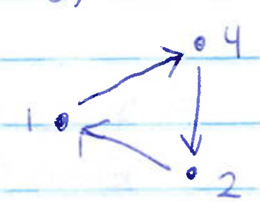
Pf: $a \in \langle a \rangle$ so $\langle a \rangle \neq \emptyset$. If $a^n, a^m \in \langle a \rangle$ then
$(a^n)(a^m)^{-1} = a^n a^{-m} = a^{n-m} \in \langle a \rangle$. By the
One-Step Subgroup Test $\langle a \rangle$ is a subgroup. $\square$

Defn:
- $\langle a \rangle$ is the cyclic subgroup of G generated by a.
- If $G = \langle a \rangle$ we call a a generator of G.
- G is cyclic if $G = \langle a \rangle$ for some $a \in G$.

Note: Cyclic groups are abelian since
$$a^i a^j = a^{i+j} = a^{j+i} = a^j a^i$$

Ex:
- In $\mathbb{Z}_{12}$, $\langle 3 \rangle = \{0, 3, 6, 9\}$
- In $\mathbb{Z}$, $\langle -1 \rangle = \langle 1 \rangle = \mathbb{Z}$
  so $\mathbb{Z}$ is cyclic. 1 and -1 are generators
- For each n, $\mathbb{Z}_n$ is cyclic with generator 1
- In $U(7)$, $\langle 4 \rangle = \{1, 2, 4\}$ since
  $4^0 = 1$, $4^1 = 4$, $4^2 = 16 \bmod 7 = 2$, $4^3 = 1$, $4^4 = 4$, $4^5 = 2$, $4^6 = 1, \ldots$
  $4^{-1} = 2$ (since $2 \cdot 4 = 1$), $4^{-2} = 4$ (since $4^2 \cdot 4 = 1$), $4^{-3} = 1$, $4^{-4} = 2, \ldots$

Multiplication by 4



- In D_n, $\langle R_{360/n} \rangle = \{ R_{i \cdot \frac{360}{n}} : 0 \le i < n, i \in \mathbb{Z} \}$

<u>Note</u>: $\langle a \rangle$ is the smallest subgroup containing a, since every subgroup containing a must contain $\{ \cdots, a^{-2}, a^{-1}, a^0, a, a^2, \cdots \} = \langle a \rangle$

<u>Defn</u>: For a group G and $S \subseteq G$ we write $\langle S \rangle$ for the smallest subgroup containing S and call $\langle S \rangle$ the <u>subgroup generated by</u> S. If $G = \langle S \rangle$ we say G is <u>generated by</u> S or that S is a <u>generating set for G</u>.

<u>Ex</u>:
- In $\mathbb{R}$, $\langle 3, \pi, \sqrt{2} \rangle = \{ 3a + b\pi + c\sqrt{2} : a, b, c \in \mathbb{Z} \}$
- In $\mathbb{C}$, $\langle 1, i \rangle = \{ a + bi : a, b \in \mathbb{Z} \}$
- In $\mathbb{C} \setminus \{0\}$, $\langle 1, i \rangle = \{ 1, -1, i, -i \} = \langle i \rangle$
- In D_4, $\langle H, V \rangle = \{ R_0, H, V, R_{180} \}$

  since $HV = VH = R_{180}$, $HR_{180} = R_{180}H = V$,
  $VR_{180} = R_{180}V = H$, $H^2 = V^2 = R_0$, $R_{180}^2 = R_0$.
- $D_4 = \langle R_{90}, H \rangle$ since

$$
\begin{array}{ll}
R_0 = R_{90}^0 & H = H \\
R_{90} = R_{90} & V = HR_{90}^2 \\
R_{180} = R_{90}^2 & D = HR_{90} \\
R_{270} = R_{90}^3 & D' = HR_{90}^3
\end{array}
$$

<u>Defn</u> The <u>center</u> of a group G is
$$Z(G) = \{ a \in G : ax = xa \text{ for all } x \in G \}$$

Thm 3.5 $Z(G)$ is a subgroup of G.

Pf: We have $e \in Z(G)$ since $ex = x = xe$ for all $x \in G$. Thus $Z(G) \neq \emptyset$. Next suppose $a, b \in Z(G)$, meaning $ax = xa$ and $bx = xb$ for all $x \in G$. Then for all $x \in G$ we have

$$(ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab)$$

and hence $ab \in Z(G)$. Finally, suppose $a \in Z(G)$. Then for all $x \in G$ we have

$$ax = xa$$

Multiply both sides on left and right by a^{-1}	OR	Move the a's across the equals sign while maintaining left/right position
$a^{-1}(ax)a^{-1} = a^{-1}(xa)a^{-1}$		$ax = xa$
$(a^{-1}a)xa^{-1} = a^{-1}x(aa^{-1})$		$xa^{-1} = a^{-1}x$
$exa^{-1} = a^{-1}xe$		
$xa^{-1} = a^{-1}x$		

By reasoning in either of the two above ways, we see that $a^{-1}x = xa^{-1}$ for all $x \in G$ and thus $a^{-1} \in Z(G)$. We conclude $Z(G)$ is a subgroup of G by the Two-Step Subgroup Test $\square$

Ex: For $n \geq 3$

$$Z(D_n) = \begin{cases} \{R_0, R_{180}\} & \text{if } n \text{ even} \\ \{R_0\} & \text{if } n \text{ odd} \end{cases}$$

D_n consists of n rotations $\{R_{i \cdot \frac{360}{n}} : 0 \leq i < n, i \in \mathbb{Z}\}$ together with n reflections (reflections over any line joining the center of the regular n-gon with any corner or any midpoint of an edge).

Let F be any reflection and R be any rotation. We claim that if $FR = RF$ then ~~$R \in \{R_0, R_{180}\}$~~ $R = R_0$ (when n odd) or $R \in \{R_0, R_{180}\}$ (when n even).

Note if $FR = R'$ for some rotation R' then $F = R'R^{-1}$ would be a rotation, contradicting the fact that F is a reflection. So FR must be a reflection.

Since FR is a reflection $(FR)^2 = R_0$, meaning $FR = (FR)^{-1}$. So

$$FR = (FR)^{-1} = R^{-1}F^{-1} = R^{-1}F$$

(F a reflection so $F^{-1} = F$)

But we are assuming $FR = RF$ so

$$RF = FR = \cdots\cdots = R^{-1}F$$

Applying right-cancellation to $RF = R^{-1}F$ we get $R = R^{-1}$, meaning $R^2 = RR = RR^{-1} = R_0$.

Thus either $R = R_0$ or n is even and $R = R_{180}$.

The above argument shows $Z(D_n)$ does not contain any reflections (for every reflection F we can find a rotation $R \neq R_0, R_{180}$ so that $FR \neq RF$). Also, while all rotations commute with one another, the only rotations that commute with reflections are R_0 when n is odd and R_0, R_{180} when n is even. Thus $Z(D_n)$ is as described.

<u>Defn</u>: Let G be a group and $a \in G$. The <u>centralizer of a</u> is

$$C(a) = \{g \in G : ga = ag\}$$

<u>Ex</u>: In D_4

$$C(R_0) = D_4 = C(R_{180})$$

$$C(R_{90}) = \{R_0, R_{90}, R_{180}, R_{270}\} = C(R_{270})$$

$$C(H) = \{R_0, R_{180}, H, V\} = C(V)$$

$$C(D) = \{R_0, R_{180}, D, D'\} = C(D')$$

<u>Thm 3.6</u>: $C(a)$ is a subgroup of G for every $a \in G$

<u>Pf</u>: Exercise. Similar to Thm 3.5.

<u>Note</u>: $Z(G) \leq C(a)$ and $\langle a \rangle \leq C(a)$ for all $a \in G$.