Notes of "Group"

Jinxin Wang

1 Overview

- Group and subgroup
  - Def: A group
    - Rmk: The uniqueness of the identity element in a group
    - Rmk: The uniqueness of the inverse element of an element in a group
    - Rmk: The definition of a group does not specify the uniqueness of the identity element and the inverse element of each element
    - Rmk: The default notation of an abstract group is with multiplication, such as the operator and the identity element
  - Def: A subgroup of a group
    - Rmk: Trivial subgroups and proper subgroups
    - Rmk: Is the identity element of a subgroup always the same as the one of its parent group?
  - Examples of groups and subgroups
    - Eg: $(\mathbb{Q}, +)$ and $(\mathbb{Z}, +)$
    - Eg: $(\mathbb{R}/\{0\}, \cdot)$ and $(\mathbb{R}^+, \cdot)$
    - Eg: S_n and the set of even permutations of order n
    - Eg: $GL_n(\mathbb{R})$ and $SL_n(\mathbb{R})$
    - Eg: The set of inversible elements in a monoid
    - Eg: $(\{1, -1\}, \cdot)$
  - Def: An abelian group
  - Examples of abelian groups
    - Eg: $(\mathbb{Z}/n\mathbb{Z}, +)$
    - Eg: $A(X, Y) = \{f : X \to Y\}$ where Y is a abelian group
    - Eg: $L(X, Y) = \{f : X \to Y \mid f \text{ is an additive map }\}$
  - Def: The order (cardinality) of a group, a finite group and an infinite group
  - Examples of finite groups and infinite groups
    - Examples of finite groups: S_n, $(\{1, -1\}, \cdot)$
    - Examples of infinite groups: $(\mathbb{Q}, +)$

- Cyclic groups
  - Rmk: An element in a group generates a subgroup of the group
  - Def: A cyclic group and its generator(s)
    - Rmk: The uniqueness of the generator(s) of a cyclic group
  - Examples of cyclic groups
    - Eg: $(\mathbb{Z}, +)$ can be generated by 1 or -1
    - Eg: $(\{1, -1\}, \cdot)$ can be generated by -1
  - Rmk: The order of a generated cyclic group by an element in a finite group
- The order of an element in a group
  - Def: An element of infinite order or finite order in a group
  - Examples of elements of infinite order and elements of finite order in groups
    - Examples of elements of finite order in groups: A permutation in S_n
    - Examples of elements of infinite order in groups: 1 and -1 in $(\mathbb{Z}, +)$
  - Prop: The relationship between the order of an element in a group and the order of the cyclic group generated by it
- Subgroups of a cyclic group
  - Prop: The form of subgroups of a cyclic group
    - Rmk: For a subgroup of a finite cyclic group, the factor k is not unique?
  - Prop: The relationship between different generators of a finite cyclic group
  - Eg: An application of the form of subgroups of a cyclic group to $(\mathbb{Z}, +)$
- Homomorphisms and isomorphisms
  - Def: A group homomorphism
  - Def: A group isomorphism
    - Rmk: Both a homomorphism and an isomorphism refer to a mapping rather than a relation between two algebraic structures
  - Prop: Some basic properties of a group homomorphism
  - Prop: Some basic properties of a group isomorphism
- Examples and conclusions of group homomorphisms and group isomorphisms
  - Prop: A necessary and sufficient condition of two cyclic groups to be isomorphic in terms of the orders of them

2 Group and subgroup

Definition 1 (A group). *A set G is called a group if a binary operation $\cdot$ is defined on it, and for any $a, b, c \in G$, it holds that*

D1 *Associative law: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$*

D2 *Identity element: There exists $e \in G$ such that $e \cdot a = a \cdot e = a$ for each $a \in G$*

D3 *Inverse element: For each $a \in G$, there exists $b \in G$ such that $ab = ba = e$*

Remark 1 (The uniqueness of the identity element in a group). *Suppose there are $e \in G$ and $e' \in G$ which satisfy the definition of the identity element, then*

$$e = e \cdot e' = e'$$

Remark 2 (The uniqueness of the inverse element of an element in a group). *For each $a \in G$, suppose there are two inverse elements $b \in G$ and $b' \in G$, then*

$$b = b \cdot e = b \cdot (a \cdot b') = (b \cdot a) \cdot b' = e \cdot b' = b'$$

Remark 3 (The definition of a group does not specify the uniqueness of the identity element and the inverse element of each element). *As we can see, the definition of a group does not require the uniqueness of the identity element and the inverse element of each element in a group. The reason is that the uniqueness is a natural property of the identity element and the inverse element of each element once a set satisfies the definition of a group. Hence, we don't need and aren't supposed to add such conditions to the definition.*

Remark 4 (The default notation of an abstract group is with multiplication, such as the operator and the identity element).

Definition 2 (A subgroup of a group).

Remark 5 (Is the identity element of a subgroup always the same as the one of its parent group?). *The identity element of a group is also the identity of its every subgroup.*

Proof: Suppose U is a group, $V \subset U$ is a subgroup of U, and e_U and e_V are the identity elements of them respectively. For e_V, we have $e_V^2 = e_V$. Since $e_V \in U$, the equation also holds in U. Then we have $e_V^{-1} e_V^2 = e_V^{-1} e_V$, which is $e_V = e_U$.

Recall that the similar conclusion doesn't hold for monoids. We can see the changes brought by the additional axioms of a group compared with a monoid.

Example 1 ($(\mathbb{Q}, +)$ and $(\mathbb{Z}, +)$). *$(\mathbb{Q}, +)$ is a group, and $(\mathbb{Z}, +)$ is a subgroup of it.*

Example 2 ($(\mathbb{R}/\{0\}, \cdot)$ and $(\mathbb{R}^+, \cdot)$). *$(\mathbb{R}/\{0\}, \cdot)$ is a group, and $(\mathbb{R}^+, \cdot)$ is a subgroup of it.*

Example 3 (S_n and the set of even permutations of order n). *The set of permutations of order n S_n is a group, and the set of even permutations of order n is a subgroup of S_n.*

Example 4 ($GL_n(\mathbb{R})$ and $SL_n(\mathbb{R})$). *The set of inversible real-valued matrices of order n, denoted by $GL_n(\mathbb{R})$, forms a group. The set of inversible real-valued matrices of order n whose determinant is 1, denoted by $SL_n(\mathbb{R})$, is a subgroup of $GL_n(\mathbb{R})$.*

3 Cyclic groups

4 The order of an element in a group

Definition 3 (An element of infinite order or finite order in a group). *Given an element a in a group, we check the sequence of its integer exponentions. If all of them are different, we say that the order of the element a is infinite, and a is called an element of infinite order in the group. If there are same elements, then there exists integers k_i such that $a^{k_i} = e$. The minimal integer in the set $\{k_i\}$, denoted by q, is called the order of the element a in the group, and a is called an element of finite order in the group, or an element of order q in the group.*

5 Subgroups of a cyclic group

6 Homomorphisms and isomorphisms

7 Examples and conclusions of group homomorphisms and group isomorphisms