

New Algebras from Old Ones



Zhang Yanmei

ymzhang@bupt.edu.cn

College of Computer Science & Technology

Beijing University of Posts &
Telecommunications

New Algebras from Old Ones

- Subalgebra
- Product Algebra
- Quotient Algebra



Subalgebras

Definition:

- Let $(G, *)$ be a semigroup, T be a ~~nonempty~~ subset of G .
- $(T, *)$ is called a *subsemigroup* of G
 - if T is closed under the operation $*$.
- Example
 - (\mathbb{Z}, \times) and (\mathbb{E}, \times)
 - $(\mathbb{Z}, +)$ and $(\mathbb{E}, +)$



Subalgebras

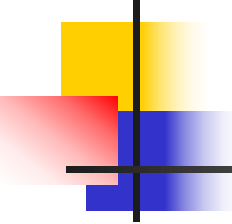
Definition:

- Let $(G, *)$ be a monoid, T be a nonempty subset of G .
- $(T, *)$ is called a *submonoid* of G
 - if T is subsemigroup and $e \in T$.
- Example
 - (\mathbb{Z}, \times) and (\mathbb{E}, \times)
 - $(\mathbb{Z}, +)$ and $(\mathbb{E}, +)$



Subalgebras

- 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 belong to H , then $a*b \in H$.
 - (c) If $a \in H$, then $a^{-1} \in H$.
- Then H is called a *subgroup* of G .



Trivial subgroups

- Let G be a group.
- Then G and $H = \{e\}$ are subgroups of G , called the *trivial subgroups* (平凡子群) of G .



Subgroup of S_3

- Consider S_3 , the group of symmetries of the equilateral triangle.
- $H = \{f_1, f_2, f_3\}$ is a subgroup of S_3 .

*	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



Definition (powers of a)

- Let
 - G be a semigroup, monoid, or group
 - $a \in G$.
- Define
 - a^n as $aa...a$ (n factors), for $n \in \mathbb{Z}^+$
 - a^0 as e , *in case of monoid.*
 - a^{-n} as $a^{-1}a^{-1}... a^{-1}$ (n factors), *in case of group.*



Theroem

- if n and m are any integers, then $a^n a^m = a^{n+m}$.
- Example:
 - It is easy to show that
 - $H = \{a^i \mid i \in \mathbb{Z}^+\}$ is a subsemigroup of G .
 - $H = \{a^i \mid i \in \mathbb{Z}^+ \text{ or } i=0\}$ is a submonoid.
 - $H = \{a^i \mid i \in \mathbb{Z}\}$ is a subgroup of G .(generated by a)



Theroem

- *Let $(G, *)$ be a group, H be a nonempty subset of G .*
- *If $\forall a, b \in H$ implies $a^{-1} * b \in H$,*
- *Then*
 - *H is a subgroup of G .*



*If $\forall a, b \in H$ implies $a^{-1} * b \in H$*

■ *Proof:*

■ *1. show $e \in H$.*

■ *If $\forall a \in H$, then $a^{-1} * a \in H$, $a^{-1} * b = e$, so $e \in H$.*

■ *2. show $\forall a \in H$ implies $a^{-1} \in H$.*

■ *If $\forall a \in H$, (1) $e \in H$, then $a^{-1} * e \in H$, $a^{-1} * e = a^{-1}$, so $a^{-1} \in H$.*

■ *3. show H is closed in $*$.*

■ *If $\forall a, b \in H$, (2) $a^{-1} \in H$, then $(a^{-1})^{-1} * b \in H$,*

■ *$(a^{-1})^{-1} * b = a * b$, so $a * b \in H$.*

New Algebras from Old Ones

- Subalgebra
- **Product Algebra**
- Quotient Algebra



Theroem

- *If $(S, *)$ and $(T, *')$ are semigroup(monoid, group), Then $(S \times T, *'')$ is a semigroup(monoid, group), where $''$ is defined by*
 - $(s1, t1) *'' (s2, t2) = (s1 * s2, t1 *' t2).$
- *Proof*
 - *Omitted.*


$$(Z_n, \oplus)$$

- $(Z, +)$ is a group,
- $a R b$ if and only if $a \equiv b \pmod{n}$, R is an equivalence relation.
- Z/R is $Z / \equiv \pmod{n} = \{[0], [1], \dots, [n-1]\}$, denoted by Z_n .
- (Z_n, \oplus) is defined by $[a] \oplus [b] = [a+b]$.
- \oplus is associative, $[0]$ is an identity, $[n-a]$ is the inverse of $[a]$. So (Z_n, \oplus) is an Abelian group.


$$(\mathbb{Z}_2, \oplus)$$

\oplus	[0]	[1]
[0]	[0]	[1]
[1]	[1]	[0]



$$\mathbb{Z}_2 \times \mathbb{Z}_2$$

- Let G_1 and G_2 be the group \mathbb{Z}_2 .
- For simplicity of notation, we shall write the elements of \mathbb{Z}_2 as $\bar{0}$ and $\bar{1}$, respectively, instead of $[0]$ and $[1]$.
- Then the multiplication table of $G = G_1 \times G_2$ is given in Table.

Table 9.10 Multiplication Table of $\mathbb{Z}_2 \times \mathbb{Z}_2$

	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{1})$
$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{1})$
$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{1})$
$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{0})$
$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{0})$

 B^n

- Let $B = \{0, 1\}$ be the group with $+$ defined as bellow

$+$	0	1
0	0	1
1	1	0

- Then $B^n = B \times B \times \dots \times B$ (n factors) is a group with operation \oplus defined by
 - $(x_1, x_2, \dots, x_n) \oplus (y_1, y_2, \dots, y_n) = (x_1 + y_1, x_2 + y_2, \dots, x_n + y_n)$.
- The identity of B^n is $(0, 0, \dots, 0)$, and every element is its own inverse.

New Algebras from Old Ones

- Subalgebra
- Product Algebra
- Quotient Algebra



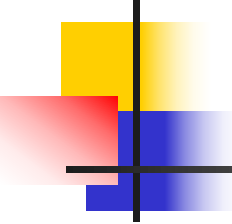
Congruence relation 同余关系

- An equivalence relation R on the groupoid(semigroup,monoid,group) $(S, *)$ is called a *congruence relation*
- if $a R a'$ and $b R b'$ imply $(a*b) R (a' * b')$.



Example 1

- Consider the semigroup $(\mathbb{Z}, +)$ and the relation R on \mathbb{Z} defined by
 - $a R b$ *if and only if* $a \equiv b \pmod{2}$.
 - If $a \equiv b \pmod{2}$, then $2|(a-b)$.
- Show that this relation is a congruence relation.



Example 1 – Proof

- R is an equivalence relation (omitted).
- R is a congruence relation
 - If $a \equiv b \pmod{2}$ and $c \equiv d \pmod{2}$
 - $2 \mid a-b$ and $2 \mid c-d$.
 - So $a-b = 2m$ and $c-d = 2n$, where m and n are integers.
 - $(a-b) + (c-d) = 2m + 2n$
 - $(a+c) - (b+d) = 2(m+n)$,
 - so $a+c \equiv b+d \pmod{2}$.
 - Hence the relation is a congruence relation.



Non-congruence relation

- Consider the group $(\mathbb{Z}, +)$
 - $f(x) = x^2 - x - 2$.
- Define
 - $a R b$ *if and only if* $f(a) = f(b)$.
- It is easy to verify that R is an equivalence relation, but R is not a congruence relation
 - $-1 R 2$, since $f(-1) = f(2) = 0$
 - $-2 R 3$, since $f(-2) = f(3) = 4$
 - but $(-1 + -2) \text{ not } R (2 + 3)$, since $f(-3) = 10 \neq f(5) = 18$



Note

- Recall that an equivalence relation R on the semigroup $(S, *)$ determines a partition of S .
 - Let $[a] = R(a)$ be the equivalence class containing a .
 - S/R is called *quotient set*, the set of all equivalence classes.



Quotient groupoid (商广群)

- Let R be a congruence relation on the groupoid $(G, *)$.
- \otimes be a relation from $G/R \times G/R$ to G/R in which the ordered pair $([a], [b])$ is related to $[a*b]$ for $a, b \in G$,
- Then
 - $\otimes([a], [b]) = [a] \otimes [b] = [a*b]$, is a function from $S/R \times S/R$ to S/R
 - So, $(S/R, \otimes)$ is a groupoid.
 - called the *quotient groupoid* or *factor groupoid*.



Proof

- \otimes is a binary operation
 - Suppose that $([a], [b]) = ([a'], [b'])$.
 - $a R a'$ and $b R b'$,
 - $a * b R a' * b'$, since R is a congruence relation.
 - Thus $[a * b] = [a' * b']$;
 - \otimes is a function, is a binary operation on S/R .
- Hence G/R is a groupoid.



Corollary

- Let
 - R be a congruence relation on the groupoid $(G, *)$,
 - G/R is the quotient groupoid,
- Then
 - If G is a semigroup (monoid, group), So is the $(G/R, \otimes)$.



Proof

- If $*$ is associative, so is \otimes .
 - $[a] \otimes ([b] \otimes [c]) = [a] \otimes [b * c] = [a * (b * c)] = [(a * b) * c] = [a * b] \otimes [c] = ([a] \otimes [b]) \otimes [c]$.
- If e is the identity in G , $[e]$ is the identity in G/R .
 - $[a] \otimes [e] = [a * e] = [a] = [e * a] = [e] \otimes [a]$.
- If a^{-1} is the inverse of a in G , then $[a^{-1}]$ is the inverse of $[a]$ in G/R .
 - $[a^{-1}] \otimes [a] = [a^{-1} * a] = [e] = [a * a^{-1}] = [a] \otimes [a^{-1}]$.



Z_4

- $(\mathbb{Z}, +)$ is a group,
 - $a R b$ *if and only if* $a \equiv b \pmod{n}$.
 - R is an equivalence relation
- $\equiv \pmod{4}$ is a congruence relation
 - $[0] = \{\dots, -8, -4, 0, 4, 8, 12, \dots\} = [4] = [8] = \dots$
 - $[1] = \{\dots, -7, -3, 1, 5, 9, 13, \dots\} = [5] = [9] = \dots$
 - $[2] = \{\dots, -6, -2, 2, 6, 10, 14, \dots\} = [6] = [10] = \dots$
 - $[3] = \{\dots, -5, -1, 3, 7, 11, 15, \dots\} = [7] = [11] = \dots$

Theroem

- $\mathbb{Z}/\equiv (\text{mod } 4)$ or \mathbb{Z}_4 is a group with
 - identity $[0]$
 - operation $[a] \oplus [b] = [a+b]$.

\oplus	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$
$[1]$	$[1]$	$[2]$	$[3]$	$[0]$
$[2]$	$[2]$	$[3]$	$[0]$	$[1]$
$[3]$	$[3]$	$[0]$	$[1]$	$[2]$

Theorem (群的一个例子, Group of Symmetries of A Square)

♪ $(S_4, *)$ is a group, where

♪ $S_4 = \{\text{张英哲, 杨珂, 张永恒, 蔡玉生, 郭帅, 易鸿伟, 彭聪, 柏洋}\}$

♪ The operation $*$ on the set S_4 is defined as follows:

*	张英哲	杨珂	张永恒	蔡玉生	郭帅	易鸿伟	彭聪	柏洋
张英哲	张英哲	杨珂	张永恒	蔡玉生	郭帅	易鸿伟	彭聪	柏洋
杨珂	杨珂	张永恒	蔡玉生	张英哲	柏洋	彭聪	郭帅	易鸿伟
张永恒	张永恒	蔡玉生	张英哲	杨珂	易鸿伟	郭帅	柏洋	彭聪
蔡玉生	蔡玉生	张英哲	杨珂	张永恒	彭聪	柏洋	易鸿伟	郭帅
郭帅	郭帅	彭聪	易鸿伟	柏洋	张英哲	张永恒	杨珂	蔡玉生
易鸿伟	易鸿伟	柏洋	郭帅	彭聪	张永恒	张英哲	蔡玉生	杨珂
彭聪	彭聪	易鸿伟	柏洋	郭帅	蔡玉生	杨珂	张英哲	张永恒
柏洋	柏洋	郭帅	彭聪	易鸿伟	杨珂	蔡玉生	张永恒	张英哲

$(S_4, *)$

*	张英哲	杨珂	张永恒	蔡玉生	郭帅	易鸿伟	彭聃	柏洋
张英哲	张英哲	杨珂	张永恒	蔡玉生	郭帅	易鸿伟	彭聃	柏洋
杨珂	杨珂	张永恒	蔡玉生	张英哲	柏洋	彭聃	郭帅	易鸿伟
张永恒	张永恒	蔡玉生	张英哲	杨珂	易鸿伟	郭帅	柏洋	彭聃
蔡玉生	蔡玉生	张英哲	杨珂	张永恒	彭聃	柏洋	易鸿伟	郭帅
郭帅	郭帅	彭聃	易鸿伟	柏洋	张英哲	张永恒	杨珂	蔡玉生
易鸿伟	易鸿伟	柏洋	郭帅	彭聃	张永恒	张英哲	蔡玉生	杨珂
彭聃	彭聃	易鸿伟	柏洋	郭帅	蔡玉生	杨珂	张英哲	张永恒
柏洋	柏洋	郭帅	彭聃	易鸿伟	杨珂	蔡玉生	张永恒	张英哲

A Subgroup of $(S_4, *)$

*	张英哲	张永恒
张英哲	张英哲	张永恒
张永恒	张永恒	张英哲

$(S_4, *)$

*	张英哲	杨珂	张永恒	蔡玉生	郭帅	易鸿伟	彭聃	柏洋
张英哲	张英哲	杨珂	张永恒	蔡玉生	郭帅	易鸿伟	彭聃	柏洋
杨珂	杨珂	张永恒	蔡玉生	张英哲	柏洋	彭聃	郭帅	易鸿伟
张永恒	张永恒	蔡玉生	张英哲	杨珂	易鸿伟	郭帅	柏洋	彭聃
蔡玉生	蔡玉生	张英哲	杨珂	张永恒	彭聃	柏洋	易鸿伟	郭帅
郭帅	郭帅	彭聃	易鸿伟	柏洋	张英哲	张永恒	杨珂	蔡玉生
易鸿伟	易鸿伟	柏洋	郭帅	彭聃	张永恒	张英哲	蔡玉生	杨珂
彭聃	彭聃	易鸿伟	柏洋	郭帅	蔡玉生	杨珂	张英哲	张永恒
柏洋	柏洋	郭帅	彭聃	易鸿伟	杨珂	蔡玉生	张永恒	张英哲

An equivalence relation on S_4 , which is a congruence relation

$$\pi = \{\{张英哲, 张永恒\}, \{杨珂, 蔡玉生\}, \{郭帅, 易鸿伟\}, \{彭聃, 柏洋\}\}$$

Equivalence classes

$$[张-张], [杨-蔡], [郭-易], [彭-柏]$$

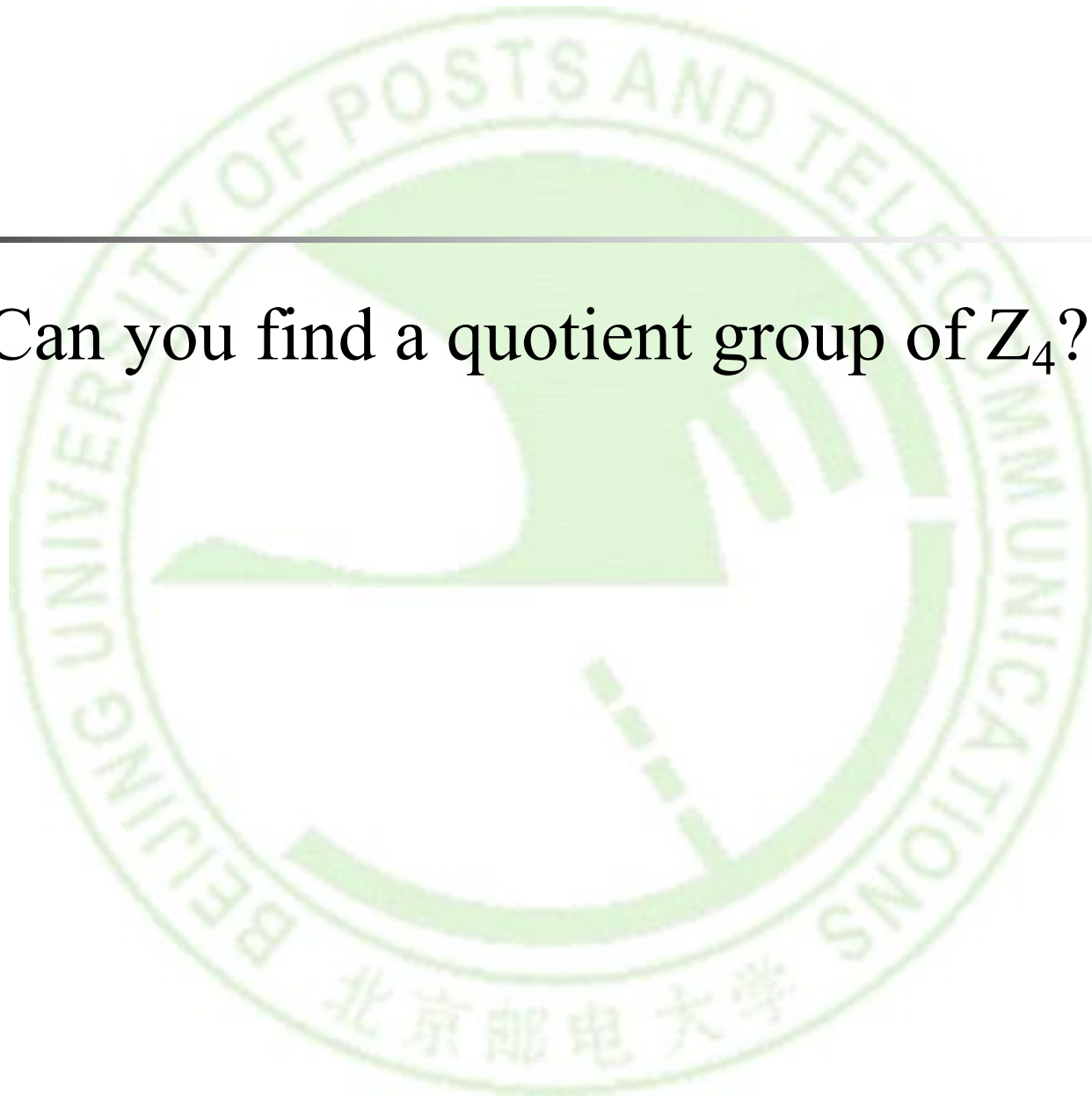
$(S_4, *)$

*	张英哲	杨珂	张永恒	蔡玉生	郭帅	易鸿伟	彭聃	柏洋
张英哲	张英哲	杨珂	张永恒	蔡玉生	郭帅	易鸿伟	彭聃	柏洋
杨珂	杨珂	张永恒	蔡玉生	张英哲	柏洋	彭聃	郭帅	易鸿伟
张永恒	张永恒	蔡玉生	张英哲	杨珂	易鸿伟	郭帅	柏洋	彭聃
蔡玉生	蔡玉生	张英哲	杨珂	张永恒	彭聃	柏洋	易鸿伟	郭帅
郭帅	郭帅	彭聃	易鸿伟	柏洋	张英哲	张永恒	杨珂	蔡玉生
易鸿伟	易鸿伟	柏洋	郭帅	彭聃	张永恒	张英哲	蔡玉生	杨珂
彭聃	彭聃	易鸿伟	柏洋	郭帅	蔡玉生	杨珂	张英哲	张永恒
柏洋	柏洋	郭帅	彭聃	易鸿伟	杨珂	蔡玉生	张永恒	张英哲

The Quotient Group, $(S_4/R, \circledast)$

\circledast	[张-张]	[杨-蔡]	[郭-易]	[彭-柏]
[张-张]	[张-张]	[杨-蔡]	[郭-易]	[彭-柏]
[杨-蔡]	[杨-蔡]	[张-张]	[彭-柏]	[郭-易]
[郭-易]	[郭-易]	[彭-柏]	[张-张]	[杨-蔡]
[彭-柏]	[彭-柏]	[郭-易]	[杨-蔡]	[张-张]

- 
- Can you find a quotient group of Z_4 ?





Homomorphism and Isomorphism(同态与同构)

Zhang Yanmei

ymzhang@bupt.edu.cn

College of Computer Science & Technology

Beijing University of Posts &
Telecommunications



Homomorphism – 同态

- Let
 - $(S, *)$ and $(T, *')$ be two groupoids, and
 - f is a function from S to T ,
- If
 - $f(a*b) = f(a) *' f(b)$ for all a and b in S .
- Then
 - f is called a *homomorphism* from $(S, *)$ to $(T, *')$.
 - S is homomorphic to T , denoted by $S \sim T$.
 - $f(S)$ is the *homomorphic image*(同态像) of S .



Isomorphism 同构

- Let f be a homomorphism from $(S, *)$ to $(T, *')$
 - If f is an onto from S to T , that is $f(S)=T$.
 - f is called an **onto-homomorphism** from $(S, *)$ to $(T, *')$.
 - If f is a bijection from S to T ,
 - f is called an **isomorphism** from $(S, *)$ to $(T, *')$
 - S is isomorphic to T , or S and T are isomorphic, denoted by **$S \cong T$** .
- Notice for both an isomorphism and a homomorphism,
 - The image of product is the product of the images.

Example (Isomorphic?)

- Let $S=\{a,b,c\}$ and $T=\{x,y,z\}$ with following operations

$*$	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

- It is easy to verify that S and T are group.

Example (Free semigroup)

■ Let

■ $A = \{0, 1\}$

■ (A^*, \cdot) , \cdot is the catenation operation

■ $(A, +)$, $+$ is defined by the table above

$+$	0	1
0	0	1
1	1	0

■ Define the function $f: A^* \rightarrow A$ by

$$f(\alpha) = \begin{cases} 1 & \text{if } \alpha \text{ has an odd number of 1's} \\ 0 & \text{if } \alpha \text{ has an even number of 1's} \end{cases}$$

■ It is easy to verify

■ $f(\alpha \cdot \beta) = f(\alpha) + f(\beta)$.

■ Thus f is a homomorphism.



Step to determine whether ...?

Homomorphism?

- **STEP 1:** Define a function $f:S \rightarrow T$.
- **STEP 2:** Show that $f(a*b) = f(a)*'f(b)$.

Isomorphism? two more steps

- **STEP 3:** Show that f is one-to-one.
- **STEP 4:** Show that f is onto.



Example 17

- Let
 - \mathbb{Z} be the set of all integers.
 - E be the set of all even integers
- Show that groups $(\mathbb{Z}, +)$ and $(E, +)$ are isomorphic.

Example 17 - Solution

- Define $f: \mathbb{Z} \rightarrow E$ by $f(a) = 2a$.
- $f(a+b) = 2(a+b) = 2a+2b = f(a)+f(b)$.
- f is one-to-one.
 - Suppose $f(a_1) = f(a_2)$. Then $2a_1 = 2a_2$, so $a_1 = a_2$.
- f is onto.
 - Suppose b is any even integer.
 - Then $a = b/2 \in \mathbb{Z}$ and $f(a) = f(b/2) = 2(b/2) = b$,
- Hence $(\mathbb{Z}, +)$ and $(E, +)$ are isomorphic groups.

Groups of order 4: Different or Isomorphic?

- Klein 4 group, Cyclic group.

Table 9.5

	<i>e</i>	<i>a</i>	<i>b</i>	<i>c</i>
<i>e</i>	<i>e</i>	<i>a</i>	<i>b</i>	<i>c</i>
<i>a</i>	<i>a</i>	<i>e</i>	<i>c</i>	<i>b</i>
<i>b</i>	<i>b</i>	<i>c</i>	<i>e</i>	<i>a</i>
<i>c</i>	<i>c</i>	<i>b</i>	<i>a</i>	<i>e</i>

Table 9.6

	<i>e</i>	<i>a</i>	<i>b</i>	<i>c</i>
<i>e</i>	<i>e</i>	<i>a</i>	<i>b</i>	<i>c</i>
<i>a</i>	<i>a</i>	<i>e</i>	<i>c</i>	<i>b</i>
<i>b</i>	<i>b</i>	<i>c</i>	<i>a</i>	<i>e</i>
<i>c</i>	<i>c</i>	<i>b</i>	<i>e</i>	<i>a</i>

Table 9.7

	<i>e</i>	<i>a</i>	<i>b</i>	<i>c</i>
<i>e</i>	<i>e</i>	<i>a</i>	<i>b</i>	<i>c</i>
<i>a</i>	<i>a</i>	<i>b</i>	<i>c</i>	<i>e</i>
<i>b</i>	<i>b</i>	<i>c</i>	<i>e</i>	<i>a</i>
<i>c</i>	<i>c</i>	<i>e</i>	<i>a</i>	<i>b</i>

Table 9.8

	<i>e</i>	<i>a</i>	<i>b</i>	<i>c</i>
<i>e</i>	<i>e</i>	<i>a</i>	<i>b</i>	<i>c</i>
<i>a</i>	<i>a</i>	<i>c</i>	<i>e</i>	<i>b</i>
<i>b</i>	<i>b</i>	<i>e</i>	<i>c</i>	<i>a</i>
<i>c</i>	<i>c</i>	<i>b</i>	<i>a</i>	<i>e</i>

Theorem: property of homomorphism

■ Let

- $(G, *)$ and $(G', *')$ be two groupoids, and
- $f: G \rightarrow G'$ be an onto homomorphism.

■ Then

- *If e is the identity in G and e' is the identity in G' , then $f(e) = e'$.*
- *If $a \in G$, then $f(a^{-1}) = (f(a))^{-1}$.*
- *If H is a subgroup of G , then $f(H) = \{f(h) \mid h \in H\}$ is a subgroup of G' .*
- *If G is a groupoid, semigroup, monoid, group, or abelian, so is G' .*

Theorem – Proof(1)

- Let b be any element of G' .
- Since f is onto, there is an element a in G such that $f(a) = b$.
- Since $a = a * e$,
 - $b = f(a) = f(a * e) = f(a) *' f(e) = b *' f(e)$.
- Similarly, $a = e * a$, $b = f(e) *' b$.
- Thus for any $b \in G'$, $b = b *' f(e) = f(e) *' b$,
 - which means that $f(e)$ is an identity for G' .
- the identity is unique, $f(e) = e'$

Theorem – Proof(2)

- Let b be any element of G' .
- Since f is onto, there is an element a in G such that $f(a) = b$.
- Since $f(e) = f(a * a^{-1}) = f(a) *' f(a^{-1}) = e'$,
 - $f(e) = f(a^{-1} * a) = f(a^{-1}) *' f(a) = e'$.
- Thus for any $b \in G'$, $f(a^{-1})$ is the inverse of $b = f(a)$.

Theorem – Proof(3)

- Let b_1 and b_2 are any elements of $f(H)$,
 - there exist a_1 and a_2 in H with $b_1 = f(a_1)$ and $a_2 = f(b_2)$.
 - $b_1 *' b_2 = f(a_1) *' f(a_2) = f(a_1 * a_2) = f(a_3)$.
 - Hence $b_1 *' b_2 \in f(H)$.
 - Thus $f(H)$ is closed under the operation $*'$.
- Since the associative property holds in G' , it holds in $f(H)$.
- base (1) and (2), $f(e) = e', f(a^{-1}) = (f(a))^{-1}$
- So $f(H)$ is a subgroup of $(G', *')$.



Theorem – Proof(4)

- Let b_1 and b_2 be any elements of G' . There exist a_1 and a_2 in G such that
 - $b_1 = f(a_1)$ and $b_2 = f(a_2)$
- Therefore
 - $b_1 *' b_2 = f(a_1) *' f(a_2) = f(a_1 * a_2) = f(a_2 * a_1) = f(a_2) *' f(a_1) = b_2 *' b_1.$
- Hence $(G', *')$ is also commutative.



Remember

- Isomorphism preserves all properties defined in terms of group operations.
 - *The group S_3 and Z_6 are both of order 6. However, S_3 is not Abelian and Z_6 is Abelian. Hence, they are not isomorphic.*



Example (Non-Isomorphic)

- Let
 - \mathbb{Z} be the set of all integers.
 - E be the set of all even integers
 - \times be ordinary multiplication
- Then the semigroups (\mathbb{Z}, \times) and (E, \times) are not isomorphic.
 - since \mathbb{Z} has identity and E does not.



Homework

- 22,28@331
- 28,32@page 349;
- 24@page338.

