Groups

Lecture 13

Discrete Mathematical Structures

Groups

- Part I: Groups
  - Basic properties of groups
  - Group of symmetries
  - Isomorphism and homomorphism
- Part II: Fundamental Homomorphism Theorem
  - Quotient group
  - Subgroup and cosets
  - Fundamental homomorphism theorem for group
  - Algebra systems with more than one operation

Group

- Group axioms
  - Association
  - Identity
  - Inverse property
- Example
  - Addition group on integers (Z,+)
  - All one-to-one functions on {1,2,3}, plus composition of function: S_3

Inverse

(Inverse can be discussed for those system with identity.)

- For a given element x in the system S, if there is some element x' in the system, satisfying that $x' \quad x=1_S$, then x' is called a left inverse of x.
- Similarly, if there is some x'' in the system, such that $x \quad x''=1_S$, then x'' is called a right inverse of x.
- For a given element x in the system S, if there is some element x^*, satisfying that: $x \quad x^*=x^* \quad x=1_S$, then x^* is called an inverse of x, denotes as x^{-1}.

An Example about Inverse

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

Note:

(1) b has different left and right inverses

(2) c has 2 right inverses, but no left inverse

(3) d has left inverse, but no right inverse

Uniqueness of Inverse

If a system (S,   ) is ***associate***:

- For a given x, if x has a left inverse, and a right inverse as well, then they must be equal, and it is the unique inverse of x.
  - Assuming left inverse is x', and right inverse is x'':

    $x'=x' \quad 1_S=x' \quad (x \quad x'')=(x' \quad x) \quad x''=1_S \quad x''=x''$

- If every element of S has a left inverse, then the left inverse is also its right inverse, and the inverse is unique.
  - For any a in S, let b is a left inverse of a, and c is a left inverse of b, then:

    $a \quad b = (1_S \quad a) \quad b = ((c \quad b) \quad a) \quad b = (c \quad (b \quad a)) \quad b$
    $= (c \quad 1_S) \quad b = c \quad b = 1_S$

Inverse Property of a System

- For any element in a system, there may or may not be its inverse.
- However, “for any element x in S, x has its inverse” is a property of the system as a whole.
- For a system for which the inverse property holds, each element has its particular inverse.

Semigroup and Group

- A group is a semigroup
  - Association
- A group is a monoid
  - Identity
- Negative exponential
  - Denotation of inverse of element a: a^{-1}
  - Expansion of exponential: $a^{-k} =(a^{-1})^k$ (k is positive integer)

- *Abelian group: commutative group*

An Example of Abelian Group

- Let G be the set of all nonzero real numbers, let $a*b=ab/2$, then $(G,*)$ is an Abelian group.
- Verifying that all requirements as described as definition are satisfied:
  - "*" is a closed binary operation on G.
  - Associativity: $(a*b)*c=a*(b*c)=(abc)/4$
  - Identity: $a*2=2*a$ for all a in G
  - Inverse: examine the equation $a*x=2$, it is easy to see that for all a in G, $a^{-1}=4/a$
  - Commutativity: obviously, $a*b=b*a$

Product of groups

- Given two groups (S,), (T,*), define operation "$\otimes$" on the Cartesian product $S\times T$ as follows:

$$<s_1,t_1> \otimes <s_2,t_2> = <s_1 \quad s_2,\ t_1{*}t_2>$$

- ($S\times T$, $\otimes$) is a group:
  - Association: $<(r_1 \quad s_1) \quad t_1,\ (r_2{*}s_2){*}t_2>$

    $= \ <r_1 \quad (s_1 \quad t_1),\ r_2{*}(s_2{*}t_2)>$
  - Identity: $<1_S,\ 1_T>$
  - Inverse property: the inverse of $<s, t>$ is $<s^{-1}, t^{-1}>$
    - (where $s, s^{-1}\in S,\ \ t, t^{-1}\in T$)

An Example of non-Abelian Group

- Six one-to-one functions can be defined on the set {1,2,3} altogether:

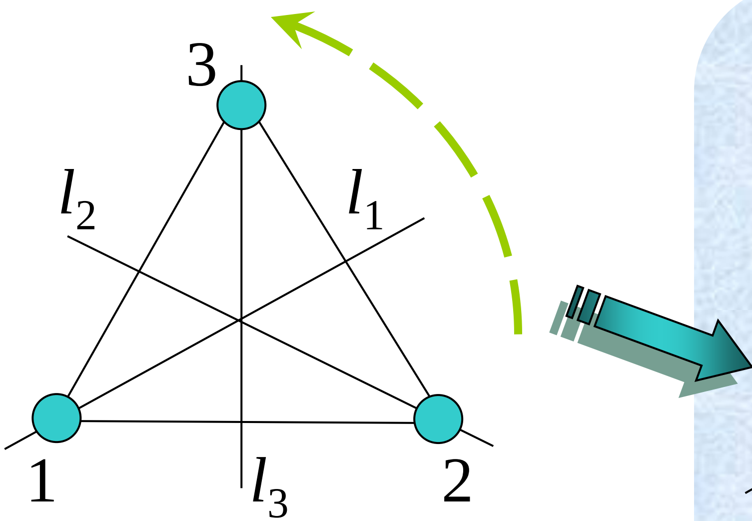
$$f_1 = \begin{pmatrix} 1\,2\,3 \\ 1\,2\,3 \end{pmatrix} \quad f_2 = \begin{pmatrix} 1\,2\,3 \\ 2\,3\,1 \end{pmatrix} \quad f_3 = \begin{pmatrix} 1\,2\,3 \\ 3\,1\,2 \end{pmatrix}$$

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

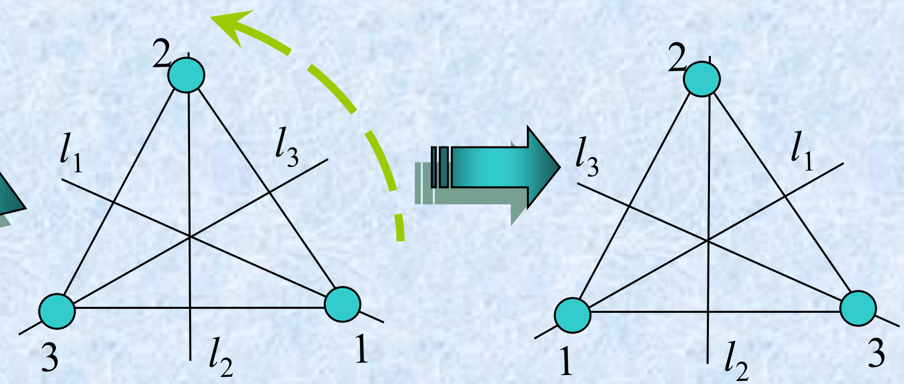
- ({e,α,β,γ,δ,ε},) is a group, here, “ ” is composition of function. One-to-one function on finite set is called a permutation, so, this is a permutation group, denoted as S_3.

Geometric Interpretation of S_3

Each one-to-one correspondence on the set of points is a symmetry of the triangle.



Note: $f_2 * g_2 = g_1$



3 rotations: f_1-0°, f_2-120°, f_3=240°

3 reflectings: g_1-by l_1, g_2-by l_2, g_3-by l_3

Cancellation Properties

- Cancellation property holds for group:
  - Let (G,) be a group, for any $a,b,c \in G$

    If a $b=a$ c, then $b=c$

    If b $a=c$ a, then $b=c$
- The algebraic system (Z^+, $\cdot$), where Z^+ is the set of positive integers, and "·" is arithematic multiplication, satisfies association and cancellation, but it is ***not*** a group.

Group Equation and Its Solution

- Group equations:
  - $a \quad x=b$ and $y \quad a=b$, where a, b are constants
- Solutions of the group equations:
  - $a \quad x=b \rightarrow a \quad (a^{-1} \quad b)=b$
  - $y \quad a=b \rightarrow (b \quad a^{-1}) \quad a=b$
- The group equation has unique solution:
  - Assuming that $a \quad x_1=b= a \quad x_2$, multiply the two sides of the equation from the left with a^{-1}, $x_1= a^{-1} \quad b=x_2$,

Second Definition of Group

- (G,) is an algebraic system, if association holds for it, and the two group equation a x=b and y a=b have unique solutions each, then (G,) is a group.
  - Sketch of proof:
  - (1) Let b is any element in G, y b=b has a unique solution e, then it is easy to prove that e is a left identity in (G,).

    For any $a \in G$， b x=a has a unique solution c, then e a=e b c= b c=a
  - (2) For any $a \in G$， y a=e has a unique solution a' ("left inverse candidate")
  - (3) then a' is also "right inverse candidate" of a:

    y a'=e has a unique solution a'', then a a'= e (a a') = (a'' a') (a a')=e
  - (4) e is also right identity: for any $a \in G$, a e= a (a' a)=a
- ***Combining (1)-(4), e is the identity of (G,), and for any element a, a has a' as its inverse.***

Finite Group and Cancellation

- Let G be a finite set, if the algebraic system (G,) satisfies association and cancellation properties, then (G,) is a group.
  - Sketch of proof:

    Assuming that $G=\{a_1,a_2,a_3,\ldots,a_n\}$, for any given a_i in G, considering the set $a_iG=\{a_i \quad a_1, a_i \quad a_2, a_i \quad a_3, \ldots, a_i \quad a_n\}$. Note that a_iG is a subset of G (closeness of G), but it must has the same number of element with G (cancellation), so, $a_iG=G$, which means that the equation $a \quad x=b$ has a unique solution. (***Why?***)

  Similarly, the equation $y \quad a=b$ has also a unique solution.

  So, (G,) is a group.

Operation Table of Group

- There is no identical elements in any row or any column.
  - Let $G=\{a_1,a_2,\ldots,a_n\}$

    If there are two identical elements in ith row, at locations k, l, then the equation $a_i*x=a_j$ has two different solution, contradiction.
  - Same for column.
  - For a group with 3 elements

	1	2	3
1	1	2	3
2	2	3	1
3	3	1	2

Isomorphism

- Group $(G_1, \quad)$ and $(G_2,*)$ are isomorphic $(G_1 \cong G_2)$ if and only if:

  There exist a one-to-one correspondence f: $G_1 \to G_2$, such that: (f is called an isomorphism)

  For any $x,y \in G_1$, $f(x \quad y) = f(x) * f(y)$
- Isomorphism is an equivalence relation.
  - Reflexibility: the identity function is a one-to-one correspondence.
  - Symmetry: inverse of a one-to-one correspondence is also a one-to-one correspondence.
  - Transitivity: the composition of two one-to-one correspondence is also a one-to-one correspondence.

Homomorphism

- Group (G_1,   ) and (G_2,*) are homomorphic, denoted as (G_1~ G_2) is and only if:

  There exists a function f: $G_1 \xrightarrow{f} G_2$ such that:

  for any x,y$\in G_1$, f(x   y) = f(x) * f(y)
- If f is also onto, then G_2 is a homomorphic image of G_1.
- Note: isomorphism is a special case of homomorphism
- Example: integer addition group (Z,+) and mod-3 addition group (Z_3,$+_3$)
  - homomorphism: f : Z$\to Z_3$, f(3k+r)=r

Homomorphic Image and System Properties

Association

- Assuming that f: $G_1 \rightarrow G_2$ is a homomorphism, and G_2 is a homomorphic image of G_1, then, if G_1 is associative, so is G_2, i.e. for any $x,y,z \in G_2$, $(x \quad y) \quad z = x \quad (y \quad z)$

Proof:

for any $x', y', z' \in G_2$, since f is onto, there must be $x,y,z \in G_1$, such that $f(x)=x'$, $f(y)=y'$, $f(z)=z'$. So, $(x'*y')*z' = (f(x)* f(y))* f(z) = f(x \quad y) * f(z) = f((x \quad y) \quad z) = f(x \quad (y \quad z)) = f(x)* (f(y)* f(z)) = x'*(y'*z')$

- Same discussion applies for commutation.

Homomorphic Image and System Properties

Identity

- Assuming that f: $G_1 \rightarrow G_2$ is a homomorphism, and G_2 is a homomorphic image of G_1, then, if G_1 has an identity e, so does G_2, i.e. there exists e' in G_2, such that for any $x \in G_2$, $(x*e)=(e*x)=x$

Proof:

for any $x' \in G_2$, since f is onto, there must be $x \in G_1$, such that $f(x)=x'$. Let $f(e)=e'$, then, $(x'*f(e)) = (f(x)* f(e))= f(x \quad e) = f(x) = x'$. $(f(e)*x)=x$ can be proved similarly.

Note that $f(e)$ is in G_2, so, it is the identity of G_2.

Subgroup

- Let H be a nonempty subset of a group G such that:
  - The identity e of G belongs to H
  - If a and b belong to H, then $ab \in H$
  - If $a \in H$, then $a^{-1} \in H$
- Then H is called a subgroup of G.
- Note: subgroup is itself a group, and the properties above are not independent

- Example: cyclic subgroup: $H = \{a^{\mathrm{i}} | i \in Z\}$, where a is a randomly specified element of G.

Homomorphism and Subsystem

- Let f be a homomorphism from a group $(S,\quad)$ to a group $(T,*)$. If S' is a subgroup of $(S,\quad)$, then

$$f(S')=\{t\in T|t=f(s) \text{ for some } s\in S'\}$$

the image of S' under f, is a subgroup of $(T,*)$

- Proof
  - Closedness of $f(S')$
  - Associativity hold on $f(S')$

Groups with Three or Four Elements

If isomorphic groups are considered as the same, then:

	1	2	3
1	1	2	3
2	2	3	1
3	3	1	2

There is only **one** group with 3 elements.

	1	2	3	4
1	1	2	3	4
2	2	3	4	1
3	3	4	1	2
4	4	1	2	3

	1	2	3	4
1	1	2	3	4
2	2	1	4	3
3	3	4	1	2
4	4	3	2	1

There is only **two** groups with 3 elements.

Product of Cyclic Group

- $(Z_n,+_n)$ is a finite cyclic group for each *n*.
- $Z_2 \times Z_2 \cong Z_4$
- $Z_m \times Z_n \cong Z_{mn}$ if and only if m,n are relatively prime
- If GCD(m,n)=1, we need only to prove that $Z_m \times Z_n$ is cyclic. In turn, it can be achieved by proving there is an element of x of order mn in $Z_m \times Z_n$.
    - $(1,1)^{mn} = (1,1)$
    - If $(1,1)^k = (1,1)$, then k must be one of the common multiplier of m,n. If $k<mn$, then $GCD(m,n)>1$, but m,n are relatively prime.
    - So, $|(1,1)| = mn$。
  - If $C_m \times C_n \cong C_{mn}$ $C_m \times C_n$ is cyclic， the generator is unique, that is (1,1).

Quotient Group

- Let R is a congruence relation on the group $(S,*)$. S/R is the quotient set, i.e. the set of all equivalence classed.
- Define an operation $\otimes$ from $S/R \times S/R$ to S/R as $[a]\otimes[b]=[a*b]$. Note the operation is well-defined because R is a congruence relation.
  - Suppose $([a],[b])=([a'],[b'])$, then aRa', bRb', by the definition of congruence relation, $a*b=a'*b'$, so $\otimes$ is a well-defined function from $S/R \times S/R$ to S/R
- $(S/R,\otimes)$ is a group, called **quotient group**, for any $[a]$, the corresponding inverse is $[a^{-1}]$

Coset – Left or Right

- H is a subgroup of group G, for any a in G, we can define a set ,aH, of G as following:

  $$aH=\{a \circ h | h \in H\}$$

- aH is called a left coset of H.
  - Closeness of G implies that aH is a subset of G.
  - $\forall h \in H$, $ah \in H$ if and only if $a \in H$, (Why?)
- Similarly, we can define right coset of H.

Normal Subgroup

- Definition: a subgroup H of G is normal means that, for any $a \in G$, $Ha=aH$。 ($H \trianglelefteq G$)
- $Ha=aH$ if and only if For any $h_i \in H$, $a \in G$， there must be some $h_j \in H$， such that $h_i a = a h_j$。

  (Not that for any $h_i \in H$, $a \in G$, $h_i a = a h_i$。)
- Let N is a subgroup of G, N is normal if and only if : for any $g \in G$, $n \in N$, $\boldsymbol{gng^{-1} \in N}$。
  - $\Rightarrow$ for any $g \in G$, $n \in N$, there is a $n_1 \in N$, such that $gn = n_1 g$, so, $gng^{-1} = n_1 \in N$;
  - $\Leftarrow$ prove that $gN \subseteq Ng$: for any $gn \in gN$, we know that $gng^{-1} \in N$ ， let $gng^{-1} = n_1$， then $gn = n_1 g \in Ng$； Similarly for $Ng \subseteq gN$。

Right Coset Relation

- H is a subgroup of a group G. Define a relation R on G as following:

  for any $a,b \in G$, aRb iff. $ab^{-1} \in H$

  - In fact, aRb means that a,b belong to the same right coset.
    - $aRb \Rightarrow ab^{-1} \in H \Rightarrow ab^{-1} = h_i,\ h_i \in H \Rightarrow a \in Hb$
  - The relation is an equivalence.

Congruence Relation

- A familiar example:
  - $a \equiv b \pmod 3$ iff. $|a-b|/3$ is an integer
    - Equivalence classes: $\pi_1=\{\ldots -3,0,3,6,9,\ldots\}$

      $\pi_2=\{\ldots -2,1,4,7,10,\ldots\}$

      $\pi_3=\{\ldots -1,2,5,8,11,\ldots\}$
- Characteristics of the operation on classes:
  - $aRb,\ cRd \Rightarrow ac\ R\ bd$
- Congruence relation in general

Coset Relation about Normal Subgroup

- If N is a normal subgroup of a group G, then:

  If $ap^{-1} \in N$, $bq^{-1} \in N$, then $(ab)(pq)^{-1} \in N$

  - Let $ap^{-1}=n_1$, $bq^{-1}=n_2$ $(n_1,n_2 \in N)$

    then $(ab)(pq)^{-1} = abq^{-1}p^{-1} = an_2p^{-1}$

    Notice that N is normal, so, $an_2=n_3a$ $(n_3 \in N)$

    So, $(ab)(pq)^{-1} = n_3ap^{-1} = n_3n_1 \in N$

Operation on Coset

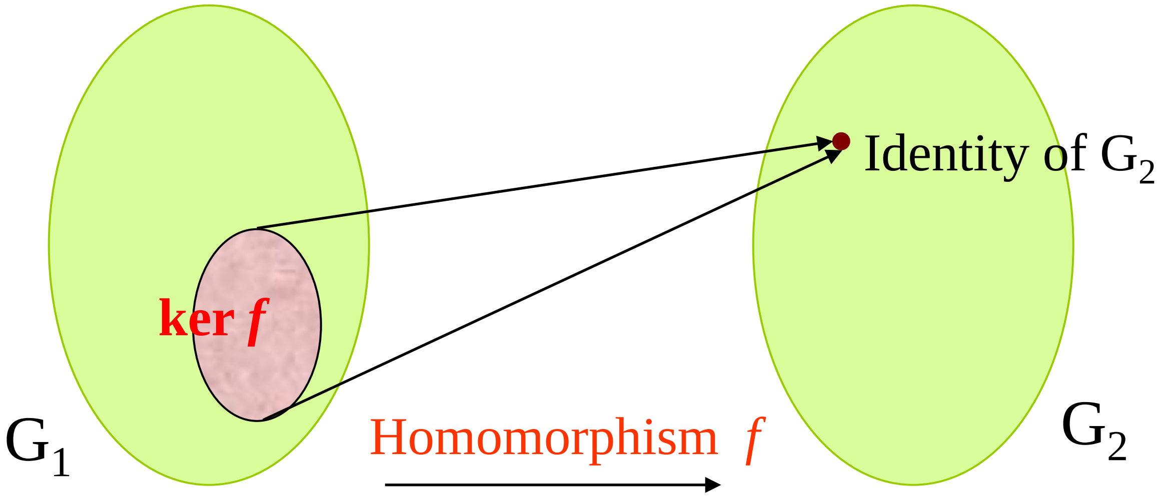
- Given a normal subgroup of a group G,
- Define an operation on right coset of H as following:
  - Ha*Hb = H(ab) , ab is the operation of G.
- * is a well-defined operation: the result of the operation "*" doesn't depend on the selection of the representative element.
  - It is guaranteed by normal subgroup.

Quotient Group

- If N is a normal subgroup of a group G, then (G/N, *) is also a group.
  - Closedness;
  - Associativity;
  - Identity: N itself;
  - Inverse: the inverse of Na is Na^{-1}
- (G/N, *) is called a quotient group of G.

Homomorphism Kernel

- G_1, G_2 are groups, f: $G_1 \rightarrow G_2$ is a homomorphism, define a set **ker *f* = {x|x∈G_1,*f*(x)=e_2}**, where e_2 is the identity of G_2, ker f is called the homomorphism kernel.



Kernel is a normal subgroup

- ker *f* is a normal subgroup of G_1
  - Nonemptiness: the identity of G_1 belongs to ker *f* ;
  - Subgroup: for any $a,b \in$ ker *f* , we have $f(a)=f(b)=e_2$;
    So, $f(ab^{-1}) = f(a)*[f(b)]^{-1} = e_2$
  - Normal: for any $a \in$ ker *f* , $x \in G_1$, we have $f(a)=e_2$;
    so, $f(xax^{-1}) = f(x)*f(a)*[f(x)]^{-1} = e_2$

Natural Homomorphism

- Any group G is onto homomorphic to its quotient G, called "Natural homomorphism"
  - Define g:G$\rightarrow$G/N, for any a$\in$G, g(a)=Na. Obviously, g is onto function.
  - G is a homomorphism
    - For any a,b$\in$G: g(ab)=N(ab) =Na*Nb= g(a)*g(b)
  - ker g is N:
    - Nis the identity of the quotient group.g(x)=N $\Leftrightarrow$ x$\in$N

A Congruence Relation Determined by a Homomorphism

R defined on *G*

It is easy to prove that *R* is an equivalence.

R is a congruence relation:

$f(a \quad b) = f(a)*f(b)$

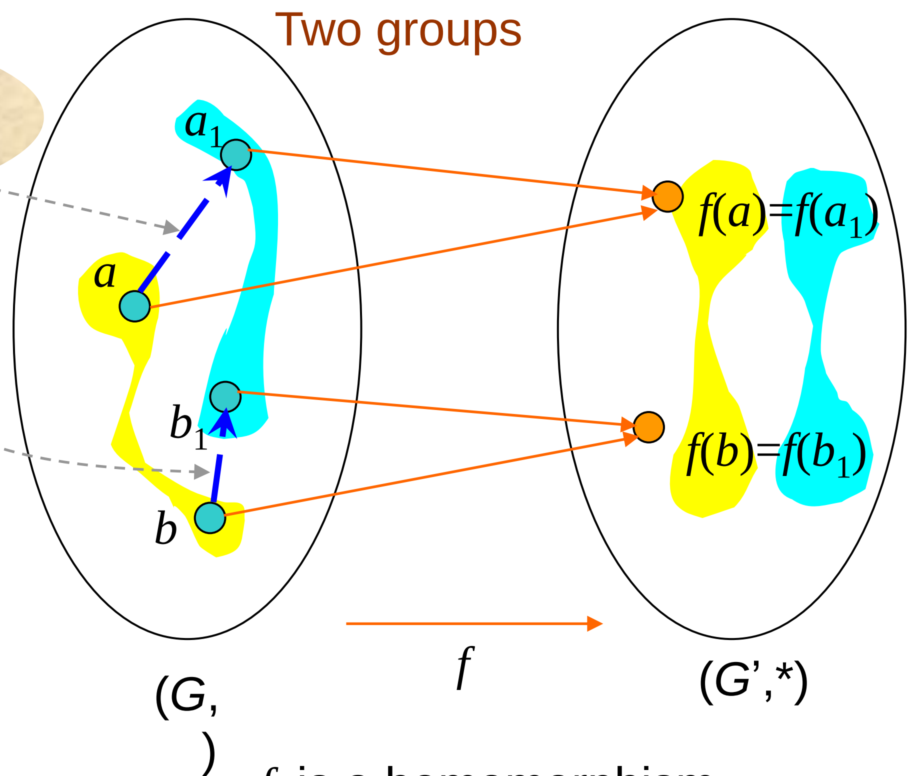
$f(a_1 \quad b_1) = f(a_1)*f(b_1)$

However: $f(a)*f(b) = f(a_1)*f(b_1)$

Which means:

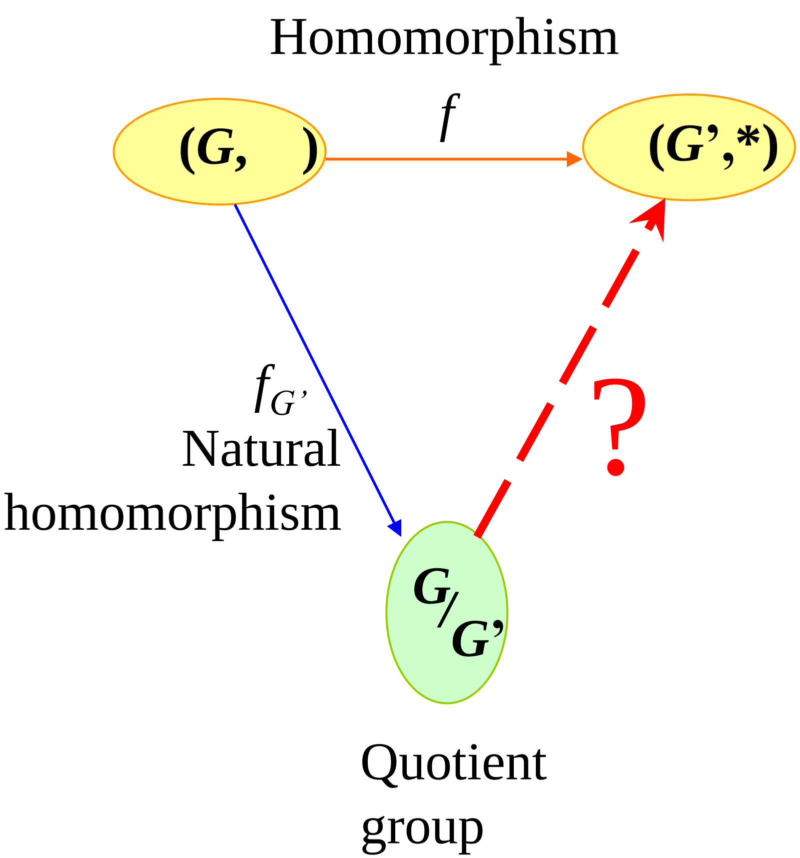
$$f(a \quad b) = f(a_1 \quad b_1)$$

That is: $(a \quad b)R(a_1*b_1)$



f is a homomorphism

Fundamental Homomorphism Theorem



Define g: $S/R \rightarrow G'$ as following:

$g([a])=f(a)$ for any $[a] \in S/G'$

1. g is a function: that is for any other element a' in $[a]$, $g[a']=f[a]$

2. g is one-to-one: all element a having the same value of $f(a)$ are in one equivalence class.

3. g is onto: for any $b \in T$, there is some $a \in S$, such that $f(a)$=b, then $g[a]$=b.

4. g is an isomorphism:

$g([a]\otimes[b])=g([a\quad b])=f(a\quad b)=f(a)*f(b)$ $=g([a])*g([b])$

System with 2 Operations - Ring

A nonempty set R is a ***ring*** if it has two closed binary operations, addition and multiplication, satisfying the following conditions.

1. $a + b = b + a$ for $a, b \in R$.
2. $(a + b) + c = a + (b + c)$ for $a, b, c \in R$.
3. There is an element 0 in R such that $a + 0 = a$ for all $a \in R$.
4. For every element $a \in R$, there exists an element $-a$ in R such that $a + (-a) = 0$.
5. $(ab)c = a(bc)$ for $a, b, c \in R$.
6. For $a, b, c \in R$,

$$a(b + c) = ab + ac$$
$$(a + b)c = ac + bc.$$

Some Properties of Ring

Let R be a ring with $a, b \in R$. Then

1. $a0 = 0a = 0$;
2. $a(-b) = (-a)b = -ab$;
3. $(-a)(-b) = ab$.

PROOF. To prove (1), observe that

$$a0 = a(0+0) = a0 + a0;$$

hence, $a0 = 0$. Similarly, $0a = 0$. For (2), we have $ab + a(-b) = a(b-b) = a0 = 0$; consequently, $-ab = a(-b)$. Similarly, $-ab = (-a)b$. Part (3) follows directly from (2) since $(-a)(-b) = -(a(-b)) = -(-ab) = ab$. $\square$

Zero Divisor

- We are taught to reasoning as following
  - If xy=0, then, x=0 or y=0
- But, it is not true in some systems:
  - For example: $(Z_6, \oplus, \otimes)$, $2\otimes 3=0$
  - In 2×2 matrix ring: $\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}=\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$
- If x,y are nonzero, but xy=0, then x,y are (left/right) zero divisors

Systems with 2 Operations - Field

- Field (F,+,*)
  - (F,+,*) is a ring;
  - * is commutative;
  - there is a unique element 1 in F, satisfying: for any x in F, 1x=x1=x;
  - Every nonzero element x in F has a multiplicative inverse
- Z_n is a field when n is a prime.

Home Assignments

- To be checked
  - pp.371: 6, 8, 12, 18, 19, 21, 24, 26, 28-39
  - pp.376: 1-3, 6, 12, 18, 22, 26-35, 37
  - pp.381: 7, 8, 26-29