§3.8 Cosets, Normal Subgroups, and Factor Groups

Shaoyun Yi

MATH 546/701I

University of South Carolina

June 15-17, 2020

Review

- $\phi : G_1 \to G_2$ is a **group homomorphism** if $\phi(a * b) = \phi(a) \cdot \phi(b)$.

Review

- $\phi : G_1 \to G_2$ is a **group homomorphism** if $\phi(a * b) = \phi(a) \cdot \phi(b)$.
- Every isomorphism is a homomorphism, but conversely not true.

Review

- $\phi : G_1 \to G_2$ is a **group homomorphism** if $\phi(a * b) = \phi(a) \cdot \phi(b)$.
- Every isomorphism is a homomorphism, but conversely not true.
- $\phi(a^n) = (\phi(a))^n$ for all $a \in G_1$ and all $n \in \mathbf{Z}$: $n = 0$ vs. $n = -1$

Review

- $\phi : G_1 \to G_2$ is a **group homomorphism** if $\phi(a * b) = \phi(a) \cdot \phi(b)$.
- Every isomorphism is a homomorphism, but conversely not true.
- $\phi(a^n) = (\phi(a))^n$ for all $a \in G_1$ and all $n \in \mathbf{Z}$: $n = 0$ vs. $n = -1$
- If $o(a) = n$ in G_1, then $o(\phi(a))$ in G_2 is a divisor of n.

Review

- $\phi : G_1 \to G_2$ is a **group homomorphism** if $\phi(a * b) = \phi(a) \cdot \phi(b)$.
- Every isomorphism is a homomorphism, but conversely not true.
- $\phi(a^n) = (\phi(a))^n$ for all $a \in G_1$ and all $n \in \mathbf{Z}$: $n = 0$ vs. $n = -1$
- If $o(a) = n$ in G_1, then $o(\phi(a))$ in G_2 is a divisor of n.
- ϕ is onto: If G_1 is abelian (cyclic), then G_2 is also abelian (cyclic).

Review

- $\phi : G_1 \to G_2$ is a **group homomorphism** if $\phi(a * b) = \phi(a) \cdot \phi(b)$.
- Every isomorphism is a homomorphism, but conversely not true.
- $\phi(a^n) = (\phi(a))^n$ for all $a \in G_1$ and all $n \in \mathbf{Z}$: $n = 0$ vs. $n = -1$
- If $o(a) = n$ in G_1, then $o(\phi(a))$ in G_2 is a divisor of n.
- ϕ is onto: If G_1 is abelian (cyclic), then G_2 is also abelian (cyclic).
- If $G_1 = \langle a \rangle$ is cyclic, then ϕ is completely determined by $\phi(a)$.

Review

- $\phi : G_1 \to G_2$ is a **group homomorphism** if $\phi(a * b) = \phi(a) \cdot \phi(b)$.
- Every isomorphism is a homomorphism, but conversely not true.
- $\phi(a^n) = (\phi(a))^n$ for all $a \in G_1$ and all $n \in \mathbf{Z}$: $n = 0$ vs. $n = -1$
- If $o(a) = n$ in G_1, then $o(\phi(a))$ in G_2 is a divisor of n.
- ϕ is onto: If G_1 is abelian (cyclic), then G_2 is also abelian (cyclic).
- If $G_1 = \langle a \rangle$ is cyclic, then ϕ is completely determined by $\phi(a)$.
- $\ker(\phi) = \{x \in G_1 \mid \phi(x) = e_2\} \subseteq G_1$ & $\mathrm{im}(\phi) = \{\phi(x) \mid x \in G_1\} \subseteq G_2$

Review

- $\phi : G_1 \to G_2$ is a **group homomorphism** if $\phi(a * b) = \phi(a) \cdot \phi(b)$.
- Every isomorphism is a homomorphism, but conversely not true.
- $\phi(a^n) = (\phi(a))^n$ for all $a \in G_1$ and all $n \in \mathbf{Z}$: $n = 0$ vs. $n = -1$
- If $o(a) = n$ in G_1, then $o(\phi(a))$ in G_2 is a divisor of n.
- ϕ is onto: If G_1 is abelian (cyclic), then G_2 is also abelian (cyclic).
- If $G_1 = \langle a \rangle$ is cyclic, then ϕ is completely determined by $\phi(a)$.
- $\ker(\phi) = \{x \in G_1 \mid \phi(x) = e_2\} \subseteq G_1$ & $\mathrm{im}(\phi) = \{\phi(x) \mid x \in G_1\} \subseteq G_2$
- ϕ is one-to-one $\Leftrightarrow \ker(\phi) = \{e_1\}$ & ϕ is onto $\Leftrightarrow \mathrm{im}(\phi) = G_2$

Review

- $\phi : G_1 \to G_2$ is a **group homomorphism** if $\phi(a * b) = \phi(a) \cdot \phi(b)$.
- Every isomorphism is a homomorphism, but conversely not true.
- $\phi(a^n) = (\phi(a))^n$ for all $a \in G_1$ and all $n \in \mathbf{Z}$: $n = 0$ vs. $n = -1$
- If $o(a) = n$ in G_1, then $o(\phi(a))$ in G_2 is a divisor of n.
- ϕ is onto: If G_1 is abelian (cyclic), then G_2 is also abelian (cyclic).
- If $G_1 = \langle a \rangle$ is cyclic, then ϕ is completely determined by $\phi(a)$.
- $\ker(\phi) = \{x \in G_1 \mid \phi(x) = e_2\} \subseteq G_1$ & $\mathrm{im}(\phi) = \{\phi(x) \mid x \in G_1\} \subseteq G_2$
- ϕ is one-to-one $\Leftrightarrow \ker(\phi) = \{e_1\}$ & ϕ is onto $\Leftrightarrow \mathrm{im}(\phi) = G_2$
- Homorphisms between cyclic groups: Understand **Four** cases

Review

- $\phi : G_1 \to G_2$ is a **group homomorphism** if $\phi(a * b) = \phi(a) \cdot \phi(b)$.
- Every isomorphism is a homomorphism, but conversely not true.
- $\phi(a^n) = (\phi(a))^n$ for all $a \in G_1$ and all $n \in \mathbf{Z}$: $n = 0$ vs. $n = -1$
- If $o(a) = n$ in G_1, then $o(\phi(a))$ in G_2 is a divisor of n.
- ϕ is onto: If G_1 is abelian (cyclic), then G_2 is also abelian (cyclic).
- If $G_1 = \langle a \rangle$ is cyclic, then ϕ is completely determined by $\phi(a)$.
- $\ker(\phi) = \{x \in G_1 \mid \phi(x) = e_2\} \subseteq G_1$ & $\mathrm{im}(\phi) = \{\phi(x) \mid x \in G_1\} \subseteq G_2$
- ϕ is one-to-one $\Leftrightarrow \ker(\phi) = \{e_1\}$ & ϕ is onto $\Leftrightarrow \mathrm{im}(\phi) = G_2$
- Homorphisms between cyclic groups: Understand **Four** cases
- **Normal subgroup** H of G: If $ghg^{-1} \in H$ for all $h \in H$ and $g \in G$.
  (a) If H_1 is a subgroup of G_1, then $\phi(H_1)$ is a subgroup of G_2.
  If ϕ is onto and H_1 is normal in G_1, then $\phi(H_1)$ is normal in G_2.
  (b) If H_2 is a subgroup of G_2, then $\phi^{-1}(H_2)$ is a subgroup of G_1.
  If H_2 is a normal in G_2, then $\phi^{-1}(H_2)$ is normal in G_1.

Review

- $\phi : G_1 \to G_2$ is a **group homomorphism** if $\phi(a * b) = \phi(a) \cdot \phi(b)$.
- Every isomorphism is a homomorphism, but conversely not true.
- $\phi(a^n) = (\phi(a))^n$ for all $a \in G_1$ and all $n \in \mathbf{Z}$: $n = 0$ vs. $n = -1$
- If $o(a) = n$ in G_1, then $o(\phi(a))$ in G_2 is a divisor of n.
- ϕ is onto: If G_1 is abelian (cyclic), then G_2 is also abelian (cyclic).
- If $G_1 = \langle a \rangle$ is cyclic, then ϕ is completely determined by $\phi(a)$.
- $\ker(\phi) = \{x \in G_1 \mid \phi(x) = e_2\} \subseteq G_1$ & $\mathrm{im}(\phi) = \{\phi(x) \mid x \in G_1\} \subseteq G_2$
- ϕ is one-to-one $\Leftrightarrow \ker(\phi) = \{e_1\}$ & ϕ is onto $\Leftrightarrow \mathrm{im}(\phi) = G_2$
- Homorphisms between cyclic groups: Understand **Four** cases
- **Normal subgroup** H of G: If $ghg^{-1} \in H$ for all $h \in H$ and $g \in G$.
  (a) If H_1 is a subgroup of G_1, then $\phi(H_1)$ is a subgroup of G_2.
  If ϕ is onto and H_1 is normal in G_1, then $\phi(H_1)$ is normal in G_2.
  (b) If H_2 is a subgroup of G_2, then $\phi^{-1}(H_2)$ is a subgroup of G_1.
  If H_2 is a normal in G_2, then $\phi^{-1}(H_2)$ is normal in G_1.
- **An extremely important theorem:** $G_1/\ker(\phi) \cong \phi(G_1) = \mathrm{im}(\phi)$.

Review

- $\phi : G_1 \to G_2$ is a **group homomorphism** if $\phi(a * b) = \phi(a) \cdot \phi(b)$.
- Every isomorphism is a homomorphism, but conversely not true.
- $\phi(a^n) = (\phi(a))^n$ for all $a \in G_1$ and all $n \in \mathbf{Z}$: $n = 0$ vs. $n = -1$
- If $o(a) = n$ in G_1, then $o(\phi(a))$ in G_2 is a divisor of n.
- ϕ is onto: If G_1 is abelian (cyclic), then G_2 is also abelian (cyclic).
- If $G_1 = \langle a \rangle$ is cyclic, then ϕ is completely determined by $\phi(a)$.
- $\ker(\phi) = \{x \in G_1 \mid \phi(x) = e_2\} \subseteq G_1$ & $\mathrm{im}(\phi) = \{\phi(x) \mid x \in G_1\} \subseteq G_2$
- ϕ is one-to-one $\Leftrightarrow \ker(\phi) = \{e_1\}$ & ϕ is onto $\Leftrightarrow \mathrm{im}(\phi) = G_2$
- Homorphisms between cyclic groups: Understand **Four** cases
- **Normal subgroup** H of G: If $ghg^{-1} \in H$ for all $h \in H$ and $g \in G$.
  - (a) If H_1 is a subgroup of G_1, then $\phi(H_1)$ is a subgroup of G_2.
    If ϕ is onto and H_1 is normal in G_1, then $\phi(H_1)$ is normal in G_2.
  - (b) If H_2 is a subgroup of G_2, then $\phi^{-1}(H_2)$ is a subgroup of G_1.
    If H_2 is a normal in G_2, then $\phi^{-1}(H_2)$ is normal in G_1.
- **An extremely important theorem:** $G_1/\ker(\phi) \cong \phi(G_1) = \mathrm{im}(\phi)$.
  - (1) *Reprove* "Every cyclic group G is isomorphic to either $\mathbf{Z}$ or $\mathbf{Z}_n$".

Review

- $\phi : G_1 \to G_2$ is a **group homomorphism** if $\phi(a * b) = \phi(a) \cdot \phi(b)$.
- Every isomorphism is a homomorphism, but conversely not true.
- $\phi(a^n) = (\phi(a))^n$ for all $a \in G_1$ and all $n \in \mathbf{Z}$: $n = 0$ vs. $n = -1$
- If $o(a) = n$ in G_1, then $o(\phi(a))$ in G_2 is a divisor of n.
- ϕ is onto: If G_1 is abelian (cyclic), then G_2 is also abelian (cyclic).
- If $G_1 = \langle a \rangle$ is cyclic, then ϕ is completely determined by $\phi(a)$.
- $\ker(\phi) = \{x \in G_1 \mid \phi(x) = e_2\} \subseteq G_1$ & $\mathrm{im}(\phi) = \{\phi(x) \mid x \in G_1\} \subseteq G_2$
- ϕ is one-to-one $\Leftrightarrow \ker(\phi) = \{e_1\}$ & ϕ is onto $\Leftrightarrow \mathrm{im}(\phi) = G_2$
- Homorphisms between cyclic groups: Understand **Four** cases
- **Normal subgroup** H of G: If $ghg^{-1} \in H$ for all $h \in H$ and $g \in G$.
  (a) If H_1 is a subgroup of G_1, then $\phi(H_1)$ is a subgroup of G_2.
  If ϕ is onto and H_1 is normal in G_1, then $\phi(H_1)$ is normal in G_2.
  (b) If H_2 is a subgroup of G_2, then $\phi^{-1}(H_2)$ is a subgroup of G_1.
  If H_2 is a normal in G_2, then $\phi^{-1}(H_2)$ is normal in G_1.
- **An extremely important theorem:** $G_1/\ker(\phi) \cong \phi(G_1) = \mathrm{im}(\phi)$.
  (1) *Reprove* "Every cyclic group G is isomorphic to either $\mathbf{Z}$ or $\mathbf{Z}_n$".
  (2) *Reprove* "Cayley's Theorem: Every group $G \cong$ a permutation group".

Motivation: Examples

Example 1

Motivation: Examples

Example 1

$\mathbf{Z}_2 = \{[0]_2, [1]_2\}$ are the sets of even and odd integers.

Motivation: Examples

Example 1

$\mathbf{Z}_2 = \{[0]_2, [1]_2\}$ are the sets of even and odd integers.
The set of even integers $= 0 + 2\mathbf{Z}$. &

Motivation: Examples

Example 1

$\mathbf{Z}_2 = \{[0]_2, [1]_2\}$ are the sets of even and odd integers.
The set of even integers $= 0 + 2\mathbf{Z}$. & The set of odd integers $= 1 + 2\mathbf{Z}$.
More generally,

Motivation: Examples

Example 1

$\mathbf{Z}_2 = \{[0]_2, [1]_2\}$ are the sets of even and odd integers.
The set of even integers $= 0 + 2\mathbf{Z}$. & The set of odd integers $= 1 + 2\mathbf{Z}$.
More generally, in $\mathbf{Z}_n$, for any integer k we can write $[k]_n = k + n\mathbf{Z}$.

Example 2 (Let $\phi : G_1 \to G_2$ be a group homomorphism and $a \in G_1$.)

Motivation: Examples

Example 1

$\mathbf{Z}_2 = \{[0]_2, [1]_2\}$ are the sets of even and odd integers.
The set of even integers $= 0 + 2\mathbf{Z}$. & The set of odd integers $= 1 + 2\mathbf{Z}$.
More generally, in $\mathbf{Z}_n$, for any integer k we can write $[k]_n = k + n\mathbf{Z}$.

Example 2 (Let $\phi : G_1 \to G_2$ be a group homomorphism and $a \in G_1$.)

For $b \in G_1$, we have $\phi(b) = \phi(a) \Leftrightarrow b = ak$ for some $k \in \ker(\phi)$. (Why?)
(

Motivation: Examples

Example 1

$\mathbf{Z}_2 = \{[0]_2, [1]_2\}$ are the sets of even and odd integers.
The set of even integers $= 0 + 2\mathbf{Z}$. & The set of odd integers $= 1 + 2\mathbf{Z}$.
More generally, in $\mathbf{Z}_n$, for any integer k we can write $[k]_n = k + n\mathbf{Z}$.

Example 2 (Let $\phi : G_1 \to G_2$ be a group homomorphism and $a \in G_1$.)

For $b \in G_1$, we have $\phi(b) = \phi(a) \Leftrightarrow b = ak$ for some $k \in \ker(\phi)$. (Why?) (Proposition 9 in §3.7) Write $b \in aK = \{ak \mid k \in K\}$, where $K = \ker(\phi)$.

Motivation: Examples

Example 1

$\mathbf{Z}_2 = \{[0]_2, [1]_2\}$ are the sets of even and odd integers.
The set of even integers $= 0 + 2\mathbf{Z}$. & The set of odd integers $= 1 + 2\mathbf{Z}$.
More generally, in $\mathbf{Z}_n$, for any integer k we can write $[k]_n = k + n\mathbf{Z}$.

Example 2 (Let $\phi : G_1 \to G_2$ be a group homomorphism and $a \in G_1$.)

For $b \in G_1$, we have $\phi(b) = \phi(a) \Leftrightarrow b = ak$ for some $k \in \ker(\phi)$. (Why?) (Proposition 9 in §3.7) Write $b \in aK = \{ak \mid k \in K\}$, where $K = \ker(\phi)$.
Define $a \sim_\phi b$ if $\phi(a) = \phi(b)$. Then the equivalence class $[a]_\phi = aK$.

Motivation: Examples

Example 1

$\mathbf{Z}_2 = \{[0]_2, [1]_2\}$ are the sets of even and odd integers.
The set of even integers $= 0 + 2\mathbf{Z}$. & The set of odd integers $= 1 + 2\mathbf{Z}$.
More generally, in $\mathbf{Z}_n$, for any integer k we can write $[k]_n = k + n\mathbf{Z}$.

Example 2 (Let $\phi : G_1 \to G_2$ be a group homomorphism and $a \in G_1$.)

For $b \in G_1$, we have $\phi(b) = \phi(a) \Leftrightarrow b = ak$ for some $k \in \ker(\phi)$. (Why?) (Proposition 9 in §3.7) Write $b \in aK = \{ak \mid k \in K\}$, where $K = \ker(\phi)$.
Define $a \sim_\phi b$ if $\phi(a) = \phi(b)$. Then the equivalence class $[a]_\phi = aK$.
Proposition 9 in §3.7 also shows that $aK = Ka$.

Example 3 (Lemma 19 in §3.2: Let H be a subgroup of the group G.)

Motivation: Examples

Example 1

$\mathbf{Z}_2 = \{[0]_2, [1]_2\}$ are the sets of even and odd integers.
The set of even integers $= 0 + 2\mathbf{Z}$. & The set of odd integers $= 1 + 2\mathbf{Z}$.
More generally, in $\mathbf{Z}_n$, for any integer k we can write $[k]_n = k + n\mathbf{Z}$.

Example 2 (Let $\phi : G_1 \to G_2$ be a group homomorphism and $a \in G_1$.)

For $b \in G_1$, we have $\phi(b) = \phi(a) \Leftrightarrow b = ak$ for some $k \in \ker(\phi)$. (Why?) (Proposition 9 in §3.7) Write $b \in aK = \{ak \mid k \in K\}$, where $K = \ker(\phi)$.
Define $a \sim_\phi b$ if $\phi(a) = \phi(b)$. Then the equivalence class $[a]_\phi = aK$.
Proposition 9 in §3.7 also shows that $aK = Ka$.

Example 3 (Lemma 19 in §3.2: Let H be a subgroup of the group G.)

For $a, b \in G$ define $a \sim b$ if $ab^{-1} \in H$. Then $\sim$ is an equivalence relation.

Motivation: Examples

Example 1

$\mathbf{Z}_2 = \{[0]_2, [1]_2\}$ are the sets of even and odd integers.
The set of even integers $= 0 + 2\mathbf{Z}$. & The set of odd integers $= 1 + 2\mathbf{Z}$.
More generally, in $\mathbf{Z}_n$, for any integer k we can write $[k]_n = k + n\mathbf{Z}$.

Example 2 (Let $\phi : G_1 \to G_2$ be a group homomorphism and $a \in G_1$.)

For $b \in G_1$, we have $\phi(b) = \phi(a) \Leftrightarrow b = ak$ for some $k \in \ker(\phi)$. (Why?) (Proposition 9 in §3.7) Write $b \in aK = \{ak \mid k \in K\}$, where $K = \ker(\phi)$.
Define $a \sim_\phi b$ if $\phi(a) = \phi(b)$. Then the equivalence class $[a]_\phi = aK$.
Proposition 9 in §3.7 also shows that $aK = Ka$.

Example 3 (Lemma 19 in §3.2: Let H be a subgroup of the group G.)

For $a, b \in G$ define $a \sim b$ if $ab^{-1} \in H$. Then $\sim$ is an equivalence relation.
Then the congruence class $[a] = Ha$. (Why?) [

Motivation: Examples

Example 1

$\mathbf{Z}_2 = \{[0]_2, [1]_2\}$ are the sets of even and odd integers.
The set of even integers $= 0 + 2\mathbf{Z}$. & The set of odd integers $= 1 + 2\mathbf{Z}$.
More generally, in $\mathbf{Z}_n$, for any integer k we can write $[k]_n = k + n\mathbf{Z}$.

Example 2 (Let $\phi : G_1 \to G_2$ be a group homomorphism and $a \in G_1$.)

For $b \in G_1$, we have $\phi(b) = \phi(a) \Leftrightarrow b = ak$ for some $k \in \ker(\phi)$. (Why?) (Proposition 9 in §3.7) Write $b \in aK = \{ak \mid k \in K\}$, where $K = \ker(\phi)$.
Define $a \sim_\phi b$ if $\phi(a) = \phi(b)$. Then the equivalence class $[a]_\phi = aK$.
Proposition 9 in §3.7 also shows that $aK = Ka$.

Example 3 (Lemma 19 in §3.2: Let H be a subgroup of the group G.)

For $a, b \in G$ define $a \sim b$ if $ab^{-1} \in H$. Then $\sim$ is an equivalence relation.
Then the congruence class $[a] = Ha$. (Why?) $[a \sim b \Rightarrow b = ha$ for $h \in H]$

Another equivalence relation

Let G be a group and let H be a subgroup of G. Define the relation

$$a \sim b \text{ if } a^{-1}b \in H, \text{ for } a, b \in G.$$

Claim: This defines an equivalence relation.

Another equivalence relation

Let G be a group and let H be a subgroup of G. Define the relation

$$a \sim b \text{ if } a^{-1}b \in H, \text{ for } a, b \in G.$$

Claim: This defines an equivalence relation.

(i) Reflexive: $a \sim a$ since $a^{-1}a \in H$;

Another equivalence relation

Let G be a group and let H be a subgroup of G. Define the relation

$$a \sim b \text{ if } a^{-1}b \in H, \text{ for } a, b \in G.$$

Claim: This defines an equivalence relation.

(i) Reflexive: $a \sim a$ since $a^{-1}a \in H$;

(ii) Symmetric: If $a \sim b$, then $a^{-1}b \in H$. $\Rightarrow b^{-1}a = (a^{-1}b)^{-1} \in H$.

Another equivalence relation

Let G be a group and let H be a subgroup of G. Define the relation

$$a \sim b \text{ if } a^{-1}b \in H, \text{ for } a, b \in G.$$

Claim: This defines an equivalence relation.

(i) Reflexive: $a \sim a$ since $a^{-1}a \in H$;

(ii) Symmetric: If $a \sim b$, then $a^{-1}b \in H$. $\Rightarrow b^{-1}a = (a^{-1}b)^{-1} \in H$.

(iii) Transitive: If $a \sim b$ and $b \sim c$, then $a^{-1}b \in H$ and $b^{-1}c \in H$. Thus,

$$a^{-1}c = (a^{-1}b)(b^{-1}c) \in H. \text{ (Why?)}$$

Thus, we prove the claim. $\square$

As a consequence,

Another equivalence relation

Let G be a group and let H be a subgroup of G. Define the relation

$$a \sim b \text{ if } a^{-1}b \in H, \text{ for } a, b \in G.$$

Claim: This defines an equivalence relation.

(i) Reflexive: $a \sim a$ since $a^{-1}a \in H$;

(ii) Symmetric: If $a \sim b$, then $a^{-1}b \in H$. $\Rightarrow b^{-1}a = (a^{-1}b)^{-1} \in H$.

(iii) Transitive: If $a \sim b$ and $b \sim c$, then $a^{-1}b \in H$ and $b^{-1}c \in H$. Thus,

$$a^{-1}c = (a^{-1}b)(b^{-1}c) \in H. \text{ (Why?)}$$

Thus, we prove the claim. $\square$

As a consequence, the congruence class $[a] = aH$ in this case.

Note 1

Another equivalence relation

Let G be a group and let H be a subgroup of G. Define the relation

$$a \sim b \text{ if } a^{-1}b \in H, \text{ for } a, b \in G.$$

Claim: This defines an equivalence relation.

(i) Reflexive: $a \sim a$ since $a^{-1}a \in H$;

(ii) Symmetric: If $a \sim b$, then $a^{-1}b \in H$. $\Rightarrow b^{-1}a = (a^{-1}b)^{-1} \in H$.

(iii) Transitive: If $a \sim b$ and $b \sim c$, then $a^{-1}b \in H$ and $b^{-1}c \in H$. Thus,

$$a^{-1}c = (a^{-1}b)(b^{-1}c) \in H. \text{ (Why?)}$$

Thus, we prove the claim. □

As a consequence, the congruence class $[a] = aH$ in this case.

Note 1

It is possible that $aH \neq Ha$. (When?) [Will see an example soon.]

First proposition: $[a] = aH$, where $a \sim b$ if $a^{-1}b \in H$

Proposition 1 (Let H be a subgroup of the group G, and let $a, b \in G$.)

Then the following conditions are equivalent:

First proposition: $[a] = aH$, where $a \sim b$ if $a^{-1}b \in H$

Proposition 1 (Let H be a subgroup of the group G, and let $a, b \in G$.)

Then the following conditions are equivalent:

(1) $bH = aH$;

(2) $bH \subseteq aH$;

(3) $b \in aH$;

(4) $a^{-1}b \in H$.

(1) $\Rightarrow$ (2):

First proposition: $[a] = aH$, where $a \sim b$ if $a^{-1}b \in H$

Proposition 1 (Let H be a subgroup of the group G, and let $a, b \in G$.)

Then the following conditions are equivalent:

(1) $bH = aH$;

(2) $bH \subseteq aH$;

(3) $b \in aH$;

(4) $a^{-1}b \in H$.

(1) $\Rightarrow$ (2): Trivial (2) $\Rightarrow$ (3):

First proposition: $[a] = aH$, where $a \sim b$ if $a^{-1}b \in H$

Proposition 1 (Let H be a subgroup of the group G, and let $a, b \in G$.)

Then the following conditions are equivalent:

(1) $bH = aH$;

(2) $bH \subseteq aH$;

(3) $b \in aH$;

(4) $a^{-1}b \in H$.

(1) $\Rightarrow$ (2): Trivial (2) $\Rightarrow$ (3): $b = be \in bH$ (3) $\Rightarrow$ (4):

Proposition 1 (Let H be a subgroup of the group G, and let $a, b \in G$.)

Then the following conditions are equivalent:

(1) $bH = aH$;

(2) $bH \subseteq aH$;

(3) $b \in aH$;

(4) $a^{-1}b \in H$.

(1) $\Rightarrow$ (2): Trivial (2) $\Rightarrow$ (3): $b = be \in bH$ (3) $\Rightarrow$ (4): $b = ah \Rightarrow a^{-1}b = h \in H$
(4) $\Rightarrow$ (1):

First proposition: $[a] = aH$, where $a \sim b$ if $a^{-1}b \in H$

Proposition 1 (Let H be a subgroup of the group G, and let $a, b \in G$.)

Then the following conditions are equivalent:

(1) $bH = aH$;

(2) $bH \subseteq aH$;

(3) $b \in aH$;

(4) $a^{-1}b \in H$.

(1) $\Rightarrow$ (2): Trivial (2) $\Rightarrow$ (3): $b = be \in bH$ (3) $\Rightarrow$ (4): $b = ah \Rightarrow a^{-1}b = h \in H$
(4) $\Rightarrow$ (1): Write $a^{-1}b = h$ for some $h \in H$, then $b = ah$ and $a = bh^{-1}$.
$bH \subseteq aH$:

First proposition: $[a] = aH$, where $a \sim b$ if $a^{-1}b \in H$

Proposition 1 (Let H be a subgroup of the group G, and let $a, b \in G$.)

Then the following conditions are equivalent:

(1) $bH = aH$;

(2) $bH \subseteq aH$;

(3) $b \in aH$;

(4) $a^{-1}b \in H$.

(1) $\Rightarrow$ (2): Trivial (2) $\Rightarrow$ (3): $b = be \in bH$ (3) $\Rightarrow$ (4): $b = ah \Rightarrow a^{-1}b = h \in H$

(4) $\Rightarrow$ (1): Write $a^{-1}b = h$ for some $h \in H$, then $b = ah$ and $a = bh^{-1}$.

$bH \subseteq aH$: For any $x = bh' \in bH$, we have $x = ahh' \in aH$.(Why?)

$aH \subseteq bH$:

First proposition: $[a] = aH$, where $a \sim b$ if $a^{-1}b \in H$

Proposition 1 (Let H be a subgroup of the group G, and let $a, b \in G$.)

Then the following conditions are equivalent:

(1) $bH = aH$;

(2) $bH \subseteq aH$;

(3) $b \in aH$;

(4) $a^{-1}b \in H$.

(1) $\Rightarrow$ (2): Trivial (2) $\Rightarrow$ (3): $b = be \in bH$ (3) $\Rightarrow$ (4): $b = ah \Rightarrow a^{-1}b = h \in H$
(4) $\Rightarrow$ (1): Write $a^{-1}b = h$ for some $h \in H$, then $b = ah$ and $a = bh^{-1}$.
$bH \subseteq aH$: For any $x = bh' \in bH$, we have $x = ahh' \in aH$.(Why?)
$aH \subseteq bH$: For any $y = ah'' \in bH$, we have $y = bh^{-1}h'' \in bH$.(Why?) $\square$

Corollary 4 (Let H be a subgroup of the group G, and let $a, b \in G$.)

First proposition: $[a] = aH$, where $a \sim b$ if $a^{-1}b \in H$

Proposition 1 (Let H be a subgroup of the group G, and let $a, b \in G$.)

Then the following conditions are equivalent:

(1) $bH = aH$;

(2) $bH \subseteq aH$;

(3) $b \in aH$;

(4) $a^{-1}b \in H$.

(1) $\Rightarrow$ (2): Trivial (2) $\Rightarrow$ (3): $b = be \in bH$ (3) $\Rightarrow$ (4): $b = ah \Rightarrow a^{-1}b = h \in H$
(4) $\Rightarrow$ (1): Write $a^{-1}b = h$ for some $h \in H$, then $b = ah$ and $a = bh^{-1}$.
$bH \subseteq aH$: For any $x = bh' \in bH$, we have $x = ahh' \in aH$.(Why?)
$aH \subseteq bH$: For any $y = ah'' \in bH$, we have $y = bh^{-1}h'' \in bH$.(Why?) $\square$

Corollary 4 (Let H be a subgroup of the group G, and let $a, b \in G$.)

Define $a \sim b$ if $aH = bH$. Then $\sim$ is an equivalence relation on G.

First proposition: $[a] = aH$, where $a \sim b$ if $a^{-1}b \in H$

Proposition 1 (Let H be a subgroup of the group G, and let $a, b \in G$.)

Then the following conditions are equivalent:

(1) $bH = aH$;

(2) $bH \subseteq aH$;

(3) $b \in aH$;

(4) $a^{-1}b \in H$.

(1) $\Rightarrow$ (2): Trivial (2) $\Rightarrow$ (3): $b = be \in bH$ (3) $\Rightarrow$ (4): $b = ah \Rightarrow a^{-1}b = h \in H$
(4) $\Rightarrow$ (1): Write $a^{-1}b = h$ for some $h \in H$, then $b = ah$ and $a = bh^{-1}$.
$bH \subseteq aH$: For any $x = bh' \in bH$, we have $x = ahh' \in aH$.(Why?)
$aH \subseteq bH$: For any $y = ah'' \in bH$, we have $y = bh^{-1}h'' \in bH$.(Why?) $\square$

Corollary 4 (Let H be a subgroup of the group G, and let $a, b \in G$.)

Define $a \sim b$ if $aH = bH$. Then $\sim$ is an equivalence relation on G.

It follows from Lemma 19 in §3.2 (see Example 3) and Proposition 1. $\square$

Definition of Cosets

Note 2

Note 2

In Proposition 1, $bH = aH$ shows that the roles of a and b can be reversed.

Definition of Cosets

Note 2

In Proposition 1, $bH = aH$ shows that the roles of a and b can be reversed. Thus $a^{-1}b \in H$ if and only if $b^{-1}a \in H$.

Definition of Cosets

Note 2

In Proposition 1, $bH = aH$ shows that the roles of a and b can be reversed. Thus $a^{-1}b \in H$ if and only if $b^{-1}a \in H$. We know that the equivalence classes must partition G, and so

Definition of Cosets

Note 2

In Proposition 1, $bH = aH$ shows that the roles of a and b can be reversed. Thus $a^{-1}b \in H$ if and only if $b^{-1}a \in H$. We know that the equivalence classes must partition G, and so if $aH \cap bH \neq \emptyset$, then $aH = bH$.

Definition 5 (Let H be a subgroup of the group G, and let $a \in G$.)

Definition of Cosets

Note 2

In Proposition 1, $bH = aH$ shows that the roles of a and b can be reversed. Thus $a^{-1}b \in H$ if and only if $b^{-1}a \in H$. We know that the equivalence classes must partition G, and so if $aH \cap bH \neq \emptyset$, then $aH = bH$.

Definition 5 (Let H be a subgroup of the group G, and let $a \in G$.)

The **left coset** of H in G determined by a is the set

$$aH = \{x \in G \mid x = ah \text{ for some } h \in H\}.$$

Definition of Cosets

Note 2

In Proposition 1, $bH = aH$ shows that the roles of a and b can be reversed. Thus $a^{-1}b \in H$ if and only if $b^{-1}a \in H$. We know that the equivalence classes must partition G, and so if $aH \cap bH \neq \emptyset$, then $aH = bH$.

Definition 5 (Let H be a subgroup of the group G, and let $a \in G$.)

The **left coset** of H in G determined by a is the set

$$aH = \{x \in G \mid x = ah \text{ for some } h \in H\}.$$

The **right coset** of H in G determined by a is the set

$$Ha = \{x \in G \mid x = ha \text{ for some } h \in H\}.$$

Definition of Cosets

Note 2

In Proposition 1, $bH = aH$ shows that the roles of a and b can be reversed. Thus $a^{-1}b \in H$ if and only if $b^{-1}a \in H$. We know that the equivalence classes must partition G, and so if $aH \cap bH \neq \emptyset$, then $aH = bH$.

Definition 5 (Let H be a subgroup of the group G, and let $a \in G$.)

The **left coset** of H in G determined by a is the set

$$aH = \{x \in G \mid x = ah \text{ for some } h \in H\}.$$

The **right coset** of H in G determined by a is the set

$$Ha = \{x \in G \mid x = ha \text{ for some } h \in H\}.$$

The number of left cosets of H in G is called the **index** of H in G, and is denoted by $[G : H]$.

The “right cosets” version of Proposition 1

Proposition 2 (Let H be a subgroup of the group G, and let $a, b \in G$.)

Then the following conditions are equivalent:

The "right cosets" version of Proposition 1

Proposition 2 (Let H be a subgroup of the group G, and let $a, b \in G$.)

Then the following conditions are equivalent:
(1) $Ha = Hb$; (2) $Ha \subseteq Hb$; (3) $a \in Hb$; (4) $ab^{-1} \in H$;

The “right cosets” version of Proposition 1

Proposition 2 (Let H be a subgroup of the group G, and let $a, b \in G$.)

Then the following conditions are equivalent:

(1) $Ha = Hb$; (2) $Ha \subseteq Hb$; (3) $a \in Hb$; (4) $ab^{-1} \in H$;

(2)′ $Hb \subseteq Ha$; (3)′ $b \in Ha$; (4)′ $ba^{-1} \in H$.

The "right cosets" version of Proposition 1

Proposition 2 (Let H be a subgroup of the group G, and let $a, b \in G$.)

Then the following conditions are equivalent:

(1) $Ha = Hb$; (2) $Ha \subseteq Hb$; (3) $a \in Hb$; (4) $ab^{-1} \in H$;

(2)' $Hb \subseteq Ha$; (3)' $b \in Ha$; (4)' $ba^{-1} \in H$.

$(2)', (3)', (4)'$ *are because of the symmetric in* (1) $Ha = Hb$. *(See Note 2)*

Note 3

The index of H in G could also be defined as the number of right cosets of H in G, since

The "right cosets" version of Proposition 1

Proposition 2 (Let H be a subgroup of the group G, and let $a, b \in G$.)

Then the following conditions are equivalent:

(1) $Ha = Hb$; (2) $Ha \subseteq Hb$; (3) $a \in Hb$; (4) $ab^{-1} \in H$;

(2)′ $Hb \subseteq Ha$; (3)′ $b \in Ha$; (4)′ $ba^{-1} \in H$.

$(2)', (3)', (4)'$ *are because of the symmetric in* (1) $Ha = Hb$. *(See Note 2)*

Note 3

The index of H in G could also be defined as the number of right cosets of H in G, since there is a one-to-one correspondence between left cosets and right cosets. (Check it!)

Let $\mathcal{R} = \{Ha\}$ and $\mathcal{L} = \{aH\}$.

The "right cosets" version of Proposition 1

Proposition 2 (Let H be a subgroup of the group G, and let $a, b \in G$.)

Then the following conditions are equivalent:

(1) $Ha = Hb$; (2) $Ha \subseteq Hb$; (3) $a \in Hb$; (4) $ab^{-1} \in H$;

(2)′ $Hb \subseteq Ha$; (3)′ $b \in Ha$; (4)′ $ba^{-1} \in H$.

$(2)', (3)', (4)'$ *are because of the symmetric in* (1) $Ha = Hb$. *(See Note 2)*

Note 3

The index of H in G could also be defined as the number of right cosets of H in G, since there is a one-to-one correspondence between left cosets and right cosets. (Check it!)

Let $\mathcal{R} = \{Ha\}$ and $\mathcal{L} = \{aH\}$. Define $\phi : \mathcal{R} \to \mathcal{L}$ by $\phi(Ha) = a^{-1}H$.

i) well-defined:

The "right cosets" version of Proposition 1

Proposition 2 (Let H be a subgroup of the group G, and let $a, b \in G$.)

Then the following conditions are equivalent:
(1) $Ha = Hb$; (2) $Ha \subseteq Hb$; (3) $a \in Hb$; (4) $ab^{-1} \in H$;
(2)′ $Hb \subseteq Ha$; (3)′ $b \in Ha$; (4)′ $ba^{-1} \in H$.
(2)′, (3)′, (4)′ are because of the symmetric in (1) $Ha = Hb$. (See Note 2)

Note 3

The index of H in G could also be defined as the number of right cosets of H in G, since there is a one-to-one correspondence between left cosets and right cosets. (Check it!)

Let $\mathcal{R} = \{Ha\}$ and $\mathcal{L} = \{aH\}$. Define $\phi : \mathcal{R} \to \mathcal{L}$ by $\phi(Ha) = a^{-1}H$.
i) well-defined: If $Ha = Hb$, then $ba^{-1} \in H \Rightarrow$

The "right cosets" version of Proposition 1

Proposition 2 (Let H be a subgroup of the group G, and let $a, b \in G$.)

Then the following conditions are equivalent:
(1) $Ha = Hb$; (2) $Ha \subseteq Hb$; (3) $a \in Hb$; (4) $ab^{-1} \in H$;
(2)′ $Hb \subseteq Ha$; (3)′ $b \in Ha$; (4)′ $ba^{-1} \in H$.
$(2)', (3)', (4)'$ *are because of the symmetric in (1) $Ha = Hb$. (See Note 2)*

Note 3

The index of H in G could also be defined as the number of right cosets of H in G, since there is a one-to-one correspondence between left cosets and right cosets. (Check it!)

Let $\mathcal{R} = \{Ha\}$ and $\mathcal{L} = \{aH\}$. Define $\phi : \mathcal{R} \to \mathcal{L}$ by $\phi(Ha) = a^{-1}H$.
i) well-defined: If $Ha = Hb$, then $ba^{-1} \in H \Rightarrow ab^{-1} \in H \Rightarrow$

The "right cosets" version of Proposition 1

Proposition 2 (Let H be a subgroup of the group G, and let $a, b \in G$.)

Then the following conditions are equivalent:

(1) $Ha = Hb$; (2) $Ha \subseteq Hb$; (3) $a \in Hb$; (4) $ab^{-1} \in H$;

(2)′ $Hb \subseteq Ha$; (3)′ $b \in Ha$; (4)′ $ba^{-1} \in H$.

(2)′, (3)′, (4)′ *are because of the symmetric in* (1) $Ha = Hb$. *(See Note 2)*

Note 3

The index of H in G could also be defined as the number of right cosets of H in G, since there is a one-to-one correspondence between left cosets and right cosets. (Check it!)

Let $\mathcal{R} = \{Ha\}$ and $\mathcal{L} = \{aH\}$. Define $\phi : \mathcal{R} \to \mathcal{L}$ by $\phi(Ha) = a^{-1}H$.

i) well-defined: If $Ha = Hb$, then $ba^{-1} \in H \Rightarrow ab^{-1} \in H \Rightarrow a^{-1}H = b^{-1}H$

ii) ϕ is onto:

The "right cosets" version of Proposition 1

Proposition 2 (Let H be a subgroup of the group G, and let $a, b \in G$.)

Then the following conditions are equivalent:

(1) $Ha = Hb$; (2) $Ha \subseteq Hb$; (3) $a \in Hb$; (4) $ab^{-1} \in H$;

(2)′ $Hb \subseteq Ha$; (3)′ $b \in Ha$; (4)′ $ba^{-1} \in H$.

(2)′, (3)′, (4)′ *are because of the symmetric in* (1) $Ha = Hb$. *(See Note 2)*

Note 3

The index of H in G could also be defined as the number of right cosets of H in G, since there is a one-to-one correspondence between left cosets and right cosets. (Check it!)

Let $\mathcal{R} = \{Ha\}$ and $\mathcal{L} = \{aH\}$. Define $\phi : \mathcal{R} \to \mathcal{L}$ by $\phi(Ha) = a^{-1}H$.

i) well-defined: If $Ha = Hb$, then $ba^{-1} \in H \Rightarrow ab^{-1} \in H \Rightarrow a^{-1}H = b^{-1}H$

ii) ϕ is onto: For any $aH \in \mathcal{L}$, we have $\phi(Ha^{-1}) = (a^{-1})^{-1}H = aH$.

iii) ϕ is one-to-one:

The "right cosets" version of Proposition 1

Proposition 2 (Let H be a subgroup of the group G, and let $a, b \in G$.)

Then the following conditions are equivalent:
(1) $Ha = Hb$; (2) $Ha \subseteq Hb$; (3) $a \in Hb$; (4) $ab^{-1} \in H$;
(2)′ $Hb \subseteq Ha$; (3)′ $b \in Ha$; (4)′ $ba^{-1} \in H$.
(2)′, (3)′, (4)′ *are because of the symmetric in* (1) $Ha = Hb$. *(See Note 2)*

Note 3

The index of H in G could also be defined as the number of right cosets of H in G, since there is a one-to-one correspondence between left cosets and right cosets. (Check it!)

Let $\mathcal{R} = \{Ha\}$ and $\mathcal{L} = \{aH\}$. Define $\phi : \mathcal{R} \to \mathcal{L}$ by $\phi(Ha) = a^{-1}H$.
i) well-defined: If $Ha = Hb$, then $ba^{-1} \in H \Rightarrow ab^{-1} \in H \Rightarrow a^{-1}H = b^{-1}H$
ii) ϕ is onto: For any $aH \in \mathcal{L}$, we have $\phi(Ha^{-1}) = (a^{-1})^{-1}H = aH$.
iii) ϕ is one-to-one: If $\phi(Ha) = \phi(Hb)$, then we need to show $Ha = Hb$.

$$\phi(Ha) = \phi(Hb) \Rightarrow$$

The "right cosets" version of Proposition 1

Proposition 2 (Let H be a subgroup of the group G, and let $a, b \in G$.)

Then the following conditions are equivalent:

(1) $Ha = Hb$; (2) $Ha \subseteq Hb$; (3) $a \in Hb$; (4) $ab^{-1} \in H$;

(2)′ $Hb \subseteq Ha$; (3)′ $b \in Ha$; (4)′ $ba^{-1} \in H$.

(2)′, (3)′, (4)′ *are because of the symmetric in* (1) $Ha = Hb$. *(See Note 2)*

Note 3

The index of H in G could also be defined as the number of right cosets of H in G, since there is a one-to-one correspondence between left cosets and right cosets. (Check it!)

Let $\mathcal{R} = \{Ha\}$ and $\mathcal{L} = \{aH\}$. Define $\phi : \mathcal{R} \to \mathcal{L}$ by $\phi(Ha) = a^{-1}H$.

i) well-defined: If $Ha = Hb$, then $ba^{-1} \in H \Rightarrow ab^{-1} \in H \Rightarrow a^{-1}H = b^{-1}H$

ii) ϕ is onto: For any $aH \in \mathcal{L}$, we have $\phi(Ha^{-1}) = (a^{-1})^{-1}H = aH$.

iii) ϕ is one-to-one: If $\phi(Ha) = \phi(Hb)$, then we need to show $Ha = Hb$.

$$\phi(Ha) = \phi(Hb) \Rightarrow a^{-1}H = b^{-1}H \Rightarrow$$

The "right cosets" version of Proposition 1

Proposition 2 (Let H be a subgroup of the group G, and let $a, b \in G$.)

Then the following conditions are equivalent:

(1) $Ha = Hb$; (2) $Ha \subseteq Hb$; (3) $a \in Hb$; (4) $ab^{-1} \in H$;

(2)′ $Hb \subseteq Ha$; (3)′ $b \in Ha$; (4)′ $ba^{-1} \in H$.

$(2)', (3)', (4)'$ *are because of the symmetric in* (1) $Ha = Hb$. *(See Note 2)*

Note 3

The index of H in G could also be defined as the number of right cosets of H in G, since there is a one-to-one correspondence between left cosets and right cosets. (Check it!)

Let $\mathcal{R} = \{Ha\}$ and $\mathcal{L} = \{aH\}$. Define $\phi : \mathcal{R} \to \mathcal{L}$ by $\phi(Ha) = a^{-1}H$.

i) well-defined: If $Ha = Hb$, then $ba^{-1} \in H \Rightarrow ab^{-1} \in H \Rightarrow a^{-1}H = b^{-1}H$

ii) ϕ is onto: For any $aH \in \mathcal{L}$, we have $\phi(Ha^{-1}) = (a^{-1})^{-1}H = aH$.

iii) ϕ is one-to-one: If $\phi(Ha) = \phi(Hb)$, then we need to show $Ha = Hb$.

$$\phi(Ha) = \phi(Hb) \Rightarrow a^{-1}H = b^{-1}H \Rightarrow ba^{-1} \in H \Rightarrow$$

The "right cosets" version of Proposition 1

Proposition 2 (Let H be a subgroup of the group G, and let $a, b \in G$.)

Then the following conditions are equivalent:

(1) $Ha = Hb$; (2) $Ha \subseteq Hb$; (3) $a \in Hb$; (4) $ab^{-1} \in H$;

(2)′ $Hb \subseteq Ha$; (3)′ $b \in Ha$; (4)′ $ba^{-1} \in H$.

(2)′, (3)′, (4)′ *are because of the symmetric in* (1) $Ha = Hb$. *(See Note 2)*

Note 3

The index of H in G could also be defined as the number of right cosets of H in G, since there is a one-to-one correspondence between left cosets and right cosets. (Check it!)

Let $\mathcal{R} = \{Ha\}$ and $\mathcal{L} = \{aH\}$. Define $\phi : \mathcal{R} \to \mathcal{L}$ by $\phi(Ha) = a^{-1}H$.

i) well-defined: If $Ha = Hb$, then $ba^{-1} \in H \Rightarrow ab^{-1} \in H \Rightarrow a^{-1}H = b^{-1}H$

ii) ϕ is onto: For any $aH \in \mathcal{L}$, we have $\phi(Ha^{-1}) = (a^{-1})^{-1}H = aH$.

iii) ϕ is one-to-one: If $\phi(Ha) = \phi(Hb)$, then we need to show $Ha = Hb$.

$$\phi(Ha) = \phi(Hb) \Rightarrow a^{-1}H = b^{-1}H \Rightarrow ba^{-1} \in H \Rightarrow Ha = Hb.$$

All left cosets of H have the same number of elements

Proposition 3 (Let H be a subgroup of the group G, and $a \in G$.)

The left coset aH has the same number of elements as H.

Proof.

All left cosets of H have the same number of elements

Proposition 3 (Let H be a subgroup of the group G, and $a \in G$.)

The left coset aH has the same number of elements as H.

Proof.

Given any left coset aH of H, define the function $f : H \to aH$ by

$$f(h) = ah, \text{ for all } h \in H.$$

All left cosets of H have the same number of elements

Proposition 3 (Let H be a subgroup of the group G, and $a \in G$.)

The left coset aH has the same number of elements as H.

Proof.

Given any left coset aH of H, define the function $f : H \to aH$ by

$$f(h) = ah, \text{ for all } h \in H.$$

Then f is one-to-one. (Why?)

All left cosets of H have the same number of elements

Proposition 3 (Let H be a subgroup of the group G, and $a \in G$.)

The left coset aH has the same number of elements as H.

Proof.

Given any left coset aH of H, define the function $f : H \to aH$ by

$$f(h) = ah, \text{ for all } h \in H.$$

Then f is one-to-one. (Why?) It is obvious that f is onto. Done ✓. □

Remark 1

All left cosets of H have the same number of elements

Proposition 3 (Let H be a subgroup of the group G, and $a \in G$.)

The left coset aH has the same number of elements as H.

Proof.

Given any left coset aH of H, define the function $f : H \to aH$ by

$$f(h) = ah, \text{ for all } h \in H.$$

Then f is one-to-one. (Why?) It is obvious that f is onto. Done ✓. □

Remark 1

If G is a finite group, this proposition is at the heart of the proof of Lagrange's theorem, and

All left cosets of H have the same number of elements

Proposition 3 (Let H be a subgroup of the group G, and $a \in G$.)

The left coset aH has the same number of elements as H.

Proof.

Given any left coset aH of H, define the function $f : H \to aH$ by

$$f(h) = ah, \text{ for all } h \in H.$$

Then f is one-to-one. (Why?) It is obvious that f is onto. Done ✓. □

Remark 1

If G is a finite group, this proposition is at the heart of the proof of Lagrange's theorem, and shows that the index $[G : H] = |G|/|H|$.

Example: List the left cosets of a given subgroup H of a finite group.

Algorithm:

Algorithm:

(1) If $a \in H$, then $aH = H$, so we begin by choosing any element $a \notin H$.

Example: List the left cosets of a given subgroup H of a finite group.

Algorithm:

(1) If $a \in H$, then $aH = H$, so we begin by choosing any element $a \notin H$.
(2) Any element in aH determines the same coset (Why?),

Example: List the left cosets of a given subgroup H of a finite group.

Algorithm:

(1) If $a \in H$, then $aH = H$, so we begin by choosing any element $a \notin H$.

(2) Any element in aH determines the same coset (Why?), so for the next coset we choose any element not in H or aH (if possible).

Algorithm:

(1) If $a \in H$, then $aH = H$, so we begin by choosing any element $a \notin H$.

(2) Any element in aH determines the same coset (Why?), so for the next coset we choose any element not in H or aH (if possible).

(3) Continuing in this way provides a method for listing all cosets.

Example 6

$G = \mathbf{Z}_{11}^{\times} = \{[1], [2], [3], [4], [5], [6], [7], [8], [9], [10]\}$ & $H = \{[1], [10]\}$:

(0)

Example: List the left cosets of a given subgroup H of a finite group.

Algorithm:

(1) If $a \in H$, then $aH = H$, so we begin by choosing any element $a \notin H$.

(2) Any element in aH determines the same coset (Why?), so for the next coset we choose any element not in H or aH (if possible).

(3) Continuing in this way provides a method for listing all cosets.

Example 6

$G = \mathbf{Z}_{11}^{\times} = \{[1], [2], [3], [4], [5], [6], [7], [8], [9], [10]\}$ & $H = \{[1], [10]\}$:

(0) The first coset we can identify is H itself, i.e., $[1]H = \{[1], [10]\}$.

(1)

Example: List the left cosets of a given subgroup H of a finite group.

Algorithm:

(1) If $a \in H$, then $aH = H$, so we begin by choosing any element $a \notin H$.

(2) Any element in aH determines the same coset (Why?), so for the next coset we choose any element not in H or aH (if possible).

(3) Continuing in this way provides a method for listing all cosets.

Example 6

$G = \mathbf{Z}_{11}^{\times} = \{[1],[2],[3],[4],[5],[6],[7],[8],[9],[10]\}$ & $H = \{[1],[10]\}$:

(0) The first coset we can identify is H itself, i.e., $[1]H = \{[1],[10]\}$.

(1) Choose $a \notin H$, say $a = [2]$: Obtain the coset $[2]H = \{[2],[9]\}$.

(2)

Algorithm:

(1) If $a \in H$, then $aH = H$, so we begin by choosing any element $a \notin H$.

(2) Any element in aH determines the same coset (Why?), so for the next coset we choose any element not in H or aH (if possible).

(3) Continuing in this way provides a method for listing all cosets.

Example 6

$G = \mathbf{Z}_{11}^{\times} = \{[1], [2], [3], [4], [5], [6], [7], [8], [9], [10]\}$ & $H = \{[1], [10]\}$:

(0) The first coset we can identify is H itself, i.e., $[1]H = \{[1], [10]\}$.

(1) Choose $a \notin H$, say $a = [2]$: Obtain the coset $[2]H = \{[2], [9]\}$.

(2) Choose $b \notin \{H, aH\}$, say $b = [3]$: Obtain $[3]H = \{[3], [8]\}$.

(3)

Example: List the left cosets of a given subgroup H of a finite group.

Algorithm:

(1) If $a \in H$, then $aH = H$, so we begin by choosing any element $a \notin H$.

(2) Any element in aH determines the same coset (Why?), so for the next coset we choose any element not in H or aH (if possible).

(3) Continuing in this way provides a method for listing all cosets.

Example 6

$G = \mathbf{Z}_{11}^{\times} = \{[1],[2],[3],[4],[5],[6],[7],[8],[9],[10]\}$ & $H = \{[1],[10]\}$:

(0) The first coset we can identify is H itself, i.e., $[1]H = \{[1],[10]\}$.

(1) Choose $a \notin H$, say $a = [2]$: Obtain the coset $[2]H = \{[2],[9]\}$.

(2) Choose $b \notin \{H, aH\}$, say $b = [3]$: Obtain $[3]H = \{[3],[8]\}$.

(3) Choose $c \notin \{H, aH, bH\}$, say $b = [4]$: Obtain $[4]H = \{[4],[7]\}$.

(4)

Example: List the left cosets of a given subgroup H of a finite group.

Algorithm:

(1) If $a \in H$, then $aH = H$, so we begin by choosing any element $a \notin H$.

(2) Any element in aH determines the same coset (Why?), so for the next coset we choose any element not in H or aH (if possible).

(3) Continuing in this way provides a method for listing all cosets.

Example 6

$G = \mathbf{Z}_{11}^{\times} = \{[1],[2],[3],[4],[5],[6],[7],[8],[9],[10]\}$ & $H = \{[1],[10]\}$:

(0) The first coset we can identify is H itself, i.e., $[1]H = \{[1],[10]\}$.

(1) Choose $a \notin H$, say $a = [2]$: Obtain the coset $[2]H = \{[2],[9]\}$.

(2) Choose $b \notin \{H, aH\}$, say $b = [3]$: Obtain $[3]H = \{[3],[8]\}$.

(3) Choose $c \notin \{H, aH, bH\}$, say $b = [4]$: Obtain $[4]H = \{[4],[7]\}$.

(4) Choose $d \notin \{H, aH, bH, cH\}$, say $d = [5]$: Obtain $[5]H = \{[5],[6]\}$.

Example: List the left cosets of a given subgroup H of a finite group.

Algorithm:

(1) If $a \in H$, then $aH = H$, so we begin by choosing any element $a \notin H$.

(2) Any element in aH determines the same coset (Why?), so for the next coset we choose any element not in H or aH (if possible).

(3) Continuing in this way provides a method for listing all cosets.

Example 6

$G = \mathbf{Z}_{11}^{\times} = \{[1],[2],[3],[4],[5],[6],[7],[8],[9],[10]\}$ & $H = \{[1],[10]\}$:

(0) The first coset we can identify is H itself, i.e., $[1]H = \{[1],[10]\}$.

(1) Choose $a \notin H$, say $a = [2]$: Obtain the coset $[2]H = \{[2],[9]\}$.

(2) Choose $b \notin \{H, aH\}$, say $b = [3]$: Obtain $[3]H = \{[3],[8]\}$.

(3) Choose $c \notin \{H, aH, bH\}$, say $b = [4]$: Obtain $[4]H = \{[4],[7]\}$.

(4) Choose $d \notin \{H, aH, bH, cH\}$, say $d = [5]$: Obtain $[5]H = \{[5],[6]\}$.

Thus the cosets of H are $H, [2]H, [3]H, [4]H, [5]H$, and so $[G : H] = 5$.

Exercise

Again let $G = \mathbf{Z}_{11}^{\times}$. Let $K = \{[1], [3], [9], [5], [4]\} = \langle [3] \rangle$.

Question 1

What are the left cosets of K?

Exercise

Again let $G = \mathbf{Z}_{11}^{\times}$. Let $K = \{[1], [3], [9], [5], [4]\} = \langle [3] \rangle$.

Question 1

What are the left cosets of K?

Since the left cosets all have the same number of elements (Why?) and

Exercise

Again let $G = \mathbf{Z}_{11}^{\times}$. Let $K = \{[1],[3],[9],[5],[4]\} = \langle [3] \rangle$.

Question 1

What are the left cosets of K?

Since the left cosets all have the same number of elements (Why?) and we already have a coset ($K = [1]K$) with half of the total number of elements,

Exercise

Again let $G = \mathbf{Z}_{11}^{\times}$. Let $K = \{[1], [3], [9], [5], [4]\} = \langle [3] \rangle$.

Question 1

What are the left cosets of K?

Since the left cosets all have the same number of elements (Why?) and we already have a coset ($K = [1]K$) with half of the total number of elements, there must be only one other coset, containing the rest of the elements.✓

Exercise

Again let $G = \mathbf{Z}_{11}^{\times}$. Let $K = \{[1], [3], [9], [5], [4]\} = \langle [3] \rangle$.

Question 1

What are the left cosets of K?

Since the left cosets all have the same number of elements (Why?) and we already have a coset ($K = [1]K$) with half of the total number of elements, there must be only one other coset, containing the rest of the elements.✓
Thus the left cosets of K are the following sets:

Exercise

Again let $G = \mathbf{Z}_{11}^{\times}$. Let $K = \{[1], [3], [9], [5], [4]\} = \langle [3] \rangle$.

Question 1

What are the left cosets of K?

Since the left cosets all have the same number of elements (Why?) and we already have a coset ($K = [1]K$) with half of the total number of elements, there must be only one other coset, containing the rest of the elements.✓
Thus the left cosets of K are the following sets:

$$K = [1]K = \{[1], [3], [9], [5], [4]\}, \qquad [2]K = \{[2], [6], [7], [10], [8]\}.$$

Similarly, in this case,

Exercise

Again let $G = \mathbf{Z}_{11}^{\times}$. Let $K = \{[1],[3],[9],[5],[4]\} = \langle [3] \rangle$.

Question 1

What are the left cosets of K?

Since the left cosets all have the same number of elements (Why?) and we already have a coset ($K = [1]K$) with half of the total number of elements, there must be only one other coset, containing the rest of the elements.✓ Thus the left cosets of K are the following sets:

$$K = [1]K = \{[1],[3],[9],[5],[4]\}, \qquad [2]K = \{[2],[6],[7],[10],[8]\}.$$

Similarly, in this case, $[G : K] = 2$.

Example: Non-abelian group $G = S_3$

Let $G = S_3 = \{e, a, a^2, b, ab, a^2b\}$, where $a^3 = e, b^2 = e$, and $ba = a^2b$.

Example 7 (Let $H = \{e, b\}$.)

Example: Non-abelian group $G = S_3$

Let $G = S_3 = \{e, a, a^2, b, ab, a^2b\}$, where $a^3 = e, b^2 = e$, and $ba = a^2b$.

Example 7 (Let $H = \{e, b\}$.)

The left cosets of H:

Example: Non-abelian group $G = S_3$

Let $G = S_3 = \{e, a, a^2, b, ab, a^2b\}$, where $a^3 = e, b^2 = e$, and $ba = a^2b$.

Example 7 (Let $H = \{e, b\}$.)

The left cosets of H: $\quad H = \{e, b\}, \quad aH = \{a, ab\}, \quad a^2H = \{a^2, a^2b\}$.

Example: Non-abelian group $G = S_3$

Let $G = S_3 = \{e, a, a^2, b, ab, a^2b\}$, where $a^3 = e, b^2 = e$, and $ba = a^2b$.

Example 7 (Let $H = \{e, b\}$.)

The left cosets of H: $\quad H = \{e, b\}, \quad aH = \{a, ab\}, \quad a^2H = \{a^2, a^2b\}$.
The right cosets of H:

Example: Non-abelian group $G = S_3$

Let $G = S_3 = \{e, a, a^2, b, ab, a^2b\}$, where $a^3 = e, b^2 = e$, and $ba = a^2b$.

Example 7 (Let $H = \{e, b\}$.)

The left cosets of H: $H = \{e, b\}$, $aH = \{a, ab\}$, $a^2H = \{a^2, a^2b\}$.
The right cosets of H: $H = \{e, b\}$, $Ha = \{a, a^2b\}$, $Ha^2 = \{a^2, ab\}$.

Example: Non-abelian group $G = S_3$

Let $G = S_3 = \{e, a, a^2, b, ab, a^2b\}$, where $a^3 = e, b^2 = e$, and $ba = a^2b$.

Example 7 (Let $H = \{e, b\}$.)

The left cosets of H: $H = \{e, b\}$, $aH = \{a, ab\}$, $a^2H = \{a^2, a^2b\}$.
The right cosets of H: $H = \{e, b\}$, $Ha = \{a, a^2b\}$, $Ha^2 = \{a^2, ab\}$.
Note that for the subgroup H the left and right cosets are not the same.

Example 8 (Let $N = \{e, a, a^2\}$.)

Example: Non-abelian group $G = S_3$

Let $G = S_3 = \{e, a, a^2, b, ab, a^2b\}$, where $a^3 = e, b^2 = e$, and $ba = a^2b$.

Example 7 (Let $H = \{e, b\}$.)

The left cosets of H: $H = \{e, b\}$, $aH = \{a, ab\}$, $a^2H = \{a^2, a^2b\}$.
The right cosets of H: $H = \{e, b\}$, $Ha = \{a, a^2b\}$, $Ha^2 = \{a^2, ab\}$.
Note that for the subgroup H the left and right cosets are not the same.

Example 8 (Let $N = \{e, a, a^2\}$.)

The left cosets of N:

Example: Non-abelian group $G = S_3$

Let $G = S_3 = \{e, a, a^2, b, ab, a^2b\}$, where $a^3 = e, b^2 = e$, and $ba = a^2b$.

Example 7 (Let $H = \{e, b\}$.)

The left cosets of H: $H = \{e, b\}$, $aH = \{a, ab\}$, $a^2H = \{a^2, a^2b\}$.
The right cosets of H: $H = \{e, b\}$, $Ha = \{a, a^2b\}$, $Ha^2 = \{a^2, ab\}$.
Note that for the subgroup H the left and right cosets are not the same.

Example 8 (Let $N = \{e, a, a^2\}$.)

The left cosets of N: $N = \{e, a, a^2\}, bN = \{b, ba, ba^2\} = \{b, a^2b, ab\}$.

Example: Non-abelian group $G = S_3$

Let $G = S_3 = \{e, a, a^2, b, ab, a^2b\}$, where $a^3 = e, b^2 = e$, and $ba = a^2b$.

Example 7 (Let $H = \{e, b\}$.)

The left cosets of H: $H = \{e, b\}$, $aH = \{a, ab\}$, $a^2H = \{a^2, a^2b\}$.
The right cosets of H: $H = \{e, b\}$, $Ha = \{a, a^2b\}$, $Ha^2 = \{a^2, ab\}$.
Note that for the subgroup H the left and right cosets are not the same.

Example 8 (Let $N = \{e, a, a^2\}$.)

The left cosets of N: $N = \{e, a, a^2\}, bN = \{b, ba, ba^2\} = \{b, a^2b, ab\}$.
The right cosets of N:

Example: Non-abelian group $G = S_3$

Let $G = S_3 = \{e, a, a^2, b, ab, a^2b\}$, where $a^3 = e, b^2 = e$, and $ba = a^2b$.

Example 7 (Let $H = \{e, b\}$.)

The left cosets of H: $H = \{e, b\}$, $aH = \{a, ab\}$, $a^2H = \{a^2, a^2b\}$.
The right cosets of H: $H = \{e, b\}$, $Ha = \{a, a^2b\}$, $Ha^2 = \{a^2, ab\}$.
Note that for the subgroup H the left and right cosets are not the same.

Example 8 (Let $N = \{e, a, a^2\}$.)

The left cosets of N: $N = \{e, a, a^2\}, bN = \{b, ba, ba^2\} = \{b, a^2b, ab\}$.
The right cosets of N: $N = \{e, a, a^2\}, Nb = \{b, ab, a^2b\}$.

Example: Non-abelian group $G = S_3$

Let $G = S_3 = \{e, a, a^2, b, ab, a^2b\}$, where $a^3 = e, b^2 = e$, and $ba = a^2b$.

Example 7 (Let $H = \{e, b\}$.)

The left cosets of H: $H = \{e, b\}$, $aH = \{a, ab\}$, $a^2H = \{a^2, a^2b\}$.
The right cosets of H: $H = \{e, b\}$, $Ha = \{a, a^2b\}$, $Ha^2 = \{a^2, ab\}$.
Note that for the subgroup H the left and right cosets are not the same.

Example 8 (Let $N = \{e, a, a^2\}$.)

The left cosets of N: $N = \{e, a, a^2\}, bN = \{b, ba, ba^2\} = \{b, a^2b, ab\}$.
The right cosets of N: $N = \{e, a, a^2\}, Nb = \{b, ab, a^2b\}$.
Note that for the subgroup N the left and right cosets are the same.

Cosets of a subgroup H in an abelian group G

Cosets of a subgroup H in an abelian group G

For abelian groups, left cosets and right cosets are always the same.(Why?)

Cosets of a subgroup H in an abelian group G

For abelian groups, left cosets and right cosets are always the same.(Why?)

Let $(G, +)$ be an abelian group. The cosets of a subgroup H have the form

$$a + H = \{x \in G \mid x = a + h \text{ for some } h \in H\}.$$

Cosets of a subgroup H in an abelian group G

For abelian groups, left cosets and right cosets are always the same.(Why?)

Let $(G, +)$ be an abelian group. The cosets of a subgroup H have the form

$$a + H = \{x \in G \mid x = a + h \text{ for some } h \in H\}.$$

Proposition 1 shows that in this case, $a + H = b + H \Leftrightarrow a - b \in H$.

Example 9

Let $G = \mathbf{Z}_{12}$, and let $H = 4\mathbf{Z}_{12} = \{[0], [4], [8]\}$. To find all cosets of H:

Cosets of a subgroup H in an abelian group G

For abelian groups, left cosets and right cosets are always the same.(Why?)

Let $(G, +)$ be an abelian group. The cosets of a subgroup H have the form

$$a + H = \{x \in G \mid x = a + h \text{ for some } h \in H\}.$$

Proposition 1 shows that in this case, $a + H = b + H \Leftrightarrow a - b \in H$.

Example 9

Let $G = \mathbf{Z}_{12}$, and let $H = 4\mathbf{Z}_{12} = \{[0], [4], [8]\}$. To find all cosets of H:

(0) $[0] + H = [4] + H = [8] + H = H = \{[0], [4], [8]\}$.

Cosets of a subgroup H in an abelian group G

For abelian groups, left cosets and right cosets are always the same.(Why?)

Let $(G, +)$ be an abelian group. The cosets of a subgroup H have the form

$$a + H = \{x \in G \mid x = a + h \text{ for some } h \in H\}.$$

Proposition 1 shows that in this case, $a + H = b + H \Leftrightarrow a - b \in H$.

Example 9

Let $G = \mathbf{Z}_{12}$, and let $H = 4\mathbf{Z}_{12} = \{[0], [4], [8]\}$. To find all cosets of H:

(0) $[0] + H = [4] + H = [8] + H = H = \{[0], [4], [8]\}$.

(1) Choose $[1] \notin H$, we obtain $[1] + H = \{[1], [5], [9]\}$.

Cosets of a subgroup H in an abelian group G

For abelian groups, left cosets and right cosets are always the same.(Why?)

Let $(G, +)$ be an abelian group. The cosets of a subgroup H have the form

$$a + H = \{x \in G \mid x = a + h \text{ for some } h \in H\}.$$

Proposition 1 shows that in this case, $a + H = b + H \Leftrightarrow a - b \in H$.

Example 9

Let $G = \mathbf{Z}_{12}$, and let $H = 4\mathbf{Z}_{12} = \{[0], [4], [8]\}$. To find all cosets of H:

(0) $[0] + H = [4] + H = [8] + H = H = \{[0], [4], [8]\}$.

(1) Choose $[1] \notin H$, we obtain $[1] + H = \{[1], [5], [9]\}$.

(2) Choose $[2] \notin \{H, [1] + H\}$, we obtain $[2] + H = \{[2], [6], [10]\}$.

Cosets of a subgroup H in an abelian group G

For abelian groups, left cosets and right cosets are always the same.(Why?)

Let $(G, +)$ be an abelian group. The cosets of a subgroup H have the form

$$a + H = \{x \in G \mid x = a + h \text{ for some } h \in H\}.$$

Proposition 1 shows that in this case, $a + H = b + H \Leftrightarrow a - b \in H$.

Example 9

Let $G = \mathbf{Z}_{12}$, and let $H = 4\mathbf{Z}_{12} = \{[0], [4], [8]\}$. To find all cosets of H:

(0) $[0] + H = [4] + H = [8] + H = H = \{[0], [4], [8]\}$.

(1) Choose $[1] \notin H$, we obtain $[1] + H = \{[1], [5], [9]\}$.

(2) Choose $[2] \notin \{H, [1] + H\}$, we obtain $[2] + H = \{[2], [6], [10]\}$.

(3) Choose $[3] \notin \{H, [1] + H, [2] + H\}$, we obtain $[3] + H = \{[3], [7], [11]\}$.

Cosets of a subgroup H in an abelian group G

For abelian groups, left cosets and right cosets are always the same.(Why?)

Let $(G, +)$ be an abelian group. The cosets of a subgroup H have the form

$$a + H = \{x \in G \mid x = a + h \text{ for some } h \in H\}.$$

Proposition 1 shows that in this case, $a + H = b + H \Leftrightarrow a - b \in H$.

Example 9

Let $G = \mathbf{Z}_{12}$, and let $H = 4\mathbf{Z}_{12} = \{[0], [4], [8]\}$. To find all cosets of H:

(0) $[0] + H = [4] + H = [8] + H = H = \{[0], [4], [8]\}$.

(1) Choose $[1] \notin H$, we obtain $[1] + H = \{[1], [5], [9]\}$.

(2) Choose $[2] \notin \{H, [1] + H\}$, we obtain $[2] + H = \{[2], [6], [10]\}$.

(3) Choose $[3] \notin \{H, [1] + H, [2] + H\}$, we obtain $[3] + H = \{[3], [7], [11]\}$.

Since G is abelian, the right cosets are precisely the same as the left cosets.

Some results in Section 3.7

For a homomorphism $\phi : G_1 \to G_2$, a natural equivalent relation on G_1 is

(Definition 14 in §3.7) $a \sim_\phi b \Leftrightarrow \phi(a) = \phi(b) \Leftrightarrow ab^{-1} \in \ker(\phi)$ (Why?)

Some results in Section 3.7

For a homomorphism $\phi : G_1 \to G_2$, a natural equivalent relation on G_1 is

(Definition 14 in §3.7) $a \sim_\phi b \Leftrightarrow \phi(a) = \phi(b) \Leftrightarrow ab^{-1} \in \ker(\phi)$ (Why?)

The equivalence classes of $\sim_\phi$ are the right cosets of $\ker(\phi)$: $[a] = \ker(\phi)a$.

Note 4 (Proposition 8 in §3.7)

Some results in Section 3.7

For a homomorphism $\phi : G_1 \to G_2$, a natural equivalent relation on G_1 is

(Definition 14 in §3.7) $a \sim_\phi b \Leftrightarrow \phi(a) = \phi(b) \Leftrightarrow ab^{-1} \in \ker(\phi)$ (Why?)

The equivalence classes of $\sim_\phi$ are the right cosets of $\ker(\phi)$: $[a] = \ker(\phi)a$.

Note 4 (Proposition 8 in §3.7)

The set G_1/ϕ of equivalence classes defined by ϕ forms a group.

Some results in Section 3.7

For a homomorphism $\phi : G_1 \to G_2$, a natural equivalent relation on G_1 is

(Definition 14 in §3.7) $a \sim_\phi b \Leftrightarrow \phi(a) = \phi(b) \Leftrightarrow ab^{-1} \in \ker(\phi)$ (Why?)

The equivalence classes of $\sim_\phi$ are the right cosets of $\ker(\phi)$: $[a] = \ker(\phi)a$.

Note 4 (Proposition 8 in §3.7)

The set G_1/ϕ of equivalence classes defined by ϕ forms a group.

Proposition 9 in §3.7 shows that the equivalence classes are also the left cosets of $\ker(\phi)$. (Why?) [

Some results in Section 3.7

For a homomorphism $\phi : G_1 \to G_2$, a natural equivalent relation on G_1 is

(Definition 14 in §3.7) $a \sim_\phi b \Leftrightarrow \phi(a) = \phi(b) \Leftrightarrow ab^{-1} \in \ker(\phi)$ (Why?)

The equivalence classes of $\sim_\phi$ are the right cosets of $\ker(\phi)$: $[a] = \ker(\phi)a$.

Note 4 (Proposition 8 in §3.7)

The set G_1/ϕ of equivalence classes defined by ϕ forms a group.

Proposition 9 in §3.7 shows that the equivalence classes are also the left cosets of $\ker(\phi)$. (Why?) [$a \sim_\phi b$ if and only if $a^{-1}b \in \ker(\phi)$] (Check it!)

Definition 10 (Definition 12 in §3.7)

Some results in Section 3.7

For a homomorphism $\phi : G_1 \to G_2$, a natural equivalent relation on G_1 is

(Definition 14 in §3.7) $a \sim_\phi b \Leftrightarrow \phi(a) = \phi(b) \Leftrightarrow ab^{-1} \in \ker(\phi)$ (Why?)

The equivalence classes of $\sim_\phi$ are the right cosets of $\ker(\phi)$: $[a] = \ker(\phi)a$.

Note 4 (Proposition 8 in §3.7)

The set G_1/ϕ of equivalence classes defined by ϕ forms a group.

Proposition 9 in §3.7 shows that the equivalence classes are also the left cosets of $\ker(\phi)$. (Why?) [$a \sim_\phi b$ if and only if $a^{-1}b \in \ker(\phi)$] (Check it!)

Definition 10 (Definition 12 in §3.7)

A subgroup H of G is **normal** if $ghg^{-1} \in H$ for all $h \in H$ and $g \in G$.

Some results in Section 3.7

For a homomorphism $\phi : G_1 \to G_2$, a natural equivalent relation on G_1 is

(Definition 14 in §3.7) $a \sim_\phi b \Leftrightarrow \phi(a) = \phi(b) \Leftrightarrow ab^{-1} \in \ker(\phi)$ (Why?)

The equivalence classes of $\sim_\phi$ are the right cosets of $\ker(\phi)$: $[a] = \ker(\phi)a$.

Note 4 (Proposition 8 in §3.7)

The set G_1/ϕ of equivalence classes defined by ϕ forms a group.

Proposition 9 in §3.7 shows that the equivalence classes are also the left cosets of $\ker(\phi)$. (Why?) [$a \sim_\phi b$ if and only if $a^{-1}b \in \ker(\phi)$] (Check it!)

Definition 10 (Definition 12 in §3.7)

A subgroup H of G is **normal** if $ghg^{-1} \in H$ for all $h \in H$ and $g \in G$.

H is normal if and only if $g^{-1}hg \in H$ for all $h \in H$ and $g \in G$. (Why?)

Looking ahead:

Some results in Section 3.7

For a homomorphism $\phi : G_1 \to G_2$, a natural equivalent relation on G_1 is

(Definition 14 in §3.7) $a \sim_\phi b \Leftrightarrow \phi(a) = \phi(b) \Leftrightarrow ab^{-1} \in \ker(\phi)$ (Why?)

The equivalence classes of $\sim_\phi$ are the right cosets of $\ker(\phi)$: $[a] = \ker(\phi)a$.

Note 4 (Proposition 8 in §3.7)

The set G_1/ϕ of equivalence classes defined by ϕ forms a group.

Proposition 9 in §3.7 shows that the equivalence classes are also the left cosets of $\ker(\phi)$. (Why?) [$a \sim_\phi b$ if and only if $a^{-1}b \in \ker(\phi)$] (Check it!)

Definition 10 (Definition 12 in §3.7)

A subgroup H of G is **normal** if $ghg^{-1} \in H$ for all $h \in H$ and $g \in G$.

H is normal if and only if $g^{-1}hg \in H$ for all $h \in H$ and $g \in G$. (Why?)

Looking ahead:

- H is normal if and only if its left and right cosets coincide.

Some results in Section 3.7

For a homomorphism $\phi : G_1 \to G_2$, a natural equivalent relation on G_1 is

(Definition 14 in §3.7) $a \sim_\phi b \Leftrightarrow \phi(a) = \phi(b) \Leftrightarrow ab^{-1} \in \ker(\phi)$ (Why?)

The equivalence classes of $\sim_\phi$ are the right cosets of $\ker(\phi)$: $[a] = \ker(\phi)a$.

Note 4 (Proposition 8 in §3.7)

The set G_1/ϕ of equivalence classes defined by ϕ forms a group.

Proposition 9 in §3.7 shows that the equivalence classes are also the left cosets of $\ker(\phi)$. (Why?) [$a \sim_\phi b$ if and only if $a^{-1}b \in \ker(\phi)$] (Check it!)

Definition 10 (Definition 12 in §3.7)

A subgroup H of G is **normal** if $ghg^{-1} \in H$ for all $h \in H$ and $g \in G$.

H is normal if and only if $g^{-1}hg \in H$ for all $h \in H$ and $g \in G$. (Why?)

Looking ahead:

- H is normal if and only if its left and right cosets coincide.
- If H is normal, then the multiplication of cosets is compatible with the structure of G, and that the set of cosets forms a group.

The set of left cosets of a normal subgroup forms a group

Theorem 11

The set of left cosets of a normal subgroup forms a group

Theorem 11

If N is a normal subgroup of G, then the set of left cosets of N forms a group under the coset multiplication given by $aNbN = abN$ for $a, b \in G$.

(i) well-defined:

The set of left cosets of a normal subgroup forms a group

Theorem 11

If N is a normal subgroup of G, then the set of left cosets of N forms a group under the coset multiplication given by $aNbN = abN$ for $a, b \in G$.

(i) well-defined: Let $a, b, c, d \in G$. If $aN = cN$ and $bN = dN$, then $a^{-1}c \in N$ and $b^{-1}d \in N$. (Why?) [

The set of left cosets of a normal subgroup forms a group

Theorem 11

If N is a normal subgroup of G, then the set of left cosets of N forms a group under the coset multiplication given by $aNbN = abN$ for $a, b \in G$.

(i) well-defined: Let $a, b, c, d \in G$. If $aN = cN$ and $bN = dN$, then

$a^{-1}c \in N$ and $b^{-1}d \in N$. (Why?) [Proposition 1]

To show $abN = cdN$. It suffices to show $(ab)^{-1}cd \in N$. (Why?)

The set of left cosets of a normal subgroup forms a group

Theorem 11

If N is a normal subgroup of G, then the set of left cosets of N forms a group under the coset multiplication given by $aNbN = abN$ for $a, b \in G$.

(i) well-defined: Let $a, b, c, d \in G$. If $aN = cN$ and $bN = dN$, then

$a^{-1}c \in N$ and $b^{-1}d \in N$. (Why?) [Proposition 1]

To show $abN = cdN$. It suffices to show $(ab)^{-1}cd \in N$. (Why?)

$$(ab)^{-1}cd = b^{-1}(a^{-1}c)d \overset{!}{=} \underbrace{b^{-1}d}_{\in N}\underbrace{(d^{-1}(a^{-1}c)d)}_{\in N \ (Why?)} \in N$$

(ii) associativity:

The set of left cosets of a normal subgroup forms a group

Theorem 11

If N is a normal subgroup of G, then the set of left cosets of N forms a group under the coset multiplication given by $aNbN = abN$ for $a, b \in G$.

(i) well-defined: Let $a, b, c, d \in G$. If $aN = cN$ and $bN = dN$, then

$a^{-1}c \in N$ and $b^{-1}d \in N$. (Why?) [Proposition 1]

To show $abN = cdN$. It suffices to show $(ab)^{-1}cd \in N$. (Why?)

$$(ab)^{-1}cd = b^{-1}(a^{-1}c)d \overset{!}{=} \underbrace{b^{-1}d}_{\in N}\underbrace{(d^{-1}(a^{-1}c)d)}_{\in N\ (Why?)} \in N$$

(ii) associativity: Let $a, b, c \in G$. Then

Theorem 11

If N is a normal subgroup of G, then the set of left cosets of N forms a group under the coset multiplication given by $aNbN = abN$ for $a, b \in G$.

(i) well-defined: Let $a, b, c, d \in G$. If $aN = cN$ and $bN = dN$, then

$$a^{-1}c \in N \text{ and } b^{-1}d \in N. \text{ (Why?) [Proposition 1]}$$

To show $abN = cdN$. It suffices to show $(ab)^{-1}cd \in N$. (Why?)

$$(ab)^{-1}cd = b^{-1}(a^{-1}c)d \overset{!}{=} \underbrace{b^{-1}d}_{\in N}\underbrace{(d^{-1}(a^{-1}c)d)}_{\in N \ (Why?)} \in N$$

(ii) associativity: Let $a, b, c \in G$. Then

$$(aNbN)cN = abNcN = (ab)cN = a(bc)N = aNbcN = aN(bNcN).$$

(iii) identity:

The set of left cosets of a normal subgroup forms a group

Theorem 11

If N is a normal subgroup of G, then the set of left cosets of N forms a group under the coset multiplication given by $aNbN = abN$ for $a, b \in G$.

(i) well-defined: Let $a, b, c, d \in G$. If $aN = cN$ and $bN = dN$, then

$a^{-1}c \in N$ and $b^{-1}d \in N$. (Why?) [Proposition 1]

To show $abN = cdN$. It suffices to show $(ab)^{-1}cd \in N$. (Why?)

$$(ab)^{-1}cd = b^{-1}(a^{-1}c)d \overset{!}{=} \underbrace{b^{-1}d}_{\in N}\underbrace{(d^{-1}(a^{-1}c)d)}_{\in N\ (Why?)} \in N$$

(ii) associativity: Let $a, b, c \in G$. Then

$$(aNbN)cN = abNcN = (ab)cN = a(bc)N = aNbcN = aN(bNcN).$$

(iii) identity: N is an identity element. Since $N = eN$, for all $a \in G$,

The set of left cosets of a normal subgroup forms a group

Theorem 11

If N is a normal subgroup of G, then the set of left cosets of N forms a group under the coset multiplication given by $aNbN = abN$ for $a, b \in G$.

(i) well-defined: Let $a, b, c, d \in G$. If $aN = cN$ and $bN = dN$, then

$a^{-1}c \in N$ and $b^{-1}d \in N$. (Why?) [Proposition 1]

To show $abN = cdN$. It suffices to show $(ab)^{-1}cd \in N$. (Why?)

$$(ab)^{-1}cd = b^{-1}(a^{-1}c)d \overset{!}{=} \underbrace{b^{-1}d}_{\in N}\underbrace{(d^{-1}(a^{-1}c)d)}_{\in N\ (Why?)} \in N$$

(ii) associativity: Let $a, b, c \in G$. Then

$$(aNbN)cN = abNcN = (ab)cN = a(bc)N = aNbcN = aN(bNcN).$$

(iii) identity: N is an identity element. Since $N = eN$, for all $a \in G$,

$$eNaN = eaN = aN \quad \text{and} \quad aNeN = aeN = aN.$$

(iv) inverses:

The set of left cosets of a normal subgroup forms a group

Theorem 11

If N is a normal subgroup of G, then the set of left cosets of N forms a group under the coset multiplication given by $aNbN = abN$ for $a, b \in G$.

(i) well-defined: Let $a, b, c, d \in G$. If $aN = cN$ and $bN = dN$, then

$a^{-1}c \in N$ and $b^{-1}d \in N$. (Why?) [Proposition 1]

To show $abN = cdN$. It suffices to show $(ab)^{-1}cd \in N$. (Why?)

$$(ab)^{-1}cd = b^{-1}(a^{-1}c)d \overset{!}{=} \underbrace{b^{-1}d}_{\in N}\underbrace{(d^{-1}(a^{-1}c)d)}_{\in N\ (Why?)} \in N$$

(ii) associativity: Let $a, b, c \in G$. Then

$$(aNbN)cN = abNcN = (ab)cN = a(bc)N = aNbcN = aN(bNcN).$$

(iii) identity: N is an identity element. Since $N = eN$, for all $a \in G$,

$$eNaN = eaN = aN \quad \text{and} \quad aNeN = aeN = aN.$$

(iv) inverses: The inverse of aN is $a^{-1}N$.

The set of left cosets of a normal subgroup forms a group

Theorem 11

If N is a normal subgroup of G, then the set of left cosets of N forms a group under the coset multiplication given by $aNbN = abN$ for $a, b \in G$.

(i) well-defined: Let $a, b, c, d \in G$. If $aN = cN$ and $bN = dN$, then

$$a^{-1}c \in N \text{ and } b^{-1}d \in N. \text{ (Why?) [Proposition 1]}$$

To show $abN = cdN$. It suffices to show $(ab)^{-1}cd \in N$. (Why?)

$$(ab)^{-1}cd = b^{-1}(a^{-1}c)d \stackrel{!}{=} \underbrace{b^{-1}d}_{\in N}\underbrace{(d^{-1}(a^{-1}c)d)}_{\in N \ (Why?)} \in N$$

(ii) associativity: Let $a, b, c \in G$. Then

$$(aNbN)cN = abNcN = (ab)cN = a(bc)N = aNbcN = aN(bNcN).$$

(iii) identity: N is an identity element. Since $N = eN$, for all $a \in G$,

$$eNaN = eaN = aN \quad \text{and} \quad aNeN = aeN = aN.$$

(iv) inverses: The inverse of aN is $a^{-1}N$.

$$aNa^{-1}N = eN = N \quad \text{and} \quad a^{-1}NaN = eN = N.$$

Factor group

Definition 12

If N is a normal subgroup of G, then the group of left cosets of N in G is called the **factor group** of G determined by N. It will be denoted by G/N.

Example 13 (Order of an element in G/N)

Factor group

Definition 12

If N is a normal subgroup of G, then the group of left cosets of N in G is called the **factor group** of G determined by N. It will be denoted by G/N.

Example 13 (Order of an element in G/N)

Let N be a normal subgroup of the finite group G. If $a \in G$, then the order of aN is the smallest positive integer n such that

$$(aN)^n = a^n N = N.$$

Factor group

Definition 12

If N is a normal subgroup of G, then the group of left cosets of N in G is called the **factor group** of G determined by N. It will be denoted by G/N.

Example 13 (Order of an element in G/N)

Let N be a normal subgroup of the finite group G. If $a \in G$, then the order of aN is the smallest positive integer n such that

$$(aN)^n = a^n N = N.$$

That is, the order of aN is the smallest positive integer n such that $a^n \in N$.

Factor group

Definition 12

If N is a normal subgroup of G, then the group of left cosets of N in G is called the **factor group** of G determined by N. It will be denoted by G/N.

Example 13 (Order of an element in G/N)

Let N be a normal subgroup of the finite group G. If $a \in G$, then the order of aN is the smallest positive integer n such that

$$(aN)^n = a^n N = N.$$

That is, the order of aN is the smallest positive integer n such that $a^n \in N$.

Let N be a normal subgroup of G. The mapping $\pi : G \to G/N$ defined by

$$\pi(x) = xN, \text{ for all } x \in G,$$

Factor group

Definition 12

If N is a normal subgroup of G, then the group of left cosets of N in G is called the **factor group** of G determined by N. It will be denoted by G/N.

Example 13 (Order of an element in G/N)

Let N be a normal subgroup of the finite group G. If $a \in G$, then the order of aN is the smallest positive integer n such that

$$(aN)^n = a^n N = N.$$

That is, the order of aN is the smallest positive integer n such that $a^n \in N$.

Let N be a normal subgroup of G. The mapping $\pi : G \to G/N$ defined by

$$\pi(x) = xN, \text{ for all } x \in G,$$

is called the **natural projection** of G onto G/N.

Properties of the *natural projection* $\pi : G \to G/N$

Note 5 (Proposition 6 in §3.7)

Properties of the *natural projection* $\pi : G \to G/N$

Note 5 (Proposition 6 in §3.7)

The kernel of any group homomorphism is a normal subgroup.

The first part of the next proposition shows that the converse is true:

Properties of the *natural projection* $\pi : G \to G/N$

Note 5 (Proposition 6 in §3.7)

The kernel of any group homomorphism is a normal subgroup.

The first part of the next proposition shows that the converse is true:

Any normal subgroup is the kernel of some group homomorphism.

Proposition 4 (Let N be a normal subgroup of G.)

Properties of the *natural projection* $\pi : G \to G/N$

Note 5 (Proposition 6 in §3.7)

The kernel of any group homomorphism is a normal subgroup.

The first part of the next proposition shows that the converse is true:

Any normal subgroup is the kernel of some group homomorphism.

Proposition 4 (Let N be a normal subgroup of G.)

(a) *The natural projection* $\pi : G \to G/N$ *defined by* $\pi(x) = xN$, *for all* $x \in G$, *is a group homomorphism, and* $\ker(\pi) = N$.

Properties of the *natural projection* $\pi : G \to G/N$

Note 5 (Proposition 6 in §3.7)

The kernel of any group homomorphism is a normal subgroup.

The first part of the next proposition shows that the converse is true:

Any normal subgroup is the kernel of some group homomorphism.

Proposition 4 (Let N be a normal subgroup of G.)

(a) *The natural projection $\pi : G \to G/N$ defined by $\pi(x) = xN$, for all $x \in G$, is a group homomorphism, and $\ker(\pi) = N$.*

(b) *There is a one-to-one correspondence between*

$$\{\textit{subgroups } K \textit{ of } G/N\} \quad \longleftrightarrow \quad \{\textit{subgroups } H \textit{ of } G \textit{ with } H \supseteq N\}$$

Properties of the *natural projection* $\pi : G \to G/N$

Note 5 (Proposition 6 in §3.7)

The kernel of any group homomorphism is a normal subgroup.

The first part of the next proposition shows that the converse is true:

Any normal subgroup is the kernel of some group homomorphism.

Proposition 4 (Let N be a normal subgroup of G.)

(a) *The natural projection $\pi : G \to G/N$ defined by $\pi(x) = xN$, for all $x \in G$, is a group homomorphism, and $\ker(\pi) = N$.*

(b) *There is a one-to-one correspondence between*

$$\{\textit{subgroups } K \textit{ of } G/N\} \quad \longleftrightarrow \quad \{\textit{subgroups } H \textit{ of } G \textit{ with } H \supseteq N\}$$

If K is a subgroup of G/N, then $\pi^{-1}(K)$ is the corresponding subgroup of G;

Properties of the *natural projection* $\pi : G \to G/N$

Note 5 (Proposition 6 in §3.7)

The kernel of any group homomorphism is a normal subgroup.

The first part of the next proposition shows that the converse is true:

Any normal subgroup is the kernel of some group homomorphism.

Proposition 4 (Let N be a normal subgroup of G.)

(a) *The natural projection $\pi : G \to G/N$ defined by $\pi(x) = xN$, for all $x \in G$, is a group homomorphism, and $\ker(\pi) = N$.*

(b) *There is a one-to-one correspondence between*

$$\{\textit{subgroups } K \textit{ of } G/N\} \quad \longleftrightarrow \quad \{\textit{subgroups } H \textit{ of } G \textit{ with } H \supseteq N\}$$

If K is a subgroup of G/N, then $\pi^{-1}(K)$ is the corresponding subgroup of G;
If H is subgroup of G with $H \supseteq N$, then $\pi(H)$ is the corresponding subgroup of G/N.

Properties of the *natural projection* $\pi : G \to G/N$

Note 5 (Proposition 6 in §3.7)

The kernel of any group homomorphism is a normal subgroup.

The first part of the next proposition shows that the converse is true:

Any normal subgroup is the kernel of some group homomorphism.

Proposition 4 (Let N be a normal subgroup of G.)

(a) *The natural projection $\pi : G \to G/N$ defined by $\pi(x) = xN$, for all $x \in G$, is a group homomorphism, and $\ker(\pi) = N$.*

(b) *There is a one-to-one correspondence between*

$$\{\text{subgroups } K \text{ of } G/N\} \quad \longleftrightarrow \quad \{\text{subgroups } H \text{ of } G \text{ with } H \supseteq N\}$$

If K is a subgroup of G/N, then $\pi^{-1}(K)$ is the corresponding subgroup of G;
If H is subgroup of G with $H \supseteq N$, then $\pi(H)$ is the corresponding subgroup of G/N.
Under this correspondence, normal subgroups $\longleftrightarrow$ normal subgroups.

Proof of Proposition 4: natural projection $\pi : G \to G/N$

(a) π is a homomorphism:

Proof of Proposition 4: natural projection $\pi : G \to G/N$

(a) π is a homomorphism: $\pi(ab) = abN = aNbN = \pi(a)\pi(b)$ for $a, b \in G$.

Proof of Proposition 4: natural projection $\pi : G \to G/N$

(a) π is a homomorphism: $\pi(ab) = abN = aNbN = \pi(a)\pi(b)$ for $a, b \in G$.
$a \in \ker(\pi) \Leftrightarrow \pi(a) = aN = N \Leftrightarrow a \in N$. That is,

Proof of Proposition 4: natural projection $\pi : G \to G/N$

(a) π is a homomorphism: $\pi(ab) = abN = aNbN = \pi(a)\pi(b)$ for $a, b \in G$.
$a \in \ker(\pi) \Leftrightarrow \pi(a) = aN = N \Leftrightarrow a \in N$. That is, $\ker(\pi) = N$.

(b) Using **Proposition 7 in §3.7:**

Proof of Proposition 4: natural projection $\pi : G \to G/N$

(a) π is a homomorphism: $\pi(ab) = abN = aNbN = \pi(a)\pi(b)$ for $a, b \in G$.
$a \in \ker(\pi) \Leftrightarrow \pi(a) = aN = N \Leftrightarrow a \in N$. That is, $\ker(\pi) = N$.

(b) Using **Proposition 7 in §3.7:** Let $\phi : G_1 \to G_2$ be a homomorphism.

(1) If H_1 is a subgroup of G_1, then $\phi(H_1)$ is a subgroup of G_2.
If ϕ is onto and H_1 is normal in G_1, then $\phi(H_1)$ is normal in G_2.

(2) If H_2 is a subgroup of G_2, then $\phi^{-1}(H_2)$ is a subgroup of G_1.
If H_2 is a normal in G_2, then $\phi^{-1}(H_2)$ is normal in G_1.

Proof of Proposition 4: natural projection $\pi : G \to G/N$

(a) π is a homomorphism: $\pi(ab) = abN = aNbN = \pi(a)\pi(b)$ for $a, b \in G$.
$a \in \ker(\pi) \Leftrightarrow \pi(a) = aN = N \Leftrightarrow a \in N$. That is, $\ker(\pi) = N$.

(b) Using **Proposition 7 in §3.7:** Let $\phi : G_1 \to G_2$ be a homomorphism.

(1) If H_1 is a subgroup of G_1, then $\phi(H_1)$ is a subgroup of G_2.
If ϕ is onto and H_1 is normal in G_1, then $\phi(H_1)$ is normal in G_2.

(2) If H_2 is a subgroup of G_2, then $\phi^{-1}(H_2)$ is a subgroup of G_1.
If H_2 is a normal in G_2, then $\phi^{-1}(H_2)$ is normal in G_1.

If K is a subgroup of G/N, then $\pi^{-1}(K)$ is a subgroup of G that contains N, and

Proof of Proposition 4: natural projection $\pi : G \to G/N$

(a) π is a homomorphism: $\pi(ab) = abN = aNbN = \pi(a)\pi(b)$ for $a, b \in G$.
$a \in \ker(\pi) \Leftrightarrow \pi(a) = aN = N \Leftrightarrow a \in N$. That is, $\ker(\pi) = N$.

(b) Using **Proposition 7 in §3.7:** Let $\phi : G_1 \to G_2$ be a homomorphism.

(1) If H_1 is a subgroup of G_1, then $\phi(H_1)$ is a subgroup of G_2.
If ϕ is onto and H_1 is normal in G_1, then $\phi(H_1)$ is normal in G_2.

(2) If H_2 is a subgroup of G_2, then $\phi^{-1}(H_2)$ is a subgroup of G_1.
If H_2 is a normal in G_2, then $\phi^{-1}(H_2)$ is normal in G_1.

If K is a subgroup of G/N, then $\pi^{-1}(K)$ is a subgroup of G that contains N, and if K is normal, then so is $\pi^{-1}(K)$.(Why?)[

Proof of Proposition 4: natural projection $\pi : G \to G/N$

(a) π is a homomorphism: $\pi(ab) = abN = aNbN = \pi(a)\pi(b)$ for $a, b \in G$.
$a \in \ker(\pi) \Leftrightarrow \pi(a) = aN = N \Leftrightarrow a \in N$. That is, $\ker(\pi) = N$.

(b) Using **Proposition 7 in §3.7:** Let $\phi : G_1 \to G_2$ be a homomorphism.

(1) If H_1 is a subgroup of G_1, then $\phi(H_1)$ is a subgroup of G_2.
If ϕ is onto and H_1 is normal in G_1, then $\phi(H_1)$ is normal in G_2.

(2) If H_2 is a subgroup of G_2, then $\phi^{-1}(H_2)$ is a subgroup of G_1.
If H_2 is a normal in G_2, then $\phi^{-1}(H_2)$ is normal in G_1.

If K is a subgroup of G/N, then $\pi^{-1}(K)$ is a subgroup of G that contains N, and if K is normal, then so is $\pi^{-1}(K)$.(Why?)[Proposition 7 in §3.7 (2)]

Goal:

Proof of Proposition 4: natural projection $\pi : G \to G/N$

(a) π is a homomorphism: $\pi(ab) = abN = aNbN = \pi(a)\pi(b)$ for $a, b \in G$.
$a \in \ker(\pi) \Leftrightarrow \pi(a) = aN = N \Leftrightarrow a \in N$. That is, $\ker(\pi) = N$.

(b) Using **Proposition 7 in §3.7:** Let $\phi : G_1 \to G_2$ be a homomorphism.

(1) If H_1 is a subgroup of G_1, then $\phi(H_1)$ is a subgroup of G_2.
If ϕ is onto and H_1 is normal in G_1, then $\phi(H_1)$ is normal in G_2.

(2) If H_2 is a subgroup of G_2, then $\phi^{-1}(H_2)$ is a subgroup of G_1.
If H_2 is a normal in G_2, then $\phi^{-1}(H_2)$ is normal in G_1.

If K is a subgroup of G/N, then $\pi^{-1}(K)$ is a subgroup of G that contains N, and if K is normal, then so is $\pi^{-1}(K)$.(Why?)[Proposition 7 in §3.7 (2)]

Goal: There is a one-to-one correspondence between

$$\{\text{subgroups } K \text{ of } G/N\} \quad \longleftrightarrow \quad \{\text{subgroups } H \text{ of } G \text{ with } H \supseteq N\}$$

Proof of Proposition 4 (b) cont.: $\pi : G \to G/N$

Goal: There is a one-to-one correspondence between

$$\{\text{subgroups } K \text{ of } G/N\} \quad \longleftrightarrow \quad \{\text{subgroups } H \text{ of } G \text{ with } H \supseteq N\}$$

Proof of Proposition 4 (b) cont.: $\pi : G \to G/N$

Goal: There is a one-to-one correspondence between

$$\{\text{subgroups } K \text{ of } G/N\} \quad \longleftrightarrow \quad \{\text{subgroups } H \text{ of } G \text{ with } H \supseteq N\}$$

Assigning to each subgroup K of G/N its inverse image $\pi^{-1}(K)$ in G is a one-to-one mapping.(Why?) [

Proof of Proposition 4 (b) cont.: $\pi : G \to G/N$

Goal: There is a one-to-one correspondence between

$$\{\text{subgroups } K \text{ of } G/N\} \quad \longleftrightarrow \quad \{\text{subgroups } H \text{ of } G \text{ with } H \supseteq N\}$$

Assigning to each subgroup K of G/N its inverse image $\pi^{-1}(K)$ in G is a one-to-one mapping.(Why?) [π is onto] *To show* that this mapping is onto.

Proof of Proposition 4 (b) cont.: $\pi : G \to G/N$

Goal: There is a one-to-one correspondence between

$$\{\text{subgroups } K \text{ of } G/N\} \quad \longleftrightarrow \quad \{\text{subgroups } H \text{ of } G \text{ with } H \supseteq N\}$$

Assigning to each subgroup K of G/N its inverse image $\pi^{-1}(K)$ in G is a one-to-one mapping.(Why?) [π is onto] *To show* that this mapping is onto. Let H be a subgroup of G with $H \supseteq N$. **Claim:** $H = \pi^{-1}(\pi(H))$.

Proof of Proposition 4 (b) cont.: $\pi : G \to G/N$

Goal: There is a one-to-one correspondence between

$$\{\text{subgroups } K \text{ of } G/N\} \quad \longleftrightarrow \quad \{\text{subgroups } H \text{ of } G \text{ with } H \supseteq N\}$$

Assigning to each subgroup K of G/N its inverse image $\pi^{-1}(K)$ in G is a one-to-one mapping.(Why?) [π is onto] *To show* that this mapping is onto. Let H be a subgroup of G with $H \supseteq N$. **Claim:** $H = \pi^{-1}(\pi(H))$.

$$\pi^{-1}(\pi(H)) = \{x \in G \mid \pi(x) \in \pi(H)\} \Rightarrow H \subseteq \pi^{-1}(\pi(H))$$

To show $\pi^{-1}(\pi(H)) \subseteq H$:

Proof of Proposition 4 (b) cont.: $\pi : G \to G/N$

Goal: There is a one-to-one correspondence between

$$\{\text{subgroups } K \text{ of } G/N\} \quad \longleftrightarrow \quad \{\text{subgroups } H \text{ of } G \text{ with } H \supseteq N\}$$

Assigning to each subgroup K of G/N its inverse image $\pi^{-1}(K)$ in G is a one-to-one mapping.(Why?) [π is onto] *To show* that this mapping is onto. Let H be a subgroup of G with $H \supseteq N$. **Claim:** $H = \pi^{-1}(\pi(H))$.

$$\pi^{-1}(\pi(H)) = \{x \in G \mid \pi(x) \in \pi(H)\} \Rightarrow H \subseteq \pi^{-1}(\pi(H))$$

To show $\pi^{-1}(\pi(H)) \subseteq H$: Let $a \in \pi^{-1}(\pi(H))$.

Proof of Proposition 4 (b) cont.: $\pi : G \to G/N$

Goal: There is a one-to-one correspondence between

$$\{\text{subgroups } K \text{ of } G/N\} \quad \longleftrightarrow \quad \{\text{subgroups } H \text{ of } G \text{ with } H \supseteq N\}$$

Assigning to each subgroup K of G/N its inverse image $\pi^{-1}(K)$ in G is a one-to-one mapping.(Why?) [π is onto] *To show* that this mapping is onto. Let H be a subgroup of G with $H \supseteq N$. **Claim:** $H = \pi^{-1}(\pi(H))$.

$$\pi^{-1}(\pi(H)) = \{x \in G \mid \pi(x) \in \pi(H)\} \Rightarrow H \subseteq \pi^{-1}(\pi(H))$$

To show $\pi^{-1}(\pi(H)) \subseteq H$: Let $a \in \pi^{-1}(\pi(H))$. Then $\pi(a) \in \pi(H)$, and so

Proof of Proposition 4 (b) cont.: $\pi : G \to G/N$

Goal: There is a one-to-one correspondence between

$$\{\text{subgroups } K \text{ of } G/N\} \quad \longleftrightarrow \quad \{\text{subgroups } H \text{ of } G \text{ with } H \supseteq N\}$$

Assigning to each subgroup K of G/N its inverse image $\pi^{-1}(K)$ in G is a one-to-one mapping.(Why?) [π is onto] *To show* that this mapping is onto. Let H be a subgroup of G with $H \supseteq N$. **Claim:** $H = \pi^{-1}(\pi(H))$.

$$\pi^{-1}(\pi(H)) = \{x \in G \mid \pi(x) \in \pi(H)\} \Rightarrow H \subseteq \pi^{-1}(\pi(H))$$

To show $\pi^{-1}(\pi(H)) \subseteq H$: Let $a \in \pi^{-1}(\pi(H))$. Then $\pi(a) \in \pi(H)$, and so

$$aN = hN \text{ for some } h \in H. \text{ This implies that } h^{-1}a \in N.$$

Proof of Proposition 4 (b) cont.: $\pi : G \to G/N$

Goal: There is a one-to-one correspondence between

$$\{\text{subgroups } K \text{ of } G/N\} \quad \longleftrightarrow \quad \{\text{subgroups } H \text{ of } G \text{ with } H \supseteq N\}$$

Assigning to each subgroup K of G/N its inverse image $\pi^{-1}(K)$ in G is a one-to-one mapping.(Why?) [π is onto] *To show* that this mapping is onto. Let H be a subgroup of G with $H \supseteq N$. **Claim:** $H = \pi^{-1}(\pi(H))$.

$$\pi^{-1}(\pi(H)) = \{x \in G \mid \pi(x) \in \pi(H)\} \Rightarrow H \subseteq \pi^{-1}(\pi(H))$$

To show $\pi^{-1}(\pi(H)) \subseteq H$: Let $a \in \pi^{-1}(\pi(H))$. Then $\pi(a) \in \pi(H)$, and so

$aN = hN$ for some $h \in H$. This implies that $h^{-1}a \in N$.

It follows from $N \subseteq H$ that $h^{-1}a \in H$,and so

Proof of Proposition 4 (b) cont.: $\pi : G \to G/N$

Goal: There is a one-to-one correspondence between

$$\{\text{subgroups } K \text{ of } G/N\} \quad \longleftrightarrow \quad \{\text{subgroups } H \text{ of } G \text{ with } H \supseteq N\}$$

Assigning to each subgroup K of G/N its inverse image $\pi^{-1}(K)$ in G is a one-to-one mapping.(Why?) [π is onto] *To show* that this mapping is onto. Let H be a subgroup of G with $H \supseteq N$. **Claim:** $H = \pi^{-1}(\pi(H))$.

$$\pi^{-1}(\pi(H)) = \{x \in G \mid \pi(x) \in \pi(H)\} \Rightarrow H \subseteq \pi^{-1}(\pi(H))$$

To show $\pi^{-1}(\pi(H)) \subseteq H$: Let $a \in \pi^{-1}(\pi(H))$. Then $\pi(a) \in \pi(H)$, and so

$$aN = hN \text{ for some } h \in H. \text{ This implies that } h^{-1}a \in N.$$

It follows from $N \subseteq H$ that $h^{-1}a \in H$,and so $a = h(h^{-1}a) \in H$. $\square_{\text{claim}}$

Proof of Proposition 4 (b) cont.: $\pi : G \to G/N$

Goal: There is a one-to-one correspondence between

$$\{\text{subgroups } K \text{ of } G/N\} \quad \longleftrightarrow \quad \{\text{subgroups } H \text{ of } G \text{ with } H \supseteq N\}$$

Assigning to each subgroup K of G/N its inverse image $\pi^{-1}(K)$ in G is a one-to-one mapping.(Why?) [π is onto] *To show* that this mapping is onto. Let H be a subgroup of G with $H \supseteq N$. **Claim:** $H = \pi^{-1}(\pi(H))$.

$$\pi^{-1}(\pi(H)) = \{x \in G \mid \pi(x) \in \pi(H)\} \Rightarrow H \subseteq \pi^{-1}(\pi(H))$$

To show $\pi^{-1}(\pi(H)) \subseteq H$: Let $a \in \pi^{-1}(\pi(H))$. Then $\pi(a) \in \pi(H)$, and so

$$aN = hN \text{ for some } h \in H. \text{ This implies that } h^{-1}a \in N.$$

It follows from $N \subseteq H$ that $h^{-1}a \in H$,and so $a = h(h^{-1}a) \in H$. $\square_{\text{claim}}$
Thus, this completes the proof of "**Goal**".

Proof of Proposition 4 (b) cont.: $\pi : G \to G/N$

Goal: There is a one-to-one correspondence between

$$\{\text{subgroups } K \text{ of } G/N\} \quad \longleftrightarrow \quad \{\text{subgroups } H \text{ of } G \text{ with } H \supseteq N\}$$

Assigning to each subgroup K of G/N its inverse image $\pi^{-1}(K)$ in G is a one-to-one mapping.(Why?) [π is onto] *To show* that this mapping is onto. Let H be a subgroup of G with $H \supseteq N$. **Claim:** $H = \pi^{-1}(\pi(H))$.

$$\pi^{-1}(\pi(H)) = \{x \in G \mid \pi(x) \in \pi(H)\} \Rightarrow H \subseteq \pi^{-1}(\pi(H))$$

To show $\pi^{-1}(\pi(H)) \subseteq H$: Let $a \in \pi^{-1}(\pi(H))$. Then $\pi(a) \in \pi(H)$, and so

$aN = hN$ for some $h \in H$. This implies that $h^{-1}a \in N$.

It follows from $N \subseteq H$ that $h^{-1}a \in H$,and so $a = h(h^{-1}a) \in H$. $\square_{\text{claim}}$
Thus, this completes the proof of "**Goal**".

If H is normal, then so is its image $\pi(H)$.(Why?) [

Proof of Proposition 4 (b) cont.: $\pi : G \to G/N$

Goal: There is a one-to-one correspondence between

$$\{\text{subgroups } K \text{ of } G/N\} \quad \longleftrightarrow \quad \{\text{subgroups } H \text{ of } G \text{ with } H \supseteq N\}$$

Assigning to each subgroup K of G/N its inverse image $\pi^{-1}(K)$ in G is a one-to-one mapping.(Why?) [π is onto] *To show* that this mapping is onto. Let H be a subgroup of G with $H \supseteq N$. **Claim:** $H = \pi^{-1}(\pi(H))$.

$$\pi^{-1}(\pi(H)) = \{x \in G \mid \pi(x) \in \pi(H)\} \Rightarrow H \subseteq \pi^{-1}(\pi(H))$$

To show $\pi^{-1}(\pi(H)) \subseteq H$: Let $a \in \pi^{-1}(\pi(H))$. Then $\pi(a) \in \pi(H)$, and so

$$aN = hN \text{ for some } h \in H. \text{ This implies that } h^{-1}a \in N.$$

It follows from $N \subseteq H$ that $h^{-1}a \in H$,and so $a = h(h^{-1}a) \in H$. $\square_{\text{claim}}$
Thus, this completes the proof of "**Goal**".

If H is normal, then so is its image $\pi(H)$.(Why?) [Proposition 7 in §3.7 (1)]

Example

Let $G = \mathbf{Z}_{12}$, and let $N = \{[0],[3],[6],[9]\} = \langle [3] \rangle$. N is normal. (Why?)

Example

Let $G = \mathbf{Z}_{12}$, and let $N = \{[0], [3], [6], [9]\} = \langle [3] \rangle$. N is normal. (Why?)

Then there are three elements of G/N. (Check it!) **[Algorithm:]**
(0)

Example

Let $G = \mathbf{Z}_{12}$, and let $N = \{[0], [3], [6], [9]\} = \langle [3] \rangle$. N is normal. (Why?)

Then there are three elements of G/N. (Check it!) **[Algorithm:]**
(0) The first element is N;
(1)

Example

Let $G = \mathbf{Z}_{12}$, and let $N = \{[0], [3], [6], [9]\} = \langle [3] \rangle$. N is normal. (Why?)

Then there are three elements of G/N. (Check it!) **[Algorithm:]**
(0) The first element is N;
(1) Choose $[1] \notin N$, we obtain $[1] + N = \{[1], [4], [7], [10]\}$;
(2)

Example

Let $G = \mathbf{Z}_{12}$, and let $N = \{[0], [3], [6], [9]\} = \langle [3] \rangle$. N is normal. (Why?)

Then there are three elements of G/N. (Check it!) **[Algorithm:]**
(0) The first element is N;
(1) Choose $[1] \notin N$, we obtain $[1] + N = \{[1], [4], [7], [10]\}$;
(2) Choose $[2] \notin \{N, [1] + N\}$, we obtain $[2] + N = \{[2], [5], [8], [11]\}$.

Example

Let $G = \mathbf{Z}_{12}$, and let $N = \{[0], [3], [6], [9]\} = \langle [3] \rangle$. N is normal. (Why?)

Then there are three elements of G/N. (Check it!) **[Algorithm:]**
(0) The first element is N;
(1) Choose $[1] \notin N$, we obtain $[1] + N = \{[1], [4], [7], [10]\}$;
(2) Choose $[2] \notin \{N, [1] + N\}$, we obtain $[2] + N = \{[2], [5], [8], [11]\}$.

Since the factor group G/N has order 3, we have $G/N \cong \mathbf{Z}_3$. (Why?)

Example

Let $G = \mathbf{Z}_{12}$, and let $N = \{[0], [3], [6], [9]\} = \langle [3] \rangle$. N is normal. (Why?)

Then there are three elements of G/N. (Check it!) **[Algorithm:]**
(0) The first element is N;
(1) Choose $[1] \notin N$, we obtain $[1] + N = \{[1], [4], [7], [10]\}$;
(2) Choose $[2] \notin \{N, [1] + N\}$, we obtain $[2] + N = \{[2], [5], [8], [11]\}$.

Since the factor group G/N has order 3, we have $G/N \cong \mathbf{Z}_3$. (Why?)

This can also be seen by considering the order of $[1] + N$. (see Example 13)

Example

Let $G = \mathbf{Z}_{12}$, and let $N = \{[0], [3], [6], [9]\} = \langle [3] \rangle$. N is normal. (Why?)

Then there are three elements of G/N. (Check it!) **[Algorithm:]**
(0) The first element is N;
(1) Choose $[1] \notin N$, we obtain $[1] + N = \{[1], [4], [7], [10]\}$;
(2) Choose $[2] \notin \{N, [1] + N\}$, we obtain $[2] + N = \{[2], [5], [8], [11]\}$.

Since the factor group G/N has order 3, we have $G/N \cong \mathbf{Z}_3$. (Why?)

This can also be seen by considering the order of $[1] + N$. (see Example 13)

Its order is the smallest positive multiple that gives the identity element of G/N, and so that is

Example

Let $G = \mathbf{Z}_{12}$, and let $N = \{[0], [3], [6], [9]\} = \langle [3] \rangle$. N is normal. (Why?)

Then there are three elements of G/N. (Check it!) **[Algorithm:]**
(0) The first element is N;
(1) Choose $[1] \notin N$, we obtain $[1] + N = \{[1], [4], [7], [10]\}$;
(2) Choose $[2] \notin \{N, [1] + N\}$, we obtain $[2] + N = \{[2], [5], [8], [11]\}$.

Since the factor group G/N has order 3, we have $G/N \cong \mathbf{Z}_3$. (Why?)

This can also be seen by considering the order of $[1] + N$. (see Example 13)

Its order is the smallest positive multiple that gives the identity element of G/N, and so that is the smallest positive multiple of $[1]$ that belongs to N.

Example

Let $G = \mathbf{Z}_{12}$, and let $N = \{[0], [3], [6], [9]\} = \langle [3] \rangle$. N is normal. (Why?)

Then there are three elements of G/N. (Check it!) **[Algorithm:]**
(0) The first element is N;
(1) Choose $[1] \notin N$, we obtain $[1] + N = \{[1], [4], [7], [10]\}$;
(2) Choose $[2] \notin \{N, [1] + N\}$, we obtain $[2] + N = \{[2], [5], [8], [11]\}$.

Since the factor group G/N has order 3, we have $G/N \cong \mathbf{Z}_3$. (Why?)

This can also be seen by considering the order of $[1] + N$. (see Example 13)

Its order is the smallest positive multiple that gives the identity element of G/N, and so that is the smallest positive multiple of $[1]$ that belongs to N.

Thus, $[1]$ has order 3. That is,

Example

Let $G = \mathbf{Z}_{12}$, and let $N = \{[0], [3], [6], [9]\} = \langle [3] \rangle$. N is normal. (Why?)

Then there are three elements of G/N. (Check it!) **[Algorithm:]**
(0) The first element is N;
(1) Choose $[1] \notin N$, we obtain $[1] + N = \{[1], [4], [7], [10]\}$;
(2) Choose $[2] \notin \{N, [1] + N\}$, we obtain $[2] + N = \{[2], [5], [8], [11]\}$.

Since the factor group G/N has order 3, we have $G/N \cong \mathbf{Z}_3$. (Why?)

This can also be seen by considering the order of $[1] + N$. (see Example 13)

Its order is the smallest positive multiple that gives the identity element of G/N, and so that is the smallest positive multiple of [1] that belongs to N.

$$\text{Thus, } [1] \text{ has order } 3. \text{ That is, } G/N = \langle [1] + N \rangle \cong \mathbf{Z}_3.$$

H is normal if and only if its left and right cosets coincide

Proposition 5 (Let H be a subgroup of the group G.)

The following conditions are equivalent:

H is normal if and only if its left and right cosets coincide

Proposition 5 (Let H be a subgroup of the group G.)

The following conditions are equivalent:

(1) *H is a normal subgroup of G;*

(2) *$aH = Ha$ for all $a \in G$;*

(3) *for all $a, b \in G$, abH is the set theoretic product $(aH)(bH)$;*

(4) *for all $a, b \in G$, $ab^{-1} \in H$ if and only if $a^{-1}b \in H$.*

$(1) \Rightarrow (2)$:

H is normal if and only if its left and right cosets coincide

Proposition 5 (Let H be a subgroup of the group G.)

The following conditions are equivalent:

(1) *H is a normal subgroup of G;*

(2) *$aH = Ha$ for all $a \in G$;*

(3) *for all $a, b \in G$, abH is the set theoretic product $(aH)(bH)$;*

(4) *for all $a, b \in G$, $ab^{-1} \in H$ if and only if $a^{-1}b \in H$.*

(1) $\Rightarrow$ (2): Let $a \in G$. *To show* that $aH \subseteq Ha$, let $h \in H$. Then

H is normal if and only if its left and right cosets coincide

Proposition 5 (Let H be a subgroup of the group G.)

The following conditions are equivalent:

(1) *H is a normal subgroup of G;*

(2) *$aH = Ha$ for all $a \in G$;*

(3) *for all $a, b \in G$, abH is the set theoretic product $(aH)(bH)$;*

(4) *for all $a, b \in G$, $ab^{-1} \in H$ if and only if $a^{-1}b \in H$.*

(1) $\Rightarrow$ (2): Let $a \in G$. *To show* that $aH \subseteq Ha$, let $h \in H$. Then

$aha^{-1} \in H$ (Why?) and so

H is normal if and only if its left and right cosets coincide

Proposition 5 (Let H be a subgroup of the group G.)

The following conditions are equivalent:

(1) *H is a normal subgroup of G;*

(2) *$aH = Ha$ for all $a \in G$;*

(3) *for all $a, b \in G$, abH is the set theoretic product $(aH)(bH)$;*

(4) *for all $a, b \in G$, $ab^{-1} \in H$ if and only if $a^{-1}b \in H$.*

(1) $\Rightarrow$ (2): Let $a \in G$. *To show* that $aH \subseteq Ha$, let $h \in H$. Then

$$aha^{-1} \in H \text{ (Why?) and so } aha^{-1} = h' \text{ for some } h' \in H.$$

H is normal if and only if its left and right cosets coincide

Proposition 5 (Let H be a subgroup of the group G.)

The following conditions are equivalent:

(1) *H is a normal subgroup of G;*

(2) *$aH = Ha$ for all $a \in G$;*

(3) *for all $a, b \in G$, abH is the set theoretic product $(aH)(bH)$;*

(4) *for all $a, b \in G$, $ab^{-1} \in H$ if and only if $a^{-1}b \in H$.*

(1) $\Rightarrow$ (2): Let $a \in G$. *To show* that $aH \subseteq Ha$, let $h \in H$. Then

$$aha^{-1} \in H \text{ (Why?) and so } aha^{-1} = h' \text{ for some } h' \in H.$$

Thus $ah = h'a \in Ha$.

H is normal if and only if its left and right cosets coincide

Proposition 5 (Let H be a subgroup of the group G.)

The following conditions are equivalent:

(1) *H is a normal subgroup of G;*

(2) *$aH = Ha$ for all $a \in G$;*

(3) *for all $a, b \in G$, abH is the set theoretic product $(aH)(bH)$;*

(4) *for all $a, b \in G$, $ab^{-1} \in H$ if and only if $a^{-1}b \in H$.*

(1) $\Rightarrow$ (2): Let $a \in G$. *To show* that $aH \subseteq Ha$, let $h \in H$. Then

$$aha^{-1} \in H \text{ (Why?) and so } aha^{-1} = h' \text{ for some } h' \in H.$$

Thus $ah = h'a \in Ha$. The proof of the reverse inclusion is similar. □

(2) $\Rightarrow$ (3):

H is normal if and only if its left and right cosets coincide

Proposition 5 (Let H be a subgroup of the group G.)

The following conditions are equivalent:

(1) *H is a normal subgroup of G;*

(2) *$aH = Ha$ for all $a \in G$;*

(3) *for all $a, b \in G$, abH is the set theoretic product $(aH)(bH)$;*

(4) *for all $a, b \in G$, $ab^{-1} \in H$ if and only if $a^{-1}b \in H$.*

(1) $\Rightarrow$ (2): Let $a \in G$. *To show* that $aH \subseteq Ha$, let $h \in H$. Then

$$aha^{-1} \in H \text{ (Why?) and so } aha^{-1} = h' \text{ for some } h' \in H.$$

Thus $ah = h'a \in Ha$. The proof of the reverse inclusion is similar. $\square$

(2) $\Rightarrow$ (3): $abH \subseteq (aH)(bH)$:

H is normal if and only if its left and right cosets coincide

Proposition 5 (Let H be a subgroup of the group G.)

The following conditions are equivalent:

(1) *H is a normal subgroup of G;*

(2) *$aH = Ha$ for all $a \in G$;*

(3) *for all $a, b \in G$, abH is the set theoretic product $(aH)(bH)$;*

(4) *for all $a, b \in G$, $ab^{-1} \in H$ if and only if $a^{-1}b \in H$.*

(1) $\Rightarrow$ (2): Let $a \in G$. *To show* that $aH \subseteq Ha$, let $h \in H$. Then

$$aha^{-1} \in H \text{ (Why?) and so } aha^{-1} = h' \text{ for some } h' \in H.$$

Thus $ah = h'a \in Ha$. The proof of the reverse inclusion is similar. $\square$

(2) $\Rightarrow$ (3): $abH \subseteq (aH)(bH)$: Let $h \in H$. So $abh = (ae)(bh) \in (aH)(bH)$.

$(aH)(bH) \subseteq abH$:

H is normal if and only if its left and right cosets coincide

Proposition 5 (Let H be a subgroup of the group G.)

The following conditions are equivalent:

(1) *H is a normal subgroup of G;*

(2) *$aH = Ha$ for all $a \in G$;*

(3) *for all $a, b \in G$, abH is the set theoretic product $(aH)(bH)$;*

(4) *for all $a, b \in G$, $ab^{-1} \in H$ if and only if $a^{-1}b \in H$.*

(1) $\Rightarrow$ (2): Let $a \in G$. *To show* that $aH \subseteq Ha$, let $h \in H$. Then

$$aha^{-1} \in H \text{ (Why?) and so } aha^{-1} = h' \text{ for some } h' \in H.$$

Thus $ah = h'a \in Ha$. The proof of the reverse inclusion is similar. □

(2) $\Rightarrow$ (3): $abH \subseteq (aH)(bH)$: Let $h \in H$. So $abh = (ae)(bh) \in (aH)(bH)$.

$(aH)(bH) \subseteq abH$: Let $(ah_1)(bh_2) \in (aH)(bH)$, for $h_1, h_2 \in H$. Then

H is normal if and only if its left and right cosets coincide

Proposition 5 (Let H be a subgroup of the group G.)

The following conditions are equivalent:

(1) *H is a normal subgroup of G;*

(2) *$aH = Ha$ for all $a \in G$;*

(3) *for all $a, b \in G$, abH is the set theoretic product $(aH)(bH)$;*

(4) *for all $a, b \in G$, $ab^{-1} \in H$ if and only if $a^{-1}b \in H$.*

(1) $\Rightarrow$ (2): Let $a \in G$. *To show* that $aH \subseteq Ha$, let $h \in H$. Then

$$aha^{-1} \in H \text{ (Why?) and so } aha^{-1} = h' \text{ for some } h' \in H.$$

Thus $ah = h'a \in Ha$. The proof of the reverse inclusion is similar. $\square$

(2) $\Rightarrow$ (3): $abH \subseteq (aH)(bH)$: Let $h \in H$. So $abh = (ae)(bh) \in (aH)(bH)$.
$(aH)(bH) \subseteq abH$: Let $(ah_1)(bh_2) \in (aH)(bH)$, for $h_1, h_2 \in H$. Then

$$(ah_1)(bh_2) = a(h_1 b)h_2 \stackrel{?}{=} a(bh_3)h_2 = ab(h_3 h_2) \in abH \text{ for some } h_3 \in H.$$

$\stackrel{?}{=}$ holds since

H is normal if and only if its left and right cosets coincide

Proposition 5 (Let H be a subgroup of the group G.)

The following conditions are equivalent:

(1) *H is a normal subgroup of G;*

(2) *$aH = Ha$ for all $a \in G$;*

(3) *for all $a, b \in G$, abH is the set theoretic product $(aH)(bH)$;*

(4) *for all $a, b \in G$, $ab^{-1} \in H$ if and only if $a^{-1}b \in H$.*

(1) $\Rightarrow$ (2): Let $a \in G$. *To show* that $aH \subseteq Ha$, let $h \in H$. Then

$$aha^{-1} \in H \text{ (Why?) and so } aha^{-1} = h' \text{ for some } h' \in H.$$

Thus $ah = h'a \in Ha$. The proof of the reverse inclusion is similar. □

(2) $\Rightarrow$ (3): $abH \subseteq (aH)(bH)$: Let $h \in H$. So $abh = (ae)(bh) \in (aH)(bH)$.
$(aH)(bH) \subseteq abH$: Let $(ah_1)(bh_2) \in (aH)(bH)$, for $h_1, h_2 \in H$. Then

$$(ah_1)(bh_2) = a(h_1 b)h_2 \stackrel{?}{=} a(bh_3)h_2 = ab(h_3 h_2) \in abH \text{ for some } h_3 \in H.$$

$\stackrel{?}{=}$ holds since $Hb = bH$. □

Proof of Proposition 5 cont.

Proposition 5: Let H be a subgroup of the group G. TFAE:

(1) H is a normal subgroup of G;

(2) $aH = Ha$ for all $a \in G$;

(3) for all $a, b \in G, abH = (aH)(bH)$;

(4) for all $a, b \in G, ab^{-1} \in H$ if and only if $a^{-1}b \in H$.

Proof.

(3) $\Rightarrow$ (1):

Proof of Proposition 5 cont.

Proposition 5: Let H be a subgroup of the group G. TFAE:

(1) H is a normal subgroup of G;

(2) $aH = Ha$ for all $a \in G$;

(3) for all $a, b \in G, abH = (aH)(bH)$;

(4) for all $a, b \in G, ab^{-1} \in H$ if and only if $a^{-1}b \in H$.

Proof.

(3) $\Rightarrow$ (1): For any $h \in H$ and any $a \in G$, *to show* $aha^{-1} \in H$. (Why?)

Proof of Proposition 5 cont.

Proposition 5: Let H be a subgroup of the group G. TFAE:

(1) H is a normal subgroup of G;

(2) $aH = Ha$ for all $a \in G$;

(3) for all $a, b \in G, abH = (aH)(bH)$;

(4) for all $a, b \in G, ab^{-1} \in H$ if and only if $a^{-1}b \in H$.

Proof.

(3) $\Rightarrow$ (1): For any $h \in H$ and any $a \in G$, *to show* $aha^{-1} \in H$. (Why?)
Take $b = a^{-1}$, then $(aH)(a^{-1}H) = H$. Thus,

Proof of Proposition 5 cont.

Proposition 5: Let H be a subgroup of the group G. TFAE:

(1) H is a normal subgroup of G;

(2) $aH = Ha$ for all $a \in G$;

(3) for all $a, b \in G, abH = (aH)(bH)$;

(4) for all $a, b \in G, ab^{-1} \in H$ if and only if $a^{-1}b \in H$.

Proof.

(3) $\Rightarrow$ (1): For any $h \in H$ and any $a \in G$, *to show* $aha^{-1} \in H$. (Why?)
Take $b = a^{-1}$, then $(aH)(a^{-1}H) = H$. Thus, $aha^{-1} = aha^{-1}e \in H$. $\square$

(2) $\Leftrightarrow$ (4):

Proof of Proposition 5 cont.

Proposition 5: Let H be a subgroup of the group G. TFAE:

(1) H is a normal subgroup of G;

(2) $aH = Ha$ for all $a \in G$;

(3) for all $a, b \in G, abH = (aH)(bH)$;

(4) for all $a, b \in G, ab^{-1} \in H$ if and only if $a^{-1}b \in H$.

Proof.

(3) $\Rightarrow$ (1): For any $h \in H$ and any $a \in G$, *to show* $aha^{-1} \in H$. (Why?)
Take $b = a^{-1}$, then $(aH)(a^{-1}H) = H$. Thus, $aha^{-1} = aha^{-1}e \in H$. $\square$

(2) $\Leftrightarrow$ (4): (2) holds if and only if the left and right cosets of H coincide.

Proof of Proposition 5 cont.

Proposition 5: Let H be a subgroup of the group G. TFAE:

(1) H is a normal subgroup of G;

(2) $aH = Ha$ for all $a \in G$;

(3) for all $a, b \in G, abH = (aH)(bH)$;

(4) for all $a, b \in G, ab^{-1} \in H$ if and only if $a^{-1}b \in H$.

Proof.

(3) $\Rightarrow$ (1): For any $h \in H$ and any $a \in G$, *to show* $aha^{-1} \in H$. (Why?)
Take $b = a^{-1}$, then $(aH)(a^{-1}H) = H$. Thus, $aha^{-1} = aha^{-1}e \in H$. □

(2) $\Leftrightarrow$ (4): (2) holds if and only if the left and right cosets of H coincide.
The left cosets are the equivalence classes $[a]$, where $a \sim b$ if $a^{-1}b \in H$.

Proof of Proposition 5 cont.

Proposition 5: Let H be a subgroup of the group G. TFAE:

(1) H is a normal subgroup of G;

(2) $aH = Ha$ for all $a \in G$;

(3) for all $a, b \in G, abH = (aH)(bH)$;

(4) for all $a, b \in G, ab^{-1} \in H$ if and only if $a^{-1}b \in H$.

Proof.

(3) $\Rightarrow$ (1): For any $h \in H$ and any $a \in G$, *to show* $aha^{-1} \in H$. (Why?)
Take $b = a^{-1}$, then $(aH)(a^{-1}H) = H$. Thus, $aha^{-1} = aha^{-1}e \in H$. $\square$

(2) $\Leftrightarrow$ (4): (2) holds if and only if the left and right cosets of H coincide. The left cosets are the equivalence classes $[a]$, where $a \sim b$ if $a^{-1}b \in H$. The right cosets are the equivalence classes $[a]$, where $a \sim b$ if $ab^{-1} \in H$.

Proof of Proposition 5 cont.

Proposition 5: Let H be a subgroup of the group G. TFAE:

(1) H is a normal subgroup of G;

(2) $aH = Ha$ for all $a \in G$;

(3) for all $a, b \in G, abH = (aH)(bH)$;

(4) for all $a, b \in G, ab^{-1} \in H$ if and only if $a^{-1}b \in H$.

Proof.

(3) $\Rightarrow$ (1): For any $h \in H$ and any $a \in G$, *to show* $aha^{-1} \in H$. (Why?)
Take $b = a^{-1}$, then $(aH)(a^{-1}H) = H$. Thus, $aha^{-1} = aha^{-1}e \in H$. $\square$

(2) $\Leftrightarrow$ (4): (2) holds if and only if the left and right cosets of H coincide. The left cosets are the equivalence classes $[a]$, where $a \sim b$ if $a^{-1}b \in H$. The right cosets are the equivalence classes $[a]$, where $a \sim b$ if $ab^{-1} \in H$. Since the two equivalence relations coincide if and only if their equivalence classes are identical,

Proof of Proposition 5 cont.

Proposition 5: Let H be a subgroup of the group G. TFAE:

(1) H is a normal subgroup of G;

(2) $aH = Ha$ for all $a \in G$;

(3) for all $a, b \in G, abH = (aH)(bH)$;

(4) for all $a, b \in G, ab^{-1} \in H$ if and only if $a^{-1}b \in H$.

Proof.

(3) $\Rightarrow$ (1): For any $h \in H$ and any $a \in G$, *to show* $aha^{-1} \in H$. (Why?) Take $b = a^{-1}$, then $(aH)(a^{-1}H) = H$. Thus, $aha^{-1} = aha^{-1}e \in H$. $\square$

(2) $\Leftrightarrow$ (4): (2) holds if and only if the left and right cosets of H coincide. The left cosets are the equivalence classes $[a]$, where $a \sim b$ if $a^{-1}b \in H$. The right cosets are the equivalence classes $[a]$, where $a \sim b$ if $ab^{-1} \in H$. Since the two equivalence relations coincide if and only if their equivalence classes are identical, (4) holds if and only if (2) holds. $\square$

Example: Normal subgroups of $S_3 = D_3$

Let $G = S_3 = \{e, a, a^2, b, ab, a^2b\}$, where $a^3 = e, b^2 = e$, and $ba = a^2b$.

-

Example: Normal subgroups of $S_3 = D_3$

Let $G = S_3 = \{e, a, a^2, b, ab, a^2b\}$, where $a^3 = e, b^2 = e$, and $ba = a^2b$.

- The trivial subgroup $\{e\}$ and the improper subgroup G are normal.
-

Example: Normal subgroups of $S_3 = D_3$

Let $G = S_3 = \{e, a, a^2, b, ab, a^2b\}$, where $a^3 = e, b^2 = e$, and $ba = a^2b$.

- The trivial subgroup $\{e\}$ and the improper subgroup G are normal.
- 4 proper nontrivial subgroups of S_3: (see the subgroup diagram in §3.6)

Example: Normal subgroups of $S_3 = D_3$

Let $G = S_3 = \{e, a, a^2, b, ab, a^2b\}$, where $a^3 = e, b^2 = e$, and $ba = a^2b$.

- The trivial subgroup $\{e\}$ and the improper subgroup G are normal.
- 4 proper nontrivial subgroups of S_3: (see the subgroup diagram in §3.6)

$$H = \{e, b\}, \quad K = \{e, ab\}, \quad L = \{e, a^2b\}, \quad N = \{e, a, a^2\}.$$

Note that

Example: Normal subgroups of $S_3 = D_3$

Let $G = S_3 = \{e, a, a^2, b, ab, a^2b\}$, where $a^3 = e, b^2 = e$, and $ba = a^2b$.

- The trivial subgroup $\{e\}$ and the improper subgroup G are normal.
- 4 proper nontrivial subgroups of S_3: (see the subgroup diagram in §3.6)

$$H = \{e, b\}, \quad K = \{e, ab\}, \quad L = \{e, a^2b\}, \quad N = \{e, a, a^2\}.$$

Note that each of b, ab, a^2b has order 2.

Example: Normal subgroups of $S_3 = D_3$

Let $G = S_3 = \{e, a, a^2, b, ab, a^2b\}$, where $a^3 = e, b^2 = e$, and $ba = a^2b$.

- The trivial subgroup $\{e\}$ and the improper subgroup G are normal.
- 4 proper nontrivial subgroups of S_3: (see the subgroup diagram in §3.6)

$$H = \{e, b\}, \quad K = \{e, ab\}, \quad L = \{e, a^2b\}, \quad N = \{e, a, a^2\}.$$

Note that each of b, ab, a^2b has order 2.

In Example 7, $aH = \{a, ab\} \neq \{a, a^2b\} = Ha$. Thus,

Example: Normal subgroups of $S_3 = D_3$

Let $G = S_3 = \{e, a, a^2, b, ab, a^2b\}$, where $a^3 = e, b^2 = e$, and $ba = a^2b$.

- The trivial subgroup $\{e\}$ and the improper subgroup G are normal.
- 4 proper nontrivial subgroups of S_3: (see the subgroup diagram in §3.6)

$$H = \{e, b\}, \quad K = \{e, ab\}, \quad L = \{e, a^2b\}, \quad N = \{e, a, a^2\}.$$

Note that each of b, ab, a^2b has order 2.

In Example 7, $aH = \{a, ab\} \neq \{a, a^2b\} = Ha$. Thus, H is not normal.

K is not normal:

Example: Normal subgroups of $S_3 = D_3$

Let $G = S_3 = \{e, a, a^2, b, ab, a^2b\}$, where $a^3 = e, b^2 = e$, and $ba = a^2b$.

- The trivial subgroup $\{e\}$ and the improper subgroup G are normal.
- 4 proper nontrivial subgroups of S_3: (see the subgroup diagram in §3.6)

$$H = \{e, b\}, \quad K = \{e, ab\}, \quad L = \{e, a^2b\}, \quad N = \{e, a, a^2\}.$$

Note that each of b, ab, a^2b has order 2.

In Example 7, $aH = \{a, ab\} \neq \{a, a^2b\} = Ha$. Thus, H is not normal.

K is not normal: $aK = \{a, a^2b\} \neq \{a, b\} \stackrel{!}{=} \{a, aba\} = Ka$.

L is not normal:

Example: Normal subgroups of $S_3 = D_3$

Let $G = S_3 = \{e, a, a^2, b, ab, a^2b\}$, where $a^3 = e, b^2 = e$, and $ba = a^2b$.

- The trivial subgroup $\{e\}$ and the improper subgroup G are normal.
- 4 proper nontrivial subgroups of S_3: (see the subgroup diagram in §3.6)

$$H = \{e, b\}, \quad K = \{e, ab\}, \quad L = \{e, a^2b\}, \quad N = \{e, a, a^2\}.$$

Note that each of b, ab, a^2b has order 2.

In Example 7, $aH = \{a, ab\} \neq \{a, a^2b\} = Ha$. Thus, H is not normal.

K is not normal: $aK = \{a, a^2b\} \neq \{a, b\} \stackrel{!}{=} \{a, aba\} = Ka$.

L is not normal: $aL = \{a, b\} \neq \{a, ab\} \stackrel{!}{=} \{a, a^2ba\} = La$.

Example: Normal subgroups of $S_3 = D_3$

Let $G = S_3 = \{e, a, a^2, b, ab, a^2b\}$, where $a^3 = e, b^2 = e$, and $ba = a^2b$.

- The trivial subgroup $\{e\}$ and the improper subgroup G are normal.
- 4 proper nontrivial subgroups of S_3: (see the subgroup diagram in §3.6)

$$H = \{e, b\}, \quad K = \{e, ab\}, \quad L = \{e, a^2b\}, \quad N = \{e, a, a^2\}.$$

Note that each of b, ab, a^2b has order 2.

In Example 7, $aH = \{a, ab\} \neq \{a, a^2b\} = Ha$. Thus, H is not normal.
K is not normal: $aK = \{a, a^2b\} \neq \{a, b\} \overset{!}{=} \{a, aba\} = Ka$.
L is not normal: $aL = \{a, b\} \neq \{a, ab\} \overset{!}{=} \{a, a^2ba\} = La$.

In Example 8, left cosets of N are $\{N, bN\} = \{N, Nb\}$ right cosets of N.
In particular, $bN = \{b, a^2b, ab\} = \{b, ab, a^2b\} = Nb$. Thus, N is normal.

In conclusion,

Example: Normal subgroups of $S_3 = D_3$

Let $G = S_3 = \{e, a, a^2, b, ab, a^2b\}$, where $a^3 = e, b^2 = e$, and $ba = a^2b$.

- The trivial subgroup $\{e\}$ and the improper subgroup G are normal.
- 4 proper nontrivial subgroups of S_3: (see the subgroup diagram in §3.6)

$$H = \{e, b\}, \quad K = \{e, ab\}, \quad L = \{e, a^2b\}, \quad N = \{e, a, a^2\}.$$

Note that each of b, ab, a^2b has order 2.

In Example 7, $aH = \{a, ab\} \neq \{a, a^2b\} = Ha$. Thus, H is not normal.
K is not normal: $aK = \{a, a^2b\} \neq \{a, b\} \overset{!}{=} \{a, aba\} = Ka$.
L is not normal: $aL = \{a, b\} \neq \{a, ab\} \overset{!}{=} \{a, a^2ba\} = La$.

In Example 8, left cosets of N are $\{N, bN\} = \{N, Nb\}$ right cosets of N.
In particular, $bN = \{b, a^2b, ab\} = \{b, ab, a^2b\} = Nb$. Thus, N is normal.

In conclusion, N is the only proper nontrivial normal subgroup of S_3.

Example: Subgroups of index 2 are normal

Let H be a subgroup of G with $[G : H] = 2$. *To show* H is normal.

Proof.

Example: Subgroups of index 2 are normal

Let H be a subgroup of G with $[G : H] = 2$. *To show* H is normal.

Proof.

H has only two left cosets.

Example: Subgroups of index 2 are normal

Let H be a subgroup of G with $[G : H] = 2$. *To show* H is normal.

Proof.

H has only two left cosets. Then these must be H and $G - H$. (Why?)

Example: Subgroups of index 2 are normal

Let H be a subgroup of G with $[G : H] = 2$. *To show* H is normal.

Proof.

H has only two left cosets. Then these must be H and $G - H$. (Why?) And these must also be the right cosets. (Why?) Thus,

Example: Subgroups of index 2 are normal

Let H be a subgroup of G with $[G : H] = 2$. *To show* H is normal.

Proof.

H has only two left cosets. Then these must be H and $G - H$. (Why?) And these must also be the right cosets. (Why?) Thus, H is normal. □

Example 14

Example: Subgroups of index 2 are normal

Let H be a subgroup of G with $[G : H] = 2$. *To show* H is normal.

Proof.

H has only two left cosets. Then these must be H and $G - H$. (Why?) And these must also be the right cosets. (Why?) Thus, H is normal. □

Example 14

In S_3, the subgroup $N = \{e, a, a^2\}$ has index 2, and so N is normal.

Note 6

Example: Subgroups of index 2 are normal

Let H be a subgroup of G with $[G : H] = 2$. *To show* H is normal.

Proof.

H has only two left cosets. Then these must be H and $G - H$. (Why?) And these must also be the right cosets. (Why?) Thus, H is normal. □

Example 14

In S_3, the subgroup $N = \{e, a, a^2\}$ has index 2, and so N is normal.

Note 6

Conversely not true:

Example: Subgroups of index 2 are normal

Let H be a subgroup of G with $[G : H] = 2$. *To show* H is normal.

Proof.

H has only two left cosets. Then these must be H and $G - H$. (Why?) And these must also be the right cosets. (Why?) Thus, H is normal. $\square$

Example 14

In S_3, the subgroup $N = \{e, a, a^2\}$ has index 2, and so N is normal.

Note 6

Conversely not true: Easy to find a counterexample from abelian groups. For example,

Example: Subgroups of index 2 are normal

Let H be a subgroup of G with $[G : H] = 2$. *To show* H is normal.

Proof.

H has only two left cosets. Then these must be H and $G - H$. (Why?) And these must also be the right cosets. (Why?) Thus, H is normal. $\square$

Example 14

In S_3, the subgroup $N = \{e, a, a^2\}$ has index 2, and so N is normal.

Note 6

Conversely not true: Easy to find a counterexample from abelian groups. For example, in $\mathbf{Z}_{100}$*, the subgroup* $10\mathbf{Z}_{100}$ *is normal, but has index* 10*.*

Example: Normal subgroups of D_4

$G = D_4 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$, where $a^4 = e, b^2 = e, ba = a^{-1}b$.

-

[1] N is contained in the center of G.

Example: Normal subgroups of D_4

$G = D_4 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$, where $a^4 = e, b^2 = e, ba = a^{-1}b$.

- The trivial subgroup $\{e\}$ and the improper subgroup G are normal.
-

[1] N is contained in the center of G.

Example: Normal subgroups of D_4

$G = D_4 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$, where $a^4 = e, b^2 = e, ba = a^{-1}b$.

- The trivial subgroup $\{e\}$ and the improper subgroup G are normal.
- The subgroups $\{e, a^2, b, a^2b\}, \{e, a, a^2, a^3\}, \{e, a^2, ab, a^3b\}$ are normal.
- Let $N = \{e, a^2\}, H = \{e, b\}, K = \{e, a^2b\}, L = \{e, ab\}, M = \{e, a^3b\}$.

Claim 1 (Refer to the subgroup diagram of D_4 in §3.6)

[1] N is contained in the center of G.

Example: Normal subgroups of D_4

$G = D_4 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$, where $a^4 = e, b^2 = e, ba = a^{-1}b$.

- The trivial subgroup $\{e\}$ and the improper subgroup G are normal.
- The subgroups $\{e, a^2, b, a^2b\}, \{e, a, a^2, a^3\}, \{e, a^2, ab, a^3b\}$ are normal.
- Let $N = \{e, a^2\}, H = \{e, b\}, K = \{e, a^2b\}, L = \{e, ab\}, M = \{e, a^3b\}$.

Claim 1 (Refer to the subgroup diagram of D_4 in §3.6)

Among the subgroups N, H, K, L, M, only the subgroup N is normal.

N is normal:

[1] N is contained in the center of G.

Example: Normal subgroups of D_4

$G = D_4 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$, where $a^4 = e, b^2 = e, ba = a^{-1}b$.

- The trivial subgroup $\{e\}$ and the improper subgroup G are normal.
- The subgroups $\{e, a^2, b, a^2b\}, \{e, a, a^2, a^3\}, \{e, a^2, ab, a^3b\}$ are normal.
- Let $N = \{e, a^2\}, H = \{e, b\}, K = \{e, a^2b\}, L = \{e, ab\}, M = \{e, a^3b\}$.

Claim 1 (Refer to the subgroup diagram of D_4 in §3.6)

Among the subgroups N, H, K, L, M, only the subgroup N is normal.

N is normal: *To show* $N = \{e, a^2\}$ commutes with every element of G. [1]
a^2 commutes with b:

[1] N is contained in the center of G.

Example: Normal subgroups of D_4

$G = D_4 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$, where $a^4 = e, b^2 = e, ba = a^{-1}b$.

- The trivial subgroup $\{e\}$ and the improper subgroup G are normal.
- The subgroups $\{e, a^2, b, a^2b\}, \{e, a, a^2, a^3\}, \{e, a^2, ab, a^3b\}$ are normal.
- Let $N = \{e, a^2\}, H = \{e, b\}, K = \{e, a^2b\}, L = \{e, ab\}, M = \{e, a^3b\}$.

Claim 1 (Refer to the subgroup diagram of D_4 in §3.6)

Among the subgroups N, H, K, L, M, only the subgroup N is normal.

N is normal: *To show* $N = \{e, a^2\}$ commutes with every element of G. [1]
a^2 commutes with b: $ba^2 = (ba)a = (a^{-1}b)a = a^{-1}(ba) = a^{-2}b = a^2b$.

[1] N is contained in the center of G.

Example: Normal subgroups of D_4

$G = D_4 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$, where $a^4 = e, b^2 = e, ba = a^{-1}b$.

- The trivial subgroup $\{e\}$ and the improper subgroup G are normal.
- The subgroups $\{e, a^2, b, a^2b\}, \{e, a, a^2, a^3\}, \{e, a^2, ab, a^3b\}$ are normal.
- Let $N = \{e, a^2\}, H = \{e, b\}, K = \{e, a^2b\}, L = \{e, ab\}, M = \{e, a^3b\}$.

Claim 1 (Refer to the subgroup diagram of D_4 in §3.6)

Among the subgroups N, H, K, L, M, only the subgroup N is normal.

N is normal: *To show* $N = \{e, a^2\}$ commutes with every element of G. [1]
a^2 commutes with b: $ba^2 = (ba)a = (a^{-1}b)a = a^{-1}(ba) = a^{-2}b = a^2b$.
And since a^2 commutes with powers of a, it commutes with every element.

[1] N is contained in the center of G.

Example: Normal subgroups of D_4

$G = D_4 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$, where $a^4 = e, b^2 = e, ba = a^{-1}b$.

- The trivial subgroup $\{e\}$ and the improper subgroup G are normal.
- The subgroups $\{e, a^2, b, a^2b\}, \{e, a, a^2, a^3\}, \{e, a^2, ab, a^3b\}$ are normal.
- Let $N = \{e, a^2\}, H = \{e, b\}, K = \{e, a^2b\}, L = \{e, ab\}, M = \{e, a^3b\}$.

Claim 1 (Refer to the subgroup diagram of D_4 in §3.6)

Among the subgroups N, H, K, L, M, only the subgroup N is normal.

N is normal: *To show* $N = \{e, a^2\}$ commutes with every element of G. [1]
a^2 commutes with b: $ba^2 = (ba)a = (a^{-1}b)a = a^{-1}(ba) = a^{-2}b = a^2b$.
And since a^2 commutes with powers of a, it commutes with every element.
This implies that N is normal since its left and right cosets coincide. $\square$

None of the subgroups H, K, L, M is normal:

[1] N is contained in the center of G.

Example: Normal subgroups of D_4

$G = D_4 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$, where $a^4 = e, b^2 = e, ba = a^{-1}b$.

- The trivial subgroup $\{e\}$ and the improper subgroup G are normal.
- The subgroups $\{e, a^2, b, a^2b\}, \{e, a, a^2, a^3\}, \{e, a^2, ab, a^3b\}$ are normal.
- Let $N = \{e, a^2\}, H = \{e, b\}, K = \{e, a^2b\}, L = \{e, ab\}, M = \{e, a^3b\}$.

Claim 1 (Refer to the subgroup diagram of D_4 in §3.6)

Among the subgroups N, H, K, L, M, only the subgroup N is normal.

N is normal: *To show* $N = \{e, a^2\}$ commutes with every element of G.[1]
a^2 commutes with b: $ba^2 = (ba)a = (a^{-1}b)a = a^{-1}(ba) = a^{-2}b = a^2b$.
And since a^2 commutes with powers of a, it commutes with every element.
This implies that N is normal since its left and right cosets coincide. $\square$

None of the subgroups H, K, L, M is normal: By the direct computations,

[1] N is contained in the center of G.

Example: Normal subgroups of D_4

$G = D_4 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$, where $a^4 = e, b^2 = e, ba = a^{-1}b$.

- The trivial subgroup $\{e\}$ and the improper subgroup G are normal.
- The subgroups $\{e, a^2, b, a^2b\}, \{e, a, a^2, a^3\}, \{e, a^2, ab, a^3b\}$ are normal.
- Let $N = \{e, a^2\}, H = \{e, b\}, K = \{e, a^2b\}, L = \{e, ab\}, M = \{e, a^3b\}$.

Claim 1 (Refer to the subgroup diagram of D_4 in §3.6)

Among the subgroups N, H, K, L, M, only the subgroup N is normal.

N is normal: *To show* $N = \{e, a^2\}$ commutes with every element of G. [1]
a^2 commutes with b: $ba^2 = (ba)a = (a^{-1}b)a = a^{-1}(ba) = a^{-2}b = a^2b$.
And since a^2 commutes with powers of a, it commutes with every element.
This implies that N is normal since its left and right cosets coincide. □

None of the subgroups H, K, L, M is normal: By the direct computations,

$$aH \neq Ha, \quad aK \neq Ka, \quad aL \neq La, \quad aM \neq Ma.$$ (Check it!)

[1] N is contained in the center of G.

Fundamental Homomorphism Theorem

Theorem 15 (Fundamental Homomorphism Theorem)

If $\phi : G_1 \to G_2$ *is a homomorphism with* $K = \ker(\phi)$*, then* $G_1/K \cong \phi(G_1)$.

Fundamental Homomorphism Theorem

Theorem 15 (Fundamental Homomorphism Theorem)

If $\phi : G_1 \to G_2$ is a homomorphism with $K = \ker(\phi)$, then $G_1/K \cong \phi(G_1)$.

This is exactly Remark 1 in §3.7. Another proof using coset notation:

Proof.

Define $\overline{\phi} : G_1/K \to \phi(G_1)$ by $\overline{\phi}(aK) = \phi(a)$, for all $aK \in G_1/K$.

(i) well-defined:

Fundamental Homomorphism Theorem

Theorem 15 (Fundamental Homomorphism Theorem)

If $\phi : G_1 \to G_2$ is a homomorphism with $K = \ker(\phi)$, then $G_1/K \cong \phi(G_1)$.

This is exactly Remark 1 in §3.7. Another proof using coset notation:

Proof.

Define $\overline{\phi} : G_1/K \to \phi(G_1)$ by $\overline{\phi}(aK) = \phi(a)$, for all $aK \in G_1/K$.

(i) well-defined: If $aK = bK$, then $a = bk$ for some $k \in \ker(\phi)$, and so

Fundamental Homomorphism Theorem

Theorem 15 (Fundamental Homomorphism Theorem)

If $\phi : G_1 \to G_2$ is a homomorphism with $K = \ker(\phi)$, then $G_1/K \cong \phi(G_1)$.

This is exactly Remark 1 in §3.7. Another proof using coset notation:

Proof.

Define $\overline{\phi} : G_1/K \to \phi(G_1)$ by $\overline{\phi}(aK) = \phi(a)$, for all $aK \in G_1/K$.

(i) well-defined: If $aK = bK$, then $a = bk$ for some $k \in \ker(\phi)$, and so

$$\overline{\phi}(aK) = \phi(a) = \phi(bk) = \phi(b)\phi(k) = \phi(b) = \overline{\phi}(bK).$$

(ii) $\overline{\phi}$ is a homomorphism:

Fundamental Homomorphism Theorem

Theorem 15 (Fundamental Homomorphism Theorem)

If $\phi : G_1 \to G_2$ is a homomorphism with $K = \ker(\phi)$, then $G_1/K \cong \phi(G_1)$.

This is exactly Remark 1 in §3.7. Another proof using coset notation:

Proof.

Define $\overline{\phi} : G_1/K \to \phi(G_1)$ by $\overline{\phi}(aK) = \phi(a)$, for all $aK \in G_1/K$.

(i) well-defined: If $aK = bK$, then $a = bk$ for some $k \in \ker(\phi)$, and so

$$\overline{\phi}(aK) = \phi(a) = \phi(bk) = \phi(b)\phi(k) = \phi(b) = \overline{\phi}(bK).$$

(ii) $\overline{\phi}$ is a homomorphism: For all $a, b \in G_1$, we have

Fundamental Homomorphism Theorem

Theorem 15 (Fundamental Homomorphism Theorem)

If $\phi : G_1 \to G_2$ is a homomorphism with $K = \ker(\phi)$, then $G_1/K \cong \phi(G_1)$.

This is exactly Remark 1 in §3.7. Another proof using coset notation:

Proof.

Define $\overline{\phi} : G_1/K \to \phi(G_1)$ by $\overline{\phi}(aK) = \phi(a)$, for all $aK \in G_1/K$.

(i) well-defined: If $aK = bK$, then $a = bk$ for some $k \in \ker(\phi)$, and so

$$\overline{\phi}(aK) = \phi(a) = \phi(bk) = \phi(b)\phi(k) = \phi(b) = \overline{\phi}(bK).$$

(ii) $\overline{\phi}$ is a homomorphism: For all $a, b \in G_1$, we have

$$\overline{\phi}(aKbK) = \overline{\phi}(abK) = \phi(ab) = \phi(a)\phi(b) = \overline{\phi}(aK)\overline{\phi}(bK).$$

(iii) one-to-one:

Fundamental Homomorphism Theorem

Theorem 15 (Fundamental Homomorphism Theorem)

If $\phi : G_1 \to G_2$ is a homomorphism with $K = \ker(\phi)$, then $G_1/K \cong \phi(G_1)$.

This is exactly Remark 1 in §3.7. Another proof using coset notation:

Proof.

Define $\overline{\phi} : G_1/K \to \phi(G_1)$ by $\overline{\phi}(aK) = \phi(a)$, for all $aK \in G_1/K$.

(i) well-defined: If $aK = bK$, then $a = bk$ for some $k \in \ker(\phi)$, and so

$$\overline{\phi}(aK) = \phi(a) = \phi(bk) = \phi(b)\phi(k) = \phi(b) = \overline{\phi}(bK).$$

(ii) $\overline{\phi}$ is a homomorphism: For all $a, b \in G_1$, we have

$$\overline{\phi}(aKbK) = \overline{\phi}(abK) = \phi(ab) = \phi(a)\phi(b) = \overline{\phi}(aK)\overline{\phi}(bK).$$

(iii) one-to-one: If $\phi(a) = \phi(b)$, then $\phi(b^{-1}a) = (\phi(b))^{-1}\phi(a) = e_2$. This implies that

Fundamental Homomorphism Theorem

Theorem 15 (Fundamental Homomorphism Theorem)

If $\phi : G_1 \to G_2$ is a homomorphism with $K = \ker(\phi)$, then $G_1/K \cong \phi(G_1)$.

This is exactly Remark 1 in §3.7. Another proof using coset notation:

Proof.

Define $\overline{\phi} : G_1/K \to \phi(G_1)$ by $\overline{\phi}(aK) = \phi(a)$, for all $aK \in G_1/K$.

(i) well-defined: If $aK = bK$, then $a = bk$ for some $k \in \ker(\phi)$, and so

$$\overline{\phi}(aK) = \phi(a) = \phi(bk) = \phi(b)\phi(k) = \phi(b) = \overline{\phi}(bK).$$

(ii) $\overline{\phi}$ is a homomorphism: For all $a, b \in G_1$, we have

$$\overline{\phi}(aKbK) = \overline{\phi}(abK) = \phi(ab) = \phi(a)\phi(b) = \overline{\phi}(aK)\overline{\phi}(bK).$$

(iii) one-to-one: If $\phi(a) = \phi(b)$, then $\phi(b^{-1}a) = (\phi(b))^{-1}\phi(a) = e_2$. This implies that $b^{-1}a \in K$, and so

Fundamental Homomorphism Theorem

Theorem 15 (Fundamental Homomorphism Theorem)

If $\phi : G_1 \to G_2$ is a homomorphism with $K = \ker(\phi)$, then $G_1/K \cong \phi(G_1)$.

This is exactly Remark 1 in §3.7. Another proof using coset notation:

Proof.

Define $\overline{\phi} : G_1/K \to \phi(G_1)$ by $\overline{\phi}(aK) = \phi(a)$, for all $aK \in G_1/K$.

(i) well-defined: If $aK = bK$, then $a = bk$ for some $k \in \ker(\phi)$, and so

$$\overline{\phi}(aK) = \phi(a) = \phi(bk) = \phi(b)\phi(k) = \phi(b) = \overline{\phi}(bK).$$

(ii) $\overline{\phi}$ is a homomorphism: For all $a, b \in G_1$, we have

$$\overline{\phi}(aKbK) = \overline{\phi}(abK) = \phi(ab) = \phi(a)\phi(b) = \overline{\phi}(aK)\overline{\phi}(bK).$$

(iii) one-to-one: If $\phi(a) = \phi(b)$, then $\phi(b^{-1}a) = (\phi(b))^{-1}\phi(a) = e_2$. This implies that $b^{-1}a \in K$, and so $aK = bK$.

(iv) onto:

Fundamental Homomorphism Theorem

Theorem 15 (Fundamental Homomorphism Theorem)

If $\phi : G_1 \to G_2$ is a homomorphism with $K = \ker(\phi)$, then $G_1/K \cong \phi(G_1)$.

This is exactly Remark 1 in §3.7. Another proof using coset notation:

Proof.

Define $\overline{\phi} : G_1/K \to \phi(G_1)$ by $\overline{\phi}(aK) = \phi(a)$, for all $aK \in G_1/K$.

(i) well-defined: If $aK = bK$, then $a = bk$ for some $k \in \ker(\phi)$, and so

$$\overline{\phi}(aK) = \phi(a) = \phi(bk) = \phi(b)\phi(k) = \phi(b) = \overline{\phi}(bK).$$

(ii) $\overline{\phi}$ is a homomorphism: For all $a, b \in G_1$, we have

$$\overline{\phi}(aKbK) = \overline{\phi}(abK) = \phi(ab) = \phi(a)\phi(b) = \overline{\phi}(aK)\overline{\phi}(bK).$$

(iii) one-to-one: If $\phi(a) = \phi(b)$, then $\phi(b^{-1}a) = (\phi(b))^{-1}\phi(a) = e_2$. This implies that $b^{-1}a \in K$, and so $aK = bK$.

(iv) onto: Trivial.

□

Simple group

Remark 2 (Let $\phi : G_1 \to G_2$ be a group homomorphism.)

-

Simple group

Remark 2 (Let $\phi : G_1 \to G_2$ be a group homomorphism.)

- *ϕ is one-to-one* $\Leftrightarrow \ker(\phi) = \{e_1\}$. *Thus,*

Simple group

Remark 2 (Let $\phi : G_1 \to G_2$ be a group homomorphism.)

- ϕ *is one-to-one* $\Leftrightarrow \ker(\phi) = \{e_1\}$. *Thus,* $G_1 \cong \phi(G_1)$ *in this case.*
-

Simple group

Remark 2 (Let $\phi : G_1 \to G_2$ be a group homomorphism.)

- ϕ *is one-to-one* $\Leftrightarrow \ker(\phi) = \{e_1\}$. *Thus,* $G_1 \cong \phi(G_1)$ *in this case.*
- *If* $\ker(\phi) = G_1$, *then* ϕ *is the trivial mapping, i.e.,*

Simple group

Remark 2 (Let $\phi : G_1 \to G_2$ be a group homomorphism.)

• *ϕ is one-to-one* $\Leftrightarrow \ker(\phi) = \{e_1\}$. *Thus, $G_1 \cong \phi(G_1)$ in this case.*

• *If* $\ker(\phi) = G_1$, *then ϕ is the trivial mapping, i.e., $\phi(G_1) = \{e_2\}$.*

Thus

Simple group

Remark 2 (Let $\phi : G_1 \to G_2$ be a group homomorphism.)

• *ϕ is one-to-one* $\Leftrightarrow \ker(\phi) = \{e_1\}$. *Thus, $G_1 \cong \phi(G_1)$ in this case.*
• *If* $\ker(\phi) = G_1$, *then ϕ is the trivial mapping, i.e., $\phi(G_1) = \{e_2\}$.*
Thus if G_1 has no proper nontrivial normal subgroups, then ϕ is either one-to-one or trivial.

Definition 16

Simple group

Remark 2 (Let $\phi : G_1 \to G_2$ be a group homomorphism.)

- *ϕ is one-to-one* $\Leftrightarrow \ker(\phi) = \{e_1\}$. *Thus, $G_1 \cong \phi(G_1)$ in this case.*
- *If* $\ker(\phi) = G_1$, *then ϕ is the trivial mapping, i.e., $\phi(G_1) = \{e_2\}$.*

Thus if G_1 has no proper nontrivial normal subgroups, then ϕ is either one-to-one or trivial.

Definition 16

The nontrivial group G is called a **simple** group if it has no proper nontrivial normal subgroups.

Example 17

Simple group

Remark 2 (Let $\phi : G_1 \to G_2$ be a group homomorphism.)

• *ϕ is one-to-one* $\Leftrightarrow \ker(\phi) = \{e_1\}$. *Thus, $G_1 \cong \phi(G_1)$ in this case.*
• *If* $\ker(\phi) = G_1$, *then ϕ is the trivial mapping, i.e., $\phi(G_1) = \{e_2\}$.*
Thus if G_1 has no proper nontrivial normal subgroups, then ϕ is either one-to-one or trivial.

Definition 16

The nontrivial group G is called a **simple** group if it has no proper nontrivial normal subgroups.

Example 17

For any prime p, the cyclic group $\mathbf{Z}_p$ is simple, since

Simple group

Remark 2 (Let $\phi : G_1 \to G_2$ be a group homomorphism.)

• *ϕ is one-to-one* $\Leftrightarrow \ker(\phi) = \{e_1\}$. *Thus, $G_1 \cong \phi(G_1)$ in this case.*
• *If* $\ker(\phi) = G_1$, *then ϕ is the trivial mapping, i.e., $\phi(G_1) = \{e_2\}$.*
Thus if G_1 has no proper nontrivial normal subgroups, then ϕ is either one-to-one or trivial.

Definition 16

The nontrivial group G is called a **simple** group if it has no proper nontrivial normal subgroups.

Example 17

For any prime p, the cyclic group $\mathbf{Z}_p$ is simple, since it has no proper nontrivial subgroups of any kind (

Simple group

Remark 2 (Let $\phi : G_1 \to G_2$ be a group homomorphism.)

• *ϕ is one-to-one* $\Leftrightarrow \ker(\phi) = \{e_1\}$. *Thus, $G_1 \cong \phi(G_1)$ in this case.*
• *If* $\ker(\phi) = G_1$, *then ϕ is the trivial mapping, i.e., $\phi(G_1) = \{e_2\}$.*
Thus if G_1 has no proper nontrivial normal subgroups, then ϕ is either one-to-one or trivial.

Definition 16

The nontrivial group G is called a **simple** group if it has no proper nontrivial normal subgroups.

Example 17

For any prime p, the cyclic group $\mathbf{Z}_p$ is simple, since it has no proper nontrivial subgroups of any kind (every nonzero element is a generator).

Example: $\mathbf{Z}_n / m\mathbf{Z}_n \cong \mathbf{Z}_m$ if $m | n$

Example: $\mathbf{Z}_n/m\mathbf{Z}_n \cong \mathbf{Z}_m$ if $m|n$

Any homomorphic image of a cyclic group is again cyclic, and so

Example: $\mathbf{Z}_n/m\mathbf{Z}_n \cong \mathbf{Z}_m$ if $m|n$

Any homomorphic image of a cyclic group is again cyclic, and so all factor groups of $\mathbf{Z}_n$ must be cyclic, and hence isomorphic to $\mathbf{Z}_m$ for some m.

Note 7

Example: $\mathbf{Z}_n/m\mathbf{Z}_n \cong \mathbf{Z}_m$ if $m|n$

Any homomorphic image of a cyclic group is again cyclic, and so all factor groups of $\mathbf{Z}_n$ must be cyclic, and hence isomorphic to $\mathbf{Z}_m$ for some m.

Note 7

The subgroups of $\mathbf{Z}_n$ correspond to divisors of n, and so

Example: $\mathbf{Z}_n/m\mathbf{Z}_n \cong \mathbf{Z}_m$ if $m|n$

Any homomorphic image of a cyclic group is again cyclic, and so all factor groups of $\mathbf{Z}_n$ must be cyclic, and hence isomorphic to $\mathbf{Z}_m$ for some m.

Note 7

The subgroups of $\mathbf{Z}_n$ correspond to divisors of n, and so to describe all factor groups of $\mathbf{Z}_n$ we only need to describe $\mathbf{Z}_n/m\mathbf{Z}_n$ for all $m|n, m > 0$.

Proof.

Example: $\mathbf{Z}_n/m\mathbf{Z}_n \cong \mathbf{Z}_m$ if $m|n$

Any homomorphic image of a cyclic group is again cyclic, and so all factor groups of $\mathbf{Z}_n$ must be cyclic, and hence isomorphic to $\mathbf{Z}_m$ for some m.

Note 7

The subgroups of $\mathbf{Z}_n$ correspond to divisors of n, and so to describe all factor groups of $\mathbf{Z}_n$ we only need to describe $\mathbf{Z}_n/m\mathbf{Z}_n$ for all $m|n, m > 0$.

Proof.

Define $\phi : \mathbf{Z}_n \to \mathbf{Z}_m$ by $\phi([x]_n) = [x]_m$.
(i) well-defined:

Example: $\mathbf{Z}_n/m\mathbf{Z}_n \cong \mathbf{Z}_m$ if $m|n$

Any homomorphic image of a cyclic group is again cyclic, and so all factor groups of $\mathbf{Z}_n$ must be cyclic, and hence isomorphic to $\mathbf{Z}_m$ for some m.

Note 7

The subgroups of $\mathbf{Z}_n$ correspond to divisors of n, and so to describe all factor groups of $\mathbf{Z}_n$ we only need to describe $\mathbf{Z}_n/m\mathbf{Z}_n$ for all $m|n, m > 0$.

Proof.

Define $\phi : \mathbf{Z}_n \to \mathbf{Z}_m$ by $\phi([x]_n) = [x]_m$.
(i) well-defined: If $[x]_n = [y]_n$, then $[x]_m = [y]_m$. (Why?) [since

Example: $\mathbf{Z}_n/m\mathbf{Z}_n \cong \mathbf{Z}_m$ if $m|n$

Any homomorphic image of a cyclic group is again cyclic, and so all factor groups of $\mathbf{Z}_n$ must be cyclic, and hence isomorphic to $\mathbf{Z}_m$ for some m.

Note 7

The subgroups of $\mathbf{Z}_n$ correspond to divisors of n, and so to describe all factor groups of $\mathbf{Z}_n$ we only need to describe $\mathbf{Z}_n/m\mathbf{Z}_n$ for all $m|n, m > 0$.

Proof.

Define $\phi : \mathbf{Z}_n \to \mathbf{Z}_m$ by $\phi([x]_n) = [x]_m$.
(i) well-defined: If $[x]_n = [y]_n$, then $[x]_m = [y]_m$. (Why?) [since $m|n$]
(ii) ϕ is a homomorphism:

Example: $\mathbf{Z}_n/m\mathbf{Z}_n \cong \mathbf{Z}_m$ if $m|n$

Any homomorphic image of a cyclic group is again cyclic, and so all factor groups of $\mathbf{Z}_n$ must be cyclic, and hence isomorphic to $\mathbf{Z}_m$ for some m.

Note 7

The subgroups of $\mathbf{Z}_n$ correspond to divisors of n, and so to describe all factor groups of $\mathbf{Z}_n$ we only need to describe $\mathbf{Z}_n/m\mathbf{Z}_n$ for all $m|n, m > 0$.

Proof.

Define $\phi : \mathbf{Z}_n \to \mathbf{Z}_m$ by $\phi([x]_n) = [x]_m$.

(i) well-defined: If $[x]_n = [y]_n$, then $[x]_m = [y]_m$. (Why?) [since $m|n$]

(ii) ϕ is a homomorphism: For any $[x]_n, [y]_n \in \mathbf{Z}_n$, we have

Example: $\mathbf{Z}_n/m\mathbf{Z}_n \cong \mathbf{Z}_m$ if $m|n$

Any homomorphic image of a cyclic group is again cyclic, and so all factor groups of $\mathbf{Z}_n$ must be cyclic, and hence isomorphic to $\mathbf{Z}_m$ for some m.

Note 7

The subgroups of $\mathbf{Z}_n$ correspond to divisors of n, and so to describe all factor groups of $\mathbf{Z}_n$ we only need to describe $\mathbf{Z}_n/m\mathbf{Z}_n$ for all $m|n, m > 0$.

Proof.

Define $\phi : \mathbf{Z}_n \to \mathbf{Z}_m$ by $\phi([x]_n) = [x]_m$.
(i) well-defined: If $[x]_n = [y]_n$, then $[x]_m = [y]_m$. (Why?) [since $m|n$]
(ii) ϕ is a homomorphism: For any $[x]_n, [y]_n \in \mathbf{Z}_n$, we have

$$\phi([x]_n + [y]_n) = \phi([x+y]_n) = [x+y]_m = [x]_m + [y]_m = \phi([x]_n) + \phi([y_n]).$$

(iii) onto:

Example: $\mathbf{Z}_n/m\mathbf{Z}_n \cong \mathbf{Z}_m$ if $m|n$

Any homomorphic image of a cyclic group is again cyclic, and so all factor groups of $\mathbf{Z}_n$ must be cyclic, and hence isomorphic to $\mathbf{Z}_m$ for some m.

Note 7

The subgroups of $\mathbf{Z}_n$ correspond to divisors of n, and so to describe all factor groups of $\mathbf{Z}_n$ we only need to describe $\mathbf{Z}_n/m\mathbf{Z}_n$ for all $m|n, m > 0$.

Proof.

Define $\phi : \mathbf{Z}_n \to \mathbf{Z}_m$ by $\phi([x]_n) = [x]_m$.
(i) well-defined: If $[x]_n = [y]_n$, then $[x]_m = [y]_m$. (Why?) [since $m|n$]
(ii) ϕ is a homomorphism: For any $[x]_n, [y]_n \in \mathbf{Z}_n$, we have

$$\phi([x]_n + [y]_n) = \phi([x+y]_n) = [x+y]_m = [x]_m + [y]_m = \phi([x]_n) + \phi([y_n]).$$

(iii) onto: Trivial.
(iv) $\ker(\phi) = \{[x]_n \mid [x]_m = [0]_m\} =$

Example: $\mathbf{Z}_n/m\mathbf{Z}_n \cong \mathbf{Z}_m$ if $m|n$

Any homomorphic image of a cyclic group is again cyclic, and so all factor groups of $\mathbf{Z}_n$ must be cyclic, and hence isomorphic to $\mathbf{Z}_m$ for some m.

Note 7

The subgroups of $\mathbf{Z}_n$ correspond to divisors of n, and so to describe all factor groups of $\mathbf{Z}_n$ we only need to describe $\mathbf{Z}_n/m\mathbf{Z}_n$ for all $m|n, m > 0$.

Proof.

Define $\phi : \mathbf{Z}_n \to \mathbf{Z}_m$ by $\phi([x]_n) = [x]_m$.
(i) well-defined: If $[x]_n = [y]_n$, then $[x]_m = [y]_m$. (Why?) [since $m|n$]
(ii) ϕ is a homomorphism: For any $[x]_n, [y]_n \in \mathbf{Z}_n$, we have

$$\phi([x]_n + [y]_n) = \phi([x+y]_n) = [x+y]_m = [x]_m + [y]_m = \phi([x]_n) + \phi([y_n]).$$

(iii) onto: Trivial.
(iv) $\ker(\phi) = \{[x]_n \mid [x]_m = [0]_m\} = \{[x]_n \mid x \text{ is a multiple of } m\} =$

Example: $\mathbf{Z}_n/m\mathbf{Z}_n \cong \mathbf{Z}_m$ if $m|n$

Any homomorphic image of a cyclic group is again cyclic, and so all factor groups of $\mathbf{Z}_n$ must be cyclic, and hence isomorphic to $\mathbf{Z}_m$ for some m.

Note 7

The subgroups of $\mathbf{Z}_n$ correspond to divisors of n, and so to describe all factor groups of $\mathbf{Z}_n$ we only need to describe $\mathbf{Z}_n/m\mathbf{Z}_n$ for all $m|n, m > 0$.

Proof.

Define $\phi : \mathbf{Z}_n \to \mathbf{Z}_m$ by $\phi([x]_n) = [x]_m$.
(i) well-defined: If $[x]_n = [y]_n$, then $[x]_m = [y]_m$. (Why?) [since $m|n$]
(ii) ϕ is a homomorphism: For any $[x]_n, [y]_n \in \mathbf{Z}_n$, we have

$$\phi([x]_n + [y]_n) = \phi([x+y]_n) = [x+y]_m = [x]_m + [y]_m = \phi([x]_n) + \phi([y_n]).$$

(iii) onto: Trivial.
(iv) $\ker(\phi) = \{[x]_n \mid [x]_m = [0]_m\} = \{[x]_n \mid x \text{ is a multiple of } m\} = m\mathbf{Z}_n$.

Example: $\mathbf{Z}_n/m\mathbf{Z}_n \cong \mathbf{Z}_m$ if $m|n$

Any homomorphic image of a cyclic group is again cyclic, and so all factor groups of $\mathbf{Z}_n$ must be cyclic, and hence isomorphic to $\mathbf{Z}_m$ for some m.

Note 7

The subgroups of $\mathbf{Z}_n$ correspond to divisors of n, and so to describe all factor groups of $\mathbf{Z}_n$ we only need to describe $\mathbf{Z}_n/m\mathbf{Z}_n$ for all $m|n, m > 0$.

Proof.

Define $\phi : \mathbf{Z}_n \to \mathbf{Z}_m$ by $\phi([x]_n) = [x]_m$.
(i) well-defined: If $[x]_n = [y]_n$, then $[x]_m = [y]_m$. (Why?) [since $m|n$]
(ii) ϕ is a homomorphism: For any $[x]_n, [y]_n \in \mathbf{Z}_n$, we have

$$\phi([x]_n + [y]_n) = \phi([x+y]_n) = [x+y]_m = [x]_m + [y]_m = \phi([x]_n) + \phi([y_n]).$$

(iii) onto: Trivial.
(iv) $\ker(\phi) = \{[x]_n \mid [x]_m = [0]_m\} = \{[x]_n \mid x \text{ is a multiple of } m\} = m\mathbf{Z}_n$.
It follows from the fundamental homomorphism theorem that $\mathbf{Z}_n/m\mathbf{Z}_n \cong \mathbf{Z}_m$. $\square$

Example: $D_4/Z(D_4) \cong \mathbf{Z}_2 \times \mathbf{Z}_2$

$G = D_4 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$, where $a^4 = e, b^2 = e, ba = a^{-1}b$.

Example: $D_4/Z(D_4) \cong \mathbf{Z}_2 \times \mathbf{Z}_2$

$G = D_4 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$, where $a^4 = e, b^2 = e, ba = a^{-1}b$.

Let $N = \{e, a^2\}$ be the center $Z(D_4)$ of D_4. (See Claim 1)

Example: $D_4/Z(D_4) \cong \mathbf{Z}_2 \times \mathbf{Z}_2$

$G = D_4 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$, where $a^4 = e, b^2 = e, ba = a^{-1}b$.

Let $N = \{e, a^2\}$ be the center $Z(D_4)$ of D_4. (See Claim 1)

The factor group G/N consists of the four cosets: (Use Algorithm)

Example: $D_4/Z(D_4) \cong \mathbf{Z}_2 \times \mathbf{Z}_2$

$G = D_4 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$, where $a^4 = e, b^2 = e, ba = a^{-1}b$.

Let $N = \{e, a^2\}$ be the center $Z(D_4)$ of D_4. (See Claim 1)

The factor group G/N consists of the four cosets: (Use Algorithm)

$$N = \{e, a^2\}, \quad aN = \{a, a^3\}, \quad bN = \{b, a^2b\}, \quad abN = \{ab, a^3b\}.$$

We have

Example: $D_4/Z(D_4) \cong \mathbf{Z}_2 \times \mathbf{Z}_2$

$G = D_4 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$, where $a^4 = e, b^2 = e, ba = a^{-1}b$.

Let $N = \{e, a^2\}$ be the center $Z(D_4)$ of D_4. (See Claim 1)

The factor group G/N consists of the four cosets: (Use Algorithm)

$$N = \{e, a^2\}, \quad aN = \{a, a^3\}, \quad bN = \{b, a^2b\}, \quad abN = \{ab, a^3b\}.$$

We have

- $aNaN = a^2N = N$

Example: $D_4/Z(D_4) \cong \mathbf{Z}_2 \times \mathbf{Z}_2$

$G = D_4 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$, where $a^4 = e, b^2 = e, ba = a^{-1}b$.

Let $N = \{e, a^2\}$ be the center $Z(D_4)$ of D_4. (See Claim 1)

The factor group G/N consists of the four cosets: (Use Algorithm)

$$N = \{e, a^2\}, \quad aN = \{a, a^3\}, \quad bN = \{b, a^2b\}, \quad abN = \{ab, a^3b\}.$$

We have

- $aNaN = a^2N = N$
- $bNbN = b^2N = N$

Example: $D_4/Z(D_4) \cong \mathbf{Z}_2 \times \mathbf{Z}_2$

$G = D_4 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$, where $a^4 = e, b^2 = e, ba = a^{-1}b$.

Let $N = \{e, a^2\}$ be the center $Z(D_4)$ of D_4. (See Claim 1)

The factor group G/N consists of the four cosets: (Use Algorithm)

$$N = \{e, a^2\}, \quad aN = \{a, a^3\}, \quad bN = \{b, a^2b\}, \quad abN = \{ab, a^3b\}.$$

We have

- $aNaN = a^2N = N$
- $bNbN = b^2N = N$
- $abNabN = ababN = a(ba)bN = aa^{-1}bbN = N$

This shows that

Example: $D_4/Z(D_4) \cong \mathbf{Z}_2 \times \mathbf{Z}_2$

$G = D_4 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$, where $a^4 = e, b^2 = e, ba = a^{-1}b$.

Let $N = \{e, a^2\}$ be the center $Z(D_4)$ of D_4. (See Claim 1)

The factor group G/N consists of the four cosets: (Use Algorithm)

$$N = \{e, a^2\}, \quad aN = \{a, a^3\}, \quad bN = \{b, a^2b\}, \quad abN = \{ab, a^3b\}.$$

We have

- $aNaN = a^2N = N$
- $bNbN = b^2N = N$
- $abNabN = ababN = a(ba)bN = aa^{-1}bbN = N$

This shows that every non-identity element of G/N has order 2. That is,

Example: $D_4/Z(D_4) \cong \mathbf{Z}_2 \times \mathbf{Z}_2$

$G = D_4 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$, where $a^4 = e, b^2 = e, ba = a^{-1}b$.

Let $N = \{e, a^2\}$ be the center $Z(D_4)$ of D_4. (See Claim 1)

The factor group G/N consists of the four cosets: (Use Algorithm)

$$N = \{e, a^2\}, \quad aN = \{a, a^3\}, \quad bN = \{b, a^2b\}, \quad abN = \{ab, a^3b\}.$$

We have

- $aNaN = a^2N = N$
- $bNbN = b^2N = N$
- $abNabN = ababN = a(ba)bN = aa^{-1}bbN = N$

This shows that every non-identity element of G/N has order 2. That is,

$$D_4/Z(D_4) \cong \mathbf{Z}_2 \times \mathbf{Z}_2.$$

Remark 3 (Another way to show each of $\{aN, bN, abN\}$ has order 2)

Example: $D_4/Z(D_4) \cong \mathbf{Z}_2 \times \mathbf{Z}_2$

$G = D_4 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$, where $a^4 = e, b^2 = e, ba = a^{-1}b$.

Let $N = \{e, a^2\}$ be the center $Z(D_4)$ of D_4. (See Claim 1)

The factor group G/N consists of the four cosets: (Use Algorithm)

$$N = \{e, a^2\}, \quad aN = \{a, a^3\}, \quad bN = \{b, a^2b\}, \quad abN = \{ab, a^3b\}.$$

We have

- $aNaN = a^2N = N$
- $bNbN = b^2N = N$
- $abNabN = ababN = a(ba)bN = aa^{-1}bbN = N$

This shows that every non-identity element of G/N has order 2. That is,

$$D_4/Z(D_4) \cong \mathbf{Z}_2 \times \mathbf{Z}_2.$$

Remark 3 (Another way to show each of $\{aN, bN, abN\}$ has order 2)

Use Example 13:

Example: $D_4/Z(D_4) \cong \mathbf{Z}_2 \times \mathbf{Z}_2$

$G = D_4 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$, where $a^4 = e, b^2 = e, ba = a^{-1}b$.

Let $N = \{e, a^2\}$ be the center $Z(D_4)$ of D_4. (See Claim 1)

The factor group G/N consists of the four cosets: (Use Algorithm)

$$N = \{e, a^2\}, \quad aN = \{a, a^3\}, \quad bN = \{b, a^2b\}, \quad abN = \{ab, a^3b\}.$$

We have

- $aNaN = a^2N = N$
- $bNbN = b^2N = N$
- $abNabN = ababN = a(ba)bN = aa^{-1}bbN = N$

This shows that every non-identity element of G/N has order 2. That is,

$$D_4/Z(D_4) \cong \mathbf{Z}_2 \times \mathbf{Z}_2.$$

Remark 3 (Another way to show each of $\{aN, bN, abN\}$ has order 2)

Use Example 13: $o(aN) = \min\{n > 0 \mid a^n \in N\}$ *for any* $aN \in G/N$.

Example: $G = \mathbf{Z}_4 \times \mathbf{Z}_4$

Let $G = \mathbf{Z}_4 \times \mathbf{Z}_4$ and let $N = \{([0],[0]),([2],[0]),([0],[2]),([2],[2])\}$.

Example: $G = \mathbf{Z}_4 \times \mathbf{Z}_4$

Let $G = \mathbf{Z}_4 \times \mathbf{Z}_4$ and let $N = \{([0],[0]),([2],[0]),([0],[2]),([2],[2])\}$.

There are four cosets of this subgroup: $([G : H] = |G|/|H| = 4)$

Example: $G = \mathbf{Z}_4 \times \mathbf{Z}_4$

Let $G = \mathbf{Z}_4 \times \mathbf{Z}_4$ and let $N = \{([0],[0]),([2],[0]),([0],[2]),([2],[2])\}$.

There are four cosets of this subgroup: $([G : H] = |G|/|H| = 4)$

$$N, \quad ([1],[0]) + N, \quad ([0],[1]) + N, \quad ([1],[1]) + N.$$

Claim 2

Example: $G = \mathbf{Z}_4 \times \mathbf{Z}_4$

Let $G = \mathbf{Z}_4 \times \mathbf{Z}_4$ and let $N = \{([0],[0]),([2],[0]),([0],[2]),([2],[2])\}$.

There are four cosets of this subgroup: $([G : H] = |G|/|H| = 4)$

$$N, \quad ([1],[0]) + N, \quad ([0],[1]) + N, \quad ([1],[1]) + N.$$

Claim 2

$G/N \cong \mathbf{Z}_2 \times \mathbf{Z}_2$.

Example: $G = \mathbf{Z}_4 \times \mathbf{Z}_4$

Let $G = \mathbf{Z}_4 \times \mathbf{Z}_4$ and let $N = \{([0],[0]),([2],[0]),([0],[2]),([2],[2])\}$.

There are four cosets of this subgroup: $([G : H] = |G|/|H| = 4)$

$$N, \quad ([1],[0]) + N, \quad ([0],[1]) + N, \quad ([1],[1]) + N.$$

Claim 2

$G/N \cong \mathbf{Z}_2 \times \mathbf{Z}_2$. Each nontrivial element of the factor group has order 2.

Use Remark 3:

Example: $G = \mathbf{Z}_4 \times \mathbf{Z}_4$

Let $G = \mathbf{Z}_4 \times \mathbf{Z}_4$ and let $N = \{([0],[0]),([2],[0]),([0],[2]),([2],[2])\}$.

There are four cosets of this subgroup: $([G:H] = |G|/|H| = 4)$

$$N, \quad ([1],[0]) + N, \quad ([0],[1]) + N, \quad ([1],[1]) + N.$$

Claim 2

$G/N \cong \mathbf{Z}_2 \times \mathbf{Z}_2$. Each nontrivial element of the factor group has order 2.

Use Remark 3: $o(aN) = \min\{n > 0 \mid a^n \in N\}$ for any $aN \in G/N$. $\square$

Let $G = \mathbf{Z}_4 \times \mathbf{Z}_4$ and let $K = \{([0],[0]),([1],[0]),([2],[0]),([3],[0])\}$.

Example: $G = \mathbf{Z}_4 \times \mathbf{Z}_4$

Let $G = \mathbf{Z}_4 \times \mathbf{Z}_4$ and let $N = \{([0],[0]),([2],[0]),([0],[2]),([2],[2])\}$.

There are four cosets of this subgroup: ($[G : H] = |G|/|H| = 4$)

$$N, \quad ([1],[0]) + N, \quad ([0],[1]) + N, \quad ([1],[1]) + N.$$

Claim 2

$G/N \cong \mathbf{Z}_2 \times \mathbf{Z}_2$. Each nontrivial element of the factor group has order 2.

Use Remark 3: $o(aN) = \min\{n > 0 \mid a^n \in N\}$ for any $aN \in G/N$. $\square$

Let $G = \mathbf{Z}_4 \times \mathbf{Z}_4$ and let $K = \{([0],[0]),([1],[0]),([2],[0]),([3],[0])\}$.

There are four cosets of this subgroup: (Use Algorithm)

Example: $G = \mathbf{Z}_4 \times \mathbf{Z}_4$

Let $G = \mathbf{Z}_4 \times \mathbf{Z}_4$ and let $N = \{([0],[0]), ([2],[0]), ([0],[2]), ([2],[2])\}$.

There are four cosets of this subgroup: ($[G : H] = |G|/|H| = 4$)

$$N, \quad ([1],[0]) + N, \quad ([0],[1]) + N, \quad ([1],[1]) + N.$$

Claim 2

$G/N \cong \mathbf{Z}_2 \times \mathbf{Z}_2$. Each nontrivial element of the factor group has order 2.

Use Remark 3: $o(aN) = \min\{n > 0 \mid a^n \in N\}$ for any $aN \in G/N$. $\square$

Let $G = \mathbf{Z}_4 \times \mathbf{Z}_4$ and let $K = \{([0],[0]), ([1],[0]), ([2],[0]), ([3],[0])\}$.

There are four cosets of this subgroup: (Use Algorithm)

$$K, \quad ([0],[1]) + K, \quad ([0],[2]) + K, \quad ([0],[3]) + K.$$

Claim 3

Example: $G = \mathbf{Z}_4 \times \mathbf{Z}_4$

Let $G = \mathbf{Z}_4 \times \mathbf{Z}_4$ and let $N = \{([0],[0]),([2],[0]),([0],[2]),([2],[2])\}$.

There are four cosets of this subgroup: ($[G:H] = |G|/|H| = 4$)

$$N, \quad ([1],[0]) + N, \quad ([0],[1]) + N, \quad ([1],[1]) + N.$$

Claim 2

$G/N \cong \mathbf{Z}_2 \times \mathbf{Z}_2$. Each nontrivial element of the factor group has order 2.

Use Remark 3: $o(aN) = \min\{n > 0 \mid a^n \in N\}$ for any $aN \in G/N$. $\square$

Let $G = \mathbf{Z}_4 \times \mathbf{Z}_4$ and let $K = \{([0],[0]),([1],[0]),([2],[0]),([3],[0])\}$.

There are four cosets of this subgroup: (Use Algorithm)

$$K, \quad ([0],[1]) + K, \quad ([0],[2]) + K, \quad ([0],[3]) + K.$$

Claim 3

$G/K \cong \mathbf{Z}_4$. In particular,

Example: $G = \mathbf{Z}_4 \times \mathbf{Z}_4$

Let $G = \mathbf{Z}_4 \times \mathbf{Z}_4$ and let $N = \{([0],[0]),([2],[0]),([0],[2]),([2],[2])\}$.

There are four cosets of this subgroup: ($[G:H] = |G|/|H| = 4$)

$$N, \quad ([1],[0]) + N, \quad ([0],[1]) + N, \quad ([1],[1]) + N.$$

Claim 2

$G/N \cong \mathbf{Z}_2 \times \mathbf{Z}_2$. Each nontrivial element of the factor group has order 2.

Use Remark 3: $o(aN) = \min\{n > 0 \mid a^n \in N\}$ for any $aN \in G/N$. □

Let $G = \mathbf{Z}_4 \times \mathbf{Z}_4$ and let $K = \{([0],[0]),([1],[0]),([2],[0]),([3],[0])\}$.

There are four cosets of this subgroup: (Use Algorithm)

$$K, \quad ([0],[1]) + K, \quad ([0],[2]) + K, \quad ([0],[3]) + K.$$

Claim 3

$G/K \cong \mathbf{Z}_4$. In particular, $G/K = \langle ([0],[1]) + K \rangle$. (

Example: $G = \mathbf{Z}_4 \times \mathbf{Z}_4$

Let $G = \mathbf{Z}_4 \times \mathbf{Z}_4$ and let $N = \{([0],[0]), ([2],[0]), ([0],[2]), ([2],[2])\}$.

There are four cosets of this subgroup: $([G : H] = |G|/|H| = 4)$

$$N, \quad ([1],[0]) + N, \quad ([0],[1]) + N, \quad ([1],[1]) + N.$$

Claim 2

$G/N \cong \mathbf{Z}_2 \times \mathbf{Z}_2$. *Each nontrivial element of the factor group has order 2.*

Use Remark 3: $o(aN) = \min\{n > 0 \mid a^n \in N\}$ for any $aN \in G/N$. $\square$

Let $G = \mathbf{Z}_4 \times \mathbf{Z}_4$ and let $K = \{([0],[0]), ([1],[0]), ([2],[0]), ([3],[0])\}$.

There are four cosets of this subgroup: (Use Algorithm)

$$K, \quad ([0],[1]) + K, \quad ([0],[2]) + K, \quad ([0],[3]) + K.$$

Claim 3

$G/K \cong \mathbf{Z}_4$. *In particular,* $G/K = \langle ([0],[1]) + K \rangle$. *(Again use Remark 3)*

Factor groups of direct products

One way to define a subgroup of a direct product $G_1 \times G_2$ is to use normal subgroups $N_1 \subseteq G_1$ and $N_2 \subseteq G_2$ to construct the following subgroup:

$$N_1 \times N_2 = \{(x_1, x_2) \mid x_1 \in N_1, x_2 \in N_2\} \subseteq G_1 \times G_2.$$

Example 18 (In the previous example)

Factor groups of direct products

One way to define a subgroup of a direct product $G_1 \times G_2$ is to use normal subgroups $N_1 \subseteq G_1$ and $N_2 \subseteq G_2$ to construct the following subgroup:

$$N_1 \times N_2 = \{(x_1, x_2) \mid x_1 \in N_1, x_2 \in N_2\} \subseteq G_1 \times G_2.$$

Example 18 (In the previous example)

we computed the factor groups for the subgroups $2\mathbf{Z}_4 \times 2\mathbf{Z}_4$ and $\mathbf{Z}_4 \times \langle 0 \rangle$.

Proposition 6 (Let N_i be a normal subgroup of G_i with $i \in \{1, 2\}$.)

Factor groups of direct products

One way to define a subgroup of a direct product $G_1 \times G_2$ is to use normal subgroups $N_1 \subseteq G_1$ and $N_2 \subseteq G_2$ to construct the following subgroup:

$$N_1 \times N_2 = \{(x_1, x_2) \mid x_1 \in N_1, x_2 \in N_2\} \subseteq G_1 \times G_2.$$

Example 18 (In the previous example)

we computed the factor groups for the subgroups $2\mathbf{Z}_4 \times 2\mathbf{Z}_4$ and $\mathbf{Z}_4 \times \langle 0 \rangle$.

Proposition 6 (Let N_i be a normal subgroup of G_i with $i \in \{1, 2\}$.)

Then $N_1 \times N_2$ is a normal subgroup of the direct product $G_1 \times G_2$ and

$$(G_1 \times G_2)/(N_1 \times N_2) \cong (G_1/N_1) \times (G_2/N_2).$$

Proof of Proposition 6

Proof of Proposition 6

Define $\phi : G_1 \times G_2 \to (G_1/N_1) \times (G_2/N_2)$ by

$$\phi((x_1, x_2)) = (x_1 N_1, x_2 N_2) \text{ for all } x_1 \in G_1, x_2 \in G_2.$$

(i) well-defined:

Proof of Proposition 6

Define $\phi : G_1 \times G_2 \to (G_1/N_1) \times (G_2/N_2)$ by

$$\phi((x_1, x_2)) = (x_1 N_1, x_2 N_2) \text{ for all } x_1 \in G_1, x_2 \in G_2.$$

(i) well-defined: Trivial.

(ii) ϕ is a homomorphism:

Proof of Proposition 6

Define $\phi : G_1 \times G_2 \to (G_1/N_1) \times (G_2/N_2)$ by

$$\phi((x_1, x_2)) = (x_1 N_1, x_2 N_2) \text{ for all } x_1 \in G_1, x_2 \in G_2.$$

(i) well-defined: Trivial.

(ii) ϕ is a homomorphism: For any $(x_1, x_2), (y_1, y_2) \in G_1 \times G_2$, we have

Proof of Proposition 6

Define $\phi : G_1 \times G_2 \to (G_1/N_1) \times (G_2/N_2)$ by

$$\phi((x_1, x_2)) = (x_1 N_1, x_2 N_2) \text{ for all } x_1 \in G_1, x_2 \in G_2.$$

(i) well-defined: Trivial.

(ii) ϕ is a homomorphism: For any $(x_1, x_2), (y_1, y_2) \in G_1 \times G_2$, we have

$$\begin{aligned}
\phi((x_1, x_2)(y_1, y_2)) &= \phi((x_1 y_1, x_2 y_2)) \\
&= (x_1 y_1 N_1, x_2 y_2 N_2) \\
&\overset{!}{=} (x_1 N_1 y_1 N_1, x_2 N_2 y_2 N_2) \\
&= (x_1 N_1, x_2 N_2)(y_1 N_1, y_2 N_2) \\
&= \phi((x_1, x_2))\phi((y_1, y_2))
\end{aligned}$$

(iii) ϕ is onto:

Proof of Proposition 6

Define $\phi : G_1 \times G_2 \to (G_1/N_1) \times (G_2/N_2)$ by

$$\phi((x_1, x_2)) = (x_1 N_1, x_2 N_2) \text{ for all } x_1 \in G_1, x_2 \in G_2.$$

(i) well-defined: Trivial.

(ii) ϕ is a homomorphism: For any $(x_1, x_2), (y_1, y_2) \in G_1 \times G_2$, we have

$$\begin{aligned} \phi((x_1, x_2)(y_1, y_2)) &= \phi((x_1 y_1, x_2 y_2)) \\ &= (x_1 y_1 N_1, x_2 y_2 N_2) \\ &\overset{!}{=} (x_1 N_1 y_1 N_1, x_2 N_2 y_2 N_2) \\ &= (x_1 N_1, x_2 N_2)(y_1 N_1, y_2 N_2) \\ &= \phi((x_1, x_2))\phi((y_1, y_2)) \end{aligned}$$

(iii) ϕ is onto: Trivial.

(iv) $\ker(\phi) = \{(x_1, x_2) \mid \phi((x_1, x_2)) = (N_1, N_2)\} =$

Proof of Proposition 6

Define $\phi : G_1 \times G_2 \to (G_1/N_1) \times (G_2/N_2)$ by

$$\phi((x_1, x_2)) = (x_1 N_1, x_2 N_2) \text{ for all } x_1 \in G_1, x_2 \in G_2.$$

(i) well-defined: Trivial.

(ii) ϕ is a homomorphism: For any $(x_1, x_2), (y_1, y_2) \in G_1 \times G_2$, we have

$$\begin{aligned}
\phi((x_1, x_2)(y_1, y_2)) &= \phi((x_1 y_1, x_2 y_2)) \\
&= (x_1 y_1 N_1, x_2 y_2 N_2) \\
&\overset{!}{=} (x_1 N_1 y_1 N_1, x_2 N_2 y_2 N_2) \\
&= (x_1 N_1, x_2 N_2)(y_1 N_1, y_2 N_2) \\
&= \phi((x_1, x_2))\phi((y_1, y_2))
\end{aligned}$$

(iii) ϕ is onto: Trivial.

(iv) $\ker(\phi) = \{(x_1, x_2) \mid \phi((x_1, x_2)) = (N_1, N_2)\} = N_1 \times N_2$. (Check it!)

Proof of Proposition 6

Define $\phi : G_1 \times G_2 \to (G_1/N_1) \times (G_2/N_2)$ by

$$\phi((x_1, x_2)) = (x_1 N_1, x_2 N_2) \text{ for all } x_1 \in G_1, x_2 \in G_2.$$

(i) well-defined: Trivial.

(ii) ϕ is a homomorphism: For any $(x_1, x_2), (y_1, y_2) \in G_1 \times G_2$, we have

$$\begin{aligned} \phi((x_1, x_2)(y_1, y_2)) =& \phi((x_1 y_1, x_2 y_2)) \\ =& (x_1 y_1 N_1, x_2 y_2 N_2) \\ \overset{!}{=}& (x_1 N_1 y_1 N_1, x_2 N_2 y_2 N_2) \\ =& (x_1 N_1, x_2 N_2)(y_1 N_1, y_2 N_2) \\ =& \phi((x_1, x_2))\phi((y_1, y_2)) \end{aligned}$$

(iii) ϕ is onto: Trivial.

(iv) $\ker(\phi) = \{(x_1, x_2) \mid \phi((x_1, x_2)) = (N_1, N_2)\} = N_1 \times N_2$. (Check it!)

The desired results follow from the fundamental homomorphism theorem.

Example: $G = \mathbf{Z}_4 \times \mathbf{Z}_4$

Let N be the "diagonal" subgroup generated by $([1], [1])$. Then

Example: $G = \mathbf{Z}_4 \times \mathbf{Z}_4$

Let N be the "diagonal" subgroup generated by $([1], [1])$. Then

$$N = \{([0], [0]), ([1], [1]), ([2], [2]), ([3], [3])\}$$

and the factor group G/N will have four elements (Why?), so

Example: $G = \mathbf{Z}_4 \times \mathbf{Z}_4$

Let N be the "diagonal" subgroup generated by $([1],[1])$. Then

$$N = \{([0],[0]),([1],[1]),([2],[2]),([3],[3])\}$$

and the factor group G/N will have four elements (Why?), so it must be isomorphic to either $\mathbf{Z}_4$ or $\mathbf{Z}_2 \times \mathbf{Z}_2$. (Why?)

Claim 4

Example: $G = \mathbf{Z}_4 \times \mathbf{Z}_4$

Let N be the "diagonal" subgroup generated by $([1],[1])$. Then

$$N = \{([0],[0]),([1],[1]),([2],[2]),([3],[3])\}$$

and the factor group G/N will have four elements (Why?), so it must be isomorphic to either $\mathbf{Z}_4$ or $\mathbf{Z}_2 \times \mathbf{Z}_2$. (Why?)

Claim 4

$G/N \cong \mathbf{Z}_4$. That is, G/N is cyclic.

Proof.

Example: $G = \mathbf{Z}_4 \times \mathbf{Z}_4$

Let N be the "diagonal" subgroup generated by $([1],[1])$. Then

$$N = \{([0],[0]),([1],[1]),([2],[2]),([3],[3])\}$$

and the factor group G/N will have four elements (Why?), so it must be isomorphic to either $\mathbf{Z}_4$ or $\mathbf{Z}_2 \times \mathbf{Z}_2$. (Why?)

Claim 4

$G/N \cong \mathbf{Z}_4$. That is, G/N is cyclic.

Proof.

Consider the coset $([1],[0]) + N$ and

Example: $G = \mathbf{Z}_4 \times \mathbf{Z}_4$

Let N be the "diagonal" subgroup generated by $([1], [1])$. Then

$$N = \{([0], [0]), ([1], [1]), ([2], [2]), ([3], [3])\}$$

and the factor group G/N will have four elements (Why?), so it must be isomorphic to either $\mathbf{Z}_4$ or $\mathbf{Z}_2 \times \mathbf{Z}_2$. (Why?)

Claim 4

$G/N \cong \mathbf{Z}_4$. That is, G/N is cyclic.

Proof.

Consider the coset $([1], [0]) + N$ and the smallest positive multiple of $([1], [0])$ that belongs to N is $4 \cdot ([1], [0]) = ([0], [0])$.

Example: $G = \mathbf{Z}_4 \times \mathbf{Z}_4$

Let N be the "diagonal" subgroup generated by $([1],[1])$. Then

$$N = \{([0],[0]),([1],[1]),([2],[2]),([3],[3])\}$$

and the factor group G/N will have four elements (Why?), so it must be isomorphic to either $\mathbf{Z}_4$ or $\mathbf{Z}_2 \times \mathbf{Z}_2$. (Why?)

Claim 4

$G/N \cong \mathbf{Z}_4$. That is, G/N is cyclic.

Proof.

Consider the coset $([1],[0]) + N$ and the smallest positive multiple of $([1],[0])$ that belongs to N is $4 \cdot ([1],[0]) = ([0],[0])$. By Remark 3, the coset $([1],[0]) + N$ has order 4.

Example: $G = \mathbf{Z}_4 \times \mathbf{Z}_4$

Let N be the "diagonal" subgroup generated by $([1],[1])$. Then

$$N = \{([0],[0]),([1],[1]),([2],[2]),([3],[3])\}$$

and the factor group G/N will have four elements (Why?), so it must be isomorphic to either $\mathbf{Z}_4$ or $\mathbf{Z}_2 \times \mathbf{Z}_2$. (Why?)

Claim 4

$G/N \cong \mathbf{Z}_4$. That is, G/N is cyclic.

Proof.

Consider the coset $([1],[0]) + N$ and the smallest positive multiple of $([1],[0])$ that belongs to N is $4 \cdot ([1],[0]) = ([0],[0])$. By Remark 3, the coset $([1],[0]) + N$ has order 4. This completes the proof. $\square$

Note 8

Example: $G = \mathbf{Z}_4 \times \mathbf{Z}_4$

Let N be the "diagonal" subgroup generated by $([1],[1])$. Then

$$N = \{([0],[0]),([1],[1]),([2],[2]),([3],[3])\}$$

and the factor group G/N will have four elements (Why?), so it must be isomorphic to either $\mathbf{Z}_4$ or $\mathbf{Z}_2 \times \mathbf{Z}_2$. (Why?)

Claim 4

$G/N \cong \mathbf{Z}_4$. That is, G/N is cyclic.

Proof.

Consider the coset $([1],[0]) + N$ and the smallest positive multiple of $([1],[0])$ that belongs to N is $4 \cdot ([1],[0]) = ([0],[0])$. By Remark 3, the coset $([1],[0]) + N$ has order 4. This completes the proof. □

Note 8

N cannot be described in the manner of $N_1 \times N_2$ as in Proposition 6.

Example: $\mathrm{GL}_n(\mathbf{R})/\mathrm{SL}_n(\mathbf{R}) \cong \mathbf{R}^\times$

Example: $\mathrm{GL}_n(\mathbf{R})/\mathrm{SL}_n(\mathbf{R}) \cong \mathbf{R}^\times$

Define $\phi : \mathrm{GL}_n(\mathbf{R}) \to \mathbf{R}^\times$ by $\phi(A) = \det(A)$, for any matrix $A \in \mathrm{GL}_n(\mathbf{R})$.

(i) well-defined:

Example: $\mathrm{GL}_n(\mathbf{R})/\mathrm{SL}_n(\mathbf{R}) \cong \mathbf{R}^\times$

Define $\phi : \mathrm{GL}_n(\mathbf{R}) \to \mathbf{R}^\times$ by $\phi(A) = \det(A)$, for any matrix $A \in \mathrm{GL}_n(\mathbf{R})$.

(i) well-defined: Trivial.

(ii) ϕ is a homomorphism: (Check it!) [

Example: $\mathrm{GL}_n(\mathbf{R})/\mathrm{SL}_n(\mathbf{R}) \cong \mathbf{R}^\times$

Define $\phi : \mathrm{GL}_n(\mathbf{R}) \to \mathbf{R}^\times$ by $\phi(A) = \det(A)$, for any matrix $A \in \mathrm{GL}_n(\mathbf{R})$.

(i) well-defined: Trivial.

(ii) ϕ is a homomorphism: (Check it!) [$\det(AB) = \det(A)\det(B)$]

(iii) ϕ is onto:

Example: $\mathrm{GL}_n(\mathbf{R})/\mathrm{SL}_n(\mathbf{R}) \cong \mathbf{R}^\times$

Define $\phi : \mathrm{GL}_n(\mathbf{R}) \to \mathbf{R}^\times$ by $\phi(A) = \det(A)$, for any matrix $A \in \mathrm{GL}_n(\mathbf{R})$.

(i) well-defined: Trivial.

(ii) ϕ is a homomorphism: (Check it!) [$\det(AB) = \det(A)\det(B)$]

(iii) ϕ is onto: For any $a \in \mathbf{R}^\times$, we have

Example: $\mathrm{GL}_n(\mathbf{R})/\mathrm{SL}_n(\mathbf{R}) \cong \mathbf{R}^\times$

Define $\phi : \mathrm{GL}_n(\mathbf{R}) \to \mathbf{R}^\times$ by $\phi(A) = \det(A)$, for any matrix $A \in \mathrm{GL}_n(\mathbf{R})$.

(i) well-defined: Trivial.

(ii) ϕ is a homomorphism: (Check it!) [$\det(AB) = \det(A)\det(B)$]

(iii) ϕ is onto: For any $a \in \mathbf{R}^\times$, we have

$$\phi\left(\begin{bmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & a \end{bmatrix}\right) = \det\left(\begin{bmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & a \end{bmatrix}\right) = a.$$

(iv) $\ker(\phi) = \{A \mid \phi(A) = \det(A) = 1\} =$

Example: $\mathrm{GL}_n(\mathbf{R})/\mathrm{SL}_n(\mathbf{R}) \cong \mathbf{R}^\times$

Define $\phi : \mathrm{GL}_n(\mathbf{R}) \to \mathbf{R}^\times$ by $\phi(A) = \det(A)$, for any matrix $A \in \mathrm{GL}_n(\mathbf{R})$.

(i) well-defined: Trivial.

(ii) ϕ is a homomorphism: (Check it!) [$\det(AB) = \det(A)\det(B)$]

(iii) ϕ is onto: For any $a \in \mathbf{R}^\times$, we have

$$\phi\left(\begin{bmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & a \end{bmatrix}\right) = \det\left(\begin{bmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & a \end{bmatrix}\right) = a.$$

(iv) $\ker(\phi) = \{A \mid \phi(A) = \det(A) = 1\} = \mathrm{SL}_n(\mathbf{R})$.

Example: $\mathrm{GL}_n(\mathbf{R})/\mathrm{SL}_n(\mathbf{R}) \cong \mathbf{R}^\times$

Define $\phi : \mathrm{GL}_n(\mathbf{R}) \to \mathbf{R}^\times$ by $\phi(A) = \det(A)$, for any matrix $A \in \mathrm{GL}_n(\mathbf{R})$.

(i) well-defined: Trivial.

(ii) ϕ is a homomorphism: (Check it!) [$\det(AB) = \det(A)\det(B)$]

(iii) ϕ is onto: For any $a \in \mathbf{R}^\times$, we have

$$\phi\left(\begin{bmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & a \end{bmatrix}\right) = \det\left(\begin{bmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & a \end{bmatrix}\right) = a.$$

(iv) $\ker(\phi) = \{A \mid \phi(A) = \det(A) = 1\} = \mathrm{SL}_n(\mathbf{R})$.

The desired results follow from the fundamental homomorphism theorem.

Example: Internal direct product

Proposition 7

Example: Internal direct product

Proposition 7

A group G with subgroups H and K is called the **internal direct product of** H **and** K *if* (i) *H and K are normal in G,* (ii) *$H \cap K = \{e\}$, and* (iii) *$HK = G$. Prove that in this case $G \cong H \times K$.*

Note 9

Example: Internal direct product

Proposition 7

A group G with subgroups H and K is called the **internal direct product of H and K** *if* (i) *H and K are normal in G,* (ii) *$H \cap K = \{e\}$, and* (iii) *$HK = G$. Prove that in this case $G \cong H \times K$.*

Note 9

Example 1 in Exam II Review is a special case of Proposition 7.

Example: Internal direct product

Proposition 7

A group G with subgroups H and K is called the **internal direct product of H and K** *if* (i) *H and K are normal in G,* (ii) *$H \cap K = \{e\}$, and* (iii) *$HK = G$. Prove that in this case $G \cong H \times K$.*

Note 9

Example 1 in Exam II Review is a special case of Proposition 7.

Define $\phi : H \times K \to G$ by $\phi((h, k)) = hk$, for all $(h, k) \in H \times K$.

(i) well-defined:

Example: Internal direct product

Proposition 7

A group G with subgroups H and K is called the **internal direct product of** H **and** K *if* (i) *H and K are normal in G,* (ii) *$H \cap K = \{e\}$, and* (iii) *$HK = G$. Prove that in this case $G \cong H \times K$.*

Note 9

Example 1 in Exam II Review is a special case of Proposition 7.

Define $\phi : H \times K \to G$ by $\phi((h, k)) = hk$, for all $(h, k) \in H \times K$.

(i) well-defined: Trivial. (Why?)

(ii) ϕ is a homomorphism: (Check it!) [

Example: Internal direct product

Proposition 7

A group G with subgroups H and K is called the **internal direct product of H and K** *if* (i) *H and K are normal in G,* (ii) *$H \cap K = \{e\}$, and* (iii) *$HK = G$. Prove that in this case $G \cong H \times K$.*

Note 9

Example 1 in Exam II Review is a special case of Proposition 7.

Define $\phi : H \times K \to G$ by $\phi((h,k)) = hk$, for all $(h,k) \in H \times K$.

(i) well-defined: Trivial. (Why?)

(ii) ϕ is a homomorphism: (Check it!) [See next slide]

(iii) onto:

Example: Internal direct product

Proposition 7

A group G with subgroups H and K is called the **internal direct product of H and K** *if* (i) *H and K are normal in G,* (ii) *$H \cap K = \{e\}$, and* (iii) *$HK = G$. Prove that in this case $G \cong H \times K$.*

Note 9

Example 1 in Exam II Review is a special case of Proposition 7.

Define $\phi : H \times K \to G$ by $\phi((h, k)) = hk$, for all $(h, k) \in H \times K$.

(i) well-defined: Trivial. (Why?)

(ii) ϕ is a homomorphism: (Check it!) [See next slide]

(iii) onto: Trivial. (Why?)

(iv) $\ker(\phi) = \{(h, k) \mid \phi((h, k)) = e\} \stackrel{!}{=}$

Example: Internal direct product

Proposition 7

A group G with subgroups H and K is called the **internal direct product of H and K** *if* (i) *H and K are normal in G,* (ii) *$H \cap K = \{e\}$, and* (iii) *$HK = G$. Prove that in this case $G \cong H \times K$.*

Note 9

Example 1 in Exam II Review is a special case of Proposition 7.

Define $\phi : H \times K \to G$ by $\phi((h,k)) = hk$, for all $(h,k) \in H \times K$.

(i) well-defined: Trivial. (Why?)

(ii) ϕ is a homomorphism: (Check it!) [See next slide]

(iii) onto: Trivial. (Why?)

(iv) $\ker(\phi) = \{(h,k) \mid \phi((h,k)) = e\} \stackrel{!}{=} \{(h,k) \mid h,k \in H \cap K\} =$

Example: Internal direct product

Proposition 7

A group G with subgroups H and K is called the **internal direct product of H and K** *if* (i) *H and K are normal in G,* (ii) *$H \cap K = \{e\}$, and* (iii) *$HK = G$. Prove that in this case $G \cong H \times K$.*

Note 9

Example 1 in Exam II Review is a special case of Proposition 7.

Define $\phi : H \times K \to G$ by $\phi((h,k)) = hk$, for all $(h,k) \in H \times K$.

(i) well-defined: Trivial. (Why?)

(ii) ϕ is a homomorphism: (Check it!) [See next slide]

(iii) onto: Trivial. (Why?)

(iv) $\ker(\phi) = \{(h,k) \mid \phi((h,k)) = e\} \overset{!}{=} \{(h,k) \mid h,k \in H \cap K\} = \{(e,e)\}$

$\overset{!}{=}$ holds since

Example: Internal direct product

Proposition 7

A group G with subgroups H and K is called the **internal direct product of H and K** *if* (i) *H and K are normal in G,* (ii) *$H \cap K = \{e\}$, and* (iii) *$HK = G$. Prove that in this case $G \cong H \times K$.*

Note 9

Example 1 in Exam II Review is a special case of Proposition 7.

Define $\phi : H \times K \to G$ by $\phi((h,k)) = hk$, for all $(h,k) \in H \times K$.

(i) well-defined: Trivial. (Why?)

(ii) ϕ is a homomorphism: (Check it!) [See next slide]

(iii) onto: Trivial. (Why?)

(iv) $\ker(\phi) = \{(h,k) \mid \phi((h,k)) = e\} \stackrel{!}{=} \{(h,k) \mid h,k \in H \cap K\} = \{(e,e)\}$

$\stackrel{!}{=}$ holds since $hk = e \Rightarrow h = k^{-1} \in K \cap H$ &

Example: Internal direct product

Proposition 7

A group G with subgroups H and K is called the **internal direct product of H and K** *if* (i) *H and K are normal in G,* (ii) *$H \cap K = \{e\}$, and* (iii) *$HK = G$. Prove that in this case $G \cong H \times K$.*

Note 9

Example 1 in Exam II Review is a special case of Proposition 7.

Define $\phi : H \times K \to G$ by $\phi((h,k)) = hk$, for all $(h,k) \in H \times K$.

(i) well-defined: Trivial. (Why?)

(ii) ϕ is a homomorphism: (Check it!) [See next slide]

(iii) onto: Trivial. (Why?)

(iv) $\ker(\phi) = \{(h,k) \mid \phi((h,k)) = e\} \overset{!}{=} \{(h,k) \mid h,k \in H \cap K\} = \{(e,e)\}$

$\overset{!}{=}$ holds since $hk = e \Rightarrow h = k^{-1} \in K \cap H$ & $k = h^{-1} \in H \cap K$

Example: Internal direct product

Proposition 7

A group G with subgroups H and K is called the **internal direct product of H and K** *if* (i) *H and K are normal in G,* (ii) *$H \cap K = \{e\}$, and* (iii) *$HK = G$. Prove that in this case $G \cong H \times K$.*

Note 9

Example 1 in Exam II Review is a special case of Proposition 7.

Define $\phi : H \times K \to G$ by $\phi((h,k)) = hk$, for all $(h,k) \in H \times K$.

(i) well-defined: Trivial. (Why?)

(ii) ϕ is a homomorphism: (Check it!) [See next slide]

(iii) onto: Trivial. (Why?)

(iv) $\ker(\phi) = \{(h,k) \mid \phi((h,k)) = e\} \overset{!}{=} \{(h,k) \mid h,k \in H \cap K\} = \{(e,e)\}$

$\overset{!}{=}$ holds since $hk = e \Rightarrow h = k^{-1} \in K \cap H$ & $k = h^{-1} \in H \cap K$

The desired results follow from the fundamental homomorphism theorem.

Proof of Proposition 7 cont.: ϕ is a homomorphism

A group G is called the **internal direct product of H and K** if
(i) H and K are normal in G, (ii) $H \cap K = \{e\}$, and (iii) $HK = G$.

Define $\phi : H \times K \to G$ by $\phi((h,k)) = hk$, for all $(h,k) \in H \times K$.

ϕ is a homomorphism:

Proof of Proposition 7 cont.: ϕ is a homomorphism

A group G is called the **internal direct product of H and K** if
(i) H and K are normal in G, (ii) $H \cap K = \{e\}$, and (iii) $HK = G$.

Define $\phi : H \times K \to G$ by $\phi((h,k)) = hk$, for all $(h,k) \in H \times K$.

ϕ is a homomorphism: For all $(h_1, k_1), (h_2, k_2) \in H \times K$, we have

$$\begin{aligned}\phi((h_1, k_1)(h_2, k_2)) &= \phi((h_1 h_2, k_1 k_2)) \\ &= h_1 h_2 k_1 k_2 \stackrel{!}{=} h_1 k_1 h_2 k_2 = \phi((h_1, k_1))\phi((h_2, k_2))\end{aligned}$$

Claim 5

$\stackrel{!}{=}$ *holds* $\Leftrightarrow$

Proof of Proposition 7 cont.: ϕ is a homomorphism

A group G is called the **internal direct product of H and K** if
(i) H and K are normal in G, (ii) $H \cap K = \{e\}$, and (iii) $HK = G$.

Define $\phi : H \times K \to G$ by $\phi((h,k)) = hk$, for all $(h,k) \in H \times K$.

ϕ is a homomorphism: For all $(h_1, k_1), (h_2, k_2) \in H \times K$, we have

$$\begin{aligned}\phi((h_1, k_1)(h_2, k_2)) &= \phi((h_1 h_2, k_1 k_2)) \\ &= h_1 h_2 k_1 k_2 \overset{!}{=} h_1 k_1 h_2 k_2 = \phi((h_1, k_1))\phi((h_2, k_2))\end{aligned}$$

Claim 5

$\overset{!}{=}$ *holds* $\Leftrightarrow h_2 k_1 = k_1 h_2 \Leftrightarrow$

Proof of Proposition 7 cont.: ϕ is a homomorphism

A group G is called the **internal direct product of H and K** if (i) H and K are normal in G, (ii) $H \cap K = \{e\}$, and (iii) $HK = G$.

Define $\phi : H \times K \to G$ by $\phi((h,k)) = hk$, for all $(h,k) \in H \times K$.

ϕ is a homomorphism: For all $(h_1, k_1), (h_2, k_2) \in H \times K$, we have

$$\begin{aligned}\phi((h_1,k_1)(h_2,k_2)) &= \phi((h_1h_2, k_1k_2)) \\ &= h_1h_2k_1k_2 \overset{!}{=} h_1k_1h_2k_2 = \phi((h_1,k_1))\phi((h_2,k_2))\end{aligned}$$

Claim 5

$\overset{!}{=}$ *holds* $\Leftrightarrow h_2k_1 = k_1h_2 \Leftrightarrow k_1^{-1}h_2k_1h_2^{-1} = e$. *To show* $k_1^{-1}h_2k_1h_2^{-1} = e$.

Proof of Claim 5.

Proof of Proposition 7 cont.: ϕ is a homomorphism

A group G is called the **internal direct product of H and K** if
(i) H and K are normal in G, (ii) $H \cap K = \{e\}$, and (iii) $HK = G$.

Define $\phi : H \times K \to G$ by $\phi((h,k)) = hk$, for all $(h,k) \in H \times K$.

ϕ is a homomorphism: For all $(h_1, k_1), (h_2, k_2) \in H \times K$, we have

$$\begin{aligned}\phi((h_1,k_1)(h_2,k_2)) &= \phi((h_1h_2, k_1k_2)) \\ &= h_1h_2k_1k_2 \stackrel{!}{=} h_1k_1h_2k_2 = \phi((h_1,k_1))\phi((h_2,k_2))\end{aligned}$$

Claim 5

$\stackrel{!}{=}$ *holds* $\Leftrightarrow h_2k_1 = k_1h_2 \Leftrightarrow k_1^{-1}h_2k_1h_2^{-1} = e$. *To show* $k_1^{-1}h_2k_1h_2^{-1} = e$.

Proof of Claim 5.

$k_1^{-1}h_2k_1h_2^{-1} \in H$: (Why?) Since

Proof of Proposition 7 cont.: ϕ is a homomorphism

A group G is called the **internal direct product of H and K** if (i) H and K are normal in G, (ii) $H \cap K = \{e\}$, and (iii) $HK = G$.

Define $\phi : H \times K \to G$ by $\phi((h,k)) = hk$, for all $(h,k) \in H \times K$.

ϕ is a homomorphism: For all $(h_1,k_1),(h_2,k_2) \in H \times K$, we have

$$\begin{aligned}\phi((h_1,k_1)(h_2,k_2)) &= \phi((h_1h_2, k_1k_2)) \\ &= h_1h_2k_1k_2 \overset{!}{=} h_1k_1h_2k_2 = \phi((h_1,k_1))\phi((h_2,k_2))\end{aligned}$$

Claim 5

$\overset{!}{=}$ *holds* $\Leftrightarrow h_2k_1 = k_1h_2 \Leftrightarrow k_1^{-1}h_2k_1h_2^{-1} = e$. *To show* $k_1^{-1}h_2k_1h_2^{-1} = e$.

Proof of Claim 5.

$k_1^{-1}h_2k_1h_2^{-1} \in H$: (Why?) Since $k_1^{-1}h_2k_1 \in H$ (Why?) and

Proof of Proposition 7 cont.: ϕ is a homomorphism

A group G is called the **internal direct product of H and K** if (i) H and K are normal in G, (ii) $H \cap K = \{e\}$, and (iii) $HK = G$.

Define $\phi : H \times K \to G$ by $\phi((h, k)) = hk$, for all $(h, k) \in H \times K$.

ϕ is a homomorphism: For all $(h_1, k_1), (h_2, k_2) \in H \times K$, we have

$$\begin{aligned}\phi((h_1, k_1)(h_2, k_2)) &= \phi((h_1 h_2, k_1 k_2)) \\ &= h_1 h_2 k_1 k_2 \overset{!}{=} h_1 k_1 h_2 k_2 = \phi((h_1, k_1))\phi((h_2, k_2))\end{aligned}$$

Claim 5

$\overset{!}{=}$ holds $\Leftrightarrow h_2 k_1 = k_1 h_2 \Leftrightarrow k_1^{-1} h_2 k_1 h_2^{-1} = e$. To show $k_1^{-1} h_2 k_1 h_2^{-1} = e$.

Proof of Claim 5.

$k_1^{-1} h_2 k_1 h_2^{-1} \in H$: (Why?) Since $k_1^{-1} h_2 k_1 \in H$ (Why?) and $h_2^{-1} \in H$.
$k_1^{-1} h_2 k_1 h_2^{-1} \in K$: (Why?) Since

Proof of Proposition 7 cont.: ϕ is a homomorphism

A group G is called the **internal direct product of H and K** if (i) H and K are normal in G, (ii) $H \cap K = \{e\}$, and (iii) $HK = G$.

Define $\phi : H \times K \to G$ by $\phi((h, k)) = hk$, for all $(h, k) \in H \times K$.

ϕ is a homomorphism: For all $(h_1, k_1), (h_2, k_2) \in H \times K$, we have

$$\begin{aligned} \phi((h_1, k_1)(h_2, k_2)) &= \phi((h_1 h_2, k_1 k_2)) \\ &= h_1 h_2 k_1 k_2 \stackrel{!}{=} h_1 k_1 h_2 k_2 = \phi((h_1, k_1))\phi((h_2, k_2)) \end{aligned}$$

Claim 5

$\stackrel{!}{=}$ *holds* $\Leftrightarrow h_2 k_1 = k_1 h_2 \Leftrightarrow k_1^{-1} h_2 k_1 h_2^{-1} = e$. *To show* $k_1^{-1} h_2 k_1 h_2^{-1} = e$.

Proof of Claim 5.

$k_1^{-1} h_2 k_1 h_2^{-1} \in H$: (Why?) Since $k_1^{-1} h_2 k_1 \in H$ (Why?) and $h_2^{-1} \in H$.
$k_1^{-1} h_2 k_1 h_2^{-1} \in K$: (Why?) Since $h_2 k_1 h_2^{-1} \in K$ (Why?) and

Proof of Proposition 7 cont.: ϕ is a homomorphism

A group G is called the **internal direct product of H and K** if (i) H and K are normal in G, (ii) $H \cap K = \{e\}$, and (iii) $HK = G$.

Define $\phi : H \times K \to G$ by $\phi((h,k)) = hk$, for all $(h,k) \in H \times K$.

ϕ is a homomorphism: For all $(h_1, k_1), (h_2, k_2) \in H \times K$, we have

$$\begin{aligned}\phi((h_1,k_1)(h_2,k_2)) &= \phi((h_1 h_2, k_1 k_2)) \\ &= h_1 h_2 k_1 k_2 \overset{!}{=} h_1 k_1 h_2 k_2 = \phi((h_1,k_1))\phi((h_2,k_2))\end{aligned}$$

Claim 5

$\overset{!}{=}$ *holds* $\Leftrightarrow h_2 k_1 = k_1 h_2 \Leftrightarrow k_1^{-1} h_2 k_1 h_2^{-1} = e$. *To show* $k_1^{-1} h_2 k_1 h_2^{-1} = e$.

Proof of Claim 5.

$k_1^{-1} h_2 k_1 h_2^{-1} \in H$: (Why?) Since $k_1^{-1} h_2 k_1 \in H$ (Why?) and $h_2^{-1} \in H$.
$k_1^{-1} h_2 k_1 h_2^{-1} \in K$: (Why?) Since $h_2 k_1 h_2^{-1} \in K$ (Why?) and $k_1^{-1} \in K$.
This implies

Proof of Proposition 7 cont.: ϕ is a homomorphism

A group G is called the **internal direct product of H and K** if (i) H and K are normal in G, (ii) $H \cap K = \{e\}$, and (iii) $HK = G$.

Define $\phi : H \times K \to G$ by $\phi((h,k)) = hk$, for all $(h,k) \in H \times K$.

ϕ is a homomorphism: For all $(h_1, k_1), (h_2, k_2) \in H \times K$, we have

$$\begin{aligned}\phi((h_1, k_1)(h_2, k_2)) &= \phi((h_1 h_2, k_1 k_2)) \\ &= h_1 h_2 k_1 k_2 \stackrel{!}{=} h_1 k_1 h_2 k_2 = \phi((h_1, k_1))\phi((h_2, k_2))\end{aligned}$$

Claim 5

$\stackrel{!}{=}$ *holds* $\Leftrightarrow h_2 k_1 = k_1 h_2 \Leftrightarrow k_1^{-1} h_2 k_1 h_2^{-1} = e$. *To show* $k_1^{-1} h_2 k_1 h_2^{-1} = e$.

Proof of Claim 5.

$k_1^{-1} h_2 k_1 h_2^{-1} \in H$: (Why?) Since $k_1^{-1} h_2 k_1 \in H$ (Why?) and $h_2^{-1} \in H$.
$k_1^{-1} h_2 k_1 h_2^{-1} \in K$: (Why?) Since $h_2 k_1 h_2^{-1} \in K$ (Why?) and $k_1^{-1} \in K$.
This implies $k_1^{-1} h_2 k_1 h_2^{-1} \in H \cap K = \{e\}$. (Why?)

Proof of Proposition 7 cont.: ϕ is a homomorphism

A group G is called the **internal direct product of H and K** if (i) H and K are normal in G, (ii) $H \cap K = \{e\}$, and (iii) $HK = G$.

Define $\phi : H \times K \to G$ by $\phi((h, k)) = hk$, for all $(h, k) \in H \times K$.

ϕ is a homomorphism: For all $(h_1, k_1), (h_2, k_2) \in H \times K$, we have

$$\begin{aligned}\phi((h_1, k_1)(h_2, k_2)) &= \phi((h_1 h_2, k_1 k_2)) \\ &= h_1 h_2 k_1 k_2 \overset{!}{=} h_1 k_1 h_2 k_2 = \phi((h_1, k_1))\phi((h_2, k_2))\end{aligned}$$

Claim 5

$\overset{!}{=}$ holds $\Leftrightarrow h_2 k_1 = k_1 h_2 \Leftrightarrow k_1^{-1} h_2 k_1 h_2^{-1} = e$. To show $k_1^{-1} h_2 k_1 h_2^{-1} = e$.

Proof of Claim 5.

$k_1^{-1} h_2 k_1 h_2^{-1} \in H$: (Why?) Since $k_1^{-1} h_2 k_1 \in H$ (Why?) and $h_2^{-1} \in H$.
$k_1^{-1} h_2 k_1 h_2^{-1} \in K$: (Why?) Since $h_2 k_1 h_2^{-1} \in K$ (Why?) and $k_1^{-1} \in K$.
This implies $k_1^{-1} h_2 k_1 h_2^{-1} \in H \cap K = \{e\}$. (Why?) Hence proved. $\square$