COURSE 1- GROUP 1

Lecture 1

Definition: A binary operation is G×G→G, a, b in G

Definition: A * is called associative if a*(b*c)=(a*b)*c, a, b, c in G.

Definition: A * is called closed if a*b in G.

Example: (N, +) is closed for all a, b in G.

$a+b\in \mathbb{N}\ \forall\ a,b\in \mathbb{N}$

Remark:

(N, -) is not closed because

$1,2\in \mathbb{N}$

but

$1-2=-1\notin \mathbb{N}$.

Definition:

A non empty set G with (*) is called a group if:

1 - $a*b\in G\ a,b\in G$.

2 - $a*b\ *c=a*(b*c)\ a,b,c\in G$.

3 - $e\in G\ a*e=e*a=a\ a\in G$.

4 - $a\in G\ a-1\in G\ a*a-1=a-1*a=e$.

EXAMPLES:

1 - $a+b\in Z$ لكل $a,b\in Z$.

2 - $a+b\ +c=a+(b+c)$, $a,b,c\in Z$.

3 - $0\in Z\ \ a+0=0+a=a$, $a\in Z$.

4 - $a\in Z\ -a\in Z$ such that $a+\ -a\ =-a\ +a$

Also:

$P\ X=\{A: A\subseteq X\}$
1 - A,$B \in P(X)$
$A\subseteq X$, $B\subseteq X$ $A\cup B\subseteq X$ $A\cup B\in P\ X$
2 - $A,B,C \in P(X)$
$A\cup B\ \cup C=A\cup(B\cup C)$
3 - $\emptyset\subseteq X$
$\emptyset\in P\ X$
$A\cup\emptyset=\emptyset\cup A=A$
4 - $A\in P(X)$
$A\cup A-1=A-1\cup A=\emptyset$
$a*b=b*a\ \forall\ a,b \in G$
مثال : $(Z,+)$ commutative group

Theorem
1-The identity is a unique
2-The inverse
3 - $a-1\ -1=a\ a\ \in$

Lecture 2

$a*e1=a\ a*e2=a\ \forall\ a\in G\ a*e1=a*e2\ a-1*\ a*e1$
$=a-1*\ a*e2\ a-1*a\ *e1=\ a-1*a\ *e2\ e1*e1=e2*e2$
$e1=e2$

The identity unique

$a*a1-1=e\ a*a2-1=e\ \forall\ a\in G$
$a*a1-1=a*a2-1$

$a-1\ -1*a-1=e\ a*a-1=\ a-1\ -1*a-1\ a*a-1\ *a=$
$a-1\ -1*a-1\ *a\ a*a-1\ *a=\ a-1\ -1*\ a-1*a\ e*a=$
$a-1\ -1*e\ a=\ a-1\ -1$
$a,b\in G$
$a*b\ *\ b-1*a-1\ =a*\ b*b-1\ *a-1$
$=a*e*a-1=a*a-1=e$
$b-1*a-1\ *\ a*b\ =b-1*\ a-1*a\ *b$
$=b-1*e*b=b-1*b=e$
$\therefore\ b-1*a-1\ a*b$
ولكن $a*b\ -1\ ,\ a*b$
$\therefore\ a*b\ -1=b-1*a-1$
: $(G,*)$ group , $a*b=a*c$ و $b=c$, $a,b,c\in G$
: Let $a,b,c\in G$
$a*b=a*c\ a-1*\ a*b\ =a-1*\ a*c\ a-1*a\ *b=\ a-1*a$
$*c\ e*b=e*c\ b=c$
Definition
: Let $(G,*)$ be a group
: let $(G,*)$ group , $a\in G$, then
1 - $ak=a*a*a*\ldots*a$, $k\in Z$.
2 - $a0=e$.
3 - $a-k=a-1*a-1*a-1*\ldots*a-1$, $k\in Z$.
$(Z,+)$, so
23=2+2+2=6 80=0 3−2=(3−1)2=(−3)2=−3+ −3
=−6
: let $(G,*)$ group , $m,n\in Z$, $a\in G$, then
1 - $an*am=an+m$.
2 - $an\ m=an\ m$.
3 - $en=e$.
4 - $a-n=\ an\ -1$

Proof
1 -
$an*am=a*a*\ldots*a * a*a*\ldots*a$
n , n-times

$=a*a*a*\ldots*a =an+m$
$n+m$, n-times

LECTURE 3

Subgroups and Langrage Theorem

A subgroup of a group G is a subset which is a group under the same operation as in G. The following definition will help to make this last phrase precise.

Definition (1): Let $*$ be an operation on a set G, and let S ⊆ G be a
subset. We say that S is closed under $*$ if $x * y \in S$ for all $x , y \in S$.
The operation on a group G is a function *: G x G G.
(for example, 2 and −2 lie in Z+, but their sum −2 + 2 = 0 ∈/Z+.
Definition (2): A subset H of a group G is a subgroup if:
(i) 1 ∈ H ; 2

(ii) If x , y ∈ H , then x y ∈ H ; that is, H is closed under ∗.
(iii) If x ∈ H , then x^{-1} ∈ H .

Proposition (3): Every subgroup H ≤ G of a group G is itself a group.

Proof: Axiom (ii) (in the definition of subgroup) shows that H is closed under the operation of G; that is, H has an operation (namely, the restriction of the operation ∗: G × G → G to H × H ⊆ G × G. This operation is associative:
since the equation (x y)z = x (yz) holds for all x , y, z ∈ G, it holds, in particular, for all x , y, z ∈ H .
Finally, axiom (i) gives the identity, and axiom (iii) gives
inverses. 3
It is quicker to check that a subset H of a group G is a subgroup (and hence that it is a group in its own right) than to verify the group axioms for H, for associativity is inherited from the operation on G and hence it need not be verified again.

CYCLIC GROUPS

LECTURE 4

Definition (9): If G is a group and a ∈ G, write
(a)= {an: n ∈Z+} = {all powers of a}
(a) is called cyclic subgroup of G generated by a.

Proposition (10): The intersection of any family of subgroups is again subgroup.

Definition (1): If H is a subgroup of a group G and a G, then the coset a H is the subset a H of G, where a H = {ah: h □ H } of course, a = ae ∈ a H. Cosets are usually not subgroups.

The cosets just defined are often called left cosets; there are also right cosets of H, namely, subsets of the form H a {ha| h in H}; these arise in further study of groups, but we shall work almost exclusively with (left) cosets. In particular, if the operation is addition, then the coset is denoted by a + H = {a + h : h in H }.

Homomorphism

LECTURE 5

An important problem is determining whether two given groups G and H are somehow the same.

Definition :
If (G, *) and (H, ◦) are groups, then a function f: G → H is a homomorphism if:
f (x * y) = f (x) ◦ f (y)
for all x , y in G. If f is also a bijective, then f is called an isomorphism. We say that G and H are isomorphic, denoted by G H, if there exists an isomorphism f: G → H.

Example (2):
Let be the group of all real numbers with operation addition, and let R+ be the group of all positive real numbers with operation multiplication. The function f: R→ R+ , defined by f(x)=tx , where t is constant number, is a homomorphism; for if x , y in R, then f (x + y) = t(x+y) = tx ty = f (x) f (y).
We now turn from isomorphisms to more general homomorphisms.

Lemma (3): Let f: G → H be a homomorphism.
(i) f (e) = e;
(ii) f (x −1) = f (x)−1;

Definition (6): If f: G → H is a homomorphism, define
kernel f = {x in G : f (x) = e}
and image f = {h in H : h = f (x) for some x inG}.
We usually abbreviate kernel f to ker f and image f to im f . So that if f: G □ H is a homomorphism and B is a subgroup of H then $f^{-1}(B)$ is a subgroup of G containing ker f .

Note: Kernel comes from the German word meaning “grain” or “seed” (corn comes from the same word).
Its usage here indicates an important ingredient of a homomorphism, we give it without proof.

Proposition: Let f: $G \to H$ be a homomorphism.

(i) ker f is a subgroup of G and im f is a subgroup of H .

LECTURE 6

(ii) If x in ker f and if a in G, then ax a^{-1} in ker f.

(ii) f is an injection if and only if ker f = {e}.

Normal Subgroups

Definition (1): A subgroup K of a group G is called normal, if for each k in K and g in G imply gkg^{-1} in K. that is gKg^{-1} in G for every g in G.

Definition (2):

Define the center of a group G, denoted by Z (G), to be Z (G) = {z in G: zg = gz for all g in G}; that is, Z (G) consists of all elements commuting with every element in G. (Note that the equation zg

= gz can be rewritten as $z = gzg^{-1}$, so that no other elements in G are conjugate to z.

Remark (3):

Let us show that Z (G) is a subgroup of G. We can easily show that Z(G is subgroup of G. It is clear that Z(G)≠ since 1 ∈ Z (G), for 1 commutes with everything. Now, If y, z in Z (G), then yg = gy and zg = gz for all g in G. Therefore, (yz)g = y(zg) = y(gz) = (yg)z = g(yz), so that yz commutes with everything, hence yz in Z (G). Finally, if z in Z (G), then zg = gz for all g in G; in particular, $zg^{-1} = g^{-1}z$. Therefore,

$$gz^{-1} = (zg^{-1})_{-1} = (g^{-1}z)^{-1} = z^{-1}g$$

(we are using $(ab)^{-1} = b^{-1}a^{-1}$ and $(a^{-1})^{-1} = a$). So that Z(G) is subgroup pf G.

Clearly che center Z (G) is a normal subgroup; since if z in Z (G) and g in G, then $gzg^{-1} = zgg^{-1} = z$ in Z (G).

A group G is abelian if and only if Z (G) = G. At the other extreme are groups G for which Z (G) = {1}; such groups are called centerless. For example, it is easy to see that Z (S3) = {1}; indeed, all large symmetric groups are centerless.

Remark (4):
We can show that any two finite cyclic groups G and H of the same order m are isomorphic. It will then follow from that any two groups of prime order p are isomorphic.

Definition (5):
A property of a group G that is shared by every other group isomorphic to it is called an invariant of G. For example, the order, G, is an invariant of G, for isomorphic groups have the same order. Being abelian is an invariant [if a and b commute, then ab = ba and
f (a) f (b) = f (ab) = f (ba) = f (b) f (a);
hence, f (a) and f (b) commute]. Thus, M2x2 and GL(2,R) are not isomorphic, for is abelian and GL(2,R) is not.

Proposition (2): Let G be a group, and H be a subgroup of G, for any a, b G we have the following:

(iii) a H = b H if and only if b−1a H . In particular, a H = H if and only if a H.

(ii) If a H ∩ b H ≠ , then a H = b H.

(iv) For each aG: Order of H is equal to the order of Ah.

Proof:

(v) It is clear.

(ii) It is clear.

(vi) The function f: H → a H which is given by f (h) = ah, is easily seen to be a bijective [its inverse a H → H is given by ah r→ a−1(ah) = h]. Therefore, H and a H have the same number of elements.

THE INDEX OF GROUP

LECTURE 7

Proposition (4):

(i) If H is a subgroup of index 2 in a group G, then g_2 H for every g in G.

(ii) If H is a subgroup of index 2 in a group G, then H is a normal subgroup of G.

Proof:

(i) Since H has index 2, there are exactly two cosets, namely, H and a H, where a inG/H. Thus, G is the disjoint union G = H =a H. Take g in G with g H. So that g = ah for some h in H. If g_2 H, then g2 = ah_1, where h_1 in H . Hence, g = g^{-1} g_2 = (ah)−1a h_1 = $h^{-1}a^{-1}a$ h_1 = h^{-1} h1in H, and this is a contradiction.

(ii) It suffices to prove that if h in H , then the conjugate ghg^{-1} in H for every
g ∈ G. Since H has index 2, there are exactly two cosets, namely, H and a H,
where a H. Now, either g inH or g in a H. If g inH, then ghg^{-1}inH,
because H is a subgroup. In the second case, write g = ax, where x in H. Then
ghg−1 = $a(x hx^{-1})a^{-1} = ahIa^{-1}$, where hI = $x hx^{-1}$ in H (for hI is a product
of three elements in H). If ghg H, then ghg^{-1} = $ahIa^{-1}$ = a H ; that is,

$ahIa^{-1}$ = ay for some y in H. Canceling a, we have hIa−1 = y, which gives the contradiction a = y^{-1}hI in H. Therefore, if h in H, every conjugate of h also lies in H; that is, H is a normal subgroup of G.

Proposition(5) : If K is a normal subgroup of a group G, then

bK = K b

for every b in G.

Proof: We must show that bK = Kb and Kb = bK.

So if bk=bK, then clearly bK = $bKb^{-1}b$.

Since bKb^{-1}inK, then bKb^{-1}= k1 for some $k_1$inK.

This implies that bK□Kb. Similarity for the other case. Thus bK = Kb.

LECTURE 8

Theorem (3): (Lagrange's Theorem)

If H is a subgroup of a finite group G, then |H | is a divisor of |G|. That is:

$$|G| = [G : H]|H|$$

This formula shows that the index [G : H] is also a divisor of |G|.

Coset of sets

Corollary (4): If H is a subgroup of a finite group G, then

$$[G : H] = |G|/|H|$$

Corollary (5): If G is a finite group and a in G, then the order of a is a divisor of |G|.

Corollary (6): If a finite group G has order m, then am = e for all a in G.

Corollary (7): If p is a prime, then every group G of order p is cyclic.

Proof: Choose a in G with $a \neq e$, and let H = (a) be the cyclic subgroup generated by a. By Lagrange's theorem, $|H|$ is a divisor of $|G| = p$. Since p is a prime and $|H| > 1$, it follows that $|H| = p = |G|$, and so H = G.

Lagrange's theorem says that the order of a subgroup of a finite group G is a divisor of G . Is the "converse" of Lagrange's theorem true? That is, if d is a divisor of G, must there exists a subgroup of G having order d? The answer is "no;" We can show that the alternating group A4 is a group of order 12 .