Abstract Algebra

Zhang Yanmei

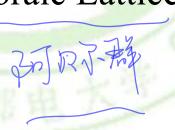
ymzhang@bupt.edu.cn

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

1

Content

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



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.

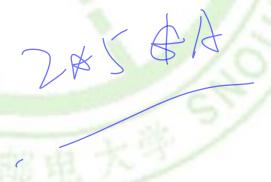


- It's customary to denote binary operations by a symbol such as *.
 - a*b instead of *(a,b)
 - * : multiplication
 - $\rightarrow a*b$: the product of a and b.
- A is closed under the operation * ,if a and b are elements in A, $a*b \in A$.

arb the product of a one of

- 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.

- Let $A = \mathbb{Z}^+$. 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, $2*5 \notin A$.



- Let $A = \mathbb{Z}$. Define a*b as a number less than both a and b.
 - * 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, 1, and so on.
 - in this case, * would be a relation from $A \times A$ to A, but not a function

Example 5,6

- marx fa, 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.

NAD EA

 $\int -32\%$

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 $a \land b$.
 - \blacksquare * is a binary operation on L.
 - This is also true of $a \lor b$

Operation table运算表 蓝纹

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

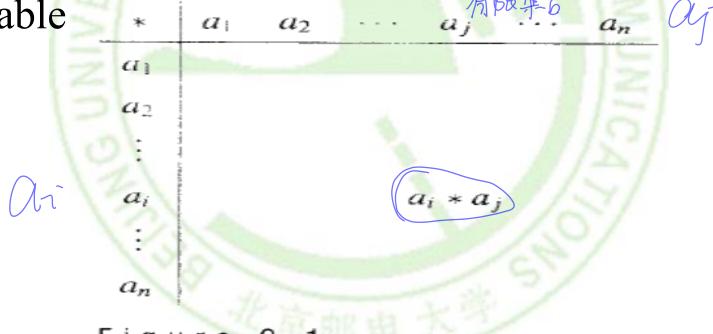


Figure 9.1

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

| | 0 | 1 | 1 | \wedge | 0 | 1 |
|---|---|---|---|----------|---|---|
| 0 | 0 | 1 | | 0 | 0 | 0 |
| 1 | 1 | 1 | | 1 | 0 | 1 |

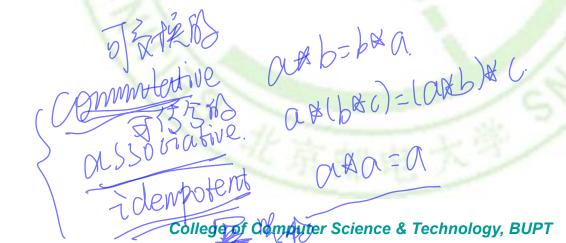
How many operations?

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

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*





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

| * | a | b | С | d | * | a | b | į · | đ |
|---|---|-----|---|---|---|---|------------|-------------|-----------------------|
| | a | _, | | | | | ϵ | | 3r - 3 - 3 |
| | b | | | | | | d | | |
| | C | | | | C | b | b | \tilde{a} | C |
| d | a | a | b | b | d | d | a | Ĉ | d |
| | | (a) | | | | | (b) | | , |



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





(arb)rc=arlb^c)

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

- Let $x = (a \land b) \land c$, $y = a \land (b \land c)$.
- (1) show $x \le y$
 - $x \le a \land b \text{, So } x \le a \land b \le a \text{, then } x \le a; x \le'$ $a \land b \le b \text{, then } x \le b; \text{ and } x \le c.$ $x \le a \land b \le b \text{, then } x \le b; \text{ and } x \le c.$
 - $x \le b \land c$, then $x \le a \land (b \land c)$, so $x \le y$.
- (2)show $y \leq x$.
 - $y \le b \land c$, So $y \le b$; $y \le b \land c \le c$, then $y \le c$; and $y \le a$.
 - $y \le a \land b$, then $y \le (a \land b) \land c$. so $y \le x$.
- (3) antisymeric, x=y. $x \le 0$

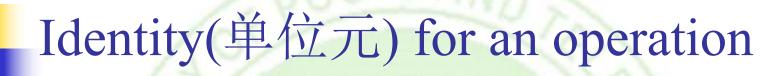
800 X=4

XEC.

XE PUC

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

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



- An elemnt e in A is called an identity element if $\forall a \in A$, then
 - a * e = e * a = a
- Note:
 - In fact, an identity for an operation must be unique.

axe= exa=a

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 at most one object with the identity property for a binary operation.



identity 单流 Inverse (逆元) inverse 遠元

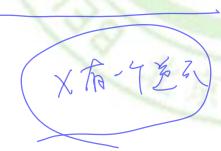
An element $a' \in A$ is called an inverse of a and written as a^{-1} if

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

$$\alpha * \alpha' = \alpha' * \alpha = e$$
,
 $\alpha * \alpha^{-1} = \alpha^{-1} * \alpha = e$

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

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



Inverse(逆元)

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

- (a) In the structure $[3 \times 3 \text{ matrices}, +, *, ^T]$, each matrix $A = [a_{ij}]$ has a inverse $-A = [-a_{ij}]$.
- (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
 - $a \le b$ 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



- \leq is reflexive, antisymmetric and transitive.
- $a*b = a \land b$ for all a and b in A.
- (1) ≤ is reflexive:
 - $a \le b$ if and only if a = a*b
 - Since a = a*a, $a \le a$ for all a in A.
 - So \leq is reflexive.

Proof (2)

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

Proof (3)

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

proof (4)

- (4) $a*b = a \land b$, 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 $a*b \le b$.
 - a*b = (a*a)*b = a*(a*b) = (a*b)*a, so $a*b \le a$.
 - so a*b is a lower bound for a and b.
- 2. if $c \le a$ and $c \le b$, then $c \le a*b$
 - c = c*a and c = c*b.
 - Thus c = (c*a)*b = c*(a*b).
 - so $c \le a * b$.
- Therefore, a*b is the greatest lower bound of a

Homework

20,24,28@323-324