离散数学习题课

第六讲 —— 代数系统

Operations

Definition:

For any nonempty set A, and any $n \in \mathbb{N}^+$,

$f : A^n \to A$ is called an <u>*n*-ary operation</u> on A

when $n = 1, 2$, f is called <u>unary</u> and <u>binary operation</u> respectively

Comments:

- The focus of "Abstract Algebra" is the properties (and interactions) of operations

Algebraic Systems

- An algebraic system has 3 components:
  - A nonempty set A, called the carrier
  - Operations
  - Axioms (declaring some properties of the system)
- Example
  - $A = \langle \mathbb{N}, + \rangle, B = \langle \mathbb{N}, +, 0 \rangle$ are different algebraic systems
  - $C = \langle \mathbb{N}^{+}, + \rangle$ is a sub-system of A but not B
  - The declaration of "algebraic constants" are the freedom of "users".

Semigroups

Definition:

A semigroup is an algebraic system $A = \langle S, * \rangle$ satisfying the following axiom:

- * is an associative binary operation on S

Comments:

- Associativity is the most fundamental property
- Semigroups are too unrestrictive to prove many important properties

Monoids

Definition:

A monoid is an algebraic system $A = \langle S, *, e \rangle$ satisfying the following axioms:

- * is an associative binary operation on S
- For all $x \in S, x * e = e * x = e$

Comments:

- According to this view, a sub-system of a monoid must have the same identity
- Example: P195. Ex.11.2

Groups

Definition:

A group is an algebraic system $A = \langle S, *, ^{-1}, e \rangle$ satisfying the following axioms:

- * is an associative binary operation on S
- For all $x \in S, x * e = e * x = e$
- $^{-1}$ is a unary operation on S, satisfying

$$\forall x(x \in S \rightarrow x * x^{-1} = x^{-1} * x = e)$$

Comments:

- This is a "modern" definition of group

Problems

1. Let $V = \langle \{a, b\}, *\rangle$ be a semigroup, with $a * a = b$, show that

   (1) $a * b = b * a$

   (2) $b * b = b$

2. Let G be a group, show that, if there is an element $a \in G$ satisfying $G = \{a^k \mid k \in \mathbb{Z}\}$, then G is an abelian group.

3. Let G be a non-abelian group, show that

$$\exists a, b \in G - \{e\}(a \neq b \wedge ab = ba)$$

Problems (cont.)

4. Let $V = \langle S, \circ \rangle$ be a semigroup, satisfying

   $$\forall a, b \in S,\ a \neq b \to a \circ b \neq b \circ a$$

   Show that (1) $\forall a \in S, a \circ a = a$

   (2) $\forall a, b \in S, a \circ b \circ a = a$

   (3) $\forall a, b, c \in S, a \circ b \circ c = a \circ c$

5. Let G be a group, show that, for any $a, b \in G$

   $$(ab)^2 = a^2b^2 \implies ab = ba$$

6. Show that, any infinite group must have infinitely many subgroups

Thank you

Any questions?