# MTHSC 412 Section 7.6 –Normal Subgroups

Kevin James

## Goal

We would like to build up to the notion of a quotient group. That is, given $K \leq G$ we would like to derive an operation on the right cosets of $K$ from the group operation on $G$.

## Problem

In order for such an operation to be well-defined, we need that if $a \equiv b \pmod{K}$ and $c \equiv d \pmod{K}$ then $ac \equiv bd \pmod{K}$. However, this is not always true.

## Example

Take $G = S_3$ and $K = \left\{ e, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}$.

Then the right cosets (or equivalence classes) of $K$ in $G$ are

$K, \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}, \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \right\}$.

So, we have $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \equiv \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \pmod{K}$, and

$e \equiv \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \pmod{K}$.

However, $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \cdot e = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$, and

$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

are in different cosets and therefore not equivalent modulo $K$.

## Note

One major difference between the situation in rings and the situation in groups is the following.
In a ring $(a-b) \in I \Leftrightarrow (b-a) \in I$, because $(b-a) = -(a-b)$.
In fact, in a ring we have $(b-a) = -(a-b) = -a+b$.
Thus $(a-b) \in I \Leftrightarrow -a+b \in I$.
However in a group the analogous statements would be $ab^{-1} \in K$ or $a^{-1}b \in K$ and these are not always equivalent!

## Definition

Let $K \leq G$ and let $a, b \in G$. We say that $a$ is <u>left congruent to $b$ modulo $K$</u> and write $a \simeq b \pmod{K}$ if $a^{-1}b \in K$.

### Theorem

*Let $K \leq G$ and let $a, c \in G$.*

1. *The relation of left congruence modulo $K$ is an equivalence relation on $G$.*
   **Note:** If $K \leq G$ and $a \in G$ then the left equivalence class of $a$ is $aK$.
2. $a \simeq c \pmod{K}$ *if and only if* $aK = cK$.
3. *Any two left cosets of $K$ are either disjoint or identical.*

### Definition

Suppose that $N \leq G$. $N$ is said to be a normal subgroup of $G$ if $aN = Na$ for every $a \in G$. In this case, we write $N \trianglelefteq G$.

### Example

1. If $G$ is abelian and $N \leq G$ then $N$ is normal.
2. Take $G = S_3$ and $K = \left\{ e, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}$. Then $K$ is **not** a normal subgroup
3. Take $G = S_3$ and $K = \left\langle \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right\rangle$. Then $K \trianglelefteq G$.

**Theorem**

*Suppose that $N \trianglelefteq G$ and $a, b, c, d \in G$ with $a \equiv b \pmod{N}$ and $c \equiv d \pmod{N}$. Then $ac \equiv bd \pmod{N}$.*

**Theorem**

*Suppose that $N \leq G$. The following conditions are equivalent.*

1. $N \trianglelefteq G$.
2. $a^{-1}Na \subseteq N$ for all $a \in G$.
3. $aNa^{-1} \subseteq N$ for all $a \in G$.
4. $a^{-1}Na = N$ for all $a \in G$.
5. $aNa^{-1} = N$ for all $a \in G$.