Chapter 3: Finite Groups; Subgroups

Definition: Order of a Group

The **order** of a group G is the number of elements it contains (finite or infinite).

Notation: $|G|$ denotes the order of G.

Examples

- $\mathbb{Z}$ under addition has **infinite order**
- $U(10) = \{1, 3, 7, 9\}$ under multiplication mod 10 has **order 4**

Definition: Order of an Element

For element g in group G, the **order** of g is the smallest positive integer n such that $g^n = e$.

Notation: $|g|$ denotes the order of element g.

If no such n exists, then g has **infinite order**.

Finding Element Orders

Compute the sequence $g, g^2, g^3, \ldots$ until reaching the identity e for the first time.

Example 1: Orders in $U(15)$

Given: $U(15) = \{1, 2, 4, 7, 8, 11, 13, 14\}$ under multiplication mod 15

Finding $|7|$:

- $7^1 = 7$
- $7^2 = 49 \equiv 4 \pmod{15}$
- $7^3 = 7 \cdot 4 = 28 \equiv 13 \pmod{15}$
- $7^4 = 7 \cdot 13 = 91 \equiv 1 \pmod{15}$

Therefore: $|7| = 4$

Computational Trick: Since $13 \equiv -2 \pmod{15}$:

- $13^2 = (-2)^2 = 4$
- $13^3 = (-2) \cdot 4 = -8 \equiv 7 \pmod{15}$
- $13^4 = (-2)(-8) = 16 \equiv 1 \pmod{15}$

Example 2: Orders in $\mathbb{Z}_{10}$

Given: $\mathbb{Z}_{10}$ under addition mod 10

Finding $|2|$ (additive notation: $n \cdot 2$ means $\underbrace{2 + 2 + \cdots + 2}_{n \text{ times}}$):

- $1 \cdot 2 = 2$
- $2 \cdot 2 = 4$
- $3 \cdot 2 = 6$
- $4 \cdot 2 = 8$
- $5 \cdot 2 = 10 \equiv 0 \pmod{10}$

Therefore: $|2| = 5$

Complete Results: $|0| = 1$, $|5| = 2$, $|2| = |4| = |6| = |8| = 5$, $|1| = |3| = |7| = |9| = 10$

Example 3: Orders in $\mathbb{Z}$

Given: $\mathbb{Z}$ under ordinary addition

For any nonzero element a:

- The sequence is $a, 2a, 3a, 4a, \ldots$
- Since $a \neq 0$, we never reach 0
- **Therefore**: Every nonzero element has **infinite order**
- **Only**: $|0| = 1$

Subgroups

Definition: Subgroup

If subset H of group G is itself a group under the operation of G, then H is a **subgroup** of G.

Notation:

- $H \leq G$ means "H is a subgroup of G"
- $H < G$ means "H is a proper subgroup of G" (not equal to G)

Special Subgroups

- **Trivial subgroup**: $\{e\}$
- **Nontrivial subgroup**: Any subgroup except $\{e\}$

Subgroup Tests

Theorem 3.1: One-Step Subgroup Test

Let G be a group and H a nonempty subset of G. If $ab^{-1} \in H$ whenever $a, b \in H$, then H is a subgroup of G.

Proof of Theorem 3.1

Associativity: Inherited from G

Identity: Since H nonempty, pick $x \in H$. Let $a = x, b = x$:
$e = xx^{-1} = ab^{-1} \in H$

Inverses: For $x \in H$, let $a = e, b = x$:
$x^{-1} = ex^{-1} = ab^{-1} \in H$

Closure: For $x, y \in H$, we have $y^{-1} \in H$. Let $a = x, b = y^{-1}$:
$xy = x(y^{-1})^{-1} = ab^{-1} \in H$

Applying the One-Step Test

Four Steps:

1. **Identify property P** that defines elements of H
2. **Verify identity has property P** (ensures H nonempty)
3. **Assume elements a, b have property P**
4. **Show ab^{-1} has property P**

Example 4: Elements of Order 2

Claim: In Abelian group G, $H = \{x \in G : x^2 = e\}$ is a subgroup.

Step 1: Property P is "$x^2 = e$"

Step 2: $e^2 = e$, so $e \in H$

Step 3: Assume $a, b \in H$, so $a^2 = e$ and $b^2 = e$

Step 4: Show $(ab^{-1})^2 = e$:
$$(ab^{-1})^2 = ab^{-1}ab^{-1} = a^2(b^{-1})^2 = a^2(b^2)^{-1} = e \cdot e^{-1} = e$$

Therefore: H is a subgroup by Theorem 3.1.

Theorem 3.2: Two-Step Subgroup Test

Let G be a group and H a nonempty subset of G. If:

1. $ab \in H$ whenever $a, b \in H$ (**closure**)
2. $a^{-1} \in H$ whenever $a \in H$ (**inverse closure**)

Then H is a subgroup of G.

Proof of Theorem 3.2

Since H nonempty and closed, pick $a \in H$.

- Then $a^{-1} \in H$ by condition 2
- So $e = aa^{-1} \in H$ by condition 1
- Associativity inherited from G

Therefore: H is a subgroup.

Example 6: Elements of Finite Order

Claim: In Abelian group G, $H = \{x \in G : |x| \text{ is finite}\}$ is a subgroup.

Property P: "Element has finite order"

Identity: $|e| = 1$ (finite), so $e \in H$

Closure: If $|a| = m$ and $|b| = n$, then:
$(ab)^{mn} = (a^m)^n (b^n)^m = e^n \cdot e^m = e$
So $|ab|$ divides mn (hence finite)

Inverses: If $|a| = m$, then:
$(a^{-1})^m = (a^m)^{-1} = e^{-1} = e$
So $|a^{-1}| \leq m$ (hence finite)

Example 7: Product of Subgroups

Claim: For Abelian group G with subgroups H, K:
$$HK = \{hk : h \in H, k \in K\}$$
is a subgroup of G.

Identity: $e = e \cdot e \in HK$ (since $e \in H$ and $e \in K$)

Closure: For $h_1k_1, h_2k_2 \in HK$:
$$(h_1k_1)(h_2k_2) = h_1k_1h_2k_2 = h_1h_2k_1k_2 \in HK$$
(using commutativity and closure in \$H, K\$)

Inverses: For $hk \in HK$:
$$(hk)^{-1} = k^{-1}h^{-1} = h^{-1}k^{-1} \in HK$$

Showing a Subset is NOT a Subgroup

Three Ways to Disprove:

1. **Show identity not in set**
2. **Find element whose inverse is not in set**
3. **Find two elements whose product is not in set**

Example 8: Non-Subgroups

Group: Nonzero reals under multiplication

Set $H = \{x : x = 1 \text{ or } x \text{ irrational}\}$:

- $\sqrt{2} \in H$ but $\sqrt{2} \cdot \sqrt{2} = 2 \notin H$
- **Not closed**, so not a subgroup

Set $K = \{x : x \geq 1\}$:

- $2 \in K$ but $2^{-1} = \frac{1}{2} \notin K$
- **Not inverse-closed**, so not a subgroup

Theorem 3.3: Finite Subgroup Test

Let H be a nonempty finite subset of group G. If H is closed under the operation of G, then H is a subgroup of G.

Proof of Theorem 3.3

Need only show inverse closure (Theorem 3.2).

For $a \in H$ with $a \neq e$, consider $a, a^2, a^3, \ldots$

Since H finite and closed, not all powers are distinct.
Say $a^i = a^j$ with $i > j$, so $a^{i-j} = e$.

Let $m = i - j > 0$ (smallest such positive integer).
Then $a^{m-1} \cdot a = a^m = e$, so $a^{-1} = a^{m-1} \in H$.

Therefore: H is a subgroup.

Cyclic Subgroups

Notation For element a in group G: $\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$

Note: Includes all integer powers (positive, negative, and zero)

Theorem 3.4: $\langle a \rangle$ Is a Subgroup

For any element a in group G, $\langle a \rangle$ is a subgroup of G.

Proof of Theorem 3.4

Since $a = a^1 \in \langle a \rangle$, the set is nonempty.

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

By Theorem 3.1, $\langle a \rangle$ is a subgroup.

Cyclic Groups and Generators

Definition:

- $\langle a \rangle$ is the **cyclic subgroup generated by** a
- If $G = \langle a \rangle$, then G is **cyclic** and a is a **generator** of G
- Every cyclic group is **Abelian**

Key Fact: In Chapter 4, we'll prove $|\langle a \rangle| = |a|$

Example 9: $U(10)$ is Cyclic

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

Computing $\langle 3 \rangle$:

- $3^1 = 3$
- $3^2 = 9$
- $3^3 = 27 \equiv 7 \pmod{10}$
- $3^4 = 21 \equiv 1 \pmod{10}$

Negative Powers (since $3^{-1} = 7$ in $U(10)$):

- $3^{-1} = 7$, $3^{-2} = 9$, $3^{-3} = 3$, $3^{-4} = 1$

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

Therefore: $U(10)$ is cyclic with generator 3.

Example 10: Additive Cyclic Group

Given: $\mathbb{Z}_{10}$ under addition mod 10

Computing $\langle 2 \rangle$ (additive notation: $n \cdot 2$):

- $1 \cdot 2 = 2$
- $2 \cdot 2 = 4$
- $3 \cdot 2 = 6$
- $4 \cdot 2 = 8$
- $5 \cdot 2 = 0$ (identity)

Result: $\langle 2 \rangle = \{0, 2, 4, 6, 8\}$

Observation: This is the subgroup of even elements in $\mathbb{Z}_{10}$.

Example 11: Infinite Cyclic Group

Given: $\mathbb{Z}$ under addition

Computing $\langle -1 \rangle$:

- Positive multiples: $1(-1) = -1, 2(-1) = -2, 3(-1) = -3, \ldots$
- Negative multiples: $(-1)(-1) = 1, (-2)(-1) = 2, (-3)(-1) = 3, \ldots$
- Zero multiple: $0(-1) = 0$

Result: $\langle -1 \rangle = \mathbb{Z}$

Therefore: $\mathbb{Z}$ is cyclic with generator -1 (also generator 1).

Example 12: Dihedral Group Rotations

Given: D_n with rotation R of $\frac{360^\circ}{n}$

Computing $\langle R \rangle$:

- $R^1 = R$ (rotation by $\frac{360^\circ}{n}$)
- R^2 (rotation by $\frac{720^\circ}{n}$)
- $\vdots$
- $R^n = R^{360^\circ} = e$ (full rotation)
- $R^{n+1} = R \cdot R^n = R \cdot e = R$

Pattern: Powers cycle with period n
$\langle R \rangle = \{e, R, R^2, \ldots, R^{n-1}\}$

Visual: Moving counterclockwise around vertices for positive powers, clockwise for negative powers.

Example 13: D_3 as Subgroup of D_6

Setup: Equilateral triangle inscribed in regular hexagon

Elements:

- Rotations: R_0, R_{120}, R_{240}
- Reflections: $F, R_{120}F, R_{240}F$

Verification: $K = \{R_0, R_{120}, R_{240}, F, R_{120}F, R_{240}F\}$ forms a subgroup of D_6.

Structure: This demonstrates how smaller dihedral groups naturally embed in larger ones.

Generated Subgroups

Definition: Subgroup Generated by Set S

For subset S of group G, $\langle S \rangle$ is the **smallest subgroup** of G containing S.

Equivalently: $\langle S \rangle$ is the intersection of all subgroups of G that contain S.

Example 14: Multiple Generators

In $\mathbb{Z}_{20}$: $\langle 8, 14\rangle = \{0, 2, 4, \ldots, 18\} = \langle 2\rangle$

In $\mathbb{Z}$: $\langle 8, 13\rangle = \mathbb{Z}$

In D_4: $\langle H, V\rangle = \{R_0, R_{180}, H, V\}$, $\langle R_{90}, V\rangle = D_4$

In $\mathbb{R}$ (addition): $\langle 2, \pi, \sqrt{2}\rangle = \{2a + b\pi + c\sqrt{2} : a, b, c \in \mathbb{Z}\}$

Center of a Group

Definition: Center of a Group

The **center** $Z(G)$ of group G is:
$$Z(G) = \{a \in G : ax = xa \text{ for all } x \in G\}$$

Interpretation: Elements that commute with every group element.

Theorem 3.5: Center Is a Subgroup

The center $Z(G)$ of any group G is a subgroup of G.

Proof of Theorem 3.5

Identity: $ex = xe$ for all $x \in G$, so $e \in Z(G)$.

Closure: For $a, b \in Z(G)$ and any $x \in G$:
$(ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab)$

So $ab \in Z(G)$.

Inverses: For $a \in Z(G)$ and any $x \in G$, we have $ax = xa$.
Multiply both sides by a^{-1} on left and right:
$a^{-1}(ax)a^{-1} = a^{-1}(xa)a^{-1}$
$xa^{-1} = a^{-1}x$

So $a^{-1} \in Z(G)$.

Example 15: Centers of Dihedral Groups

Statement: For ($n \geq 3$), $Z(D_n) = \{ R_0, R_{180} \quad \text{if } n \text{ is even } R_0 \ \text{ if } n \text{ is odd}$

Detailed Verification:

Step 1: Rotations commute with each other

- Every rotation in (D_n) is a power of ($R_{360/n}$)
- Powers of the same element commute: ($R^i \cdot R^j = R^{i+j} = R^{j+i} = R^j \cdot R^i$)

Step 2: When do rotations commute with reflections?

- Let (R) be any rotation in (D_n) and (F) any reflection in (D_n)
- Key insight: (RF) is a reflection (composition of rotation and reflection)
- Therefore: ($RF = (RF)^{-1} = F^{-1}R^{-1} = FR^{-1}$) (since reflections are self-inverse)

Step 3: Condition for commutativity

- R and F commute if and only if $RF = FR$
- From Step 2: $RF = FR^{-1}$
- So: $RF = FR$ if and only if $FR = FR^{-1}$
- By cancellation: $R = R^{-1}$

Step 4: When does $R = R^{-1}$?

- ($R = R^{-1}$) if and only if ($R^2 = e$)
- In (D_n): only (R_0) (identity) and (R_{180}) (when it exists) satisfy this
- (R_{180}) exists in (D_n) only when (n) is even

Conclusion:

- When (n) is odd: only (R_0) commutes with all elements $\rightarrow$ $(Z(D_n) = R_0$)
- When (n) is even: both (R_0) and (R_{180}) commute with all elements $\rightarrow$ $(Z(D_n) = R_0, R_{180}$)

Definition: Centralizer of a in G

Definition: Let a be a fixed element of a group G. The **centralizer of a in G**, denoted $C(a)$, is the set of all elements in G that commute with a.

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

Key Properties:

- $a \in C(a)$ (every element commutes with itself)
- All powers of a are in $C(a)$: $a^n \in C(a)$ for all $n \in \mathbb{Z}$
- $e \in C(a)$ (identity commutes with everything)
- $Z(G) \subseteq C(a)$ for every $a \in G$

Example 16: Centralizers in D_4

Setup: Recall $D_4 = \{R_0, R_{90}, R_{180}, R_{270}, H, V, D, D'\}$

- Rotations: R_0 (identity), R_{90}, R_{180}, R_{270}
- Reflections: H (horizontal), V (vertical), D (diagonal), D' (other diagonal)

Detailed Calculations:

1. Centralizers of Rotations:

- $C(R_0) = D_4$ (identity commutes with everything)
- $C(R_{180}) = D_4$ (from Example 15, $R_{180} \in Z(D_4)$)
- $C(R_{90}) = \{R_0, R_{90}, R_{180}, R_{270}\}$
  - All rotations commute with each other
  - No reflections commute with R_{90} (since $R_{90} \neq R_{90}^{-1} = R_{270}$)
- $C(R_{270}) = \{R_0, R_{90}, R_{180}, R_{270}\} = C(R_{90})$
  - Same reasoning as for R_{90}

2. Centralizers of Reflections:

- $C(H) = \{R_0, H, R_{180}, V\}$
  - R_0, R_{180} are in the center
  - H commutes with itself
  - V commutes with H because both are "axis-parallel" reflections
- $C(V) = \{R_0, H, R_{180}, V\} = C(H)$
- $C(D) = \{R_0, D, R_{180}, D'\}$
  - R_0, R_{180} are in the center
  - D commutes with itself
  - D' commutes with D because both are diagonal reflections
- $C(D') = \{R_0, D, R_{180}, D'\} = C(D)$

Pattern: Each centralizer forms a subgroup of order 4 in D_4 (which has order 8).

Theorem 3.6: C(a) Is a Subgroup

Theorem: For each a in a group G, the centralizer of a is a subgroup of G.

Proof: We use the Two-Step Subgroup Test (Theorem 3.2).

Step 1: Show $C(a)$ is nonempty

- Since $ae = ea = a$, we have $e \in C(a)$
- Therefore $C(a) \neq \emptyset$

Step 2: Show closure under the operation

- Let $g_1, g_2 \in C(a)$
- This means $g_1 a = a g_1$ and $g_2 a = a g_2$
- We must show $(g_1 g_2)a = a(g_1 g_2)$

Computation: $(g_1 g_2)a = g_1(g_2 a) = g_1(a g_2) = (g_1 a)g_2 = (a g_1)g_2 = a(g_1 g_2)$

- Therefore $g_1 g_2 \in C(a)$

Step 3: Show closure under inverses

- Let $g \in C(a)$, so $ga = ag$
- We must show $g^{-1}a = ag^{-1}$

Computation: From $ga = ag$, multiply both sides on the left by g^{-1} and on the right by g^{-1}:

- $g^{-1}(ga)g^{-1} = g^{-1}(ag)g^{-1}$
- $(g^{-1}g)ag^{-1} = g^{-1}a(gg^{-1})$
- $eag^{-1} = g^{-1}ae$
- $ag^{-1} = g^{-1}a$
- Therefore $g^{-1} \in C(a)$

Conclusion: By the Two-Step Subgroup Test, $C(a)$ is a subgroup of G. □

Key Relationships: Center and Centralizers

1. Center is contained in every centralizer:

$$Z(G) \subseteq C(a) \text{ for all } a \in G$$

Proof: If $z \in Z(G)$, then $za = az$ for all $a \in G$, so $z \in C(a)$ for any particular a.

2. Characterization of Abelian groups:

$$G \text{ is Abelian} \iff C(a) = G \text{ for all } a \in G$$

Proof:

- ($\Rightarrow$) If G is Abelian, every element commutes with every other element
- ($\Leftarrow$) If $C(a) = G$ for all a, then every element commutes with every other element

3. Self-centralizing property: $a \in C(a)$ always holds

4. Hierarchy of containment:

For any element a in group G:

$\{e\} \subseteq \langle a \rangle \subseteq C(a) \subseteq G$

$Z(G) \subseteq C(a) \subseteq G$