CHAPTER 3

Finite Groups; Subgroups

DEFINITION (Order of a Group). The number of elements of a group (finite or infinite) is called its order. We denote the order of G by $|G|$.

DEFINITION (Order of an Element). The order of an element g in a group G is the smallest positive integer n such that $g^n = e$ ($ng = 0$ in additive notation). If no such integer exists, we say g has infinite order. The order of g is denoted by $|g|$.

EXAMPLE. $U(18) = \{1, 5, 7, 11, 13, 17\}$, so $|U(18)| = 6$. Also,

$$5^1 = 5, \quad 5^2 = 7, \quad 5^3 = 17, \quad 5^4 = 13, \quad 5^5 = 11, 5^6 = 1,$$

so $|5| = 6$.

EXAMPLE. $|\mathbb{Z}_{12}| = 12$ under addition modulo n.

$$1 \cdot 4 = 4, \quad 2 \cdot 4 = 8, \quad 3 \cdot 4 = 0,$$

so $|4| = 3$.

PROBLEM (Page 69 # 20). Let G be a group, $x \in G$. If $x^2 \neq e$ and $x^6 = e$, prove (1) $x^4 \neq e$ and (2) $x^5 \neq e$. What can we say about $|x|$?

PROOF.

(1) Suppose $x^4 = e$. Then

$$x^8 = e \Longrightarrow x^2x^6 = e \Longrightarrow x^2e = e \Longrightarrow x^2 = e,$$

a contradiction, so $x^4 \neq e$.

(2) Suppose $x^5 = e$. Then

$$x^{10} = e \Longrightarrow x^4x^6 = e \Longrightarrow x^4e = e \Longrightarrow x^4 = e,$$

a contradiction, so $x^5 \neq e$.

Therefore, $|x| = 3$ or $|x| = 6$. □

DEFINITION (Subgroup). If a subset H of a group G is itself a group under the operation of G, we say that H is a subgroup of G, denoted $H \leq G$.

If H is a proper subset of G, then H is a proper subgroup of G.

$\{e\}$ is the trivial subgroup of G. If $H \neq \{e\}$ and $H \leq G$, H is called nontrivial.

THEOREM (3.1 — One-Step Subgroup Test). *Let G be a group and $\emptyset \neq H \subseteq G$. Then H is a subgroup of G if $a, b \in H \Longrightarrow ab^{-1} \in H$ (for additive notation, $a - b \in H$).*

PROOF.

Associativity of H derives from that of G.

[To show $e \in H$.] $H \neq \emptyset$, so $\exists\ x \in H$. Then $xx^{-1} = e \in H$ by hypothesis.

[To show $x^{-1} \in H$.] Also, $ex^{-1} = x^{-1} \in H$ by hypothesis.

[To show H is closed.] Suppose $x, y \in H$. Then $y^{-1} \in H$ and, by hypothesis, $xy = x(y^{-1})^{-1} \in H$.

Thus $H \leq G$. □

PROBLEM (Page 74 # 73). Let

$$H = \{a + bi \mid a, b \in \mathbb{R},\ a^2 + b^2 = 1\}.$$

This is the set of points on the unit circle in the complex plane. Then $H \leq \mathbb{C}^*$ under complex multiplication.

PROOF.

$1 = 1 + 0i \in H$ since $1^2 + 0^2 = 1$.

Suppose $a + bi, c + di \in H$. Then $a^2 + b^2 = 1$ and $c^2 + d^2 = 1$.

$$(a + bi)(c + di)^{-1} = \frac{a + bi}{c + di} = \frac{(a + bi)(c - di)}{(c + di)(c - di)} = \frac{ac + bd + bci - adi}{c^2 + d^2} = (ac + bd) + (bc - ad)i$$

and

$$(ac + bd)^2 + (bc - ad)^2 = a^2c^2 + 2abcd + b^2d^2 + b^2c^2 - 2abcd + a^2d^2 = a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 = a^2(c^2 + d^2) + b^2(c^2 + d^2) = (a^2 + b^2)(c^2 + d^2) = 1 + 1 = 1,$$

so $(a + bi)(c + di)^{-1} \in H$. Thus $H \leq \mathbb{C}^*$. □

THEOREM (3.2 — Two-Step Subgroup Test). *Let G be a group and $\emptyset \neq H \subseteq G$. Then $H \leq G$ if*

(1) $a, b \in H \Longrightarrow ab \in H$ (closed under multiplication);

(2) $a \in H \Longrightarrow a^{-1} \in H$ (closed under inverses).

PROOF.

Suppose $a, b \in H$. Then $b^{-1} \in H$ by (2). By (1), $ab^{-1} \in H$, so $H \leq G$ by Theorem 3.1. □

EXAMPLE. $\langle R_{360/n} \rangle \leq D_n$.

PROOF.

$$\langle R_{360/n} \rangle = \left\{ R_0, R_{\frac{360}{n}}, R_{\frac{2 \cdot 360}{n}}, \cdots, R_{\frac{(n-1)360}{n}} \right\}$$

where $R_i + R_j = R_{(i+j) \bmod 360}$.

Let $R_i, R_j \in \langle R_{360/n} \rangle$ and suppose $i = \dfrac{a \cdot 360}{n}$ and $j = \dfrac{b \cdot 360}{n}$.

Now $a + b = qn + r$, $0 \leq r < n$, so

$$i + j = \frac{(a+b)360}{n} = \frac{(qn+r)360}{n} = q \cdot 360 + \frac{r \cdot 360}{n}.$$

Then

$$(i+j) \bmod 360 = \frac{r \cdot 360}{n}, \quad 0 \leq r < n,$$

so

$$R_{i+j} \bmod 360 \in \langle R_{360/n} \rangle.$$

Now suppose $R_i \in \langle R_{360/n} \rangle, i = \dfrac{a \cdot 360}{n}$.

$$360 - i = 360 - \frac{a \cdot 360}{n} = \frac{n \cdot 360 - a \cdot 360}{n} = \frac{(n-a)360}{n},$$

so $R_{360-i} \in \langle R_{360/n} \rangle$. Since

$R_i + R_{360-i} = R_{360} \bmod 360 = R_0$ and $R_{360-i} + R_i = R_{360} \bmod 360 = R_0$,

$R_{360-i} = R_i^{-1}$. Thus, by the Two-Step Subgroup Test, $\langle R_{360/n} \rangle \leq D_n$. □

THEOREM (3.3 — Finite Subgroup Test). *Let H be a finite nonempty subset of a group G. If H is closed under the operation of G, then H is a subgroup of G.*

PROOF.

In view of Theorem 3.2, we need only show that $a^{-1} \in H$ whenever $a \in H$.

If $a = e$, then $a^{-1} = a$, and we are done. So suppose $a \neq e$.

Consider the sequence $a, a^2, \ldots$.

By closure, each of these elements are in H. Since H is finite, not all of these elements are distinct. Suppose $a^i = a^j$, $i > j$.

Then $a^{i-j} = e$, and since $a \neq e$, $i - j > 1$. Thus,

$$aa^{i-j-1} = a^{i-j} = e, \text{ so } a^{i-j-1} = a^{-1}.$$

But $i - j - 1 \geq 1$, so $a^{i-j-1} \in H$ and we are done. □

Suppose $H \subseteq G$. To show $H \not\leq G$, show any of the following:

(1) The identity is not in H.

(2) $\exists$ an element of H whose inverse is not in H.

(3) $\exists$ two elements of H whose product is not in H.

NOTATION. Let G be a group, $a \in G$, and let

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

Note $a^0 = e$.

THEOREM (3.4 — $\langle a \rangle$ is a Subgroup).

Let G be a group and $a \in G$. Then $\langle a \rangle \leq G$.

PROOF.

Since $a \in \langle a \rangle$, $\langle a \rangle \neq \emptyset$. Let $a^n, a^m \in \langle a \rangle$. Then

$$a^n(a^m)^{-1} = a^n a^{-m} = a^{n-m} \in \langle a \rangle,$$

so by Theorem 3.1, $\langle a \rangle \leq G$. □

EXAMPLE. In $U(14)$, find $\langle 9 \rangle$.

$$9^1 = 9, \quad 9^2 = 81 = 11 \bmod 14, \quad 9^3 = 99 = 1 \bmod 14.$$

Thus $\langle 9 \rangle = \{1, 9, 11\}$ with $9^{-1} = 11$ and $11^{-1} = 9$.

EXAMPLE. In D_4, $\langle R_{270} \rangle = \{R_0, R_{90}, R_{180}, R_{270}\} \leq D_4$.

$$R_{270} + R_{270} = R_{180}, \quad R_{180} + R_{270} = R_{90}, \quad R_{90} + R_{270} = R_0.$$

EXAMPLE. In $\mathbb{Z}_{15}$, $\langle 3 \rangle = \{3, 6, 9, 12, 0\} \leq \mathbb{Z}_{15}$.

Recall here that a^n is na since the operation is addition modulo n.

DEFINITION (Center of a Group). The center, $Z(G)$, lof a group G is the subset of elements of G that commute with every element of G:

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

THEOREM (3.5 — Center is a Subgroup). $Z(G) \leq G$.

PROOF.

$e \in Z(G)$, so $Z(G) \neq \emptyset$. Suppose $a, b \in Z(G)$. Then

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

so $ab \in Z(G)$.

Now suppose $a \in Z(G)$. Then $ax = xa \ \forall \ x \in G$, so

$$a^{-1}(ax)a^{-1} = a^{-1}(xa)a^{-1} \Longrightarrow (a^{-1}a)xa^{-1} = a^{-1}x(aa^{-1}) \Longrightarrow$$
$$exa^{-1} = a^{-1}xe \Longrightarrow xa^{-1} = a^{-1}x.$$

Thus $a^{-1} \in Z(G)$, and so $Z(G) \leq G$ by Theorem 3.2. $\square$

PROBLEM (Page 75 # 79c). Let $G = GL(2, \mathbb{R})$. Find $Z(G)$.

SOLUTION.

Suppose $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in Z(G)$. Then

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} e & f \\ g & h \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \ \forall \ \begin{bmatrix} e & f \\ g & h \end{bmatrix} \in GL(2, \mathbb{R}) \Longrightarrow$$

$$\begin{bmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{bmatrix} = \begin{bmatrix} ae+cf & be+df \\ ag+ch & bg+dh \end{bmatrix} \ \forall\, e, f, g, h \in \mathbb{R} \ni eh - fg \neq 0.$$

Now $ae + bg = ae + cf \Longrightarrow bg = cf$.

For $e = f = g = 1$ and $h = 0$, $eh - fg = -1 \Longrightarrow b = c$.

For $e = g = h = 1$ and $f = 0$, $eh - fg = 1 \Longrightarrow b = 0 \Longrightarrow c = 0$.

Also, for $e = h = 0$ and $f = g = 1$, $af + bh = be + df \Longrightarrow af = df \Longrightarrow a = d$.

Thus $Z(G) = \left\{ \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \middle| a \neq 0 \right\}$. □

DEFINITION (Centralizer of a in G).

Let $a \in G$, G a group. The centralizer of a in G is the set of all elements in G that commute with a:

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

EXAMPLE. In D_4,

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

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

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

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

Thus $Z(D_4) = \{R_0, R_{180}\}$.

THEOREM (3.6 — $C(a)$ is a Subgroup). *For each a in a group G, $C(a) \leq G$.*

PROOF.

Will be assigned as homework (Page 72 # 41). Similar to the proof of Theorem 3.5. □

PROBLEM (Page 75 # 79a). Let $G = GL(2, \mathbb{R})$. Find $C\left(\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \right)$.

SOLUTION.

Let $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in C\left(\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \right)$. Then

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \Longrightarrow \begin{bmatrix} a+c & b+d \\ a & b \end{bmatrix} = \begin{bmatrix} a+b & a \\ c+d & c \end{bmatrix} \Longrightarrow$$

$$b = c \text{ and } a = b + d \Longrightarrow d = a - b.$$

Thus

$$C\left(\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \right) = \left\{ \begin{bmatrix} a & b \\ b & a-b \end{bmatrix} \middle| a^2 - ab - b^2 \neq 0, a, b \in \mathbb{R} \right\}.$$

□

PROBLEM (Page 71 #33). Let G be a group. Show that

$$Z(G) = \bigcap_{a \in G} C(a).$$

[This means the intersection of all subgroups of the form $C(a)$].

PROOF.

[We show $Z(G) = \bigcap_{a \in G} C(a)$ by showing mutual set inclusion.]

Let $x \in Z(G)$. Then x commutes with all $a \in G \Longrightarrow x \in C(a)\ \forall\ a \in G$.

Thus $Z(G) \subseteq \bigcap_{a \in G} C(a)$.

Now suppose $x \in \bigcap_{a \in G} C(a)$. Then x commutes with every $a \in G$,

so $x \in C(a)\ \forall\ a \in G$. Thus $\bigcap_{a \in G} C(a) \subseteq Z(G)$, and so

$Z(G) = \bigcap_{a \in G} C(a)$ by mutual set inclusion. □

PROBLEM (Page 71 # 37). Suppose G is the group defined by the following Cayley table:

	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	1	8	7	6	5	4	3
3	3	4	5	6	7	8	1	2
4	4	3	2	1	8	7	6	5
5	5	6	7	8	1	2	3	4
6	6	5	4	3	2	1	8	7
7	7	8	1	2	3	4	5	6
8	8	7	6	5	4	3	2	1

(a) Find the centralizer of each member of G.

SOLUTION.

$$C(1) = G, \quad C(2) = \{1, 2, 5, 6\}, \quad C(3) = \{1, 3, 5, 7\}, \quad C(4) = \{1, 4, 5, 8\}$$
$$C(5) = G, \quad C(6) = \{1, 2, 5, 6\}, \quad C(7) = \{1, 3, 5, 7\}, \quad C(8) = \{1, 4, 5, 8\}$$

□

(b) Find $Z(G)$.

SOLUTION.

$$Z(G) = \bigcap_{i=1}^{8} C(i) = \{1, 5\}.$$

□

(c) Find the order of each element of G. How are these orders arithmetically related to the order of the group?

SOLUTION.

$$|1| = 1, \quad 2^2 = 1 \Longrightarrow |2| = 2, \quad 3^2 = 5, 3^3 = 5{\cdot}3 = 7, 3^4 = 7{\cdot}3 = 1 \Longrightarrow |3| = 4,$$
$$4^2 = 1 \Longrightarrow |4| = 2, \quad 5^2 = 1 \Longrightarrow |5| = 2, \quad 6^2 = 1 \Longrightarrow |6| = 2,$$
$$7^2 = 5, 7^3 = 5 \cdot 7 = 3, 7^4 = 3 \cdot 7 = 1 \Longrightarrow |7| = 4. \quad 8^2 = 2 \Longrightarrow |8| = 2.$$

We have that for all $g \in G$, $|g| \big| |G|$. □