Semigroups

Lecture 12

Discrete Mathematical Structures

Semigroups

- Part I: Semigroup and Monoid
  - Binary operations and their properties
  - Semigroup and monoid
  - Isomorphism and homomorphism
- Part II: Fundamental Homomorphism Theorem
  - Congruence relation
  - Quotient semigroup
  - Natural homomorphism
  - Fundamental homomorphism theorem for semigroup

Binary Operation

- Function $f{:}A^n \to B$ is called an n-nary operation from A to B.
  - Binary operation: $f{:}A \times A \to B$
  - An example: a new operation "*" defined on the set of real number, using common arithmatic operations:

    x*y = x+y-ab

    Note: 2*3 = -1； 0.5*0.7 = 0.85
- An operation is a function, so the following are not operations:
  - Let A=R, define * on A: $a*b$ as a/b
  - Let A=Z, define * on A: $a*b$ as a number less than a,b

Closedness of Operations

- For any operation f:$A^n \rightarrow B$, if $B \subseteq A$, then it is said that *A* is closed with respect to f. Or, we say that f is closed on *A*.
  (What does the operation table of a closed operation look like?)

- Example:
  - Set A={1,2,3,…,10}, gcd is closed, but lcm is not.
  - Discuss the closeness of common addition on the following set:
    - {n | there exists a positive integer *k*, such that $16|n^k$}
    - {n | 9 divides 21n}

- Assuming $A \subset B$， if *A* is closed with respect to *, what about *B*? And if *B* is closed with respect to *, what about *A*?

Algebraic System

- Definition:
  - A nonempty set *S* (no limitation about its elements)
  - One or more operations (binary operations in most cases)
  - *S* is closed with respect to these operations
- Denotation: (*S*,)

- Example:
  - (*Z*, +), here, *Z* is the set of integers and + is arithmatic addition

Operation Table

- Operation table can be used to define unary or binary operations on a finite set (usually only with several elements)

*	a	b	c	d
a	1	®	❋	M
b	&	6	K	M
c	7	6	Q	0
d	G	#	~	⧈

Properties of Binary Operations

- Associativity
  - Operation "∘" defined on the set *A* is associative if and only if:

    For any x, y, z ∈ A, (x y) z = x (y z)

- Commutativity
  - Operation " " defined on the set *A* is commutative if and only if:

    For any x, y ∈ A, x y = y x

- Idempotence
  - Operation " " defined on the set *A* is idempotent if and only if:

    For any x ∈ A, x x = x

Identity of an Algebraic System

- For arithmatic multiplication on the set of real number, there is a specific real number 1, satisfying that for any real number *x*, $1 \cdot x = x \cdot 1 = x$

- An element *e* is called the identity element of an algebraic system (S,) if and only if :

  For any $x \in S$, e x=x e=x。

- Denotation: 1_S, or simply 1, but remember that it is not *that* "1".
- It is not that every algebraic system has its identity element.

An Example about Coding

- Given an alphabet A={0,1}, A* is the set of string of length *n* on A.
- Define a binary operation $\oplus$ on A* as follows:
  - For any x,y$\in$A*, x$\oplus$y is a binary string of length *n*, in which, the *i*th bit is 1 if and only if the corresponding bits in *x* and *y* are different. (i=0,1,…,n-1)
- (A*, $\oplus$) is an algebraic system
- Satisfied properties: association, commutation, identity

A System with Specified Properties

- Let $(A,*)$ is a system satisfying idempotent, commutative and associative properties. Define a relation $\leq$ on A by $a\leq b$ iff. $a=a*b$. Then $(A,\leq)$ is a poset, and for all a,b in A, $\mathrm{GLB}(a,b)=a*b$
- Proof
  - Reflexivity: since $a*a = a$, so, $a\leq a$ for all a in A
  - Antisymmetry: if $a\leq b$, $b\leq a$, then $a=a*b$, and $b=b*a$, but $a*b=b*a$, so, $a=b$
  - Transitivity: if $a\leq b$, $b\leq c$, then $a=a*b$, $b=b*c$, so, $a=a*(b*c)=(a*b)*c=a*c$, so, $a\leq c$
  - GLB:
    - $a*b$ is a lower bound of $\{a,b\}$: $(a*b)=(a*a)*b=(a*b)*a$, and similarly, $(a*b)=a*(b*b)=(a*b)*b$
    - $a*b$ is GLB: if $c\leq a$, and $c\leq b$, then $c=c*a$ and $c=c*b$, so, $c=(c*a)*b=c*(a*b)$

Axiomatic System

- Abstract system: too general
- Concrete system: too many

- Abstract algebra as a branch of modern mathematics: axiomatic system
  - Axioms of the system: usually, one or more of the properties discussed above

Semigroup

- Axiom of semigroup
  - Association
- An example ({1,2},*) is a semigroup, where * defined as:

$$\text{For any } x,y \in \{1,2\},\ x*y=y$$

- Proof: it should be proved that for any x,y,z in {1,2}, $(x*y)*z = x*(y*z)$

Note: if checking by operation table, we have to check as many as 8 equations.

Generalized Associative Law

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

$$\text{Proof by induction: Let } \prod_{i=1}^{n} a_i = ((\ldots((a_1 * a_2) * a_3)\ldots * a_{n-1}) * a_n$$

For any insertion of parenthese, let the last step is $u * v$

$$\text{By inductive hypothesis: } u = \prod_{i=1}^{m} a_i,\ v = \prod_{j=1}^{n-m} a_{m+j} \quad (m < n)$$

$$u * v = \prod_{i=1}^{m} a_i * \prod_{j=1}^{n-m} a_{m+j} = \left(\prod_{i=1}^{m} a_i\right) * \left(\prod_{j=1}^{n-m} a_{m+j} * a_n\right) = \left(\prod_{i=1}^{n-1} a_i\right) * a_n = \prod_{i=1}^{n} a_i$$

Power

- If operation “ ” is associative, then we can define the exponential function as follows:

  $x^1 = x$

  $x^{n+1} = x^n \quad x$ (n is positive integer)

- In addition, if “ ” has the identity, then:

  $x^0 = e$ (e is the identity)

  $x^{n+1} = x^n \quad x$ (n is nonnegative integer)

- Properties
  - $x^n \quad x^m = x^{n+m}$
  - $(x^n)^m = x^{nm}$

Several Examples of Semigroup

- Example 1: $(A,*)$ is a semigroup satisfying that for any a,b, if $a \neq b$, then $a*b \neq b*a$, (a*b = b*a implies a = b) show:
  - (1) $a*a = a$
    Note: $(a*a)*a = a*(a*a)$
  - (2) $a*b*a = a$
    Note: $(a*b*a)*a = a*(a*b*a)$
  - (3) $a*b*c = a*c$
    Note: $a*b*c = a*b*(c*a*c) = (a*b*c*a)*c = a*c$

Several Examples of Semigroup

- Example 2: $(A,*)$ is a semigroup. There exists an element a in A, such that, for any x in A, there exist u,v, such that $a*u=v*a=x$.

$$\exists a(\ a \in A\ \wedge \forall x \left(x \in A \Rightarrow \exists u, v \left(\begin{array}{c} u \in A \wedge v \in A \wedge \\ (a * u = v * a = x) \end{array} \right) \right))$$

  Prove that A has an identity.

- Proof:
  - for a itself, there are also u_a,v_a, such that, $a*u_a=a$; $v_a*a=a$.
  - For any x, exists u_a ,v_a such that $a*u_x = v_x*a = x$
    - $x*u_a=(v_x*\mathrm{a})*u_a=v_x*a=x$, ($\mathrm{u}_\mathrm{a}$ is a right identity).
    - $v_\mathrm{a}*x=v_a*(a*u_x)=a*v_x=x$, ($v_\mathrm{a}$ is also left identity).
  - $v_a*u_a = v_a = u_a$

Monoid

- Axioms of the system
  - Association
  - Identity
- Examples
  - $P(S)$, where S is a set, together with the operation union or intersection are both commutative monoids
  - The set of all functions $f: S \to S$, denoted as S^S, together with the operation of composition is a monoid

Subsystems

- Subsemigroup
  - Let $(S,*)$ be a semigroup and let $T \subseteq S$. If T is closed under the operation $*$, then $(T,*)$, which is obviously a semigroup itself, is called a subsemigroup of $(S,*)$
  - $(Z,+)$, $(Q,+)$ are both subsemigroups of $(R,+)$
- Submonoid
  - Let $(S,*)$ be a monoid with identity e, and let $T \subseteq S$. If T is closed under the operation $*$ and $e \in T$, then $(T,*)$, which is obviously a monoid itself, is called a submonoid of $(S,*)$

Examples of Subsystem

- An Example:

$$S = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \middle| a, d \in R \right\} \qquad T = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \middle| a \in R \right\}$$

- Let “*” be matric multiplication, then both (S,*) and (*T*,*) are both monoids. *T* is a subsemigroup of *S*, but it is not a submonoid(*why*?).

Systems that look alike

- "Logical *or*" and "Boolean sum"

$\vee$	F	T
F	F	T
T	T	T

$+$	0	1
0	0	1
1	1	1

  - Note: if the signs and their meaning are ignored, the two tables are same

Isomorphism

- Semigroup (S,   ) and (T,*) are isomorphic ($S \cong T$) iff:
  There exist a one-to-one correspondence f: $S \to T$, such that:
  For any x,y$\in S$, f(x   y) = f(x) * f(y)
  (f is called an isomophism)

- 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.

Show Isomorphism of Two Systems

- Basic approach: find a one-to-to correspondence and check it for the requirements for the isomorphism
- Examples
  - "logical *OR*" semigroup ($\{F,T\},\vee$) and Boolean sum semigroup ($\{0,1\},+$)

    isomorphism $f : \{F,T\} \rightarrow \{0,1\}$: $f(F)=0$, $f(T)=1$

  - Positive real number multiplication semigroup ($R^+,\bullet$) and real number addition semigroup ($R,+$)

    isomorphism $f: R^+ \rightarrow R$: $f(x)=\ln x$

    Note: $f(x)=\lg x$ is another isomorphism

How to Negate isomorphism

- To prove semigroups (S,) and (T,*) are **not** isomorphic to each other, you must prove that **any** functions from (S,) to (T,*) **cannot** be an isomorphism between them.
- Example:
  - nonzero rational number multiplication semigroup (Q-{0},•) and rational number addition semigroup (Q,+) are not isomorphic to each other

  If there exists an isomorphism f : Q-{0}→Q,

  then $f(1)=0$ (otherwise, $f(1\bullet x)\neq f(1)+f(x)$)

  However, $f(-1)+f(-1)= f((-1)\bullet(-1))=f(1)=0$

  So, $f(-1)=f(1)$， f is not one-to-one, contradiction.

Homomorphism

- Semigroup (S,) and (T,*) are homomorphic, denoted as (S~T) if and only if:

  There exists a function f: $S \rightarrow T$ such that:

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

Isomorphism and Homomorphism: Generalized

- The discussion about isomorphism and homomorphism can be generalized to general algebraic systems
  - ***Algebraic systems*** $(G_1,\ \ )$ and $(G_2,*)$ are isomorphic if and only if:

    there exists a one-to-one correspondence f: $G_1 \to G_2$, such that:

    for any $x,y \in G_1$, $f(x\ \ \ y) = f(x) * f(y)$

  - ***Algebraic systems*** $(G_1,\ \ )$ and $(G_2,*)$ homomorphic if and only if:

    there exists a function f: $G_1 \to G_2$, such that:

    for any $x,y \in G_1$, $f(x\ \ \ y) = f(x) * f(y)$

    And if f is onto, then G_2 is a homomorphic image of G_1.

Homomorphic Image and System Properties

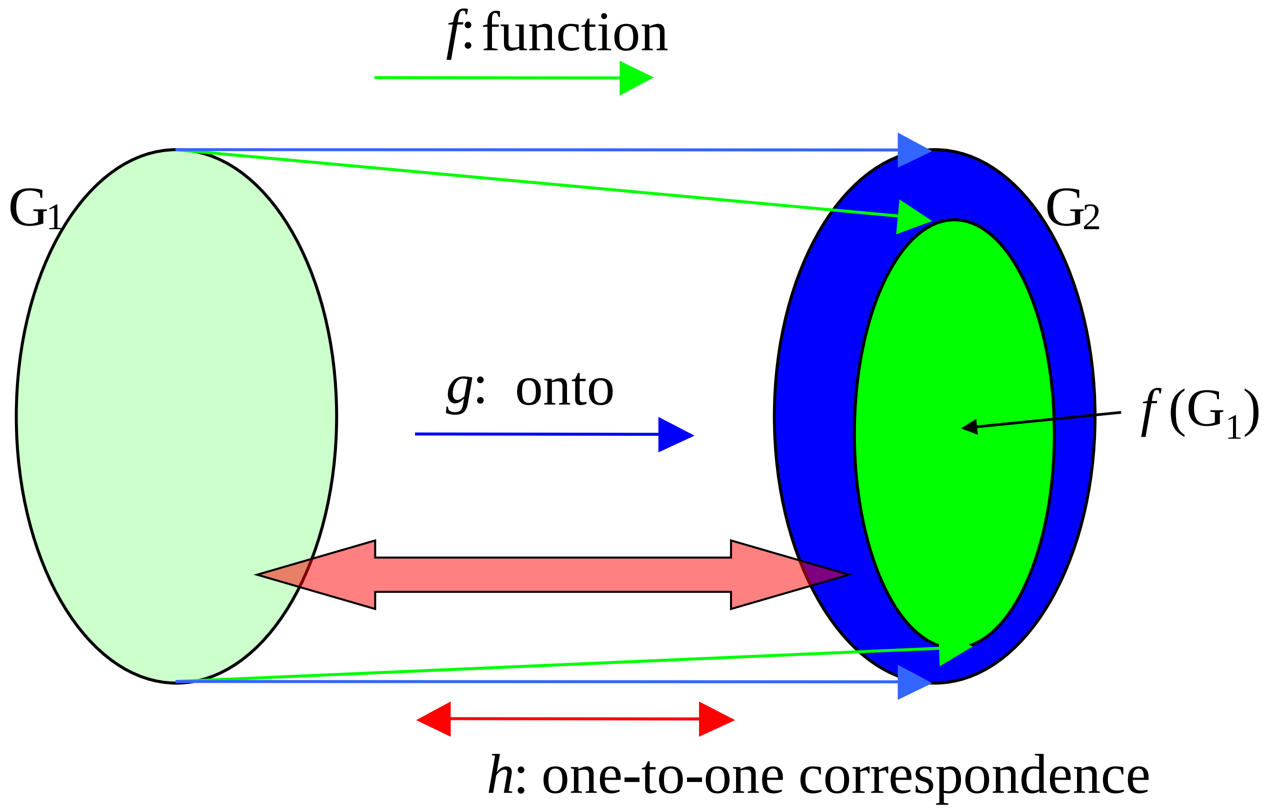
- Association
  - Assuming that f: $G_1 \rightarrow G_2$ is a homomorphism, and G_2 is a homomorphic image of G_1, then, if G_1 is associative, so is G_2, i.e. for any $x,y,z \in G_2$, (x y) z=x (y z)
- Proof:
  - for any $x',y',z' \in G_2$, since f is onto, there must be $x,y,z \in G_1$, such that $f(x)=x'$, $f(y)=y'$, $f(z)=z'$. So, $(x'*y')*z' =$ $(f(x)*f(y))*f(z) = f($x y$) * f(z) = f(($x y$)$ z$) = f($x (y z$)) = f(x)*(f(y)*f(z)) = x'*(y'*z')$
- Same discussion applies for commutation.

Homomorphic Image and System Properties

- Identity
  - Assuming that f: $G_1 \to G_2$ 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.

Holding the System Properties



Homomorphism and Subsystem

- Let f be a homomorphism from a semigroup (S,) to a semigroup (T,*). If S' is a subsemigroup of (S,), then

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

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

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

Products of Semigroup

- If $(S,\ \ )$ and $(T,*)$ are semigroups, then $(S\times T, \otimes)$ is also a semigroup, called **product of semigroups** $(S,\ \ )$ and $(T,*)$, where $\otimes$ is defined by $(s_1,t_1)\otimes(s_2,t_2)=(s_1\ \ s_2, t_1*t_2)$
- Proof
  - Obviously, $(S\times T, \otimes)$ is a algebraic system
  - [Associative] $((s_1,t_1)\otimes(s_2,t_2))\otimes(s_3,t_3) = ((s_1\ \ s_2)\ \ s_3, (t_1*t_2)*t_3) = (s_1\ \ (s_2\ \ s_3), t_1*(t_2*t_3)) = (s_1,t_1)\otimes((s_2,t_2)\otimes(s_3,t_3))$

Products of Monoid

- If $(S,\ \ )$ and $(T,*)$ are monoids, with identities e_s and e_t, then $(S\times T, \otimes)$ is also a monoid , called **product of monoids** $(S,\ \ )$ and $(T,*)$, where $\otimes$ is defined by $(s_1,t_1)\otimes(s_2,t_2)=(s_1\ \ s_2, t_1*t_2)$. And the identity of $(S\times T, \otimes)$ is (e_S,e_T)
- Proof
  - Obviously, $(S\times T, \otimes)$ is a algebraic system
  - [Associative] $((s_1,t_1)\otimes(s_2,t_2))\otimes(s_3,t_3) = ((s_1\ \ s_2)\ \ s_3, (t_1*t_2)*t_3) = (s_1\ \ (s_2\ \ s_3), t_1*(t_2*t_3)) = (s_1,t_1)\otimes((s_2,t_2)\otimes(s_3,t_3))$
  - [Identity] For any $s\in S$, $t\in T$, $(s,t)\otimes(e_s,e_t) = (s\ \ e_S, t*e_T) = (s,t)$; same with $(e_s,e_t)\otimes(s,t)$

Congruence

- An example: defining a relation on the set of integer as: a≡b (mod 3) iff. |a-b|/3 is an integer
  - It is an equivalence
  - equivalence class: $\pi_1=\{\ldots -3,0,3,6,9,\ldots\}$

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

    $\pi_3=\{\ldots -1,2,5,8,11,\ldots\}$
- Note: if x_1,x_2 are in the same class, and y_1,y_2 in same class, then x_1+y_1 and x_2+y_2 are in the same class.
- Generalized: An equivalence relation R on the semigroup $(S,*)$ is called a congruence relation if

$$aRa' \text{ and } bRb' \text{ imply } (a*b)R(a'*b')$$

Congruence on a Free Semigroup

- Let $A=\{0,1\}$. A^* is the set of all finite sequence of elements of A. Then, A^* with the operation catenation is a semigroup, called free semigroup generated by A.
- Define relation R on A^* as following:

$$\alpha R \beta \text{ iff. } \alpha \text{ and } \beta \text{ have the same number of 1's}$$

- R is an equivalence
- R is a congruence relation
  - Suppose α_1 and α_2 have the same number of 1's, and β_1 and β_2 have the same number of 1's. Note the number of the number of 1's in $\alpha\beta$ is the sum of that in α and β, so, $\alpha_1\beta_1$ and $\alpha_2\beta_2$ have the same number of 1's

All Equivalences are not Congruence

- (Z,+) is a semigroup, where "+" is common addition operation.
- Given a function $f(x)=x^2-x-2=(x+1)(x-2)$, a relation on Z is defined as following:

$$aRb \text{ if and only if } f(a)=f(b)$$

- R is an equivalence
- R is **not** a congruence relation
  - Note that $(-1)R2$, and, $(-2)R3$, but **not** $(-3)R5$

Quotient Semigroup

- Let R is a congruence relation on the semigroup $(S,*)$. 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 semigroup, called **quotient semigroup**

Natural Homomorphism

- Any semigroup and its corresponding quotient semigroup are onto homomorphic
- Let $(S/R,\otimes)$ is the corresponding quotient semigroup of semigroup $(S,*)$, define a function $f_R:S\rightarrow S/R$ as following:

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

  - By the definition of equivalence class, f_R is a well-defined onto function from S to S/R.
  - For any a,b in S, $f_R(a*b)=[a*b]=[a]\otimes[b]=f_R(a)\otimes f_R(b)$, which means f_R is a homomorphism.

A Congruence Relation Determined by a Homomorphism

R defined on *S*

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

R is a congruence relation:

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

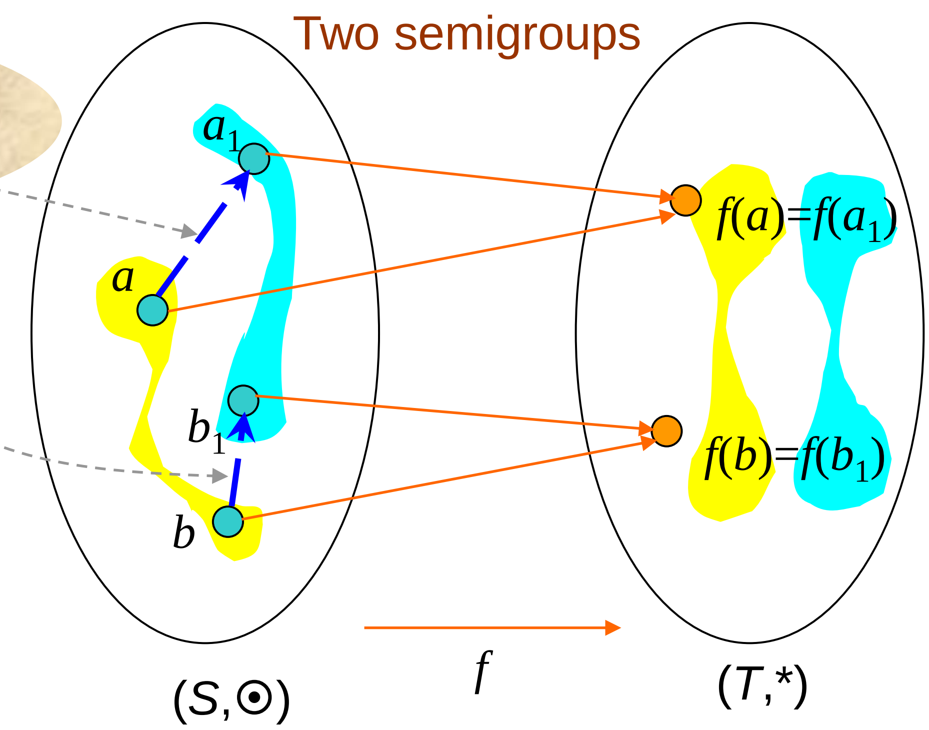
$f(a_1 \odot b_1) = f(a_1) * f(b_1)$

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

Which means:

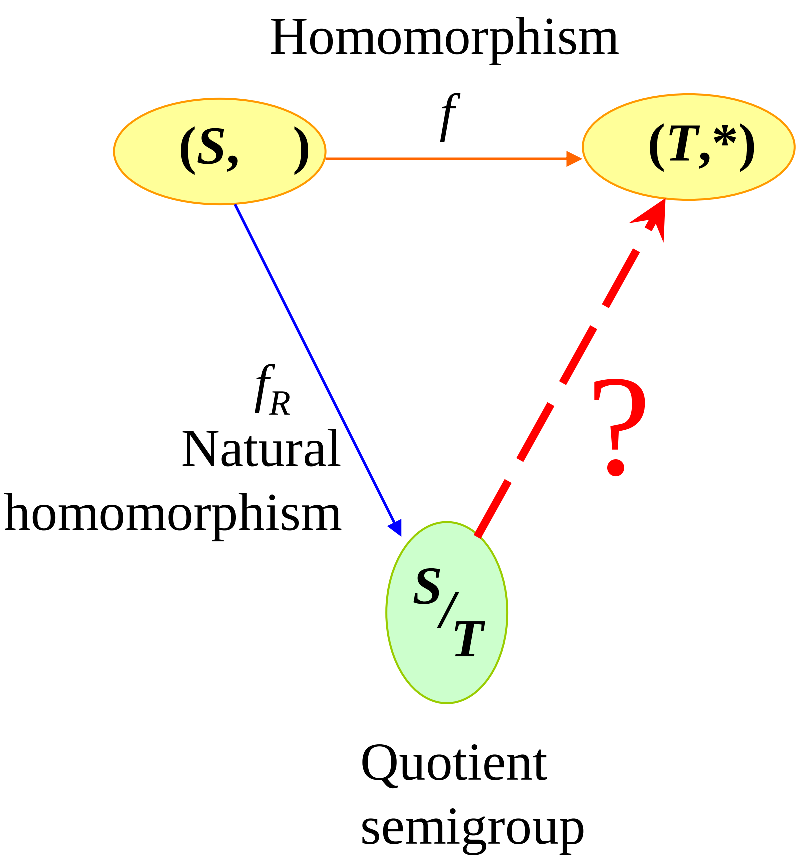
$$f(a \odot b) = f(a_1 \odot b_1)$$

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



f is a homomorphism

Fundamental Homomorphism Theorem



Define g: $S/T \to T$ as following:

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

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:

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

An Example of Free Semigroup

f: $A^*\to N$: $f(\alpha)$=the number of 1's in α

Define relation R on A^* as following:

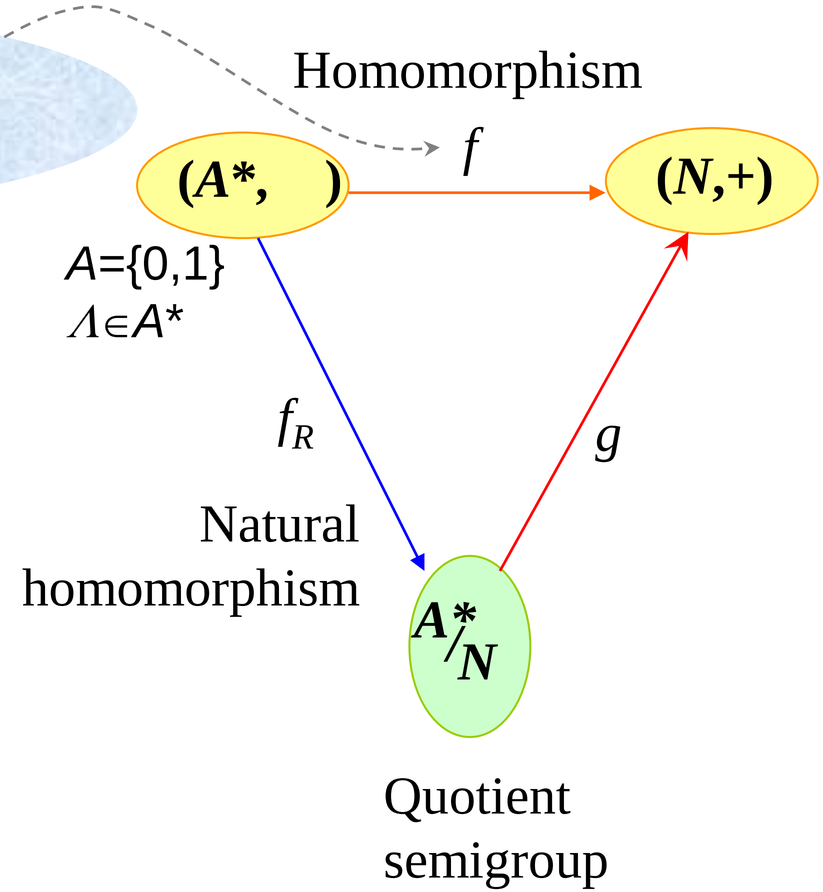
$\alpha R\beta$ iff. $f(\alpha)=f(\beta)$

Then, by the fundamental homomorphism theorem:

$A^*/N \cong N$,

and the ismorphism is:

$g[\alpha]$=the number of 1's in α. and $f = g \quad f_R$



Home Assignments

- To be checked
  - pp.348-: 5-8, 15-19, 20,22,25, 27-29, 32
  - pp.354 -: 6,8,10,14,18,21,22,26-27, 31-32, 35-36
  - pp.361 -: 2, 4, 8,10,14,16,18,23-24, 26, 28, 30