كورس ١- زمر
المحاضرة ١

) ثنائية عممية تسمى $G\times G \longrightarrow G$: ∗ الة الد فان خالية غير مجموعة G لتكن **:**

Binary operation (عمى G

تعريف : لتكن $A\subseteq G$ ولتكن ∗ عممية ثنائية عمى G تسمى المجموعة A مغمقة بفعل

العممية ∗ إذا كان

لأنو وذلك) + الطبيعية الأعداد مجموعة **:**

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

لأنو وذلك (−) الطرح عممية بفعل مغمقة ليست ولكنيا

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

ولكن

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

تعريف : لتكن G مجموعة غير خالية , ∗ عممية ثنائية معرفة عمى G فيقال لمزوج المرتب

زمرة $(G,*)$

(Group (إذا تحققت الشروط الآتية :

1 - $a*b\in G$ لكل $a,b\in G$.

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

3 - وٌجد $e\in G$ بح ثٌ ان $a*e=e*a=a$ لكل $a\in G$.

) سٌمى e العنصر المحا دٌ (

4 - لكل $a\in G$ وٌجد $a-1\in G$ بح ثٌ ان $a*a-1=a-1*a=e$.

) سٌمى $a-1$ العنصر النظ رٌ للعنصر a)

مثال : مجموعة الأعداد الصحيحة Z مع عممية الجمع) + (تشكل زمرة

1 - $a+b\in Z$ لكل $a,b\in Z$.

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

3 - وٌجد $0\in Z$ بح ثٌ ان $a+0=0+a=a$ لكل $a\in Z$.

4 - لكل $a\in Z$ وٌجد $-a\in Z$ بح ثٌ ان $a+\ -a\ =\ -a\ +a$

مثال : إذا كانت X مجموعة غير خالية . فان الزوج المرتب $(P\ X\ ,\text{U})$ يكون شبو زمرة ذات

عنصر

محايد

$P\ X\ =\{A:\ A\subseteq X\}$

1 - ل كٌن $A,B\ \in P(X)$

$A\subseteq X\ ,\ B\subseteq X\ A\cup B\subseteq X\ A\cup B\in P\ X$

2 - ل كٌن $A,B,C\ \in P(X)$

$A\cup B\ \cup C=A\cup(B\cup C)$ المجموعات خواص حسب

3 - $\emptyset\subseteq X$
$\emptyset\in P\ X$
$A\cup\emptyset=\emptyset\cup A=A$
∴ العنصر المحا دٌ هو $\emptyset$
4 - لِ كُنْ $A\in P(X)$
ان ثُ بح رٌ نظ وٌجد لا
$A\cup A_{-1}=A_{-1}\cup A=\emptyset$
∴ $(P\ X\ ,\cup)$ لِ سٌ زمرة لكن شبه زمرة ذات عنصر محا دٌ .

تعريف : لمزمرة يقال $(G,*)$ زمرة بانيا ابدالية اذا وفقط اذا كان

$a*b=b*a\ \forall\ a,b\ \in G$

مثال : $(Z,+)$ زمرة ابدالية

مبرهنة 1 : لتكن $(G,*)$ زمرة فان

1 - العنصر المحا دٌ وح دٌ .
2 - العنصر النظ رٌ وح دٌ .

$a\in$ لكل3 - $a_{-1}{}_{-1}=a$

المحاضرة ٢

$a*e_1=a\ a*e_2=a\ \forall\ a\in G\ a*e_1=a*e_2\ a_{-1}*\ a*e_1\ =a_{-1}*\ a*e_2\ a_{-1}*a\ *e_1= a_{-1}*a\ *e_2\ e_1*e_1=e_2*e_2\ e_1=e_2$

∴ وحيد المحايد العنصر

2 - لِ كُنْ من كل a_{1-1} , a_{2-1} للعنصر رٌ نظ عنصر a

$a*a_{1-1}=e\ a*a_{2-1}=e\ \forall\ a\in G$

وحيد المحايد العنصر ان بما

$a*a_{1-1}=a*a_{2-1}$
$a_{-1}{}_{-1}*a_{-1}=e\ a*a_{-1}=\ a_{-1}{}_{-1}*a_{-1}\ a*a_{-1}\ *a=\ a_{-1}{}_{-1}*a_{-1}\ *a\ a*a_{-1}\ *a= a_{-1}{}_{-1}*\ a_{-1}*a\ e*a=\ a_{-1}{}_{-1}*e\ a=\ a_{-1}{}_{-1}$

ليكن $a,b\in G$

$a*b\ *\ b_{-1}*a_{-1}\ =a*\ b*b_{-1}\ *a_{-1}\ =a*e*a_{-1}=a*a_{-1}=e$
$b_{-1}*a_{-1}\ *\ a*b\ =b_{-1}*\ a_{-1}*a\ *b\ =b_{-1}*e*b=b_{-1}*b=e$

∴ $b_{-1}*a_{-1}$ هو نظير العنصر $a*b$

ولكن $a*b\ _{-1}$ هو نظير العنصر $a*b$

وبما ان العنصر النظير وحيد

∴ $a*b\ _{-1}=b_{-1}*a_{-1}$

: لتكن $(G,*)$ زمرة , $a*b=a*c$ فان $b=c$ لكل $a,b,c\in G$

: ليكن $a,b,c\in G$

$a*b=a*c$ $a_{-1}*$ $a*b$ $=a_{-1}*$ $a*c$ $a_{-1}*a$ $*b=$ $a_{-1}*a$ $*c$ $e*b=e*c$ $b=c$

تعريف : لتكن $(G,*)$ زمرة

: لتكن $(G,*)$ زمرة , $a\in G$ فان القوى العددية لمعنصر بي كالآتي :

1 - $a_k=a*a*a*\ldots*a$ ح ثٌ ان $k\in Z$.

k من الم ا رت

2 - $a_0=e$.

3 - $a_{-k}=a_{-1}*a_{-1}*a_{-1}*\ldots*a_{-1}$ ح ثٌ ان $k\in Z$.

k من الم ا رت

ان نجد $(Z,+)$ الزمرة في

$2_3=2+2+2=6$ $8_0=0$ $3_{-2}=(3_{-1})_2=(-3)_2=-3+\ -3\ =-6$

: لتكن $(G,*)$ زمرة , $m,n\in Z$, $a\in G$ فان :

1 - $a_n*a_m=a_{n+m}$.

2 - $a_{n\ m}=a_{n\ m}$.

3 - $e_n=e$.

4 - $a_{-n}=\ a_{n\ -1}$

البرهان :

1 -

$a_n*a_m=a*a*\ldots*a\ *\ a*a*\ldots*a$

m من المرات n من المرات

$=a*a*a*\ldots*a\ =a_{n+m}$

المرات من$n+m$

المحاضرة ٣

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) $1 \in H$; 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

المحاضرة ٤

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 □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 □ H }.

Homomorphism

المحاضرة ٥

An important problem is determining whether two given groups G and H are somehow the same. 155

Definition (1): 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 □ 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 □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 □ G : f (x) = e}

and **image f** = {h □ H : h = f (x) for some x □G}.

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 → H be a homomorphism.

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

المحاضرة ٦

(ii) If x □ ker f and if a □ G, then ax a−1□ ker f.

(iii) 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 □ K and g □ G imply gkg−1□ K. that is gKg-1 □ G for every g□G.

Definition (2):

Define the **center of a group G,** denoted by Z (G), to be

Z (G) = {z □ G: zg = gz for all g □ 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 □ Z (G), then yg = gy and zg = gz for all g □ G. Therefore, (yz)g = y(zg) = y(gz) = (yg)z = g(yz), so that yz commutes with everything, hence yz □ Z (G). Finally, if z □ Z (G), then zg = gz for all g □ G; in particular, zg−1 = g−1 z. Therefore,

gz−1 = (zg−1)−1 = (g−1z)−1 = z−1g

(we are using (ab)−1 = b−1a−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 □ Z (G) and g □ G, then

gzg−1 = zgg−1 = z □ 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:

(i) 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.

(iii) For each a□G: Order of H is equal to the order of aH.

Proof:

(i) It is clear.

(ii) It is clear.

(ii) 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

المحاضرة ٧

Proposition (4):

(i) If H is a subgroup of index 2 in a group G, then g2 □ H for every g □ 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 □G\H. Thus, G is the disjoint union G = H □a H. Take g □ G with g H. So that g = ah for some h □ H. If g2 H, then g2 = ah1, where h1 □ H . Hence, g = g−1 g2 = (ah)−1a h1 = h−1a−1a h1 = h−1 h1□ H, and this is a contradiction.

(ii) It suffices to prove that if h □ H , then the conjugate ghg−1 □ 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 □H or g □a H. If g □H, then ghg−1□H, because H is a subgroup. In the second case, write g = ax, where x □ H. Then ghg−1 = a(x hx −1)a−1 = ahIa−1, where hI = x hx −1 □ 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 □ H. Canceling a, we have hIa−1 = y, which gives the contradiction a = y−1hI □ H. Therefore, if h □ 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 □ G.

Proof: We must show that bK □ Kb and Kb □ bK. So if bk□bK, then clearly bK = bKb-1b.

Since bKb-1□K, then bKb-1= k1 for some k1□K. This implies that bK□Kb. Similarity for the other case. Thus bK = Kb. 125

المحاضرة ٨

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 □ 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 □ G.

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

Proof: Choose a □ G with a≠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 .