MTHSC 412 Section 7.3 – Subgroups

Kevin James

Definition

A subset H of a group G is a <u>subgroup</u> of G if H is a group under the group operation of G. If H is a subgroup of G, we will write $H \leq G$.

Example

1. If G is a group with identity e, then $\{e\} \leq G$.
2. If G is a group then $G \leq G$.
3. $\mathbb{Q}^*$ is a group under multiplication. Let $H = \{r \in \mathbb{Q} \mid r > 0\|$ Then, $H \leq \mathbb{Q}^*$.

Theorem

A nonempty subset H of a group G is a subgroup of G if

1. *For all $a, b \in H$, $ab \in H$.*
2. *For all $a \in H$, $a^{-1} \in H$.*

Definition

If R is a commutative ring with identity, then we define $\mathbb{SL}_n(R) = \{A \in \mathbb{M}_n(R) \mid \det(A) = 1_R\}$

Fact

Show that $\mathbb{SL}_2(\mathbb{R}) \leq \mathbb{GL}_2(\mathbb{R})$.

Theorem

Let H be a nonempty finite subset of a group G. If H is closed under the group operation of G, then $H \leq G$.

Example

Consider the set

$$H = \left\{ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$$

in $\mathbb{GL}_2(\mathbb{R})$. Show that $H \leq \mathbb{GL}_2(\mathbb{R})$.

Definition

If G is a group we define the center $Z(G)$ as follows.

$$Z(G) = \{g \in G \mid ag = ga \text{ for all } a \in G\}.$$

Example

1. $Z(\mathbb{Q}^*) = \mathbb{Q}^*$.
2. $Z(S_3) = \{e\}$.
3. $Z(D_4) = \{e = r^0, r^2\}$.

Theorem

If G is a group then $Z(G) \leq G$.

Definition

If G is a group and $a \in G$, then $< a >= \{a^n \mid n \in \mathbb{Z}\}$.

Theorem

If G is a group and $a \in G$, then $< a > \leq G$.

Definition

If G is a group and $a \in G$, $< a >$ is called the cyclic subroup of G generated by a.
If $G =< a >$, then we say that G is cyclic.

Example

In S_3,

$$\left\langle \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right\rangle = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}.$$

Note

If we are using additive notation, then we write $< a >= \{na \mid n \in \mathbb{Z}\}$.

Example

$\mathbb{Z} =< 1 >$.

Theorem

Suppose that G is a group and that $a \in G$.

1. *If a has infinite order then $< a >$ is an infinite subgroup of G consisting of the distinct elements a^k with $k \in \mathbb{Z}$.*
2. *If $|a| = n$, then $< a >= \{a^0 = e, a^1, \ldots, a^{n-1}\}$.*

Theorem

If F is a field, $G \leq F^*$ and G is finite, then G is cyclic.

Theorem

Every subgroup of a cyclic group is cyclic.

Theorem

Let S be a nonempty subset of a group G. Let $< S >$ denote the set

$$\{s_1 \cdot s_2 \cdot \ldots \cdot s_k \mid k \in \mathbb{N};\ \text{for each } 1 \le i \le k,\ s_i \in S \text{ or } s_i^{-1} \in S\ \}.$$

Then,

1. $S \subseteq < S > \le G$.
2. *If* $S \subseteq H \le G$, *then* $< S > \le H$.

Example

$U_{12} = < \{5, 7\} >$.