Semigroups and Groups
（半群与群）

Zhang Yanmei

ymzhang@bupt.edu.cn

College of Computer Science & Technology

Beijing University of Posts & Telecommunications

Content

- *Binary Operations and It's properties*
- *Free Semigroup (A*,.)* $(A^*, \cdot)$
- *An Abelian Group*
- *Theroems*
- *Finite Groups*
- *Group of order 1,2,and 3*
- *Group of order 4*
- *An Interesting Group:*
- *Permutation Group and Cyclic Group*

Definition

- Given a set G and a binary operation * on G. For any element a,b,and c in G,
  - Closure: $a*b \in G$
  - Associative: $(a*b)*c=a*(b*c)$
  - Identity: *a unique element* $e \in G$, *such that*

  $a*e=e*a=a$
  - Inverse: *an element* $a' \in G$ *of* a, *written as* a^{-1},*such that* $a*a^{-1} = a^{-1}*a = e$.
  - Commutative: $a*b=b*a$

Groupoid 广群

- A nonempty set G with a binary operation * is called Groupoid if for any element a,b in G,
  - Closure: $a*b \in G$

Semigroup 半群

- A nonempty set G with a binary operation * is called Semigroup if for any element a,b and c in G,
  - Closure: $a*b \in G$
  - Associative: $(a*b)*c=a*(b*c)$

半群

Monoid 独异点/含幺半群

- A nonempty set G with a binary operation * is called Semigroup if for any element a,b and c in G,
  - Closure: $a*b \in G$
  - Associative: $(a*b)*c=a*(b*c)$
  - Identity: *a unique element* $e \in G$, *such that*

$a*e=e*a=a$

Group 群

- A nonempty set G with a binary operation * is called Group if for any element a, b and c in G,
  - Closure: $a*b \in G$
  - Associative: $(a*b)*c=a*(b*c)$
  - Identity: *a unique element* $e \in G$, *such that* $a*e=e*a=a$
  - Inverse: *an element* $a' \in G$ *of* a, *written as* a^{-1}, *such that* $a*a^{-1} = a^{-1}*a = e$.

Abelian Groupoid

- A groupoid is called Abelian groupoid if for any element a,b in G, Commutative: $a*b=b*a$.
- A semigroup is called Abelian semigroup if for any element a,b in G, Commutative: $a*b=b*a$.
- A monoid is called Abelian monoid if for any element a,b in G, Commutative: $a*b=b*a$.
- A group is called Abelian group if for any element a,b in G, Commutative: $a*b=b*a$.

Theorem(Associativity)

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

Notice

- Theorem 1 shows that the products
  - $((a_1*a_2)*a_3)*a_4$
  - $a_1*(a_2*(a_3*a_4))$
  - $(a_1*(a_2*a_3))*a_4$
  - are all equal.
- If a_1, a_2,..., a_n are elements in a semigroup (S, *), then the product can be written as
  - $a_1*a_2*\ldots *a_n$

Examples

- $(Z, +)$
  - Z : the set of all integers.
  - $+$: ordinary addtion.
- $(Z, -)$
  - Z : the set of all integers.
  - $-$: ordinary subtraction.
- $(P(S), \cup)$
  - $P(S)$: the powerset of S.
  - $\cup$: union operation on sets

Example 5

- Let $(L, \leq)$ be a lattice. Define a binary operation on L by
  - $a*b = a \vee b$.

半群

封闭

结合

- Then L is a semigroup.

Semigroup

Free semigroup $(A^*,.)$

- Let $A = \{a_1, a_2,..., a_n\}$ be an alphabet.
  - *Let* A^* is the set of all finite sequences of elements of A.
  - α ,β and γ be elements of A^*.
- The catenation is a binary operation $\cdot$ on A^*.
  - if $\alpha = a_1a_2...a_s$ and $\beta = b_1b_2...b_t$
    - $\alpha \cdot \beta = a_1a_2...a_sb_1b_2...b_t$
  - if α, β, and γ are any elements of A^*,
    - $\alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$.

Theroem(Free semigroup)

- (A*, ·) is a semigroup.
- *called the free semigroup generated by A(由A生成的自由半群).*

An Abelian Group

- Example:
  - Let G be the set of all nonzero real numbers, and
  - $a*b=ab/2$
- Show $(G,*)$ is an abelian group.

Proof (1)

- $*$ is a binary operation
  - If a and b are elements of G,
  - then $ab/2$ is a nonzero real number and
  - hence is in G.
- associativity
  - $(a*b)*c = (ab/2)*c = (ab)c/4$
  - $a*(b*c) = a*(bc/2) = a(bc)/4 = (ab)c/4$.
  - $*$ is associative.

Proof(2)

- 2 is the identity.
  - $a*2 = (a)(2)/2 = a = (2)(a)/2 = 2*a$.
- $a' = 4/a$ is an inverse of a
  - $a*a' = a*4/a = a(4/a)/2 = 2 = (4/a)(a)/2 = (4/a)*a = a' *a$.
- Abelian
  - $a*b = ab/2 = ba/2 = b*a$
- So, G is an Abelian group.

Theorem(Uniqueness of Inverse)

- Let G be a group. Each element a in G has only one inverse in G.
- Proof
  - Let
    - a' and a'' be inverses of a.
  - Then
    - $a' = a'e = a'(aa'') = (a'a)a'' = ea'' = a''$.

Theorem(Left/Right Cancellation)

- Let
  - G be a group and
  - a, b, and c be elements of G.
- Then
  - $ab = ac$ implies that $b = c$
  - $ba = ca$ implies that $b = c$

Proof

- Left cancellation
  - Suppose that $ab = ac$.
  - $a^{-1}(ab) = a^{-1}(ac)$
  - $(a^{-1}a)b = (a^{-1}a)c$ by associativity
  - $eb = ec$ by the definition of an inverse
  - $b = c$ by definition of an identity.
- Right cancellation
  - The proof is similar to above.

Theorem(Inverse of Inverse)

- Let
  - G be a group and
  - a and b be elements of G.
- Then
  - $(a^{-1})^{-1} = a$.
  - $(ab)^{-1} = b^{-1}a^{-1}$

Proof

- $(a^{-1})^{-1} = a$
  - $a^{-1}a = aa^{-1} = e$
  - the inverse of an element is unique,
  - So, $(a^{-1})^{-1} = a$
- $(ab)^{-1} = b^{-1}a^{-1}$
  - $(ab)(b^{-1}a^{-1}) = a(b(b^{-1}a^{-1})) = a((bb^{-1})\, a^{-1}) = a(ea^{-1}) = aa^{-1} = e$
  - similarly, $(b^{-1}a^{-1})(ab) = e$
  - so $(ab)^{-1} = b^{-1}a^{-1}$

Theorem(Solution to Equation)

- Let
  - G be a group, and a and b be elements of G
- Then
  - The equation $ax = b$ has a unique solution in G.
  - The equation $ya = b$ has a unique solution in G.
- Proof is omitted

Finite group – 有限群

- If G is a group that has a finite number of elements, G is said to be a *finite group*, and the *order*(阶) of G is the number of elements $|G|$ in G.

元素个数为阶

- A finite group can be represented in the form of the multiplication table.

Group of order 1, 2

- If G is a group of order 1, then
  - $G = \{e\}$, and $ee = e$.
- Let $G = \{e, a\}$ be a group of order 2.
  - The blank can be filled in by e or by a?

Table 9.1

	e	a
e	e	a
a	a	

Table 9.2

	e	a
e	e	a
a	a	e

Nonisomorphic groups of order 3

- Let $G = \{e, a, b\}$ be a group of order 3.

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

Groups of order 4

- Let $G = \{e, a, b, c\}$ be a group of order 4

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

34

35

Example 5

- Let $B = \{0, 1\}$, and let $+$ be the operation defined on B as follows:

$+$	0	1
0	0	1
1	1	0

- Then B is a group.

An interesting group

- Given the equilateral triangle with vertices l, 2, and 3
- Consider it’s symmetries.

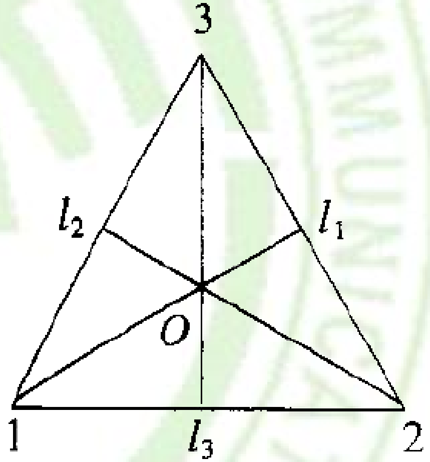


Figure 9.3

Symmetries of the triangle

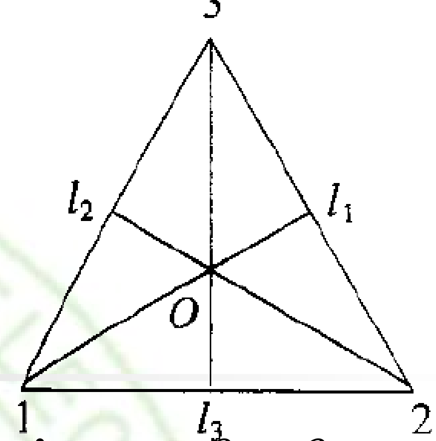


Figure 9 3

- There are counter-clockwise rotations f_2, f_3, f_1 of the triangle about O through 120º, 240º, 360º(or 0º) respectively.
- f_1, f_2, f_3 can be written as the permutations.

$$f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Symmetries of the triangle

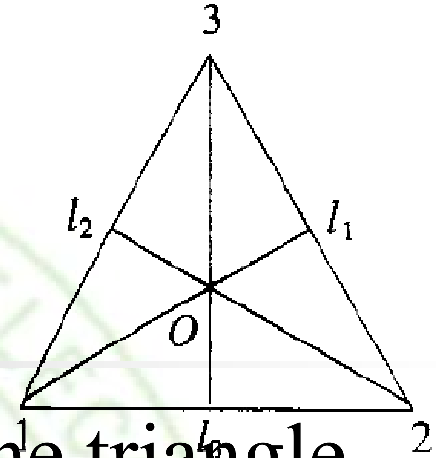


Figure 9.3

- Three additional symmetries of the triangle are g_1, g_2, and g_3, by reflecting about the lines l_1, l_2, and l_3, respectively.
- Denote these reflections as the following permutations:

$$g_1=\begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}, g_2=\begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}, g_3=\begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}$$

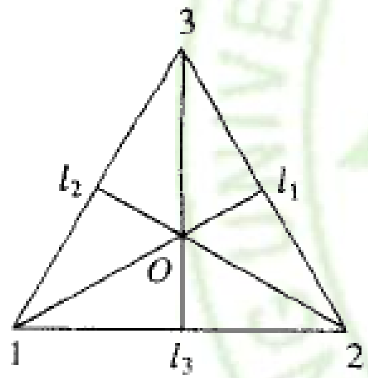
Group of symmetries of the triangle

- Let $S_3 = \{f_1, f_2, f_3, g_1, g_2, g_3\}$ and the operation *, *followed by*, on the set S_3 is defined as follows:

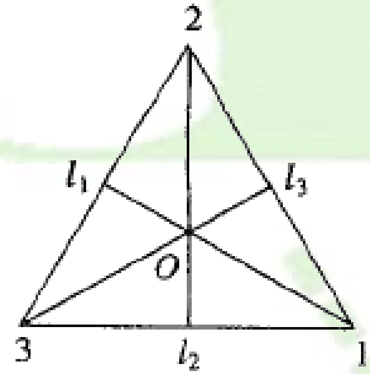
$*$	f_1	f_2	f_3	g_1	g_2	g_3
f_1	f_1	f_2	f_3	g_1	g_2	g_3
f_2	f_2	f_3	f_1	g_3	g_1	g_2
f_3	f_3	f_1	f_2	g_2	g_3	g_1
g_1	g_1	g_2	g_3	f_1	f_2	f_3
g_2	g_2	g_3	g_1	f_3	f_1	f_2
g_3	g_3	g_1	g_2	f_2	f_3	f_1

Compute $f_2 * g_2$ geometrically

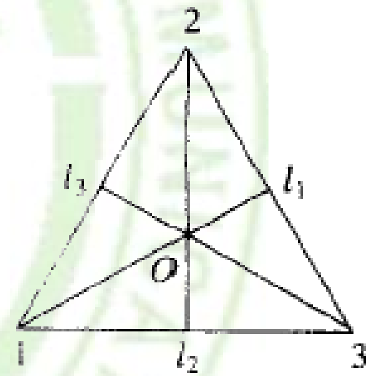
- We can compute $f_2 * g_2$ geometrically by roating and flipping the triangle.



Given triangle



Triangle resulting after applying f_2



Triangle resulting after applying g_2 to the triangle at the left

Compute $f_2 * g_2$ algebraically

- To compute $f_2 * g_2$ algebraically, we compute $f_2 \circ g_2$ (composition of functions).

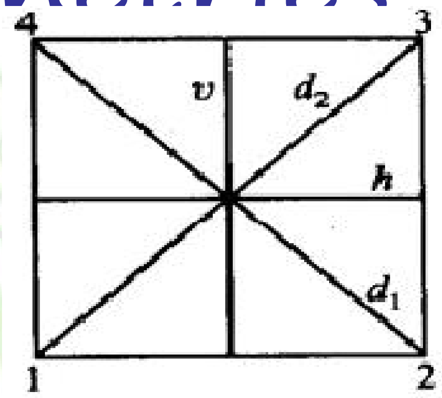
$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = g_1$$

- Therefore $f_2 * g_2 = g_1$.

Permutation Group

- 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 on n letters* (*n*次对称群) and is denoted by S_n.
- permutation group(置换群): a group with some permutations of n elements.

S4 Group of symmetries of the squre



$$f_1=\begin{pmatrix}1234\\1234\end{pmatrix}\quad f_2=\begin{pmatrix}1234\\2341\end{pmatrix}\quad f_3=\begin{pmatrix}1234\\3412\end{pmatrix}$$

$$f_4=\begin{pmatrix}1234\\4123\end{pmatrix}\quad f_5=\begin{pmatrix}1234\\2143\end{pmatrix}\quad f_6=\begin{pmatrix}1234\\4321\end{pmatrix}$$

$$f_7=\begin{pmatrix}1234\\3214\end{pmatrix}\quad f_8=\begin{pmatrix}1234\\1432\end{pmatrix}$$

S4 Group of symmetries of the squre

$\circ$	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8
f_1	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8
f_2	f_2	f_3	f_4	f_1	f_8	f_7	f_5	f_6
f_3	f_3	f_4	f_1	f_2	f_6	f_5	f_8	f_7
f_4	f_4	f_1	f_2	f_3	f_7	f_8	f_6	f_5
f_5	f_5	f_7	f_6	f_8	f_1	f_3	f_2	f_4
f_6	f_6	f_8	f_5	f_7	f_3	f_1	f_4	f_2
f_7	f_7	f_6	f_8	f_5	f_4	f_2	f_1	f_3
f_8	f_8	f_5	f_7	f_6	f_2	f_4	f_3	f_1

Carley's Group Theroem

- Every Finite Group of order *n* can be represented as a Permutation Group on n letters.

Homework

- 12,16 @348
- Ex1. Let G be a group. For $a,b \in G$,we say that b is conjugate to a,written by $b \sim a$, if there exist $g \in G$ such that $b=gag^{-1}$.show that is a equivalence relation on G. The equivalence classes of are called the conjugacy classes of G.
- Ex2. Let G be a group, and suppose that a *and* b are any elements of G. Show that if $(ab)^2=a^2b^2$,then $ba=ab$.
- Ex3: Let $G = \{x \in R | x>1\}$ be the set of all real numbers greater than 1. For $x,y \in G$,define $x*y=xy-x-y+2$. Show that $(G,*)$ is a group.