MTHSC 412 Section 3.3 – Subgroups

Kevin James

Definition

Let G be a group with respect to the binary operation $*$. $H \subseteq G$ is a *subgroup* of G if H is a group under the binary operation $*$.
In this case, we will write $H \leq G$.

Example

1. Since $\mathbb{C}, \mathbb{R}, \mathbb{Q}$ and $\mathbb{Z}$ are all groups under the same addition operation (namely addition of complex numbers), we have

$$\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}.$$

2. Note that $G = \mathbb{C} - \{0\}$ is a group under multiplication of complex numbers.
   Also, $H = \{\pm 1, \pm i\}$ is a group under multiplication of complex numbers and $H \subseteq G$.
   Thus $H \leq G$.

Theorem

A subset H of a group G is a subgroup of G if and only if the following conditions are satisfied.

1. H *is nonempty,*
2. $x, y \in H \Rightarrow x * y \in H$,
3. $x \in H \Rightarrow x^{-1} \in H$.

Example

Recall that $\mathbb{GL}_n(\mathbb{R})$ is a group under matrix multiplication.
Let $\mathbb{SL}_n(\mathbb{R}) = \{A \in \mathbb{GL}_n(\mathbb{R}) \quad | \quad \det(A) = 1\}$.
Show that $\mathbb{SL}_n(\mathbb{R}) \leq \mathbb{GL}_n(\mathbb{R})$.

Theorem

Suppose that G is a group under $*$ and that $H \subseteq G$. Then $H \leq G$ if and only if the following conditions hold.

1. $H \neq \emptyset$,
2. $a, b \in H \Rightarrow ab^{-1} \in H$.

Example

Let $\mathbb{GL}_n^+(\mathbb{R}) = \{A \in \mathbb{GL}_n(\mathbb{R}) \quad | \quad \det(A) > 0\}$.
Show that $\mathbb{GL}_n^+(\mathbb{R}) \leq \mathbb{GL}_n(\mathbb{R})$.

Fact

Suppose that G is a group and $H, K \leq G$. Then $H \cap K \leq G$ also.

Definition

Let G be a group with binary operation written as multiplication. For any $a \in G$ we define *nonnegative integral exponents* by

$$a^0 = e, \qquad a^1 = a, \qquad a^{n+1} = a^n a \quad n > 0.$$

Negative integral exponents are defined by

$$a^{-n} = (a^{-1})^n \qquad n > 0.$$

Definition

Let G be a group with binary operation written as addition. For any $a \in G$ we define *nonnegative integral multiples* by

$$0a = 0, \qquad 1a = a, \qquad (n+1)a = na + 1 \quad n > 0.$$

Negative integral multiples are defined by

$$(-n)a = n(-a) \qquad n > 0.$$

Theorem (Laws of Exponents)

Suppose that G is a group with binary operation denoted by multiplication and that $a, b \in G$, and $m, n \in \mathbb{Z}$. Then,

1. $x^n \cdot x^{-n} = e$,
2. $x^m \cdot x^n = x^{m+n}$,
3. $(x^m)^n = x^{mn}$, *and*
4. *If G is abelian then $(xy)^n = x^n y^n$.*

Theorem (Laws of Multiples)

Suppose that G is a group with binary operation denoted by addition and that $a, b \in G$, and $m, n \in \mathbb{Z}$. Then,

1. $nx + (-n)x = 0$,
2. $mx + nx = (m+n)x$,
3. $n(mx) = (nm)x$, *and*
4. *If G is abelian then $n(x+y) = nx + ny$.*

Example

Suppose that G is a group and $a \in G$. Let $H = \{x \in G \quad | \quad x = a^m \text{ for some } m \in \mathbb{Z}\}$.
Show that $H \leq G$.

Definition

Let G be a group. For any $a \in G$, the subgroup

$$H = \{x \in G \quad | \quad x = a^m \text{ for some } m \in \mathbb{Z}\}$$

is the *cyclic subgroup* of G generated by a.
This subgroup is sometimes denoted $< a >$.
A subgroup $K \leq G$ is said to be *cyclic* if there is a $b \in G$ such that $K =< b >$.
In particular, G is said to be a cyclic group if $G =< a >$ for some $a \in G$.

Example

1. $\mathbb{Z}$ is a cyclic subgroup since it is generated by 1.
2. In $\mathbb{Z}$, the cyclic subgroup $< 2 >$ is the subgroup of even numbers.
3. S_3 is not a cyclic group.
4. $\mathbb{Z}_n$ is a cyclic group generated by [1].