Modern Algebra I

Lecture 2

Jung-Chen Liu

liujc@math.ntnu.edu.tw

2009, Fall

We will cover the following sections today:

We will cover the following sections today:

Section I.4: Cosets and Counting

We will cover the following sections today:

Section I.4: Cosets and Counting

Section I.5: Normality, Quotient Groups, and Homomorphisms

Equivalence Relations

Equivalence Relations

Let A and B be nonempty sets

Equivalence Relations

Let A and B be nonempty sets and consider the set $A \times B = \{(a, b) \mid a \in A,\ b \in B\}$.

Equivalence Relations

Let A and B be nonempty sets and consider the set $A \times B = \{(a, b) \mid a \in A,\ b \in B\}$.

- A relation R on $A \times B$

Equivalence Relations

Let A and B be nonempty sets and consider the set $A \times B = \{(a, b) \mid a \in A,\ b \in B\}$.

- A relation R on $A \times B$ is a subset of $A \times B$,

Equivalence Relations

Let A and B be nonempty sets and consider the set $A \times B = \{(a, b) \mid a \in A,\ b \in B\}$.

- A relation R on $A \times B$ is a subset of $A \times B$, i.e., $R \subseteq A \times B$.

Equivalence Relations

Let A and B be nonempty sets and consider the set $A \times B = \{(a, b) \mid a \in A,\ b \in B\}$.

- A relation R on $A \times B$ is a subset of $A \times B$, i.e., $R \subseteq A \times B$.
- A relation R on $A \times A$ is an equivalence relation on A if R is

Equivalence Relations

Let A and B be nonempty sets and consider the set $A \times B = \{(a, b) \mid a \in A,\ b \in B\}$.

- A relation R on $A \times B$ is a subset of $A \times B$, i.e., $R \subseteq A \times B$.
- A relation R on $A \times A$ is an equivalence relation on A if R is
  - reflexive,

Equivalence Relations

Let A and B be nonempty sets and consider the set $A \times B = \{(a, b) \mid a \in A,\ b \in B\}$.

- A relation R on $A \times B$ is a subset of $A \times B$, i.e., $R \subseteq A \times B$.
- A relation R on $A \times A$ is an equivalence relation on A if R is
  - reflexive, i.e., $\forall a \in A, (a, a) \in R$;

Equivalence Relations

Let A and B be nonempty sets and consider the set $A \times B = \{(a, b) \mid a \in A,\ b \in B\}$.

- A relation R on $A \times B$ is a subset of $A \times B$, i.e., $R \subseteq A \times B$.
- A relation R on $A \times A$ is an equivalence relation on A if R is
  - reflexive, i.e., $\forall a \in A, (a, a) \in R$;
  - symmetric,

Equivalence Relations

Let A and B be nonempty sets and consider the set $A \times B = \{(a, b) \mid a \in A,\ b \in B\}$.

- A relation R on $A \times B$ is a subset of $A \times B$, i.e., $R \subseteq A \times B$.
- A relation R on $A \times A$ is an equivalence relation on A if R is
  - reflexive, i.e., $\forall a \in A, (a, a) \in R$;
  - symmetric, i.e., $(a, b) \in R \implies (b, a) \in R$;

Equivalence Relations

Let A and B be nonempty sets and consider the set $A \times B = \{(a, b) \mid a \in A,\ b \in B\}$.

- A relation R on $A \times B$ is a subset of $A \times B$, i.e., $R \subseteq A \times B$.
- A relation R on $A \times A$ is an equivalence relation on A if R is
  - reflexive, i.e., $\forall a \in A, (a, a) \in R$;
  - symmetric, i.e., $(a, b) \in R \implies (b, a) \in R$;
  - transitive,

Equivalence Relations

Let A and B be nonempty sets and consider the set $A \times B = \{(a, b) \mid a \in A,\ b \in B\}$.

- A relation R on $A \times B$ is a subset of $A \times B$, i.e., $R \subseteq A \times B$.
- A relation R on $A \times A$ is an equivalence relation on A if R is
  - reflexive, i.e., $\forall a \in A, (a, a) \in R$;
  - symmetric, i.e., $(a, b) \in R \implies (b, a) \in R$;
  - transitive, i.e., $(a, b) \in R$ and $(b, c) \in R \implies (a, c) \in R$.

Equivalence Relations

Let A and B be nonempty sets and consider the set $A \times B = \{(a, b) \mid a \in A,\ b \in B\}$.

- A relation R on $A \times B$ is a subset of $A \times B$, i.e., $R \subseteq A \times B$.
- A relation R on $A \times A$ is an equivalence relation on A if R is
  - reflexive, i.e., $\forall a \in A, (a, a) \in R$;
  - symmetric, i.e., $(a, b) \in R \implies (b, a) \in R$;
  - transitive, i.e., $(a, b) \in R$ and $(b, c) \in R \implies (a, c) \in R$.
- If R is an equivalence relation on A and if $(a, b) \in R$,

Equivalence Relations

Let A and B be nonempty sets and consider the set $A \times B = \{(a, b) \mid a \in A,\ b \in B\}$.

- A relation R on $A \times B$ is a subset of $A \times B$, i.e., $R \subseteq A \times B$.
- A relation R on $A \times A$ is an equivalence relation on A if R is
  - reflexive, i.e., $\forall a \in A, (a, a) \in R$;
  - symmetric, i.e., $(a, b) \in R \implies (b, a) \in R$;
  - transitive, i.e., $(a, b) \in R$ and $(b, c) \in R \implies (a, c) \in R$.
- If R is an equivalence relation on A and if $(a, b) \in R$, we say that a is equivalent to b under R

Equivalence Relations

Let A and B be nonempty sets and consider the set $A \times B = \{(a, b) \mid a \in A,\ b \in B\}$.

- A relation R on $A \times B$ is a subset of $A \times B$, i.e., $R \subseteq A \times B$.
- A relation R on $A \times A$ is an equivalence relation on A if R is
  - reflexive, i.e., $\forall a \in A, (a, a) \in R$;
  - symmetric, i.e., $(a, b) \in R \implies (b, a) \in R$;
  - transitive, i.e., $(a, b) \in R$ and $(b, c) \in R \implies (a, c) \in R$.
- If R is an equivalence relation on A and if $(a, b) \in R$, we say that a is equivalent to b under R and write aRb or $a \sim b$.

Equivalence Relations

Let A and B be nonempty sets and consider the set $A \times B = \{(a, b) \mid a \in A,\ b \in B\}$.

- A relation R on $A \times B$ is a subset of $A \times B$, i.e., $R \subseteq A \times B$.
- A relation R on $A \times A$ is an equivalence relation on A if R is
  - reflexive, i.e., $\forall a \in A, (a, a) \in R$;
  - symmetric, i.e., $(a, b) \in R \implies (b, a) \in R$;
  - transitive, i.e., $(a, b) \in R$ and $(b, c) \in R \implies (a, c) \in R$.
- If R is an equivalence relation on A and if $(a, b) \in R$, we say that a is equivalent to b under R and write aRb or $a \sim b$. With this notation, the above conditions become:

Equivalence Relations

Let A and B be nonempty sets and consider the set $A \times B = \{(a, b) \mid a \in A,\ b \in B\}$.

- A relation R on $A \times B$ is a subset of $A \times B$, i.e., $R \subseteq A \times B$.
- A relation R on $A \times A$ is an equivalence relation on A if R is
  - reflexive, i.e., $\forall a \in A,\ a \sim a$;
  - symmetric, i.e., $(a, b) \in R \implies (b, a) \in R$;
  - transitive, i.e., $(a, b) \in R$ and $(b, c) \in R \implies (a, c) \in R$.
- If R is an equivalence relation on A and if $(a, b) \in R$, we say that a is equivalent to b under R and write aRb or $a \sim b$. With this notation, the above conditions become:

Equivalence Relations

Let A and B be nonempty sets and consider the set $A \times B = \{(a, b) \mid a \in A,\ b \in B\}$.

- A relation R on $A \times B$ is a subset of $A \times B$, i.e., $R \subseteq A \times B$.
- A relation R on $A \times A$ is an equivalence relation on A if R is
  - reflexive, i.e., $\forall a \in A,\ a \sim a$;
  - symmetric, i.e., $a \sim b \implies b \sim a$;
  - transitive, i.e., $(a, b) \in R$ and $(b, c) \in R \implies (a, c) \in R$.
- If R is an equivalence relation on A and if $(a, b) \in R$, we say that a is equivalent to b under R and write aRb or $a \sim b$. With this notation, the above conditions become:

Equivalence Relations

Let A and B be nonempty sets and consider the set $A \times B = \{(a, b) \mid a \in A,\ b \in B\}$.

- A relation R on $A \times B$ is a subset of $A \times B$, i.e., $R \subseteq A \times B$.
- A relation R on $A \times A$ is an equivalence relation on A if R is
  - reflexive, i.e., $\forall a \in A,\ a \sim a$;
  - symmetric, i.e., $a \sim b \implies b \sim a$;
  - transitive, i.e., $a \sim b$ and $b \sim c \implies a \sim c$.
- If R is an equivalence relation on A and if $(a, b) \in R$, we say that a is equivalent to b under R and write aRb or $a \sim b$. With this notation, the above conditions become:

Equivalence Classes

Let $R(\sim)$ be an equivalence relation on A.

Equivalence Classes

Let $R(\sim)$ be an equivalence relation on A.

- If $a \in A$,

Equivalence Classes

Let $R(\sim)$ be an equivalence relation on A.

- If $a \in A$, the equivalence class of a is

Equivalence Classes

Let $R(\sim)$ be an equivalence relation on A.

- If $a \in A$, the equivalence class of a is $\overline{a} := \{b \in A \mid b \sim a\}$.

Equivalence Classes

Let $R(\sim)$ be an equivalence relation on A.

- If $a \in A$, the equivalence class of a is $\overline{a} := \{b \in A \mid b \sim a\}$.
- The quotient class of A by R

Equivalence Classes

Let $R(\sim)$ be an equivalence relation on A.

- If $a \in A$, the equivalence class of a is $\overline{a} := \{b \in A \mid b \sim a\}$.
- The quotient class of A by R is $A/R = \{\overline{a} \mid a \in A\}$.

Equivalence Classes

Let $R(\sim)$ be an equivalence relation on A.

- If $a \in A$, the equivalence class of a is $\overline{a} := \{b \in A \mid b \sim a\}$.
- The quotient class of A by R is $A/R = \{\overline{a} \mid a \in A\}$.
- Since $a \in \overline{a}$ for all $a \in A$,

Equivalence Classes

Let $R(\sim)$ be an equivalence relation on A.

- If $a \in A$, the equivalence class of a is $\overline{a} := \{b \in A \mid b \sim a\}$.
- The quotient class of A by R is $A/R = \{\overline{a} \mid a \in A\}$.
- Since $a \in \overline{a}$ for all $a \in A$, $A = \bigcup_{a \in A} \overline{a}$

Equivalence Classes

Let $R(\sim)$ be an equivalence relation on A.

- If $a \in A$, the equivalence class of a is $\overline{a} := \{b \in A \mid b \sim a\}$.
- The quotient class of A by R is $A/R = \{\overline{a} \mid a \in A\}$.
- Since $a \in \overline{a}$ for all $a \in A$, $A = \bigcup_{a \in A} \overline{a} = \bigcup_{\overline{a} \in A/R} \overline{a}$.

Equivalence Classes

Let $R(\sim)$ be an equivalence relation on A.

- If $a \in A$, the equivalence class of a is $\overline{a} := \{b \in A \mid b \sim a\}$.
- The quotient class of A by R is $A/R = \{\overline{a} \mid a \in A\}$.
- Since $a \in \overline{a}$ for all $a \in A$, $A = \bigcup_{a \in A} \overline{a} = \bigcup_{\overline{a} \in A/R} \overline{a}$.
- Observe that $a \sim b \iff \overline{a} = \overline{b}$.

Equivalence Classes

Let $R(\sim)$ be an equivalence relation on A.

- If $a \in A$, the equivalence class of a is $\overline{a} := \{b \in A \mid b \sim a\}$.
- The quotient class of A by R is $A/R = \{\overline{a} \mid a \in A\}$.
- Since $a \in \overline{a}$ for all $a \in A$, $A = \bigcup_{a \in A} \overline{a} = \bigcup_{\overline{a} \in A/R} \overline{a}$.
- Observe that $a \sim b \iff \overline{a} = \overline{b}$. Thus for any $a, b \in A$,

Equivalence Classes

Let $R(\sim)$ be an equivalence relation on A.

- If $a \in A$, the equivalence class of a is $\overline{a} := \{b \in A \mid b \sim a\}$.
- The quotient class of A by R is $A/R = \{\overline{a} \mid a \in A\}$.
- Since $a \in \overline{a}$ for all $a \in A$, $A = \bigcup_{a \in A} \overline{a} = \bigcup_{\overline{a} \in A/R} \overline{a}$.
- Observe that $a \sim b \iff \overline{a} = \overline{b}$. Thus for any $a, b \in A$, either $\overline{a} \cap \overline{b} = \varnothing$

Equivalence Classes

Let $R(\sim)$ be an equivalence relation on A.

- If $a \in A$, the equivalence class of a is $\overline{a} := \{b \in A \mid b \sim a\}$.
- The quotient class of A by R is $A/R = \{\overline{a} \mid a \in A\}$.
- Since $a \in \overline{a}$ for all $a \in A$, $A = \bigcup_{a \in A} \overline{a} = \bigcup_{\overline{a} \in A/R} \overline{a}$.
- Observe that $a \sim b \iff \overline{a} = \overline{b}$. Thus for any $a, b \in A$, either $\overline{a} \cap \overline{b} = \varnothing$ or $\overline{a} = \overline{b}$.

Partition

Let A be a nonempty set and let $\{A_i \mid i \in I\}$ be a family of subsets of A.

Partition

Let A be a nonempty set and let $\{A_i \mid i \in I\}$ be a family of subsets of A. $\{A_i \mid i \in I\}$ is called a partition of A if

Partition

Let A be a nonempty set and let $\{A_i \mid i \in I\}$ be a family of subsets of A. $\{A_i \mid i \in I\}$ is called a partition of A if

- $A_i \neq \varnothing \; \forall i \in I$,

Partition

Let A be a nonempty set and let $\{A_i \mid i \in I\}$ be a family of subsets of A. $\{A_i \mid i \in I\}$ is called a partition of A if

- $A_i \neq \varnothing \; \forall i \in I$,
- $\bigcup_{i \in I} A_i = A$,

Partition

Let A be a nonempty set and let $\{A_i \mid i \in I\}$ be a family of subsets of A. $\{A_i \mid i \in I\}$ is called a partition of A if

- $A_i \neq \varnothing \; \forall i \in I$,
- $\bigcup_{i \in I} A_i = A$,
- $A_i \cap A_j = \varnothing$, $\forall i, j \in I$ and $i \neq j$.

Partition

Let A be a nonempty set and let $\{A_i \mid i \in I\}$ be a family of subsets of A. $\{A_i \mid i \in I\}$ is called a partition of A if

- $A_i \neq \varnothing \; \forall i \in I$,
- $\bigcup_{i \in I} A_i = A$,
- $A_i \cap A_j = \varnothing$, $\forall i, j \in I$ and $i \neq j$.

Theorem (Introduction, 4.1)**.** If A is a nonempty set,

Partition

Let A be a nonempty set and let $\{A_i \mid i \in I\}$ be a family of subsets of A. $\{A_i \mid i \in I\}$ is called a partition of A if

- $A_i \neq \varnothing \; \forall i \in I$,
- $\bigcup_{i \in I} A_i = A$,
- $A_i \cap A_j = \varnothing$, $\forall i, j \in I$ and $i \neq j$.

Theorem (Introduction, 4.1)**.** If A is a nonempty set, then the assignment $R \mapsto A/R$ defines a bijection

Partition

Let A be a nonempty set and let $\{A_i \mid i \in I\}$ be a family of subsets of A. $\{A_i \mid i \in I\}$ is called a partition of A if

- $A_i \neq \varnothing \; \forall i \in I$,
- $\bigcup_{i \in I} A_i = A$,
- $A_i \cap A_j = \varnothing$, $\forall i, j \in I$ and $i \neq j$.

Theorem (Introduction, 4.1)**.** If A is a nonempty set, then the assignment $R \mapsto A/R$ defines a bijection from the set $E(A)$ of all equivalence relations on A

Partition

Let A be a nonempty set and let $\{A_i \mid i \in I\}$ be a family of subsets of A. $\{A_i \mid i \in I\}$ is called a partition of A if

- $A_i \neq \varnothing \; \forall i \in I$,
- $\bigcup_{i \in I} A_i = A$,
- $A_i \cap A_j = \varnothing$, $\forall i, j \in I$ and $i \neq j$.

Theorem (Introduction, 4.1)**.** If A is a nonempty set, then the assignment $R \mapsto A/R$ defines a bijection from the set $E(A)$ of all equivalence relations on A onto the set $Q(A)$ of all partitions of A.

Section I.4: Cosets and Counting

Section I.4: Cosets and Counting

Definition (4.1)**.** Let H be a subgroup of a group G

Section I.4: Cosets and Counting

Definition (4.1)**.** Let H be a subgroup of a group G and let $a, b \in G$.

Section I.4: Cosets and Counting

Definition (4.1)**.** Let H be a subgroup of a group G and let $a, b \in G$.

- If $ab^{-1} \in H$,

Section I.4: Cosets and Counting

Definition (4.1)**.** Let H be a subgroup of a group G and let $a, b \in G$.

- If $ab^{-1} \in H$, we say a is right congruent to b modulo H,

Section I.4: Cosets and Counting

Definition (4.1)**.** Let H be a subgroup of a group G and let $a, b \in G$.

- If $ab^{-1} \in H$, we say a is right congruent to b modulo H, and we denote $a \equiv_r b \pmod{H}$.

Section I.4: Cosets and Counting

Definition (4.1)**.** Let H be a subgroup of a group G and let $a, b \in G$.

- If $ab^{-1} \in H$, we say a is right congruent to b modulo H, and we denote $a \equiv_r b \pmod{H}$.

$\equiv_r$ is an equivalence relation on G:

Section I.4: Cosets and Counting

Definition (4.1)**.** Let H be a subgroup of a group G and let $a, b \in G$.

- If $ab^{-1} \in H$, we say a is right congruent to b modulo H, and we denote $a \equiv_r b \pmod{H}$.

$\equiv_r$ is an equivalence relation on G:

- Reflexive:

Section I.4: Cosets and Counting

Definition (4.1)**.** Let H be a subgroup of a group G and let $a, b \in G$.

- If $ab^{-1} \in H$, we say a is right congruent to b modulo H, and we denote $a \equiv_r b \pmod{H}$.

$\equiv_r$ is an equivalence relation on G:

- Reflexive: $\forall a \in G$,

Section I.4: Cosets and Counting

Definition (4.1)**.** Let H be a subgroup of a group G and let $a, b \in G$.

- If $ab^{-1} \in H$, we say a is right congruent to b modulo H, and we denote $a \equiv_r b \pmod{H}$.

$\equiv_r$ is an equivalence relation on G:

- Reflexive: $\forall a \in G$, $aa^{-1} = e$

Section I.4: Cosets and Counting

Definition (4.1)**.** Let H be a subgroup of a group G and let $a, b \in G$.

- If $ab^{-1} \in H$, we say a is right congruent to b modulo H, and we denote $a \equiv_r b \pmod{H}$.

$\equiv_r$ is an equivalence relation on G:

- Reflexive: $\forall a \in G$, $aa^{-1} = e \in H$,

Section I.4: Cosets and Counting

Definition (4.1)**.** Let H be a subgroup of a group G and let $a, b \in G$.

- If $ab^{-1} \in H$, we say a is right congruent to b modulo H, and we denote $a \equiv_r b \pmod{H}$.

$\equiv_r$ is an equivalence relation on G:

- Reflexive: $\forall a \in G$, $aa^{-1} = e \in H$, so $a \equiv_r a$;

Section I.4: Cosets and Counting

Definition (4.1)**.** Let H be a subgroup of a group G and let $a, b \in G$.

- If $ab^{-1} \in H$, we say a is right congruent to b modulo H, and we denote $a \equiv_r b \pmod{H}$.

$\equiv_r$ is an equivalence relation on G:

- Reflexive: $\forall a \in G$, $aa^{-1} = e \in H$, so $a \equiv_r a$;
- Symmetric:

Section I.4: Cosets and Counting

Definition (4.1)**.** Let H be a subgroup of a group G and let $a, b \in G$.

- If $ab^{-1} \in H$, we say a is right congruent to b modulo H, and we denote $a \equiv_r b \pmod{H}$.

$\equiv_r$ is an equivalence relation on G:

- Reflexive: $\forall a \in G$, $aa^{-1} = e \in H$, so $a \equiv_r a$;
- Symmetric: $a \equiv_r b$

Section I.4: Cosets and Counting

Definition (4.1)**.** Let H be a subgroup of a group G and let $a, b \in G$.

- If $ab^{-1} \in H$, we say a is right congruent to b modulo H, and we denote $a \equiv_r b \pmod{H}$.

$\equiv_r$ is an equivalence relation on G:

- Reflexive: $\forall a \in G$, $aa^{-1} = e \in H$, so $a \equiv_r a$;
- Symmetric: $a \equiv_r b \implies ab^{-1} \in H$

Section I.4: Cosets and Counting

Definition (4.1)**.** Let H be a subgroup of a group G and let $a, b \in G$.

- If $ab^{-1} \in H$, we say a is right congruent to b modulo H, and we denote $a \equiv_r b \pmod{H}$.

$\equiv_r$ is an equivalence relation on G:

- Reflexive: $\forall a \in G$, $aa^{-1} = e \in H$, so $a \equiv_r a$;
- Symmetric: $a \equiv_r b \implies ab^{-1} \in H \implies ba^{-1} = (ab^{-1})^{-1} \in H$

Section I.4: Cosets and Counting

Definition (4.1)**.** Let H be a subgroup of a group G and let $a, b \in G$.

- If $ab^{-1} \in H$, we say a is right congruent to b modulo H, and we denote $a \equiv_r b \pmod{H}$.

$\equiv_r$ is an equivalence relation on G:

- Reflexive: $\forall a \in G$, $aa^{-1} = e \in H$, so $a \equiv_r a$;
- Symmetric: $a \equiv_r b \implies ab^{-1} \in H \implies ba^{-1} = (ab^{-1})^{-1} \in H \implies b \equiv_r a$;

Section I.4: Cosets and Counting

Definition (4.1)**.** Let H be a subgroup of a group G and let $a, b \in G$.

- If $ab^{-1} \in H$, we say a is right congruent to b modulo H, and we denote $a \equiv_r b \pmod{H}$.

$\equiv_r$ is an equivalence relation on G:

- Reflexive: $\forall a \in G$, $aa^{-1} = e \in H$, so $a \equiv_r a$;
- Symmetric: $a \equiv_r b \implies ab^{-1} \in H \implies ba^{-1} = (ab^{-1})^{-1} \in H \implies b \equiv_r a$;
- Transitive:

Section I.4: Cosets and Counting

Definition (4.1)**.** Let H be a subgroup of a group G and let $a, b \in G$.

- If $ab^{-1} \in H$, we say a is right congruent to b modulo H, and we denote $a \equiv_r b \pmod{H}$.

$\equiv_r$ is an equivalence relation on G:

- Reflexive: $\forall a \in G$, $aa^{-1} = e \in H$, so $a \equiv_r a$;
- Symmetric: $a \equiv_r b \implies ab^{-1} \in H \implies ba^{-1} = (ab^{-1})^{-1} \in H \implies b \equiv_r a$;
- Transitive: $a \equiv_r b$ and $b \equiv_r c$

Section I.4: Cosets and Counting

Definition (4.1)**.** Let H be a subgroup of a group G and let $a, b \in G$.

- If $ab^{-1} \in H$, we say a is right congruent to b modulo H, and we denote $a \equiv_r b \pmod{H}$.

$\equiv_r$ is an equivalence relation on G:

- Reflexive: $\forall a \in G$, $aa^{-1} = e \in H$, so $a \equiv_r a$;
- Symmetric: $a \equiv_r b \implies ab^{-1} \in H \implies ba^{-1} = (ab^{-1})^{-1} \in H \implies b \equiv_r a$;
- Transitive: $a \equiv_r b$ and $b \equiv_r c \implies ab^{-1} \in H$ and $bc^{-1} \in H$

Section I.4: Cosets and Counting

Definition (4.1)**.** Let H be a subgroup of a group G and let $a, b \in G$.

- If $ab^{-1} \in H$, we say a is right congruent to b modulo H, and we denote $a \equiv_r b \pmod{H}$.

$\equiv_r$ is an equivalence relation on G:

- Reflexive: $\forall a \in G$, $aa^{-1} = e \in H$, so $a \equiv_r a$;
- Symmetric: $a \equiv_r b \implies ab^{-1} \in H \implies ba^{-1} = (ab^{-1})^{-1} \in H \implies b \equiv_r a$;
- Transitive: $a \equiv_r b$ and $b \equiv_r c \implies ab^{-1} \in H$ and $bc^{-1} \in H \implies ac^{-1}$

Section I.4: Cosets and Counting

Definition (4.1). Let H be a subgroup of a group G and let $a, b \in G$.

- If $ab^{-1} \in H$, we say a is right congruent to b modulo H, and we denote $a \equiv_r b \pmod{H}$.

$\equiv_r$ is an equivalence relation on G:

- Reflexive: $\forall a \in G$, $aa^{-1} = e \in H$, so $a \equiv_r a$;
- Symmetric: $a \equiv_r b \implies ab^{-1} \in H \implies ba^{-1} = (ab^{-1})^{-1} \in H \implies b \equiv_r a$;
- Transitive: $a \equiv_r b$ and $b \equiv_r c \implies ab^{-1} \in H$ and $bc^{-1} \in H \implies ac^{-1} = (ab^{-1})(bc^{-1})$

Section I.4: Cosets and Counting

Definition (4.1)**.** Let H be a subgroup of a group G and let $a, b \in G$.

- If $ab^{-1} \in H$, we say a is right congruent to b modulo H, and we denote $a \equiv_r b \pmod{H}$.

$\equiv_r$ is an equivalence relation on G:

- Reflexive: $\forall a \in G$, $aa^{-1} = e \in H$, so $a \equiv_r a$;
- Symmetric: $a \equiv_r b \implies ab^{-1} \in H \implies ba^{-1} = (ab^{-1})^{-1} \in H \implies b \equiv_r a$;
- Transitive: $a \equiv_r b$ and $b \equiv_r c \implies ab^{-1} \in H$ and $bc^{-1} \in H \implies ac^{-1} = (ab^{-1})(bc^{-1}) \in H$

Section I.4: Cosets and Counting

Definition (4.1)**.** Let H be a subgroup of a group G and let $a, b \in G$.

- If $ab^{-1} \in H$, we say a is right congruent to b modulo H, and we denote $a \equiv_r b \pmod{H}$.

$\equiv_r$ is an equivalence relation on G:

- Reflexive: $\forall a \in G$, $aa^{-1} = e \in H$, so $a \equiv_r a$;
- Symmetric: $a \equiv_r b \implies ab^{-1} \in H \implies ba^{-1} = (ab^{-1})^{-1} \in H \implies b \equiv_r a$;
- Transitive: $a \equiv_r b$ and $b \equiv_r c \implies ab^{-1} \in H$ and $bc^{-1} \in H \implies ac^{-1} = (ab^{-1})(bc^{-1}) \in H \implies a \equiv_r c$.

Section I.4: Cosets and Counting

Definition (4.1). Let H be a subgroup of a group G and let $a, b \in G$.

- If $ab^{-1} \in H$, we say a is right congruent to b modulo H, and we denote $a \equiv_r b \pmod{H}$.
- If $a^{-1}b \in H$,

$\equiv_r$ is an equivalence relation on G:

- Reflexive: $\forall a \in G$, $aa^{-1} = e \in H$, so $a \equiv_r a$;
- Symmetric: $a \equiv_r b \implies ab^{-1} \in H \implies ba^{-1} = (ab^{-1})^{-1} \in H \implies b \equiv_r a$;
- Transitive: $a \equiv_r b$ and $b \equiv_r c \implies ab^{-1} \in H$ and $bc^{-1} \in H \implies ac^{-1} = (ab^{-1})(bc^{-1}) \in H \implies a \equiv_r c$.

Section I.4: Cosets and Counting

Definition (4.1). Let H be a subgroup of a group G and let $a, b \in G$.

- If $ab^{-1} \in H$, we say a is right congruent to b modulo H, and we denote $a \equiv_r b \pmod{H}$.
- If $a^{-1}b \in H$, we say a is left congruent to b modulo H,

$\equiv_r$ is an equivalence relation on G:

- Reflexive: $\forall a \in G$, $aa^{-1} = e \in H$, so $a \equiv_r a$;
- Symmetric: $a \equiv_r b \implies ab^{-1} \in H \implies ba^{-1} = (ab^{-1})^{-1} \in H \implies b \equiv_r a$;
- Transitive: $a \equiv_r b$ and $b \equiv_r c \implies ab^{-1} \in H$ and $bc^{-1} \in H \implies ac^{-1} = (ab^{-1})(bc^{-1}) \in H \implies a \equiv_r c$.

Section I.4: Cosets and Counting

Definition (4.1). Let H be a subgroup of a group G and let $a, b \in G$.

- If $ab^{-1} \in H$, we say a is right congruent to b modulo H, and we denote $a \equiv_r b \pmod{H}$.
- If $a^{-1}b \in H$, we say a is left congruent to b modulo H, and we denote $a \equiv_l b \pmod{H}$.

$\equiv_r$ is an equivalence relation on G:

- Reflexive: $\forall a \in G$, $aa^{-1} = e \in H$, so $a \equiv_r a$;
- Symmetric: $a \equiv_r b \implies ab^{-1} \in H \implies ba^{-1} = (ab^{-1})^{-1} \in H \implies b \equiv_r a$;
- Transitive: $a \equiv_r b$ and $b \equiv_r c \implies ab^{-1} \in H$ and $bc^{-1} \in H \implies ac^{-1} = (ab^{-1})(bc^{-1}) \in H \implies a \equiv_r c$.

Theorem (4.2)

Let H be a subgroup of a group G.

Theorem (4.2)

Let H be a subgroup of a group G.

- Right (resp. left) congruence modulo H is an equivalence relation on G.

Theorem (4.2)

Let H be a subgroup of a group G.

- Right (resp. left) congruence modulo H is an equivalence relation on G.
- The equivalence class of $a \in G$ under right (resp. left) congruence modulo H is

Theorem (4.2)

Let H be a subgroup of a group G.

- Right (resp. left) congruence modulo H is an equivalence relation on G.
- The equivalence class of $a \in G$ under right (resp. left) congruence modulo H is $Ha = \{ha \mid h \in H\}$

Theorem (4.2)

Let H be a subgroup of a group G.

- Right (resp. left) congruence modulo H is an equivalence relation on G.
- The equivalence class of $a \in G$ under right (resp. left) congruence modulo H is $Ha = \{ha \mid h \in H\}$

$x \equiv_r a$

Theorem (4.2)

Let H be a subgroup of a group G.

- Right (resp. left) congruence modulo H is an equivalence relation on G.
- The equivalence class of $a \in G$ under right (resp. left) congruence modulo H is $Ha = \{ha \mid h \in H\}$

$x \equiv_r a \iff xa^{-1} \in H$

Theorem (4.2)

Let H be a subgroup of a group G.

- Right (resp. left) congruence modulo H is an equivalence relation on G.
- The equivalence class of $a \in G$ under right (resp. left) congruence modulo H is $Ha = \{ha \mid h \in H\}$

$x \equiv_r a \iff xa^{-1} \in H \iff xa^{-1} = h$ for some $h \in H$

Theorem (4.2)

Let H be a subgroup of a group G.

- Right (resp. left) congruence modulo H is an equivalence relation on G.
- The equivalence class of $a \in G$ under right (resp. left) congruence modulo H is $Ha = \{ha \mid h \in H\}$

$$x \equiv_r a \iff xa^{-1} \in H \iff xa^{-1} = h \text{ for some } h \in H$$
$$\iff x = ha \text{ for some } h \in H$$

Theorem (4.2)

Let H be a subgroup of a group G.

- Right (resp. left) congruence modulo H is an equivalence relation on G.
- The equivalence class of $a \in G$ under right (resp. left) congruence modulo H is $Ha = \{ha \mid h \in H\}$

$$x \equiv_r a \iff xa^{-1} \in H \iff xa^{-1} = h \text{ for some } h \in H$$
$$\iff x = ha \text{ for some } h \in H \iff x \in Ha.$$

Theorem (4.2)

Let H be a subgroup of a group G.

- Right (resp. left) congruence modulo H is an equivalence relation on G.
- The equivalence class of $a \in G$ under right (resp. left) congruence modulo H is $Ha = \{ha \mid h \in H\}$ (resp. $aH = \{ah \mid h \in H\}$).

$$x \equiv_r a \iff xa^{-1} \in H \iff xa^{-1} = h \text{ for some } h \in H$$
$$\iff x = ha \text{ for some } h \in H \iff x \in Ha.$$

Theorem (4.2)

Let H be a subgroup of a group G.

- Right (resp. left) congruence modulo H is an equivalence relation on G.
- The equivalence class of $a \in G$ under right (resp. left) congruence modulo H is $Ha = \{ha \mid h \in H\}$ (resp. $aH = \{ah \mid h \in H\}$).

$$x \equiv_r a \iff xa^{-1} \in H \iff xa^{-1} = h \text{ for some } h \in H$$
$$\iff x = ha \text{ for some } h \in H \iff x \in Ha.$$

$$x \equiv_l a$$

Theorem (4.2)

Let H be a subgroup of a group G.

- Right (resp. left) congruence modulo H is an equivalence relation on G.
- The equivalence class of $a \in G$ under right (resp. left) congruence modulo H is $Ha = \{ha \mid h \in H\}$ (resp. $aH = \{ah \mid h \in H\}$).

$$x \equiv_r a \iff xa^{-1} \in H \iff xa^{-1} = h \text{ for some } h \in H$$
$$\iff x = ha \text{ for some } h \in H \iff x \in Ha.$$
$$x \equiv_l a \iff a^{-1}x \in H$$

Theorem (4.2)

Let H be a subgroup of a group G.

- Right (resp. left) congruence modulo H is an equivalence relation on G.
- The equivalence class of $a \in G$ under right (resp. left) congruence modulo H is $Ha = \{ha \mid h \in H\}$ (resp. $aH = \{ah \mid h \in H\}$).

$$x \equiv_r a \iff xa^{-1} \in H \iff xa^{-1} = h \text{ for some } h \in H$$
$$\iff x = ha \text{ for some } h \in H \iff x \in Ha.$$
$$x \equiv_l a \iff a^{-1}x \in H \iff a^{-1}x = h \text{ for some } h \in H$$

Theorem (4.2)

Let H be a subgroup of a group G.

- Right (resp. left) congruence modulo H is an equivalence relation on G.
- The equivalence class of $a \in G$ under right (resp. left) congruence modulo H is $Ha = \{ha \mid h \in H\}$ (resp. $aH = \{ah \mid h \in H\}$).

$$
\begin{aligned}
x \equiv_r a &\iff xa^{-1} \in H \iff xa^{-1} = h \text{ for some } h \in H \\
&\iff x = ha \text{ for some } h \in H \iff x \in Ha. \\
x \equiv_l a &\iff a^{-1}x \in H \iff a^{-1}x = h \text{ for some } h \in H \\
&\iff x = ah \text{ for some } h \in H
\end{aligned}
$$

Theorem (4.2)

Let H be a subgroup of a group G.

- Right (resp. left) congruence modulo H is an equivalence relation on G.
- The equivalence class of $a \in G$ under right (resp. left) congruence modulo H is $Ha = \{ha \mid h \in H\}$ (resp. $aH = \{ah \mid h \in H\}$).

$$x \equiv_r a \iff xa^{-1} \in H \iff xa^{-1} = h \text{ for some } h \in H$$
$$\iff x = ha \text{ for some } h \in H \iff x \in Ha.$$
$$x \equiv_l a \iff a^{-1}x \in H \iff a^{-1}x = h \text{ for some } h \in H$$
$$\iff x = ah \text{ for some } h \in H \iff x \in aH.$$

Theorem (4.2)

Let H be a subgroup of a group G.

- Right (resp. left) congruence modulo H is an equivalence relation on G.
- The equivalence class of $a \in G$ under right (resp. left) congruence modulo H is $Ha = \{ha \mid h \in H\}$ (resp. $aH = \{ah \mid h \in H\}$).
- $|Ha| = |H| = |aH|, \forall a \in G$.

Theorem (4.2)

Let H be a subgroup of a group G.

- Right (resp. left) congruence modulo H is an equivalence relation on G.
- The equivalence class of $a \in G$ under right (resp. left) congruence modulo H is $Ha = \{ha \mid h \in H\}$ (resp. $aH = \{ah \mid h \in H\}$).
- $|Ha| = |H| = |aH|, \forall a \in G$.

Consider the map $f : H \to Ha$ defined by $h \mapsto ha$.

Theorem (4.2)

Let H be a subgroup of a group G.

- Right (resp. left) congruence modulo H is an equivalence relation on G.
- The equivalence class of $a \in G$ under right (resp. left) congruence modulo H is $Ha = \{ha \mid h \in H\}$ (resp. $aH = \{ah \mid h \in H\}$).
- $|Ha| = |H| = |aH|, \forall a \in G$.

Consider the map $f : H \to Ha$ defined by $h \mapsto ha$. It is clear that f is onto.

Theorem (4.2)

Let H be a subgroup of a group G.

- Right (resp. left) congruence modulo H is an equivalence relation on G.
- The equivalence class of $a \in G$ under right (resp. left) congruence modulo H is $Ha = \{ha \mid h \in H\}$ (resp. $aH = \{ah \mid h \in H\}$).
- $|Ha| = |H| = |aH|, \forall a \in G$.

Consider the map $f : H \longrightarrow Ha$ defined by $h \mapsto ha$. It is clear that f is onto. Moreover, since $h_1a = h_2a \implies h_1 = h_2$,

Theorem (4.2)

Let H be a subgroup of a group G.

- Right (resp. left) congruence modulo H is an equivalence relation on G.
- The equivalence class of $a \in G$ under right (resp. left) congruence modulo H is $Ha = \{ha \mid h \in H\}$ (resp. $aH = \{ah \mid h \in H\}$).
- $|Ha| = |H| = |aH|, \forall a \in G$.

Consider the map $f : H \longrightarrow Ha$ defined by $h \mapsto ha$. It is clear that f is onto. Moreover, since $h_1a = h_2a \implies h_1 = h_2$, f is one-to-one.

Theorem (4.2)

Let H be a subgroup of a group G.

- Right (resp. left) congruence modulo H is an equivalence relation on G.
- The equivalence class of $a \in G$ under right (resp. left) congruence modulo H is $Ha = \{ha \mid h \in H\}$ (resp. $aH = \{ah \mid h \in H\}$).
- $|Ha| = |H| = |aH|, \forall a \in G$.

Consider the map $f : H \to Ha$ defined by $h \mapsto ha$. It is clear that f is onto. Moreover, since $h_1 a = h_2 a \implies h_1 = h_2$, f is one-to-one. Therefore, $|H| = |Ha|$.

Theorem (4.2)

Let H be a subgroup of a group G.

- Right (resp. left) congruence modulo H is an equivalence relation on G.
- The equivalence class of $a \in G$ under right (resp. left) congruence modulo H is $Ha = \{ha \mid h \in H\}$ (resp. $aH = \{ah \mid h \in H\}$).
- $|Ha| = |H| = |aH|, \forall a \in G$.

Consider the map $f : H \longrightarrow Ha$ defined by $h \mapsto ha$. It is clear that f is onto. Moreover, since $h_1a = h_2a \implies h_1 = h_2$, f is one-to-one. Therefore, $|H| = |Ha|$. Similarly, consider the map $g : H \longrightarrow aH$ defined by $h \mapsto ah$,

Theorem (4.2)

Let H be a subgroup of a group G.

- Right (resp. left) congruence modulo H is an equivalence relation on G.
- The equivalence class of $a \in G$ under right (resp. left) congruence modulo H is $Ha = \{ha \mid h \in H\}$ (resp. $aH = \{ah \mid h \in H\}$).
- $|Ha| = |H| = |aH|, \forall a \in G$.

Consider the map $f : H \to Ha$ defined by $h \mapsto ha$. It is clear that f is onto. Moreover, since $h_1a = h_2a \implies h_1 = h_2$, f is one-to-one. Therefore, $|H| = |Ha|$. Similarly, consider the map $g : H \to aH$ defined by $h \mapsto ah$, then we can see that g is one-to-one and onto

Theorem (4.2)

Let H be a subgroup of a group G.

- Right (resp. left) congruence modulo H is an equivalence relation on G.
- The equivalence class of $a \in G$ under right (resp. left) congruence modulo H is $Ha = \{ha \mid h \in H\}$ (resp. $aH = \{ah \mid h \in H\}$).
- $|Ha| = |H| = |aH|, \forall a \in G$.

Consider the map $f : H \to Ha$ defined by $h \mapsto ha$. It is clear that f is onto. Moreover, since $h_1 a = h_2 a \implies h_1 = h_2$, f is one-to-one. Therefore, $|H| = |Ha|$. Similarly, consider the map $g : H \to aH$ defined by $h \mapsto ah$, then we can see that g is one-to-one and onto and so $|H| = |aH|$.

Theorem (4.2)

Let H be a subgroup of a group G.

- Right (resp. left) congruence modulo H is an equivalence relation on G.
- The equivalence class of $a \in G$ under right (resp. left) congruence modulo H is $Ha = \{ha \mid h \in H\}$ (resp. $aH = \{ah \mid h \in H\}$).
- $|Ha| = |H| = |aH|, \forall a \in G$.

Definition. Ha is called a right coset of H in G

Theorem (4.2)

Let H be a subgroup of a group G.

- Right (resp. left) congruence modulo H is an equivalence relation on G.
- The equivalence class of $a \in G$ under right (resp. left) congruence modulo H is $Ha = \{ha \mid h \in H\}$ (resp. $aH = \{ah \mid h \in H\}$).
- $|Ha| = |H| = |aH|, \forall a \in G$.

Definition. Ha is called a right coset of H in G and aH is called a left coset of H in G.

Theorem (4.2)

Let H be a subgroup of a group G.

- Right (resp. left) congruence modulo H is an equivalence relation on G.
- The equivalence class of $a \in G$ under right (resp. left) congruence modulo H is $Ha = \{ha \mid h \in H\}$ (resp. $aH = \{ah \mid h \in H\}$).
- $|Ha| = |H| = |aH|, \forall a \in G$.

Definition. Ha is called a right coset of H in G and aH is called a left coset of H in G.

Remark. In general, it is NOT the case that a right coset is also a left coset.

Corollary (4.3)

Let H be a subgroup of a group G.

Corollary (4.3)

Let H be a subgroup of a group G.

- G is the union of the right (resp. left) cosets of H in G.

Corollary (4.3)

Let H be a subgroup of a group G.

- G is the union of the right (resp. left) cosets of H in G.
- Two right (resp. left) cosets of H in G are either disjoint

Corollary (4.3)

Let H be a subgroup of a group G.

- G is the union of the right (resp. left) cosets of H in G.
- Two right (resp. left) cosets of H in G are either disjoint or equal,

Corollary (4.3)

Let H be a subgroup of a group G.

- G is the union of the right (resp. left) cosets of H in G.
- Two right (resp. left) cosets of H in G are either disjoint or equal, i.e., for all $a, b \in G$,

Corollary (4.3)

Let H be a subgroup of a group G.

- G is the union of the right (resp. left) cosets of H in G.
- Two right (resp. left) cosets of H in G are either disjoint or equal, i.e., for all $a, b \in G$, either $Ha \cap Hb = \varnothing$

Corollary (4.3)

Let H be a subgroup of a group G.

- G is the union of the right (resp. left) cosets of H in G.
- Two right (resp. left) cosets of H in G are either disjoint or equal, i.e., for all $a, b \in G$, either $Ha \cap Hb = \varnothing$ or $Ha = Hb$

Corollary (4.3)

Let H be a subgroup of a group G.

- G is the union of the right (resp. left) cosets of H in G.
- Two right (resp. left) cosets of H in G are either disjoint or equal, i.e., for all $a, b \in G$, either $Ha \cap Hb = \varnothing$ or $Ha = Hb$ (resp. either $aH \cap bH = \varnothing$

Corollary (4.3)

Let H be a subgroup of a group G.

- G is the union of the right (resp. left) cosets of H in G.
- Two right (resp. left) cosets of H in G are either disjoint or equal, i.e., for all $a, b \in G$, either $Ha \cap Hb = \varnothing$ or $Ha = Hb$ (resp. either $aH \cap bH = \varnothing$ or $aH = bH$).

Corollary (4.3)

Let H be a subgroup of a group G.

- G is the union of the right (resp. left) cosets of H in G.
- Two right (resp. left) cosets of H in G are either disjoint or equal, i.e., for all $a, b \in G$, either $Ha \cap Hb = \varnothing$ or $Ha = Hb$ (resp. either $aH \cap bH = \varnothing$ or $aH = bH$).
- For all $a, b \in G$,

Corollary (4.3)

Let H be a subgroup of a group G.

- G is the union of the right (resp. left) cosets of H in G.
- Two right (resp. left) cosets of H in G are either disjoint or equal, i.e., for all $a, b \in G$, either $Ha \cap Hb = \varnothing$ or $Ha = Hb$ (resp. either $aH \cap bH = \varnothing$ or $aH = bH$).
- For all $a, b \in G$, $Ha = Hb \iff ab^{-1} \in H$

Corollary (4.3)

Let H be a subgroup of a group G.

- G is the union of the right (resp. left) cosets of H in G.
- Two right (resp. left) cosets of H in G are either disjoint or equal, i.e., for all $a, b \in G$, either $Ha \cap Hb = \varnothing$ or $Ha = Hb$ (resp. either $aH \cap bH = \varnothing$ or $aH = bH$).
- For all $a, b \in G$, $Ha = Hb \iff ab^{-1} \in H$ and $aH = bH \iff a^{-1}b \in H$.

Corollary (4.3)

Let H be a subgroup of a group G.

- G is the union of the right (resp. left) cosets of H in G.
- Two right (resp. left) cosets of H in G are either disjoint or equal, i.e., for all $a, b \in G$, either $Ha \cap Hb = \varnothing$ or $Ha = Hb$ (resp. either $aH \cap bH = \varnothing$ or $aH = bH$).
- For all $a, b \in G$, $Ha = Hb \iff ab^{-1} \in H$ and $aH = bH \iff a^{-1}b \in H$.

These are all because the left cosets and the right cosets are indeed equivalence classes.

Corollary (4.3)

Let H be a subgroup of a group G.

- G is the union of the right (resp. left) cosets of H in G.
- Two right (resp. left) cosets of H in G are either disjoint or equal, i.e., for all $a, b \in G$, either $Ha \cap Hb = \varnothing$ or $Ha = Hb$ (resp. either $aH \cap bH = \varnothing$ or $aH = bH$).
- For all $a, b \in G$, $Ha = Hb \iff ab^{-1} \in H$ and $aH = bH \iff a^{-1}b \in H$.
- If $\mathcal{R}$ is the set of distinct right cosets of H in G

Corollary (4.3)

Let H be a subgroup of a group G.

- G is the union of the right (resp. left) cosets of H in G.
- Two right (resp. left) cosets of H in G are either disjoint or equal, i.e., for all $a, b \in G$, either $Ha \cap Hb = \varnothing$ or $Ha = Hb$ (resp. either $aH \cap bH = \varnothing$ or $aH = bH$).
- For all $a, b \in G$, $Ha = Hb \iff ab^{-1} \in H$ and $aH = bH \iff a^{-1}b \in H$.
- If $\mathcal{R}$ is the set of distinct right cosets of H in G and $\mathcal{L}$ is the set of distinct left cosets of H in G,

Corollary (4.3)

Let H be a subgroup of a group G.

- G is the union of the right (resp. left) cosets of H in G.
- Two right (resp. left) cosets of H in G are either disjoint or equal, i.e., for all $a, b \in G$, either $Ha \cap Hb = \varnothing$ or $Ha = Hb$ (resp. either $aH \cap bH = \varnothing$ or $aH = bH$).
- For all $a, b \in G$, $Ha = Hb \iff ab^{-1} \in H$ and $aH = bH \iff a^{-1}b \in H$.
- If $\mathcal{R}$ is the set of distinct right cosets of H in G and $\mathcal{L}$ is the set of distinct left cosets of H in G, then $|\mathcal{R}| = |\mathcal{L}|$.

Corollary (4.3)

Let H be a subgroup of a group G.

- G is the union of the right (resp. left) cosets of H in G.
- Two right (resp. left) cosets of H in G are either disjoint or equal, i.e., for all $a, b \in G$, either $Ha \cap Hb = \varnothing$ or $Ha = Hb$ (resp. either $aH \cap bH = \varnothing$ or $aH = bH$).
- For all $a, b \in G$, $Ha = Hb \iff ab^{-1} \in H$ and $aH = bH \iff a^{-1}b \in H$.
- If $\mathcal{R}$ is the set of distinct right cosets of H in G and $\mathcal{L}$ is the set of distinct left cosets of H in G, then $|\mathcal{R}| = |\mathcal{L}|$.

Note that

Corollary (4.3)

Let H be a subgroup of a group G.

- G is the union of the right (resp. left) cosets of H in G.
- Two right (resp. left) cosets of H in G are either disjoint or equal, i.e., for all $a, b \in G$, either $Ha \cap Hb = \varnothing$ or $Ha = Hb$ (resp. either $aH \cap bH = \varnothing$ or $aH = bH$).
- For all $a, b \in G$, $Ha = Hb \iff ab^{-1} \in H$ and $aH = bH \iff a^{-1}b \in H$.
- If $\mathcal{R}$ is the set of distinct right cosets of H in G and $\mathcal{L}$ is the set of distinct left cosets of H in G, then $|\mathcal{R}| = |\mathcal{L}|$.

Note that $Ha = Hb \iff ab^{-1} \in H$,

Corollary (4.3)

Let H be a subgroup of a group G.

- G is the union of the right (resp. left) cosets of H in G.
- Two right (resp. left) cosets of H in G are either disjoint or equal, i.e., for all $a, b \in G$, either $Ha \cap Hb = \varnothing$ or $Ha = Hb$ (resp. either $aH \cap bH = \varnothing$ or $aH = bH$).
- For all $a, b \in G$, $Ha = Hb \iff ab^{-1} \in H$ and $aH = bH \iff a^{-1}b \in H$.
- If $\mathcal{R}$ is the set of distinct right cosets of H in G and $\mathcal{L}$ is the set of distinct left cosets of H in G, then $|\mathcal{R}| = |\mathcal{L}|$.

Note that $Ha = Hb \iff ab^{-1} \in H$, i.e., $(a^{-1})^{-1}b^{-1} \in H$,

Corollary (4.3)

Let H be a subgroup of a group G.

- G is the union of the right (resp. left) cosets of H in G.
- Two right (resp. left) cosets of H in G are either disjoint or equal, i.e., for all $a, b \in G$, either $Ha \cap Hb = \varnothing$ or $Ha = Hb$ (resp. either $aH \cap bH = \varnothing$ or $aH = bH$).
- For all $a, b \in G$, $Ha = Hb \iff ab^{-1} \in H$ and $aH = bH \iff a^{-1}b \in H$.
- If $\mathcal{R}$ is the set of distinct right cosets of H in G and $\mathcal{L}$ is the set of distinct left cosets of H in G, then $|\mathcal{R}| = |\mathcal{L}|$.

Note that $Ha = Hb \iff ab^{-1} \in H$, i.e., $(a^{-1})^{-1}b^{-1} \in H$, $\iff a^{-1}H = b^{-1}H$.

Corollary (4.3)

Let H be a subgroup of a group G.

- G is the union of the right (resp. left) cosets of H in G.
- Two right (resp. left) cosets of H in G are either disjoint or equal, i.e., for all $a, b \in G$, either $Ha \cap Hb = \varnothing$ or $Ha = Hb$ (resp. either $aH \cap bH = \varnothing$ or $aH = bH$).
- For all $a, b \in G$, $Ha = Hb \iff ab^{-1} \in H$ and $aH = bH \iff a^{-1}b \in H$.
- If $\mathcal{R}$ is the set of distinct right cosets of H in G and $\mathcal{L}$ is the set of distinct left cosets of H in G, then $|\mathcal{R}| = |\mathcal{L}|$.

Note that $Ha = Hb \iff ab^{-1} \in H$, i.e., $(a^{-1})^{-1}b^{-1} \in H$, $\iff a^{-1}H = b^{-1}H$. Hence the map

Corollary (4.3)

Let H be a subgroup of a group G.

- G is the union of the right (resp. left) cosets of H in G.
- Two right (resp. left) cosets of H in G are either disjoint or equal, i.e., for all $a, b \in G$, either $Ha \cap Hb = \varnothing$ or $Ha = Hb$ (resp. either $aH \cap bH = \varnothing$ or $aH = bH$).
- For all $a, b \in G$, $Ha = Hb \iff ab^{-1} \in H$ and $aH = bH \iff a^{-1}b \in H$.
- If $\mathcal{R}$ is the set of distinct right cosets of H in G and $\mathcal{L}$ is the set of distinct left cosets of H in G, then $|\mathcal{R}| = |\mathcal{L}|$.

Note that $Ha = Hb \iff ab^{-1} \in H$, i.e., $(a^{-1})^{-1}b^{-1} \in H$, $\iff a^{-1}H = b^{-1}H$. Hence the map $\phi : \mathcal{R} \to \mathcal{L}$

Corollary (4.3)

Let H be a subgroup of a group G.

- G is the union of the right (resp. left) cosets of H in G.
- Two right (resp. left) cosets of H in G are either disjoint or equal, i.e., for all $a, b \in G$, either $Ha \cap Hb = \varnothing$ or $Ha = Hb$ (resp. either $aH \cap bH = \varnothing$ or $aH = bH$).
- For all $a, b \in G$, $Ha = Hb \iff ab^{-1} \in H$ and $aH = bH \iff a^{-1}b \in H$.
- If $\mathcal{R}$ is the set of distinct right cosets of H in G and $\mathcal{L}$ is the set of distinct left cosets of H in G, then $|\mathcal{R}| = |\mathcal{L}|$.

Note that $Ha = Hb \iff ab^{-1} \in H$, i.e., $(a^{-1})^{-1}b^{-1} \in H$, $\iff a^{-1}H = b^{-1}H$. Hence the map $\phi : \mathcal{R} \to \mathcal{L}$ defined by $Ha \mapsto a^{-1}H$

Corollary (4.3)

Let H be a subgroup of a group G.

- G is the union of the right (resp. left) cosets of H in G.
- Two right (resp. left) cosets of H in G are either disjoint or equal, i.e., for all $a, b \in G$, either $Ha \cap Hb = \varnothing$ or $Ha = Hb$ (resp. either $aH \cap bH = \varnothing$ or $aH = bH$).
- For all $a, b \in G$, $Ha = Hb \iff ab^{-1} \in H$ and $aH = bH \iff a^{-1}b \in H$.
- If $\mathcal{R}$ is the set of distinct right cosets of H in G and $\mathcal{L}$ is the set of distinct left cosets of H in G, then $|\mathcal{R}| = |\mathcal{L}|$.

Note that $Ha = Hb \iff ab^{-1} \in H$, i.e., $(a^{-1})^{-1}b^{-1} \in H$, $\iff a^{-1}H = b^{-1}H$. Hence the map $\phi : \mathcal{R} \to \mathcal{L}$ defined by $Ha \mapsto a^{-1}H$ is well-defined and one-to-one.

Corollary (4.3)

Let H be a subgroup of a group G.

- G is the union of the right (resp. left) cosets of H in G.
- Two right (resp. left) cosets of H in G are either disjoint or equal, i.e., for all $a, b \in G$, either $Ha \cap Hb = \varnothing$ or $Ha = Hb$ (resp. either $aH \cap bH = \varnothing$ or $aH = bH$).
- For all $a, b \in G$, $Ha = Hb \iff ab^{-1} \in H$ and $aH = bH \iff a^{-1}b \in H$.
- If $\mathcal{R}$ is the set of distinct right cosets of H in G and $\mathcal{L}$ is the set of distinct left cosets of H in G, then $|\mathcal{R}| = |\mathcal{L}|$.

Note that $Ha = Hb \iff ab^{-1} \in H$, i.e., $(a^{-1})^{-1}b^{-1} \in H$, $\iff a^{-1}H = b^{-1}H$. Hence the map $\phi : \mathcal{R} \to \mathcal{L}$ defined by $Ha \mapsto a^{-1}H$ is well-defined and one-to-one. Moreover, it is clear that ϕ is onto.

Corollary (4.3)

Let H be a subgroup of a group G.

- G is the union of the right (resp. left) cosets of H in G.
- Two right (resp. left) cosets of H in G are either disjoint or equal, i.e., for all $a, b \in G$, either $Ha \cap Hb = \varnothing$ or $Ha = Hb$ (resp. either $aH \cap bH = \varnothing$ or $aH = bH$).
- For all $a, b \in G$, $Ha = Hb \iff ab^{-1} \in H$ and $aH = bH \iff a^{-1}b \in H$.
- If $\mathcal{R}$ is the set of distinct right cosets of H in G and $\mathcal{L}$ is the set of distinct left cosets of H in G, then $|\mathcal{R}| = |\mathcal{L}|$.

Note that $Ha = Hb \iff ab^{-1} \in H$, i.e., $(a^{-1})^{-1}b^{-1} \in H$, $\iff a^{-1}H = b^{-1}H$. Hence the map $\phi : \mathcal{R} \to \mathcal{L}$ defined by $Ha \mapsto a^{-1}H$ is well-defined and one-to-one. Moreover, it is clear that ϕ is onto. Hence, ϕ is a bijection

Corollary (4.3)

Let H be a subgroup of a group G.

- G is the union of the right (resp. left) cosets of H in G.
- Two right (resp. left) cosets of H in G are either disjoint or equal, i.e., for all $a, b \in G$, either $Ha \cap Hb = \varnothing$ or $Ha = Hb$ (resp. either $aH \cap bH = \varnothing$ or $aH = bH$).
- For all $a, b \in G$, $Ha = Hb \iff ab^{-1} \in H$ and $aH = bH \iff a^{-1}b \in H$.
- If $\mathcal{R}$ is the set of distinct right cosets of H in G and $\mathcal{L}$ is the set of distinct left cosets of H in G, then $|\mathcal{R}| = |\mathcal{L}|$.

Note that $Ha = Hb \iff ab^{-1} \in H$, i.e., $(a^{-1})^{-1}b^{-1} \in H$, $\iff a^{-1}H = b^{-1}H$. Hence the map $\phi : \mathcal{R} \to \mathcal{L}$ defined by $Ha \mapsto a^{-1}H$ is well-defined and one-to-one. Moreover, it is clear that ϕ is onto. Hence, ϕ is a bijection and so $|\mathcal{R}| = |\mathcal{L}|$.

Corollary (4.3)

Let H be a subgroup of a group G.

- G is the union of the right (resp. left) cosets of H in G.
- Two right (resp. left) cosets of H in G are either disjoint or equal, i.e., for all $a, b \in G$, either $Ha \cap Hb = \varnothing$ or $Ha = Hb$ (resp. either $aH \cap bH = \varnothing$ or $aH = bH$).
- For all $a, b \in G$, $Ha = Hb \iff ab^{-1} \in H$ and $aH = bH \iff a^{-1}b \in H$.
- If $\mathcal{R}$ is the set of distinct right cosets of H in G and $\mathcal{L}$ is the set of distinct left cosets of H in G, then $|\mathcal{R}| = |\mathcal{L}|$.

Definition (4.4)**.** With the notations as above,

Corollary (4.3)

Let H be a subgroup of a group G.

- G is the union of the right (resp. left) cosets of H in G.
- Two right (resp. left) cosets of H in G are either disjoint or equal, i.e., for all $a, b \in G$, either $Ha \cap Hb = \varnothing$ or $Ha = Hb$ (resp. either $aH \cap bH = \varnothing$ or $aH = bH$).
- For all $a, b \in G$, $Ha = Hb \iff ab^{-1} \in H$ and $aH = bH \iff a^{-1}b \in H$.
- If $\mathcal{R}$ is the set of distinct right cosets of H in G and $\mathcal{L}$ is the set of distinct left cosets of H in G, then $|\mathcal{R}| = |\mathcal{L}|$.

Definition (4.4)**.** With the notations as above, The cardinal number $|\mathcal{R}| = |\mathcal{L}|$

Corollary (4.3)

Let H be a subgroup of a group G.

- G is the union of the right (resp. left) cosets of H in G.
- Two right (resp. left) cosets of H in G are either disjoint or equal, i.e., for all $a, b \in G$, either $Ha \cap Hb = \varnothing$ or $Ha = Hb$ (resp. either $aH \cap bH = \varnothing$ or $aH = bH$).
- For all $a, b \in G$, $Ha = Hb \iff ab^{-1} \in H$ and $aH = bH \iff a^{-1}b \in H$.
- If $\mathcal{R}$ is the set of distinct right cosets of H in G and $\mathcal{L}$ is the set of distinct left cosets of H in G, then $|\mathcal{R}| = |\mathcal{L}|$.

Definition (4.4)**.** With the notations as above, The cardinal number $|\mathcal{R}| = |\mathcal{L}|$ is called the index of H in G

Corollary (4.3)

Let H be a subgroup of a group G.

- G is the union of the right (resp. left) cosets of H in G.
- Two right (resp. left) cosets of H in G are either disjoint or equal, i.e., for all $a, b \in G$, either $Ha \cap Hb = \varnothing$ or $Ha = Hb$ (resp. either $aH \cap bH = \varnothing$ or $aH = bH$).
- For all $a, b \in G$, $Ha = Hb \iff ab^{-1} \in H$ and $aH = bH \iff a^{-1}b \in H$.
- If $\mathcal{R}$ is the set of distinct right cosets of H in G and $\mathcal{L}$ is the set of distinct left cosets of H in G, then $|\mathcal{R}| = |\mathcal{L}|$.

Definition (4.4)**.** With the notations as above, The cardinal number $|\mathcal{R}| = |\mathcal{L}|$ is called the index of H in G and denoted $[G : H]$.

Definition/Remark

Let H be a subgroup of a group G.

Definition/Remark

Let H be a subgroup of a group G.

- A complete set of right coset representatives of H in G

Definition/Remark

Let H be a subgroup of a group G.

- A complete set of right coset representatives of H in G is a set $\{a_i \mid i \in I\}$

Definition/Remark

Let H be a subgroup of a group G.

- A complete set of right coset representatives of H in G is a set $\{a_i \mid i \in I\}$ consisting precisely one element from each right coset of H in G.

Definition/Remark

Let H be a subgroup of a group G.

- A complete set of right coset representatives of H in G is a set $\{a_i \mid i \in I\}$ consisting precisely one element from each right coset of H in G.
  - The set $\{a_i \mid i \in I\}$ has cardinality $[G : H]$.

Definition/Remark

Let H be a subgroup of a group G.

- A complete set of right coset representatives of H in G is a set $\{a_i \mid i \in I\}$ consisting precisely one element from each right coset of H in G.
  - The set $\{a_i \mid i \in I\}$ has cardinality $[G : H]$.
  - Since $H = He$ is a right coset,

Definition/Remark

Let H be a subgroup of a group G.

- A complete set of right coset representatives of H in G is a set $\{a_i \mid i \in I\}$ consisting precisely one element from each right coset of H in G.
  - The set $\{a_i \mid i \in I\}$ has cardinality $[G : H]$.
  - Since $H = He$ is a right coset, $\{a_i \mid i \in I\}$ contains exactly one element of H.

Definition/Remark

Let H be a subgroup of a group G.

- A complete set of right coset representatives of H in G is a set $\{a_i \mid i \in I\}$ consisting precisely one element from each right coset of H in G.
  - The set $\{a_i \mid i \in I\}$ has cardinality $[G : H]$.
  - Since $H = He$ is a right coset, $\{a_i \mid i \in I\}$ contains exactly one element of H.
- Similarly,

Definition/Remark

Let H be a subgroup of a group G.

- A complete set of right coset representatives of H in G is a set $\{a_i \mid i \in I\}$ consisting precisely one element from each right coset of H in G.
  - The set $\{a_i \mid i \in I\}$ has cardinality $[G : H]$.
  - Since $H = He$ is a right coset, $\{a_i \mid i \in I\}$ contains exactly one element of H.
- Similarly, a complete set of left coset representatives of H in G

Definition/Remark

Let H be a subgroup of a group G.

- A complete set of right coset representatives of H in G is a set $\{a_i \mid i \in I\}$ consisting precisely one element from each right coset of H in G.
  - The set $\{a_i \mid i \in I\}$ has cardinality $[G : H]$.
  - Since $H = He$ is a right coset, $\{a_i \mid i \in I\}$ contains exactly one element of H.
- Similarly, a complete set of left coset representatives of H in G is a set $\{b_i \mid i \in I\}$

Definition/Remark

Let H be a subgroup of a group G.

- A complete set of right coset representatives of H in G is a set $\{a_i \mid i \in I\}$ consisting precisely one element from each right coset of H in G.
  - The set $\{a_i \mid i \in I\}$ has cardinality $[G : H]$.
  - Since $H = He$ is a right coset, $\{a_i \mid i \in I\}$ contains exactly one element of H.
- Similarly, a complete set of left coset representatives of H in G is a set $\{b_i \mid i \in I\}$ consisting precisely one element from each left coset of H in G.

Definition/Remark

Let H be a subgroup of a group G.

- A complete set of right coset representatives of H in G is a set $\{a_i \mid i \in I\}$ consisting precisely one element from each right coset of H in G.
  - The set $\{a_i \mid i \in I\}$ has cardinality $[G : H]$.
  - Since $H = He$ is a right coset, $\{a_i \mid i \in I\}$ contains exactly one element of H.
- Similarly, a complete set of left coset representatives of H in G is a set $\{b_i \mid i \in I\}$ consisting precisely one element from each left coset of H in G.
  - The set $\{b_i \mid i \in I\}$ has cardinality $[G : H]$.

Definition/Remark

Let H be a subgroup of a group G.

- A complete set of right coset representatives of H in G is a set $\{a_i \mid i \in I\}$ consisting precisely one element from each right coset of H in G.
  - The set $\{a_i \mid i \in I\}$ has cardinality $[G : H]$.
  - Since $H = He$ is a right coset, $\{a_i \mid i \in I\}$ contains exactly one element of H.
- Similarly, a complete set of left coset representatives of H in G is a set $\{b_i \mid i \in I\}$ consisting precisely one element from each left coset of H in G.
  - The set $\{b_i \mid i \in I\}$ has cardinality $[G : H]$.
  - Since $H = eH$ is a left coset,

Definition/Remark

Let H be a subgroup of a group G.

- A complete set of right coset representatives of H in G is a set $\{a_i \mid i \in I\}$ consisting precisely one element from each right coset of H in G.
  - The set $\{a_i \mid i \in I\}$ has cardinality $[G : H]$.
  - Since $H = He$ is a right coset, $\{a_i \mid i \in I\}$ contains exactly one element of H.
- Similarly, a complete set of left coset representatives of H in G is a set $\{b_i \mid i \in I\}$ consisting precisely one element from each left coset of H in G.
  - The set $\{b_i \mid i \in I\}$ has cardinality $[G : H]$.
  - Since $H = eH$ is a left coset, $\{b_i \mid i \in I\}$ contains exactly one element of H.

Theorem (4.5)

Let $K \leq H \leq G$ be groups.

Theorem (4.5)

Let $K \leq H \leq G$ be groups. Then $[G : K] = [G : H][H : K]$.

Theorem (4.5)

Let $K \leq H \leq G$ be groups. Then $[G : K] = [G : H][H : K]$.
Hence, $[G : K] < \infty \iff [G : H] < \infty$ and $[H : K] < \infty$.

Theorem (4.5)

Let $K \leq H \leq G$ be groups. Then $[G : K] = [G : H][H : K]$. Hence, $[G : K] < \infty \iff [G : H] < \infty$ and $[H : K] < \infty$.

Proof. Let $\{a_i \mid i \in I\}$ be a complete set of right coset representatives of H in G

Theorem (4.5)

Let $K \leq H \leq G$ be groups. Then $[G : K] = [G : H][H : K]$. Hence, $[G : K] < \infty \iff [G : H] < \infty$ and $[H : K] < \infty$.

Proof. Let $\{a_i \mid i \in I\}$ be a complete set of right coset representatives of H in G and let $\{b_j \mid j \in J\}$ be a complete set of right coset representatives of K in H.

Theorem (4.5)

Let $K \leq H \leq G$ be groups. Then $[G : K] = [G : H][H : K]$.
Hence, $[G : K] < \infty \iff [G : H] < \infty$ and $[H : K] < \infty$.

Proof. Let $\{a_i \mid i \in I\}$ be a complete set of right coset representatives of H in G and let $\{b_j \mid j \in J\}$ be a complete set of right coset representatives of K in H.
Claim: $\{b_j a_i \mid i \in I \text{ and } j \in J\}$ is a complete set of right coset representatives of K in G.

Theorem (4.5)

Let $K \leq H \leq G$ be groups. Then $[G : K] = [G : H][H : K]$.
Hence, $[G : K] < \infty \iff [G : H] < \infty$ and $[H : K] < \infty$.

Proof. Let $\{a_i \mid i \in I\}$ be a complete set of right coset representatives of H in G and let $\{b_j \mid j \in J\}$ be a complete set of right coset representatives of K in H.
Claim: $\{b_j a_i \mid i \in I \text{ and } j \in J\}$ is a complete set of right coset representatives of K in G. (Then we will have $[G : K] = |I||J| = [G : H][H : K]$.)

Theorem (4.5)

Let $K \leq H \leq G$ be groups. Then $[G : K] = [G : H][H : K]$.
Hence, $[G : K] < \infty \iff [G : H] < \infty$ and $[H : K] < \infty$.

Proof. Let $\{a_i \mid i \in I\}$ be a complete set of right coset representatives of H in G and let $\{b_j \mid j \in J\}$ be a complete set of right coset representatives of K in H.
Claim: $\{b_j a_i \mid i \in I \text{ and } j \in J\}$ is a complete set of right coset representatives of K in G.
Note that we have

Theorem (4.5)

Let $K \leq H \leq G$ be groups. Then $[G : K] = [G : H][H : K]$.
Hence, $[G : K] < \infty \iff [G : H] < \infty$ and $[H : K] < \infty$.

Proof. Let $\{a_i \mid i \in I\}$ be a complete set of right coset representatives of H in G and let $\{b_j \mid j \in J\}$ be a complete set of right coset representatives of K in H.

Claim: $\{b_j a_i \mid i \in I \text{ and } j \in J\}$ is a complete set of right coset representatives of K in G.

Note that we have $G = \bigcup_{i \in I} Ha_i$ and $Ha_i = Ha_\imath \implies a_i = a_\imath$

Theorem (4.5)

Let $K \leq H \leq G$ be groups. Then $[G : K] = [G : H][H : K]$.
Hence, $[G : K] < \infty \iff [G : H] < \infty$ and $[H : K] < \infty$.

Proof. Let $\{a_i \mid i \in I\}$ be a complete set of right coset representatives of H in G and let $\{b_j \mid j \in J\}$ be a complete set of right coset representatives of K in H.

Claim: $\{b_j a_i \mid i \in I \text{ and } j \in J\}$ is a complete set of right coset representatives of K in G.

Note that we have $G = \bigcup_{i \in I} Ha_i$ and $Ha_i = Ha_\imath \implies a_i = a_\imath$ and $H = \bigcup_{j \in J} Kb_j$ and $Kb_j = Kb_\jmath \implies b_j = b_\jmath$.

Theorem (4.5)

Let $K \leq H \leq G$ be groups. Then $[G : K] = [G : H][H : K]$.
Hence, $[G : K] < \infty \iff [G : H] < \infty$ and $[H : K] < \infty$.

Proof. Let $\{a_i \mid i \in I\}$ be a complete set of right coset representatives of H in G and let $\{b_j \mid j \in J\}$ be a complete set of right coset representatives of K in H.
Claim: $\{b_j a_i \mid i \in I \text{ and } j \in J\}$ is a complete set of right coset representatives of K in G.
Note that we have $G = \bigcup_{i \in I} Ha_i$ and $Ha_i = Ha_\imath \implies a_i = a_\imath$
and $H = \bigcup_{j \in J} Kb_j$ and $Kb_j = Kb_\jmath \implies b_j = b_\jmath$.
We will show (1) $G = \bigcup_{i \in I} \bigcup_{j \in J} Kb_j a_i$

Theorem (4.5)

Let $K \leq H \leq G$ be groups. Then $[G : K] = [G : H][H : K]$.
Hence, $[G : K] < \infty \iff [G : H] < \infty$ and $[H : K] < \infty$.

Proof. Let $\{a_i \mid i \in I\}$ be a complete set of right coset representatives of H in G and let $\{b_j \mid j \in J\}$ be a complete set of right coset representatives of K in H.
Claim: $\{b_j a_i \mid i \in I \text{ and } j \in J\}$ is a complete set of right coset representatives of K in G.
Note that we have $G = \bigcup_{i \in I} Ha_i$ and $Ha_i = Ha_\imath \implies a_i = a_\imath$ and $H = \bigcup_{j \in J} Kb_j$ and $Kb_j = Kb_\jmath \implies b_j = b_\jmath$.
We will show (1) $G = \bigcup_{i \in I} \bigcup_{j \in J} Kb_j a_i$ and
(2) $Kb_j a_i = Kb_\jmath a_\imath \implies (b_j, a_i) = (b_\jmath, a_\imath)$.

Theorem (4.5)

Let $K \leq H \leq G$ be groups. Then $[G : K] = [G : H][H : K]$.
Hence, $[G : K] < \infty \iff [G : H] < \infty$ and $[H : K] < \infty$.

Proof. Let $\{a_i \mid i \in I\}$ be a complete set of right coset representatives of H in G and let $\{b_j \mid j \in J\}$ be a complete set of right coset representatives of K in H.

Claim: $\{b_j a_i \mid i \in I \text{ and } j \in J\}$ is a complete set of right coset representatives of K in G.

Note that we have $G = \bigcup_{i \in I} Ha_i$ and $Ha_i = Ha_\imath \implies a_i = a_\imath$ and $H = \bigcup_{j \in J} Kb_j$ and $Kb_j = Kb_\jmath \implies b_j = b_\jmath$.

We will show (1) $G = \bigcup_{i \in I} \bigcup_{j \in J} Kb_j a_i$ and

(2) $Kb_j a_i = Kb_\jmath a_\imath \implies (b_j, a_i) = (b_\jmath, a_\imath)$.

$G = \bigcup_{i \in I} Ha_i$

Theorem (4.5)

Let $K \leq H \leq G$ be groups. Then $[G : K] = [G : H][H : K]$.
Hence, $[G : K] < \infty \iff [G : H] < \infty$ and $[H : K] < \infty$.

Proof. Let $\{a_i \mid i \in I\}$ be a complete set of right coset representatives of H in G and let $\{b_j \mid j \in J\}$ be a complete set of right coset representatives of K in H.

Claim: $\{b_j a_i \mid i \in I \text{ and } j \in J\}$ is a complete set of right coset representatives of K in G.

Note that we have $G = \bigcup_{i \in I} Ha_i$ and $Ha_i = Ha_\imath \implies a_i = a_\imath$ and $H = \bigcup_{j \in J} Kb_j$ and $Kb_j = Kb_\jmath \implies b_j = b_\jmath$.

We will show (1) $G = \bigcup_{i \in I} \bigcup_{j \in J} Kb_j a_i$ and

(2) $Kb_j a_i = Kb_\jmath a_\imath \implies (b_j, a_i) = (b_\jmath, a_\imath)$.

$G = \bigcup_{i \in I} Ha_i = \bigcup_{i \in I} \left(\bigcup_{j \in J} Kb_j \right) a_i$

Theorem (4.5)

Let $K \leq H \leq G$ be groups. Then $[G : K] = [G : H][H : K]$.
Hence, $[G : K] < \infty \iff [G : H] < \infty$ and $[H : K] < \infty$.

Proof. Let $\{a_i \mid i \in I\}$ be a complete set of right coset representatives of H in G and let $\{b_j \mid j \in J\}$ be a complete set of right coset representatives of K in H.

Claim: $\{b_j a_i \mid i \in I \text{ and } j \in J\}$ is a complete set of right coset representatives of K in G.

Note that we have $G = \bigcup_{i \in I} Ha_i$ and $Ha_i = Ha_\imath \implies a_i = a_\imath$ and $H = \bigcup_{j \in J} Kb_j$ and $Kb_j = Kb_\jmath \implies b_j = b_\jmath$.

We will show (1) $G = \bigcup_{i \in I} \bigcup_{j \in J} Kb_j a_i$ and

(2) $Kb_j a_i = Kb_\jmath a_\imath \implies (b_j, a_i) = (b_\jmath, a_\imath)$.

$G = \bigcup_{i \in I} Ha_i = \bigcup_{i \in I} \left(\bigcup_{j \in J} Kb_j \right) a_i = \bigcup_{i \in I} \bigcup_{j \in J} Kb_j a_i$,

Theorem (4.5)

Let $K \leq H \leq G$ be groups. Then $[G : K] = [G : H][H : K]$.
Hence, $[G : K] < \infty \iff [G : H] < \infty$ and $[H : K] < \infty$.

Proof. Let $\{a_i \mid i \in I\}$ be a complete set of right coset representatives of H in G and let $\{b_j \mid j \in J\}$ be a complete set of right coset representatives of K in H.
Claim: $\{b_j a_i \mid i \in I \text{ and } j \in J\}$ is a complete set of right coset representatives of K in G.
Note that we have $G = \bigcup_{i \in I} Ha_i$ and $Ha_i = Ha_\imath \implies a_i = a_\imath$ and $H = \bigcup_{j \in J} Kb_j$ and $Kb_j = Kb_\jmath \implies b_j = b_\jmath$.
We will show (1) $G = \bigcup_{i \in I} \bigcup_{j \in J} Kb_j a_i$ and

(2) $Kb_j a_i = Kb_\jmath a_\imath \implies (b_j, a_i) = (b_\jmath, a_\imath)$.

$G = \bigcup_{i \in I} Ha_i = \bigcup_{i \in I} \left(\bigcup_{j \in J} Kb_j \right) a_i = \bigcup_{i \in I} \bigcup_{j \in J} Kb_j a_i$, so (1) is proved.

Theorem (4.5)

Let $K \leq H \leq G$ be groups. Then $[G : K] = [G : H][H : K]$.
Hence, $[G : K] < \infty \iff [G : H] < \infty$ and $[H : K] < \infty$.

Proof. Let $\{a_i \mid i \in I\}$ be a complete set of right coset representatives of H in G and let $\{b_j \mid j \in J\}$ be a complete set of right coset representatives of K in H.

Claim: $\{b_j a_i \mid i \in I \text{ and } j \in J\}$ is a complete set of right coset representatives of K in G.

Note that we have $G = \bigcup_{i \in I} Ha_i$ and $Ha_i = Ha_\imath \implies a_i = a_\imath$ and $H = \bigcup_{j \in J} Kb_j$ and $Kb_j = Kb_\jmath \implies b_j = b_\jmath$.

We will show (1) $G = \bigcup_{i \in I} \bigcup_{j \in J} Kb_j a_i$ and

(2) $Kb_j a_i = Kb_\jmath a_\imath \implies (b_j, a_i) = (b_\jmath, a_\imath)$.

Note $Kb_j a_i = Kb_\jmath a_\imath$

Theorem (4.5)

Let $K \leq H \leq G$ be groups. Then $[G : K] = [G : H][H : K]$.
Hence, $[G : K] < \infty \iff [G : H] < \infty$ and $[H : K] < \infty$.

Proof. Let $\{a_i \mid i \in I\}$ be a complete set of right coset representatives of H in G and let $\{b_j \mid j \in J\}$ be a complete set of right coset representatives of K in H.

Claim: $\{b_j a_i \mid i \in I \text{ and } j \in J\}$ is a complete set of right coset representatives of K in G.

Note that we have $G = \bigcup_{i \in I} Ha_i$ and $Ha_i = Ha_\imath \implies a_i = a_\imath$ and $H = \bigcup_{j \in J} Kb_j$ and $Kb_j = Kb_\jmath \implies b_j = b_\jmath$.

We will show (1) $G = \bigcup_{i \in I} \bigcup_{j \in J} Kb_j a_i$ and

(2) $Kb_j a_i = Kb_\jmath a_\imath \implies (b_j, a_i) = (b_\jmath, a_\imath)$.

Note $Kb_j a_i = Kb_\jmath a_\imath \subseteq Ha_i \cap Ha_\imath$,

Theorem (4.5)

Let $K \leq H \leq G$ be groups. Then $[G : K] = [G : H][H : K]$.
Hence, $[G : K] < \infty \iff [G : H] < \infty$ and $[H : K] < \infty$.

Proof. Let $\{a_i \mid i \in I\}$ be a complete set of right coset representatives of H in G and let $\{b_j \mid j \in J\}$ be a complete set of right coset representatives of K in H.

Claim: $\{b_j a_i \mid i \in I \text{ and } j \in J\}$ is a complete set of right coset representatives of K in G.

Note that we have $G = \bigcup_{i \in I} Ha_i$ and $Ha_i = Ha_\imath \implies a_i = a_\imath$ and $H = \bigcup_{j \in J} Kb_j$ and $Kb_j = Kb_\jmath \implies b_j = b_\jmath$.

We will show (1) $G = \bigcup_{i \in I} \bigcup_{j \in J} Kb_j a_i$ and

(2) $Kb_j a_i = Kb_\jmath a_\imath \implies (b_j, a_i) = (b_\jmath, a_\imath)$.

Note $Kb_j a_i = Kb_\jmath a_\imath \subseteq Ha_i \cap Ha_\imath$, $Ha_i \cap Ha_\imath \neq \varnothing$

Theorem (4.5)

Let $K \leq H \leq G$ be groups. Then $[G : K] = [G : H][H : K]$.
Hence, $[G : K] < \infty \iff [G : H] < \infty$ and $[H : K] < \infty$.

Proof. Let $\{a_i \mid i \in I\}$ be a complete set of right coset representatives of H in G and let $\{b_j \mid j \in J\}$ be a complete set of right coset representatives of K in H.
Claim: $\{b_j a_i \mid i \in I \text{ and } j \in J\}$ is a complete set of right coset representatives of K in G.
Note that we have $G = \bigcup_{i \in I} Ha_i$ and $Ha_i = Ha_\imath \implies a_i = a_\imath$ and $H = \bigcup_{j \in J} Kb_j$ and $Kb_j = Kb_\jmath \implies b_j = b_\jmath$.
We will show (1) $G = \bigcup_{i \in I} \bigcup_{j \in J} Kb_j a_i$ and

(2) $Kb_j a_i = Kb_\jmath a_\imath \implies (b_j, a_i) = (b_\jmath, a_\imath)$.

Note $Kb_j a_i = Kb_\jmath a_\imath \subseteq Ha_i \cap Ha_\imath$, $Ha_i \cap Ha_\imath \neq \varnothing$ and this implies $a_i = a_\imath$.

Theorem (4.5)

Let $K \leq H \leq G$ be groups. Then $[G : K] = [G : H][H : K]$.
Hence, $[G : K] < \infty \iff [G : H] < \infty$ and $[H : K] < \infty$.

Proof. Let $\{a_i \mid i \in I\}$ be a complete set of right coset representatives of H in G and let $\{b_j \mid j \in J\}$ be a complete set of right coset representatives of K in H.

Claim: $\{b_j a_i \mid i \in I \text{ and } j \in J\}$ is a complete set of right coset representatives of K in G.

Note that we have $G = \bigcup_{i \in I} Ha_i$ and $Ha_i = Ha_\imath \implies a_i = a_\imath$ and $H = \bigcup_{j \in J} Kb_j$ and $Kb_j = Kb_\jmath \implies b_j = b_\jmath$.

We will show (1) $G = \bigcup_{i \in I} \bigcup_{j \in J} Kb_j a_i$ and

(2) $Kb_j a_i = Kb_\jmath a_\imath \implies (b_j, a_i) = (b_\jmath, a_\imath)$.

Note $Kb_j a_i = Kb_\jmath a_\imath \subseteq Ha_i \cap Ha_\imath$, $Ha_i \cap Ha_\imath \neq \varnothing$ and this implies $a_i = a_\imath$. Thus $Kb_j a_i = Kb_\jmath a_\imath \implies Kb_j = Kb_\jmath$

Theorem (4.5)

Let $K \leq H \leq G$ be groups. Then $[G : K] = [G : H][H : K]$.
Hence, $[G : K] < \infty \iff [G : H] < \infty$ and $[H : K] < \infty$.

Proof. Let $\{a_i \mid i \in I\}$ be a complete set of right coset representatives of H in G and let $\{b_j \mid j \in J\}$ be a complete set of right coset representatives of K in H.

Claim: $\{b_j a_i \mid i \in I \text{ and } j \in J\}$ is a complete set of right coset representatives of K in G.

Note that we have $G = \bigcup_{i \in I} Ha_i$ and $Ha_i = Ha_\imath \implies a_i = a_\imath$ and $H = \bigcup_{j \in J} Kb_j$ and $Kb_j = Kb_\jmath \implies b_j = b_\jmath$.

We will show (1) $G = \bigcup_{i \in I} \bigcup_{j \in J} Kb_j a_i$ and

(2) $Kb_j a_i = Kb_\jmath a_\imath \implies (b_j, a_i) = (b_\jmath, a_\imath)$.

Note $Kb_j a_i = Kb_\jmath a_\imath \subseteq Ha_i \cap Ha_\imath$, $Ha_i \cap Ha_\imath \neq \varnothing$ and this implies $a_i = a_\imath$. Thus $Kb_j a_i = Kb_\jmath a_\imath \implies Kb_j = Kb_\jmath$ and this implies $b_j = b_\jmath$.

Theorem (4.5)

Let $K \leq H \leq G$ be groups. Then $[G : K] = [G : H][H : K]$.
Hence, $[G : K] < \infty \iff [G : H] < \infty$ and $[H : K] < \infty$.

Proof. Let $\{a_i \mid i \in I\}$ be a complete set of right coset representatives of H in G and let $\{b_j \mid j \in J\}$ be a complete set of right coset representatives of K in H.
Claim: $\{b_j a_i \mid i \in I \text{ and } j \in J\}$ is a complete set of right coset representatives of K in G.
Note that we have $G = \bigcup_{i \in I} Ha_i$ and $Ha_i = Ha_\imath \implies a_i = a_\imath$ and $H = \bigcup_{j \in J} Kb_j$ and $Kb_j = Kb_\jmath \implies b_j = b_\jmath$.
We will show (1) $G = \bigcup_{i \in I} \bigcup_{j \in J} Kb_j a_i$ and

(2) $Kb_j a_i = Kb_\jmath a_\imath \implies (b_j, a_i) = (b_\jmath, a_\imath)$.

Note $Kb_j a_i = Kb_\jmath a_\imath \subseteq Ha_i \cap Ha_\imath$, $Ha_i \cap Ha_\imath \neq \varnothing$ and this implies $a_i = a_\imath$. Thus $Kb_j a_i = Kb_\jmath a_\imath \implies Kb_j = Kb_\jmath$ and this implies $b_j = b_\jmath$. Hence (2) is proved.

Theorem (4.5)

Let $K \leq H \leq G$ be groups. Then $[G : K] = [G : H][H : K]$.
Hence, $[G : K] < \infty \iff [G : H] < \infty$ and $[H : K] < \infty$.

Corollary (4.6 Lagrange)**.** If H is a subgroup of a group G,

Theorem (4.5)

Let $K \leq H \leq G$ be groups. Then $[G : K] = [G : H][H : K]$. Hence, $[G : K] < \infty \iff [G : H] < \infty$ and $[H : K] < \infty$.

Corollary (4.6 Lagrange)**.** If H is a subgroup of a group G, then $|G| = [G : H] \cdot |H|$.

Theorem (4.5)

Let $K \leq H \leq G$ be groups. Then $[G : K] = [G : H][H : K]$. Hence, $[G : K] < \infty \iff [G : H] < \infty$ and $[H : K] < \infty$.

Corollary (4.6 Lagrange)**.** If H is a subgroup of a group G, then $|G| = [G : H] \cdot |H|$. In particular, if G is finite,

Theorem (4.5)

Let $K \leq H \leq G$ be groups. Then $[G : K] = [G : H][H : K]$. Hence, $[G : K] < \infty \iff [G : H] < \infty$ and $[H : K] < \infty$.

Corollary (4.6 Lagrange)**.** If H is a subgroup of a group G, then $|G| = [G : H] \cdot |H|$. In particular, if G is finite, then $|H|$ divides $|G|$

Theorem (4.5)

Let $K \leq H \leq G$ be groups. Then $[G : K] = [G : H][H : K]$. Hence, $[G : K] < \infty \iff [G : H] < \infty$ and $[H : K] < \infty$.

Corollary (4.6 Lagrange)**.** If H is a subgroup of a group G, then $|G| = [G : H] \cdot |H|$. In particular, if G is finite, then $|H|$ divides $|G|$ and for every $a \in G$, the order of a divides $|G|$.

Theorem (4.5)

Let $K \leq H \leq G$ be groups. Then $[G : K] = [G : H][H : K]$. Hence, $[G : K] < \infty \iff [G : H] < \infty$ and $[H : K] < \infty$.

Corollary (4.6 Lagrange)**.** If H is a subgroup of a group G, then $|G| = [G : H] \cdot |H|$. In particular, if G is finite, then $|H|$ divides $|G|$ and for every $a \in G$, the order of a divides $|G|$.

Proof. Let $K = \{e\}$ be the trivial subgroup of G.

Theorem (4.5)

Let $K \leq H \leq G$ be groups. Then $[G : K] = [G : H][H : K]$. Hence, $[G : K] < \infty \iff [G : H] < \infty$ and $[H : K] < \infty$.

Corollary (4.6 Lagrange)**.** If H is a subgroup of a group G, then $|G| = [G : H] \cdot |H|$. In particular, if G is finite, then $|H|$ divides $|G|$ and for every $a \in G$, the order of a divides $|G|$.

Proof. Let $K = \{e\}$ be the trivial subgroup of G. Then $[G : K] = |G|$

Theorem (4.5)

Let $K \leq H \leq G$ be groups. Then $[G : K] = [G : H][H : K]$. Hence, $[G : K] < \infty \iff [G : H] < \infty$ and $[H : K] < \infty$.

Corollary (4.6 Lagrange)**.** If H is a subgroup of a group G, then $|G| = [G : H] \cdot |H|$. In particular, if G is finite, then $|H|$ divides $|G|$ and for every $a \in G$, the order of a divides $|G|$.

Proof. Let $K = \{e\}$ be the trivial subgroup of G. Then $[G : K] = |G|$ and $[H : K] = |H|$.

Theorem (4.5)

Let $K \leq H \leq G$ be groups. Then $[G : K] = [G : H][H : K]$. Hence, $[G : K] < \infty \iff [G : H] < \infty$ and $[H : K] < \infty$.

Corollary (4.6 Lagrange)**.** If H is a subgroup of a group G, then $|G| = [G : H] \cdot |H|$. In particular, if G is finite, then $|H|$ divides $|G|$ and for every $a \in G$, the order of a divides $|G|$.

Proof. Let $K = \{e\}$ be the trivial subgroup of G. Then $[G : K] = |G|$ and $[H : K] = |H|$. Theorem (4.5) tells us $|G| = [G : H] \cdot |H|$.

Theorem (4.5)

Let $K \leq H \leq G$ be groups. Then $[G : K] = [G : H][H : K]$. Hence, $[G : K] < \infty \iff [G : H] < \infty$ and $[H : K] < \infty$.

Corollary (4.6 Lagrange)**.** If H is a subgroup of a group G, then $|G| = [G : H] \cdot |H|$. In particular, if G is finite, then $|H|$ divides $|G|$ and for every $a \in G$, the order of a divides $|G|$.

Proof. Let $K = \{e\}$ be the trivial subgroup of G. Then $[G : K] = |G|$ and $[H : K] = |H|$. Theorem (4.5) tells us $|G| = [G : H] \cdot |H|$. In particular, if $|G| < \infty$,

Theorem (4.5)

Let $K \leq H \leq G$ be groups. Then $[G : K] = [G : H][H : K]$. Hence, $[G : K] < \infty \iff [G : H] < \infty$ and $[H : K] < \infty$.

Corollary (4.6 Lagrange)**.** If H is a subgroup of a group G, then $|G| = [G : H] \cdot |H|$. In particular, if G is finite, then $|H|$ divides $|G|$ and for every $a \in G$, the order of a divides $|G|$.

Proof. Let $K = \{e\}$ be the trivial subgroup of G. Then $[G : K] = |G|$ and $[H : K] = |H|$. Theorem (4.5) tells us $|G| = [G : H] \cdot |H|$. In particular, if $|G| < \infty$, then $|H| \Big| |G|$

Theorem (4.5)

Let $K \leq H \leq G$ be groups. Then $[G : K] = [G : H][H : K]$. Hence, $[G : K] < \infty \iff [G : H] < \infty$ and $[H : K] < \infty$.

Corollary (4.6 Lagrange)**.** If H is a subgroup of a group G, then $|G| = [G : H] \cdot |H|$. In particular, if G is finite, then $|H|$ divides $|G|$ and for every $a \in G$, the order of a divides $|G|$.

Proof. Let $K = \{e\}$ be the trivial subgroup of G. Then $[G : K] = |G|$ and $[H : K] = |H|$. Theorem (4.5) tells us $|G| = [G : H] \cdot |H|$. In particular, if $|G| < \infty$, then $|H| \Big| |G|$ and for every $a \in G$,

Theorem (4.5)

Let $K \leq H \leq G$ be groups. Then $[G : K] = [G : H][H : K]$. Hence, $[G : K] < \infty \iff [G : H] < \infty$ and $[H : K] < \infty$.

Corollary (4.6 Lagrange)**.** If H is a subgroup of a group G, then $|G| = [G : H] \cdot |H|$. In particular, if G is finite, then $|H|$ divides $|G|$ and for every $a \in G$, the order of a divides $|G|$.

Proof. Let $K = \{e\}$ be the trivial subgroup of G. Then $[G : K] = |G|$ and $[H : K] = |H|$. Theorem (4.5) tells us $|G| = [G : H] \cdot |H|$. In particular, if $|G| < \infty$, then $|H| \Big| |G|$ and for every $a \in G$, $|a| = |\langle a \rangle|$

Theorem (4.5)

Let $K \leq H \leq G$ be groups. Then $[G : K] = [G : H][H : K]$. Hence, $[G : K] < \infty \iff [G : H] < \infty$ and $[H : K] < \infty$.

Corollary (4.6 Lagrange)**.** If H is a subgroup of a group G, then $|G| = [G : H] \cdot |H|$. In particular, if G is finite, then $|H|$ divides $|G|$ and for every $a \in G$, the order of a divides $|G|$.

Proof. Let $K = \{e\}$ be the trivial subgroup of G. Then $[G : K] = |G|$ and $[H : K] = |H|$. Theorem (4.5) tells us $|G| = [G : H] \cdot |H|$. In particular, if $|G| < \infty$, then $|H| \Big| |G|$ and for every $a \in G$, $|a| = |\langle a \rangle| \Big| |G|$.

The product of two subgroups

Notation. Let G be a group and let H and K be subgroups of G.

The product of two subgroups

Notation. Let G be a group and let H and K be subgroups of G.

$$HK := \{hk \mid h \in H,\ k \in K\}$$

The product of two subgroups

Notation. Let G be a group and let H and K be subgroups of G.

$$HK := \{hk \mid h \in H,\ k \in K\}$$

Note that even if H and K are subgroups,

The product of two subgroups

Notation. Let G be a group and let H and K be subgroups of G.

$$HK := \{hk \mid h \in H,\ k \in K\}$$

Note that even if H and K are subgroups, HK may NOT be a subgroup of G.

The product of two subgroups

Notation. Let G be a group and let H and K be subgroups of G.

$$HK := \{hk \mid h \in H,\ k \in K\}$$

Note that even if H and K are subgroups, HK may NOT be a subgroup of G.

Theorem (4.7)**.** Let H and K be finite subgroups of a group G.

The product of two subgroups

Notation. Let G be a group and let H and K be subgroups of G.

$$HK := \{hk \mid h \in H,\ k \in K\}$$

Note that even if H and K are subgroups, HK may NOT be a subgroup of G.

Theorem (4.7)**.** Let H and K be finite subgroups of a group G. Then

The product of two subgroups

Notation. Let G be a group and let H and K be subgroups of G.

$$HK := \{hk \mid h \in H,\ k \in K\}$$

Note that even if H and K are subgroups, HK may NOT be a subgroup of G.

Theorem (4.7)**.** Let H and K be finite subgroups of a group G. Then

$$|HK| =$$

The product of two subgroups

Notation. Let G be a group and let H and K be subgroups of G.

$$HK := \{hk \mid h \in H,\ k \in K\}$$

Note that even if H and K are subgroups, HK may NOT be a subgroup of G.

Theorem (4.7)**.** Let H and K be finite subgroups of a group G. Then

$$|HK| = \frac{|H||K|}{}$$

The product of two subgroups

Notation. Let G be a group and let H and K be subgroups of G.

$$HK := \{hk \mid h \in H,\ k \in K\}$$

Note that even if H and K are subgroups, HK may NOT be a subgroup of G.

Theorem (4.7)**.** Let H and K be finite subgroups of a group G. Then

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Theorem (4.7)

Let H and K be finite subgroups of a group G. Then

$$|HK| = \frac{|H||K|}{|H \cap K|} \ .$$

Theorem (4.7)

Let H and K be finite subgroups of a group G. Then

$$|HK| = \frac{|H||K|}{|H \cap K|} \ .$$

Proof. Let $C = H \cap K$

Theorem (4.7)

Let H and K be finite subgroups of a group G. Then

$$|HK| = \frac{|H||K|}{|H \cap K|} \ .$$

Proof. Let $C = H \cap K$ (then $C \leq K$)

Theorem (4.7)

Let H and K be finite subgroups of a group G. Then

$$|HK| = \frac{|H||K|}{|H \cap K|} \ .$$

Proof. Let $C = H \cap K$ (then $C \leq K$) and let $\{a_1, \ldots, a_n\}$ be a complete set of right coset representatives of C in K.

Theorem (4.7)

Let H and K be finite subgroups of a group G. Then

$$|HK| = \frac{|H||K|}{|H \cap K|} \ .$$

Proof. Let $C = H \cap K$ (then $C \leq K$) and let $\{a_1, \ldots, a_n\}$ be a complete set of right coset representatives of C in K. Then $K = Ca_1 \cup \cdots \cup Ca_n$

Theorem (4.7)

Let H and K be finite subgroups of a group G. Then

$$|HK| = \frac{|H||K|}{|H \cap K|} \ .$$

Proof. Let $C = H \cap K$ (then $C \leq K$) and let $\{a_1, \ldots, a_n\}$ be a complete set of right coset representatives of C in K. Then $K = Ca_1 \cup \cdots \cup Ca_n$ is a disjoint union

Theorem (4.7)

Let H and K be finite subgroups of a group G. Then

$$|HK| = \frac{|H||K|}{|H \cap K|} \ .$$

Proof. Let $C = H \cap K$ (then $C \leq K$) and let $\{a_1, \ldots, a_n\}$ be a complete set of right coset representatives of C in K. Then $K = Ca_1 \cup \cdots \cup Ca_n$ is a disjoint union and

Theorem (4.7)

Let H and K be finite subgroups of a group G. Then

$$|HK| = \frac{|H||K|}{|H \cap K|} .$$

Proof. Let $C = H \cap K$ (then $C \leq K$) and let $\{a_1, \ldots, a_n\}$ be a complete set of right coset representatives of C in K. Then $K = Ca_1 \cup \cdots \cup Ca_n$ is a disjoint union and

$$n = [K : C]$$

Theorem (4.7)

Let H and K be finite subgroups of a group G. Then

$$|HK| = \frac{|H||K|}{|H \cap K|} \ .$$

Proof. Let $C = H \cap K$ (then $C \leq K$) and let $\{a_1, \ldots, a_n\}$ be a complete set of right coset representatives of C in K. Then $K = Ca_1 \cup \cdots \cup Ca_n$ is a disjoint union and

$$n = [K : C] = \frac{|K|}{|C|}$$

Theorem (4.7)

Let H and K be finite subgroups of a group G. Then

$$|HK| = \frac{|H||K|}{|H \cap K|} \ .$$

Proof. Let $C = H \cap K$ (then $C \leq K$) and let $\{a_1, \ldots, a_n\}$ be a complete set of right coset representatives of C in K. Then $K = Ca_1 \cup \cdots \cup Ca_n$ is a disjoint union and

$$n = [K : C] = \frac{|K|}{|C|} = \frac{|K|}{|H \cap K|} \ .$$

Theorem (4.7)

Let H and K be finite subgroups of a group G. Then

$$|HK| = \frac{|H||K|}{|H \cap K|} .$$

Proof. Let $C = H \cap K$ (then $C \leq K$) and let $\{a_1, \ldots, a_n\}$ be a complete set of right coset representatives of C in K. Then $K = Ca_1 \cup \cdots \cup Ca_n$ is a disjoint union and

$$n = [K : C] = \frac{|K|}{|C|} = \frac{|K|}{|H \cap K|} .$$

Note that $HC = H$.

Theorem (4.7)

Let H and K be finite subgroups of a group G. Then

$$|HK| = \frac{|H||K|}{|H \cap K|} .$$

Proof. Let $C = H \cap K$ (then $C \leq K$) and let $\{a_1, \ldots, a_n\}$ be a complete set of right coset representatives of C in K. Then $K = Ca_1 \cup \cdots \cup Ca_n$ is a disjoint union and

$$n = [K : C] = \frac{|K|}{|C|} = \frac{|K|}{|H \cap K|} .$$

Note that $HC = H$. "$\supseteq$" is because $\forall h \in H$, $h = he \in HC$.

Theorem (4.7)

Let H and K be finite subgroups of a group G. Then

$$|HK| = \frac{|H||K|}{|H \cap K|} .$$

Proof. Let $C = H \cap K$ (then $C \leq K$) and let $\{a_1, \ldots, a_n\}$ be a complete set of right coset representatives of C in K. Then $K = Ca_1 \cup \cdots \cup Ca_n$ is a disjoint union and

$$n = [K : C] = \frac{|K|}{|C|} = \frac{|K|}{|H \cap K|} .$$

Note that $HC = H$. "$\supseteq$" is because $\forall h \in H$, $h = he \in HC$.
"$\subseteq$" is because $\forall h \in H$ and $\forall c \in C$,

Theorem (4.7)

Let H and K be finite subgroups of a group G. Then

$$|HK| = \frac{|H||K|}{|H \cap K|} .$$

Proof. Let $C = H \cap K$ (then $C \leq K$) and let $\{a_1, \ldots, a_n\}$ be a complete set of right coset representatives of C in K. Then $K = Ca_1 \cup \cdots \cup Ca_n$ is a disjoint union and

$$n = [K : C] = \frac{|K|}{|C|} = \frac{|K|}{|H \cap K|} .$$

Note that $HC = H$. "$\supseteq$" is because $\forall h \in H$, $h = he \in HC$.

"$\subseteq$" is because $\forall h \in H$ and $\forall c \in C$, since $C \subseteq H$, $c \in H$

Theorem (4.7)

Let H and K be finite subgroups of a group G. Then

$$|HK| = \frac{|H||K|}{|H \cap K|} .$$

Proof. Let $C = H \cap K$ (then $C \leq K$) and let $\{a_1, \ldots, a_n\}$ be a complete set of right coset representatives of C in K. Then $K = Ca_1 \cup \cdots \cup Ca_n$ is a disjoint union and

$$n = [K : C] = \frac{|K|}{|C|} = \frac{|K|}{|H \cap K|} .$$

Note that $HC = H$. "$\supseteq$" is because $\forall h \in H$, $h = he \in HC$. "$\subseteq$" is because $\forall h \in H$ and $\forall c \in C$, since $C \subseteq H$, $c \in H$ and so $hc \in H$.

Theorem (4.7)

Let H and K be finite subgroups of a group G. Then

$$|HK| = \frac{|H||K|}{|H \cap K|} .$$

Proof. Let $C = H \cap K$ (then $C \leq K$) and let $\{a_1, \ldots, a_n\}$ be a complete set of right coset representatives of C in K. Then $K = Ca_1 \cup \cdots \cup Ca_n$ is a disjoint union and

$$n = [K : C] = \frac{|K|}{|C|} = \frac{|K|}{|H \cap K|} .$$

Note that $HC = H$. Thus

Theorem (4.7)

Let H and K be finite subgroups of a group G. Then

$$|HK| = \frac{|H||K|}{|H \cap K|} .$$

Proof. Let $C = H \cap K$ (then $C \leq K$) and let $\{a_1, \ldots, a_n\}$ be a complete set of right coset representatives of C in K. Then $K = Ca_1 \cup \cdots \cup Ca_n$ is a disjoint union and

$$n = [K : C] = \frac{|K|}{|C|} = \frac{|K|}{|H \cap K|} .$$

Note that $HC = H$. Thus

$$HK = H(Ca_1 \cup \cdots \cup Ca_n)$$

Theorem (4.7)

Let H and K be finite subgroups of a group G. Then

$$|HK| = \frac{|H||K|}{|H \cap K|} .$$

Proof. Let $C = H \cap K$ (then $C \leq K$) and let $\{a_1, \ldots, a_n\}$ be a complete set of right coset representatives of C in K. Then $K = Ca_1 \cup \cdots \cup Ca_n$ is a disjoint union and

$$n = [K : C] = \frac{|K|}{|C|} = \frac{|K|}{|H \cap K|} .$$

Note that $HC = H$. Thus

$$HK = H(Ca_1 \cup \cdots \cup Ca_n) = HCa_1 \cup \cdots \cup HCa_n$$

Theorem (4.7)

Let H and K be finite subgroups of a group G. Then

$$|HK| = \frac{|H||K|}{|H \cap K|} .$$

Proof. Let $C = H \cap K$ (then $C \leq K$) and let $\{a_1, \ldots, a_n\}$ be a complete set of right coset representatives of C in K. Then $K = Ca_1 \cup \cdots \cup Ca_n$ is a disjoint union and

$$n = [K : C] = \frac{|K|}{|C|} = \frac{|K|}{|H \cap K|} .$$

Note that $HC = H$. Thus

$$\begin{aligned} HK &= H(Ca_1 \cup \cdots \cup Ca_n) = HCa_1 \cup \cdots \cup HCa_n \\ &= Ha_1 \cup \cdots \cup Ha_n. \end{aligned}$$

Theorem (4.7)

Let H and K be finite subgroups of a group G. Then

$$|HK| = \frac{|H||K|}{|H \cap K|} .$$

Proof. Let $C = H \cap K$ (then $C \leq K$) and let $\{a_1, \ldots, a_n\}$ be a complete set of right coset representatives of C in K. Then $K = Ca_1 \cup \cdots \cup Ca_n$ is a disjoint union and

$$n = [K : C] = \frac{|K|}{|C|} = \frac{|K|}{|H \cap K|} .$$

Note that $HC = H$. Thus

$$\begin{aligned} HK &= H(Ca_1 \cup \cdots \cup Ca_n) = HCa_1 \cup \cdots \cup HCa_n \\ &= Ha_1 \cup \cdots \cup Ha_n. \end{aligned}$$

Note that the last union is disjoint.

Theorem (4.7)

Let H and K be finite subgroups of a group G. Then

$$|HK| = \frac{|H||K|}{|H \cap K|} .$$

Proof. Let $C = H \cap K$ (then $C \leq K$) and let $\{a_1, \ldots, a_n\}$ be a complete set of right coset representatives of C in K. Then $K = Ca_1 \cup \cdots \cup Ca_n$ is a disjoint union and

$$n = [K : C] = \frac{|K|}{|C|} = \frac{|K|}{|H \cap K|} .$$

Note that $HC = H$. Thus

$$\begin{aligned} HK &= H(Ca_1 \cup \cdots \cup Ca_n) = HCa_1 \cup \cdots \cup HCa_n \\ &= Ha_1 \cup \cdots \cup Ha_n. \end{aligned}$$

Note that the last union is disjoint. If not,

Theorem (4.7)

Let H and K be finite subgroups of a group G. Then

$$|HK| = \frac{|H||K|}{|H \cap K|} .$$

Proof. Let $C = H \cap K$ (then $C \leq K$) and let $\{a_1, \ldots, a_n\}$ be a complete set of right coset representatives of C in K. Then $K = Ca_1 \cup \cdots \cup Ca_n$ is a disjoint union and

$$n = [K : C] = \frac{|K|}{|C|} = \frac{|K|}{|H \cap K|} .$$

Note that $HC = H$. Thus

$$\begin{aligned} HK &= H(Ca_1 \cup \cdots \cup Ca_n) = HCa_1 \cup \cdots \cup HCa_n \\ &= Ha_1 \cup \cdots \cup Ha_n. \end{aligned}$$

Note that the last union is disjoint. If not, then $H_{a_i} = H_{a_j}$ for some $i \neq j$,

Theorem (4.7)

Let H and K be finite subgroups of a group G. Then

$$|HK| = \frac{|H||K|}{|H \cap K|} .$$

Proof. Let $C = H \cap K$ (then $C \leq K$) and let $\{a_1, \ldots, a_n\}$ be a complete set of right coset representatives of C in K. Then $K = Ca_1 \cup \cdots \cup Ca_n$ is a disjoint union and

$$n = [K : C] = \frac{|K|}{|C|} = \frac{|K|}{|H \cap K|} .$$

Note that $HC = H$. Thus

$$\begin{aligned} HK &= H(Ca_1 \cup \cdots \cup Ca_n) = HCa_1 \cup \cdots \cup HCa_n \\ &= Ha_1 \cup \cdots \cup Ha_n. \end{aligned}$$

Note that the last union is disjoint. If not, then $H_{a_i} = H_{a_j}$ for some $i \neq j$, i.e., $a_i a_j^{-1} \in H$;

Theorem (4.7)

Let H and K be finite subgroups of a group G. Then

$$|HK| = \frac{|H||K|}{|H \cap K|} .$$

Proof. Let $C = H \cap K$ (then $C \leq K$) and let $\{a_1, \ldots, a_n\}$ be a complete set of right coset representatives of C in K. Then $K = Ca_1 \cup \cdots \cup Ca_n$ is a disjoint union and

$$n = [K : C] = \frac{|K|}{|C|} = \frac{|K|}{|H \cap K|} .$$

Note that $HC = H$. Thus

$$\begin{aligned} HK &= H(Ca_1 \cup \cdots \cup Ca_n) = HCa_1 \cup \cdots \cup HCa_n \\ &= Ha_1 \cup \cdots \cup Ha_n. \end{aligned}$$

Note that the last union is disjoint. If not, then $Ha_i = Ha_j$ for some $i \neq j$, i.e., $a_i a_j^{-1} \in H$; however, since $a_i, a_j \in K$,

Theorem (4.7)

Let H and K be finite subgroups of a group G. Then

$$|HK| = \frac{|H||K|}{|H \cap K|} .$$

Proof. Let $C = H \cap K$ (then $C \leq K$) and let $\{a_1, \ldots, a_n\}$ be a complete set of right coset representatives of C in K. Then $K = Ca_1 \cup \cdots \cup Ca_n$ is a disjoint union and

$$n = [K : C] = \frac{|K|}{|C|} = \frac{|K|}{|H \cap K|} .$$

Note that $HC = H$. Thus

$$\begin{aligned} HK &= H(Ca_1 \cup \cdots \cup Ca_n) = HCa_1 \cup \cdots \cup HCa_n \\ &= Ha_1 \cup \cdots \cup Ha_n. \end{aligned}$$

Note that the last union is disjoint. If not, then $H_{a_i} = H_{a_j}$ for some $i \neq j$, i.e., $a_i a_j^{-1} \in H$; however, since $a_i, a_j \in K$, $a_i a_j^{-1} \in H$

Theorem (4.7)

Let H and K be finite subgroups of a group G. Then

$$|HK| = \frac{|H||K|}{|H \cap K|} .$$

Proof. Let $C = H \cap K$ (then $C \leq K$) and let $\{a_1, \ldots, a_n\}$ be a complete set of right coset representatives of C in K. Then $K = Ca_1 \cup \cdots \cup Ca_n$ is a disjoint union and

$$n = [K : C] = \frac{|K|}{|C|} = \frac{|K|}{|H \cap K|} .$$

Note that $HC = H$. Thus

$$\begin{aligned} HK &= H(Ca_1 \cup \cdots \cup Ca_n) = HCa_1 \cup \cdots \cup HCa_n \\ &= Ha_1 \cup \cdots \cup Ha_n. \end{aligned}$$

Note that the last union is disjoint. If not, then $Ha_i = Ha_j$ for some $i \neq j$, i.e., $a_i a_j^{-1} \in H$; however, since $a_i, a_j \in K$, $a_i a_j^{-1} \in H \cap K = C$

Theorem (4.7)

Let H and K be finite subgroups of a group G. Then

$$|HK| = \frac{|H||K|}{|H \cap K|} .$$

Proof. Let $C = H \cap K$ (then $C \leq K$) and let $\{a_1, \ldots, a_n\}$ be a complete set of right coset representatives of C in K. Then $K = Ca_1 \cup \cdots \cup Ca_n$ is a disjoint union and

$$n = [K : C] = \frac{|K|}{|C|} = \frac{|K|}{|H \cap K|} .$$

Note that $HC = H$. Thus

$$\begin{aligned} HK &= H(Ca_1 \cup \cdots \cup Ca_n) = HCa_1 \cup \cdots \cup HCa_n \\ &= Ha_1 \cup \cdots \cup Ha_n. \end{aligned}$$

Note that the last union is disjoint. If not, then $Ha_i = Ha_j$ for some $i \neq j$, i.e., $a_i a_j^{-1} \in H$; however, since $a_i, a_j \in K$, $a_i a_j^{-1} \in H \cap K = C$ and we reach a contradiction.

Theorem (4.7)

Let H and K be finite subgroups of a group G. Then

$$|HK| = \frac{|H||K|}{|H \cap K|} .$$

Proof. Let $C = H \cap K$ (then $C \leq K$) and let $\{a_1, \ldots, a_n\}$ be a complete set of right coset representatives of C in K. Then $K = Ca_1 \cup \cdots \cup Ca_n$ is a disjoint union and

$$n = [K : C] = \frac{|K|}{|C|} = \frac{|K|}{|H \cap K|} .$$

Note that $HC = H$. Thus

$$\begin{aligned} HK &= H(Ca_1 \cup \cdots \cup Ca_n) = HCa_1 \cup \cdots \cup HCa_n \\ &= Ha_1 \cup \cdots \cup Ha_n. \end{aligned}$$

Note that the last union is disjoint. Thus,

Theorem (4.7)

Let H and K be finite subgroups of a group G. Then

$$|HK| = \frac{|H||K|}{|H \cap K|} .$$

Proof. Let $C = H \cap K$ (then $C \leq K$) and let $\{a_1, \ldots, a_n\}$ be a complete set of right coset representatives of C in K. Then $K = Ca_1 \cup \cdots \cup Ca_n$ is a disjoint union and

$$n = [K : C] = \frac{|K|}{|C|} = \frac{|K|}{|H \cap K|} .$$

Note that $HC = H$. Thus

$$\begin{aligned} HK &= H(Ca_1 \cup \cdots \cup Ca_n) = HCa_1 \cup \cdots \cup HCa_n \\ &= Ha_1 \cup \cdots \cup Ha_n. \end{aligned}$$

Note that the last union is disjoint. Thus,

$$|HK|$$

Theorem (4.7)

Let H and K be finite subgroups of a group G. Then

$$|HK| = \frac{|H||K|}{|H \cap K|} .$$

Proof. Let $C = H \cap K$ (then $C \leq K$) and let $\{a_1, \ldots, a_n\}$ be a complete set of right coset representatives of C in K. Then $K = Ca_1 \cup \cdots \cup Ca_n$ is a disjoint union and

$$n = [K : C] = \frac{|K|}{|C|} = \frac{|K|}{|H \cap K|} .$$

Note that $HC = H$. Thus

$$\begin{aligned} HK &= H(Ca_1 \cup \cdots \cup Ca_n) = HCa_1 \cup \cdots \cup HCa_n \\ &= Ha_1 \cup \cdots \cup Ha_n. \end{aligned}$$

Note that the last union is disjoint. Thus,

$$|HK| = |H| \cdot n$$

Theorem (4.7)

Let H and K be finite subgroups of a group G. Then

$$|HK| = \frac{|H||K|}{|H \cap K|} .$$

Proof. Let $C = H \cap K$ (then $C \leq K$) and let $\{a_1, \ldots, a_n\}$ be a complete set of right coset representatives of C in K. Then $K = Ca_1 \cup \cdots \cup Ca_n$ is a disjoint union and

$$n = [K : C] = \frac{|K|}{|C|} = \frac{|K|}{|H \cap K|} .$$

Note that $HC = H$. Thus

$$\begin{aligned} HK &= H(Ca_1 \cup \cdots \cup Ca_n) = HCa_1 \cup \cdots \cup HCa_n \\ &= Ha_1 \cup \cdots \cup Ha_n. \end{aligned}$$

Note that the last union is disjoint. Thus,

$$|HK| = |H| \cdot n = |H| \cdot \frac{|K|}{|H \cap K|}.$$

Proposition (4.8)

Let H and K be subgroups of a group G.

Proposition (4.8)

Let H and K be subgroups of a group G.

- $[H : H \cap K] \leq [G : K]$.

Proposition (4.8)

Let H and K be subgroups of a group G.

- $[H : H \cap K] \leq [G : K]$.
- If $[G : K]$ is finite,

Proposition (4.8)

Let H and K be subgroups of a group G.

- $[H : H \cap K] \leq [G : K]$.
- If $[G : K]$ is finite, then
$$[H : H \cap K] = [G : K]$$

Proposition (4.8)

Let H and K be subgroups of a group G.

- $[H : H \cap K] \leq [G : K]$.
- If $[G : K]$ is finite, then

$$[H : H \cap K] = [G : K] \iff G = KH.$$

Proposition (4.8)

Let H and K be subgroups of a group G.

- $[H : H \cap K] \leq [G : K]$.
- If $[G : K]$ is finite, then

$$[H : H \cap K] = [G : K] \iff G = KH.$$

We will come back to prove this later.

Proposition (4.8)

Let H and K be subgroups of a group G.

- $[H : H \cap K] \leq [G : K]$.
- If $[G : K]$ is finite, then

$$[H : H \cap K] = [G : K] \iff G = KH.$$

We will come back to prove this later. We first use this theorem to prove the following Proposition.

Proposition (4.8)

Let H and K be subgroups of a group G.

- $[H : H \cap K] \leq [G : K]$.
- If $[G : K]$ is finite, then
$$[H : H \cap K] = [G : K] \iff G = KH.$$

Proposition (4.9)**.** Let H and K be subgroups of a group G

Proposition (4.8)

Let H and K be subgroups of a group G.

- $[H : H \cap K] \leq [G : K]$.
- If $[G : K]$ is finite, then
$$[H : H \cap K] = [G : K] \iff G = KH.$$

Proposition (4.9)**.** Let H and K be subgroups of a group G with finite index,

Proposition (4.8)

Let H and K be subgroups of a group G.

- $[H : H \cap K] \leq [G : K]$.
- If $[G : K]$ is finite, then
$$[H : H \cap K] = [G : K] \iff G = KH.$$

Proposition (4.9)**.** Let H and K be subgroups of a group G with finite index, i.e., $[G : H] < \infty$ and $[G : K] < \infty$.

Proposition (4.8)

Let H and K be subgroups of a group G.

- $[H : H \cap K] \leq [G : K]$.
- If $[G : K]$ is finite, then
$$[H : H \cap K] = [G : K] \iff G = KH.$$

Proposition (4.9)**.** Let H and K be subgroups of a group G with finite index, i.e., $[G : H] < \infty$ and $[G : K] < \infty$.

- $[G : H \cap K] < \infty$

Proposition (4.8)

Let H and K be subgroups of a group G.

- $[H : H \cap K] \leq [G : K]$.
- If $[G : K]$ is finite, then
$$[H : H \cap K] = [G : K] \iff G = KH.$$

Proposition (4.9)**.** Let H and K be subgroups of a group G with finite index, i.e., $[G : H] < \infty$ and $[G : K] < \infty$.

- $[G : H \cap K] < \infty$ and $[G : H \cap K] \leq [G : H][G : K]$.

Proposition (4.8)

Let H and K be subgroups of a group G.

- $[H : H \cap K] \leq [G : K]$.
- If $[G : K]$ is finite, then
$$[H : H \cap K] = [G : K] \iff G = KH.$$

Proposition (4.9)**.** Let H and K be subgroups of a group G with finite index, i.e., $[G : H] < \infty$ and $[G : K] < \infty$.

- $[G : H \cap K] < \infty$ and $[G : H \cap K] \leq [G : H][G : K]$.
- $[G : H \cap K] = [G : H][G : K] \iff G = KH$.

Proposition (4.8)

Let H and K be subgroups of a group G.

- $[H : H \cap K] \leq [G : K]$.
- If $[G : K]$ is finite, then
$$[H : H \cap K] = [G : K] \iff G = KH.$$

Proposition (4.9)**.** Let H and K be subgroups of a group G with finite index, i.e., $[G : H] < \infty$ and $[G : K] < \infty$.

- $[G : H \cap K] < \infty$ and $[G : H \cap K] \leq [G : H][G : K]$.
- $[G : H \cap K] = [G : H][G : K] \iff G = KH$.

$$[G : H \cap K] = [G : H][H : H \cap K]$$

by Theorem (4.5)

Proposition (4.8)

Let H and K be subgroups of a group G.

- $[H : H \cap K] \leq [G : K]$.
- If $[G : K]$ is finite, then
$$[H : H \cap K] = [G : K] \iff G = KH.$$

Proposition (4.9)**.** Let H and K be subgroups of a group G with finite index, i.e., $[G : H] < \infty$ and $[G : K] < \infty$.

- $[G : H \cap K] < \infty$ and $[G : H \cap K] \leq [G : H][G : K]$.
- $[G : H \cap K] = [G : H][G : K] \iff G = KH$.

$$[G : H \cap K] = [G : H][H : H \cap K] \leq [G : H][G : K]$$

by Proposition (4.8)

Proposition (4.8)

Let H and K be subgroups of a group G.

- $[H : H \cap K] \leq [G : K]$.
- If $[G : K]$ is finite, then
$$[H : H \cap K] = [G : K] \iff G = KH.$$

Proposition (4.9)**.** Let H and K be subgroups of a group G with finite index, i.e., $[G : H] < \infty$ and $[G : K] < \infty$.

- $[G : H \cap K] < \infty$ and $[G : H \cap K] \leq [G : H][G : K]$.
- $[G : H \cap K] = [G : H][G : K] \iff G = KH$.

$$[G : H \cap K] = [G : H][H : H \cap K] \leq [G : H][G : K] < \infty.$$

by the assumption

Proposition (4.8)

Let H and K be subgroups of a group G.

- $[H : H \cap K] \leq [G : K]$.
- If $[G : K]$ is finite, then
$$[H : H \cap K] = [G : K] \iff G = KH.$$

Proposition (4.9)**.** Let H and K be subgroups of a group G with finite index, i.e., $[G : H] < \infty$ and $[G : K] < \infty$.

- $[G : H \cap K] < \infty$ and $[G : H \cap K] \leq [G : H][G : K]$.
- $[G : H \cap K] = [G : H][G : K] \iff G = KH$.

$[G : H \cap K] = [G : H][H : H \cap K] \leq [G : H][G : K] < \infty$.
So, $[G : H \cap K] = [G : H][G : K] \Leftrightarrow [H : H \cap K] = [G : K]$

Proposition (4.8)

Let H and K be subgroups of a group G.

- $[H : H \cap K] \leq [G : K]$.
- If $[G : K]$ is finite, then
$$[H : H \cap K] = [G : K] \iff G = KH.$$

Proposition (4.9)**.** Let H and K be subgroups of a group G with finite index, i.e., $[G : H] < \infty$ and $[G : K] < \infty$.

- $[G : H \cap K] < \infty$ and $[G : H \cap K] \leq [G : H][G : K]$.
- $[G : H \cap K] = [G : H][G : K] \iff G = KH$.

$[G : H \cap K] = [G : H][H : H \cap K] \leq [G : H][G : K] < \infty$.

So, $[G : H \cap K] = [G : H][G : K] \Leftrightarrow [H : H \cap K] = [G : K]$

$\Leftrightarrow G = KH$

by Proposition (4.8)

Proposition (4.8)

Let H and K be subgroups of a group G.

- $[H : H \cap K] \leq [G : K]$.
- If $[G : K]$ is finite, then
$$[H : H \cap K] = [G : K] \iff G = KH.$$

Proposition (4.9)**.** Let H and K be subgroups of a group G with finite index, i.e., $[G : H] < \infty$ and $[G : K] < \infty$.

- $[G : H \cap K] < \infty$ and $[G : H \cap K] \leq [G : H][G : K]$.
- $[G : H \cap K] = [G : H][G : K] \iff G = KH$.

$[G : H \cap K] = [G : H][H : H \cap K] \leq [G : H][G : K] < \infty$.

So, $[G : H \cap K] = [G : H][G : K] \Leftrightarrow [H : H \cap K] = [G : K]$
$\Leftrightarrow G = KH$

In the proof, if we exchange the roles of H and K, we get

Proposition (4.8)

Let H and K be subgroups of a group G.

- $[H : H \cap K] \leq [G : K]$.
- If $[G : K]$ is finite, then
$$[H : H \cap K] = [G : K] \iff G = KH.$$

Proposition (4.9)**.** Let H and K be subgroups of a group G with finite index, i.e., $[G : H] < \infty$ and $[G : K] < \infty$.

- $[G : H \cap K] < \infty$ and $[G : H \cap K] \leq [G : H][G : K]$.
- $[G : H \cap K] = [G : H][G : K] \iff G = HK$.

$[G : H \cap K] = [G : H][H : H \cap K] \leq [G : H][G : K] < \infty$.

So, $[G : H \cap K] = [G : H][G : K] \Leftrightarrow [H : H \cap K] = [G : K]$
$\Leftrightarrow G = KH$

In the proof, if we exchange the roles of H and K, we get

Proposition (4.8)

Let H and K be subgroups of a group G.

- $[H : H \cap K] \leq [G : K]$.
- If $[G : K]$ is finite, then
$$[H : H \cap K] = [G : K] \iff G = KH.$$

Proposition (4.9)**.** Let H and K be subgroups of a group G with finite index, i.e., $[G : H] < \infty$ and $[G : K] < \infty$.

- $[G : H \cap K] < \infty$ and $[G : H \cap K] \leq [G : H][G : K]$.
- $[G : H \cap K] = [G : H][G : K] \iff G = HK$.

$[G : H \cap K] = [G : H][H : H \cap K] \leq [G : H][G : K] < \infty$.
So, $[G : H \cap K] = [G : H][G : K] \Leftrightarrow [H : H \cap K] = [G : K]$
$\Leftrightarrow G = KH$

In the proof, if we exchange the roles of H and K, we get
This is the statement in your book.

Proposition (4.8)

Let H and K be subgroups of a group G.

- $[H : H \cap K] \leq [G : K]$.
- If $[G : K]$ is finite, then

$$[H : H \cap K] = [G : K] \iff G = KH.$$

Proposition (4.8)

Let H and K be subgroups of a group G.

- $[H : H \cap K] \leq [G : K]$.
- If $[G : K]$ is finite, then

$$[H : H \cap K] = [G : K] \iff G = KH.$$

Proof. Let $\Gamma = \{(H \cap K)h \mid h \in H\}$

Proposition (4.8)

Let H and K be subgroups of a group G.

- $[H : H \cap K] \leq [G : K]$.
- If $[G : K]$ is finite, then

$$[H : H \cap K] = [G : K] \iff G = KH.$$

Proof. Let $\Gamma = \{(H \cap K)h \mid h \in H\}$ and $\Delta = \{Kg \mid g \in G\}$.

Proposition (4.8)

Let H and K be subgroups of a group G.

- $[H : H \cap K] \leq [G : K]$.
- If $[G : K]$ is finite, then

$$[H : H \cap K] = [G : K] \iff G = KH.$$

Proof. Let $\Gamma = \{(H \cap K)h \mid h \in H\}$ and $\Delta = \{Kg \mid g \in G\}$. Then $|\Gamma| = [H : H \cap K]$

Proposition (4.8)

Let H and K be subgroups of a group G.

- $[H : H \cap K] \leq [G : K]$.
- If $[G : K]$ is finite, then

$$[H : H \cap K] = [G : K] \iff G = KH.$$

Proof. Let $\Gamma = \{(H \cap K)h \mid h \in H\}$ and $\Delta = \{Kg \mid g \in G\}$. Then $|\Gamma| = [H : H \cap K]$ and $|\Delta| = [G : K]$.

Proposition (4.8)

Let H and K be subgroups of a group G.

- $[H : H \cap K] \leq [G : K]$.
- If $[G : K]$ is finite, then

$$[H : H \cap K] = [G : K] \iff G = KH.$$

Proof. Let $\Gamma = \{(H \cap K)h \mid h \in H\}$ and $\Delta = \{Kg \mid g \in G\}$. Then $|\Gamma| = [H : H \cap K]$ and $|\Delta| = [G : K]$. Note that for $h_1, h_2 \in H$,

Proposition (4.8)

Let H and K be subgroups of a group G.

- $[H : H \cap K] \leq [G : K]$.
- If $[G : K]$ is finite, then

$$[H : H \cap K] = [G : K] \iff G = KH.$$

Proof. Let $\Gamma = \{(H \cap K)h \mid h \in H\}$ and $\Delta = \{Kg \mid g \in G\}$. Then $|\Gamma| = [H : H \cap K]$ and $|\Delta| = [G : K]$. Note that for $h_1, h_2 \in H$,

$$(H \cap K)h_1 = (H \cap K)h_2$$

Proposition (4.8)

Let H and K be subgroups of a group G.

- $[H : H \cap K] \leq [G : K]$.
- If $[G : K]$ is finite, then

$$[H : H \cap K] = [G : K] \iff G = KH.$$

Proof. Let $\Gamma = \{(H \cap K)h \mid h \in H\}$ and $\Delta = \{Kg \mid g \in G\}$. Then $|\Gamma| = [H : H \cap K]$ and $|\Delta| = [G : K]$. Note that for $h_1, h_2 \in H$,

$$(H \cap K)h_1 = (H \cap K)h_2$$

$$\iff \quad h_1 h_2^{-1} \in H \cap K$$

Proposition (4.8)

Let H and K be subgroups of a group G.

- $[H : H \cap K] \leq [G : K]$.
- If $[G : K]$ is finite, then

$$[H : H \cap K] = [G : K] \iff G = KH.$$

Proof. Let $\Gamma = \{(H \cap K)h \mid h \in H\}$ and $\Delta = \{Kg \mid g \in G\}$. Then $|\Gamma| = [H : H \cap K]$ and $|\Delta| = [G : K]$. Note that for $h_1, h_2 \in H$,

$$\begin{aligned} & (H \cap K)h_1 = (H \cap K)h_2 \\ \iff \quad & h_1 h_2^{-1} \in H \cap K \\ \iff \quad & h_1 h_2^{-1} \in K \quad (\text{since } h_1 h_2^{-1} \in H) \end{aligned}$$

Proposition (4.8)

Let H and K be subgroups of a group G.

- $[H : H \cap K] \leq [G : K]$.
- If $[G : K]$ is finite, then

$$[H : H \cap K] = [G : K] \iff G = KH.$$

Proof. Let $\Gamma = \{(H \cap K)h \mid h \in H\}$ and $\Delta = \{Kg \mid g \in G\}$. Then $|\Gamma| = [H : H \cap K]$ and $|\Delta| = [G : K]$. Note that for $h_1, h_2 \in H$,

$$\begin{aligned} & (H \cap K)h_1 = (H \cap K)h_2 \\ \iff \quad & h_1 h_2^{-1} \in H \cap K \\ \iff \quad & h_1 h_2^{-1} \in K \quad (\text{since } h_1 h_2^{-1} \in H) \\ \iff \quad & Kh_1 = Kh_2. \end{aligned}$$

Proposition (4.8)

Let H and K be subgroups of a group G.

- $[H : H \cap K] \leq [G : K]$.
- If $[G : K]$ is finite, then

$$[H : H \cap K] = [G : K] \iff G = KH.$$

Proof. Let $\Gamma = \{(H \cap K)h \mid h \in H\}$ and $\Delta = \{Kg \mid g \in G\}$. Then $|\Gamma| = [H : H \cap K]$ and $|\Delta| = [G : K]$. Note that for $h_1, h_2 \in H$,

$$\begin{aligned} & (H \cap K)h_1 = (H \cap K)h_2 \\ \iff \quad & h_1 h_2^{-1} \in H \cap K \\ \iff \quad & h_1 h_2^{-1} \in K \quad (\text{since } h_1 h_2^{-1} \in H) \\ \iff \quad & Kh_1 = Kh_2. \end{aligned}$$

Hence the map $\phi : \Gamma \to \Delta$ with $(H \cap K)h \mapsto Kh$

Proposition (4.8)

Let H and K be subgroups of a group G.

- $[H : H \cap K] \leq [G : K]$.
- If $[G : K]$ is finite, then

$$[H : H \cap K] = [G : K] \iff G = KH.$$

Proof. Let $\Gamma = \{(H \cap K)h \mid h \in H\}$ and $\Delta = \{Kg \mid g \in G\}$. Then $|\Gamma| = [H : H \cap K]$ and $|\Delta| = [G : K]$. Note that for $h_1, h_2 \in H$,

$$\begin{aligned} & (H \cap K)h_1 = (H \cap K)h_2 \\ \iff \quad & h_1 h_2^{-1} \in H \cap K \\ \iff \quad & h_1 h_2^{-1} \in K \quad (\text{since } h_1 h_2^{-1} \in H) \\ \iff \quad & Kh_1 = Kh_2. \end{aligned}$$

Hence the map $\phi : \Gamma \to \Delta$ with $(H \cap K)h \mapsto Kh$ is well-defined

Proposition (4.8)

Let H and K be subgroups of a group G.

- $[H : H \cap K] \leq [G : K]$.
- If $[G : K]$ is finite, then
$$[H : H \cap K] = [G : K] \iff G = KH.$$

Proof. Let $\Gamma = \{(H \cap K)h \mid h \in H\}$ and $\Delta = \{Kg \mid g \in G\}$. Then $|\Gamma| = [H : H \cap K]$ and $|\Delta| = [G : K]$. Note that for $h_1, h_2 \in H$,

$$\begin{aligned} & (H \cap K)h_1 = (H \cap K)h_2 \\ \iff \quad & h_1 h_2^{-1} \in H \cap K \\ \iff \quad & h_1 h_2^{-1} \in K \quad (\text{since } h_1 h_2^{-1} \in H) \\ \iff \quad & Kh_1 = Kh_2. \end{aligned}$$

Hence the map $\phi : \Gamma \to \Delta$ with $(H \cap K)h \mapsto Kh$ is well-defined and is injective,

Proposition (4.8)

Let H and K be subgroups of a group G.

- $[H : H \cap K] \leq [G : K]$.
- If $[G : K]$ is finite, then

$$[H : H \cap K] = [G : K] \iff G = KH.$$

Proof. Let $\Gamma = \{(H \cap K)h \mid h \in H\}$ and $\Delta = \{Kg \mid g \in G\}$. Then $|\Gamma| = [H : H \cap K]$ and $|\Delta| = [G : K]$. Note that for $h_1, h_2 \in H$,

$$\begin{aligned} & (H \cap K)h_1 = (H \cap K)h_2 \\ \iff \quad & h_1 h_2^{-1} \in H \cap K \\ \iff \quad & h_1 h_2^{-1} \in K \quad (\text{since } h_1 h_2^{-1} \in H) \\ \iff \quad & Kh_1 = Kh_2. \end{aligned}$$

Hence the map $\phi : \Gamma \to \Delta$ with $(H \cap K)h \mapsto Kh$ is well-defined and is injective, so $|\Gamma| \leq |\Delta|$.

Proposition (4.8)

Let H and K be subgroups of a group G.

- $[H : H \cap K] \leq [G : K]$.
- If $[G : K]$ is finite, then

$$[H : H \cap K] = [G : K] \iff G = KH.$$

Proof. Let $\Gamma = \{(H \cap K)h \mid h \in H\}$ and $\Delta = \{Kg \mid g \in G\}$. Then $|\Gamma| = [H : H \cap K]$ and $|\Delta| = [G : K]$. Hence the map $\phi : \Gamma \to \Delta$ with $(H \cap K)h \mapsto Kh$ is well-defined and is injective.

Proposition (4.8)

Let H and K be subgroups of a group G.

- $[H : H \cap K] \leq [G : K]$.
- If $[G : K]$ is finite, then

$$[H : H \cap K] = [G : K] \iff G = KH.$$

Proof. Let $\Gamma = \{(H \cap K)h \mid h \in H\}$ and $\Delta = \{Kg \mid g \in G\}$. Then $|\Gamma| = [H : H \cap K]$ and $|\Delta| = [G : K]$. Hence the map $\phi : \Gamma \to \Delta$ with $(H \cap K)h \mapsto Kh$ is well-defined and is injective. Furthermore, if $[G : K] < \infty$, i.e., $|\Delta| < \infty$,

Proposition (4.8)

Let H and K be subgroups of a group G.

- $[H : H \cap K] \leq [G : K]$.
- If $[G : K]$ is finite, then

$$[H : H \cap K] = [G : K] \iff G = KH.$$

Proof. Let $\Gamma = \{(H \cap K)h \mid h \in H\}$ and $\Delta = \{Kg \mid g \in G\}$. Then $|\Gamma| = [H : H \cap K]$ and $|\Delta| = [G : K]$. Hence the map $\phi : \Gamma \to \Delta$ with $(H \cap K)h \mapsto Kh$ is well-defined and is injective. Furthermore, if $[G : K] < \infty$, i.e., $|\Delta| < \infty$, then

Proposition (4.8)

Let H and K be subgroups of a group G.

- $[H : H \cap K] \leq [G : K]$.
- If $[G : K]$ is finite, then

$$[H : H \cap K] = [G : K] \iff G = KH.$$

Proof. Let $\Gamma = \{(H \cap K)h \mid h \in H\}$ and $\Delta = \{Kg \mid g \in G\}$. Then $|\Gamma| = [H : H \cap K]$ and $|\Delta| = [G : K]$. Hence the map $\phi : \Gamma \to \Delta$ with $(H \cap K)h \mapsto Kh$ is well-defined and is injective. Furthermore, if $[G : K] < \infty$, i.e., $|\Delta| < \infty$, then

$$|\Gamma| = |\Delta|$$

Proposition (4.8)

Let H and K be subgroups of a group G.

- $[H : H \cap K] \leq [G : K]$.
- If $[G : K]$ is finite, then

$$[H : H \cap K] = [G : K] \iff G = KH.$$

Proof. Let $\Gamma = \{(H \cap K)h \mid h \in H\}$ and $\Delta = \{Kg \mid g \in G\}$. Then $|\Gamma| = [H : H \cap K]$ and $|\Delta| = [G : K]$. Hence the map $\phi : \Gamma \to \Delta$ with $(H \cap K)h \mapsto Kh$ is well-defined and is injective. Furthermore, if $[G : K] < \infty$, i.e., $|\Delta| < \infty$, then

$$|\Gamma| = |\Delta| \iff \phi \text{ is surjective}$$

Proposition (4.8)

Let H and K be subgroups of a group G.

- $[H : H \cap K] \leq [G : K]$.
- If $[G : K]$ is finite, then

$$[H : H \cap K] = [G : K] \iff G = KH.$$

Proof. Let $\Gamma = \{(H \cap K)h \mid h \in H\}$ and $\Delta = \{Kg \mid g \in G\}$. Then $|\Gamma| = [H : H \cap K]$ and $|\Delta| = [G : K]$. Hence the map $\phi : \Gamma \to \Delta$ with $(H \cap K)h \mapsto Kh$ is well-defined and is injective. Furthermore, if $[G : K] < \infty$, i.e., $|\Delta| < \infty$, then

$|\Gamma| = |\Delta| \iff \phi$ is surjective (since ϕ is injective)

Proposition (4.8)

Let H and K be subgroups of a group G.

- $[H : H \cap K] \leq [G : K]$.
- If $[G : K]$ is finite, then

$$[H : H \cap K] = [G : K] \iff G = KH.$$

Proof. Let $\Gamma = \{(H \cap K)h \mid h \in H\}$ and $\Delta = \{Kg \mid g \in G\}$. Then $|\Gamma| = [H : H \cap K]$ and $|\Delta| = [G : K]$. Hence the map $\phi : \Gamma \to \Delta$ with $(H \cap K)h \mapsto Kh$ is well-defined and is injective. Furthermore, if $[G : K] < \infty$, i.e., $|\Delta| < \infty$, then

$$|\Gamma| = |\Delta| \iff \phi \text{ is surjective (since } \phi \text{ is injective)}$$

$$\iff \Delta = \{Kg \mid g \in G\}$$

Proposition (4.8)

Let H and K be subgroups of a group G.

- $[H : H \cap K] \leq [G : K]$.
- If $[G : K]$ is finite, then

$$[H : H \cap K] = [G : K] \iff G = KH.$$

Proof. Let $\Gamma = \{(H \cap K)h \mid h \in H\}$ and $\Delta = \{Kg \mid g \in G\}$. Then $|\Gamma| = [H : H \cap K]$ and $|\Delta| = [G : K]$. Hence the map $\phi : \Gamma \to \Delta$ with $(H \cap K)h \mapsto Kh$ is well-defined and is injective. Furthermore, if $[G : K] < \infty$, i.e., $|\Delta| < \infty$, then

$$|\Gamma| = |\Delta| \iff \phi \text{ is surjective (since } \phi \text{ is injective)}$$

$$\iff \Delta = \{Kg \mid g \in G\} = \{Kh \mid h \in H\}$$

Proposition (4.8)

Let H and K be subgroups of a group G.

- $[H : H \cap K] \leq [G : K]$.
- If $[G : K]$ is finite, then

$$[H : H \cap K] = [G : K] \iff G = KH.$$

Proof. Let $\Gamma = \{(H \cap K)h \mid h \in H\}$ and $\Delta = \{Kg \mid g \in G\}$. Then $|\Gamma| = [H : H \cap K]$ and $|\Delta| = [G : K]$. Hence the map $\phi : \Gamma \to \Delta$ with $(H \cap K)h \mapsto Kh$ is well-defined and is injective. Furthermore, if $[G : K] < \infty$, i.e., $|\Delta| < \infty$, then

$$\begin{aligned} |\Gamma| = |\Delta| &\iff \phi \text{ is surjective (since } \phi \text{ is injective)} \\ &\iff \Delta = \{Kg \mid g \in G\} = \{Kh \mid h \in H\} \\ &\iff G = KH. \end{aligned}$$

Proposition (4.8)

Let H and K be subgroups of a group G.

- $[H : H \cap K] \leq [G : K]$.
- If $[G : K]$ is finite, then

$$[H : H \cap K] = [G : K] \iff G = KH.$$

Proof. Let $\Gamma = \{(H \cap K)h \mid h \in H\}$ and $\Delta = \{Kg \mid g \in G\}$. Then $|\Gamma| = [H : H \cap K]$ and $|\Delta| = [G : K]$. Hence the map $\phi : \Gamma \to \Delta$ with $(H \cap K)h \mapsto Kh$ is well-defined and is injective. Furthermore, if $[G : K] < \infty$, i.e., $|\Delta| < \infty$, then

$$|\Gamma| = |\Delta| \iff \phi \text{ is surjective (since } \phi \text{ is injective)}$$

$$\iff \Delta = \{Kg \mid g \in G\} = \{Kh \mid h \in H\}$$

$$\iff G = KH.$$

"$\Longrightarrow$": $\forall g \in G$,

Proposition (4.8)

Let H and K be subgroups of a group G.

- $[H : H \cap K] \leq [G : K]$.
- If $[G : K]$ is finite, then

$$[H : H \cap K] = [G : K] \iff G = KH.$$

Proof. Let $\Gamma = \{(H \cap K)h \mid h \in H\}$ and $\Delta = \{Kg \mid g \in G\}$. Then $|\Gamma| = [H : H \cap K]$ and $|\Delta| = [G : K]$. Hence the map $\phi : \Gamma \to \Delta$ with $(H \cap K)h \mapsto Kh$ is well-defined and is injective. Furthermore, if $[G : K] < \infty$, i.e., $|\Delta| < \infty$, then

$$|\Gamma| = |\Delta| \iff \phi \text{ is surjective (since } \phi \text{ is injective)}$$

$$\iff \Delta = \{Kg \mid g \in G\} = \{Kh \mid h \in H\}$$

$$\iff G = KH.$$

"$\Longrightarrow$": $\forall g \in G$, since $Kg = Kh$ for some $h \in H$,

Proposition (4.8)

Let H and K be subgroups of a group G.

- $[H : H \cap K] \leq [G : K]$.
- If $[G : K]$ is finite, then

$$[H : H \cap K] = [G : K] \iff G = KH.$$

Proof. Let $\Gamma = \{(H \cap K)h \mid h \in H\}$ and $\Delta = \{Kg \mid g \in G\}$. Then $|\Gamma| = [H : H \cap K]$ and $|\Delta| = [G : K]$. Hence the map $\phi : \Gamma \to \Delta$ with $(H \cap K)h \mapsto Kh$ is well-defined and is injective. Furthermore, if $[G : K] < \infty$, i.e., $|\Delta| < \infty$, then

$$|\Gamma| = |\Delta| \iff \phi \text{ is surjective (since } \phi \text{ is injective)}$$

$$\iff \Delta = \{Kg \mid g \in G\} = \{Kh \mid h \in H\}$$

$$\iff G = KH.$$

"$\Longrightarrow$": $\forall g \in G$, since $Kg = Kh$ for some $h \in H$, we have $g \in Kg$

Proposition (4.8)

Let H and K be subgroups of a group G.

- $[H : H \cap K] \leq [G : K]$.
- If $[G : K]$ is finite, then

$$[H : H \cap K] = [G : K] \iff G = KH.$$

Proof. Let $\Gamma = \{(H \cap K)h \mid h \in H\}$ and $\Delta = \{Kg \mid g \in G\}$. Then $|\Gamma| = [H : H \cap K]$ and $|\Delta| = [G : K]$. Hence the map $\phi : \Gamma \to \Delta$ with $(H \cap K)h \mapsto Kh$ is well-defined and is injective. Furthermore, if $[G : K] < \infty$, i.e., $|\Delta| < \infty$, then

$$|\Gamma| = |\Delta| \iff \phi \text{ is surjective (since } \phi \text{ is injective)}$$

$$\iff \Delta = \{Kg \mid g \in G\} = \{Kh \mid h \in H\}$$

$$\iff G = KH.$$

"$\Longrightarrow$": $\forall g \in G$, since $Kg = Kh$ for some $h \in H$, we have $g \in Kg = Kh$

Proposition (4.8)

Let H and K be subgroups of a group G.

- $[H : H \cap K] \leq [G : K]$.
- If $[G : K]$ is finite, then

$$[H : H \cap K] = [G : K] \iff G = KH.$$

Proof. Let $\Gamma = \{(H \cap K)h \mid h \in H\}$ and $\Delta = \{Kg \mid g \in G\}$. Then $|\Gamma| = [H : H \cap K]$ and $|\Delta| = [G : K]$. Hence the map $\phi : \Gamma \to \Delta$ with $(H \cap K)h \mapsto Kh$ is well-defined and is injective. Furthermore, if $[G : K] < \infty$, i.e., $|\Delta| < \infty$, then

$$|\Gamma| = |\Delta| \iff \phi \text{ is surjective (since } \phi \text{ is injective)}$$

$$\iff \Delta = \{Kg \mid g \in G\} = \{Kh \mid h \in H\}$$

$$\iff G = KH.$$

"$\Longrightarrow$": $\forall g \in G$, since $Kg = Kh$ for some $h \in H$, we have $g \in Kg = Kh \subseteq KH$.

Proposition (4.8)

Let H and K be subgroups of a group G.

- $[H : H \cap K] \leq [G : K]$.
- If $[G : K]$ is finite, then

$$[H : H \cap K] = [G : K] \iff G = KH.$$

Proof. Let $\Gamma = \{(H \cap K)h \mid h \in H\}$ and $\Delta = \{Kg \mid g \in G\}$. Then $|\Gamma| = [H : H \cap K]$ and $|\Delta| = [G : K]$. Hence the map $\phi : \Gamma \to \Delta$ with $(H \cap K)h \mapsto Kh$ is well-defined and is injective. Furthermore, if $[G : K] < \infty$, i.e., $|\Delta| < \infty$, then

$$|\Gamma| = |\Delta| \iff \phi \text{ is surjective (since } \phi \text{ is injective)}$$

$$\iff \Delta = \{Kg \mid g \in G\} = \{Kh \mid h \in H\}$$

$$\iff G = KH.$$

"$\Longleftarrow$":

Proposition (4.8)

Let H and K be subgroups of a group G.

- $[H : H \cap K] \leq [G : K]$.
- If $[G : K]$ is finite, then

$$[H : H \cap K] = [G : K] \iff G = KH.$$

Proof. Let $\Gamma = \{(H \cap K)h \mid h \in H\}$ and $\Delta = \{Kg \mid g \in G\}$. Then $|\Gamma| = [H : H \cap K]$ and $|\Delta| = [G : K]$. Hence the map $\phi : \Gamma \to \Delta$ with $(H \cap K)h \mapsto Kh$ is well-defined and is injective. Furthermore, if $[G : K] < \infty$, i.e., $|\Delta| < \infty$, then

$$|\Gamma| = |\Delta| \iff \phi \text{ is surjective (since } \phi \text{ is injective)}$$

$$\iff \Delta = \{Kg \mid g \in G\} = \{Kh \mid h \in H\}$$

$$\iff G = KH.$$

"$\Longleftarrow$":

Proposition (4.8)

Let H and K be subgroups of a group G.

- $[H : H \cap K] \leq [G : K]$.
- If $[G : K]$ is finite, then

$$[H : H \cap K] = [G : K] \iff G = KH.$$

Proof. Let $\Gamma = \{(H \cap K)h \mid h \in H\}$ and $\Delta = \{Kg \mid g \in G\}$. Then $|\Gamma| = [H : H \cap K]$ and $|\Delta| = [G : K]$. Hence the map $\phi : \Gamma \to \Delta$ with $(H \cap K)h \mapsto Kh$ is well-defined and is injective. Furthermore, if $[G : K] < \infty$, i.e., $|\Delta| < \infty$, then

$$|\Gamma| = |\Delta| \iff \phi \text{ is surjective (since } \phi \text{ is injective)}$$

$$\iff \Delta = \{Kg \mid g \in G\} = \{Kh \mid h \in H\}$$

$$\iff G = KH.$$

"$\Longleftarrow$": $\forall g \in G$,

Proposition (4.8)

Let H and K be subgroups of a group G.

- $[H : H \cap K] \leq [G : K]$.
- If $[G : K]$ is finite, then

$$[H : H \cap K] = [G : K] \iff G = KH.$$

Proof. Let $\Gamma = \{(H \cap K)h \mid h \in H\}$ and $\Delta = \{Kg \mid g \in G\}$. Then $|\Gamma| = [H : H \cap K]$ and $|\Delta| = [G : K]$. Hence the map $\phi : \Gamma \to \Delta$ with $(H \cap K)h \mapsto Kh$ is well-defined and is injective. Furthermore, if $[G : K] < \infty$, i.e., $|\Delta| < \infty$, then

$$|\Gamma| = |\Delta| \iff \phi \text{ is surjective (since } \phi \text{ is injective)}$$

$$\iff \Delta = \{Kg \mid g \in G\} = \{Kh \mid h \in H\}$$

$$\iff G = KH.$$

"$\Longleftarrow$": $\forall g \in G$, since $g \in G = KH$,

Proposition (4.8)

Let H and K be subgroups of a group G.

- $[H : H \cap K] \leq [G : K]$.
- If $[G : K]$ is finite, then

$$[H : H \cap K] = [G : K] \iff G = KH.$$

Proof. Let $\Gamma = \{(H \cap K)h \mid h \in H\}$ and $\Delta = \{Kg \mid g \in G\}$. Then $|\Gamma| = [H : H \cap K]$ and $|\Delta| = [G : K]$. Hence the map $\phi : \Gamma \to \Delta$ with $(H \cap K)h \mapsto Kh$ is well-defined and is injective. Furthermore, if $[G : K] < \infty$, i.e., $|\Delta| < \infty$, then

$$|\Gamma| = |\Delta| \iff \phi \text{ is surjective (since } \phi \text{ is injective)}$$

$$\iff \Delta = \{Kg \mid g \in G\} = \{Kh \mid h \in H\}$$

$$\iff G = KH.$$

"$\Longleftarrow$": $\forall g \in G$, since $g \in G = KH$, $g = kh$ for some $k \in K$ and $h \in H$,

Proposition (4.8)

Let H and K be subgroups of a group G.

- $[H : H \cap K] \leq [G : K]$.
- If $[G : K]$ is finite, then

$$[H : H \cap K] = [G : K] \iff G = KH.$$

Proof. Let $\Gamma = \{(H \cap K)h \mid h \in H\}$ and $\Delta = \{Kg \mid g \in G\}$. Then $|\Gamma| = [H : H \cap K]$ and $|\Delta| = [G : K]$. Hence the map $\phi : \Gamma \to \Delta$ with $(H \cap K)h \mapsto Kh$ is well-defined and is injective. Furthermore, if $[G : K] < \infty$, i.e., $|\Delta| < \infty$, then

$$|\Gamma| = |\Delta| \iff \phi \text{ is surjective (since } \phi \text{ is injective)}$$

$$\iff \Delta = \{Kg \mid g \in G\} = \{Kh \mid h \in H\}$$

$$\iff G = KH.$$

"$\Longleftarrow$": $\forall g \in G$, since $g \in G = KH$, $g = kh$ for some $k \in K$ and $h \in H$, and so $Kg = Kkh$

Proposition (4.8)

Let H and K be subgroups of a group G.

- $[H : H \cap K] \leq [G : K]$.
- If $[G : K]$ is finite, then

$$[H : H \cap K] = [G : K] \iff G = KH.$$

Proof. Let $\Gamma = \{(H \cap K)h \mid h \in H\}$ and $\Delta = \{Kg \mid g \in G\}$. Then $|\Gamma| = [H : H \cap K]$ and $|\Delta| = [G : K]$. Hence the map $\phi : \Gamma \to \Delta$ with $(H \cap K)h \mapsto Kh$ is well-defined and is injective. Furthermore, if $[G : K] < \infty$, i.e., $|\Delta| < \infty$, then

$$|\Gamma| = |\Delta| \iff \phi \text{ is surjective (since } \phi \text{ is injective)}$$

$$\iff \Delta = \{Kg \mid g \in G\} = \{Kh \mid h \in H\}$$

$$\iff G = KH.$$

"$\Longleftarrow$": $\forall g \in G$, since $g \in G = KH$, $g = kh$ for some $k \in K$ and $h \in H$, and so $Kg = Kkh = Kh$.

Chapter I

Section I.5: Normality, Quotient Groups, and Homomorphisms

Chapter I

Section I.5: Normality, Quotient Groups, and Homomorphisms

Recall: Let H be a subgroup of a group G.

Chapter I

Section I.5: Normality, Quotient Groups, and Homomorphisms

Recall: Let H be a subgroup of a group G.

- For $a, b \in G$,

Chapter I

Section I.5: Normality, Quotient Groups, and Homomorphisms

Recall: Let H be a subgroup of a group G.

- For $a, b \in G$,
  - ⋆ if $ab^{-1} \in H$,

Chapter I

Section I.5: Normality, Quotient Groups, and Homomorphisms

Recall: Let H be a subgroup of a group G.

- For $a, b \in G$,
  - ⋆ if $ab^{-1} \in H$, a is right congruent to b modulo H,

Chapter I

Section I.5: Normality, Quotient Groups, and Homomorphisms

Recall: Let H be a subgroup of a group G.

- For $a, b \in G$,
  - ⋆ if $ab^{-1} \in H$, a is right congruent to b modulo H, denoted $a \equiv_r b \pmod{H}$;

Chapter I

Section I.5: Normality, Quotient Groups, and Homomorphisms

Recall: Let H be a subgroup of a group G.

- For $a, b \in G$,
  - ⋆ if $ab^{-1} \in H$, a is right congruent to b modulo H, denoted $a \equiv_r b \pmod{H}$;
  - ⋆ if $a^{-1}b \in H$,

Chapter I

Section I.5: Normality, Quotient Groups, and Homomorphisms

Recall: Let H be a subgroup of a group G.

- For $a, b \in G$,
  - ⋆ if $ab^{-1} \in H$, a is right congruent to b modulo H, denoted $a \equiv_r b \pmod{H}$;
  - ⋆ if $a^{-1}b \in H$, a is left congruent to b modulo H,

Chapter I

Section I.5: Normality, Quotient Groups, and Homomorphisms

Recall: Let H be a subgroup of a group G.

- For $a, b \in G$,
  - ⋆ if $ab^{-1} \in H$, a is right congruent to b modulo H, denoted $a \equiv_r b \pmod{H}$;
  - ⋆ if $a^{-1}b \in H$, a is left congruent to b modulo H, denoted $a \equiv_l b \pmod{H}$.

Chapter I

Section I.5: Normality, Quotient Groups, and Homomorphisms

Recall: Let H be a subgroup of a group G.

- For $a, b \in G$,
  - ⋆ if $ab^{-1} \in H$, a is right congruent to b modulo H, denoted $a \equiv_r b \pmod{H}$;
  - ⋆ if $a^{-1}b \in H$, a is left congruent to b modulo H, denoted $a \equiv_l b \pmod{H}$.
- Right (resp. left) congruence modulo H

Chapter I

Section I.5: Normality, Quotient Groups, and Homomorphisms

Recall: Let H be a subgroup of a group G.

- For $a, b \in G$,
  - ⋆ if $ab^{-1} \in H$, a is right congruent to b modulo H, denoted $a \equiv_r b \pmod{H}$;
  - ⋆ if $a^{-1}b \in H$, a is left congruent to b modulo H, denoted $a \equiv_l b \pmod{H}$.
- Right (resp. left) congruence modulo H is an equivalence relation on G.

Chapter I

Section I.5: Normality, Quotient Groups, and Homomorphisms

Recall: Let H be a subgroup of a group G.

- For $a, b \in G$,
  - ⋆ if $ab^{-1} \in H$, a is right congruent to b modulo H, denoted $a \equiv_r b \pmod{H}$;
  - ⋆ if $a^{-1}b \in H$, a is left congruent to b modulo H, denoted $a \equiv_l b \pmod{H}$.
- Right (resp. left) congruence modulo H is an equivalence relation on G.

Chapter I

Section I.5: Normality, Quotient Groups, and Homomorphisms

Recall: Let H be a subgroup of a group G.

- For $a, b \in G$,
  - ⋆ if $ab^{-1} \in H$, a is right congruent to b modulo H, denoted $a \equiv_r b \pmod{H}$;
  - ⋆ if $a^{-1}b \in H$, a is left congruent to b modulo H, denoted $a \equiv_l b \pmod{H}$.
- Right (resp. left) congruence modulo H is an equivalence relation on G.
- The equivalence class of $a \in G$ under right (resp. left) congruence modulo H is

Chapter I

Section I.5: Normality, Quotient Groups, and Homomorphisms

Recall: Let H be a subgroup of a group G.

- For $a, b \in G$,
  - ⋆ if $ab^{-1} \in H$, a is right congruent to b modulo H, denoted $a \equiv_r b \pmod{H}$;
  - ⋆ if $a^{-1}b \in H$, a is left congruent to b modulo H, denoted $a \equiv_l b \pmod{H}$.
- Right (resp. left) congruence modulo H is an equivalence relation on G.
- The equivalence class of $a \in G$ under right (resp. left) congruence modulo H is the right coset $Ha = \{ha \mid h \in H\}$

Chapter I

Section I.5: Normality, Quotient Groups, and Homomorphisms

Recall: Let H be a subgroup of a group G.

- For $a, b \in G$,
  - ⋆ if $ab^{-1} \in H$, a is right congruent to b modulo H, denoted $a \equiv_r b \pmod{H}$;
  - ⋆ if $a^{-1}b \in H$, a is left congruent to b modulo H, denoted $a \equiv_l b \pmod{H}$.
- Right (resp. left) congruence modulo H is an equivalence relation on G.
- The equivalence class of $a \in G$ under right (resp. left) congruence modulo H is the right coset $Ha = \{ha \mid h \in H\}$

Chapter I

Section I.5: Normality, Quotient Groups, and Homomorphisms

Recall: Let H be a subgroup of a group G.

- For $a, b \in G$,
  - ⋆ if $ab^{-1} \in H$, a is right congruent to b modulo H, denoted $a \equiv_r b \pmod{H}$;
  - ⋆ if $a^{-1}b \in H$, a is left congruent to b modulo H, denoted $a \equiv_l b \pmod{H}$.
- Right (resp. left) congruence modulo H is an equivalence relation on G.
- The equivalence class of $a \in G$ under right (resp. left) congruence modulo H is the right coset $Ha = \{ha \mid h \in H\}$ (resp. the left coset $aH = \{ah \mid h \in H\}$).

Theorem 5.1

Let N be a subgroup of a group G. The following conditions are equivalent:

Theorem 5.1

Let N be a subgroup of a group G. TFAE:

Theorem 5.1

Let N be a subgroup of a group G. TFAE:

(i) Left and right congruence modulo N coincide,

Theorem 5.1

Let N be a subgroup of a group G. TFAE:

(i) Left and right congruence modulo N coincide, that is, they define the same equivalence relation on G.

Theorem 5.1

Let N be a subgroup of a group G. TFAE:

(i) Left and right congruence modulo N coincide, that is, they define the same equivalence relation on G.

(ii) Every left coset of N in G is a right coset of N in G.

Theorem 5.1

Let N be a subgroup of a group G. TFAE:

(i) Left and right congruence modulo N coincide, that is, they define the same equivalence relation on G.

(ii) Every left coset of N in G is a right coset of N in G.

(iii) $aN = Na, \forall a \in G$.

Theorem 5.1

Let N be a subgroup of a group G. TFAE:

(i) Left and right congruence modulo N coincide, that is, they define the same equivalence relation on G.

(ii) Every left coset of N in G is a right coset of N in G.

(iii) $aN = Na, \forall a \in G$.

(iv) $\forall a \in G, \forall x \in N, axa^{-1} \in N$

Theorem 5.1

Let N be a subgroup of a group G. TFAE:

(i) Left and right congruence modulo N coincide, that is, they define the same equivalence relation on G.

(ii) Every left coset of N in G is a right coset of N in G.

(iii) $aN = Na, \forall a \in G$.

(iv) $\forall a \in G$, $aNa^{-1} \subseteq N$, where $aNa^{-1} = \{axa^{-1} \mid x \in N\}$.

Theorem 5.1

Let N be a subgroup of a group G. TFAE:

(i) Left and right congruence modulo N coincide, that is, they define the same equivalence relation on G.

(ii) Every left coset of N in G is a right coset of N in G.

(iii) $aN = Na, \forall a \in G$.

(iv) $\forall a \in G, aNa^{-1} \subseteq N$, where $aNa^{-1} = \{axa^{-1} \mid x \in N\}$.

(v) $\forall a \in G, aNa^{-1} = N$.

Theorem 5.1

Let N be a subgroup of a group G. TFAE:

(i) Left and right congruence modulo N coincide, that is, they define the same equivalence relation on G.

(ii) Every left coset of N in G is a right coset of N in G.

(iii) $aN = Na, \forall a \in G$.

(iv) $\forall a \in G$, $aNa^{-1} \subseteq N$, where $aNa^{-1} = \{axa^{-1} \mid x \in N\}$.

(v) $\forall a \in G$, $aNa^{-1} = N$.

Proof.

(i) $\Leftrightarrow$ (iii),

Theorem 5.1

Let N be a subgroup of a group G. TFAE:

(i) Left and right congruence modulo N coincide, that is, they define the same equivalence relation on G.

(ii) Every left coset of N in G is a right coset of N in G.

(iii) $aN = Na, \forall a \in G$.

(iv) $\forall a \in G$, $aNa^{-1} \subseteq N$, where $aNa^{-1} = \{axa^{-1} \mid x \in N\}$.

(v) $\forall a \in G$, $aNa^{-1} = N$.

Proof.

(i) $\Leftrightarrow$ (iii), since the left (resp. right) cosets

Theorem 5.1

Let N be a subgroup of a group G. TFAE:

(i) Left and right congruence modulo N coincide, that is, they define the same equivalence relation on G.

(ii) Every left coset of N in G is a right coset of N in G.

(iii) $aN = Na, \forall a \in G$.

(iv) $\forall a \in G$, $aNa^{-1} \subseteq N$, where $aNa^{-1} = \{axa^{-1} \mid x \in N\}$.

(v) $\forall a \in G$, $aNa^{-1} = N$.

Proof.

(i) $\Leftrightarrow$ (iii), since the left (resp. right) cosets are precisely the equivalence classes under the equivalence relation defined by left (resp. right) congruence.

Theorem 5.1

Let N be a subgroup of a group G. TFAE:

(i) Left and right congruence modulo N coincide, that is, they define the same equivalence relation on G.

(ii) Every left coset of N in G is a right coset of N in G.

(iii) $aN = Na, \forall a \in G$.

(iv) $\forall a \in G$, $aNa^{-1} \subseteq N$, where $aNa^{-1} = \{axa^{-1} \mid x \in N\}$.

(v) $\forall a \in G$, $aNa^{-1} = N$.

Proof. (i) $\Leftrightarrow$ (iii)

(i) $\Leftrightarrow$ (iii), since the left (resp. right) cosets are precisely the equivalence classes under the equivalence relation defined by left (resp. right) congruence.

Theorem 5.1

Let N be a subgroup of a group G. TFAE:

(i) Left and right congruence modulo N coincide, that is, they define the same equivalence relation on G.

(ii) Every left coset of N in G is a right coset of N in G.

(iii) $aN = Na, \forall a \in G$.

(iv) $\forall a \in G$, $aNa^{-1} \subseteq N$, where $aNa^{-1} = \{axa^{-1} \mid x \in N\}$.

(v) $\forall a \in G$, $aNa^{-1} = N$.

Proof. (i) $\Leftrightarrow$ (iii)

(iii) $\Rightarrow$ (ii) is clear.

Theorem 5.1

Let N be a subgroup of a group G. TFAE:

(i) Left and right congruence modulo N coincide, that is, they define the same equivalence relation on G.

(ii) Every left coset of N in G is a right coset of N in G.

(iii) $aN = Na, \forall a \in G$.

(iv) $\forall a \in G$, $aNa^{-1} \subseteq N$, where $aNa^{-1} = \{axa^{-1} \mid x \in N\}$.

(v) $\forall a \in G$, $aNa^{-1} = N$.

Proof. (i) $\Leftrightarrow$ (iii) $\Rightarrow$ (ii)

(iii) $\Rightarrow$ (ii) is clear.

Theorem 5.1

Let N be a subgroup of a group G. TFAE:

(i) Left and right congruence modulo N coincide, that is, they define the same equivalence relation on G.

(ii) Every left coset of N in G is a right coset of N in G.

(iii) $aN = Na, \forall a \in G$.

(iv) $\forall a \in G$, $aNa^{-1} \subseteq N$, where $aNa^{-1} = \{axa^{-1} \mid x \in N\}$.

(v) $\forall a \in G$, $aNa^{-1} = N$.

Proof. (i) $\Leftrightarrow$ (iii) $\Rightarrow$ (ii)

(ii) says that $\forall a \in G$,

Theorem 5.1

Let N be a subgroup of a group G. TFAE:

(i) Left and right congruence modulo N coincide, that is, they define the same equivalence relation on G.

(ii) Every left coset of N in G is a right coset of N in G.

(iii) $aN = Na, \forall a \in G$.

(iv) $\forall a \in G$, $aNa^{-1} \subseteq N$, where $aNa^{-1} = \{axa^{-1} \mid x \in N\}$.

(v) $\forall a \in G$, $aNa^{-1} = N$.

Proof. (i) $\Leftrightarrow$ (iii) $\Rightarrow$ (ii)

(ii) says that $\forall a \in G$, $\exists b \in G$ such that $aN = Nb$.

Theorem 5.1

Let N be a subgroup of a group G. TFAE:

(i) Left and right congruence modulo N coincide, that is, they define the same equivalence relation on G.

(ii) Every left coset of N in G is a right coset of N in G.

(iii) $aN = Na, \forall a \in G$.

(iv) $\forall a \in G$, $aNa^{-1} \subseteq N$, where $aNa^{-1} = \{axa^{-1} \mid x \in N\}$.

(v) $\forall a \in G$, $aNa^{-1} = N$.

Proof. (i) $\Leftrightarrow$ (iii) $\Rightarrow$ (ii)

(ii) says that $\forall a \in G$, $\exists b \in G$ such that $aN = Nb$. But $a \in Nb \cap Na$

Theorem 5.1

Let N be a subgroup of a group G. TFAE:

(i) Left and right congruence modulo N coincide, that is, they define the same equivalence relation on G.

(ii) Every left coset of N in G is a right coset of N in G.

(iii) $aN = Na, \forall a \in G$.

(iv) $\forall a \in G$, $aNa^{-1} \subseteq N$, where $aNa^{-1} = \{axa^{-1} \mid x \in N\}$.

(v) $\forall a \in G$, $aNa^{-1} = N$.

Proof. (i) $\Leftrightarrow$ (iii) $\Rightarrow$ (ii)

(ii) says that $\forall a \in G$, $\exists b \in G$ such that $aN = Nb$. But

$a \in Nb \cap Na \implies Nb = Na$

Theorem 5.1

Let N be a subgroup of a group G. TFAE:

(i) Left and right congruence modulo N coincide, that is, they define the same equivalence relation on G.

(ii) Every left coset of N in G is a right coset of N in G.

(iii) $aN = Na, \forall a \in G$.

(iv) $\forall a \in G$, $aNa^{-1} \subseteq N$, where $aNa^{-1} = \{axa^{-1} \mid x \in N\}$.

(v) $\forall a \in G$, $aNa^{-1} = N$.

Proof. (i) $\Leftrightarrow$ (iii) $\Rightarrow$ (ii)

(ii) says that $\forall a \in G$, $\exists b \in G$ such that $aN = Nb$. But

$a \in Nb \cap Na \implies Nb = Na \implies aN = Na$.

Theorem 5.1

Let N be a subgroup of a group G. TFAE:

(i) Left and right congruence modulo N coincide, that is, they define the same equivalence relation on G.

(ii) Every left coset of N in G is a right coset of N in G.

(iii) $aN = Na, \forall a \in G$.

(iv) $\forall a \in G$, $aNa^{-1} \subseteq N$, where $aNa^{-1} = \{axa^{-1} \mid x \in N\}$.

(v) $\forall a \in G$, $aNa^{-1} = N$.

Proof. (i) $\Leftrightarrow$ (iii) $\Rightarrow$ (ii)

(ii) says that $\forall a \in G$, $\exists b \in G$ such that $aN = Nb$. But

$a \in Nb \cap Na \implies Nb = Na \implies aN = Na$.

Thus we have (ii) $\Rightarrow$ (iii).

Theorem 5.1

Let N be a subgroup of a group G. TFAE:

(i) Left and right congruence modulo N coincide, that is, they define the same equivalence relation on G.

(ii) Every left coset of N in G is a right coset of N in G.

(iii) $aN = Na, \forall a \in G$.

(iv) $\forall a \in G$, $aNa^{-1} \subseteq N$, where $aNa^{-1} = \{axa^{-1} \mid x \in N\}$.

(v) $\forall a \in G$, $aNa^{-1} = N$.

Proof. (i) $\Leftrightarrow$ (iii) $\Rightarrow$ (ii) $\Rightarrow$ (iii)

(ii) says that $\forall a \in G$, $\exists b \in G$ such that $aN = Nb$. But

$a \in Nb \cap Na \implies Nb = Na \implies aN = Na$.

Thus we have (ii) $\Rightarrow$ (iii).

Theorem 5.1

Let N be a subgroup of a group G. TFAE:

(i) Left and right congruence modulo N coincide, that is, they define the same equivalence relation on G.

(ii) Every left coset of N in G is a right coset of N in G.

(iii) $aN = Na, \forall a \in G$.

(iv) $\forall a \in G$, $aNa^{-1} \subseteq N$, where $aNa^{-1} = \{axa^{-1} \mid x \in N\}$.

(v) $\forall a \in G$, $aNa^{-1} = N$.

Proof. (i) $\Leftrightarrow$ (iii) $\Rightarrow$ (ii) $\Rightarrow$ (iii)

So far, we have (i) $\Leftrightarrow$ (iii) $\Leftrightarrow$ (ii).

Theorem 5.1

Let N be a subgroup of a group G. TFAE:

(i) Left and right congruence modulo N coincide, that is, they define the same equivalence relation on G.

(ii) Every left coset of N in G is a right coset of N in G.

(iii) $aN = Na, \forall a \in G$.

(iv) $\forall a \in G$, $aNa^{-1} \subseteq N$, where $aNa^{-1} = \{axa^{-1} \mid x \in N\}$.

(v) $\forall a \in G$, $aNa^{-1} = N$.

Proof. (i) $\Leftrightarrow$ (iii) $\Rightarrow$ (ii) $\Rightarrow$ (iii)

So far, we have (i) $\Leftrightarrow$ (iii) $\Leftrightarrow$ (ii). Moreover, (iii) $\Leftrightarrow$ (v) $\Rightarrow$ (iv) is clear.

Theorem 5.1

Let N be a subgroup of a group G. TFAE:

(i) Left and right congruence modulo N coincide, that is, they define the same equivalence relation on G.

(ii) Every left coset of N in G is a right coset of N in G.

(iii) $aN = Na, \forall a \in G$.

(iv) $\forall a \in G, aNa^{-1} \subseteq N$, where $aNa^{-1} = \{axa^{-1} \mid x \in N\}$.

(v) $\forall a \in G, aNa^{-1} = N$.

Proof. (i) $\Leftrightarrow$ (iii) $\Rightarrow$ (ii) $\Rightarrow$ (iii) $\Leftrightarrow$ (v) $\Rightarrow$ (iv)

So far, we have (i) $\Leftrightarrow$ (iii) $\Leftrightarrow$ (ii). Moreover, (iii) $\Leftrightarrow$ (v) $\Rightarrow$ (iv) is clear.

Theorem 5.1

Let N be a subgroup of a group G. TFAE:

(i) Left and right congruence modulo N coincide, that is, they define the same equivalence relation on G.

(ii) Every left coset of N in G is a right coset of N in G.

(iii) $aN = Na, \forall a \in G$.

(iv) $\forall a \in G, aNa^{-1} \subseteq N$, where $aNa^{-1} = \{axa^{-1} \mid x \in N\}$.

(v) $\forall a \in G, aNa^{-1} = N$.

Proof. (i) $\Leftrightarrow$ (iii) $\Rightarrow$ (ii) $\Rightarrow$ (iii) $\Leftrightarrow$ (v) $\Rightarrow$ (iv)

So far, we have (i) $\Leftrightarrow$ (iii) $\Leftrightarrow$ (ii). Moreover, (iii) $\Leftrightarrow$ (v) $\Rightarrow$ (iv) is clear. Hence it remains to show (iv) $\Rightarrow$ (v).

Theorem 5.1

Let N be a subgroup of a group G. TFAE:

(i) Left and right congruence modulo N coincide, that is, they define the same equivalence relation on G.

(ii) Every left coset of N in G is a right coset of N in G.

(iii) $aN = Na, \forall a \in G$.

(iv) $\forall a \in G, aNa^{-1} \subseteq N$, where $aNa^{-1} = \{axa^{-1} \mid x \in N\}$.

(v) $\forall a \in G, aNa^{-1} = N$.

Proof. (i) $\Leftrightarrow$ (iii) $\Rightarrow$ (ii) $\Rightarrow$ (iii) $\Leftrightarrow$ (v) $\Rightarrow$ (iv)

(iv) $\Rightarrow$ (v) :

Theorem 5.1

Let N be a subgroup of a group G. TFAE:

(i) Left and right congruence modulo N coincide, that is, they define the same equivalence relation on G.

(ii) Every left coset of N in G is a right coset of N in G.

(iii) $aN = Na, \forall a \in G$.

(iv) $\forall a \in G, aNa^{-1} \subseteq N$, where $aNa^{-1} = \{axa^{-1} \mid x \in N\}$.

(v) $\forall a \in G, aNa^{-1} = N$.

Proof. (i) $\Leftrightarrow$ (iii) $\Rightarrow$ (ii) $\Rightarrow$ (iii) $\Leftrightarrow$ (v) $\Rightarrow$ (iv)

(iv) $\Rightarrow$ (v) : $a, a^{-1} \in G$

Theorem 5.1

Let N be a subgroup of a group G. TFAE:

(i) Left and right congruence modulo N coincide, that is, they define the same equivalence relation on G.

(ii) Every left coset of N in G is a right coset of N in G.

(iii) $aN = Na, \forall a \in G$.

(iv) $\forall a \in G$, $aNa^{-1} \subseteq N$, where $aNa^{-1} = \{axa^{-1} \mid x \in N\}$.

(v) $\forall a \in G$, $aNa^{-1} = N$.

Proof. (i) $\Leftrightarrow$ (iii) $\Rightarrow$ (ii) $\Rightarrow$ (iii) $\Leftrightarrow$ (v) $\Rightarrow$ (iv)

(iv) $\Rightarrow$ (v) : $a, a^{-1} \in G \Rightarrow aNa^{-1} \subseteq N$ and $a^{-1}Na \subseteq N$

Theorem 5.1

Let N be a subgroup of a group G. TFAE:

(i) Left and right congruence modulo N coincide, that is, they define the same equivalence relation on G.

(ii) Every left coset of N in G is a right coset of N in G.

(iii) $aN = Na, \forall a \in G$.

(iv) $\forall a \in G, aNa^{-1} \subseteq N$, where $aNa^{-1} = \{axa^{-1} \mid x \in N\}$.

(v) $\forall a \in G, aNa^{-1} = N$.

Proof. (i) $\Leftrightarrow$ (iii) $\Rightarrow$ (ii) $\Rightarrow$ (iii) $\Leftrightarrow$ (v) $\Rightarrow$ (iv)

(iv) $\Rightarrow$ (v) : $a, a^{-1} \in G \Rightarrow aNa^{-1} \subseteq N$ and $a^{-1}Na \subseteq N$

$\Rightarrow aNa^{-1} \subseteq N$ and $N \subseteq aNa^{-1}$

Theorem 5.1

Let N be a subgroup of a group G. TFAE:

(i) Left and right congruence modulo N coincide, that is, they define the same equivalence relation on G.

(ii) Every left coset of N in G is a right coset of N in G.

(iii) $aN = Na, \forall a \in G$.

(iv) $\forall a \in G, aNa^{-1} \subseteq N$, where $aNa^{-1} = \{axa^{-1} \mid x \in N\}$.

(v) $\forall a \in G, aNa^{-1} = N$.

Proof. (i) $\Leftrightarrow$ (iii) $\Rightarrow$ (ii) $\Rightarrow$ (iii) $\Leftrightarrow$ (v) $\Rightarrow$ (iv)

(iv) $\Rightarrow$ (v) : $a, a^{-1} \in G \Rightarrow aNa^{-1} \subseteq N$ and $a^{-1}Na \subseteq N$

$\Rightarrow aNa^{-1} \subseteq N$ and $N \subseteq aNa^{-1}$

$\Rightarrow aNa^{-1} = N$

Theorem 5.1

Let N be a subgroup of a group G. TFAE:

(i) Left and right congruence modulo N coincide, that is, they define the same equivalence relation on G.

(ii) Every left coset of N in G is a right coset of N in G.

(iii) $aN = Na, \forall a \in G$.

(iv) $\forall a \in G, aNa^{-1} \subseteq N$, where $aNa^{-1} = \{axa^{-1} \mid x \in N\}$.

(v) $\forall a \in G, aNa^{-1} = N$.

Proof. (i) $\Leftrightarrow$ (iii) $\Rightarrow$ (ii) $\Rightarrow$ (iii) $\Leftrightarrow$ (v) $\Rightarrow$ (iv) $\Rightarrow$ (v)

(iv) $\Rightarrow$ (v) : $a, a^{-1} \in G$ $\Rightarrow$ $aNa^{-1} \subseteq N$ and $a^{-1}Na \subseteq N$

$\Rightarrow$ $aNa^{-1} \subseteq N$ and $N \subseteq aNa^{-1}$

$\Rightarrow$ $aNa^{-1} = N$

Theorem 5.1

Let N be a subgroup of a group G. TFAE:

(i) Left and right congruence modulo N coincide, that is, they define the same equivalence relation on G.

(ii) Every left coset of N in G is a right coset of N in G.

(iii) $aN = Na, \forall a \in G$.

(iv) $\forall a \in G$, $aNa^{-1} \subseteq N$, where $aNa^{-1} = \{axa^{-1} \mid x \in N\}$.

(v) $\forall a \in G$, $aNa^{-1} = N$.

Definition (5.2)**.** A subgroup N of a group G satisfying the equivalence conditions in Theorem 5.1

Theorem 5.1

Let N be a subgroup of a group G. TFAE:

(i) Left and right congruence modulo N coincide, that is, they define the same equivalence relation on G.

(ii) Every left coset of N in G is a right coset of N in G.

(iii) $aN = Na, \forall a \in G$.

(iv) $\forall a \in G, aNa^{-1} \subseteq N$, where $aNa^{-1} = \{axa^{-1} \mid x \in N\}$.

(v) $\forall a \in G, aNa^{-1} = N$.

Definition (5.2)**.** A subgroup N of a group G satisfying the equivalence conditions in Theorem 5.1 is said to be normal in G

Theorem 5.1

Let N be a subgroup of a group G. TFAE:

(i) Left and right congruence modulo N coincide, that is, they define the same equivalence relation on G.

(ii) Every left coset of N in G is a right coset of N in G.

(iii) $aN = Na, \forall a \in G$.

(iv) $\forall a \in G, aNa^{-1} \subseteq N$, where $aNa^{-1} = \{axa^{-1} \mid x \in N\}$.

(v) $\forall a \in G, aNa^{-1} = N$.

Definition (5.2)**.** A subgroup N of a group G satisfying the equivalence conditions in Theorem 5.1 is said to be normal in G or a normal subgroup of G,

Theorem 5.1

Let N be a subgroup of a group G. TFAE:

(i) Left and right congruence modulo N coincide, that is, they define the same equivalence relation on G.

(ii) Every left coset of N in G is a right coset of N in G.

(iii) $aN = Na, \forall a \in G$.

(iv) $\forall a \in G, aNa^{-1} \subseteq N$, where $aNa^{-1} = \{axa^{-1} \mid x \in N\}$.

(v) $\forall a \in G, aNa^{-1} = N$.

Definition (5.2)**.** A subgroup N of a group G satisfying the equivalence conditions in Theorem 5.1 is said to be normal in G or a normal subgroup of G, denoted $N \lhd G$.

Remark

If $N \leq H \leq G$ and if $N \lhd G$,

Remark

If $N \leq H \leq G$ and if $N \lhd G$, then $N \lhd H$.

Remark

If $N \leq H \leq G$ and if $N \lhd G$, then $N \lhd H$.

Proof. $\forall h \in H$ and $\forall n \in N$,

Remark

If $N \leq H \leq G$ and if $N \lhd G$, then $N \lhd H$.

Proof. $\forall h \in H$ and $\forall n \in N$, because $h \in G$ and $N \lhd G$,

Remark

If $N \leq H \leq G$ and if $N \lhd G$, then $N \lhd H$.

Proof. $\forall h \in H$ and $\forall n \in N$, because $h \in G$ and $N \lhd G$, $hnh^{-1} \in N$.

Remark

If $N \leq H \leq G$ and if $N \lhd G$, then $N \lhd H$.

WARNING: $N \lhd H$ and $H \lhd G$

Remark

If $N \leq H \leq G$ and if $N \lhd G$, then $N \lhd H$.

WARNING: $N \lhd H$ and $H \lhd G$ do NOT imply $N \lhd G$.

Remark

If $N \leq H \leq G$ and if $N \lhd G$, then $N \lhd H$.

WARNING: $N \lhd H$ and $H \lhd G$ do NOT imply $N \lhd G$.

Can you give me an example?

Remark

If $N \leq H \leq G$ and if $N \lhd G$, then $N \lhd H$.

WARNING: $N \lhd H$ and $H \lhd G$ do NOT imply $N \lhd G$.

Can you give me an example?

Example. In the group S_4, we have

Remark

If $N \leq H \leq G$ and if $N \lhd G$, then $N \lhd H$.

WARNING: $N \lhd H$ and $H \lhd G$ do NOT imply $N \lhd G$.

Can you give me an example?

Example. In the group S_4, we have

$$\{e, (1,2)(3,4)\} \lhd \{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$$

Remark

If $N \leq H \leq G$ and if $N \lhd G$, then $N \lhd H$.

WARNING: $N \lhd H$ and $H \lhd G$ do NOT imply $N \lhd G$.

Can you give me an example?

Example. In the group S_4, we have

$$\{e, (1,2)(3,4)\} \lhd \{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$$

and $\{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\} \lhd S_4$

Remark

If $N \leq H \leq G$ and if $N \lhd G$, then $N \lhd H$.

WARNING: $N \lhd H$ and $H \lhd G$ do NOT imply $N \lhd G$.

Can you give me an example?

Example. In the group S_4, we have

$$\{e, (1,2)(3,4)\} \lhd \{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$$

and $\{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\} \lhd S_4$

but $\{e, (1,2)(3,4)\}$ is not a normal subgroup of S_4.

Theorem (5.3)

Let K and N be subgroups of a group G with $N \lhd G$. Then

Theorem (5.3)

Let K and N be subgroups of a group G with $N \lhd G$. Then

(i) $(N \cap K) \lhd K$;

Theorem (5.3)

Let K and N be subgroups of a group G with $N \lhd G$. Then

(i) $(N \cap K) \lhd K$;

Proof. For each $k \in K$,

Theorem (5.3)

Let K and N be subgroups of a group G with $N \lhd G$. Then

(i) $(N \cap K) \lhd K$;

Proof. For each $k \in K$,

$k(N \cap K)$

Theorem (5.3)

Let K and N be subgroups of a group G with $N \lhd G$. Then

(i) $(N \cap K) \lhd K$;

Proof. For each $k \in K$,

$k(N \cap K) = kN \cap kK$

Theorem (5.3)

Let K and N be subgroups of a group G with $N \lhd G$. Then

(i) $(N \cap K) \lhd K$;

Proof. For each $k \in K$,

$$k(N \cap K) = kN \cap kK = Nk \cap Kk$$

because $N \lhd G$

Theorem (5.3)

Let K and N be subgroups of a group G with $N \lhd G$. Then

(i) $(N \cap K) \lhd K$;

Proof. For each $k \in K$,

$k(N \cap K) = kN \cap kK = Nk \cap Kk$

because $kK = K = Kk$

Theorem (5.3)

Let K and N be subgroups of a group G with $N \lhd G$. Then

(i) $(N \cap K) \lhd K$;

Proof. For each $k \in K$,
$k(N \cap K) = kN \cap kK = Nk \cap Kk = (N \cap K)k.$

Theorem (5.3)

Let K and N be subgroups of a group G with $N \lhd G$. Then

(i) $(N \cap K) \lhd K$;

(ii) $N \lhd (N \vee K)$;

Theorem (5.3)

Let K and N be subgroups of a group G with $N \lhd G$. Then

(i) $(N \cap K) \lhd K$;

(ii) $N \lhd (N \vee K)$;

Proof. This is clear since $N \vee K = \langle N \cup K \rangle \leq G$.

Theorem (5.3)

Let K and N be subgroups of a group G with $N \lhd G$. Then

(i) $(N \cap K) \lhd K$;

(ii) $N \lhd (N \vee K)$;

(iii) $NK = N \vee K = KN$;

Theorem (5.3)

Let K and N be subgroups of a group G with $N \lhd G$. Then

(i) $(N \cap K) \lhd K$;

(ii) $N \lhd (N \vee K)$;

(iii) $NK = N \vee K = KN$;

Proof. Since KN and NK are both subsets of $N \vee K = \langle N \cup K \rangle$,

Theorem (5.3)

Let K and N be subgroups of a group G with $N \lhd G$. Then

(i) $(N \cap K) \lhd K$;

(ii) $N \lhd (N \vee K)$;

(iii) $NK = N \vee K = KN$;

Proof. Since KN and NK are both subsets of $N \vee K = \langle N \cup K \rangle$, it suffices to show that NK and KN are subgroups of G.

Theorem (5.3)

Let K and N be subgroups of a group G with $N \lhd G$. Then

(i) $(N \cap K) \lhd K$;

(ii) $N \lhd (N \vee K)$;

(iii) $NK = N \vee K = KN$;

Proof. Since KN and NK are both subsets of $N \vee K = \langle N \cup K \rangle$, it suffices to show that NK and KN are subgroups of G. Note that $N \lhd G$ and $K \subseteq G$.

Theorem (5.3)

Let K and N be subgroups of a group G with $N \lhd G$. Then

(i) $(N \cap K) \lhd K$;

(ii) $N \lhd (N \vee K)$;

(iii) $NK = N \vee K = KN$;

Proof. Since KN and NK are both subsets of $N \vee K = \langle N \cup K \rangle$, it suffices to show that NK and KN are subgroups of G. Note that $N \lhd G$ and $K \subseteq G$. Thus $Nk = kN$, $\forall k \in K$.

Theorem (5.3)

Let K and N be subgroups of a group G with $N \lhd G$. Then

(i) $(N \cap K) \lhd K$;

(ii) $N \lhd (N \vee K)$;

(iii) $NK = N \vee K = KN$;

Proof. Since KN and NK are both subsets of $N \vee K = \langle N \cup K \rangle$, it suffices to show that NK and KN are subgroups of G. Note that $N \lhd G$ and $K \subseteq G$. Thus $Nk = kN$, $\forall k \in K$. Hence, $\forall n \in N$ and $\forall k \in K$,

Theorem (5.3)

Let K and N be subgroups of a group G with $N \lhd G$. Then

(i) $(N \cap K) \lhd K$;

(ii) $N \lhd (N \vee K)$;

(iii) $NK = N \vee K = KN$;

Proof. Since KN and NK are both subsets of $N \vee K = \langle N \cup K \rangle$, it suffices to show that NK and KN are subgroups of G. Note that $N \lhd G$ and $K \subseteq G$. Thus $Nk = kN$, $\forall k \in K$. Hence, $\forall n \in N$ and $\forall k \in K$, $nk \in Nk$

Theorem (5.3)

Let K and N be subgroups of a group G with $N \lhd G$. Then

(i) $(N \cap K) \lhd K$;

(ii) $N \lhd (N \vee K)$;

(iii) $NK = N \vee K = KN$;

Proof. Since KN and NK are both subsets of $N \vee K = \langle N \cup K \rangle$, it suffices to show that NK and KN are subgroups of G. Note that $N \lhd G$ and $K \subseteq G$. Thus $Nk = kN$, $\forall k \in K$. Hence, $\forall n \in N$ and $\forall k \in K$, $nk \in Nk = kN$

Theorem (5.3)

Let K and N be subgroups of a group G with $N \lhd G$. Then

(i) $(N \cap K) \lhd K$;

(ii) $N \lhd (N \vee K)$;

(iii) $NK = N \vee K = KN$;

Proof. Since KN and NK are both subsets of $N \vee K = \langle N \cup K \rangle$, it suffices to show that NK and KN are subgroups of G. Note that $N \lhd G$ and $K \subseteq G$. Thus $Nk = kN$, $\forall k \in K$. Hence, $\forall n \in N$ and $\forall k \in K$, $nk \in Nk = kN$ $\Rightarrow \exists n' \in N$ such that $nk = kn'$.

Theorem (5.3)

Let K and N be subgroups of a group G with $N \lhd G$. Then

(i) $(N \cap K) \lhd K$;

(ii) $N \lhd (N \vee K)$;

(iii) $NK = N \vee K = KN$;

Proof. Since KN and NK are both subsets of $N \vee K = \langle N \cup K \rangle$, it suffices to show that NK and KN are subgroups of G. Note that $N \lhd G$ and $K \subseteq G$. Thus $Nk = kN$, $\forall k \in K$. Hence, $\forall n \in N$ and $\forall k \in K$, $nk \in Nk = kN$ $\Rightarrow \exists n' \in N$ such that $nk = kn'$. Now, it is easy to check that KN is a subgroup of G.

Theorem (5.3)

Let K and N be subgroups of a group G with $N \lhd G$. Then

(i) $(N \cap K) \lhd K$;

(ii) $N \lhd (N \vee K)$;

(iii) $NK = N \vee K = KN$;

Proof. Since KN and NK are both subsets of $N \vee K = \langle N \cup K \rangle$, it suffices to show that NK and KN are subgroups of G. Note that $N \lhd G$ and $K \subseteq G$. Thus $Nk = kN$, $\forall k \in K$. Hence, $\forall n \in N$ and $\forall k \in K$, $nk \in Nk = kN$ $\Rightarrow \exists n' \in N$ such that $nk = kn'$. Now, it is easy to check that KN is a subgroup of G. More precisely,

Theorem (5.3)

Let K and N be subgroups of a group G with $N \lhd G$. Then

(i) $(N \cap K) \lhd K$;

(ii) $N \lhd (N \vee K)$;

(iii) $NK = N \vee K = KN$;

Proof. Since KN and NK are both subsets of $N \vee K = \langle N \cup K \rangle$, it suffices to show that NK and KN are subgroups of G. Note that $N \lhd G$ and $K \subseteq G$. Thus $Nk = kN$, $\forall k \in K$. Hence, $\forall n \in N$ and $\forall k \in K$, $nk \in Nk = kN$ $\Rightarrow \exists n' \in N$ such that $nk = kn'$. Now, it is easy to check that KN is a subgroup of G. More precisely, $(k_1 n_1)(k_2 n_2)^{-1}$

Theorem (5.3)

Let K and N be subgroups of a group G with $N \lhd G$. Then

(i) $(N \cap K) \lhd K$;

(ii) $N \lhd (N \vee K)$;

(iii) $NK = N \vee K = KN$;

Proof. Since KN and NK are both subsets of $N \vee K = \langle N \cup K \rangle$, it suffices to show that NK and KN are subgroups of G. Note that $N \lhd G$ and $K \subseteq G$. Thus $Nk = kN$, $\forall k \in K$. Hence, $\forall n \in N$ and $\forall k \in K$, $nk \in Nk = kN$ $\Rightarrow \exists n' \in N$ such that $nk = kn'$. Now, it is easy to check that KN is a subgroup of G. More precisely, $(k_1 n_1)(k_2 n_2)^{-1}$ $= k_1 n_1 (n_2^{-1} k_2^{-1})$

Theorem (5.3)

Let K and N be subgroups of a group G with $N \lhd G$. Then

(i) $(N \cap K) \lhd K$;

(ii) $N \lhd (N \vee K)$;

(iii) $NK = N \vee K = KN$;

Proof. Since KN and NK are both subsets of $N \vee K = \langle N \cup K \rangle$, it suffices to show that NK and KN are subgroups of G. Note that $N \lhd G$ and $K \subseteq G$. Thus $Nk = kN$, $\forall k \in K$. Hence, $\forall n \in N$ and $\forall k \in K$, $nk \in Nk = kN$ $\Rightarrow \exists n' \in N$ such that $nk = kn'$. Now, it is easy to check that KN is a subgroup of G. More precisely, $(k_1 n_1)(k_2 n_2)^{-1}$ $= k_1 n_1 (n_2^{-1} k_2^{-1}) = k_1 \big((n_1 n_2^{-1}) k_2^{-1}\big)$

Theorem (5.3)

Let K and N be subgroups of a group G with $N \lhd G$. Then

(i) $(N \cap K) \lhd K$;

(ii) $N \lhd (N \vee K)$;

(iii) $NK = N \vee K = KN$;

Proof. Since KN and NK are both subsets of $N \vee K = \langle N \cup K \rangle$, it suffices to show that NK and KN are subgroups of G. Note that $N \lhd G$ and $K \subseteq G$. Thus $Nk = kN$, $\forall k \in K$. Hence, $\forall n \in N$ and $\forall k \in K$, $nk \in Nk = kN$ $\Rightarrow \exists n' \in N$ such that $nk = kn'$. Now, it is easy to check that KN is a subgroup of G. More precisely, $(k_1 n_1)(k_2 n_2)^{-1}$ $= k_1 n_1 (n_2^{-1} k_2^{-1}) = k_1 \big((n_1 n_2^{-1}) k_2^{-1}\big) = k_1 (k_2^{-1} n')$

Theorem (5.3)

Let K and N be subgroups of a group G with $N \lhd G$. Then

(i) $(N \cap K) \lhd K$;

(ii) $N \lhd (N \vee K)$;

(iii) $NK = N \vee K = KN$;

Proof. Since KN and NK are both subsets of $N \vee K = \langle N \cup K \rangle$, it suffices to show that NK and KN are subgroups of G. Note that $N \lhd G$ and $K \subseteq G$. Thus $Nk = kN$, $\forall k \in K$. Hence, $\forall n \in N$ and $\forall k \in K$, $nk \in Nk = kN$ $\Rightarrow \exists n' \in N$ such that $nk = kn'$. Now, it is easy to check that KN is a subgroup of G. More precisely, $(k_1 n_1)(k_2 n_2)^{-1}$ $= k_1 n_1 (n_2^{-1} k_2^{-1}) = k_1 \big((n_1 n_2^{-1}) k_2^{-1}\big) = k_1 (k_2^{-1} n') \in KN$.

Theorem (5.3)

Let K and N be subgroups of a group G with $N \lhd G$. Then

(i) $(N \cap K) \lhd K$;

(ii) $N \lhd (N \vee K)$;

(iii) $NK = N \vee K = KN$;

Proof. Since KN and NK are both subsets of $N \vee K = \langle N \cup K \rangle$, it suffices to show that NK and KN are subgroups of G. Note that $N \lhd G$ and $K \subseteq G$. Thus $Nk = kN$, $\forall k \in K$. Hence, $\forall n \in N$ and $\forall k \in K$, $nk \in Nk = kN$ $\Rightarrow \exists n' \in N$ such that $nk = kn'$. Now, it is easy to check that KN is a subgroup of G. More precisely, $(k_1 n_1)(k_2 n_2)^{-1}$ $= k_1 n_1 (n_2^{-1} k_2^{-1}) = k_1 \big((n_1 n_2^{-1}) k_2^{-1}\big) = k_1 (k_2^{-1} n') \in KN$. Similarly, we can show that NK is a subgroup of G.

Theorem (5.3)

Let K and N be subgroups of a group G with $N \lhd G$. Then

(i) $(N \cap K) \lhd K$;

(ii) $N \lhd (N \vee K)$;

(iii) $NK = N \vee K = KN$;

(iv) if $K \lhd G$ and $K \cap N = \{e\}$,

Theorem (5.3)

Let K and N be subgroups of a group G with $N \lhd G$. Then

(i) $(N \cap K) \lhd K$;

(ii) $N \lhd (N \vee K)$;

(iii) $NK = N \vee K = KN$;

(iv) if $K \lhd G$ and $K \cap N = \{e\}$, then $\forall n \in N$ and $\forall k \in K$,

Theorem (5.3)

Let K and N be subgroups of a group G with $N \lhd G$. Then

(i) $(N \cap K) \lhd K$;

(ii) $N \lhd (N \vee K)$;

(iii) $NK = N \vee K = KN$;

(iv) if $K \lhd G$ and $K \cap N = \{e\}$, then $\forall n \in N$ and $\forall k \in K$, $nk = kn$.

Theorem (5.3)

Let K and N be subgroups of a group G with $N \lhd G$. Then

(i) $(N \cap K) \lhd K$;

(ii) $N \lhd (N \vee K)$;

(iii) $NK = N \vee K = KN$;

(iv) if $K \lhd G$ and $K \cap N = \{e\}$, then $\forall n \in N$ and $\forall k \in K$, $nk = kn$.

Proof. Let $n \in N$ and $k \in K$.

Theorem (5.3)

Let K and N be subgroups of a group G with $N \lhd G$. Then

(i) $(N \cap K) \lhd K$;

(ii) $N \lhd (N \vee K)$;

(iii) $NK = N \vee K = KN$;

(iv) if $K \lhd G$ and $K \cap N = \{e\}$, then $\forall n \in N$ and $\forall k \in K$, $nk = kn$.

Proof. Let $n \in N$ and $k \in K$.

$$nkn^{-1}k^{-1}$$

Theorem (5.3)

Let K and N be subgroups of a group G with $N \lhd G$. Then

(i) $(N \cap K) \lhd K$;

(ii) $N \lhd (N \vee K)$;

(iii) $NK = N \vee K = KN$;

(iv) if $K \lhd G$ and $K \cap N = \{e\}$, then $\forall n \in N$ and $\forall k \in K$, $nk = kn$.

Proof. Let $n \in N$ and $k \in K$.

$$nkn^{-1}k^{-1} = (nkn^{-1})k^{-1}$$

Theorem (5.3)

Let K and N be subgroups of a group G with $N \lhd G$. Then

(i) $(N \cap K) \lhd K$;

(ii) $N \lhd (N \vee K)$;

(iii) $NK = N \vee K = KN$;

(iv) if $K \lhd G$ and $K \cap N = \{e\}$, then $\forall n \in N$ and $\forall k \in K$, $nk = kn$.

Proof. Let $n \in N$ and $k \in K$.

$$nkn^{-1}k^{-1} = (nkn^{-1})k^{-1} \in K \text{ (since } K \lhd G)$$

Theorem (5.3)

Let K and N be subgroups of a group G with $N \lhd G$. Then

(i) $(N \cap K) \lhd K$;

(ii) $N \lhd (N \vee K)$;

(iii) $NK = N \vee K = KN$;

(iv) if $K \lhd G$ and $K \cap N = \{e\}$, then $\forall n \in N$ and $\forall k \in K$, $nk = kn$.

Proof. Let $n \in N$ and $k \in K$.

$$\begin{aligned} nkn^{-1}k^{-1} &= (nkn^{-1})k^{-1} \in K \text{ (since } K \lhd G) \\ &= n(kn^{-1}k^{-1}) \end{aligned}$$

Theorem (5.3)

Let K and N be subgroups of a group G with $N \lhd G$. Then

(i) $(N \cap K) \lhd K$;

(ii) $N \lhd (N \vee K)$;

(iii) $NK = N \vee K = KN$;

(iv) if $K \lhd G$ and $K \cap N = \{e\}$, then $\forall n \in N$ and $\forall k \in K$, $nk = kn$.

Proof. Let $n \in N$ and $k \in K$.

$$\begin{aligned} nkn^{-1}k^{-1} &= (nkn^{-1})k^{-1} \in K \text{ (since } K \lhd G) \\ &= n(kn^{-1}k^{-1}) \in N \text{ (since } N \lhd G) \end{aligned}$$

Theorem (5.3)

Let K and N be subgroups of a group G with $N \lhd G$. Then

(i) $(N \cap K) \lhd K$;

(ii) $N \lhd (N \vee K)$;

(iii) $NK = N \vee K = KN$;

(iv) if $K \lhd G$ and $K \cap N = \{e\}$, then $\forall n \in N$ and $\forall k \in K$, $nk = kn$.

Proof. Let $n \in N$ and $k \in K$.

$$\begin{aligned} nkn^{-1}k^{-1} &= (nkn^{-1})k^{-1} \in K \text{ (since } K \lhd G) \\ &= n(kn^{-1}k^{-1}) \in N \text{ (since } N \lhd G) \\ &\in K \cap N = \{e\} \end{aligned}$$

Theorem (5.3)

Let K and N be subgroups of a group G with $N \lhd G$. Then

(i) $(N \cap K) \lhd K$;

(ii) $N \lhd (N \vee K)$;

(iii) $NK = N \vee K = KN$;

(iv) if $K \lhd G$ and $K \cap N = \{e\}$, then $\forall n \in N$ and $\forall k \in K$, $nk = kn$.

Proof. Let $n \in N$ and $k \in K$.

$$\begin{aligned} nkn^{-1}k^{-1} &= (nkn^{-1})k^{-1} \in K \text{ (since } K \lhd G) \\ &= n(kn^{-1}k^{-1}) \in N \text{ (since } N \lhd G) \\ &\in K \cap N = \{e\} \end{aligned}$$

$$\Longrightarrow \quad nkn^{-1}k^{-1} = e$$

Theorem (5.3)

Let K and N be subgroups of a group G with $N \lhd G$. Then

(i) $(N \cap K) \lhd K$;

(ii) $N \lhd (N \vee K)$;

(iii) $NK = N \vee K = KN$;

(iv) if $K \lhd G$ and $K \cap N = \{e\}$, then $\forall n \in N$ and $\forall k \in K$, $nk = kn$.

Proof. Let $n \in N$ and $k \in K$.

$$\begin{aligned} nkn^{-1}k^{-1} &= (nkn^{-1})k^{-1} \in K \text{ (since } K \lhd G) \\ &= n(kn^{-1}k^{-1}) \in N \text{ (since } N \lhd G) \\ &\in K \cap N = \{e\} \end{aligned}$$

$$\Longrightarrow \quad nkn^{-1}k^{-1} = e \implies nk = kn$$

Theorem (5.4)

Let N be a normal subgroup of a group G

Theorem (5.4)

Let N be a normal subgroup of a group G and let G/N be the set of all (left) cosets of N in G,

Theorem (5.4)

Let N be a normal subgroup of a group G and let G/N be the set of all (left) cosets of N in G, i.e., $G/N = \{aN \mid a \in G\}$.

Theorem (5.4)

Let N be a normal subgroup of a group G and let G/N be the set of all (left) cosets of N in G, i.e., $G/N = \{aN \mid a \in G\}$. Then G/N is a group

Theorem (5.4)

Let N be a normal subgroup of a group G and let G/N be the set of all (left) cosets of N in G, i.e., $G/N = \{aN \mid a \in G\}$. Then G/N is a group of order $[G : N]$

Theorem (5.4)

Let N be a normal subgroup of a group G and let G/N be the set of all (left) cosets of N in G, i.e., $G/N = \{aN \mid a \in G\}$. Then G/N is a group of order $[G : N]$ under the binary operation given by $(aN)(bN) = abN$.

Theorem (5.4)

Let N be a normal subgroup of a group G and let G/N be the set of all (left) cosets of N in G, i.e., $G/N = \{aN \mid a \in G\}$. Then G/N is a group of order $[G : N]$ under the binary operation given by $(aN)(bN) = abN$.

Proof. We first show that the binary operation given by $(aN)(bN) = abN$ is well-defined.

Theorem (5.4)

Let N be a normal subgroup of a group G and let G/N be the set of all (left) cosets of N in G, i.e., $G/N = \{aN \mid a \in G\}$. Then G/N is a group of order $[G : N]$ under the binary operation given by $(aN)(bN) = abN$.

Proof. Suppose $aN = a_1N$ and $bN = b_1N$.

Theorem (5.4)

Let N be a normal subgroup of a group G and let G/N be the set of all (left) cosets of N in G, i.e., $G/N = \{aN \mid a \in G\}$. Then G/N is a group of order $[G : N]$ under the binary operation given by $(aN)(bN) = abN$.

Proof. Suppose $aN = a_1N$ and $bN = b_1N$. Then $a^{-1}a_1 \in N$ and $b^{-1}b_1 \in N$.

Theorem (5.4)

Let N be a normal subgroup of a group G and let G/N be the set of all (left) cosets of N in G, i.e., $G/N = \{aN \mid a \in G\}$. Then G/N is a group of order $[G : N]$ under the binary operation given by $(aN)(bN) = abN$.

Proof. Suppose $aN = a_1N$ and $bN = b_1N$. Then $a^{-1}a_1 \in N$ and $b^{-1}b_1 \in N$. Hence

Theorem (5.4)

Let N be a normal subgroup of a group G and let G/N be the set of all (left) cosets of N in G, i.e., $G/N = \{aN \mid a \in G\}$. Then G/N is a group of order $[G : N]$ under the binary operation given by $(aN)(bN) = abN$.

Proof. Suppose $aN = a_1N$ and $bN = b_1N$. Then $a^{-1}a_1 \in N$ and $b^{-1}b_1 \in N$. Hence
$(ab)^{-1}(a_1b_1)$

Theorem (5.4)

Let N be a normal subgroup of a group G and let G/N be the set of all (left) cosets of N in G, i.e., $G/N = \{aN \mid a \in G\}$. Then G/N is a group of order $[G : N]$ under the binary operation given by $(aN)(bN) = abN$.

Proof. Suppose $aN = a_1N$ and $bN = b_1N$. Then $a^{-1}a_1 \in N$ and $b^{-1}b_1 \in N$. Hence
$(ab)^{-1}(a_1b_1) = b^{-1}a^{-1}a_1b_1$

Theorem (5.4)

Let N be a normal subgroup of a group G and let G/N be the set of all (left) cosets of N in G, i.e., $G/N = \{aN \mid a \in G\}$. Then G/N is a group of order $[G : N]$ under the binary operation given by $(aN)(bN) = abN$.

Proof. Suppose $aN = a_1N$ and $bN = b_1N$. Then $a^{-1}a_1 \in N$ and $b^{-1}b_1 \in N$. Hence

$$(ab)^{-1}(a_1b_1) = b^{-1}a^{-1}a_1b_1 = \left[b^{-1}(a^{-1}a_1)b\right](b^{-1}b_1)$$

Theorem (5.4)

Let N be a normal subgroup of a group G and let G/N be the set of all (left) cosets of N in G, i.e., $G/N = \{aN \mid a \in G\}$. Then G/N is a group of order $[G : N]$ under the binary operation given by $(aN)(bN) = abN$.

Proof. Suppose $aN = a_1N$ and $bN = b_1N$. Then $a^{-1}a_1 \in N$ and $b^{-1}b_1 \in N$. Hence

$$(ab)^{-1}(a_1b_1) = b^{-1}a^{-1}a_1b_1 = \left[b^{-1}(a^{-1}a_1)b\right](b^{-1}b_1)$$

because $a^{-1}a_1 \in N$

Theorem (5.4)

Let N be a normal subgroup of a group G and let G/N be the set of all (left) cosets of N in G, i.e., $G/N = \{aN \mid a \in G\}$. Then G/N is a group of order $[G : N]$ under the binary operation given by $(aN)(bN) = abN$.

Proof. Suppose $aN = a_1N$ and $bN = b_1N$. Then $a^{-1}a_1 \in N$ and $b^{-1}b_1 \in N$. Hence

$$(ab)^{-1}(a_1b_1) = b^{-1}a^{-1}a_1b_1 = \left[b^{-1}(a^{-1}a_1)b\right](b^{-1}b_1)$$

because $a^{-1}a_1 \in N$ and $N \lhd G$,

Theorem (5.4)

Let N be a normal subgroup of a group G and let G/N be the set of all (left) cosets of N in G, i.e., $G/N = \{aN \mid a \in G\}$. Then G/N is a group of order $[G : N]$ under the binary operation given by $(aN)(bN) = abN$.

Proof. Suppose $aN = a_1N$ and $bN = b_1N$. Then $a^{-1}a_1 \in N$ and $b^{-1}b_1 \in N$. Hence

$$(ab)^{-1}(a_1b_1) = b^{-1}a^{-1}a_1b_1 = \left[b^{-1}(a^{-1}a_1)b\right](b^{-1}b_1)$$

because $a^{-1}a_1 \in N$ and $N \lhd G$, $b^{-1}(a^{-1}a_1)b \in N$;

Theorem (5.4)

Let N be a normal subgroup of a group G and let G/N be the set of all (left) cosets of N in G, i.e., $G/N = \{aN \mid a \in G\}$. Then G/N is a group of order $[G : N]$ under the binary operation given by $(aN)(bN) = abN$.

Proof. Suppose $aN = a_1N$ and $bN = b_1N$. Then $a^{-1}a_1 \in N$ and $b^{-1}b_1 \in N$. Hence

$$(ab)^{-1}(a_1b_1) = b^{-1}a^{-1}a_1b_1 = \left[b^{-1}(a^{-1}a_1)b\right](b^{-1}b_1)$$

because $a^{-1}a_1 \in N$ and $N \lhd G$, $b^{-1}(a^{-1}a_1)b \in N$;

also, $b^{-1}b_1 \in N$.

Theorem (5.4)

Let N be a normal subgroup of a group G and let G/N be the set of all (left) cosets of N in G, i.e., $G/N = \{aN \mid a \in G\}$. Then G/N is a group of order $[G : N]$ under the binary operation given by $(aN)(bN) = abN$.

Proof. Suppose $aN = a_1N$ and $bN = b_1N$. Then $a^{-1}a_1 \in N$ and $b^{-1}b_1 \in N$. Hence

$$(ab)^{-1}(a_1b_1) = b^{-1}a^{-1}a_1b_1 = \left[b^{-1}(a^{-1}a_1)b\right](b^{-1}b_1) \in N$$

because $a^{-1}a_1 \in N$ and $N \lhd G$, $b^{-1}(a^{-1}a_1)b \in N$;

also, $b^{-1}b_1 \in N$.

Theorem (5.4)

Let N be a normal subgroup of a group G and let G/N be the set of all (left) cosets of N in G, i.e., $G/N = \{aN \mid a \in G\}$. Then G/N is a group of order $[G : N]$ under the binary operation given by $(aN)(bN) = abN$.

Proof. Suppose $aN = a_1N$ and $bN = b_1N$. Then $a^{-1}a_1 \in N$ and $b^{-1}b_1 \in N$. Hence
$(ab)^{-1}(a_1b_1) = b^{-1}a^{-1}a_1b_1 = \left[b^{-1}(a^{-1}a_1)b\right](b^{-1}b_1) \in N$ and this implies $abN = a_1b_1N$.

Theorem (5.4)

Let N be a normal subgroup of a group G and let G/N be the set of all (left) cosets of N in G, i.e., $G/N = \{aN \mid a \in G\}$. Then G/N is a group of order $[G : N]$ under the binary operation given by $(aN)(bN) = abN$.

Proof. Suppose $aN = a_1N$ and $bN = b_1N$. Then $a^{-1}a_1 \in N$ and $b^{-1}b_1 \in N$. Hence $(ab)^{-1}(a_1b_1) = b^{-1}a^{-1}a_1b_1 = \left[b^{-1}(a^{-1}a_1)b\right](b^{-1}b_1) \in N$ and this implies $abN = a_1b_1N$. Hence this binary operation is well-defined.

Theorem (5.4)

Let N be a normal subgroup of a group G and let G/N be the set of all (left) cosets of N in G, i.e., $G/N = \{aN \mid a \in G\}$. Then G/N is a group of order $[G : N]$ under the binary operation given by $(aN)(bN) = abN$.

Proof. Suppose $aN = a_1N$ and $bN = b_1N$. Then $a^{-1}a_1 \in N$ and $b^{-1}b_1 \in N$. Hence $(ab)^{-1}(a_1b_1) = b^{-1}a^{-1}a_1b_1 = \left[b^{-1}(a^{-1}a_1)b\right](b^{-1}b_1) \in N$ and this implies $abN = a_1b_1N$. Hence this binary operation is well-defined. It is easy to check that this binary operation is associative.

Theorem (5.4)

Let N be a normal subgroup of a group G and let G/N be the set of all (left) cosets of N in G, i.e., $G/N = \{aN \mid a \in G\}$. Then G/N is a group of order $[G : N]$ under the binary operation given by $(aN)(bN) = abN$.

Proof. Suppose $aN = a_1N$ and $bN = b_1N$. Then $a^{-1}a_1 \in N$ and $b^{-1}b_1 \in N$. Hence $(ab)^{-1}(a_1b_1) = b^{-1}a^{-1}a_1b_1 = \left[b^{-1}(a^{-1}a_1)b\right](b^{-1}b_1) \in N$ and this implies $abN = a_1b_1N$. Hence this binary operation is well-defined. It is easy to check that this binary operation is associative. Moreover, $eN = N$ is the identity

Theorem (5.4)

Let N be a normal subgroup of a group G and let G/N be the set of all (left) cosets of N in G, i.e., $G/N = \{aN \mid a \in G\}$. Then G/N is a group of order $[G : N]$ under the binary operation given by $(aN)(bN) = abN$.

Proof. Suppose $aN = a_1N$ and $bN = b_1N$. Then $a^{-1}a_1 \in N$ and $b^{-1}b_1 \in N$. Hence $(ab)^{-1}(a_1b_1) = b^{-1}a^{-1}a_1b_1 = \left[b^{-1}(a^{-1}a_1)b\right](b^{-1}b_1) \in N$ and this implies $abN = a_1b_1N$. Hence this binary operation is well-defined. It is easy to check that this binary operation is associative. Moreover, $eN = N$ is the identity and $(aN)^{-1} = a^{-1}N$ for all $aN \in G/N$.

Theorem (5.4)

Let N be a normal subgroup of a group G and let G/N be the set of all (left) cosets of N in G, i.e., $G/N = \{aN \mid a \in G\}$. Then G/N is a group of order $[G : N]$ under the binary operation given by $(aN)(bN) = abN$.

Proof. Suppose $aN = a_1N$ and $bN = b_1N$. Then $a^{-1}a_1 \in N$ and $b^{-1}b_1 \in N$. Hence $(ab)^{-1}(a_1b_1) = b^{-1}a^{-1}a_1b_1 = \left[b^{-1}(a^{-1}a_1)b\right](b^{-1}b_1) \in N$ and this implies $abN = a_1b_1N$. Hence this binary operation is well-defined. It is easy to check that this binary operation is associative. Moreover, $eN = N$ is the identity and $(aN)^{-1} = a^{-1}N$ for all $aN \in G/N$. Therefore, G/N is a group under the defined binary operation.

Theorem (5.4)

Let N be a normal subgroup of a group G and let G/N be the set of all (left) cosets of N in G, i.e., $G/N = \{aN \mid a \in G\}$. Then G/N is a group of order $[G : N]$ under the binary operation given by $(aN)(bN) = abN$.

Proof. Suppose $aN = a_1N$ and $bN = b_1N$. Then $a^{-1}a_1 \in N$ and $b^{-1}b_1 \in N$. Hence $(ab)^{-1}(a_1b_1) = b^{-1}a^{-1}a_1b_1 = \left[b^{-1}(a^{-1}a_1)b\right](b^{-1}b_1) \in N$ and this implies $abN = a_1b_1N$. Hence this binary operation is well-defined. It is easy to check that this binary operation is associative. Moreover, $eN = N$ is the identity and $(aN)^{-1} = a^{-1}N$ for all $aN \in G/N$. Therefore, G/N is a group under the defined binary operation. Since $|G/N| = [G : N]$, we finish the proof.

Theorem (5.4)

Let N be a normal subgroup of a group G and let G/N be the set of all (left) cosets of N in G, i.e., $G/N = \{aN \mid a \in G\}$. Then G/N is a group of order $[G : N]$ under the binary operation given by $(aN)(bN) = abN$.

This group G/N

Theorem (5.4)

Let N be a normal subgroup of a group G and let G/N be the set of all (left) cosets of N in G, i.e., $G/N = \{aN \mid a \in G\}$. Then G/N is a group of order $[G : N]$ under the binary operation given by $(aN)(bN) = abN$.

This group G/N is called the quotient group

Theorem (5.4)

Let N be a normal subgroup of a group G and let G/N be the set of all (left) cosets of N in G, i.e., $G/N = \{aN \mid a \in G\}$. Then G/N is a group of order $[G : N]$ under the binary operation given by $(aN)(bN) = abN$.

This group G/N is called the quotient group or factor group of G by N.

Theorem (5.4)

Let N be a normal subgroup of a group G and let G/N be the set of all (left) cosets of N in G, i.e., $G/N = \{aN \mid a \in G\}$. Then G/N is a group of order $[G : N]$ under the binary operation given by $(aN)(bN) = abN$.

This group G/N is called the quotient group or factor group of G by N.

Example. $\mathbb{Z}_m = \mathbb{Z}/\langle m \rangle$.