

MTHSC 412 SECTION 7.3 – SUBGROUPS

Kevin James

DEFINITION

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

DEFINITION

A subset H of a group G is a subgroup 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 $\{e\} \leq G$.

DEFINITION

A subset H of a group G is a subgroup 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 $G \leq G$.

DEFINITION

A subset H of a group G is a subgroup 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 $a \in H$, $a^{-1} \in H$.*

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

$$\mathrm{SL}_n(R) = \{A \in \mathbb{M}_n(R) \mid \det(A) = 1_R\}$$

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

$$\mathrm{SL}_n(R) = \{A \in \mathbb{M}_n(R) \mid \det(A) = 1_R\}$$

FACT

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

THEOREM

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

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

DEFINITION

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

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

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 $Z(D_4) = \{e = r^0, r^2\}$.

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 $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$.

DEFINITION

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

THEOREM

If G is a group and $a \in G$, then $\langle a \rangle \leq G$.

DEFINITION

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

THEOREM

If G is a group and $a \in G$, then $\langle a \rangle \leq G$.

DEFINITION

If G is a group and $a \in G$, $\langle a \rangle$ is called the cyclic subgroup of G generated by a .

DEFINITION

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

THEOREM

If G is a group and $a \in G$, then $\langle a \rangle \leq G$.

DEFINITION

If G is a group and $a \in G$, $\langle a \rangle$ is called the cyclic subgroup of G generated by a .

If $G = \langle a \rangle$, then we say that G is cyclic.

EXAMPLE

In S_3 ,

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

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

$$\langle a \rangle = \{na \mid n \in \mathbb{Z}\}.$$

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

$$\langle a \rangle = \{na \mid n \in \mathbb{Z}\}.$$

EXAMPLE

$$\mathbb{Z} = \langle 1 \rangle.$$

THEOREM

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

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

THEOREM

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

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

THEOREM

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

THEOREM

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

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

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 $\langle S \rangle$ denote the set

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

Then,

- ① $S \subseteq \langle S \rangle \leq G$.
- ② If $S \subseteq H \leq G$, then $\langle S \rangle \leq H$.

THEOREM

Let S be a nonempty subset of a group G . Let $\langle S \rangle$ denote the set

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

Then,

- ① $S \subseteq \langle S \rangle \leq G$.
- ② If $S \subseteq H \leq G$, then $\langle S \rangle \leq H$.

EXAMPLE

$$U_{12} = \langle \{5, 7\} \rangle.$$