MTHSC 412 Section 7.5 – Congruence and Lagrange's Theorem

Kevin James

Definition

Suppose that G is a group and that $K \leq G$. For $a, b \in G$, we say that a and b are congruent modulo K if $ab^{-1} \in K$. In this case, we write $a \equiv b \pmod{K}$.

Definition

Suppose that G is a group and that $K \leq G$. For $a, b \in G$, we say that a and b are <u>congruent modulo K</u> if $ab^{-1} \in K$. In this case, we write $a \equiv b \pmod{K}$.

Example

Let $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ be the quaternian group and let $K = \{\pm 1, \pm j\}$.

Definition

Suppose that G is a group and that $K \leq G$. For $a, b \in G$, we say that a and b are <u>congruent modulo K</u> if $ab^{-1} \in K$. In this case, we write $a \equiv b \pmod{K}$.

Example

Let $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ be the quaternian group and let $K = \{\pm 1, \pm j\}$.
Then $[1] = \{\pm 1, \pm j\}$.

Definition

Suppose that G is a group and that $K \leq G$. For $a, b \in G$, we say that a and b are congruent modulo K if $ab^{-1} \in K$. In this case, we write $a \equiv b \pmod{K}$.

Example

Let $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ be the quaternian group and let $K = \{\pm 1, \pm j\}$.
Then $[1] = \{\pm 1, \pm j\}$.
$[k] = \{\pm k, \pm i\}$.

Definition

Suppose that G is a group and that $K \leq G$. For $a, b \in G$, we say that a and b are congruent modulo K if $ab^{-1} \in K$. In this case, we write $a \equiv b \pmod{K}$.

Example

Let $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ be the quaternian group and let $K = \{\pm 1, \pm j\}$.
Then $[1] = \{\pm 1, \pm j\}$.
$[k] = \{\pm k, \pm i\}$.

Theorem

Suppose that $K \leq G$. Then the relation $\equiv \pmod{K}$ is an equivalence relation on G.

Note

If $K \leq G$ then the congruence class of $a \in G$ is

Note

If $K \leq G$ then the congruence class of $a \in G$ is
$[a] = \{b \in G \mid ba^{-1} = k \in K\} =$

Note

If $K \leq G$ then the congruence class of $a \in G$ is
$[a] = \{b \in G \mid ba^{-1} = k \in K\} = \{b \in G \mid b = ka\} =$

Note

If $K \leq G$ then the congruence class of $a \in G$ is $[a] = \{b \in G \mid ba^{-1} = k \in K\} = \{b \in G \mid b = ka\} = \{ka \mid k \in K\} =$

Note

If $K \leq G$ then the congruence class of $a \in G$ is $[a] = \{b \in G \mid ba^{-1} = k \in K\} = \{b \in G \mid b = ka\} = \{ka \mid k \in K\} = Ka.$

Note

If $K \leq G$ then the congruence class of $a \in G$ is $[a] = \{b \in G \mid ba^{-1} = k \in K\} = \{b \in G \mid b = ka\} = \{ka \mid k \in K\} = Ka$.

Definition

The set $Ka = \{ka \mid k \in K\}$ is called a right coset of K in G.

Note

If $K \leq G$ then the congruence class of $a \in G$ is $[a] = \{b \in G \mid ba^{-1} = k \in K\} = \{b \in G \mid b = ka\} = \{ka \mid k \in K\} = Ka$.

Definition

The set $Ka = \{ka \mid k \in K\}$ is called a right coset of K in G.

Theorem

Suppose that $K \leq G$ and that $a, c \in G$. Then $a \equiv c \pmod{K}$ if and only if $Ka = Kc$.

Note

If $K \leq G$ then the congruence class of $a \in G$ is $[a] = \{b \in G \mid ba^{-1} = k \in K\} = \{b \in G \mid b = ka\} = \{ka \mid k \in K\} = Ka$.

Definition

The set $Ka = \{ka \mid k \in K\}$ is called a right coset of K in G.

Theorem

Suppose that $K \leq G$ and that $a, c \in G$. Then $a \equiv c \pmod{K}$ if and only if $Ka = Kc$.

Corollary

Let $K \leq G$. Then two right cosets of K are either disjoint or identical.

Theorem

Let $K \leq G$. Then,

1. $G = \cup_{a \in G} Ka.$

Theorem

Let $K \leq G$. Then,

1. $G = \cup_{a \in G} Ka$.
2. *The map $f : K \to Ka$ defined by $f(x) = xa$ is a bijection.*

Theorem

Let $K \leq G$. Then,

1. $G = \cup_{a \in G} Ka$.
2. *The map $f : K \to Ka$ defined by $f(x) = xa$ is a bijection. Thus, if K is finite of size m, then each coset of K has size m also.*

Theorem

Let $K \leq G$. Then,

1. $G = \cup_{a \in G} Ka$.
2. *The map $f : K \to Ka$ defined by $f(x) = xa$ is a bijection. Thus, if K is finite of size m, then each coset of K has size m also.*

Definition

If $H \leq G$ then the number of right cosets of H is G is called the <u>index of H in G</u> and is denoted $[G : H]$.

Theorem (Lagrange)

Suppose that G is a finite group and that $K \leq G$. Then, $|G| = |K|[G : K]$.

Theorem (Lagrange)

Suppose that G is a finite group and that $K \leq G$. Then, $|G| = |K|[G : K]$.

Corollary

Let G be a finite group.

1. *For all $a \in G$, $|a|$ divides $|G|$.*
2. *If $|G| = k$, then $a^k = e$ for all $a \in G$.*

Theorem

Let $p \in \mathbb{Z}$ be a positive prime. Any group G of order p is cyclic and therefore isomorphic to $\mathbb{Z}_p$.

Theorem

Let $p \in \mathbb{Z}$ be a positive prime. Any group G of order p is cyclic and therefore isomorphic to $\mathbb{Z}_p$.

Theorem

Every group of order 4 is isomorphic to either $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Theorem

Let $p \in \mathbb{Z}$ be a positive prime. Any group G of order p is cyclic and therefore isomorphic to $\mathbb{Z}_p$.

Theorem

Every group of order 4 is isomorphic to either $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Theorem

Every group of order 6 is isomorphic to $\mathbb{Z}_6$ or to S_3.