Abstract Algebra

Zhang Yanmei
ymzhang@bupt.edu.cn

College of Computer Science & Technology
Beijing University of Posts & Telecommunications

Content

- Binary Operations
  - Binary Operations
  - Operation Table
  - A Ccounting Problem
  - Properties of Binary Operations
  - Distinguished Elements
  - An example - Algebraic Lattice

二元操作

Binary Operations

阿贝尔群

Binary Operations（二元运算）

- An binary operation on the set A is an everywhere defined function
  - $f: A \times A \rightarrow A$.
- Note: A binary operation must satisfy
  - f assign an element $f(a,b)$ of A to each ordered pair (a,b) in $A \times A$.
  - Since a binary operation is a function, only one element of A is assigned to each ordered pair.

二元运算

Notation

- It's customary to denote binary operations by a symbol such as $*$.
  - $a*b$ instead of $*(a,b)$
    - $*$: multiplication
    - $a*b$: the product of a and b.
- A is closed under the operation $*$,if a and b are elements in A, $a*b \in A$.

a*b the product of a and b

Example

- Let A=Z, Define $a*b$ as $a+b$.
  - * is a binary operation on Z.
- Let A=R, Define $a*b$ as a / b.
  - * is not a binary operation, since it is not defined for every ordered pair of elements of R.
  - For example, 3*0 is not defined, since we can not divide by zero. 这就不是二元运算

Example 3

- Let $A = Z^+$. Define $a*b$ as a-b.
  - $*$ is not a binary operation .
  - it does not assign an element of A to every ordered pair of elements of A;
  - for example, $2*5 \notin A$.

$2*5 \notin A$

Example 4

- Let $A = \mathbb{Z}$. Define $a*b$ as a number less than both a and b.

并不是一个确定的数

  - $*$ is not a binary operation, since it does not assign a *unique* element of A to each ordered pair of elements of A; for example, $8*6$ could be 5, 4, 3, l, and so on.
  - in this case, $*$ would be a relation from $A\times A$ to A, but not a function

Example 5,6

max{a, b}.

- Let A = $\mathbb{Z}$. Define $a*b$ as max$\{a, b\}$.
  - $*$ is a binary operation; for example,$2*4 = 4$, $-3*(-5)=-3$.
- Let $A = P(S)$, for some set S. If V and W are subsets of S, define $V*W$ as $V\cup W$.
  - $*$ is a binary operation on A.
  - if we define $V *' W$ as $V\cap W$, then $*'$ is another binary operation on A.
    - Note: It's possible to define many binary operations on the same set.

$a\in A$, $b\in A$

$a*b \in A$ ✓ 二元运算

Example 7,8

- Let M be the set of all $n \times n$ Boolean matrices for a fixed n. Define $A*B$ as $A \vee B$
  - $*$ is a binary operation.
  - This is also true of $A \wedge B$.
- Let L be a lattice. Define $a*b$ as $a \wedge b$.
  - $*$ is a binary operation on L.
  - This is also true of $a \vee b$

Operation table运算表

运算表

- If $A = \{a_1, a_2, \ldots, a_n\}$ is a *finite* set, a binary operation on A can be defined by means of a table

有限集合

a_j

$*$	a_1	a_2	$\cdots$	a_j	$\cdots$	a_n
a_1						
a_2						
$\vdots$						
a_i				$a_i * a_j$		
$\vdots$						
a_n						

a_i

Figure 9.1

Example 9

- Let $A = \{0, 1\}$.
- Define binary operations $\vee$ and $\wedge$ by the following tables:

$\vee$	0	1
0	0	1
1	1	1

$\wedge$	0	1
0	0	0
1	0	1

How many operations?

- If $A = \{a, b\}$, how many binary operations can be defined on A.
  - Every binary operation $*$ on A can be described by a table.

$*$	a	b
a		
b		

$2^4 = 16$

  - There are $2 \times 2 \times 2 \times 2 = 2^4$ or 16 ways to complete the table.

Properties of Binary Operations（二元运算的性质）

- For all elements *a*, *b*, and *c* in *A*
  - Commutative(可交换的): $a*b = b*a$
  - Associative(可结合的): $a*(b*c) = (a*b)*c$
  - Idempotent(幂等的): $a*a = a$

可交换的
Commutative $a*b=b*a$
可结合的
associative. $a*(b*c)=(a*b)*c$
idempotent $a*a=a$
幂等的

Example 12

- Which of the following binary operations on $A = \{a, b, c, d\}$ are commutative?

$*$	a	b	c	d
a	a	c	b	d
b	b	c	b	a
c	c	d	b	c
d	a	a	b	b

(a)

$*$	a	b	c	d
a	a	c	b	d
b	c	d	b	a
c	b	b	a	c
d	d	a	c	d

(b)

Example 15

- Let L be a lattice. The binary operation defined by $a*b = a \wedge b$ is
  - *commutative* and ✓
  - *associative*. ✓
  - It also satisfies the *idempotent* property $a \wedge a = a$.

幂等

可交换的

可结合的

幂等

$(a\wedge b)\wedge c = a\wedge(b\wedge c)$

Proof $a*b = a\wedge b$ is associative

∨ 最小上界

∧ 最大下界

- Let $x=(a\wedge b)\wedge c$, $y=a\wedge(b\wedge c)$.
- (1) show $x\le y$
  - $x \le a\wedge b$, So $x \le a\wedge b \le a$, then $x \le a$; $x \le a\wedge b \le b$, then $x \le b$; and $x \le c$.

    $x\le a \Rightarrow x\le a\wedge b$
  - $x \le b\wedge c$, then $x \le a\wedge(b\wedge c)$. so $x\le y$.
- (2)show $y \le x$.
  - $y \le b\wedge c$, So $y\le b$; $y \le b\wedge c \le c$, then $y \le c$; and $y \le a$.
  - $y \le a\wedge b$, then $y \le (a\wedge b)\wedge c$. so $y \le x$.
- (3)antisymeric, $x=y$.

$x\le a\wedge b \Rightarrow x\le a$, $x\le b$ 性质

$x\le c$. $x\le b\wedge c$

同相 $x=y$ $x\le y$ ✓

Proof $a*b = a \vee b$ is associative

- Let $x=(a\vee b)\vee c$, $y=a\vee(b\vee c)$.

$y \le x$

- (1) show $y\le x$
  - $a\vee b \le x$, So $a \le a\vee b \le x$, then $a \le x$; $b \le a \vee b \le x$, then $b \le x$; and $c \le x$.
  - $b \vee c \le x$, then $a \vee (b \vee c) \le x$. so $y\le x$.
- (2)show $x\le y$.
  - $b \vee c \le y$, So $b \le b\vee c \le y$, then $b \le y$; $c \le b\vee c \le y$, then $c \le y$; and $a\le y$.
  - $a\vee b \le y$, then $(a\vee b)\vee c \le y$. so $x\le y$.
- (3)antisymeric, $x=y$.

Identity(单位元) for an operation

- An elemnt *e* in A is called an identity element if $\forall a \in A$, then
  - $a * e = e * a = a$.

单位元

$\boxed{a * e = e * a = a}$

- Note:
  - In fact, an identity for an operation must be unique.

Theorem 1

- If e is an identity for a binary operation *, then e is unique.
- Proof
  - Assume another object i also has the identity property, so $x * i = i * x = x$.
  - Then $e * i = e$, but since e is an identity for *,

    $i * e = e * i = i$.
  - Thus, $i = e$.
- There is <u>at most one</u> object with the identity property for a binary operation.

identity 单位元

Inverse（逆元）

inverse 逆元

- An element $a' \in A$ is called an inverse of a and written as a^{-1} if
  - $a * a' = a' * a = e$, *or*
  - $a * a^{-1} = a^{-1} * a = e$.

$a * a' = a' * a = e$,

$a * a^{-1} = a^{-1} * a = e$

- Theorem 2: If $*$ is an associative operation and x has an inverse y, then y is unique.

x有一个逆元

Inverse（逆元）

- Theorem 2: If $*$ is an associative operation and x has an inverse y, then y is unique.
- Proof
  - Assume there is another inverse for x, say z.
  - Then $(z * x) * y = e * y = y$ and $z * (x * y) = z * e = z$.
  - Since $*$ is associative, $(z * x) * y = z * (x * y)$ and so $y = z$.

Example 11

- (a) In the structure [3×3 matrices, +, *, ^{T}] , each matrix $\boldsymbol{A} = [\ a_{ij}\ ]$ has a inverse $-\boldsymbol{A} = [\ -a_{ij}\ ]$.
- (b) In the structure [integers, +, *], only the integers 1 and -1 have multiplicative inverses.

An example:Algebraic Lattice

- Let * be a binary operation on a set A, and suppose that * satisfies the following properties for any a, b, and c in A:
  - $a = a*a$
  - $a*b = b*a$
  - $a*(b*c) = (a*b)*c$
- Define a relation $\leq$ on A by
  - $a \leq b$ if and only if $a = a*b$.
- Show that $(A, \leq)$ is a poset, and for all a, b in A, GLB$(a, b) = a*b$.

Proof (1)

- We must show that $\boxed{a*b} = a \wedge b$
  - $\leq$ is reflexive, antisymmetric and transitive.
  - $a*b = a \wedge b$ for all a and b in A.
- (1) $\leq$ is reflexive : 最大下界
  - a $\leq$ b if and only if a = a*b
  - Since a = a*a, a $\leq$ a for all a in A.
  - So $\leq$ is reflexive.

Proof (2)

- (2) $\leq$ is antisymmetric:
  - $a \leq b$ if and only if $a = a*b$
- Now suppose that
  - $a \leq b$ and $b \leq a$.
  - Then, by definition and property 2,
  - $a = a*b$, $b= b*a$, and $a*b = b*a$,
  - so $a = b$.
  - Thus $\leq$ is antisymmetric.

Proof (3)

- (3) $\leq$ is transitive:
  - $a \leq b$ if and only if $a = a*b$
- If $a \leq b$ and $b \leq c$,
  - then $a = a*b = a*(b*c) = (a*b)*c = a*c$,
  - so $a \leq c$.
  - Then $\leq$ is transitive.

proof (4)

- (4) $a*b = a \wedge b$, for all a and b in A :
- 1. $a*b$ is a lower bound for a and b.
  - $a*b = a*(b*b) = (a*b)*b$, so $a*b \leq b$.
  - $a*b = (a*a)*b = a*(a*b) = (a*b)*a$, so $a*b \leq a$.
  - so $a*b$ is a lower bound for a and b.
- 2. if $c \leq a$ and $c \leq b$, then $c \leq a*b$
  - $c = c*a$ and $c = c*b$.
  - Thus $c = (c*a)*b = c*(a*b)$.
  - so $c \leq a*b$.
- Therefore, $a*b$ is the greatest lower bound of a and b.

Homework

- 20,24,28@323-324