|  |
| --- |
| **SUBMITTED BY:**  **Bishal Pandey**  **ROLL NO: 17**  **A assignment submitted to our respective Teacher**  **MR. Kalyan Dahal**  **IN PARTIAL FULFILLMENT OF INTERNA ASSIGNMENT**  **BICTE 2ND SEMESTER**  C:\Users\HP\AppData\Local\Microsoft\Windows\INetCache\Content.Word\Screenshot 2023-04-20 214228.png  **AT**  **SUNDARHARAINCH-12, MORANG** |

**1.De-moirreme's Theorem: If h is any positive integers and z=r(cos θ + I \*sin θ) be a complex number, then[r(cos θ+ i\*sin θ)]n =rn ( cos θ + I\*sin θ ).**

proof: we prove this theorem by mathematical induction method.

if n=1, [r (Cos θ+ I \*Sin θ)]1= r(cos θ+ I \*sin θ) which is true for n=1.

if n=2, [r (Cos θ +i\*Sin θ)]2= r2[(cos2 θ +I \*2\*cos θ + sin θ+i2sin2\*sin2 θ]

= r2[cos2 θ – Sin2 θ) + i\*Sin2 θ]

= r2[cos2 θ – Sin2 θ) which is true for n=2.

The statement is true for n=1 and n=2. let us assume that the statement is true for n=k. i.e. [r (Cos θ + i\*Sin θ)k=rk( Cos k θ + I \*Sin k θ)

Now, we have to show that is true for n=k+1.

so, [r (Cos θ+ i\*sin θ)]k+1=[r (cos θ +I \*sin θ)]k\*[r cos θ +I \*sin θ +I \*sin θ)]1

= rk [ cos k θ+ sin k θ] \*r(cos θ+ i\*sin θ)­­­­­­­­­­

= rk+1[cos (k θ+ θ )+i\*sin(k θ+ θ)­­­]

= rk+1[cos (k +1) θ +i\*sin(k + 1) θ ­­­] which is true for n=k+1.

Hence. the statements is true for n=1 and n=2.then, it is also true for n=k and n=k+1. so, the statement is true for all n.

**2. Theorem:- A non-empty subset H of group G is a subgroup G if (i) a, b ∈ H=a\*b ∈H (ii)a ∈H=a-1∈H**

proof: Let His subgroup of G then H itself is a group with the same binary operation in G. So, a, b ∈H=a\*b ∈H by closure axiom and a ∈H=a-1∈H by inverse. Conversely, let His non-empty subset of G and (i)a, b ∈H=a\*b ∈H (ii)a ∈H=a-1∈H. We have to show that H is subgroup of G. By(i) we have a\*b ∈H, closure property holds, \*is associative through G, so it also associative on the subset H of G. also, we have H is non-empty subset of G, so a∈ H by (ii),a ∈H=a-1∈ H (Inverse element) again by (I),a ,a-1 ∈H =a\* a-1∈ H =a\* a-1 = e ∈ H (Identity element).so , H satisfies all the conditions of G. Hence H is subgroup of G.

**3. Theorem:- Let G be a group the a subset H of G is subgroup G if (i) H≠ ø (ii) ab-1∈H for all a, b ∈ H.**

Proof. let H is a subgroup of G the H ≠ ø. Let a, b∈ H. since, H itself is a group. So, b∈ H=b-1∈ H. so, ab-1∈H.

Conversely, Let H is a subset of G such that (i) H≠ ø (ii) ab-1∈H for all a, b ∈ H.

We have to show that H is subgroup of G since, The binary operation'.' is associative throughout G so, it is also associative on the subset H. Since H≠ ø, so let a, b∈ H, by(ii)a, a ∈=a\*a-1∈ H=e∈ H since a\* a-1=e.

Let b ∈ H. since e∈ H so e, b ∈ H=e\* ab-1∈H. so, inverse also exists.

Again, Let a, b∈ H. Then a, b-1∈ H by (ii)a, b-1∈ H=a (b-1)-1=a\*b ∈ H, so closure is also existed.

4.Theorem:- The intersection of two subgroups of a group is also a subgroup.

proof:- let H and k are two subgroups of G. We have to show that H ∩ K is subgroup of G. Since H ∩ K is non-empty subset of G. Let a ,b ∈ H∩ K than, a, b∈ H and a, b∈ k=a –b∈K . since H and k are sub group of G then a, b∈ H = a –b∈ H and ab-1=a-b ∈ H and ab∈ K and ab-1∈K=a-b ∈H∩ K and ab-1∈H∩ K= H∩ K is subgroup of G.

5. Theorem:- Every cyclic group is an abelian group.

Let G be a cyclic group generated by an element g. That is, G = <g> = {gn: n ∈ Z}. Let x and y be any two elements in G. Then, by the definition of a cyclic group, we can write x = gm and y = gn for some integers m and n. Now, the product of these two elements is

xy = gm . gn

By using the associative and commutative properties of integer addition, we can rewrite this as

xy = gm+n = gn+m = gn . gm

xy = yx This shows that the group operation in G is commutative, and hence G is an abelian group.

**6 Theorem :- Prove that every subgroup of a cyclic group is cyclic.**

Let G be a cyclic group generated by an element g. That is, G = <g> = {gn: n ∈ Z}. Let H be a subgroup of G. We want to show that H is also cyclic.

If H is the trivial subgroup {e}, then H is cyclic and we are done.

If H is not trivial, then there must be some element h in H that is not e. Since h is in G, we can write h = gm for some integer m.

Let n be the smallest positive integer such that gn is in H. We claim that H is generated by gn, that is, H = <gn>.

To prove this, we need to show that every element of H is a power of gn. Let h be any element of H, and write h = gk for some integer k. By the division algorithm, we can find integers q and r such that k = nq + r, where 0 <= r < n.

Then, we have h = gk = gnq + r = (gn)q \* gr, so gr = (gn) -q \* h. Now since h is in H, gn is in H, and H is closed under inverses and multiplication, we have (gn) -q and h are in H. Thus (gn) -q \* h is in H; that is, gr is in H.

Since n was the smallest positive integer such that gn is in H and 0 <= r < n, we must have r = 0. Thus k = nq and h = gk = (gn)q, so h is a power of gn.

**7. Theorem:- If a is generator of cyclic group G, then a-1is a also generator of cyclic group.**

Let G be a cyclic group generated by a, and let n be the order of a. Then, for any element g in G, we can write g = a^k for some integer k. Now, the inverse of g is g^-1 = (ak)-1 = a^-k. We can also write a^-k as a^(n-k), since a^n = e. Therefore, g^-1 is also a power of a.

Now, let m be the order of a^-1. Then, a^m = (a-1)-m = e. This implies that m divides n, since a has order n. On the other hand, a^n = e implies that a^-n = e, so n is also a multiple of m. Hence, m and n are equal, and a and a^-1 have the same order.

This shows that a^-1 is also a generator of G, since any element of G can be written as a power of a^-1.

**8. Theorem :- The order of a cyclic group is same as the order of its generator.**

If G is a finite cyclic group generated by a, then we can write G = {a^k: k ∈ Z}, where Z is the set of integers. The order of G is the number of distinct elements in this set, and the order of a is the smallest positive n such that a^n = e, where e is the identity element of G. It can be shown that these two numbers are equal, that is, |G| = |a|, where |.| denotes the order.

**9. Theorem:- Every field is an integral domain.**

Let F be a field. We want to show that F is an integral domain, i.e., F is a commutative ring with identity, and the product of any two nonzero elements is nonzero.

First, we show that F is a commutative ring with identity. By definition, a field is a set with two binary operations, usually called addition and multiplication, that satisfy the following properties:

- F is closed under both addition and multiplication, i.e., for any a, b \in F, we have a + b \in F and a \cdot b \in F.

- Both addition and multiplication are associative, i.e., for any a, b, c \in F, we have (a + b) + c = a + (b + c) and (a \cdot b) \cdot c = a \cdot (b \cdot c).

- Both addition and multiplication are commutative, i.e., for any a, b \in F, we have a + b = b + a and a \cdot b = b \cdot a.

- There exists an additive identity, usually denoted by 0, such that for any a \in F, we have a + 0 = 0 + a = a.

- There exists a multiplicative identity, usually denoted by 1, such that for any a \in F, we have a \cdot 1 = 1 \cdot a = a.

- For every a \in F, there exists an additive inverse, usually denoted by -a, such that a + (-a) = (-a) + a = 0.

- For every a \in F \setminus \{0\}, there exists a multiplicative inverse, usually denoted by a^{-1}, such that a \cdot a^{-1} = a^{-1} \cdot a = 1.

These properties imply that F is a commutative ring with identity, where the identity elements are 0 and 1, respectively.

Next, we show that the product of any two nonzero elements is nonzero. Suppose a, b \in F \setminus \{0\}. Then, by the property of multiplicative inverses, we have a^{-1}, b^{-1} \in F \setminus \{0\}. Now, suppose for a contradiction that a \cdot b = 0. Then, multiplying both sides by a^{-1} \cdot b^{-1}, we get

a^{-1} \cdot b^{-1} \cdot a \cdot b = a^{-1} \cdot b^{-1} \cdot 0

Using the associativity and commutativity of multiplication, we can simplify the left-hand side as

(a^{-1} \cdot a) \cdot (b^{-1} \cdot b) = 1 \cdot 1 = 1Hence, we have 1 = a^{-1} \cdot b^{-1} \cdot 0. But this contradicts the property of the additive identity, which states that for any a \in F, we have a \cdot 0 = 0 \cdot a = 0. Therefore, we must have a \cdot b \neq 0, as desired. Hence, we have shown that every field is an integral domain.

**10 Theorem:- A skew field (division ring) has no zero divisor.**

A zero divisor is an element that can multiply with another nonzero element to produce zero. For example, in the ring Z6​, 2 and 3 are zero divisors, since 2×3=0. However, in a skew field, if a and b are nonzero elements, then ab=0 implies that a−1ab=a−10, which gives b=0, a contradiction. Therefore, a skew field has no zero divisors.

**11 Theorem:- An Ideal I of a ring R is a sub ring of R.**

Proof:- let be an ideal of a ring R. By definition of ideal I is non-empty subset of R.

let a, b ∈ I = a, b ∈ R = a- b ∈ I.

again, let a, b ∈ I ten b ∈ R.

By definition, a, b∈ I = a\*b ∈ I and b\*a ∈ I.

Hence, I is subring of R.

**12 Theorem :- The intersection of two ideal of a ring is again an ideal.**

Let R be a ring and let I and J be two ideals of R. We want to show that I∩J is also an ideal of R. To do this, we need to check the following properties:

I∩J is a subgroup of R under addition.

For any r∈R and x∈I∩J, we have rx∈I∩J and xr∈I∩J.

For the first property, we need to show that I∩J is nonempty, closed under addition and additive inverses. Since I and J are both ideals, they contain the zero element of R, so 0∈I∩J. Therefore, I∩J is nonempty.

Now, let x,y∈I∩J. Then x,y∈I and x,y∈J. Since I and J are both closed under addition, we have x+y∈I and x+y∈J. Therefore, x+y∈I∩J. Similarly, since I and J are both closed under additive inverses, we have −x∈I and −x∈J. Therefore, −x∈I∩J. Hence, I∩J is closed under addition and additive inverses.

For the second property, let r∈R and x∈I∩J. Then x∈I and x∈J. Since I and J are both closed under multiplication by any element of R, we have rx∈I and rx∈J. Therefore, rx∈I∩J. Similarly, we have xr∈I∩J. Hence, I∩J is closed under multiplication by any element of R.

Therefore, I∩J is an ideal of R. This completes the proof.

**13 Theorem:- The commutative ring with unit element having {0} and R are only ideals in a field.**

Let R be a commutative ring with unit element. We want to show that R is a field if and only if the only ideals of R are R itself and the zero ideal (0).

(⇒) Suppose R is a field. Let I be an ideal of R. Then I is nonempty and contains 0. If I contains a nonzero element a, then a has a multiplicative inverse a^-1 in R, since R is a field. But then aa^-1 = 1 belongs to I, by the definition of an ideal. Therefore, I contains 1, and hence I contains every element of R, by the definition of an ideal. Thus, I = R. Therefore, the only ideals of R are (0) and R.

(⇐) Suppose the only ideals of R are (0) and R. Let a be a nonzero element of R. Then the principal ideal (a) generated by a is an ideal of R. Since a is nonzero, (a) is not (0), and hence (a) must be R, by the assumption. This means that 1 belongs to (a), which means that there exists b in R such that ab = 1, by the definition of a principal ideal. Therefore, a has a multiplicative inverse b in R. Since a was arbitrary, every nonzero element of R has a multiplicative inverse. Thus, R is a field.

**14. Theorem:- A finite integral domain is field.**

Let R be a finite integral domain. Then R is a commutative ring with unity and has no zero divisors1. We want to show that every nonzero element of R has a multiplicative inverse in R.

Let a be a nonzero element of R. Consider the set S={a,a2,a3,…} of all positive powers of a. Since R is finite, S cannot be infinite,and therefore there exist positive integers m>n such that am=an. This implies that am−n=1. Since a=1, we have m−n>1.

Therefore, am−n−1 is the multiplicative inverse of a in R.

Hence, every nonzero element of R has a multiplicative inverse in R, and thus R is a field. This completes the proof.

**15. Theorem:- For any three T= (V, E) with |v|= n, |E|= n-1.**

Proof : Let any leaf of T. This vertex is adjacent to exactly one edge. Remove this vertex and edge contributing 1 each to the number to vertices and edges. Continuing removing leaf or edger pair until we are left with just a single edge. A group with a single edge has one more vertex than edge. Hence the total number of edges is one less than total number of vertices. Hence if |v|= n then |E| = n-1.

**16 Theorem: given integer a and b both of which are non zero, x, y Z such that gcd(a, b) = ax + by.**

Proof: consider the non empty set of all positive linear combination of a and b such that S = { a

+ b > 0 where , + b : a Z}

Let us choose x and y such that ax + by will give a least positive integer d in the set s. thus ax + by = d.

Now, we can write gcd(a, b) = d for this we have to show that d|a and d|b.

If possible, suppose that d a. Thus by division algorithm q, r Z such that a = dq + r, 0≤ r< d.

Thus r = a – dq = a –q(ax + by) =a(1-qx) +b(-qy)

Hence r S, s0 d cannot be a least positive integer since r < d. which is contradiction so we must have d|a.

By same process, we can show d|b.

Now, if c is an arbitrary common positive divisor of a and b. Then we can write, c|a and c|b. It follows that

c|ax + by, i.e. c|d. where d = ax +by and we know that c ≤ d. so that d is greater than every positive common

divisor of a and b. So, gcd(a, b) = d= ax + by .

**17 Theorem: if gcd(a, b) = d then gcd( , ) = 1.**

Proof: since gcd(a, b) = d it can expressed as the linear combination of a and b such that d = ax + by for any

x, y Z. Dividing both sides by d, we get 1 = x + y

Since and are integer with gcd(a, b) = d then for any a, b Z and a 0, b 0.

If 1 = x + y, then we can write gcd(, ) = 1. gcd(,) = 1

**18 Theorem: Let a, b be integers not both zero for a positive integer d, d = gcd(a, b) iff (i) d|a and d|b (ii)**

**whenever c|a and c|b then c|d.**

Proof: since gcd(a, b) = d then d|a and d|b

If a and b are integers, a 0, b 0 then x, y Z such that gcd(a, b) = ax + by. Thus, if c|a and c|b then

c|ax + by c|d

Conversely, let d|a and d|b. Let c|a and c|b then c|d implies that c ≤ d because d > 0. Hence gcd(a, b) = d

**19 Proof: we know that the equation of Euclidean algorithm multiplying by k, then we get,**

ak = + k , 0 ≤ k < bk …… (1)

bk = k + k , 0 ≤ k< k …… (2)

………………………………

…………………………………

k = k + k, 0 ≤ k< k …… (n-1) and

k = k+ 0 ……….…… (n)

By Euclidean algorithm, gcd(ak, bk) = k = k = k gcd(a, b).

Examples: find the gcd(427, 616) and express it in terms of 42

**20 Theorem: Let n Z be an integer and n 0 then a b(modn) iff a (modn)where r is remainder when n dividesb**.

Proof: Let n and a b(modn) then we have to show that a r(modn) We have a b(modn) n|a- b a – b = n a = b + n, Z ….. (i) By division algorithm, for b and n there exists q, r Z such that b = nq + r….. (ii) From (i) and (ii), a = nq + n + r a – r = (q + )n n|a- r a (modn) conversely, suppose a (modn), where r is the remainder upon division by n then we have to show that a (modn). Since r is remainder upon division b by n then b = qn + r with quotient q. i.e. r = b – qn and a (modn) a (modn) a - b 0(modn) n|a- b a b(modn)