9: Normal Subgroups and Factor Groups

In previous chapters, we studied:

- Groups and their basic properties
- Subgroups and their structure
- Cosets and Lagrange's Theorem

Key Question: When can we make the set of cosets into a group?

This Chapter's Goals:

1. Define normal subgroups
2. Understand when cosets form a group (factor groups)
3. Explore the structure of factor groups
4. See applications and examples

Definition: Normal Subgroup: Let G be a group and H a subgroup of G. We say H is a **normal subgroup** of G, denoted $H \triangleleft G$, if: $gH = Hg \text{ for all } g \in G$.

Important: This does NOT mean $gh = hg$ for all $g \in G, h \in H$. It means the LEFT cosets equal the RIGHT cosets as sets.

Theorem 1: Normal Subgroup Test: A subgroup H of G is normal in G if and only if: $xHx^{-1} \subseteq H \text{ for all } x \in G$.

Proof of Theorem: ($\Rightarrow$) Assume $H \triangleleft G$: For any $h \in H$ and $g \in G$: $gh \in gH = Hg$. So $gh = h'g$ for some $h' \in H$. Therefore $ghg^{-1} = h' \in H$. This shows $gHg^{-1} \subseteq H$.

($\Leftarrow$) Assume $xHx^{-1} \subseteq H$ for all $x \in G$: We need to show $xH = Hx$ for all $x \in G$. Take any $xh \in xH$ where $h \in H$. Since $xHx^{-1} \subseteq H$, we have $xhx^{-1} = h'$ for some $h' \in H$. Thus $xh = h'x \in Hx$, so $xH \subseteq Hx$. Similarly, $x^{-1}Hx \subseteq H$ implies $Hx \subseteq xH$. Therefore $xH = Hx$ ∎

Note: The condition $xHx^{-1} \subseteq H$ actually implies $xHx^{-1} = H$ because: If $xHx^{-1} \subseteq H$ for all $x \in G$. Then $x^{-1}Hx \subseteq H$ (replacing x with x^{-1}). Multiplying on left by x and right by x^{-1}: $H \subseteq xHx^{-1}$. Therefore $xHx^{-1} = H$. In fact $H \triangleleft G$ iff any of the following equivalent conditions is satisfied:

- $gH = Hg$ for all $g \in G$.
- $gHg^{-1} = H$ for all $g \in G$.
- $ghg^{-1} \in H$ for all $g \in G$ and all $h \in H$.

Example 1: Every subgroup of an abelian group is normal.

Proof: Let G be an abelian group and H be any subgroup of G. For any $g \in G$ and $h \in H$:

- Since G is abelian: $gh = hg$
- Therefore: $ghg^{-1} = hgg^{-1} = he = h \in H$
- This shows $gHg^{-1} \subseteq H$ for all $g \in G$. By Theorem 1, $H \triangleleft G$. ■

Key Insight: In abelian groups, left and right cosets are always equal because elements commute. This makes every subgroup normal.

Interactive Question: [Quiz]

Q: Consider the group $\mathbb{Z}_{12}$ under addition. How many normal subgroups does it have?

A) 2 (only $\{0\}$ and $\mathbb{Z}_{12}$)

B) 3

C) 4

D) All of its subgroups are normal.

Example 2: The center $Z(G)$ of a group G is always a normal subgroup.

Recall: $Z(G) = \{z \in G : zg = gz \text{ for all } g \in G\}$

Proof: Let $z \in Z(G)$ and $g \in G$. We have $gzg^{-1} = zgg^{-1} = z \in Z(G)$, so $Z(G) \triangleleft G$.

Example 3: The alternating group A_n is normal in the symmetric group S_n.

Proof: We'll show that $\sigma A_n = A_n \sigma$ for all $\sigma \in S_n$.

Case 1: If $\sigma \in A_n$ (even permutation). Then $\sigma A_n = A_n$ (since A_n is a subgroup). And $A_n \sigma = A_n$. So $\sigma A_n = A_n \sigma$.

Case 2: If $\sigma \notin A_n$ (odd permutation). Then σA_n consists of all odd permutations (odd × even = odd). And $A_n \sigma$ also consists of all odd permutations (even × odd = odd). Both equal $S_n \setminus A_n$. So $\sigma A_n = A_n \sigma$.

Therefore $A_n \triangleleft S_n$. ■

Example 4: $SL(n, \mathbb{R}) \triangleleft GL(n, \mathbb{R})$

Recall:

- $GL(n, \mathbb{R}) = \{n \times n \text{ matrices with } \det(A) \neq 0\}$
- $SL(n, \mathbb{R}) = \{n \times n \text{ matrices with } \det(A) = 1\}$

Proof: Let $A \in SL(n, \mathbb{R})$ and $B \in GL(n, \mathbb{R})$. We need to show $BAB^{-1} \in SL(n, \mathbb{R})$. Using the determinant property $\det(XY) = \det(X)\det(Y)$:

$$\det(BAB^{-1}) = \det(B) \cdot \det(A) \cdot \det(B^{-1}) = \det(B) \cdot 1 \cdot \frac{1}{\det(B)} = 1$$

Therefore $BAB^{-1} \in SL(n, \mathbb{R})$. So $SL(n, \mathbb{R}) \triangleleft GL(n, \mathbb{R})$. ∎

Example 5: Any subgroup H of index 2 in a group G is normal.

Proof: If $g \in H$, then $gH = H = Hg$. If $g \notin H$, then since $[G : H] = 2$, G is **partitioned** into the **disjoint** left cosets H and gH and into the **disjoint** right cosets H and **Hg**. Since H is shared, we must have $gH = Hg$. Therefore $H \triangleleft G$. ■

Example 6: Not all subgroups are normal. Consider $H = \{e, (12)\}$ in S_3. Claim $H \not\triangleleft S_3$:

Method 1: $(13) \cdot (12) \cdot (13)^{-1} = (13) \cdot (12) \cdot (13) = (23) \notin H$.

Method 2: $(13)H = \{(13), (123)\} \neq H(13) = \{(13), (132)\}$

Example 7: Let $K = \langle (123) \rangle = \{e, (123), (132)\}$ in S_3. Then $K \triangleleft S_3$:

Proof: Index argument: $|S_3| = 6$ and $|K| = 3$. So $[S_3 : K] = 6/3 = 2$. By Example 5, any subgroup of index 2 is normal. Therefore $K \triangleleft S_3$.

Example 8: Consider D_4, the dihedral group of order 8. **Recall:** $D_4 = \{e, r, r^2, r^3, f, rf, r^2f, r^3f\}$ where:

- r = rotation by 90°
- f = reflection (flip)
- $r^4 = e, f^2 = e, frf = r^{-1}$

The subgroup: $H = \{e, r^2\} \triangleleft D_4$ because $H = Z(D_4)$.

The subgroup $K = < r > \triangleleft D_4$ because it has index 2.

Example 9: The Klein four-group $V = \{e, (12)(34), (13)(24), (14)(23)\}$ is normal in A_4.

Proof: For any $\sigma \in A_4$ and any $\tau \in V$. Since $(\sigma\tau\sigma^{-1})^2 = e$ and the elements outside of V are 3-cycles, we must have $\sigma\tau\sigma^{-1} \in V$.

Question: Which statement is **FALSE** about normal subgroups?

A) If $H \triangleleft G$ and $K \triangleleft G$, then $H \cap K \triangleleft G$

B) If $H \triangleleft G$ and $K \triangleleft H$, then $K \triangleleft G$

C) If G is abelian, then every subgroup is normal

D) If $[G : H] = 2$, then $H \triangleleft G$.

Theorem 2: Let G be a group and H a normal subgroup of G. The set of cosets $G/H = \{gH : g \in G\}$ forms a group under the operation: $(aH)(bH) = (ab)H$. This group is called the **factor group** (or **quotient group**) of G by H.

Proof: Well-Definedness: We must show that if $aH = a'H$ and $bH = b'H$, then $(ab)H = (a'b')H$. **Given:** $aH = a'H$ and $bH = b'H$. This means:

- $a' = ah_1$ for some $h_1 \in H$
- $b' = bh_2$ for some $h_2 \in H$

Then using normality:

$$a'b' = (ah_1)(bh_2) = a(h_1b)h_2 = a(bh_3)h_2 = ab(h_3h_2) \in abH$$

Conclusion: $a'b' \in abH$, which means $(a'b')H = (ab)H$.

Now we verify that G/H with operation $(aH)(bH) = (ab)H$ satisfies the group axioms.

1. Closure: For any $aH, bH \in G/H$, we have $(ab)H \in G/H$ since $ab \in G$.

2. Associativity: (using associativity in G)
$aH(bHcH) = aHbcH = a(bc)H = (ab)cH = abHcH = (aHbH)cH$

3. Identity: $eH = H$ is the identity since: $(eH)(gH) = (eg)H = gH$ and $(gH)(eH) = (ge)H = gH$ for all $gH \in G/H$.

4. Inverses: For $gH \in G/H$, the inverse is $g^{-1}H$ because:
$(gH)(g^{-1}H) = (gg^{-1})H = eH = H$ and $(g^{-1}H)(gH) = (g^{-1}g)H = eH = H$.

Therefore G/H is a group. ∎

Example 10: The factor group $\mathbb{Z}/4\mathbb{Z}$

Setup: $G = \mathbb{Z}$ (integers under addition). $H = 4\mathbb{Z} = \{0, \pm 4, \pm 8, \pm 12, \ldots\}$ (multiples of 4). Since $\mathbb{Z}$ is abelian, $4\mathbb{Z} \triangleleft \mathbb{Z}$. **The cosets of $4\mathbb{Z}$ in $\mathbb{Z}$:**

- $0 + 4\mathbb{Z} = \{\ldots, -8, -4, 0, 4, 8, \ldots\}$
- $1 + 4\mathbb{Z} = \{\ldots, -7, -3, 1, 5, 9, \ldots\}$
- $2 + 4\mathbb{Z} = \{\ldots, -6, -2, 2, 6, 10, \ldots\}$
- $3 + 4\mathbb{Z} = \{\ldots, -5, -1, 3, 7, 11, \ldots\}$

The factor group: $\mathbb{Z}/4\mathbb{Z} = \{0 + 4\mathbb{Z}, 1 + 4\mathbb{Z}, 2 + 4\mathbb{Z}, 3 + 4\mathbb{Z}\}$

Operation (addition of cosets): $(a + 4\mathbb{Z}) + (b + 4\mathbb{Z}) = (a + b) + 4\mathbb{Z}$

The factor group $\mathbb{Z}/4\mathbb{Z}$ is isomorphic to $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ under addition modulo 4.

Example 11: The factor group $\mathbb{Z}_{18}/\langle 6\rangle$

Setup: $G = \mathbb{Z}_{18} = \{0, 1, 2, \ldots, 17\}$ under addition modulo 18. $H = \langle 6\rangle = \{0, 6, 12\}$ (cyclic subgroup generated by 6). Since $\mathbb{Z}_{18}$ is abelian, $H \triangleleft \mathbb{Z}_{18}$. **Finding the cosets:**

- $0 + H = \{0, 6, 12\}$
- $1 + H = \{1, 7, 13\}$
- $2 + H = \{2, 8, 14\}$
- $3 + H = \{3, 9, 15\}$
- $4 + H = \{4, 10, 16\}$
- $5 + H = \{5, 11, 17\}$

The factor group: $\mathbb{Z}_{18}/\langle 6\rangle = \{0 + H, 1 + H, 2 + H, 3 + H, 4 + H, 5 + H\}$

Order: $|\mathbb{Z}_{18}/\langle 6\rangle| = \dfrac{18}{3} = 6$

Structure: This factor group is isomorphic to $\mathbb{Z}_6$.

Example 12: Factor group of the dihedral group D_4

Setup: $D_4 = \{e, r, r^2, r^3, f, rf, r^2f, r^3f\}$ (order 8). $K = \{e, r^2, f, r^2f\}$ (order 4).
First, verify K is a subgroup:

- Closure: Check all products (can verify from D_4 multiplication table)
- Identity: $e \in K$ ✓
- Inverses: $e^{-1} = e$, $(r^2)^{-1} = r^2$, $f^{-1} = f$, $(r^2f)^{-1} = r^2f$ ✓

K is normal: Since $[D_4 : K] = 8/4 = 2$, by Example 5, $K \triangleleft D_4$. So $D_4/K \cong \mathbb{Z}_2$.

Table1: Summary of Factor Group Examples

Group G	Normal Subgroup H	Factor Group G/H	Order	Structure
$\mathbb{Z}$	$n\mathbb{Z}$	$\mathbb{Z}/n\mathbb{Z}$	n	$\cong \mathbb{Z}_n$
$\mathbb{Z}_n$	$\langle d \rangle$ (where $d \mid n$)	$\mathbb{Z}_n/\langle d \rangle$	d	$\cong \mathbb{Z}_d$
$\mathbb{Z}_{18}$	$\langle 6 \rangle$	$\mathbb{Z}_{18}/\langle 6 \rangle$	6	$\cong \mathbb{Z}_6$
S_n	A_n	S_n/A_n	2	$\cong \mathbb{Z}_2$
$GL(n,\mathbb{R})$	$SL(n,\mathbb{R})$	$GL(n,\mathbb{R})/SL(n,\mathbb{R})$	∞	$\cong \mathbb{R}^*$
D_4	$K = \{e, r^2, f, r^2 f\}$	D_4/K	2	$\cong \mathbb{Z}_2$
A_4	V (Klein 4-group)	A_4/V	3	$\cong \mathbb{Z}_3$

General Pattern:

- Cyclic groups factor to cyclic groups
- Factor groups can be simpler (more abelian) than the original
- $|G/H| = |G|/|H|$ when G is finite

Question: If G is a non-abelian group and $H \triangleleft G$, which is possible?

A) G/H must be non-abelian

B) G/H must be abelian

C) G/H could be either abelian or non-abelian

D) G/H cannot exist

KEY APPLICATIONS OF FACTOR GROUPS:

- **Proving groups are Abelian** (G/Z Theorem)
- **Finding elements of specific orders** (pull-back constructions)
- **Computing automorphism groups** (Inn(G) theorem)
- **Proving existence theorems** (Cauchy's Theorem)

The following theorems demonstrate the power of this approach.

Theorem 3: Let G be a group and let $Z(G)$ be the center of G. If $G/Z(G)$ is cyclic, then G is Abelian.

Proof: Assume $G/Z(G)$ is cyclic. Then $G/Z(G) = \langle aZ(G) \rangle$ for some $a \in G$. Let $x, y \in G$ be arbitrary. We need to show $xy = yx$. Since $G/Z(G)$ is generated by $aZ(G)$, we can write:

- $xZ(G) = a^i Z(G)$ for some integer i, and $yZ(G) = a^j Z(G)$ for some integer j. So:
- $x = a^i z_1$ for some $z_1 \in Z(G)$, and $y = a^j z_2$ for some $z_2 \in Z(G)$.
- Now compute: $xy = (a^i z_1)(a^j z_2) = a^i (z_1 a^j) z_2 = a^i (a^j z_1) z_2 = a^{i+j} z_1 z_2$
- Similarly: $yx = (a^j z_2)(a^i z_1) = a^j (z_2 a^i) z_1 = a^j (a^i z_2) z_1 = a^{i+j} z_2 z_1 = a^{i+j} z_1 z_2$

Therefore, $xy = yx$. So G is Abelian. ∎

Remarks on Theorem 3

Remark 1: A Better Result: The theorem actually proves something stronger: If $G/Z(G)$ is cyclic, then $G/Z(G)$ must be trivial (i.e., $G = Z(G)$).

Proof: If G is Abelian (as we just proved), then $Z(G) = G$, so $G/Z(G) = \{Z(G)\}$ is the trivial group.

Remark 2: The Contrapositive: The contrapositive of Theorem 9 is often more useful: *If G is non-Abelian, then $G/Z(G)$ is not cyclic.* This gives us a tool for proving that certain factor groups are non-cyclic.

Remark 3: Trivial Consequence: As a special case: If $|G/Z(G)| = p$ (a prime), then $G/Z(G)$ is cyclic (by Lagrange), so G must be Abelian. But then $G = Z(G)$, contradicting $|G/Z(G)| = p > 1$. **So:** There is no group G with $|G/Z(G)| = p$ for any prime p.

Example 16: If G/H has an element of order n, then G has an element of order n.

Proof: Let $aH \in G/H$ have order n. Let $k = |a|$ (the order of a in G). Since $(aH)^k = a^k H = H$, so $n|k$. writing $k = mn$ we have $(a^m)^n = a^k = e$ and n is the smallest such positive integer. So our element is a^m.

Theorem 4: For any group G, $G/Z(G)$ is isomorphic to $\mathrm{Inn}(G)$.

Proof: Recall that $\mathrm{Inn}(G) = \{\phi_a : a \in G\}$ where $\phi_a(x) = axa^{-1}$ is the inner automorphism induced by a. Define $\psi : G/Z(G) \to \mathrm{Inn}(G)$ by $\psi(aZ(G)) = \phi_a$. We need to verify that ψ is a well-defined isomorphism.

1. Well-Defined: Suppose $aZ(G) = bZ(G)$. Then $b = az$ for some $z \in Z(G)$. For any $x \in G$: $\phi_b(x) = bxb^{-1} = (az)x(az)^{-1} = azxz^{-1}a^{-1} = axa^{-1} = \phi_a(x)$, (using that $z \in Z(G)$ commutes with x). Therefore, $\phi_b = \phi_a$, so ψ is well-defined.

2. Operation Preserving: $\psi((aZ(G))(bZ(G))) = \psi(abZ(G)) = \phi_{ab}$. Also: $\psi(aZ(G)) \circ \psi(bZ(G)) = \phi_a \circ \phi_b$. For any $x \in G$:
$(\phi_a \circ \phi_b)(x) = \phi_a(\phi_b(x)) = \phi_a(bxb^{-1}) = a(bxb^{-1})a^{-1} = (ab)x(ab)^{-1} = \phi_{ab}(x)$
Therefore, $\phi_a \circ \phi_b = \phi_{ab}$.

3. One-to-One: Suppose $\psi(aZ(G)) = \psi(bZ(G))$. Then $\phi_a = \phi_b$. This means $axa^{-1} = bxb^{-1}$ for all $x \in G$. Which gives $b^{-1}ax = xb^{-1}a$ for all $x \in G$. This means $b^{-1}a \in Z(G)$, so $a \in bZ(G)$, i.e., $aZ(G) = bZ(G)$.

4. Onto: Let $\phi_a \in \mathrm{Inn}(G)$ be arbitrary. Then $\psi(aZ(G)) = \phi_a$, so ψ is onto.

Example 17: Determining $\mathbf{Inn}(D_6)$

Example 17: Determine $\mathbf{Inn}(D_6)$ without computing all inner automorphisms directly.

Solution: We'll use Theorem 4: $\mathbf{Inn}(D_6) \cong D_6/Z(D_6)$.

Step 1: We know: $Z(D_6) = \{R_0, R_{180}\}$, so $|Z(D_6)| = 2$.

Step 2: Compute $|D_6/Z(D_6)|$. $|D_6/Z(D_6)| = \dfrac{|D_6|}{|Z(D_6)|} = \dfrac{12}{2} = 6$

Step 3: Determine which group of order 6. By the classification of groups of order 6, we have either $D_6/Z(D_6) \cong \mathbb{Z}_6$ or $D_6/Z(D_6) \cong D_3$. **Using Theorem 3:** If $D_6/Z(D_6) \cong \mathbb{Z}_6$, then $D_6/Z(D_6)$ is cyclic, so D_6 would be Abelian. But D_6 is not Abelian. So, $D_6/Z(D_6) \ncong \mathbb{Z}_6$.

Conclusion: $D_6/Z(D_6) \cong D_3$. By Theorem 4: $\mathbf{Inn}(D_6) \cong D_3$.

Theorem 9.5: Let G be a finite Abelian group and let p be a prime that divides the order of G. Then G has an element of order p.

Proof (by strong induction on $|G|$):

Base Case: If $|G| = 2$, then clearly the statement is true.

Inductive Step: Assume $|G| > 2$ and that the theorem holds for all Abelian groups of smaller order than G.

Case 1: G has an element a whose order is divisible by p. Say $|a| = pm$ for some positive integer m.

Then $|a^m| = \dfrac{|a|}{\gcd(|a|, m)} = \dfrac{pm}{\gcd(pm, m)} = \dfrac{pm}{m} = p$. So a^m is an element of order p, and we're done!

Case 2: Every nonidentity element of G has order not divisible by p. Pick any nonidentity element $a \in G$. Let $|a| = k$ where $p \nmid k$. Consider the factor group $G/\langle a \rangle$. Since $\langle a \rangle$ is a subgroup of G and G is Abelian, $\langle a \rangle \triangleleft G$.

Now, $|G/\langle a \rangle| = \dfrac{|G|}{|\langle a \rangle|} = \dfrac{|G|}{k}$. Since $p \mid |G|$ and $p \nmid k$, we have $p \mid \dfrac{|G|}{k}$. Also, $|G/\langle a \rangle| = \dfrac{|G|}{k} < |G|$ (since $k > 1$). By the **inductive hypothesis**, $G/\langle a \rangle$ has an element of order p. By example 16 so is G.

Motivation: Reversing the External Direct Product

Recall: Given groups G and H, we can form the **external direct product** $G \oplus H$.

- Elements: ordered pairs (g, h)
- Operation: $(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2)$

New Question: Can we go in reverse? Given a group G, can we find subgroups H and K such that G "looks like" $H \oplus K$?

Example: Starting from $\mathbb{Z}_2$ and $\mathbb{Z}_3$, we formed $\mathbb{Z}_2 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_6$. We can also write $\mathbb{Z}_6 = \langle 3 \rangle \times \langle 2 \rangle$ where $\langle 3 \rangle = \{0, 3\}$ and $\langle 2 \rangle = \{0, 2, 4\}$ are subgroups of $\mathbb{Z}_6$.

Goal: Formalize when a group G can be "decomposed" as a product of its subgroups. This is called an **internal direct product**.

Definition: Let H and K be subgroups of a group G. We say G is the **internal direct product** of H and K, written $G = H \times K$, if:

1. H and K are normal.
2. $G = HK = \{hk : h \in H, k \in K\}$ (every element can be written as a product)
3. $H \cap K = \{e\}$.

Example:

- $U(st) = U_s(st) \times U_t(st)$, where s and t be relatively prime positive integers. (Thm 8.3).
- $D_6 = \{R_0, R_{120}, R_{240}, F, R_{120}F, R_{240}F\} \times \{R_0, R_{180}\}$.
- $S_3 \neq \{(1), (123), (132)\} \times \{(1), (12)\}$.

Definition: Let $H_1, H_2, \ldots, H_n$ be subgroups of a group G. We say G is the **internal direct product** of $H_1, H_2, \ldots, H_n$, written: $G = H_1 \times H_2 \times \cdots \times H_n$, if:

1. $H_1, H_2, \cdots H_n$ are normal.
2. $G = H_1 H_2 \cdots H_n = \{h_1 h_2 \cdots h_n : h_i \in H_i\}$
3. $(H_1 H_2 \cdots H_i) \cap H_{i+1} = \{e\}$ for all $i = 1, 2, \ldots, n-1$

Note: Condition 3 is stronger than just requiring $H_i \cap H_j = \{e\}$ for $i \neq j$.

Theorem 6(Internal ≅ External): If $G = H_1 \times H_2 \times \cdots \times H_n$ (internal direct product), then: $G \cong H_1 \oplus H_2 \oplus \cdots \oplus H_n$.

Proof: First, we show **elements from different subgroups commute** with each other: For $h_i \in H_i$ and $h_j \in H_j$ with $i \neq j$, $h_i h_j = h_j h_i$ iff $e = h_i h_j h_i^{-1} h_j^{-1}$:

- By normality, $h_i(h_j h_i^{-1} h_j^{-1}) = (h_i h_j h_i^{-1}) h_j^{-1} \in H_i \cap H_j = \{e\}$. Therefore, $h_i h_j = h_j h_i$ for all $h_i \in H_i$ and $h_j \in H_j$.

Next, we prove each element of G has a **unique representation** as $h_1 h_2 \dots h_n$ with $h_i \in H_i$. Suppose $g = h_1 h_2 \dots h_n = h_1' h_2' \dots h_n'$ where $h_i, h_i' \in H_i$. Then:

- $h_1^{-1} h_1' = h_2 h_2'^{-1} h_3 h_3'^{-1} \dots h_n h_n'^{-1}$. The left side belongs to H_1, while the right side belongs to $H_2 H_3 \dots H_n$. Since $(H_1) \cap (H_2 H_3 \dots H_n) = \{e\}$ (by condition 3), we have $h_1 = h_1'$. Continuing, we get $h_i = h_i'$ for all i.

The map $\varphi : G \to H_1 \oplus H_2 \oplus \ldots \oplus H_n$ by: $\varphi(h_1 h_2 \ldots h_n) = (h_1, h_2, \ldots, h_n)$ is:

- **Well-defined** (by unique representation)
- **One-to-one** (by unique representation)
- **Onto** (by construction)
- **Operation-preserving** (using the commutativity of elements from different subgroups):
  $\varphi(g_1 g_2) = \varphi((h_1 \ldots h_n)(h_1' \ldots h_n')) = \varphi(h_1 h_1' \ldots h_n h_n') = (h_1 h_1', \ldots, h_n h_n') = (h_1, \ldots, h_n) \cdot (h_1', \ldots, h_n')$

Therefore, $G \cong H_1 \oplus H_2 \oplus \ldots \oplus H_n$.

Theorem 9.7: Every finite Abelian group G of square free order is cyclic.

Proof: Let $|G| = p_1 p_2 \cdots p_r$, where $p_1, p_2, \ldots, p_r$ are distinct primes. By **Cauchy's Theorem** (Theorem 9.5), for each p_i, there exists an element $a_i \in G$ with $|a_i| = p_i$:

- It follows from Thm 7.2 that $G = < a_1 > \times < a_2 > \times \ldots \times < a_r >$
- By Thm 9.6, $G \cong < a_1 > \oplus < a_2 > \oplus \ldots \oplus < a_r >$
- By Cor of Thm8.2 $G \cong \mathbb{Z}_{p_1 p_2 \cdots p_r}$

Theorem8: Every group of order p^2, where p is a prime, is isomorphic to either: $\mathbb{Z}_{p^2}$, or $\mathbb{Z}_p \oplus \mathbb{Z}_p$.

Proof: Let G be a group of order p^2, where p is prime. If G has an element of order p^2, then $G \cong \mathbb{Z}_{p^2}$ and we are done. Otherwise, by Corollary 2 of Lagrange's Theorem, every non-identity element a has order p. We first prove that the cyclic subgroup $\langle a \rangle$ is normal in G:

- Suppose $\langle a \rangle$ is not normal. Then there exists $b \in G$ such that $bab^{-1} \notin \langle a \rangle$. So $\langle a \rangle \neq \langle bab^{-1} \rangle$ and $\langle a \rangle \cap \langle bab^{-1} \rangle = \{e\}$.
- The distinct left cosets of $\langle bab^{-1} \rangle$: $\langle bab^{-1} \rangle, a\langle bab^{-1} \rangle, a^2\langle bab^{-1} \rangle, \ldots, a^{p-1}\langle bab^{-1} \rangle$.
- Since b^{-1} belongs to one of these cosets, we have $b^{-1} = a^i(bab^{-1})^j = a^i b a^j b^{-1}$ for some i, j. Cancelling b^{-1} we get $e = a^i b a^j$. So $b = a^{-i-j} \in \langle a \rangle$. But then $b\langle a \rangle b^{-1} = \langle a \rangle$, contradicting our assumption.

Therefore, $\langle a \rangle$ is normal in G for any $a \in G$.

Now, let x be any non-identity element in G and $y \in G$ not in $\langle x \rangle$. Claim $G = \langle x \rangle \times \langle y \rangle$:

- Both $\langle x \rangle$ and $\langle y \rangle$ are normal in G (as we just proved)
- $|\langle x \rangle| = |\langle y \rangle| = p$ (as all non-identity elements have order p)
- $\langle x \rangle \cap \langle y \rangle = \{e\}$ (since both have prime order)
- $|\langle x \rangle \langle y \rangle| = |\langle x \rangle||\langle y \rangle|/|\langle x \rangle \cap \langle y \rangle| = p \cdot p = p^2 = |G|$

Therefore, $G = \langle x \rangle \times \langle y \rangle$ is an internal direct product. By Theorem 9.6, $G \cong \langle x \rangle \oplus \langle y \rangle \cong \mathbb{Z}_p \oplus \mathbb{Z}_p$.

Exercise:

True or False?

Every group of order p^2, where p is a prime, is Abelian.

Corollary: Every group of order p^2, where p is a prime, is Abelian.

Proof: Every group of order p^2 is isomorphic to either $\mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \oplus \mathbb{Z}_p$. Both $\mathbb{Z}_{p^2}$ and $\mathbb{Z}_p \oplus \mathbb{Z}_p$ are Abelian groups. Therefore, every group of order p^2 is Abelian