5 Subgroups

5.1 Notation and Terminology

By convention, the binary operation $+$ is considered commutative, whereas multiplication, such as ab may or may not be commutative. We may continue to use 0 as the identity of $+$ and 1 as the identity element of multiplication. We use $-a$ to denote the additive inverse of an element a, and a^{-1} to denote the multiplicative inverse of a.

We use the usual convention that the product of n factors of a is a^n and the sum of n elements a is na. Similarly, $(a^{-1})^n = a^{-n}$ and $n(-a) = -na$.

Remark. *In both na and a^n, $a \in G$ and $n \in \mathbb{Z}$. In particular, $n \notin G$.*

Remark. *We use the multiplication to denote a general binary operation.*

We define the **order** of a group G, denoted by $|G|$, as the number of elements in G (compare to the cardinality of a set).

5.2 Subsets and Subgroups

Definition 1. *If a subset H of a group G is closed under the binary operation of G and if H with the induced operation from G is itself a group, then H is a **subgroup** of G, denoted by $H \leq G$ or $G \geq H$. If $H \neq G$, we write $H < G$ or $G > H$.*

Thus $\langle \mathbb{Z}, + \rangle < \langle \mathbb{R}, + \rangle$ and $\langle \mathbb{Q}^+, \cdot \rangle$ is *not* a subgroup of $\langle \mathbb{R}, + \rangle$ (why?), even though $\mathbb{Q}^+ \subset \mathbb{R}$.

Definition 2. *If G is a group, then G is the only improper subgroup of G and all other subgroups of G are proper subgroups. The subgroup $\{e\}$ is the trivial subgroup of G and all other subgroups are nontrivial.*

Example 1. *There are two different groups of order 4: $\langle \mathbb{Z}_4, + \rangle$, which is isomorphic to the fourth roots of unity under multiplication $\langle U_4, \cdot \rangle$, where $U_4 = \{1, i, -1, -i\}$:*

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

and the Klein 4-group, denoted by V (from German "vier" for "four"):

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

The only nontrivial proper subgroup of $\mathbb{Z}_4$ is $\{0, 2\}$. The Klein 4-group has three nontrivial proper subgroups: $\{e, a\}, \{e, b\}, \{e, c\}$.

A subgroup diagram shows the subgroups under their parent groups.

Theorem. *Suppose $\langle G, \cdot \rangle$ is a group and $H \subseteq G$. $\langle H, \cdot \rangle$ is a subgroup of G if and only if*

1. *H is closed under $*$*
2. *the identity element $e \in G$ is also the identity element in H*
3. *for all $a \in H$, $a^{-1} \in H$.*

An argument for the proof follows the fact that every equation in H is also an equation in G.

5.3 Cyclic Subgroups

Definition 3. *Let G be a group and $a \in G$. The* ***cyclic subgroup of G generated by*** *a is*

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

Theorem. *Let G be a group and let $a \in G$. Then $\langle a \rangle$ is a subgroup of G and is the smallest subgroup of G that contains a. That is, every subgroup of G that contains a, contains $\langle a \rangle$.*

Definition 4. *If $G = \langle a \rangle$ for some $a \in G$, then the element a* ***generates*** *G and is a generator for G. If an element generates a group G, we say G is* ***cyclic****.*

Example 2. *We have $\langle 1 \rangle = \mathbb{Z}_4 = \langle 3 \rangle$. However, the Klein 4-group is* not *cyclic, because $\langle a \rangle, \langle b \rangle, \langle c \rangle$ are proper subgroups of V.*

Example 3. *If $n > 1$, then $\mathbb{Z}_n = \langle 1 \rangle = \langle n - 1 \rangle$.*

Example 4. *We have $\langle 3 \rangle = 3\mathbb{Z}$ and $6\mathbb{Z} < 3\mathbb{Z}$.*

Example 5. *Determine whether the set of $n \times n$ invertible matrices with determinant 2 is a subgroup of $GL(n, \mathbb{R})$.*

Example 6. *Describe all the elements in the cyclic subgroup of $GL(2, \mathbb{R})$ generated by* $\begin{bmatrix} 3 & 0 \\ 0 & 2 \end{bmatrix}$.