CHAPTER 1. GROUPS AND SUBGROUPS

1.5 Subgroups

1.5.1 Notation and Terminology

Some conventional notation in group theory:

1. **Group with product:** Usually we use “ab” (read as “the product of \(a\) and \(b\)”) in place of “\(a \ast b\)” for the binary operation of a group. The identity element is denoted by “1” (Occasionally, “e” or “u” may be used). The inverse of an element \(x\) is denoted by \(x^{-1}\). The \(n\)-th power of \(x\) is denoted by \(x^n\).

2. **Group with sum:** If a group is abelian (i.e. the binary operation is commutative), we may use “\(a + b\)” (read as “the sum of \(a\) and \(b\)”) for the binary operation. The identity element is denoted by “0”. The inverse of \(x\) is denoted by \(-x\). The \(n\)-th power of \(x\) is denoted by \(nx\).

So sum is always commutative, but product may not be.

**Def 1.51.** The order \(|G|\) of a group \(G\) is the number of elements in \(G\).

1.5.2 Subsets and Subgroups

**Ex 1.52.** With the sum operation, \(\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}\). So \(2 + 3 = 5\) in all these groups. However, the group \(\mathbb{Q}^+\) with product is different from the group \(\mathbb{R}\) with sum. For example, \(2 \cdot 3 = 6\) in \(\mathbb{Q}^+\) but \(2 + 3 = 5\) in \(\mathbb{R}\). So \(\langle \mathbb{Q}^+ , \cdot \rangle\) may not be viewed as a “subgroup” of \(\langle \mathbb{R}, + \rangle\).

**Def 1.53 (Subgroup).** If a subset \(H\) of a group \(G\) is itself a group under the binary operation of \(G\), then \(H\) is a subgroup of \(G\), written as \(H \leq G\) or \(G \geq H\).

If \(H \leq G\) but \(H \neq G\), we write \(H < G\) or \(G > H\).

**Ex 1.54.** Two examples of subgroups:

1. The set \(m\mathbb{Z} := \{mk \mid k \in \mathbb{Z}\}\) is a group under addition (Caution: \(m\mathbb{Z} \neq \mathbb{Z}_m\)). We get

\[
\langle 6\mathbb{Z}, + \rangle < \langle 2\mathbb{Z}, + \rangle < \langle \mathbb{Z}, + \rangle < \langle \frac{1}{3}\mathbb{Z}, + \rangle < \langle \mathbb{Q}, + \rangle < \langle \mathbb{R}, + \rangle < \langle \mathbb{C}, + \rangle.
\]

2. \(\langle \mathbb{Q}^+, \cdot \rangle < \langle \mathbb{R}^+, \cdot \rangle < \langle \mathbb{R}^*, \cdot \rangle < \langle \mathbb{C}^*, \cdot \rangle\).
1.5. SUBGROUPS

Ex 1.55. If \( K \leq H \) and \( H \leq G \), then \( K \leq G \).

Def 1.56. If \( G \) is a group, then \( G \) is the improper subgroup of \( G \). All other subgroups are proper subgroups. The subgroup \( \{e\} \) is the trivial subgroup of \( G \). All other subgroups are nontrivial.

Ex 1.57 (Ex 5.9, p51). Two different types of group structures of order 4. (See group tables 5.10 and 5.11). The subgroup diagrams for \( \mathbb{Z}_4 \) and for \( V \) are different.

If \( H \) is a subgroup of \( G \), then the identity element of \( H \) is exactly that of \( G \), the inverse of \( x \in H \) in \( H \) is exactly that of \( x \) in \( G \) (by cancellation theorem).

Process to determine whether \( H \) is a subgroup of \( G \):

Thm 1.58. A subset \( H \) of a group \( G \) is a subgroup of \( G \) if and only if

1. \( H \) is closed under the binary operation of \( G \).
2. the identity of \( G \) is in \( H \).
3. for all \( a \in H \) the inverse \( a^{-1} \in H \) also.

Ex 1.59 (Ex 5.16, p53). The set of all \( n \times n \) real matrices \( A \) with \( \det A = 1 \) under matrix multiplication is a group (since \( \det(AB) = \det A \det B \)), denoted by \( SL(n, \mathbb{R}) \). It is a subgroup of \( GL(n, \mathbb{R}) \) = “the set of all \( n \times n \) invertible matrices under matrix multiplication”.

Ex 1.60. Let \( F([a,b]) \) be the set of all functions from \([a,b]\) to \( \mathbb{R} \). Let \( C^0([a,b]) \) be the set of all continuous functions from \([a,b]\) to \( \mathbb{R} \). Under the function addition, \( C^0([a,b]) \) is a subgroup of \( F([a,b]) \).

1.5.3 Cyclic Subgroups

If \( H \) is a subgroup of \( G \) and \( a \in H \), we see how large \( H \) should be.

\[ H \text{ contains } a \implies H \text{ contains } a^2 \text{ (since } H \text{ is closed under the binary operation)} \]

\[ \implies H \text{ contains } a^3 \text{ (the same reason)} \]

\[ \implies H \text{ contains } a^4 \text{ (the same reason)} \]

\[ \implies \ldots \ldots \]

\(^2\)1st hw: 4, 6, 10, 14
CHAPTER 1. GROUPS AND SUBGROUPS

\[ H \text{ contains } a \implies H \text{ contains } a^{-1} \text{ (the inverse is also in } H) \]
\[ \implies H \text{ contains } a^{-2} \text{ (} H \text{ is closed under the binary operation)} \]
\[ \implies H \text{ contains } a^{-3} \text{ (the same reason)} \]
\[ \implies \ldots \ldots \]

**Conclusion:** Denote \( a^0 := e \). Then \( H \) contains \( a \) if and only if \( H \) contains \( \{a^n \mid n \in \mathbb{Z}\} = \{\ldots, a^{-3}, a^{-2}, a^{-1}, e, a^1, a^2, a^3, \ldots\} \)

**Thm 1.61.** Let \( G \) be a group and \( a \in G \). Then
\[ \langle a \rangle := \{a^n \mid n \in \mathbb{Z}\} \]
is the smallest subgroup of \( G \) that contains \( a \), that is, every subgroup containing \( a \) contains the subgroup \( \langle a \rangle \).

We call \( \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\} \) the cyclic subgroup of \( G \) generated by \( a \).

**Def 1.62.** If \( G \) is a group and \( \langle a \rangle = G \), then \( a \) is called a generator for \( G \). A group \( G \) is cyclic if there is one element in \( G \) that generates \( G \).

**Ex 1.63 (Ex 5.20, p54).** The groups of order 4.

**Ex 1.64.** The group \( \langle \mathbb{Z}, + \rangle \) is cyclic. 1 and -1 are the only generators.

**Ex 1.65.** For \( m \in \mathbb{Z} \), the group \( \langle \mathbb{Z}_m, + \rangle \) is cyclic (Discuss the generators for \( \mathbb{Z}_4 \) and \( \mathbb{Z}_5 \)).

**Ex 1.66.** The group \( \langle m\mathbb{Z}, + \rangle \) is cyclic.

**Ex 1.67.** Show by contradiction that \( \langle \mathbb{Q}, + \rangle \) is not cyclic.

1.5.4 Homework (Section I-5, p55-59)

1st 4, 6, 10, 14

2nd 23, 39, 41, 54.

(opt) 20, 26, 36, 40, 45, 52