Math 521A

7.3 – Subgroups

Definition

Let G be a group. A nonempty subset H of G is a subgroup of G if H is itself a group under the operation of G.

Every group G has at least two subgroups: $\{e\}$ (the trivial subgroup, consisting of the identity only) and G itself.

Example

The set of nonzero rational numbers, denoted by, $\mathbb{Q}^*$ is a group under multiplication. The set of all positive rational numbers, $\mathbb{Q}^{>0}$, is a subgroup of $\mathbb{Q}^*$.

Example

Let $G = D_3 = \{\mathrm{id}, r, r^2, s, rs, r^2s\}$. Then $H = \{\mathrm{id}, r, r^2\}$ and $K = \{\mathrm{id}, s\}$ are subgroups of G.

Example

Let $G = \mathbb{Z} \times \mathbb{Z}_4$. Then $H = 2\mathbb{Z} \times \{0, 2\}$ is a subgroup of G.

Theorem

Let H be a nonempty subset of a group G. Then H is a subgroup of G if

(i) $a, b \in H \Longrightarrow ab \in H$; *and*

(ii) $a \in H \Longrightarrow a^{-1} \in H$.

Example

Let $H = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{R} \text{ and } ad - bc = 1 \right\}$. Is H a subgroup of $\mathrm{GL}(2, \mathbb{R})$?

Theorem

Let H be a nonempty finite subset of a group G. If H is closed under the operation in G, then H is a subgroup of G.

Example

Refer to the second example on the previous slide. Also, $H = \{\pm 1, \pm i\}$ is a subgroup of $\mathbb{C}^*$.

- Let G be a group and $a \in G$. Then

$$\langle a \rangle = \{\ldots, a^{-3}, a^{-2}, a^{-1}, a^0, a^1, a^2, \ldots\} = \{a^n \mid n \in \mathbb{Z}\}$$

  is a subgroup of G. See the proof on the board.
- The group $\langle a \rangle$ is called the cyclic subgroup generated by a.
- If G has an element g such that $\langle g \rangle = G$, we say that G is a cyclic group.
- Note that $\langle a \rangle$ is always Abelian for $a^i \cdot a^j = a^{i+j} = a^j \cdot a^i$ for any $i, j \in \mathbb{Z}$.

Example

Let $G = D_3$. Then $\langle r \rangle = \{\mathrm{id}, r, r^2\}$, $\langle s \rangle = \{\mathrm{id}, s\}$.

Example

Let $G = \mathbb{Z}$. Then $\langle 1 \rangle = \langle -1 \rangle = G$.

The proofs of the next theorems are presented on the board.

Theorem

Let G be a group and let $a \in G$.

(1) *If $|a| = \infty$, then $\langle a \rangle$ is an infinite cyclic group consisting of the elements a^k, with $k \in \mathbb{Z}$.*

(2) *If $|a| = n$ (where n is a positive integer), then $\langle a \rangle$ is a subgroup of order n and $\langle a \rangle = \{e = a^0, a, a^2, \ldots, a^{n-1}\}$.*

Theorem

Let F^* be the multiplicative group of nonzero elements of a field F. If G is a finite subgroup of F^*, then G is cyclic.

Theorem

Every subgroup of a cyclic group is itself cyclic.