MTHSC 412 Section 3.2 – Properties of Group Elements

Kevin James

Theorem (Properties of Group Elements)

Let G be a group with binary operation written as multiplication.

1. *The identity element e of G is unique.*
2. *For each $x \in G$ the inverse x^{-1} in G is unique.*
3. *For each $x \in G$, $(x^{-1})^{-1} = x$.*
4. *For any $x, y \in G$, $(xy)^{-1} = y^{-1}x^{-1}$.*
5. *Suppose that $a, x, y \in G$ then*
    1. $ax = ay \Rightarrow x = y$.
    2. $xa = ya \Rightarrow x = y$.

Theorem (Properties of Group Elements)

Let G be a group with binary operation written as multiplication.

1. *The identity element e of G is unique.*
2. *For each $x \in G$ the inverse x^{-1} in G is unique.*
3. *For each $x \in G$, $(x^{-1})^{-1} = x$.*
4. *For any $x, y \in G$, $(xy)^{-1} = y^{-1}x^{-1}$.*
5. *Suppose that $a, x, y \in G$ then*
    1. $ax = ay \Rightarrow x = y$.
    2. $xa = ya \Rightarrow x = y$.

Note

Part 5 of the previous theorem says that no element of a group appears twice in the same row or column of the group's multiplication table.

Theorem

Let G be a nonempty set and suppose that there is an associative binary operation (which we will denote by multiplication) defined on G. G is a group if and only if the equations $ax = b$ and $ya = b$ have solutions x and y for all $a, b \in G$.

Definition

Suppose that $a_1, a_2, \ldots, a_n \in G$. Then we define $a_1 a_2 \ldots a_n$ recursively by

$$a_1 \ldots a_{k+1} = (a_1 \ldots a_k) a_{k+1} \quad \text{for } k \geq 1.$$

That is, $a_1 a_2 \ldots a_n = ((\ldots(a_1 a_2) a_3) a_4) \ldots a_n)$.

Definition

Suppose that $a_1, a_2, \ldots, a_n \in G$. Then we define $a_1 a_2 \ldots a_n$ recursively by

$$a_1 \ldots a_{k+1} = (a_1 \ldots a_k) a_{k+1} \quad \text{for } k \geq 1.$$

That is, $a_1 a_2 \ldots a_n = ((\ldots(a_1 a_2) a_3) a_4) \ldots a_n)$.

Theorem (Generalized Associative Law)

Suppose that $a_1, \ldots, a_n \in G$ and that $1 \leq m < n$. Then

$$(a_1 \ldots a_m)(a_{m+1} \ldots a_n) = a_1 \ldots a_n$$

Fact

We proved that $M_{m\times n}(\mathbb{R})$ *is a group under addition of matrices.*

Fact

We proved that $M_{m\times n}(\mathbb{R})$ *is a group under addition of matrices. The same proof will show that* $M_{m\times n}(\mathbb{C})$, $M_{m\times n}(\mathbb{Z})$ *and* $M_{m\times n}(\mathbb{Q})$ *are groups under addition as well.*

Fact

We proved that $M_{m\times n}(\mathbb{R})$ is a group under addition of matrices. The same proof will show that $M_{m\times n}(\mathbb{C}), M_{m\times n}(\mathbb{Z})$ and $M_{m\times n}(\mathbb{Q})$ are groups under addition as well.
Since we have an addition law defined on $\mathbb{Z}_k$ we can make the obvious definition of addition on $M_{m\times n}(\mathbb{Z}_k)$ as well.

Fact

We proved that $M_{m\times n}(\mathbb{R})$ is a group under addition of matrices. The same proof will show that $M_{m\times n}(\mathbb{C}), M_{m\times n}(\mathbb{Z})$ and $M_{m\times n}(\mathbb{Q})$ are groups under addition as well.
Since we have an addition law defined on $\mathbb{Z}_k$ we can make the obvious definition of addition on $M_{m\times n}(\mathbb{Z}_k)$ as well.
It is fairly easy to check that with this addition operation, $M_{m\times n}(\mathbb{Z}_k)$ is a finite abelian group as well.

Fact

Let

$$\mathbb{GL}_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \quad | \quad \textit{there is } B \in M_n(\mathbb{R}) \textit{ with } AB = I_n\}.$$

Fact

Let

$$\mathbb{GL}_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \quad | \quad \textit{there is } B \in M_n(\mathbb{R}) \textit{ with } AB = I_n\}.$$

Then $\mathbb{GL}_n(\mathbb{R})$ *is a group under matrix multiplication.*

Fact

Let

$$\mathbb{GL}_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \quad | \quad \textit{there is } B \in M_n(\mathbb{R}) \textit{ with } AB = I_n\}.$$

Then $\mathbb{GL}_n(\mathbb{R})$ *is a group under matrix multiplication.*
In fact, the same is true if we replace $\mathbb{R}$ *by* $\mathbb{Z}, \mathbb{Q}, \mathbb{C}$ *or* $\mathbb{Z}_n$.