1.4 Groups

1.4.1 Definition and Examples

Def 1.32. A group \((G, \ast)\) is a set \(G\), closed under a binary operation \(\ast\), such that the following axioms are satisfied:

1. **Associativity**: \((a \ast b) \ast c = a \ast (b \ast c)\) for all \(a, b, c \in G\).

2. **Identity**: There is an element \(e \in G\) such that \(e \ast x = x \ast e = x\) for all \(x \in G\).

3. **Inverse**: For each \(x \in G\), there is an element \(x^{-1} \in G\) corresponding to \(x\), such that \(x \ast x^{-1} = x^{-1} \ast x = e\).

Def 1.33. A group \(G\) is **abelian** if its binary operation is commutative.

Historical Notes in p38-39, and Galois’s tale.

* To determine whether \((G, \ast)\) is a group or not, we should check whether the operation \(\ast\) is closed, and whether \(\ast\) satisfies the axioms for associativity, identity, and inverse.

* Examples of groups:

Ex 1.34. The set \(\mathbb{Z}\) under addition is an abelian group. (Similarly, \(\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_n\) and \(\mathbb{R}_c\) under addition are abelian groups.)

Ex 1.35. The sets \(\mathbb{Q}^+\) and \(\mathbb{R}^+\) of positive numbers and the sets \(\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*\) of nonzero numbers under multiplication are abelian groups.

Ex 1.36. The set \(S\) of all real-valued functions with domain \(\mathbb{R}\) under function addition is an abelian group.

Ex 1.37. The set \(S\) of all real-valued bijections \(f : \mathbb{R} \rightarrow \mathbb{R}\) under function composition is a nonabelian group.

Ex 1.38 (Linear Algebra). A vector space \(V\) under addition is an abelian group.

Ex 1.39. The set \(M_n(\mathbb{R})\) of all \(n \times n\) real matrices with addition is an abelian group. However, \(M_n(\mathbb{R})\) with matrix multiplication is NOT a group (e.g. the zero matrix has no inverse).

---

1st hw: 1, 2, 3, 8. 2nd hw: 10, 23, 28.
Ex 1.40 (⋆). The set of all invertible \( n \times n \) real matrices with matrix multiplication is a group. This is a nonabelian group. It is the \textit{general linear group of degree} \( n \) and is usually denoted by \( GL(n, \mathbb{R}) \).

Ex 1.41. The permutations of \( \{1, 2, \ldots, n\} \) form a permutation group \( S_n \). It is a non-abelian group. (Use \( S_3 \) as an example)

* Examples of NOT groups:

Ex 1.42. The set \( \mathbb{Z}^+ \) under addition is NOT a group. (associative, no identity element, no inverse)

Ex 1.43. The set \( \mathbb{Z}^+ \) under multiplication is NOT a group. (associative, having an identity element, not always having an inverse)

Ex 1.44. The set \( \mathbb{R}^\ast \) under addition is NOT a group. ("+" is not closed)

1.4.2 Elementary Properties of Groups

In the following theorems, we always assume that \( G \) is a group with binary operation \(*\).

Thm 1.45. \textit{The left and right cancellation laws hold in the group} \( G \), \textit{that is}, \( a \ast b = a \ast c \) implies \( b = c \), and \( b \ast a = c \ast a \) implies \( b = c \) for all \( a, b, c \in G \).

Proof. See p 41.

Thm 1.46. \textit{Let} \( a \) \textit{and} \( b \) \textit{be any elements of the group} \( G \). \textit{Then the linear equation} \( a \ast x = b \) \textit{has the unique solution} \( x = a^{-1} \ast b \); \textit{the equation} \( y \ast a = b \) \textit{has the unique solution} \( y = b \ast a^{-1} \).

Thm 1.47 (Uniqueness of the identity and an inverse in a group). \textit{There is only one element} \( e \) \textit{in a group} \( G \) \textit{such that}

\[
e \ast x = x \ast e = x
\]

\textit{for all} \( x \in G \). \textit{For each element} \( x \) \textit{of} \( G \), \textit{there is only one} \( x' \) \textit{in} \( G \) \textit{such that}

\[
x' \ast x = x \ast x' = e.
\]

Thm 1.48. \textit{In a group} \( G \), \textit{we have} \( (a \ast b)^{-1} = b^{-1} \ast a^{-1} \) \textit{for all} \( a, b \in G \).

(Optional) A set with an associative binary operation is called a \textit{semigroup}. A semigroup with an identity element is called a \textit{monoid}.
1.4.3 Finite Groups and Group Tables

Some properties about the table of a finite group $G$ with operation $\ast$:

1. Identity element: there is $e \in G$ such that $e \ast a = a = a \ast e$ for all $a \in G$.

2. Left and right cancellation law: each element $b$ of $G$ must appear once and only once in each row and each column of the table. (Similar to Latin squares, Sudoku games)

There are some other requirements needed for a group table.

**Ex 1.49.** The group table of a two-element group.

**Ex 1.50.** The group table of a three-element group.

1.4.4 Homework, Section 1.4, p45-49

1st: 1, 2, 3, 8,

2nd: 10, 23, 28,

3rd: 25, 33, 41.

(opt) 20, 29, 32, Think about an example of groups in the real world.