Chapter 7 Cosets and Lagrange's Theorem

Definition of Cosets of H in G:

Let G be a group and let H be a nonempty subset of G. For any $a \in G$:

- **Left coset:** $aH = \{ah \mid h \in H\}$
- **Right coset:** $Ha = \{ha \mid h \in H\}$
- **Conjugate:** $aHa^{-1} = \{aha^{-1} \mid h \in H\}$

When H is a subgroup of G:

- The set aH is called the **left coset of H in G containing a**
- The set Ha is called the **right coset of H in G containing a**
- The element a is called the **coset representative** of aH (or Ha)

Example 1 (Cosets in S_3): Let $G = S_3$ and $H = \{(1), (13)\}$. Left cosets of H in G are:

1. $(1)H = H = \{(1), (13)\}$
2. $(12)H = \{(12), (12)(13)\} = \{(12), (132)\} = (132)H$
3. $(13)H = \{(13), (1)\} = H$
4. $(23)H = \{(23), (23)(13)\} = \{(23), (123)\} = (123)H$

Observations:

- Different elements can generate the same coset: $(12)H = (132)H$
- Elements in H generate H itself: $(1)H = (13)H = H$
- We have exactly 3 distinct cosets: H, $(12)H$, and $(23)H$

Example 2: Left Cosets in the Dihedral Group Let $K = \{R_0, R_{180}\}$ in D_4, the dihedral group of order 8. The left cosets of K in D_4 are:

- $R_0K = K = \{R_0, R_{180}\}$
- $R_{90}K = \{R_{90}, R_{270}\} = R_{270}K$
- $R_{180}K = \{R_{180}, R_0\} = K$
- $VK = \{V, H\} = HK$
- $DK = \{D, D'\} = D'K$

Key Point: The group D_4 is partitioned into distinct cosets, each of size $|K| = 2$.

Example 3: Cosets in Additive Groups: Let $H = \{0, 3, 6\}$ in $\mathbb{Z}_9$ under addition.

Note: For additive notation, we write $a + H$ instead of aH. The cosets of H in $\mathbb{Z}_9$ are:

- $0 + H = \{0, 3, 6\} = 3 + H = 6 + H$
- $1 + H = \{1, 4, 7\} = 4 + H = 7 + H$
- $2 + H = \{2, 5, 8\} = 5 + H = 8 + H$

Important Observations:

1. Cosets are usually **not subgroups** (e.g., $1 + H$ is not closed)
2. aH may equal bH even when $a \neq b$
3. Left and right cosets may differ: $aH \neq Ha$ in general

Lemma: Properties of Cosets: Let H be a subgroup of G, and let $a, b \in G$. Then:

Property 1: $a \in aH$ (Every left coset contains its representative)

Property 2: $aH = H$ if and only if $a \in H$ (H "absorbs" elements that belong to it)

Property 3: $(ab)H = a(bH)$ and $H(ab) = (Ha)b$ (Coset multiplication is associative with group elements)

Property 4: $aH = bH$ if and only if $a \in bH$ (A coset is uniquely determined by any of its elements)

Property 5: $aH = bH$ or $aH \cap bH = \emptyset$ (Two cosets are either identical or disjoint)

Property 6: $aH = bH$ if and only if $a^{-1}b \in H$ (Coset equality can be tested via membership in H)

Property 7: $|aH| = |bH|$ (All cosets have the same size)

Property 8: $aH = Ha$ if and only if $H = aHa^{-1}$ (Left and right cosets coincide iff H is conjugate to itself)

Property 9: aH is a subgroup of G if and only if $a \in H$ (Only H itself is both a coset and a subgroup)

Key Insight: Properties 1, 5, and 7 show that the left cosets of H partition G into blocks of equal size.

Proofs:

Property 1: $a \in aH$

Proof of Property 1: $a = ae \in aH$ (since $e \in H$)

Property 2: $aH = H$ if and only if $a \in H$

Proof of Property 2:

- ($\Rightarrow$) If $aH = H$, then $a = ae \in aH = H$.
- ($\Leftarrow$) Assume $a \in H$.
  - To show $aH \subseteq H$: For $h \in H$, we have $ah \in H$ by closure.
  - To show $H \subseteq aH$: Let $h \in H$. Since $a \in H$, we have $a^{-1} \in H$, so $a^{-1}h \in H$. Thus $h = e \cdot h = (aa^{-1})h = a(a^{-1}h) \in aH$

Property 3: $(ab)H = a(bH)$ and $H(ab) = (Ha)b$

Proof of Property 3: This follows directly from associativity:

- $(ab)h = a(bh)$ for all $h \in H$
- $h(ab) = (ha)b$ for all $h \in H$

Property 4: $aH = bH$ if and only if $a \in bH$

Proof of Property 4:

- ($\Rightarrow$) If $aH = bH$, then $a = ae \in aH = bH$.
- ($\Leftarrow$) If $a \in bH$, then $a = bh$ for some $h \in H$. Therefore:
  - $aH = (bh)H = b(hH) = bH$
  - where the last equality uses Property 2 (since $h \in H$, we have $hH = H$).

Property 5: $aH = bH$ or $aH \cap bH = \emptyset$

Proof of Property 5:

- If there exists $c \in aH \cap bH$, then by Property 4:
  - $c \in aH$ implies $cH = aH$
  - $c \in bH$ implies $cH = bH$
  - Therefore $aH = bH$
- If $aH \neq bH$, then $aH \cap bH = \emptyset$.

Property 6: $aH = bH$ if and only if $a^{-1}b \in H$

Proof of Property 6: We have $aH = bH$ if and only if $H = a^{-1}bH$ (multiply both sides by a^{-1} on left).

This holds if and only if $a^{-1}b \in H$ (by Property 2).

Property 7: $|aH| = |bH|$

Proof of Property 7: Define $\phi : aH \to bH$ by $\phi(ah) = bh$ for $h \in H$.

- **Well-defined and onto:** Clear from definition
- **One-to-one:** If $\phi(ah_1) = \phi(ah_2)$, then $bh_1 = bh_2$. By cancellation, $h_1 = h_2$, so $ah_1 = ah_2$.

Therefore ϕ is a bijection, so $|aH| = |bH|$

Property 8: $aH = Ha$ if and only if $H = aHa^{-1}$

Proof of Property 8: We have $aH = Ha$ if and only if $(aH)a^{-1} = (Ha)a^{-1}$.

This holds if and only if $aHa^{-1} = H(aa^{-1}) = H$.

Property 9: aH is a subgroup of G if and only if $a \in H$

Proof of Property 9:

- ($\Rightarrow$) If aH is a subgroup, then $e \in aH$. So $aH \cap eH = aH \cap H \neq \emptyset$. By Property 5, $aH = eH = H$. By Property 2, $a \in H$.
- ($\Leftarrow$) If $a \in H$, then by Property 2, $aH = H$, which is a subgroup.

Example: Cosets of $H = \{1, 15\}$ in $U(32)$

$$G = U(32) = \{1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31\}$$

Strategy: Use Property 5 to systematically find all distinct cosets. **Step-by-step:**

1. Start with $H = \{1, 15\}$
2. Choose $3 \notin H$: Get $3H = \{3, 45 \bmod 32\} = \{3, 13\}$
3. Choose $5 \notin H \cup 3H$: Get $5H = \{5, 75 \bmod 32\} = \{5, 11\}$
4. Continue choosing representatives not yet in any coset
5. Continue until all elements of $U(32)$ are accounted for

Result: We obtain $|U(32)|/|H| = 16/2 = 8$ distinct cosets.

Practical Application: This method works for any finite group and subgroup!

Cosets partition groups in meaningful ways:

Example (Geometric Views of Cosets)**: Geometry in 3-Space**

- Let $G = \mathbb{R}^3$ and H = a plane through the origin
- The coset $(a, b, c) + H$ is the plane through (a, b, c) parallel to H
- Cosets partition 3-space into parallel planes

Example(Algebraic Views of Cosets**): Matrix Determinants**

- Let $G = GL(2, \mathbb{R})$ and $H = SL(2, \mathbb{R})$ (matrices with $\det = 1$)
- For any matrix $A \in G$, the coset AH consists of all 2×2 matrices with the same determinant as A
- Example: $\begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix} H$ = all matrices with determinant 2

Theorem (Lagrange's Thm): If G is a finite group and H is a subgroup of G, then $|H|$ divides $|G|$. Moreover, the number of distinct left (right) cosets of H in G is $|G|/|H|$.

Proof: Let $a_1H, a_2H, \ldots, a_rH$ denote the distinct left cosets of H in G.

1. For each $a \in G$, we have $aH = a_iH$ for some i. By Property 1 of Lemma 7.1, $a \in aH$. Therefore, every element of G belongs to some coset: $G = a_1H \cup a_2H \cup \cdots \cup a_rH$.
2. By Property 5 of Lemma 7.1, this union is **disjoint.** Therefore: $|G| = |a_1H| + |a_2H| + \cdots + |a_rH|$
3. By Property 7 of Lemma 7.1, $|a_iH| = |H|$ for each i. Thus: $|G| = r|H|$, where r is the number of distinct left cosets.
4. This gives us $|H|$ divides $|G|$ and $r = |G|/|H|$. ∎

Definition: The **index** of a subgroup H in G is the number of distinct left cosets of H in G.

Notation: $|G : H|$

Corollary (Formula for Index): If G is a finite group and H is a subgroup of G, then:
$|G : H| = \frac{|G|}{|H|}$. (**Proof:** This is immediate from Lagrange's Theorem.)

Example: In S_3 with $H = \{(1), (13)\}$:

- $|S_3| = 6$, $|H| = 2$
- $|S_3 : H| = 6/2 = 3$ (we found 3 distinct cosets in Example 1)

Corollary ($|a|$ divides $|G|$): In a finite group, the order of each element of the group divides the order of the group.

Proof: Let $a \in G$. Since $|a| = |\langle a \rangle|$ and $\langle a \rangle$ is a subgroup of G, Lagrange's Theorem gives us that $|\langle a \rangle|$ divides $|G|$.

Important Consequence: In a group of order n, every element a satisfies $a^n = e$.

Corollary (Groups of Prime Order Are Cyclic):

Every group of prime order is isomorphic to $\mathbb{Z}_p$.

Proof:

- Suppose $|G| = p$ where p is prime
- Let $a \in G$ with $a \neq e$
- Then $|\langle a \rangle|$ divides p by Lagrange's Theorem
- Since p is prime, either $|\langle a \rangle| = 1$ or $|\langle a \rangle| = p$
- Since $a \neq e$, we have $|\langle a \rangle| \neq 1$
- Therefore $|\langle a \rangle| = p = |G|$
- This means $\langle a \rangle = G$, so G is cyclic
- Every cyclic group of order p is isomorphic to $\mathbb{Z}_p$ (From Chapter 6). ∎

Corollary: Let G be a finite group, and let $a \in G$. Then $a^{|G|} = e$.

Proof:

- By aprevious Corollary, we know $|a|$ divides $|G|$
- Therefore $|G| = |a| \cdot k$ for some positive integer k
- Thus: $a^{|G|} = a^{|a| \cdot k} = (a^{|a|})^k = e^k = e$

Example: In any group of order 12, every element a satisfies $a^{12} = e$.

Corollary: For every integer a and every prime p: $a^p \bmod p = a \bmod p$

Proof:

- By the division algorithm, $a = pm + r$ where $0 \leq r < p$
- Thus $a \bmod p = r$, so it suffices to prove $r^p \bmod p = r$
- If $r = 0$, the result is trivial
- Assume $r \neq 0$. Then $r \in U(p) = \{1, 2, \dots, p-1\}$ under multiplication modulo p
- Since $|U(p)| = p - 1$, Corollary 4 gives us: $r^{p-1} \bmod p = 1$
- Multiplying both sides by r: $r^p \bmod p = r \bmod p$

Warning - Converse of Lagrange is False!

False Statement: If d divides $|G|$, then G has a subgroup of order d.

Counterexample: A_4 has order 12 but has **no subgroup of order 6**.

Why this matters:

- Lagrange gives us *necessary* conditions for subgroup orders
- It does **not** give *sufficient* conditions
- We need additional theorems to guarantee existence of subgroups

Good News: Later theorems (Cauchy's Theorem, Sylow Theorems) do guarantee existence of subgroups of certain orders.

Example: A_4 Has No Subgroup of Order 6

Proof by contradiction: A_4 contains 8 elements of order 3. Suppose H is a subgroup of order 6. Let a be any element of order 3 in A_4.

Case 1: Assume $a \notin H$. Then $A_4 = H \cup aH$ (since $|A_4| = 12$ and $|aH| = 6$). So $a^2 \in H$ or $a^2 \in aH$:

- If $a^2 \in H$. Since H is a subgroup, $(a^2)^2 = a^4 = a \in H$. This contradicts our assumption that $a \notin H$.
- If $a^2 \in aH$. Then $a^2 = ah$ for some $h \in H$. Multiplying by a^{-1} on the left: $a = h \in H$. This contradicts our assumption that $a \notin H$.

So every element of order 3 must be in H. But $|H| = 6 < 8$, which is impossible. Therefore, A_4 has no subgroup of order 6. ∎

Definition: For subgroups H and K of a group G: $HK = \{hk \mid h \in H, k \in K\}$

Theorem 7.2: For two finite subgroups H and K of a group: $|HK| = |H||K|/|H \cap K|$.

Important Note: HK is not always a subgroup! (See Exercise 6)

Proof of $|HK| = |H||K|/|H \cap K|$:

1. The set HK contains $|H||K|$ products, but these may not all be distinct
2. For every $t \in H \cap K$ and every product $hk \in HK$: $(ht)(t^{-1}k) = h(tt^{-1})k = hk$
   So each element in HK is represented at least $|H \cap K|$ times.
3. Conversely, if $hk = h'k'$, then: $t = h^{-1}h' = kk'^{-1} \in H \cap K$. And we can write $h' = ht$ and $k' = t^{-1}k$.
4. So each element in HK is represented **exactly** $|H \cap K|$ times. Therefore,
   $$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Theorem 7.3: Let G be a group of order $2p$, where p is a prime greater than 2. Then G is isomorphic to $\mathbb{Z}_{2p}$ or D_p.

Strategy of proof:

- Assume G has no element of order $2p$ (otherwise $G \cong \mathbb{Z}_{2p}$).
- Show G must have an element of order p.
- Show G must have an element of order 2.
- Determine the multiplication structure uniquely.
- Verify this gives D_p.

Proof: Finding an Element of Order p

Assume G has no element of order $2p$. **Claim:** G must have an element of order p:

- By Lagrange's Theorem, every nonidentity element has order 2 or p
- Suppose every nonidentity element has order 2. Then for all $a, b \in G$: $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$. So G would be Abelian.
- Pick distinct nonidentity elements $a, b \in G$ with $a \neq b$
- The set $\{e, a, b, ab\}$ is closed under multiplication. Therefore it's a subgroup of order 4.

Contradiction: $4 \nmid 2p$ for prime $p > 2$. **So** G must have an element of order p. Call it a.

Next step: Let b be any element not in $\langle a \rangle$. **Determine** $|b|$:

- By Lagrange, $|\langle a\rangle \cap \langle b\rangle|$ divides $|\langle a\rangle| = p$.
- Since $b \notin \langle a\rangle$, we have $\langle a\rangle \neq \langle b\rangle$. Therefore $|\langle a\rangle \cap \langle b\rangle| = 1$.
- If $|b| = p$. Then $|\langle a\rangle\langle b\rangle| = \dfrac{p \cdot p}{1} = p^2 > 2p$. This is impossible since $|\langle a\rangle\langle b\rangle| \leq |G| = 2p$. So $|b| = 2$ for any $b \notin \langle a\rangle$.

Structure of G: $G = \langle a\rangle \cup \langle a\rangle b = \{e, a, a^2, \dots, a^{p-1}, b, ab, a^2b, \dots, a^{p-1}b\}$

Now the multiplication table is **uniquely** determined by **Key relations:**

1. $\boxed{a^p = b^2 = e}$.

2. Since $ab \notin \langle a \rangle$, $|ab| = 2$. So $(ab)(ab) = e \Rightarrow abab = e \Rightarrow bab = a^{-1} \Rightarrow$ $ba^j = (bab)(ba^{j-1}) = a^{-1}(ba^{j-1}) = \cdots = a^{-j}b$. So $\boxed{ba^j = a^{-j}b}$

The three types of products in Cayley table for G:

1. $a^i \cdot a^j = a^{i+j}$ (usual cyclic group multiplication)
2. $a^i \cdot (a^j b) = a^{i+j} b$ (clear)
3. $(a^i b) \cdot (a^j b) = a^i (ba^j) b = a^i (a^{-j} b) b = a^{i-j} b^2 = a^{i-j}$

What we've shown: When $p > 2$ is prime, a group G of order $2p$ satisfies one of two conditions:

Case 1: G has an element of order $2p$. Then G is cyclic. Therefore $G \cong \mathbb{Z}_{2p}$

Case 2: G has no element of order $2p$:

- Then G has exactly the structure: $G = \{e, a, a^2, \ldots, a^{p-1}, b, ab, \ldots, a^{p-1}b\}$
- With relations: $|a| = p$, $b^2 = e$, $bab = a^{-1}$
- The multiplication table is uniquely determined
- These are precisely the defining relations of D_p
- Therefore $G \cong D_p$

Final conclusion: $G \cong \mathbb{Z}_{2p}$ or $G \cong D_p$. ∎

Immediate Corollary:

- $S_3 \cong D_3$ (both are non-abelian groups of order 6)
- $GL(2, \mathbb{Z}_2) \cong D_3$ (from Exercise 47, Chapter 2)