LECTURE 38
GROUPS

Scribe prepared by:
Anshul Gupta
07CS3020

Teacher: Prof. Niloy Ganguly
Department of Computer Science and Engineering
IIT Kharagpur
10-11-2008

Groups :

A group (G,x) is a monoid, with identity *e* ,that has the additional property that for every element a in G, there exists a_1 in G such that

$a * a_1 = a_1 * a = e$ i.e.

- (a*b)*c = a*(b*c).
- There exists a unique identity element *e*
- There exists an inverse for every element of G

Abelian Group :

An abelian group is a special type of group in which apart from the above properties, the commutative property should also be satisfied i.e.

$$a*b = b*a$$

Example :

Let G be the set of all nonzero real numbers and define a*b as: a*b=ab/ 2.

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

Solution :

We first verify that * is a binary operation. If a and b are elements in G, then ab/2 is a nonzero real number and hence is in G.

We next verify associativity ,

$$(a*b)*c = (ab/2)*c = ((ab/2)c/2) = abc/4$$

$$a*(b*c) = a*(bc/2) = (a(bc/2)/2) = abc/4$$

Hence the operation * is associative.

It is easy to see that a*2 = 2*a = a . Hence 2 is the identity in G.

Finally we verify that $a^{-1} = 4/a$.

$$a*(4/a) = 2 = (4/a)*a$$

Also since a*b = b*a for all a,b in G,we conclude that G is an Abelian group.

Theorem 1:

Let G be a group. Each element a in G has only one inverse in G i.e. inverse of an element is unique.

Proof:

Let , if possible, a’ and a” be two inverses of a. Then

$$a'(aa'') = a'e = a' \quad \text{and}$$

$$(a'a)a'' = ea'' = a''$$

By associativity , we get that that a’ = a”.

Hence the inverse of a is unique.

Theorem 2:

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

i. ab = ac implies that b=c. **(left cancellation law)**
ii. ba = ca implies that b=c. **(right cancellation law)**

Proof:

i.

$$ab = ac$$

Multiplying both sides by a^{-1} , we obtain

$$a^{-1}(ab) = a^{-1}(ac)$$

$$(a^{-1}a)b = (a^{-1}a)c$$

$$eb=ec$$

$$b=c.$$

ii. The proof is similar to part 1

Corollary:

Let G be a group and a its element. Define a function M_a : G -> G by the formula $M_a(g)$ = ag . Then M_a is one to one .

Theorem 3:

Let G be a group and a,b its elements. Then

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

Proof:

1. We show that a acts as an inverse for a^{-1}

$$a^{-1}a = a\,a^{-1} = e$$

Since the inverse is unique, $(a^{-1})^{-1} = a$.

2. We easily verify that

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

Similarly

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

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

Theorem 3:

Let G be a group and a,b its elements. Then

1. The equation ax=b has a unique solution in G
2. The equation ya=b has a unique solution in G

Proof:

1. We see that the element $x=a^{-1}b$ is the solution of the equation

   Suppose now that x_1 and x_2 are two solutions , then

$$ax_1 = ax_2 = b$$

   Therefore $x_1=x_2$ from Theorem 2.

2. Proof is similar to part 1

Groups of different sizes:

1. Size =1 :

	e
e	e

2. Size =2 :

	e	a
e	e	a
a	a	e

3. Size = 3 :

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

Subgroup :

If g is a group ,H is a subgroup of G if

1) The identity of G belongs to H
2) If a belongs to H, then a^{-1} should also belong to H
3) If a and b belong to H, then ab should also belong to H

Note that G is itself a subgroup of G

Isomorphism :

Let (S,*) and (T, ^) be two groups. A function f : S -> T is called an isomorphism from (S,*) to (T, ^) if it is a one to one correspondence from S to T such that

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

for all a and b in S.

Homomorphism :

Let (S,*) and (T, ^) be two groups. An everywhere defined function f : S -> T is called a homomorphism from (S,*) to (T, ^) if

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

for all a and b in S.

Theorem :

Let (S,*) and (T, ^) be two groups. A function f : S -> T be a homomorphism from S to T. Then

1) If e is an identity in S and e' in T. Then f(e) = e'
2) If a is in S, then $f(a^{-1})=(f(a))^{-1}$
3) If H is a subgroup of S, its image H' will be a subgroup in T