DISCRETE MATHEMATICS
（离散数学）

云南大学数学系
李 建 平

Chapter 9 Semigroups and Groups

9.1 Binary Operations Revisited

9.2 Semigroups

9.3 Products and Quotients of Semigroups

9.4 Groups

9.5 Products and Quotients of Groups

9.1 BINARY OPERATIONS REVISITED

A **binary operation** on a set A is an everywhere defined function $f : A \times A \rightarrow A$. Observe the following properties that a binary operation must satisfy:

1. Since Dom(*f*)=$A \times A$, *f* assigns element $f(a,b)$ of A to each ordered pair(a,b)in $A \times A$. That is, the binary operation must be defined for each ordered pair of elements of A.

2. Since a binary operation is a function, only one

element of A is assigned to each ordered pair.

Thus we can say that a binary operation is a rule that assigns to each ordered pair of elements of A a unique element of A.

It is customary to denote binary operations by a symbol such as $*$, instead of f, and to denote the element assigned to (a,b) by $a*b$ [instead of $*(a,b)$]. If a and b are elements in A, then $a*b \in A$, and this property is often described by saying that A is **closed** under the operation $*$.

EXAMPLE 1 Let $A = Z$. Define $a * b$ as $a + b$. Then $*$ is a binary operation on Z.

EXAMPLE 5

Let $A = Z$. Define $a * b$ as $\max\{a, b\}$. Then $*$ is a binary operation.

EXAMPLE 6

Let $A = P(S)$, for some set S. If V and W are subsets of S, define $V * W$ as $V \cup W$. Then $*$ is a binary operation on A. Moreover, if we define $V *' W$ as $V \cap W$, then $*'$ is another binary operation on A.

EXAMPLE 7

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

- Tables

If $A = \{a_1, a_2, \cdots, a_n\}$ is a finite set, we can define a binary operation of A by means of a table as shown in Figure 9.1. The entry in position i , j denotes the element $a_i * a_j$.

$$
\begin{array}{c|ccccc}
* & a_1 & a_2 \ldots & a_j & \ldots & a_n \\
\hline
a_1 & & & & & \\
a_2 & & & & & \\
\vdots & & & & & \\
a_i & & & a_i * a_j & & \\
\vdots & & & & & \\
a_n & & & & &
\end{array}
$$

Figure 9.1

If $A=\{a,b\}$, we shall determine the number of binary operations that can be defined on A .

Every binary operation $*$ on A can be described by a table

$*$	a	b
a		
b		

Since every blank can be filled in with the element a or b , we conclude that there are

$2 \cdot 2 \cdot 2 \cdot 2 = 2^4$ or 16 ways to complete the table.

Thus, there are 16 binary operations on A .

- Properties of Binary Operations

A binary operation on a set A is said to be **commutative**（交换）if

$$a * b = b * a$$

for all elements a and b in A

A binary operation that is described by a table is commutative if and only if the entries in the table are symmetric with respect to the main diagonal.

A binary operation $*$ on a set A is said to be

associative（结合） if

$$a*(b*c)=(a*b)*c$$

for all elements a , b , and c in A .

EXAMPLE 16

Let $*$ be a binary operation on a set A , and suppose that $*$ satisfies the following properties for any a , b , and c in A.

1. $a=a*a$ Idempotent property (幂等)
2. $a*b=b*a$ Commutative property
3. $a*(b*c)=(a*b)*c$ Associative property

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$(a,b) = a * b$.

Solution: By the definition of the binary on the set A.

9.2 SEMIGROUPS（半群）

A **semigroup** is a nonempty set *S* together with an associative binary operation * defined on *S*. We shall denote the semigroup by $(S,*)$ or *S*. We also refer to $a*b$ as the **product** of a and b.

The semigroup $(S,*)$ is said to be commutative if $*$ is a commutative operation.

EXAMPLE 2

The set $P(S)$, where S is a set, together with the operation of union is a commutative semigroup.

EXAMPLE 6

Let $A=\{x_1,x_2,\cdots,x_n\}$ be a nonempty set. A^* is the set of all finite sequences of elements of A. If $\alpha=a_1a_2\cdots a_n$ and $\beta=b_1b_2\cdots b_k$, then $\alpha\cdot\beta=a_1a_2\cdots a_nb_1b_2\cdots b_k$. It is easy to see that if α, β, and γ are any elements of A^*, then

$$\alpha\cdot(\beta\cdot\gamma)=(\alpha\cdot\beta)\cdot\gamma$$

So that $\cdot$ is an associative binary operation, and $(A^*,\cdot)$ is a semigroup. The semigroup $(A^*,\cdot)$ is called the **free semigroup**（自由半群）generated by A.

Theorem 1

If $a_1, a_2, \cdots, a_n$, $n \geq 3$, are arbitrary elements of a semigroup, then all products of the elements $a_1, a_2, \cdots, a_n$ that can be formed by inserting meaningful parentheses arbitrarily are equal.

If $a_1, a_2, \cdots, a_n$ are elements in a semigroup $(S, *)$, we shall write their product as

$$a_1 * a_2 * \cdots * a_n$$

omitting the parentheses.

An element e in a semigroup $(S, *)$ is called an **identity** element（幺元素、单位元素）if

$$e * a = a * e = a$$

for all $a \in S$.

A **monoid**（含幺半群）is a semigroup $(S,*)$ that has an identity.

Let $(S,*)$ be a semigroup and T a subset of S. If T is closed under the operation $*$(that is, $a*b \in T$ whenever a and b are elelments of T), then $(T,*)$ is called a **subsemigroup** of $(S,*)$. Similarly, let $(S,*)$ be a monoid with identity e , and let T be a nonempty subset of S . If T is closed under the operation $*$ and $e \in T$, then $(T,*)$ is called a **submonoid**（含幺子半群）of $(S,*)$.

Suppose that $(S,*)$ is a semigroup, and let $a \in S$. For $n \in Z^+$, we define the powers of a^n recursively as follows:

$$a^1 = a, a^n = a^{n-1} * a, n \geq 2.$$

Moreover, if $(S,*)$ is a monoid, we also define

$$a^0 = e.$$

It can be shown that if m and n are nonnegative integers, then

$$a^m * a^n = a^{m+n}.$$

- Isomorphism (同构) and Homomorphism (同态)

Let $(S,*)$ and $(T,*')$ be two semigroups. A function

$f: S \to T$ is called an **isomorphism** (同构) from $(S, *)$ to $(T, *')$ if it is a one-to-one correspondence from S to T, and if

$$f(a * b) = f(a) *' f(b)$$

for all a and b in S.

If f is an isomorphism from $(S, *)$ to $(T, *')$, f^{-1} exists and is a one-to-one correspondence from T to S. We now show that f^{-1} is an isomorphism from $(T, *')$ to $(S, *)$. Let a' and b' be any elements of T. Since f is onto, we can find elements a and b in S such that $f(a) = a'$ and $f(b) = b'$. Then $a = f^{-1}(a')$ and

$b = f^{-1}(b')$. Now we have

$$f^{-1}(a' * b')$$

$$= f^{-1}(f(a) *' f(b))$$

$$= f^{-1}(f(a * b))$$

$$= (f^{-1} \circ f)(a * b)$$

$$= a * b$$

$$= f^{-1}(a') * f^{-1}(b')$$

Hence f^{-1} is an isomorphism.

We now say that the semigroup $(S, *)$ and $(T, *')$

are **isomorphic** and we write $S \simeq T$.

To show that two semigroups $(S,*)$ and $(T,*')$ are isomorphic, we use the following procedure:

Step 1: Define a function $f: S \to T$ with

$$\operatorname{dom}(f) = S .$$

Step 2: Show that f is one-to-one.

Step 3: Show that f is onto.

Step 4: Show that $f(a*b) = f(a)*' f(b)$.

EXAMPLE 18

Let $S = \{a,b,c\}$ and $T = \{x,y,z\}$. It easy to verify that the following operation tables give semigroup structures for S and T, respectively.

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

$*$	x	y	z
x	z	x	y
y	x	y	z
z	y	z	x

Let

$$f(a) = y$$

$$f(b) = x$$

$$f(c) = z$$

Replacing the elements in S by their images and rearranging the table, we obtain exactly the table for T. Thus S and T are isomorphic.

Theorem 2

Let $(S,*)$ and $(T,*')$ be monoids with identities e and e', respectively. Let $f:S\rightarrow T$ be an isomorphism. Then $f(e)=e'$.

Let $(S,*)$ and $(T,*')$ be two semigroups. An everywhere-defined function $f:S\rightarrow T$ is called a **homomorphism** (同态) from $(S,*)$ to $(T,*')$ if

$$f(a*b)=f(a)*'f(b)$$

for all a and b in S. If f is also onto, we say that T is a **homomorphic image** (同态像) of S.

Theorem 3

Let $(S,*)$ and $(T,*')$ be monoids with identities e and e', respectively. Let $f: S \to T$ be a homomorphism from $(S,*)$ onto $(T,*')$. Then $f(e)=e'$.

Theorem 4

Let f be a homomorphism from a semigroup $(S,*)$ to a semigroup $(T,*')$. If S' is a subsemigroup of $(S,*)$, Then $f(S')=\{t\in T \mid t=f(x)$ for some $s\in S'\}$, the image of S' under f, is a subsemigroup of $(T,*')$.

Theorem 5

If f is a homomorphism from a commutative semigroup $(S, *)$ onto a semigroup $(T, *')$, then $(T, *')$ is also commutative.

9.3 PRODUCTS AND QUOTIENTS OF SEMIGROUPS

Theorem 1

If $(S,*)$ and $(T,*')$ are semigroups, then $(S\times T,*'')$ is a semigroups, where $*''$ is defined by $(s_1,t_1)*''(s_2,t_2)=(s_1*s_2,t_1*'t_2)$.

If S and T are monoids with identities e_S and e_T , respectively, then $S\times T$ is a monoid with identity (e_S,e_T).

An equivalence relation R on the semigroup $(S,*)$ is called a **congruence relation**（同余关系）if

$a\ R\ a'$ and $b\ R\ b'$ imply $(a*b)\ R\ (a'*b')$

EXAMPLE 1

Consider the semigroup $(Z,+)$ and the equivalence relation R on Z defined by

$a\ R\ b$ if and only if $a \equiv b$(mod 2).

We know that this relation is a congruence relation (同余关系或合同关系).

Theorem 2

Let R be a congruence relation on the semigroup $(S,*)$. Consider the relation $\circledast$ from $S/R \times S/R$ to S/R in which the ordered pair $([a],[b])$ is, for a and b

in S, related to $[a*b]$.

(a) $\circledast$ is function from $S/R \times S/R$ to S/R, and as usual we denote $\circledast$ $([a],[b])$ by $[a] \circledast [b]$. Thus $[a] \circledast [b] = [a*b]$.

(b) $(S/R, \circledast)$ is a semigroup.

We call S/R the **quotient semigroup**（商半群） or **factor semigroup**.

Theorem 3

Let R be a congruence relation on a semigroup $(S,*)$ and $(S/R,\circledast)$ the corresponding quotient semigroup. Then the function $f_R : S \rightarrow S/R$ defined by

$$f_R(a) = [a]$$

is an onto homomorphism, called the **natural homomorphism**（自然同态）.

9.4 GROUPS（群）

A **group** $(G, *)$ is a monoid, with identity e, that has the additional property that, for every element $a \in G$, there exists an element $a' \in G$ such that $a * a' = a' * a = e$. Thus a group is a set together with a binary operation $*$ on G such that

1. For any elements a, b, and c in G,

$$(a * b) * c = a * (b * c)$$

2. There is a unique element e in G such that

$$a * e = e * a \quad \text{for any } a \in G.$$

3. For every $a \in G$, there is an element $a' \in G$, called an inverse of a, such that

$$a * a' = a' * a = e.$$

Observe that if $(G, *)$ is a group, then $*$ is a binary operation, so G must be closed under $*$; that is $a * b \in G$ for any elements a and b in G.

We shall write the product $a * b$ of the elements a and b in the group $(G, *)$ simply as ab, and we shall also refer to $(G, *)$ simply as G.

A group G is said to be **Abelian** if $ab = ba$ for all elements a and b in G.

EXAMPLE 4

Let G be the set of all nonzero real numbers and let

$$a * b = \frac{ab}{2}$$

Show that $(G, *)$ is an Abelian group.

Theorem 1

Let G be a group. Each element a in G has only one inverse in G.

Theorem 2

Let G be a group and let a, b, and c be elements of G. Then

(a) $ab = ac$ implies that $b = c$ (**left cancellation property**，左消去律).

(b) $ba = ca$ implies that $b = c$ (**right cancellation property**，右消去律).

Theorem 3

Let G be a group and let a and b be elements of G. Then

(a) $(a^{-1})^{-1} = a$.

(b) $(ab)^{-1} = b^{-1}a^{-1}$.

Theorem 4

Let G be a group, and let a and b be elements of G. Then

(a) The equation $ax = b$ has a unique solution in G.

(b) The equation $ya = b$ has a unique solution in G.

If a group G has a finite number of elements, then its binary operation can be given by a table, which is generally called a **multiplication table**(乘法表). The multiplication table of a group $G = \{a_1, a_2, \cdots, a_n\}$ under the binary operation $*$ must satisfy the following properties:

1. The row labeled by e must be

$$a_1, a_2, \cdots, a_n$$

and the column labeled by e must be

$$\begin{matrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{matrix}$$

2. From Theorem 4, it follows that each element b of the group must appear exactly once in each row and column of the table. Thus each row and column is a permutation of the elements $a_1, a_2, \cdots, a_n$

of G, and each row (and each column) determines a different permutation.

If G is a group that has a finite number of elements, we say that G is a **finite group**, and the **order** of G is the number of elements $|G|$ in G.

If G is a group of order 1, then $G=\{e\}$, and we have $ee=e$. $G=\{e,a\}$ be a group of order 2. Then we obtain a multiplication table (Table 9.1).

Table 9.1

	e	a
e	e	a
a	a	

Table 9.2

	e	a
e	e	a
a	a	e

Next, let $G=\{e,a,b\}$ be a group of order 3. we can only complete the table as shown in Table 9.4.

Table 9.3

	e	a	b
e	e	a	b
a	a		
b	b		

Table 9.4

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

We next come to a group $G = \{e, a, b, c\}$ of order 4. It is not difficult to show that the possible multiplication table for G can be completed as shown in Tables 9.5 through 9.8.

Table 9.5

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Table 9.6

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

Table 9.7

	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

Table 9.8

	e	a	b	c
e	e	a	b	c
a	a	c	e	b
b	b	e	c	a
c	c	b	a	e

EXAMPLE 7

The set of all permutations of n elements is a group of order $n!$ under the operation of composition. This group is called the **symmetric group** (对称群) **on n letters** and is denoted by S_n.

We next turn to a discussion of important subsets of a group. Let H be a subset of a group G such that

(a) The identity e of G belongs to H.

(b) If a and b belongs to H, then $ab \in H$.

(c) If $a \in H$, then $a^{-1} \in H$.

Then H is called a **subgroup** of G. Part (b) says that H is a subsemigroup of G. Thus a subgroup of G can be viewed as a subsemigroup having properties (a) and (c).

Theorem 5

Let $(G,*)$ and $(G',*')$ be two groups, and let $f:G\to G'$ be a homomorphism from G to G'.

(a) If e is the identity in G and e' is the identity in G', then $f(e)=e'$.

(b) If $a\in G$, then $f(a^{-1})=(f(a))^{-1}$.

(c) If H is a subgroup of G, then

$$f(H)=\left\{f(h) \middle| h\in H\right\}$$

is a subgroup of G'.

The group with multiplication Table 9.5 is called the **Klein 4 group** and it is denoted by V, The one with multiplication Table 9.6, 9.7, or 9.8 is denoted by Z_4.

9.5 PRODUCTS AND QUOTIENTS OF GROUPS

Theorem 1

If G_1 and G_2 are groups, then $G = G_1 \times G_2$ is a group with binary operation defined by

$$(a_1, b_1)(a_2, b_2) = (a_1 a_2, b_1 b_2).$$

Theorem 2

Let R be congruence relation on the group $(G, *)$. Then the semigroup $(G/R, \circledast)$ is a group, where the operation $\circledast$ is defined on G/R by

$$[a] \circledast [b] = [a * b]$$ (see Section 9.3)

Let H be a subgroup of a group G, and let $a \in G$. The left **coset** (左培集) of H in G determined by a is the set $aH = \{ah | h \in H\}$. The right **coset** (右培集) of H in G determined by a is the set $Ha = \{ha | h \in H\}$. Finally, we say that a subgroup H of G is **normal** (正规的) if $aH = Ha$ for all a in G.

We note that if $aH = Ha$, it does not follow that, for $h \in H$ and $a \in G$, $ha = ah$. It does follows that $ha = ah'$, where h' is some element in H.

9.6 Other Mathematical Structures

- Rings

    Let S be a nonempty set with two binary operations $+$ and $*$ such that $(S,+)$ is an Abelian group and $*$ is distributive over $+$. The structure $(S,+,*)$ is called a ring if $*$ is associative, i.e., $(S,*)$ is a semigroup.

    Moreover, if $*$ is associative and commutative, then $(S,+,*)$ is called a commutative ring. If $(S,*)$ is a monoid, then $(S,+,*)$ is a ring with identity.

The identity for * is denoted by 1; the identity for + is denoted by 0.

Generally, we will refer to + and * as addition and multiplication even when they are not the usual operations with these names.

Example 1 Let S=Z, the set of all integers, and let + and * be the usual addition and multiplication of integers. Then (S,+,*) is a commutative ring with identity.

Theorem 1 Let R be a commutative ring with additive identity 0 and multiplicative identity 1. Then

(1) For any x in R, 0*x=0;

(2) For any x in R, -x=(-1)*x.

- **Fields**

Let (F,+,*) be a commutative ring with identity e. F is called a **field** if every nonzero element x in F has a multiplicative inverse.

Field Properties

The field (F,+,*) has two binary operations: an addition + and a multiplication *, and two special elements denoted as 0 and 1, so that for all x, y and z in F,

(1) $x+y=y+x$ (2) $x*y=y*x$

(3) $(x+y)+z=x+(y+z)$ (4) $(x*y)*z=x*(y*z)$

(5) $x+0 = x$ (6) $x*1 = x$

(7) $x*(y+z)=(x*y)+(x*z)$ (8) $(y+z)*x=(y*x)+(z*x)$

(9) For each x in F there is a unique element in F, denoted by –x, so that x+(-x)=0

(10) For each $x \neq 0$ in F there is a unique element in F, denoted by x^{-1}, so that

$x*x^{-1} = 1$.

Theorem 2 The ring Z_n is a field when n is a prime.

Theorem 3 (a) If $G=\{g_1,g_2,\ldots,g_n\}$ is a finite Abelian group with identity denoted by e, and x is any element of G, then $x^n=e$;

(b) (Fermat's Little Theorem) If p is a prime number, and GCD(a,p)=1, then $a^{p-1} \equiv 1 \pmod{p}$;

© If p is a prime number, and a is any integer, then $a^p \equiv a \pmod{p}$.

THE END