2 - YEAR - I SEMESTAR.

ABSTRACT ALGEBRA - 7BMA3C1

UNIT - I

Groups - Definition and examples - Elementery properties of a group - Equivalent Definition of a group - permutation Groups.

UNIT - II

Subgroups - cyclic groups - order of an Element - cosets and lagranges Theorems.

UNIT - III

Normal subgroups and Quotient groups - Isomorphism - Homorphism.

UNIT - IV

Rings : Definition and examples - Elementary properties of rings - Isomorphism - Types of rings - characteristic ring - subring - Ideals - Quotient rings.

UNIT - V

Maximal and prime Ideals - Homomorphis -n of rings - Field of Quotient of an Integrals domain - unique factorzation domain - Euclidean domain.

Text book:

1. S. Arumugam and A. Thangapandian Issac, modern Algebra Sci Tech publications pvt. Ltd chennai 2003.

UNIT - I	chapter 3 Section 3.1 to 3.4
UNIT - II	chapter 3 Section 3.5 to 3.8
UNIT - III	chapter 3 Section 3.9 to 3.11
UNIT - IV	chapter 4 Section 4.1 to 4.8
UNIT - V	chapter 4 Section 4.9 to 4.11 4.13 & 4.16

(vii) R^* -> The set of all non zero Real number.

(viii) C^* -> The set of all non-zero complex number.

(ix) Q^+ -> The set all positive rational nu

Then $Q^+ = \{x / x \in Q$ and $x > 0\}$

(i) N -> The set of all Natural number

ie) $N = \{1, 2, 3, \ldots\}$

(ii) Z -> The set of all integer number

ie) $Z = \{\pm 1, \pm 2, \ldots\}$

(iii) R -> The set of all Real number

ie) $R = Q \cup Q'$ Q is rational, Q' is irrational.

(iv) W -> The set of all Whole number

$W = \{0, 1, 2, \ldots\}$

(v) C -> The set of all complex $c = a + ib$ a, b is real

(vi) Q^* -> the set of all non-zero rational

2020.12.11 14:41

UNIT- I

Definition : GROUP

A non-empty set G together with binary operation $*: G \times G \to G$ is called a group if the following conditions are satisfy.

(i) closure law:

Let $\forall\ a \in G$

$\Rightarrow *$ is closure

(ii) Associative:

Let $a, b, c \in G$

$*$ is associative

$\Rightarrow a*(b*c) = (a*b)*c \ \forall\ a, b, c \in G.$

(iii) Identity:

There exists an $e \in G$ such that $a*e = e*a = a \ \forall\ a \in G.$

e is called the Identity element of G.

(iv) Inverse:

For any element a in G. There exists and element $a^{-1} \in G$ such that $a*a^{-1} = a^{-1}*a = e$. For all $a \in G$. a^{-1} is called the inverse of a

Example:

(i) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are prove under usual addition

(ii) The set of all 2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where $a, b, c, d \in R$ is a group under matrices addition. $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ is a Identity element. and $\begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$ is the Inverse of $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

(iii) The set of all 2×2 non-singular matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where $a, b, c, d \in R$, is a group under matrices multiple group. we know that matrices multiplication with associative. $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is the Identity element. The Inverse of $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is $\frac{1}{|A|} \times adj(A) \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ where

$$|A| = \begin{pmatrix} a & b \\ -b & c \end{pmatrix} \neq 0$$

(iv) Let $U_n = \{z / z \in C \text{ and } |z| = 1\}$ if U_n is a group under usual multiplication.

Proof:

Let $z_1, z_2 \in U_n$

Then $|z_1| = |z_2| = 1$ and hence $z_1 . z_2 \in U_n$

we know that usual multiplication of complex number is associative.

Also $1 = 1 + i0 \in U_n$ and is the identify element.

Now let $z \in U_n$. Then $|z| = 1$

Hence $|1/z| = \frac{1}{|z|} = 1$.

$\therefore \frac{1}{z} \in U_n$ and is the inverse of z

Hence U_n is a group.

v) The set of all n^{th} roots of unity with usual multiplication.

Proof:

Let $w = \cos\left(\frac{2\pi}{n}\right) + i \sin\left(\frac{2\pi}{n}\right)$

The n^{th} roots of unity are given by $1, w, w^2, \ldots, w^{n-1}$.

Let $U_n = \{1, w^2, w^2, \ldots w^{n-1}\}$

we know that $w^n = 1$ $w^{n+1} = w$.

Let $w^r, w^s \in U_n$ Let $r + s = qn + t$.

where $0 \leq k \leq n$.

$\therefore \omega^r \omega^k = \omega^{r+k} = \omega^{qn+k}$

$= (\omega^n)^q \cdot \omega^k$

$= 1 \cdot \omega^k \quad (\because \omega^n = 1)$

$= \omega^k$

$= \omega^k \in U_n$.

We know that usual multiplication of complex number is associative.

$1 \in U_n$ is the identity element.

Inverse of ω^r is ω^{n-r}

Hence U_n is a group.

vi) Let $U_n = \{a + b\sqrt{2} / a, b \in Z\}$ Then U_n is a group under usual addition.

Proof

Let $a+b\sqrt{2}$ and $c+d\sqrt{2} \in U_n$

Then $(a+b\sqrt{2}) + (c+d\sqrt{2})$

$= (a+c) + (b+d)\sqrt{2} \in U_n$

We know that usual addition is associative

$0 = 0 + 0\sqrt{2} \in U_n$ is the identity element.

$-a-b\sqrt{2}$ is the Inverse of $a+b\sqrt{2}$.

Hence U is group.

(vii) Let U be the set of all real number except -1 define $*$ on U by $a*b = a+b+ab$.

Then $(U, *)$ is a group.

Proof:

Let $a, b \in U$. Then $a \neq -1$ and $b \neq -1$.

we claim that $a*b = -1$. Suppose $a*b = -1$.

Then $a+b+ab = -1$ so that $a+b+ab+1 = 0$

i.e) $(a+1)(b+1) = 0$. so that either $a = -1$.

(or) $b = -1$ which is a contradiction.

Hence $a*b \neq -1$ and thus $*$ is a binary operation on U.

$*$ is associative for $a*(b*c)$

$= a*(b+c+bc)$

$= a+(b+c+bc)+a(b+c+bc)$

$= a+b+c+bc+ab+ac+abc$

Also $(a*b)*c = (a+b+ab)*c$

$= a+b+ab+ac+bc+abc$.

Hence $a*(b*c) = (a*b)*c$ e is the identity

2020.12.11 14:40

For $a * 0 = a + 0 + 0a = a$.

Now let a' be such that $a * a' = 0$

Hence $a + a' + aa' = 0$. so that

$$a' = -a/(1+a)$$

Since $a \neq -1$ we have $a' \in R - \{-1\}$

Also $a' * a = \frac{-a}{1+a} * a$.

$$= \frac{-a}{1+a} + a + -\frac{a^2}{1+a} = 0$$

Hence a' is the inverse of a.

Thus G is a group.

Problem:

In R^* define $a * b = (1/2)ab$ then $(R^*, *)$ is a group.

Proof:

Obviously $*$ is a binary operation in R^*

Let $a, b, c \in R^*$

Then $(a * b) * c = [(1/2)ab] * c = (1/4)abc$.

$= a * (b * c)$.

Hence $*$ is associative.

2020.12.11 14:40

Let $e \in R^*$ be such that $a * e = a$.

$\therefore \left(\frac{1}{2}\right) ae = a$ and hence $e = 2$.

$\therefore 2 * a = a * 2 = a$.

Hence 2 is the identity.

Let $a \in R^*$ let $b \in R^*$ such that $a * b = 2$.

Then $\left(\frac{1}{2}\right) ab = 2$

i.e $b = \frac{4}{a}$

$\therefore a * (4/a) = \frac{1}{2}(4/a)\, a = 2$.

i.e $(4/a)$ is the inverse of a.

Thus $(R^*, *)$ is a group.

Problem: 2

Let $f_a : R \to R$ be the function defined by $f_a(x) = x + a$. Then $G = \{f_a \mid a \in R\}$ is a group under composition of functions.

Proof:

Let $f_a, f_b \in G$.

Then $(f_a \cdot f_b)(x) = f_a(f_b(x))$

$= f_a(x + b) = x + b + a$

$= f_{b+a}(x)$

Hence $f_a \cdot f_b = f_{b+a} \in G$

2020.12.11 14:40

We know that composition of mapping is associative.

Also $f_a \cdot f_0 = f_{a+0} = f_a = f_0 \cdot f_a$

Hence f_0 is the identity.

Also $f_a \cdot f_{-a} = f_0 = f_{-a} \cdot f_a$ Hence f_{-a} is the inverse of f_a.

Hence U is a group.

Definition:

Let $Z_n = \{0, 1, 2, \ldots, n-1\}$

Let $a, b \in Z_n$. Let $a+b = qn+r$ where $0 \leq r < n$.

We define $a \oplus b = s$

The binary operations $\oplus$ and $\odot$ are called addition modulo n and multiplication modulo n respectively.

Problem: 1

$(Z_n, \oplus)$ is a group.

Proof:

Clearly $\oplus$ is a binary operation in Z_n.

Let $a, b, c \in Z_n$.

Let $a+b = q_1 n + r_1$ where $0 \le r_1 < n$ ——> (1)

$b+c = q_2 n + r_2$ where $0 \le r_2 < n$ ——> (2)

$r_1 + c = q_3 n + r_3$ where $0 \le r_3 < n$ ——> (3)

$a+b+c = (q_1 + q_3) n + r_3$ (using 1 and 3)

$a + q_2 n + r_2 = (q_1 + q_3) n + r_3$ (by 2)

$a + r_2 = q_4 n + r_3$.

where $q_4 = q_1 + q_3 - q_2$ ——> (4)

Now $(a \oplus b) \oplus c = r_1 \oplus c = r_3$ (by 2)

Also $a \oplus (b \oplus c) = a \oplus r_2 = r_3$ (by 4)

Hence $\oplus$ is associative.

clearly the identity element is 0 and the inverse of $a \in Z_n$ is a group.

Problem:2

Let n be a prime. Then $Z_n - \{0\}$ is a group under multiplication modulo n.

Proof:

Let $a, b \in Z_n - \{0\}$ Then $a \neq 0$ and $b \neq 0$

Now by definition $a \odot b \neq 0$ suppose $a \odot b \in Z_n$.

we claim that $a \odot b \neq 0$ suppose $a \odot b = 0$.

Then n / ab. since n is prime n/a or n/b

$a = 0$ (or) $b = 0$ which is a contradi

Hence, $a \odot b \in Z_n - \{0\}$

Now. Let $a, b, c \in Z_n - \{0\}$.

Let

$ab = q_1 n + r_1$ where $0 \leq r_1 < n$ —→(1)

$bc = q_2 n + r_2$ where $0 \leq r_2 < n$ —→(2).

$r_1 c = q_3 n + r_3$ where $0 \leq r_3 < n$ —→(3).

$abc = q_1 nc + r_1 c$ (by (1)

$a(q_2 n + r_2) = q_1 cn + q_3 n + r_3$.

(using 2 & (3))

$ar_2 = q_4 n + r_3$.

where $q_4 = q_1 c + q_3 - aq_2$.

Now, $(a \odot b) \odot c = r_1 \odot c = r_3$ (by 3)

Also $(a \odot b) \odot c = r_1 \odot c = r_3$ (by 4)

$(a \odot b) \odot c = a \odot (b \odot c)$

Hence $\odot$ is associative.

$1 \in Z_n - \{0\}$ is the identity element.

Let $a \in Z_n - \{0\}$

Since n is prime $(a, n) = 1$.

Hence the linear congruence

$ax \equiv 1 \pmod{n}$ has a unique.

solution say $b \in Z_n - \{0\}$.

2020.12.11 14:40

clearly $a \otimes b = b \otimes a = 1$

Thus b is an inverse of a.

Hence $Z_n - \{0\}$ is a group.

Problem: 3

The set of all positive integers less than and prime to it a group under multiplication modulo n.

Proof:

Let $U_n = \{ m / m < n \text{ and } (m, n) = 1 \}$

Let $p, q \in U_n$ obviously $pq \neq n$ and $(pq, n) =$

Now Let $pq = sn + r$, $0 < r < n$

Hence $p \otimes q = r$ (by definition)

we claim that $(r, n) = 1$

Suppose $(r, n) = a > 1$ then a/r and a/n.

Hence $a / (r + sn)$ i.e. a / pq also a/n.

Hence $(pq, n) \neq 1$ which is a contradictio

Hence $r \in U_n$. Hence U_n is a closed under $\oplus$ we know that multiplication Modulo n is associ -ve. $1 \in U_n$ is the identity element. Let $a \in U_n$. Then $(a, n) = 1$ Hence the linear congruence $ax \equiv 1 \pmod{n}$ has a unique solution for x say b

$ab \equiv 1 \pmod{n}$ Hence $a \in b$ $= 1$ Now.

we have to prove that $b \in U_n$ suppose $(b, n) = c$.

since $ab \equiv 1 \pmod{n}$ $ab = qn + 1$.

Now c/b and $c/n \Rightarrow (c/ab - qn) \Rightarrow c/1$.

$c = 1$ Thus $(b, n) = 1$ Hence $b \in U_n$ and is the inverse of a.

Thus U_n is a group.

Problem: 4

Let U_n denote the set of all matrices of the form $\begin{pmatrix} x & x \\ x & x \end{pmatrix}$ where $x \in R^*$. Then U_n is a group under matrix multiplication.

Let $A, B \in G$, Let $A = \begin{pmatrix} x & x \\ x & x \end{pmatrix}$ and $B = \begin{pmatrix} y & y \\ y & y \end{pmatrix}$

Then $AB = \begin{pmatrix} 2xy & 2xy \\ 2xy & 2xy \end{pmatrix} \in G$

we know that matrix Multiplication is associative.

Let $E = \begin{pmatrix} e & e \\ e & e \end{pmatrix}$ be such that

$AE = A$

$$\begin{pmatrix} x & x \\ x & x \end{pmatrix}\begin{pmatrix} e & e \\ e & e \end{pmatrix} = \begin{pmatrix} x & x \\ x & x \end{pmatrix}$$

$$\begin{pmatrix} 2xe & 2xe \\ 2xe & 2xe \end{pmatrix} = \begin{pmatrix} x & x \\ x & x \end{pmatrix}$$

$2xe = x$ Hence $= 1/2$

Hence $E = \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}$ is the identity element of G.

Let $\begin{pmatrix} y & y \\ y & y \end{pmatrix}$ be the inverse of $\begin{pmatrix} x & x \\ x & x \end{pmatrix}$

Then $\begin{pmatrix} x & x \\ x & x \end{pmatrix}\begin{pmatrix} y & y \\ y & y \end{pmatrix} = \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}$

$$\begin{pmatrix} 2xy & 2xy \\ 2xy & 2xy \end{pmatrix} = \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}$$

$2xy = 1/2$ Hence $y = 1/4$.

Problem: 5

Let $G = \{(a, b) / a \in R, b \in R\}$ then G is a group under the operation $*$ defined by $(a, b) * (c, d) = (ac, bc + d)$

clearly * is a binary operation defined on G.

Now Let $x = (a,b)$ $y = (c,d)$ $z = (e,f)$ be three elements in G.

Then $x * (y * z) = (a,b) * (ce, de, f)$

$= (ace, bce + de, f)$

Also $(x * y) * z = (ac, bc + d) * (e,f)$

$= (ace, bce + de + f)$

$x * (y * z) = (x * y) * z$ So that * is associative. Now to Find the identity element in G. Suppose $(a,b) * (c,d) = (a,b)$

Then $(ac, bc + d) = (a,b)$

$ac = a$ and $bc + d = b$

Hence $c = 1$ and $d = 0$.

Thus $(a*b)(1*0) = (1,0) * (a:b)$

$= (ab)$

$(1,0) \in G$ is the identity element

Now Suppose $(a,b) * (a'b') = (1,0)$

$(aa', ba' + b') = (1,0)$

$a' = 1/a$ and $b' = -b/a$

Thus $(a,b) * (1/a - b/a)$

$= (1/a, -b/a)$ $\because * (a,b) = (1,0)$

Hence $(1/a, -b/a)$ is the inverse of (a,b)

Hence G is a group.

Problem: 6

In N we define $a * b = a$ Then $(N, *)$ is not a group.

Clearly $*$ is an associative binary operation on N. However there is no element $e \in N$ such that $e * a = a$ For all $a \in N$.

Hence there is no identity element in $(N, *)$

Hence $(N, *)$ is not a group.

In the group $(Z, +)$ the binary operation is commutative where as in the group of 3×3 Non - Singular Matrices the matrix

multiplication is not Commutative.

Definition: ABELIAN GROUP (i.e.) Commutative Law

A Group is said to be abelian if $ab = ba$ For all $a, b \in G$. A group which is not abelian is called a non-abelian group.

1) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ under usual addition are abelian group.

2) Let $B(R)$ denote the Set of all bijections From R to R. Then $B(R)$ is a group under the Composition of Function of Functions. This group is non-abelian For Consider

$f : R \to R$ given by $f(x) = x + 3$

and $g : R \to R$ given by $g(x) = 2x$.

Clearly f and g are bijections.

Now $(f \cdot g)(x) = g[f(x)] = f(2x) = 2x + 3$

and $(g \cdot f)(x) = g[f(x)] = g(x + 3) = 2x + 6$

Hence $f \cdot g \neq g \cdot f$

2020.12.11 14:39

Hence $B(R)$ is non-abelian.

3) $(Z_n, \oplus)$ is an abelian group.

4) Consider the group given in examples 2^b of 2.1. Here $(2,3) * (4,5) = (8,7)$ and $(4,5) * (2,3) = (8,13)$

Thus $(2,3) * (4,5) \neq (4,5) * (2,3)$

So that this group is non-abelian

Elementary properties of a Group:

Theorem 3.1 :-

Let G be a group then

i) Identity element of G is unique

ii) For any $a \in G$ the inverse of a. unique.

(i) Let e and e' be two identity elements of G. Then $ee' = e'$ [since e is an identity]

Hence $e = e'$

(ii) Let a' and a'' be two inverse

of a.

Hence $aa' = a'a = e$ and $aa'' = a''a = e$

$a' = a'e = a'(aa'') = (a'a)a'' = ea'' = a''$

Note :

we denote the inverse of a by a^{-1}

Theorem : 3.2

In a group the left and right Cancellation Laws hold ie) $ab = ac \Rightarrow b = c$ and $ba = ca \Rightarrow b = c$.

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

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

$\Rightarrow eb = ec$

$\Rightarrow b = c$

Similarly we can prove that $ba = ca \Rightarrow b = c$

Theorem : 3.3

Let G be a group and $a, b \in G$ Then the equations $ax = b$ and $ya = b$ have unique Solution For x and y in G.

Consider $a^{-1}b \in G$

Then $a(a^{-1}b) = (aa^{-1})b = eb = b$

Hence $a^{-1}b$ is a Solution of $ax = b$

Now to prove the uniqueness, Let x_1 and x_2 be two Solution of $ax = b$.

Then $ax_1 = b$ and $ax_2 = b$.

$\therefore x = a^{-1}b$ is the unique Solution for $ax = b$

Similarly we can prove that $y = ba^{-1}$ is the unique Solution of the equation

$$y * a = b$$

theorem: 3.4

Let G be a group. Let $a, b \in G$. Then $(ab)^{-1} = b^{-1}a^{-1}$ and $(a^{-1})^{-1} = a$

Let G be a group

Let $a, b \in G$

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

$\Rightarrow b^{-1}a^{-1}$

Multiplying on ab we get.

$\Rightarrow ab\,(b^{-1}a^{-1})$

$\Rightarrow a(bb^{-1})a^{-1}$

$\Rightarrow aea^{-1}$

$= e$

Similarly

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

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

(ii)

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

Let $a \in G \Rightarrow (a^{-1})^{-1} = a$

Definition : Integer :

Let G be a group and $a \in G$

For any positive integer n, we define obtain

$a^n = a.a.\ldots a.$ (a written n times)

clearly $(a^n)^{-1} = (aa\ldots a)^{-1}$

$= (a^{-1}a^{-1}\ldots a^{-1})$

$= (a^{-1})^n$

we now define $a^{-n} = (a^{-1})^n = (a^n)^{-1}$

Finally we define $a^0 = e$

Thus a^n is defined for all integer n.

2020.12.11 14:38

Theorem: 3.5

If (i) $a^m a^n = a^{m+n}$ $m, n \in Z$

(ii) $(a^m)^n = a^{mn}$ $m, n \in Z$.

when $n=0$ there result follows directly from the definition

Now Let $n>0$. we prove the result by induction on n.

when $n=0$, $a^{m+1} = a^m a^1$ (by definition)

when $m=-1$, $e^{m+1} = a^0 = e$

$a^m a^1 = a^{-1} a = e$

Hence $a^{m+1} = a^m a^1$

when $m \leq -2$. Let $m=-p$ where $p \geq 2$.

$\therefore (a^m)^a = (a^{-p}) a = (a^{-1})^p a$

$= (a^{-1})^{p-1} a^{-1} a$

$= (a^{-1})^{p-1} = a^{-p+1} = a^{m+1}$

Hence $a^{m+1} = a^m a^1$ For all $m \in Z$

Hence the result is true For $n=1$

Suppose Now that there is valied

For $n = k+1$ Then

$$a^m a^k = a^{m+k}$$

$$\therefore a^m a^{k+1} = a^m (a^k a)$$

$$= (a^m a^k) a$$

$$= (a^{m+k}) a$$

$$= a^{m+k+1}$$

Thus the Follows that theorem is valued For $n = k+1$.

Hence by induction the theorem hold For all positive integer n.

Finally if $n < 0$ we can prove the result by induction on $-n$.

Proof :(ii)

$$(a^m)^n = a^{mn} \qquad m, n \in z$$

$$(a^m)^n = (a^{-nm}) \quad \text{(by hypothesis)}$$

$$= (a^{mn})$$

Problem: 1

Show that in a group G, $x^2 = x$ if and only if $x = e$

Proof: Let G be a group.

Direct Part:

Assume that: $x^2 = x$

Prove that: $x = e$

Let $x^2 = x$

$e^2 = e.e$

$x = e$

Converse part:

Assume that: $x = e$

Prove that: $x^2 = x$

$\Rightarrow x = e$

Pre and Post Multiplying on x we get

$x.x = e.x$ (identity Law)

$x^2 = ex$

$x^2 = x$.

Definition: Idempotent Law

An element $a \in G$ is called idempotent if $a^2 = a$. Thus we have shows that in a group G. The identity element is the only Idempotent element.

Problem: 2 In an abelian group $(ab)^2 = a^2 b^2$

$$(ab)^2 = (ab)(ab)$$
$$= a(ba)b$$
$$= (aa)(bb)$$
$$= a^2 b^2$$

Note :

In General any positive integer n. $(ab)^n = a^n b^n$ (Prove by direct induction)

Problem: 3 Let G be a group. Such that $a^2 = a$ For all $a \in G$. Then G is a abelian.

$$a^2 = e$$
$$a = a^{-1}$$

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

$$\therefore ab = ba$$

Hence G is abelian.

Problem: 4 Let G be a group In which $(ab)^M = a^M b^M$ For three consecutive integers and For all $a, b \in G$

G is abelian.

Let $a, b \in G$

Let $(ab)^m = a^m b^m$,

$(ab)^{m+1} = a^{m+1} b^{m+1}$

and $(ab)^{m+2} = a^{m+2} b^{m+2}$

$(ab)^{m+1} = a^{m+1} b^{m+1}$

$\Rightarrow (ab)^m (ab) = (a^m a)(b^m b)$

$\Rightarrow b^m a = a b^m$ (by Cancellation $\rightarrow$ (1))

Similarly

$(ab)^{m+2} = a^{m+2} b^{m+2}$

$\Rightarrow b^{m+a} = a b^{m+1}$

$\Rightarrow b^m b^a = a b^m b$

$\Rightarrow ba = ab$

$\therefore G$ is a abelian.

Problem: 5

Let $(H, \cdot)$ and $(K, *)$ be groups

we define a binary operation $\square$ on $H \times K$ by $(h_1, k_1) \square (h_2, k_2) = (h_1 h_2, k_1 * k_2)$

Then $H \times K$ is a group.

Direct product:

$H \times K$ is called the direct product of H and K.

Problem:6

Let $H \times K$ with is the direct product of H and K.

Soln:

First we shall prove that $\square$ is associative.

Let $(h_1, k_1), (h_2, k_2), (h_3, k_3) \in H \times K$.

$$\left[(h_1, k_1) \square (h_2, k_2)\right] \square (h_3, k_3)$$

$$= (h_1 h_2, k_1 * k_2) \square (h_3, k_3)$$

$$= (h_1, h_2) h_3, (k_1 * k_2) * k_3$$

$$= (h_1, k_1) \square (h_2 h_3, k_2 * k_3)$$

$$= (h_1, k_1) \square \left[(h_2, k_2) \square (h_3, k_3)\right]$$

Let e, e_1 we the identidy of the groups H and K respectively. clearly e, e_1 is the identity element $H \times K$. (also $H^{-1} \times K^{-1}$ is the inverse $H.K$

Hence $H.K$ is a group.

Equivalent Definition of a Group:-

Left Identity

Right Identity.

Left Identity:-

Definition:- Let $*$ be a binary operation defined on G and element $e \in G$ is called a left identity.

$e * a = a$ for all $a \in G$.

Right Identity:-

Definition:- e is called right identity if $a * e = a$ for all $a \in G$.

Ex:-

In $\mathbb{C}$ we define $z_1 \circ z_2 = |z_1| \cdot z_2$

here all are the element z such that

1.8.21.

Right Identity Ex:

1. In $\mathbb{R}$ we define $a*b = ab^{-1}$

here 1 and -1. are Right Identity.

2. In N we define $a*b = a$.

here every element is a right Identity.

Left Inverse and Right Inverse:

Definition:

Let $*$ be a binary operation defined on G Let $e \in G$. be the identity element. Let $a \in G$ An element $a' \in G$ is called a Left Inverse of a if $a' * a = e$.

a' is called Right Inverse of a if $a * a' = e$.

Note:

The Identity element e of group G is a both Left Identity

$a \in G$ is both left Inverse Identity and right Identity. Inverse.

Theorem: 3.6

Let G be a non-empty set with an associative binary operation defined on it such that there exists a left identity e in G. and each element $a \in G$ has a left inverse a' with respect to e then G is a group

Proof:

a' is a left inverse of a

so that $a'a = e$.

Let a'' be the left inverse of a'.

so that $a''a' = e$.

Then $aa' = e(aa')$ (since e is left identity)

$= (a''a')(aa')$

$= a''(a'a)a'$ (associativity)

$= a''(ea')$ (since e is identity)

$= a''a'$

$= e.$

2020.12.11 14:37

Hence a' is also a Right Inverse of a.

also $a = ea = (aa')a = a(a'a)ae$

Hence e is also a Right identity.

Thus $ea = a = ae$ and $a'a = aa' = e$ and for all $a \in G$.

Hence G is a Group.

Theorem: 3.7

Let G a non-empty set with an associative binary operation defined on it such that there exists a Right identity e in G and each element $a \in G$ has a write Inverse of a'. with respect to Then G is a Group.

Proof:

a' is a Right inverse of a.

So that $aa' = e$.

Let a'' be the right inverse of a'.

So that $a'a'' = e$.

Then $a'a = (aa')e$. (since Right

$= (a')^{-1}$

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

$= a''(a'(aa''))$ (associativity)

$= a''(ea'')$ (since e is identity)

$= a'a''$

$= e.$

Hence a' is also a Left inverse of a. also $a = ae = (aa')a = a(a'a)a$.

Hence e is also a Right identity.

Thus $ae = a = ea$ and $aa' = a'a = e$ and for all $a \in G$.

Hence G is a group.

Note:-

If G is a non-empty set with and associative binary operation $*$ defined on it such that there exists a Left identity and a Right inverse

Then $(G, *)$ need not be a group

2020.12.11 14:37

Ex:-

Consider $(\mathbb{R}^*, *)$ were $a*b = |a|b$

clearly $*$ is a binary operation on $\mathbb{R}^*$ Now

$a*(b*c) = (a*b)*c = |a||b|c$ and

hence $*$ is associative $(-1)*a = |-1|a = a$.

hence -1 is a left identity. Now when

$a < 0$.

$$a*(1/a) = |a|(1/a) = (-a)(1/a) = -1.$$

and when $a > 0$ $a*(-1/a) = |a|\left(\frac{-1}{a}\right) = (a)(-1/a)$

hence if $a<0$, $(1/a)$ is the right inverse of a.
and if $a>0$, $(-1/a)$ is the right inverse of a.
however $(\mathbb{R}^*, *)$ is not a group.

Since the equation $y*a = a$ has
two solutions nearly 1 and -1.

Theorem: 3.8

Let G be a non-empty set
with an associative binary operation defined
on it such that $\exists$ an existence $ax = b$ & $ya = b$ unique
soln for x and y in G Then G is a group

oln:

Let $a \in G$.

Then there exists a unique $e \in G$ such that $ea = a$.

Now, Let b be any other element in G. Then there exists a unique x in G such that $ax = b$. Now, $eb = e(ax) = (ea)x = ax = b$.

$\therefore eb = b$ for all $b \in G$ so that e is left identity.

Let $a \in G$.

Then $ya = a$ has a unique solution a'.

$\therefore a'a = e$ so that a' is the left inverse of a. Hence by theorem 3.6

G is a group.

Theorem: 3.9

Let G be a finite set with an associati binary operation defined on G In which both cancellation law hold could than G is a group.

Let G be a binary operation

which an associative binary

2020.12.11 14:36

operation $*$ defined on G.

Let $G = \{a_1, a_2, \ldots a_n\}$

Now let $a, b \in G$.

Consider the element $aa_1, aa_2, \ldots aa_n$

all this element are distinct For if

$aa_r = aa_s$.

Then $a_r = a_s$. (by cancellation Law)

Hence $aa_1, aa_2, \ldots, aa_n$ are just the elements $a_1, a_2, \ldots a_n$ of G. in same order and hence $aa_i = b$ for some i.

Thus the equation $ax = b$. has a unique solution for x in G.

Similarly taking the elements $a_2 a$ $a_1 a, a_2 a, \ldots a_n a$.

we can prove that the equation $ya = b$. has a unique solution for y in G.

hence by theorem 3.8 G is a group.

Permutation groups:-

Definition: Permutation

Let A be a finite set. A by section from A to it self is called a permutation of A.

Ex:-

$A = \{1, 2, 3, 4\}$ $f: A \to A$

Given

$f(1) = 2$

$f(2) = 1$

$f(3) = 4$

$f(4) = 3$

is a permutation of A we shall write this permutation $P = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$

symmetric groups:-

Definition :-

Let A be a finite set containing n elements. The set of all permutation of A is clearly a group under the composition of functions. This group is called the symmetric group of degree n and is denoted by S_n.

Ex:-

Let $A = \{1, 2, 3\}$ Then S_3 consists of $e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ $P_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

$P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ $P_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

$P_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ $P_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

	e	P_1	P_2	P_3	P_4	P_5
e	e	P_1	P_2	P_3	P_4	P_5
P_1	P_1	P_2	e	P_4	P_5	P_3
P_2	P_2	e	P_1	P_5	P_3	P_4
P_3	P_3	P_5	P_4	e	P_2	P_1
P_4	P_4	P_3	P_5	P_1	e	P_2
P_5	P_5	P_4	P_3	P_2	P_1	e

1) $P_1 e = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix} = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = P_1$

(4) ⇒

2) $P_1 P_1 = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = P_2.$

3) $P_1 P_2 = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix} = e.$

4) $P_1 P_3 = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} = P_4.$

5) $P_1 P_4 = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = P_5.$

6) $P_1 P_5 = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} = P_3.$

7) $P_2 e = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix} = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = P_2.$

8) $P_2 P_1 = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix} = e.$

9) $P_2 P_2 = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = P_1.$

10) $P_2 P_3 = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = P_5.$

11) $P_2 P_4 = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} = P_3.$

12) $P_2 P_5 = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} = P_4.$

19) $P_3 e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = P_3.$

20) $P_3 P_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = P_5.$

21) $P_3 P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = P_4.$

22) $P_3 P_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = e.$

23) $P_3 P_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = P_2.$

24) $P_3 P_5 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = P_1.$

25) $P_4 e = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = P_4.$

26) $P_4 P_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = P_3.$

27) $P_4 P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = P_5.$

28) $P_4 P_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = P_1.$

29) $P_4 P_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = e.$

2020.12.11 14:35

30) $P_4 P_5 = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = P_2.$

31) $P_5 e = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix} = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = P_5.$

32) $P_5 P_1 = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} = P_4.$

33) $P_5 P_2 = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} = P_3.$

34) $P_5 P_3 = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = P_2.$

35) $P_5 P_4 = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = P_1$

36) $P_5 P_5 = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix} = e.$

Thus S_3 is a group of containing $3! = 6$.

Definition: order:

Let G be a finite group. Then the number of elements is called the order of G. and is denoted by $|G|$ or $O(G)$.

Definition: cycle of

Let p be a permutation on $A = \{1, 2, \ldots n\}$. p is called a cycle of length r if there

exist distinct simples $a_1, a_2, \ldots a_r$ such that $p(a_1) = a_2$, $p(a_2) = a_3 \ldots\ldots p(a_{r-1}) = a_r$, and $p(a_r) = a_1$ and $p(b) = b$ For all $b \in A - \{a_1, a_2, \ldots a_r\}$

Ex:

Let $A = \{1, 2, 3, 4, 5\}$ consider cycle of length 4. given by $p = (2\ 4\ 5\ 1)$

Then $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{pmatrix}$

Soln:

Let $p = (2\ 4\ 5\ 1)$

$(2\ 4\ 5\ 1) = (4\ 5\ 1\ 2) = (5\ 1\ 2\ 4) = (1\ 2\ 4\ 5)$.

Definition: disjoint:

Two cycles are set to be disjoint if the have no simples symbols in common

Ex:

$(2\ 1\ 5)$ and $(3, 4)$ are disjoint cycles.

Theorem: 3.10

[Any permutation can be capressed as a product of disjoint cycle] Proof: Let p be a given permutation of the set $S = \{1, 2, \ldots n\}$.

Proof:

Let p be a given permutation of the set $S = \{1, 2, \ldots n\}$.

Let S_n start with any symbol $a_1 \in S$.

Let $P(a_1) = a_2$, $P(a_2) = a_3$, $P(a_3) = a_4 \ldots\ldots$

since S is finite. This symbol cannot all be distinct. and hence there exists a least positive integer r such that $1 \leq r \leq n$ and $P(a_r) = a_1$.

Let $c = a_1, a_2, \ldots a_r$. if $r = n$

Then $p = c$ so that p is cycle.

If $r < n$ Let b_1 be a symbol in S. such that we can construct the cycle $d = b_1, b_2, \ldots\ldots b_s$.

As before clearly the cycle c and d are disjoint.

If $r + s = n$. Then $p = cd$

If $r + s < n$ be repate the above proceed to obtain more cycles and Fill all the symbols appear in one of the cycles.

Thus we get a decomposition of p if to disjoint cycles.

Definition: Transposition

A cycle of length Two is called a Transposition. Thus a transposition (a_1, a_2) inter change the symbols a_1 and a_2. and Uses leaves all other element fixed.

Theorem: 3.11

Any permutation can be expressed as a Product of Transposition.

Proof:

Since any permutation product of disjoint it is enough if we prove that each cycle is a product of transposition.

Hence Let $c = (a_1, a_2 \cdots a_r)$ be a cycle

clearly $(a_1, a_2 \cdots a_r) = (a_1, a_2)(a_1, a_3) \cdots (a_1, a_r)$.

Ex:

1) Let $P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix} = (1\ 2\ 4\ 5)$

Soln:

$P = (1\ 2\ 4\ 5)$

$= (12)(14)(15)$

$p^1 = (2451) = (24)(25)(21)$

$\therefore p = p^1$

$(1245) = (2451)$.

Thus the representation of a permutation as a product of transposition is not unique.

$p = (1245)$

$= (12)(14)(15)$

$p^1 = (2451) = (24)(25)(21)$

$\therefore p \neq p_1$

$(1245) \neq (2451)$.

Theorem: 3.12 If a permutation $p \in S_n$. Is a product of r transposition and also a product of s transposition. Then either r and s are both e, (or) both add.

Proof:

Let $p = t_1 t_2 \cdots t_r = t_1' t_2' \cdots t's$ where t_i are transposition. Now consider the polynomial

in n variables $x_1, x_2 \ldots x_n$ given by

$$\Delta = (x_1 - x_2)(x_1 - x_3) \ldots (x_1 - x_n) \cdot$$
$$(x_2 - x_3)(x_2 - x_4) \ldots (x_2 - x_n) \cdot$$
$$\ldots\ldots$$
$$\ldots\ldots\ldots$$
$$\times (x_{n-1} - x_n) = \prod_{i<j} (x_i - x_j)$$

For any permutation $p \in S_n$ we define.

$$p(\Delta) = \prod_{i<j} (x_{p(i)} - x_{p(j)})$$

Consider the transposition $t = (ij)$

Then the factor $x_i - x_j$ in Δ becomes $x_j - x_i$ Any factor $(x_k - x_l)$ of Δ in which neither i nor j is equal to k or l is unchanged. All other factors of Δ can be paired to form products of the form $\pm (x_i - x_k)(x_k - x_j)$

The sign being determined by the relative magnitudes of i, j and k.

Since t interchanges x_i and x_j any such product is unchanged.

Hence the effect to the transposition t on Δ is just to change the sign of Δ i.e. $t(\Delta) = -\Delta$.

$\therefore P(\Delta) = (t_1 . t_2 . \cdots t_r)(\Delta) = (-1)^r \Delta$.

Also $P(\Delta) = (t_1' t_2' \ldots t_s')(\Delta) = (-1)^s \Delta$.

$\therefore (-1)^r = (-1)^s \Rightarrow r$ and s are both even or both odd.

Definition:

A permutation $p \in S_n$ is called even or odd according as p can be expressed as product of an even number of transposition or odd number of transpositions exclusively.

Ex:

1) Consider the permutation

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 4 & 1 & 7 & 2 & 5 \end{pmatrix}$$

$p = (1\,3\,4)(2\,6)(5\,7) = (1\,3)(1\,4)(2\,6)(5\,7)$

$\therefore p$ is a product of 4 transposition.

Hence p is an even permutation.

2) Consider the permutation

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 5 & 4 & 3 & 6 & 1 & 7 & 9 & 8 \end{pmatrix}$$

$P = (1\ 2\ 5\ 6)(3\ 4)(8\ 9) = (1\ 2)(1\ 5)(1\ 6)$

$(3\ 4)(8\ 9)$

∴ P is product of 5 transposition.

Hence p is an odd permutation.

Theorem: 3.13

(i) The product of two even permutation is an even permutations.

(ii) The product of two odd permutation is an even permutation is an odd permutation

(iii) The product of an even permutation and an odd permutation is an odd permutation.

(iv) The inverse of an odd permutation is an even permutations.

(v) The inverse of an odd permutation is an odd permutation.

(vi) the identity permutation ϵ is an even permutation

Proof:

Let P_1, P_2 be two permutation. If P_1 is a product of r transposition and P_2 is a product of s transpositim. Then $P_1 P_2$ is product of $r+s$ transposibion.

Hence (i), (ii) and (iii) follow Now suppose that a permutation p is a product of transpositi$_n$

say $p = t_1 + t_2 + \cdots t_r$ then

$$p^{-1} = (t_1 \cdot t_2 \cdots t_r)^{-1}$$

$$= t_r^{-1} \cdots t_2^{-1} t_1^{-1} = t_r \cdots t_2 t_1.$$

p^{-1} is also a product of r transposition.

This proves (iv) and (v).

Now $e = (1\,2)(1\,2)$ and hence e is an even permutation. which proves (vi).

Theorem: 3.14

Let A_n be the set of all even permutations in S_n. Then A_n is a group containing $\frac{n!}{2}$ permutations.

Proof:

From (i), (vi) and (iv) of theorem 3.13

we see that An is a group.

Now Let Bn be the set of all odd permutations in Sn.

Define $f: A_n \to B_n$ by $f(P) = (12)P$.

f is 1-1 For $f(P_1) = f(P_2) \Rightarrow (12)P_1 = (12)P_2$

$\Rightarrow P_1 = P_2$.

f is on to, for $\alpha \in B_n$ then $(12)\alpha \in A_n$ and $f[(12)\alpha] = (12)(12)\alpha = \alpha$.

Thus f is a bijection and hence the number of odd permutations in Sn = the number of even permutations in Sn. Since Sn contains n! Permutations An has $\frac{n!}{2}$ elements.

Definition: (Alternating group)

The group An of all even permutations in Sn is called alternating group. on n symbols.

UNIT - II

Definition: (sub groups) :.

Let U be a set with a binary operation * defined on it. Let $S \subseteq U$.

2020.12.11 14:34

If for each a, b, ∈ S a*b [computed in G] is in S we say that S is closed with respect to the binary operation *.

Examples:

1) (Z, +) is a group. The set E of all even Integers. is closed under + and further (E, +) is it self a group.

2) The set of G of all non-singular 2×2. Matrices form a group under Matrix multiplicati-on Let H be the set of all Matrices of the form $\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$. H is subset of G. Also H itself is a group under Matrix Multiplication.

Definition: Subgroup

A subset H of group G is called a sub-group of G if H forms a group with respect to the binary operation in G.

Definition: Improper subgroup

Let G be any group. Then {e} and G are subgroups of G. They are called

Define: normaliser

Note: Let G be a group. Let $H_a = \{x / x \in G \text{ and } ax = xa\}$.

H_a is called the normaliser of a in G.

cyclic groups: define

Let G be a group. Let $a \in G$

Then $H = \{a^n / n \in \mathbb{Z}\}$ is a subgroup of G (verify).

H is called the cyclic subgroup of G generated by a and is denoted by $\langle a \rangle$.

Examples:

1) In $(\mathbb{Z}, +)$, $\langle 2 \rangle = 2\mathbb{Z}$ which is the group of even integers.

2) In the group $G = (\mathbb{Z}_{12}, \oplus)$ $\langle 3 \rangle = \{0, 3, 6, \ldots$

$\langle 6 \rangle = \{0, 5, 10, 3, 8, 1, 6, 11, 4, 9, 2, 7\} = \mathbb{Z}_{12}$.

3) In the group $G = \{1, i, -1, -i\}$ $\langle i \rangle = \{i, i^2, i^3 \ldots\} = \{1, -1, -i, 1$

Definition: generator

Let G be a group and let $a \in G$. a is called a generator of G if $\langle a \rangle$

2020.12.11 14:33

Define: cyclic A group G is cyclic if there exist an element $a \in G$ such that $\langle a \rangle = G$.

Note:

If G is a cyclic if there exists an element a then every element of G is of the form a^n for some $n \in \mathbb{Z}$.

Examples:

1) $(\mathbb{Z}, +)$ is a cyclic group. is a generator of this group -1 is also a generator of this group Thus a cyclic group can have more than one generator.

2) $(n\mathbb{Z}, +)$ is a cyclic group n and $-n$ are generators of this group.

3) $(Z_8, \oplus)$ is a cyclic group $1, 3, 5, 7$ are all generator of this group.

4) $(Z_n, \oplus)$ is a cyclic group for all $n \in \mathbb{N}:1$ is a generator of this group. In fact if $m \in Z_n$ and $(m, n) = 1$. then m is a generator of this group.

5) $G = \{1, 1, -i\}$ is a cyclic group under usual multiplication i is a generator $-i$ is

2020.12.11 14:38

a generator of U. However -1 is not a generator of this group.

6) $U = \{1, w, w^2\}$ where $w \neq 1$ is a cube root of unity is a cyclic group. w and w^2 are both generators of this group.

7) In The group $U = (Z_7 - \{0\}, \cdot)$ 3 and 5 are both generators. Here 2 is not a generator of U since $\langle 2 \rangle = \{2, 4, 1\} \neq U$.

8) Let A be a set containing more than one element. Then $(\mathcal{P}(A), \Delta)$ is not cyclic for Let $B \in \mathcal{P}(A)$ be any element. Then $B \Delta B \neq \phi$ so that $\langle B \rangle = \{B, \phi\} \neq \mathcal{P}(A)$.

9) $(R, +)$ is not a cyclic group since for any $x \in R$ $\langle x \rangle = \{nx / n \in Z\} \neq R$.

Theorem: 3.22

Any cyclic group is abelian.

Proof:

Let $U = \langle a \rangle$ be a cyclic group.

Let $x, y \in Z$. Then $x = a^r$ and $y = a^s$ for some

Hence $xy = a^r a^s = a^{r+s} = a^s a^r = yx$.

G is abelian.

Theorem: 3.23

A subgroup of cyclic group is cyclic.

Proof:

Let G be a cyclic group generated by a and let H be a subgroup of G. We claim that H is cyclic.

clearly every element of H is of the form a^n for some Integer n.

Let m be the smallest positive Integer such that $a^m \in H$. We claim that a^m is a generator of H.

Let $b \in H$ Then $b = a^n$ for some $n \in \mathbb{Z}$

Let $n = mq + r$ where $0 \leq r \leq m$.

Then $b = a^n = a^{mq+r} = a^{mq} a^r = (a^m)^q a^r$.

$$a^r = (a^m)^{-q} b. \quad \text{---}(1)$$

Now $a^m \in H$. since H is a subgroup $(a^m)^{-q} \in H$.

ALSO $b \in H$.

By (1) $a^r \in H$ and $0 \leq r < m$.

2020.12.11 14:32

But m is the least positive Integer such that $a^n \in H$.

$r = 0$ Hence $b = a^n = a^{qm} = (a^m)^q$.

Every element of H is a power of a^m.

$H = \langle a^m \rangle$ and hence H is cyclic.

$\therefore$ A subgroup of cyclic group is cyclic.

Hence H is cyclic.

Order of an element:

Define: order

Let G be a group. and let $a \in G$. The least positive Integer n such that $a^n = e$ is called the order of a.

Definition: Infinite

If there is no positive integer n such that $a^n = e$ then the order of a is said to be Infinite.

Ex:

$(\mathbb{C}^*, \cdot)$, i is an element of order 4.

theorem: 3.24

Let G be a group and $a \in G$. Then the order of a is the same as the order of the cyclic group generated by a.

proof:

Let a be an element of order n. Then $a^n = e$ we claim that $e, a, a^2 \ldots a^{n-1}$ are all distinct.

Suppose $a^r = a^s$ where $0 < r < s < n$.

Then $a^{s-r} = e$ and $s - r < n$ which contradicts the definition of the order of a.

Hence $e, a, a^2 \ldots a^{n-1}$ are n distinct elements and $\langle a \rangle = \{e, a, a^2 \ldots a^{n-1}\}$ which is of order n.

If a is of infinite order. The sequence of elements $a, a^2 \ldots a^n \ldots$ are all distinct and are in $\langle a \rangle$. Hence $\langle a \rangle$ is an infinite group.

Theorem: 3.25

In a finite group every element is of finite order.

proof:

Let $a \in U$. If a is of infinite order then $\langle a \rangle$ is an infinite subgroup of U which is a contradiction. since U is finite.

Hence the order of a finite.

Remark:

The converse of the above theorem is not true ie) if U is a group in which every elements is of finite order then the group. U need not be finite For example if S is any infinite set the $(\mathcal{P}(S), \Delta)$ is an infinite group. In this group $A \Delta A = \phi$ for every $A \in \mathcal{P}(S)$ so that the order of every element other than ϕ is 2.

Theorem: 3.26

Let U be a group and a be an element of order n in U. Then $a^m = e$ iff n divides m.

Proof:

Suppose n/m Then $m = nq$ where $q \in \mathbb{Z}$.

$$a^m = a^{nq} = (a^n)^q = e^q = e.$$

Conversely Let $a^m = e$.

Let $m = nq + r$ where $0 \leq r < n$.

$$a^m = a^{nq+r} = a^{nq} a^r = e a^r = a^r.$$

$a^r = e$ and $0 \leq r < n$.

Now since n is the smallest positive Integer such that $a^n = e$. we have $r = 0$

Hence $m = nq$.

Therefore n/m.

Theorem: 3.27

Let G be a group and $a, b \in G$ then

(i) order of a = order of a^{-1}

(ii) order of a = order of $b^{-1}ab$.

(iii) order of ab = order of ba.

Proof:

Let a be an element of order n.

Then $a^n = e$.

$$(a^{-1})^n = (a^n)^{-1} = e^{-1} = e.$$

Now if possible Let $0 < m < n$ and $(a^1)^m = e$

$(a^m)^{-1} = e$.

Hence $a^m = e$ which contradicts

The definition of the order of a. Thus n is the least positive Integer such that $(a^{-1})^n = e$.

The order of a^{-1} is n.

ii) we shall first prove that for any positive Integer r.

$$(b^{-1}ab)^r = b^{-1}a^r b \quad \rightarrow (1).$$

(1) is trivialy true if $r=1$.

Now, suppose that in (1) is true for $r=k$ so that $(b^{-1}ab)^k = b^{-1}a^k b$.

Then, $(b^{-1}ab)^{k+1} = (b^{-1}ab)^k (b^{-1}ab)$.

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

$$= b^{-1}a^{k+1}b.$$

Hence by induction (1) is true For all positive Integers.

Now let a be an element of order n. Then $a^n = e$.

$$(b^{-1}ab)^n = b^{-1}a^n b \quad [\text{by (1)}]$$

$$= b^{-1}eb = e.$$

Now, if possible let $0<m<n$ and

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

$b^{-1}a^m b = e$. Hence $a^m = e$ which contradicts the definition of the order n. Then is the least positive integer such that:

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

The order of $b^{-1}ab$ is n.

(iii) The order of ab = The order of $a^{-1}(ab)a$ (by (ii))

= The order of ba.

Theorem: 3.28

Let G be a group and let a be an element of order n in G. Then the order of a^s where $e \leq s \leq n$ is n/d where d is the g.c.d of n and s.

Proof:

Let $(n/d) = k$ and $(s/d) = l$. so that k and l are relatively prime.

Now $(a^s)^k = a^{sk} = a^{ldk} = a^{ln} = (a^n)^l = e$

Further if m is any positive integer such that $(a^s)^m = e$ then $a^{sm} = e$.

Since order of a is n we have n/sm.

kd / lm. Hence k / lm.

But k and l are relatively prime.

Hence k/m so that $m \geq k$.

Then k is the least positive integer such that $(a^s)^k = e$.

order of $a^s = k = n/d$.

Problem: 1

If G is a finite group with even number of elements then G contains at least one element of order 2

Sol:

a is an element of order $2 \Leftrightarrow a^2 = e$.

$\Leftrightarrow a^{-1} = a$.

Hence it is enough if we prove that there exists an element different form in G whose inverse it self.

Let $S = \{a / a \in G,\ a \neq a^{-1}\}$

clearly $a \in S \Rightarrow a^{-1} \in S$ and $a \neq a^{-1}$

Hence S contains an even number of elements

Also $e \notin A$.

Hence $A \cup \{e\}$ contains an odd number of elements since the order of the group is even there exists at least one element $a \notin A \cup \{e\}$ clearly $a = a^{-1}$.

Problem: 2

The order of a permutation p is the l.c.m (least common multiple) of the lengths if its disjoin cycle.

Soln: Let $p = c_1 c_2 \cdots c_r$ where c_i's are mutually disjoin cycles of lengths l_i NOW let $p^m = e$. since, product of disjoin . cycles is commutative $e = p^m = (c_1 c_2 \cdots c_r)^m = c_1^m c_2^m \cdots c_r^m$.

Now, since the element moved by one cycle were left fixed by all the order cycles. $c_1^m = c_2^m \cdots c_r^m = e$.

Now $c_1^m = e \Rightarrow l_1 / m$ since the order of $c_1 = l_1$ similarly $l_1 l_2 \cdots l_r$ divide m.

Thus m is common multipule of $l_1, l_2 \cdots l_r$. The order of p in the least such that

n, which is obviously the l.c.m of $k_1, k_2, \ldots, k_r$.

Problem: 8

If a is a generator of the cyclic group G and if there exists two unequal integers m and n such that $a^m = a^n$, prove that G is finite group.

Soln:

Since m and n are unequal we may assume that $m > n$.

Hence $m-n$ is a positive Integer.

Also $a^m = a^n \Rightarrow a^{m-n} = e$.

order of a is finite.

$G = \langle a \rangle$ is a finite group. [by Theorem 3.24]

Cosets and Lagrange's theorem:

Definition: Left coset and Right coset:

Let H be a subgroup of a group G. Let $a \in G$. Then the set $aH = \{ah / h \in H\}$ is called the **Left coset** of H defined by a in G.

2020.12.11 14:31

Similarly $Ha = \{ha / h \in H\}$ is called the right coset of H defined by a.

Examples:

1) Let us determine the Left cosets of $(5\mathbb{Z}, +)$ in $(\mathbb{Z}, +)$ Here the operations is +

$0+5\mathbb{Z} = 5\mathbb{Z}$ is itself a left coset.

Anoth Left coset is $1+5\mathbb{Z} = \{1+5n / n \in \mathbb{Z}\}$

we noticed That this Left contains all integers having remainder 1 when devided by 5.

Similarly $2+5\mathbb{Z} = \{2+5n / n \in \mathbb{Z}\}$

$3+5\mathbb{Z} = \{3+5n / n \in \mathbb{Z}\}$

$4+5\mathbb{Z} = \{4+5n / n \in \mathbb{Z}\}$.

These are all the left coset of $(5\mathbb{Z}, +)$ Here also we note that all the left cosets are mutually disjoint. and their union is $\mathbb{Z}$. In other words the collection of all left cosets forms a partition. of a group.

2) Consider $(\mathbb{Z}_{12}, \oplus)$. Then $H = \{0, 4, 8\}$ is a subgroup of U_{12}.

The Left cosets of H are given by

$0+H = \{0, 4, 8\} = H.$

$1+H = \{1, 5, 9\}$:

$2+H = \{2, 6, 10\}$

$3+H = \{3, 7, 11\}$

we notice that

$4+H = \{4, 8, 0\} = H$ and

$5+H = \{5, 9, 1\} = 1+H$ etc.

Theorem: 3.29

Let G be a group and H be a subgroup of G Then

(i) $a \in H \Rightarrow aH = H$.

(ii) $aH = bH \Rightarrow a^{-1}b \in H$.

(iii) $a \in bH \Rightarrow a^{-1} \in H b^{-1}$

(iv) $a \in bH \Rightarrow aH = bH$.

Proof:

(i) Let $a \in H$. we claim that $aH = H$.

Let $x \in aH$. Then $x = ah$. for some $h \in H$.

Now. $a \in H$ and $h \in H \Rightarrow ah = x \in H$.

(since H is a subgroup).

Hence $aH \subseteq H$. —(1)

Let $x \in H$. Then $x = a(a^{-1}x) \in aH$.

Hence $H \subseteq aH$ Thus $H = aH$. —(2)

From (1) & (2)

Conversely, let $aH = H$ Now $a = ae \in aH$.

$\therefore a \in H$.

(ii) Let $aH = bH$.

$\therefore a^{-1}(aH) = a^{-1}(bH)$. (pre and post multiplication of a^{-1})

$\therefore H = (a^{-1}b)H$.

$\therefore a^{-1}b \in H$ (by (i))

Conversely let $a^{-1}b \in H$.

Then $a^{-1}bH = H$ (by (ii))

$\therefore aa^{-1}bH = aH$ and hence $bH = aH$.

(iii) Let $a \in bH$. Then $a = bh$ for some $h \in H$.

$\therefore a^{-1} = (bh)^{-1} = h^{-1}b^{-1} \in Hb^{-1}$.

Converse can be similarly proved.

(iv) Let $a \in bH$. We claim that $aH = bH$.

Let $x \in aH$ Then $x = ah_1$ for some $h_1 \in H$

$a \in bH \Rightarrow a = bh_2$ for some $h_2 \in H$ $\rightarrow (1)$

$\therefore x = (bh_2)h_1 = b(h_2 h_1) \in bH.$

$\therefore aH \subseteq bH.$ $\rightarrow (2)$

Now, Let $x \in bH$. Then $x = bh_3$ for some $h_3 \in H$.

Also from (1), $b = ah_2^{-1}$.

$\therefore x = ah_2^{-1} h_3 \in aH.$

$\therefore bH \subseteq aH$. Hence $aH = bH.$ $\rightarrow (3)$

from eqn (2) & (3) we get

Conversely, let $aH = bH$.

Then $a = ae \in aH.$

$\therefore a \in bH$ //.

Theorem: 3.30

Let H be a subgroup of G. Then

(i) any two left cosets of H are either identical or disjoint.

(ii) union of all the left cosets of H in G.

(iii) The number of elements in any left coset aH is the same as the number of elements in H.

Proof:

(i) Let aH and bH be two Left cosets.

suppose aH and bH are not disjoint.

we claim that $aH = bH$.

since aH and bH are not disjoint.

$aH \cap bH \neq \phi$.

$\therefore$ there exists an element $c \in aH \cap bH$

$\therefore$ $c \in aH$ and $c \in bH$.

$\therefore$ $aH = cH$ and $bH = cH$ [by (iv) of theorem 3.2.9]

$\therefore$ $aH = bH$.

which is contradiction. our assumption is not true.

(ii) Let $a \in G$. Then $a = ae \in aH$.

Every element of G belongs to a left coset of H.

$\therefore$ The union of all the Left cosets of H is G.

(iii) The map $f : H \to aH$ defined by $f(h) = ah$. is clearly a bijection. Hence every left cosets has the same number of elements as H.

Note:

This theorem shows that the collection of all Left cosets forms a partition of the group.

Note: 2

The above result is true if we replace Left cosets by Right cosets. In what follows the result we prove for Left cosets are also true for right cosets.

Remark:

Let H be a subgroup of G. We define a relation in G as follows. Define

$$a \sim b \iff a^{-1}b \in H.$$

Then $\sim$ is an equivalence relation

For $a^{-1}a = e \in H$. Hence $a \sim a$ Hence $\sim$ is reflexive.

$$a \sim b \Rightarrow a^{-1}b \in H \Rightarrow (a^{-1}b)^{-1} \in H.$$

$$\Rightarrow b^{-1}a \in H \Rightarrow b \sim a.$$

Hence $\sim$ is symmetric.

Now,

$a \sim b$ and $b \sim c \Rightarrow a^{-1}b \in H$ and $b^{-1}c \in H$

$$\Rightarrow (a^{-1}b)(b^{-1}c) \in H.$$

$$\Rightarrow a^{-1}c \in H.$$

$$\Rightarrow a \sim c.$$

Hence $\sim$ is transitive.

Thus $\sim$ is an equivalence relation.

2020.12.11 14:30

Now - we claim that equivalence class $[a] = aH$

Let $b \in [a]$. Then $b \sim a$.

$a^{-1}b \in H$.

$a^{-1}b = h$. For some $h \in H$.

$b = ah$. Hence $b \in aH$.

$[a] \subseteq aH$.

Also, $b \in aH \Rightarrow b = ah$ for some $h \in H$.

$\Rightarrow a^{-1}b = h \in H$.

$\Rightarrow a \sim b$.

$\Rightarrow b \in [a]$.

Thus the left cosets of H in G are precisely the equivalence classes determined by $\sim$. Hence the left cosets form a partition of G. This gives another proof of Theorem 3.

Theorem : 3.31

Let H be a subgroup of G. The number of left cosets of H is the same as the number of right cosets of H.

Proof:

Let L and R respectively denote the set of left and right cosets of H. We define a map $f : L \to R$ by $f(aH) = Ha^{-1}$.

f is well defined for $aH = bH \Rightarrow$

$a^{-1}b \in H$.

$\Rightarrow a^{-1} \in Hb^{-1}$.

$\Rightarrow Ha^{-1} = Hb^{-1}$.

f is 1-1 for,

$f(aH) = f(bH)$

$\Rightarrow Ha^{-1} = Hb^{-1}$.

$\Rightarrow a^{-1} \in Hb^{-1}$.

$\Rightarrow a^{-1} = hb^{-1}$ for some $h \in H$.

$\Rightarrow a = bh^{-1}$.

$\Rightarrow a \in bH$

$\Rightarrow aH = bH$.

f is onto. Forevery right coset Ha has a pre. Image under f namely $a^{-1}H$.

Hence f is a bijection from L to R.

Hence the number of Left coset is the same as the number of right cosets.

definition: Index

Let H be a subgroup of G. Then number of distinct Left (Right) cosets of H. in G is called the Index of H in G and is denoted by $[G : H]$.

2020.12.11 14:29

Examples:

In $(Z_8, \oplus)$, $H = \{0, 4\}$ is a subgroup

The left cosets of H are given by

$0+H = \{0, 4\} = H.$

$1+H = \{1, 5\}$

$2+H = \{2, 6\}$

$3+H = \{3, 7\}.$

These are the four distinct left cosets of H.

Hence the index of the subgroup H is 4.

Note that $[Z_8 : H] \times [H] = 4 \times 2 = 8 = |Z_8|$

Theorem: 3.32

(Lagrange's theorem) Let G be a finite group of order n and H be any subgroup of G. Then the order of H divides the order of G.

Proof:

Let $|G| = n$ and $[G : H] = r$.

Then the number of distinct left cosets of H in G is r.

By theorem 3.30 these r left cosets are mutually disjoint, they have the same number of elements namely m and their

union in G.

$\therefore n = rm$. Hence m divides n.

Corollary:

$$[G : H] = \frac{|G|}{|H|}.$$

Note: 1

Lagrang's theorem has many important applications in Groups theory. For example a Group G of order 8 cannot have Subgroups of order 3, 5, 6, or 7 In fact any proper subgroup of G must be of order 2 or 4.

Note: 2

Any Group of prime order has no proper subgroups.

Note: 3 The converse of Lagrange's theorem is false.

(c) If G is a group of order n and m divides n, then G need not have a Subgroups of order m.

2020.12.11 14:29

For example A_4 is a group of order 12 and it does not have a subgroup of order 6.

However there are groups in which the converse of Lagrange's theorem is true.

For example consider S_3. This is a of order 6. $\{e, p_4\}$ is a subgroup of order 2 and $\{e, p_1, p_2\}$ is a subgroup of order 3 Hence for every divisor m of 6. there is a subgroup of S_3 of order m.

Theorem: 3.33

The order of any element of a finite group G divides the order of G.

Proof:

Let G be a group of order n. Let $a \in G$ be an element of order m. Then the order of a is the same as the order of the cyclic group $\langle a \rangle$.

Now. by Lagrange's theorem the order of the subgroup $\langle a \rangle$ divides the order of G.

Hence m/n.

Proof:

Suppose $H \cap K = \{e\}$.

$\therefore |H \cap K| = 1$

$\therefore |HK| = \frac{|H||K|}{|H \cap K|}$ (by Th A)

$= |H||K|$

$> \sqrt{|G|}\sqrt{|G|} = |G|$

$|H||K| > |G|$ which is a contradiction.

$\therefore H \cap K \neq \{e\}$.

UNIT-III

Normal subgroups and Quotient Groups:

Definition:

A subgroup H of G is called a normal subgroup of G if $gH = Hg$ $\forall g \in G$.

Examples:

1) For any group G, $\{e\}$ and G are normal subgroups.

2) In S_3, the subgroup $\{e, R, R^2\}$ is normal,

3) In S_3, the subgroup $\{e, F_1\}$ is not a normal.

Theorem: 3.39

Every subgroup of an abelian group is a normal subgroup.

Proof:

Let G be an abelian group and let H be a subgroup of G. Let $a \in G$.

We claim that $aH = Ha$.

Let $x \in aH$. Then

$x = ah$ for some $h \in H$.

$= ha$ (since G is abelian).

$\therefore x \in Ha$ Hence $aH \subseteq Ha$.

Similarly $Ha \subseteq aH$.

$\therefore aH = Ha$ and hence H is a normal subgroup of G.

Examples:

(i) nZ is a normal subgroup of $(Z, +)$

(ii) Every subgroup of $(Z_n, \oplus)$ is norma

(iii) Since any cyclic group is abeli any subgroup of a cyclic group is normal.

Theorem: 3.40

Let H be a subgroup of index 2 in a group G. Then H is a normal subgroup o

2020.12.11 14:28

Proof:

If $a \in H$ then $H = aH = Ha$.

If $a \notin H$, then aH is a left coset different from H.

Hence $H \cap aH = \phi$.

Further, since index of H in G is 2.

$H \cup aH = G$.

Hence $aH = G - H$.

Similarly $Ha = G - H$ so that $aH = Ha$.

Hence H is a normal subgroup of G.

Example:

The alternating group A_n is a subgroup of index 2 in S_n and hence is a normal subgroup of S_n.

Theorem: 3.41

Let N be a subgroup of G. Then the following are equivalent.

(i) N is a normal subgroup of G.

(ii) $aNa^{-1} = N$ for all $a \in G$.

(iii) $aNa^{-1} \subseteq N$ for all $a \in G$.

(iv) $ana^{-1} \in N$ for all $n \in N$ and $a \in G$.

2020.12.11 14:28

Proof:

(i) $\Rightarrow$ (ii)

Suppose N is a normal subgroup of G.

$\therefore aN = Na$ for all $a \in G$.

$\therefore aNa^{-1} = Naa^{-1} = Ne = N$ $(\because ne = en = n)$

(ii) $\Rightarrow$ (iii) and (iii) $\Rightarrow$ (iv) are obvious (iv) $\Rightarrow$ (i)

(i) $\Rightarrow$ (iv) Suppose N is a normal subgroup of G. Suppose that $aNa^{-1} \subseteq N$ for all $n \in N$ and $a \in G$.

We claim that $aN = Na$.

Let $x \in aN$.

$\therefore x = an$ for some $n \in N$.

$\therefore x = (ana^{-1})a \in Na$ (since $ana^{-1} \in N$)

$\therefore aN \subseteq Na \rightarrow (1)$.

Now, Let $x \in Na$

$\therefore x = na$ for some $n \in N$.

$\therefore x = a(a^{-1}na) = a(a^{-1}n(a^{-1})^{-1}) \in aN$.

$\therefore Na \subseteq aN \rightarrow (2)$

From (1) and (2) we get $Na = aN$.

Hence N is a normal subgroup of G.

is transitive.

$\therefore$ Isomorphism is an equivalence relation among groups.

Examples:

1) $(\mathbb{Z}, +) \cong (2\mathbb{Z}, +)$

Consider $f: \mathbb{Z} \to 2\mathbb{Z}$ given by $f(x) = 2x$.

Clearly f is a bijection. Also

$$f(x+y) = 2(x+y)$$

$$= 2x + 2y$$

$$= f(x) + f(y).$$

Hence f is an isomorphism.

2) Let $U = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \middle/ \; a \in \mathbb{R}^* \right\}$

U is a group under matrix multiplication we claim that $U \cong (\mathbb{R}^*, \cdot)$

Consider $f: U \to \mathbb{R}^*$ given by

$$f\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = a.$$

Clearly f is a bijection.

Now Let $A = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$ $= y$

Then $AB = \begin{pmatrix} ab & 0 \\ 0 & 0 \end{pmatrix}$

$f(AB) = ab = f(A)\, f(B)$.

Hence f is an isomorphism.

3) $(\mathbb{R}, +) \cong (\mathbb{R}^+, \cdot)$

Consider $f: \mathbb{R} \to \mathbb{R}^+$ given by $f(x) = e^x$.

clearly f is bijection.

Also $f(x+y) = e^{x+y} = e^x e^y = f(x)\, f(y)$.

Hence f is an isomorphism.

4) $U = \mathbb{R} - \{-1\}$ is a group under $*$ defined by $a * b = a + b + ab$. We claim that $U \cong (\mathbb{R}^*, \cdot)$

Consider $f: U \to \mathbb{R}^*$ given by $f(x) = x+1$

clearly f is an bijection.

Also

$$f(x * y) = f(x + y + xy)$$

$$= x + y + xy + 1$$

$$= (x+1)(y+1)$$

$$= f(x)\, f(y).$$

Hence f is an isomorphism.

5) $(\mathbb{Z}_n, \oplus)$ is a group.

Let U_n denote the set of all n^{th}

ots of unity U_n is a group under

and multiplication.

We claim that $(\mathbb{Z}_n, \oplus) \cong U_n$.

Consider $f: \mathbb{Z}_n \to U_n$ given by $f(m) = \omega^m$.

where $\omega = \cos(2\pi/n) + i \sin(2\pi/n)$

clearly f is a bijection.

Let $a, b \in \mathbb{Z}_n$ Let $a+b = q_n + r$ where $0 \le r \le n$

Then $a \oplus b = r$ Hence $f(a \oplus b) = \omega^r \longrightarrow (1)$.

Also $f(a)\, f(b) = \omega^a \omega^b = \omega^{a+b} = \omega^{q_n + r}$.

$= \omega^{q_n} \omega^r$ (since $a+b = q_n + r$)

$= 1 \cdot \omega^r$ (since $\omega^n = 1$)

$= \omega^r \longrightarrow (2)$.

From (1) & (2) we get

$f(a \oplus b) = f(a)\, f(b)$.

Hence f is an isomorphism.

Theorem: 3.45

Let $f: U \to U'$ be an isomorphism.

Then (i) $f(e) = e'$ where e and e' are the

Identity elements of G and G' respectively

(ie) In an isomorphism identity is mapped onto identity.

(ii) $f(a^{-1}) = [f(a)]^{-1}$.

Proof:

To prove that $f(e) = e'$ it is enough if we prove that $a' f(e) = f(e) a' = a'$ for all $a' \in G'$

Let $a' \in G'$ since $f: G \to G'$ is a bijection.

There exists such that $a \in G$ such that $f(a) = a'$. similarly $f(e)\, a' = a'$.

$f(e) = e'$.

(ii) It is enough to prove that

$f(a)\, f(a^{-1}) = f(a^{-1})\, f(a) = e'$.

Now $f(a)\, f(a^{-1}) = f(a a^{-1}) = f(e) = e'$.

Also $f(a^{-1})\, f(a) = f(a^{-1} a) = f(e) = e'$.

$f(a)\, f(a^{-1}) = f(a^{-1} a) = f(e) = e'$.

$f(a)\, f(a^{-1}) = f(a^{-1})\, f(a) = e'$.

$[f(a)]^{-1} = f(a^{-1})$.

Remark:

The concept of isomorphism for

groups is extremely important. Since two isomorphic groups G and G' have essentially the same structure if one group G has an additional property [for example abelian or cyclic] then the group G' also has this additional property. This is seen in the following three theorems.

Theorem: 3.46

Let $f: G \to G'$ be an isomorphism If G is abelian Then G' is also abelian.

proof:

Let $a'\ b' \in G'$. Then there exists $a, b \in G$ such that $f(a) = a'$ and $f(b) = b'$.

Now $a'b' = f(a)\,f(b) = f(ab) = f(ba)$.

$= f(b)\,f(a)$

$= b'\,a'$.

Hence G is abelian.

Theorem: 3.47

Let $f: G \to G'$ be an isomorphism. Let $a \in G$ Then the order of a is equal to the

order of $f(a)$ (ie) Isomorphism preserves the order of each element in a group

Proof:

Subgroup Suppose the order of a is n. Then n is the least positive integer such that $a^n = e$.

Now, $[f(a)]^n = f(a) \ldots\ldots f(a)$ [$f(a)$ written n times]

$= f(a^n)$ [since f is an Isomorphism]

$= f(e)$

$= e'$.

Now if possible Let m be a positive integer such that $0 < m < n$ and $[f(a)]^m = e'$.

Then $f(a^m) = [f(a)]^m = e'$.

But $f(e) = e'$. {since f is 1-1 we have $a^m = e$. which contradicts the definition of the order of a.

h is the least positive integer such that $[f(a)^n] = e'$.

$\therefore$ The order of $f(a)$ is n.

2020.12.11 14:27

$= a^{3n} a^{t}$

$= (a^{n})^{3} a^{t}$

$= ea^{t}$

$= a^{t} \longrightarrow (2)$.

From (1) & (2) we get $f(r \oplus s) = f(r) \cdot f(s)$.

Hence f is an isomorphism.

[Theorem: 3.5] [cayley's theorem] :.

State and prove cayley's theorem.

Statement:

Any finite group is isomorphic to a group of permutations.

Proof:

We shall prove this theorem in 3 steps. we shall first find a set G' of permutations. Then we prove that G' is a group of permutations and finally we exhibit an isomorphism $\phi : G \to G'$.

Step : 1

Let G be a finite group of order n.

Let $a \in G$.

Define $f_a : G \to G'$ by $f_a(x) = ax$.

Now f_a is 1-1 since $f_a(x) = f_a(y) \Rightarrow ax = ay \Rightarrow x = y$.

f_a is onto (since if $y \in G$ then

$$f_a(a^{-1}y) = a(a^{-1}y) = y).$$

Thus f_a is a bijection.

Since G has n element f_a is just a permutations on n symbols.

Let $G' = \{ f_a / a \in G \}$.

Step : 2

We prove that G' is a group. Let $f_a, f_b \in G'$

$$(f_a \circ f_b)(x) = f_a(f_b(x)) = f_a(bx) \quad (\because f_b(x) = bx)$$

$$= a(bx)$$

$$= (ab)x$$

$$= f_{ab}(x).$$

Hence $f_a \circ f_b = f_{ab}$. Hence G' is

is closed under composition of mappings.

$f_e \in U'$ is the identity element.

The inverse of f_a in U' is $f_{a^{-1}}$.

Step 3

We prove that $U \cong U'$.

Define $\phi : U \to U'$ by $\phi(a) = f_a$.

$\phi(a) = \phi(b) \Rightarrow f_a = f_b \Rightarrow f_a(x) = f_b(x)$.

$\Rightarrow ax = bx \Rightarrow a = b$.

Hence ϕ is 1-1. obviously ϕ is onto.

Also $\phi(ab) = f_{ab} = f_a \circ f_b = \phi(a) \circ \phi(b)$.

Hence ϕ is an isomorphism.

Example:

Consider the group $U = \{e, a, b\}$.

whose multiplication table is given by

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

2020.12.11 14:26

By Cayley's theorem G is isomorphic to the permutation group $G' = \{ f_e, f_a, f_b \}$ where

$$f_e = \begin{pmatrix} e & a & b \\ e & a & b \end{pmatrix} \quad f_a = \begin{pmatrix} e & a & b \\ a & b & e \end{pmatrix}.$$

and $$f_b = \begin{pmatrix} e & a & b \\ b & e & a \end{pmatrix}.$$

Definition: (Automorphism) :-

An isomorphism of a group G to itself is called an automorphism of G.

Example: (inner automorphism) Define:

(* Let G be any group. Let $a \in G$

Then $\phi_a : G \to G$ defined by $\phi_a(x) = axa^{-1}$ is an automorphism of G.)

For let $x, y \in G$. Then

$$\phi_a(x) = \phi_a(y) \Rightarrow axa^{-1} = aya^{-1}.$$

$$\Rightarrow x = y \quad \text{(by cancellation Law)}$$

ϕ_a is 1-1.

Also

$$\phi_a(a^{-1}xa) = a(a^{-1}xa)a^{-1}.$$

$$= (aa^{-1})x(aa^{-1})$$

2020.12.11 14:26

Hence $a^{-1}xa$ is the pre image of x under ϕ_a.

Also $\phi_a(xy) = axya^{-1}$.

$= (axa^{-1})(aya^{-1})$.

$= \phi_a(x)\,\phi_a(y)$.

Thus ϕ_a is an automorphism of G.

Definition: Inner automorphism:

The automorphism $\phi_a : G \to G$ defined in example 4 is called an inner automorphism of the group G.

Let G be a group. The set of all automorphism of G is denoted by $Aut\ G$. The set of all inner automorphisms of G is denoted by $I(G)$.

Theorem: 3.62

For any group G.

(i) Automorphism of G is a group under composition of functions.

(ii) $I(G)$ is a normal subgroup of Automorphism G.

Proof:

(i) Let $f, g \in$ automorphism G.

f and g are isomorphisms of G to itself.

$f \circ g$ is an isomorphism of G to itself

[Theorem 3.44]

$f \circ g \in$ automorphism G.

$f \in$ Automorphism $G \Rightarrow f^{-1} \in$ Aut G [Theorem 3.44]

clearly composition of function is associative

Hence Aut G is a group.

(ii) Let $\phi_a \cdot \phi_{ebe} \in I(G)$. Then

$$(\phi_a \phi_b)(x) = \phi_a(bxb^{-1})$$

$$= a(bxb^{-1})a^{-1}.$$

$$= (ab)x(ab)^{-1}$$

$$= \phi_{ab}(x)$$

Hence $\phi_a \phi_b = \phi_{ab} \in I(G)$.

ϕ_e is the identity element of $I(G)$ and inverse of ϕ_a is $\phi_{a^{-1}}$.

$I(G)$ is a subgroup of

2020.12.11 14:26

We now prove that $I(G)$ is a normal subgroup of automorphism G.

Let $\alpha \in Aut(G)$ and $\phi_a \in I(G)$. Then

$$(\alpha \phi_a \alpha^{-1})(x) = \alpha \phi_a(\alpha^{-1}(x))$$

$$= \alpha(a\alpha^{-1}(x)a^{-1})$$

$$= \alpha(a)\alpha\alpha^{-1}(x)\alpha(a^{-1})$$

$$= \alpha(a)x[\alpha(a)]^{-1}.$$

$$= \phi_{\alpha(a)}(x).$$

$$\alpha\phi_a\alpha^{-1} = \phi_{\alpha(a)} \in I(G).$$

Hence $I(G)$ is a normal subgroup of Automorphism G.

Theorem: 3.52

Let G be a cyclic group generated by a. Let $f: G \to G$ be a mapping such that $f(xy) = f(x)f(y)$. Then f is an automorphism of G. iff $f(a)$ is a generator of G.

Proof:

2020.12.11 14:25

Let f be an automorphism of U. We shall prove that $f(a)$ is a generator of U.

CASE (i)

Let U be a finite cyclic group of order n. Then order of a is n. By theorem 3.46.

using statement of proof

$f(a)$ is also an element of order n and hence $f(a)$ is a generator of U.

We claim that $f(U) = H$.

Let $x' \in f(U)$. Then $x' = f(x)$ for some $x \in U$.

Now $x = a^n$ for some n since $U = \langle a \rangle$.

$\therefore x = f(a^n)$

$= [f(a)]^n \in H$.

$f(U) \subseteq H$.

Now Let $x \in H$. Then $x = [f(a)]^n$ for some n.

$x = f(a^n)$. Hence $x \in f(a)$.

$H \subseteq f(U)$. Hence $f(U) = H$.

Since H is a proper subgroup of U

f is not onto which is a contradiction.

Hence $f(a)$ is generator of U.

2020/12/11 14:25

Conversely Let $f: U \to U$ be a mapping such that $f(xy) = f(x)\, f(y)$ and Let $f(a)$ be a generator of U. we shall prove that f is an automorphism.

It is enough if we prove that f is 1-1 and onto.

Let $x \in U$. since $f(a)$ is a generator of U $x = [f(a)]^n$ for some n.

clearly $f(a)^n = [f(a)]^n = x$. Thus x has a pre Image a^n under f.

Hence f is onto.

NOW To prove f is 1-1

Case(i)

U is finite.

Since any function from a finite set onto itself.

Is neccessarily 1-1 (verify) f is 1-1

$= 3 \oplus 3 \oplus 3 \oplus 3 \oplus 3.$

$= 7$

$= f_q(1).$

Homomorphism: Definition

A map f from a group G into a group G' is called a homomorphism if $f(ab) = f(a)\,f(b)$ for all $a, b \in G$.

Isomorphism :-

Obviously every isomorphism is a homomorphism and a bijective homomorphism is an isomorphism.

Examples:

(i) $f(\mathbb{Z}, +) \to (\mathbb{Z}, +)$ defined by $f(x) = 2x$.

is a homomorphism. For $f(x+y) = 2(x+y) = 2x+2y.$

$= f(x) + f(y)$

Note that f is 1-1.

(iii) $f:(\mathbb{R}^*, \cdot) \to (\mathbb{R}^+, \cdot)$ defined by $f(x) = |x|$ is a homomorphism. For $f(xy) = |xy| = |x||y| = f(x)f(y)$.

This homomorphism is onto.

Definition: (Canonical homomorphism)

Let G be a group and N a normal subgroup of G.

$f: G \to G/N$ given by $f(a) = Na$ is a homomorphism. For $f(ab) = Nab = Na\,Nb = f(a)f(b)$.

f is called the canonical homomorphism from G to G/N. Note that f is onto.

Definition: (epimorphism)

Let $f: G \to G'$ be a homomorphism.

(i) If f is onto, then it is called an epimorphism.

(ii) If f is 1-1, then it is called a monomorphism.

Note:

2) Consider the homomorphism

$f: (\mathbb{R}^*, \cdot) \to (\mathbb{R}^+, \cdot)$ which is given by

$f(x) = |x|$.

Let $K = \{x / x \in \mathbb{R}^*, f(x) = 1\}$.

clearly $K = \{1, -1\}$ which is a normal subgroup of $(\mathbb{R}^*, \cdot)$

Definition: [Kernal]

Let $f: G \to G'$ be a homomorphism. Let $K = \{x / x \in G, f(x) = e'\}$. Then K is called the kernal of f and denoted by $\ker f$.

Theorem: 3.56

Let $f: G \to G'$ be a homomorphism. Then the kernal K of f is a normal subgroup of G.

Proof:

Since $f(e) = e'$, $e \in K$ and hence $K \neq \phi$.

now, Let $x, y \in K$. Then $f(x) = e' = f(y)$.

$\therefore f(xy^{-1}) = f(x)\,f(y^{-1}) = f(x)\left[f(y)\right]^{-1} = e'(e')^{-1} = e'.$

Thus $xy^{-1} \in K$. Hence K is a subgroup of G.

Now let $x \in K$ and $a \in G$.

Then,

$$f(axa^{-1}) = f(a)\,f(x)\,f(a^{-1}).$$

$$= f(a)\,e'\left[f(a)\right]^{-1}.$$

$$= f(a)\left[f(a)\right]^{-1}.$$

$$= e'.$$

$axa^{-1} \in K$. Hence K is a normal subgroup of G.

Also $\{e'\}$ is a normal subgroup of $f(G)$.

Hence $\ker f = f^{-1}(\{e'\})$ is a normal subgroup of G.

Theorem: 3.57 (Fundamental theorem of homomorphism).

Let $f: G \to G'$ be an epimorphism. Let K be the kernel of f. Then $G/K \cong G'$.

Proof:

Define $\phi : G/K \to G'$ by $\phi(Ka) = f(a)$.

Step-1

$$\phi(kh) = f(kh) = f(k)f(h)$$

$$= e' f(h)$$

$$= f(h).$$

$$\therefore \phi(kh) = f(h) = f(m) = \phi(km).$$

Hence $\phi(km) = \phi(kh)$.

ϕ is 1-1.

for $\phi(km) = \phi(kh) \Rightarrow f(m) = f(h)$.

$$\Rightarrow f(m)[f(h)]^{-1} = e'.$$

$$\Rightarrow f(mh^{-1}) = e'.$$

$$\Rightarrow mh^{-1} \in K.$$

$$\Rightarrow m \in Kh.$$

$$\Rightarrow Km = Kh.$$

2020.12.11 14:24

Step-3

ϕ is onto.

Let $a' \in G'$.

Since f is onto, there exists $a \in G$ such that $f(a) = a'$.

Hence $\phi(Ka) = f(a) = a'$.

Step-4

ϕ is a homomorphism.

$$\phi(Ka\,Kb) = \phi(Kab) = f(ab) = f(a)\,f(b)$$

$$= \phi(Ka)\,\phi(Kb).$$

Thus ϕ is an isomorphism from G/K onto G'.

$\therefore G/K \cong G'$.

Solved problems:

problem:1

Let $f : G \to G'$ be a homomorphism. Then f is 1-1 iff $\ker f = \{e\}$.

Soln:

obviously f is 1-1 $\Rightarrow \ker f = \{e\}$.

Conversely let $\ker f = \{e\}$.

We prove f is 1-1.

$f(x) = f(y) \Rightarrow f(x)[f(y)]^{-1} = e'$.

$\Rightarrow f(xy^{-1}) = e'$

$\Rightarrow xy^{-1} \in \ker f$.

$\Rightarrow xy^{-1} = e$.

$\Rightarrow x = y$.

Hence f is 1-1.

Problem: 2

Let G be any group and H be the centre of G. Then $G/H \cong I(G)$. The group of inner automorphisms of G.

Soln:

Consider $f: G \to I(G)$ defined by $f(a) = \phi_a$.

Then $f(ab) = \phi_{ab} = \phi_a \circ \phi_b = f(a) f(b)$.

Hence f is a homomorphism.

clearly f is onto.

Now we claim that $\ker f = H$.

$a \in \ker f \Leftrightarrow f(a) = \phi_e$.

$\Leftrightarrow \phi_a = \phi_e$.

$\Leftrightarrow \phi_a(x) = x$ for all $x \in G$.

$\Leftrightarrow axa^{-1} = x$ for all $x \in G$.

$\Leftrightarrow ax = xa$ for all $x \in G$.

$\Leftrightarrow a \in H$.

Hence $\ker f = H$.

By the fundamental theorem of

2020.12.11 14:24

Problem: 3

Show that $R^*/\{1,-1\} \cong R^+$.

Soln:

Consider $f: R^* \to R^+$ defined by $f(x) = |x|$.

Clearly f is an epimorphism and $\ker f = \{1,-1\}$.

Hence by the Fundamental Theorem of Homomorphism $R^*/\{1,-1\} \cong R^+$.

Problem: 4

Any homomorphism image of a cyclic group is cyclic.

Soln:

Let G be a cyclic group and $f: G \to G'$ be an epimorphism.

Let a be a generator of G. Then $f(a)$ is a generator of G' (refer proof of theorem 3.48)

Hence G' is cyclic.

Problem: 5

Show that the map $f: (C,+) \to (R,+)$ defined by $f(x+iy) = y$ is an epimorphism

and $\ker f = R$. Prove that $\frac{C}{R} \cong R$.

Sol:

Let $z_1 = x_1 + iy_1$; and $z_2 = x_2 + iy_2$.

Then $z_1 + z_2 = (x_1 + x_2) + i(y_1 + y_2)$

$f(z_1 + z_2) = y_1 + y_2 = f(z_1) + f(z_2)$.

Hence f is a homomorphism clearly f is onto.

$\ker f = \{x+iy / f(x+iy) = 0\}$

$= \{x+iy / y = 0\}$

$= R$.

$\therefore$ By the fundamental theorem of homomorphism $C/R \cong R$.

Unit - IV

Definition: Rings

A non-empty set R together with two binary operations denoted by "+" and "$\cdot$" and called addition and multiplication which satisfy the following

A ring.

(i) $(R, +)$ is abelian group.

(ii) "$\cdot$" is an associative binary operation on R.

(iii) $a \cdot (b+c) = a \cdot b + a \cdot c$ and $(a+b) \cdot c = a \cdot c + b \cdot c$ for all $a, b, c \in R$.

Definition : zero - element :

The unique identity of the additive group $(R, +)$ is denoted by 0 and is called zero element of the ring. and the unique additive inverse of a is denoted by $-a$.

Definition : ring of Gaussian integers :

Let $R = \{a+ib / a, b \in \mathbb{Z}\}$. Then R is a ring under usual addition and multiplication. This ring is called the ring of Gaussian integers. In general, any subset of complex numbers which is a group under addition and is closed for multiplication is a ring (verify).

2020.12.11 14:23

Definition: null ring

$\{0\}$ with binary operations "+" and "." defined as $0+0=0$ and $0 \cdot 0 = 0$ in a ring. This is called the null ring.

Example:

(i) In $R \times R$ we define $(a,b)+(c,d) = (a+c, b+d)$ and $(a,b)\cdot(c,d) = (ac, bd)$. Here $(R \times R, +)$ is an abelian group. The identity is $(0,0)$ and the inverse of (a,b) is $(-a,-b)$.

Further $(a,b)\left[(c,d)+(e,f)\right]$

$= (a,b)(c+e, d+f)$

$= (ac+ae, bd+bf)$

$= (ae, bd)+(ae, bf)$

$= (a,c)(c,d)+(a,b)(e,f)$.

Similarly $\left[(a,b)+(c,d)\right](e,f)$.

$= (a,b)(e,f)+(c,d)(e,f)$

Hence $(R \times R, +, \cdot)$ is a ring.

Definition : Zero ring

Let $(R, +)$ be any abelian group with identity 0.

We define multiplication in R by $ab = 0$ for all $a, b \in R$. Clearly $a(bc) = 0 = (ab)c$. so that multiplication is associative.

Also $a(b+c) = 0 = ab + ac$ and

$$(a+b)c = 0 = ac + bc.$$

Hence R is a ring under these operations. This ring is called the zero ring

This example shows that any abelian group with identity 0 can be made into a ring by defining $ab = 0$.

(iii) $(Z_n, \oplus, \odot)$ is a ring. For we know that $(Z_n, \oplus)$ is an abelian group and $\odot$ is an associative binary operation.

We now prove the distributive Laws.

Let $a, b, c \in Z_n$.

Then $b \oplus c = (b+c) \pmod n$.

Hence $a \odot (b \oplus c) \equiv a(b+c) \pmod n$.

Also $a \odot b \equiv ab \pmod n$ and

$a \odot c \equiv ac \pmod n$ so that

$[a \odot b] \oplus (a \odot b) \equiv [ab + ac] \pmod n$.

Since $a \odot (b \oplus c)$ and $(a \odot b) \oplus [a \odot c] \in Z_n$.

we have $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$

Similarly $(a \oplus b) \odot c = (a \odot c) \oplus (b \odot c)$

Hence $(Z_n, \oplus, \odot)$ is a ring.

(iv) Let A be any abelian group. Let $\mathrm{Hom}(A)$ be the set of all endomorphism of A.

Let $f, g \in \mathrm{Hom}(A)$, we define,

$f+g$ by $(f+g)(x) = f(x) + g(x)$ and

$fg = f \circ g$. Then $\mathrm{Hom}(A)$ is a ring.

Proof:

Let $f, g \in \mathrm{Hom}(A)$

Then $(f+g)(x+y)$

2020.12.11 14:22

$= f(x+y) + g(x+y)$

$= f(x) + f(y) + g(x) + g(y).$

$= f(x) + g(x) + f(y) + g(y).$

$= (f+g)(x) + (f+g)(y).$

Hence $f+g \in Hom(A)$.

obviously $+$ is associative.

Since A is an abelian group $f+g = g+f$.

If 0 is the identity element of the group A then the homomorphism o defined by $o(a) = 0$. for all $a \in A$ is the zero element of $Hom(A)$.

Now, let $f \in Hom(A)$. the function f defined by $(-f)(x) = -[f(x)]$ is also a homomorphism

Since,

$-f(x+y) = -[f(x+y)]$

$= -[f(x) + f(y)]$

$= (-f(x)) + (-f(y)).$

clearly $f + (-f) = 0$. and hence $-f$ is

Thus Hom(A) is an abelian group.

Now, $(f \circ g)(x+y)$

$= f[g(x+y)]$

$= f[g(x) + g(y)]$

$= f[g(x)] + f[g(y)]$.

$= (f \circ g)(x) + (f \circ g)(y)$.

Hence $f \circ g \in \text{Hom}(A)$.

Similarly $(f+g) \circ h = f \circ h + g \circ h$

Thus Hom(A) is a ring.

(V) The set R of all matrices of the form $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ where $a, b \in R$ is a ring under matrix addition and matrix multiplication.

Proof:

Let $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ and $B = \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \in R$.

Then

$A + B = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix}$

2020.12.11 14:22

$$= \begin{pmatrix} a+c & b+d \\ -(b+d) & a+c \end{pmatrix} \in R.$$

$$AB = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c & d \\ -d & c \end{pmatrix}$$

$$= \begin{pmatrix} ac - bd & ad+bc \\ -(ad+ac) & ac-bd \end{pmatrix} \in R.$$

clearly matrix addition is commutative and associative.

$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in R$ is the zero element.

$\begin{pmatrix} -a & -b \\ b & -a \end{pmatrix}$ is the inverse of matrix.

$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$

Further matrix multiplication is assoc and the distribute Laws are valid for 2×2 mat

Hence R is a ring.

Elementary properties of ring:-

Theorem: 4.1

Let R be a ring and $a, b \in R$. Then

(i) $0a = a0 = 0$ (ii) $a(-b) = (-a)b = -(ab)$.

(iii) $(-a)(-b) = ab$ (iv) $a(b-c) = ab - ac$

Proof:

(i) $a0 = a(0+0) = a0 + a0$.

$\therefore a0 = 0$ [by cancellation law in $(R,+)$].

Similarly $0a = 0$.

(ii) $a(-b) + ab = a(-b+b) = a0 = 0$.

$a(-b) = -(ab)$.

Similarly, $(-a)b = -(ab)$.

(iii) By (ii), $(-a)(-b) = -[a(-b)] = -(-ab)$

$= ab$.

(iv) $a(b-c) = a[b+(-c)] = ab + a(-c)$

$= ab - ac$.

Solved Problems:

Problem :1

If R is a ring such that $a^2 = a$ for all $a \in R$, prove that (i) $a+a = 0$. (ii) $a+b = 0 \Rightarrow a = b$.

(ii) $ab = ba$.

Soln:

$$a+a = (a+a)(a+a)$$

$$= a(a+a)+a(a+a).$$

$$= aa+aa+aa+aa$$

$$= (a+a)+(a+a) \quad (\text{since } a^2 = a).$$

Hence $a+a = 0$.

(i) Let $a+b = 0$ By (i) $a+a = 0$

$\therefore a+b = a+a$.

so that $a = b$.

(iii) $a+b = (a+b)(a+b)$

$= a(a+b)+b(a+b)$

$= aa+ab+ba+bb$

$= a+ab+ba+b$.

Hence $ab+ba = 0$. so that by (ii) $ab = ba$.

Definition: Boolean Ring

A Ring R is called a Boolean ring if $a^2 = a$ for all $a \in R$. For example

$(P(S), \Delta, \cap)$ is a Boolean ring.

Problem: 2

Complete the cayley table for the ring $R = \{a, b, c, d\}$.

+	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

·	a	b	c	d
a	a	a	a	a
b	a	b		
c	a			a
d	a	b	c	

Soln:

First we shall compute cb.

$cb = (b+d)b$ (From addition table)

$= bb + db.$

$= b+b$ [From multiplication table].

$= a$ (From addition table).

Now,

$cc = c(b+d) = cb + cd = a + a = 0.$

$bc = (b+d)c = cc + dc =$

$bd = b(b+c) = bb+bc = b+c = d.$

$dd = (b+c)d = bd+cd = d+a = d.$

Hence the completed table for multiplication in

.	a	b	c	d
a	a	a	a	a
b	a	b	c	d
c	a	a	a	a
d	a	b	c	d.

Definition: Isomorphism

Let $(R,+,\cdot)$ and $(R',+,\cdot)$ be two rings. A bijection $f: R \to R'$ is called an isomorphism if

i) $f(a+b) = f(a) + f(b)$ and

ii) $f(ab) = f(a)\,f(b)$ for all $a, b \in R$.

If $f: R \to R'$ is an isomorphism we say that R is isomorphic to R' and we write $R \cong R'$.

Example:

i) $f: C \to C$ defined by $f(z) = \bar{z}$ is an isomorphism for, clearly f is a bijection.

$$f(z_1+z_2) = \overline{z_1+z_2} = \bar{z}_1 + \bar{z}_2.$$

$$= f(z_1) + f(z_2) \text{ and}$$

$$f(z_1 \cdot z_2) = \overline{z_1 z_2} = \bar{z}_1 \bar{z}_2 = f(z_1) f(z_2).$$

(ii) the groups $(\mathbb{Z}, +)$ and $(2\mathbb{Z}, +)$ are isomorphic under the map $f: \mathbb{Z} \to 2\mathbb{Z}$, given by $f(x) = 2x$.

However f is not an isomorphism of the ring $(\mathbb{Z}, +, \cdot)$ to $(2\mathbb{Z}, +, \cdot)$. since $f(xy) = 2xy$ and $f(x) f(y) = 2x \cdot 2y = 4xy$. so that $f(xy) \neq f(x) f(y)$

In fact there is no isomorphism between the rings $(\mathbb{Z}, +, \cdot)$ and $(2\mathbb{Z}, +, \cdot)$ (verify).

Types of rings:

Definition: Commutative

A Ring R is said to be commutative if $ab = ba$. for all $a, b \in R$.

Example:

(i) The familiar rings $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ are all commutative the following are examples of non commutative rings.

(iii) Let F denote the set of all functions from $R \to R$. We define $(f+g)(x) = f(x)+g(x)$ and $f \cdot g = f \circ g$. Then $(F, +, \cdot)$ is non-commutative ring.

(iii) The ring of quaternions given in example 13 of 4.1 is non commutative ring since $ij = k$ and $ji = -k$. (iv) $M_2(R)$ is non commutative ring.

Definition: ring with identity:

Let R be a ring. We say that R is a ring with identity if there exists an element $1 \in R$ such $a1 = 1a = a$ for all $a \in R$.

Theorem: 4.2

In a ring with identity the identity element is unique.

Proof:

Let $1, 1'$ be multiplicative identities.

Then $1 \cdot 1' = 1$ (considering $1'$ as identity)

and $1 \cdot 1' = 1'$ (considering 1 as identity).

$1 = 1'$. Hence the identity element in unique.

2020.12.11 14:20

Definition: unit

Let R be a ring with identity. An element $u \in R$ is called a unit in R if it has a multiplicative inverse in R. The multiplicative inverse of u is denoted by u^{-1}.

For example:

In $(\mathbb{Z}, +, \cdot)$, 1 and -1 are units. In $M_2(\mathbb{R})$, all the non-singular matrices are units. In $\mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ every non-zero elements is a unit.

Theorem: 4.3

Let R be a ring with identity. The set all units in R is a group under multiplication.

Proof:

Let U denote the set of all units in R.

Clearly $1 \in U$. Let $a, b \in U$.

Hence a^{-1}, b^{-1} exists in R.

Now $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = a1a^{-1}$.

$= aa^{-1}$

$= 1$.

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

Hence $ab \in U$.

2020.12.11 14:20

$(a^{-1})^{-1} = a$ and hence $a \in U \Rightarrow a^{-1} \in U$.

Hence U is a group under multiplication.

Definition: skew field (or) division ring

Let R be a ring with identity element. R is called a skew field or a division ring if every non-zero element in R is a unit.

(i.e) for every non-zero element $a \in R$.

there exists a multiplicative inverse $a^{-1} \in R$ such that $aa^{-1} = a^{-1}a = 1$.

Thus in a skew field the non-zero elements form a group under multiplication

Definition: Field

A commutative skew field is called a field. In other words a field is a system $(F, +, \cdot)$ satisfying the following conditions.

(i) $(F, +)$ is an abelian group.

(ii) $(F - \{0\}, \cdot)$ is an abelian group.

(iii) $a \cdot (b+c) = a \cdot b + a \cdot c$ for all $a, b, c \in F$

2020.12.11 14:20

Examples:

(i) $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are fields under usual addition and multiplication.

(ii) Let M be the set of all matrices of the form $\begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}$ where $a, b, \in$

Then M is a skew field under matrix addition and matrix multiplication.

Proof:

Let $A, B \in M$.

Let $A = \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}$ and $B = \begin{pmatrix} c & d \\ -\bar{d} & \bar{c} \end{pmatrix}$

Then

$$A+B = \begin{pmatrix} a+b & b+d \\ -\bar{b}+\bar{d} & \bar{a}+\bar{c} \end{pmatrix}$$

$$= \begin{pmatrix} a+c & b+d \\ -\overline{(b+d)} & \overline{a+c} \end{pmatrix} \in M.$$

Hence M is closed under matrix addition obviously matrix addition is associative and commutative. $(0, 0)$ is the

$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ is the zero element of M.

$\begin{pmatrix} -a & -b \\ \bar{b} & -\bar{a} \end{pmatrix}$ is the additive inverse of $\begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}$

Hence M is an abelian group under matrix addition ✓

Now,

$$AB = \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \begin{pmatrix} c & d \\ -\bar{d} & \bar{c} \end{pmatrix}$$

$$= \begin{pmatrix} ac - b\bar{d} & ad + b\bar{c} \\ -b\bar{c} - \bar{a}\bar{d} & -\bar{b}d + a\bar{c} \end{pmatrix}$$

Which is of form $\begin{pmatrix} z & w \\ -\bar{w} & \bar{z} \end{pmatrix}$.

Hence M is closed under matrix multiplication

further matrix multiplication is associative.

and $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in M$ is the multiplicative identity.

Now, Let $A = \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}$ be a non-zero matrix in M.

then either $a \neq 0$ or $b \neq 0$ so that either

$|a| > 0$ or $|b| > 0$

2020.12.11 14:20

Hence $|A| = a\bar{a} + b\bar{b}\,b\bar{b}$

$= |a^2| + |b^2| > 0.$

Thus A is a non-singular matrix and hence has an inverse and $\bar{A}^{-1} \in M$. Thus M is a skew field. Also since matrix multiplication is not commutative, M is not a field.

Theorem: 4.4 :

In a skew field R

(i) $ax = ay \;\; : a \neq 0 \Rightarrow x = y$

(ii) $xa = ya, \;\; a \neq 0 \Rightarrow a = y$

} (cancellation laws in

(iii) $ax = 0 \Leftrightarrow a = 0$ (or) $x = 0$

Proof:

(i) Let $ax = ay$ and $a \neq 0$

since R is a skew field there exists

$\bar{a}^1 \in R$ such that $a\bar{a}^1 = \bar{a}^1 a = 1.$

Hence $ax = ay \Rightarrow \bar{a}^1(ax) = \bar{a}^1(ay)$

$\Rightarrow x = y.$

(ii) can be proved similarly

(iii) If $a = 0$ (or) $x = 0$. then clearly $ax = 0$.

Conversely Let $x = 0$ and $a \neq 0$.

$\therefore ax = a0$

$x = 0$ (by (i))

Definition: zero divisor

Let R be a ring. A non-zero element $a \in R$ is said to be a zero divisor if there exists a non-zero element $b \in R$ such that $ab = 0$ (or) $ba = 0$.

Example:

In the ring Z_{12}, 3 is a zero divisor since $3 \odot 4 = 0$. Also 2, 4, 6 are zero divisors.

theorem: 4.5

A ring R has no zero-divisors iff Cancellation law is valid in R.

Proof:

Let R be a ring without zero-divisors

Let $ax = ay$ and $a \neq 0$.

$\therefore ax - ay = 0$. Hence $a(x-y) = 0$ and $a \neq 0$

$\therefore x - y = 0$ [since R has no zero divisors]

$\therefore x = y$. Then cancellation law is valid in R.

Conversely Let the cancellation Law be valid in R.

Let $ab = 0$ and $a \neq 0$. Then $ab = 0 = a0$.

Hence by cancellation Law $b = 0$.

Hence R has no zero-divisors.

Theorem: 4.6

Any unit in R cannot be a zero-divisor.

Proof:

Let $a \in R$. be a unit

Then $ab = 0 \Rightarrow a^{-1}(ab) = 0 \Rightarrow b = 0$.

similarly $ba = 0 \Rightarrow b = 0$.

Hence a cannot be a zero divisor.

Note:

The converse of the above result is not true. (ie) a is not a zero-divisor [illegible]

imply a is a unit.

For example:

In $\mathbb{Z}$, 2 is not a zero-divisor and 2 is not a unit.

Definition: integral domain

A commutative ring with identity having no zero-divisors is called in integral domain.

Thus in an integral domain $ab = 0 \Rightarrow$ either $a = 0$ (or) $b = 0$.

or equivalently $ab = 0$ and $a \neq 0 \Rightarrow b$

or $a \neq 0$ and $b \neq 0 \Rightarrow ab \neq 0$.

Example:

(i) $\mathbb{Z}$ is an integral domain.

(ii) $\mathbb{Z}_7$ is an integral domain.

Theorem: 4.7

$\mathbb{Z}_n$ is an integral domain iff n is prime.

Other proof:

Let Z_n be an integral domain.

We claim that n is prime. Suppose is not prime.

Then $n = pq$ where $1 < p < n$ and $1 < q < n$.

clearly $p \odot q = 0$.

Hence p and q are zero-divisors.

$\therefore Z_n$ is not an integral domain which is a contradiction.

Hence n is prime.

Conversely suppose n is prime.

Let $a, b \in Z_n$.

Then $a \odot b = 0 \Rightarrow ab = qn$. where $q \in Z_n$.

$\Rightarrow n / ab$

$\Rightarrow n/a$ or n/b (since n is prime)

$\Rightarrow a = 0$ or $b = 0$.

$\therefore Z_n$ has no zero-divisors.

Also Z_n is a commutative ring with identity.

2020.12.11 14:19

Hence Z_n is an integral domain.

Theorem: 4.8

Any field F is an integral domain

Proof:

It is enough if we prove that F has no zero-divisors.

Let $a, b \in F$, $ab = 0$ and $a \neq 0$.

Since F is a field a^{-1} exists

Now $ab = 0 \Rightarrow a^{-1}(ab) = 0$

$\Rightarrow b = 0$.

$\therefore$ F has no zero-divisors.

Hence F is an integral domain. Test.

Note:

The converse of the above theorem is not true. (ie) An integral domain need not be a field.

For example Z is an integral domain but not a field.

theorem: 4.9

Let R be a commutative ring with identity 1. Then R is an integral domain iff the set of non-zero elements in R is closed under multiplication

proof:

Let R be an integral domain.

Let $a, b \in R - \{0\}$.

Since R has no zero-divisors $ab \neq 0$.

So that $R - \{0\}$ is closed under multiplication

Conversely, suppose $R - \{0\}$ is closed under multiplication Then the product of any two non-zero elements is a non-zero element.

Hence R has no zero-divisors so that R is an integral domain.

Theorem: 4.10

Let R be a commutative ring with identity then R is an integral domain iff cancellation law is valid in R

Proof:

The result is an commutative consequence of Theorem 4.5.

Theorem: 4.11

Any finite integral domain is a field.

Proof:

Let R be a finite integral domain.

We need only to prove that every non-zero element in R has a multiplicative inverse.

Let $a \in R$ and $a \neq 0$.

Let $R = \{0, 1, a, a_2, \ldots a_n\}$.

Consider $\{a1, aa_1, aa_2, \ldots aa_n\}$.

By theorem 4.9 all these elements are distinct by Theorem 4.10.

Hence $aa_i = 1$ for some $a_i \in R$.

Since R is commutative, $aa_i = a_i a = 1$.

So that $a_i = a^{-1}$.

Hence R is a field.

theorem 4.12

By theorem 4.7 Z_n is an integral domain iff n is prime.

Further Z_n is finite.

Z_n is a field iff n is prime.

proof

Further Z_n is finite. By theorem 4.7 Z_n is an integral domain iff n is prime.

Further Z_n is finite.

Hence the result follows from theorem 4.11

theorem 4.13

Any finite commutative ring R without zero-divisors is a field.

proof

If we prove that R has an identity element then R becomes a integral domain and hence by theorem 4.11. it is a field.

So we prove the existence of identity

Let $R = \{0, a, \ldots a_n\}$

Let $a \in R$ and $a \neq 0$.

Then the elements $aa_1, aa_2, \ldots aa_n$ are distinct and non-zero.

$\therefore aa_i = a$ for some i.

Since R is a commutative we have

$aa_i = a_i a = a$.

We now prove that a_i is the identity element of R.

Let $b \in R$. Then $b = aa_j$ for some j.

$a_i b = a_i(aa_j) = (a_i a)a_j = aa_j = b$.

Thus $a_i b = b a_i = b$.

Since $b \in R$ is arbitrary, a_i is the identity of R.

Hence the theorem //

Problem: 1

Prove that the set of all real numbers of the form $a + b\sqrt{2}$ where $a, b \in \mathbb{Q}$ is a field under the usual addition and multiplication of

$= mna^2$

$= nma^2.$

$= nama.$

$= yx.$

Hence R is a commutative ring.

Now, Let R be a ring with 7 elements.

Then $(R, +)$ is a group of order 7.

Hence $(R, +)$ is cyclic.

Hence R is commutative.

Problem:8

Let R and R' be rings and $f: R \to R'$ be an isomorphism. Then

(i) R is commutative $\Leftrightarrow$ R' is commutative

(ii) R is ring with identity $\Rightarrow$ R' is ring with identity.

(iii) R is an integral domain $\Rightarrow$ R' is an integral domain

(iv) R is a field $\Rightarrow$ R' is a field.

(i) Let $a', b' \in R'$. Since f is onto, there exists $a, b \in R$ such that $f(a) = a'$ and $f(b) = b'$. Now,

$$\begin{aligned} a'b' &= f(a)\,f(b) \\ &= f(ab) \quad (\text{since } f \text{ is an isomorphism}) \\ &= f(ba) \quad (\text{since } R \text{ is a commutative ring}) \\ &= f(b)\,f(a) \\ &= b'a'. \end{aligned}$$

$\therefore R'$ is a commutative ring.

(ii) Let $1 \in R$ be the identity element of R. Let $a' \in R'$. Then there exists $a \in R$ such that $f(a) = a'$.

Now,

$$\begin{aligned} f(1)\,a' &= f(1)\,f(a) = f(1a) \\ &= f(a) = a'. \end{aligned}$$

Similarly $a'f(1) = a'$ and hence $f(1)$ is the identity element in R'.

$\therefore R'$ is a ring with identity.

(iii) Let R be an integral domain. Then

by (i) and (ii), R' is a commutative ring.

with identity.

Now, we prove that R' has no zero

divisors.

Let $a'b' \in R'$ and Let $b' \neq 0$.

since f is onto there exists $a, b \in R$ such

that $f(a) = a'$ and $f(b) = b'$.

$\therefore a'b' = 0 \Rightarrow f(a) f(b) = 0.$

$\Rightarrow f(ab) = 0$

$\Rightarrow ab = 0$ (since f is 1-1).

$\Rightarrow a = 0$ (or) $b = 0$.

(since R is an

integral domain).

$\Rightarrow f(a) = 0$ (or) $f(b) = 0$.

$\Rightarrow a' = 0$ (or) $b' = 0$.

$\therefore e'$ is an integral domain.

(iv) We need to prove that every non-zero element in R' has an inverse. Let $a' \in R'$ and $a' \neq 0$.

Then there exists $a \in R - \{0\}$ such that $f(a) = a'$.

Now, $f(a^{-1}) = a' = f(a^{-1}) f(a)$

$= f(a^{-1}) a$

$= f(1)$.

Hence $f(a^{-1})$ is the inverse of a'.

Problem: 9

Prove that the only isomorphism $f: Q \to Q$ is the identity map.

Soln:

Since f is an isomorphism $f(0) = 0$ and $f(1) = 1$. Now, Let n be a positive Integer.

$f(n) = f(1 + 1 + \cdots + 1)$ (written n times)

$= f(1) + f(1) + \cdots f(1)$ (written n times).

$= 1 + 1 + 1 \cdots + 1$ (written n times)

$= n$.

Now, if n is a negative

Let $n = m$. where $m \in N$.

Then $f(n) = f(m) = -f(m) = -m = n$.

Thus for any integer n. $f(n) = n$.

Now Let $a \in Q$. Then $a = p/q$ where $p, q \in Z$.

Hence

$$f(a) = f(p/q) = f(pq^{-1}) = f(p) f(q^{-1})$$

$$f(p)[f(q)]^{-1} = pq^{-1} = p/q = a.$$

Hence f is the identity map.

characteristic of a ring:

Definition:

Let R be a ring. If there exists a positive integer n such that $na = 0$. for all $a \in R$. Then the least such positive integer is called the characteristic of the ring R. If no such positive integer exists then the ring is said to be of characteristic zero.

Example:

i) Z_6 is a ring of characteristic 6.

In general 2n is a ring of characteristic n.

Theorem: 4.14

Let R be a ring with identity 1. If 1 is an element of finite order in the group (R, +) then the order of 1 in the characteristic of R. If 1 is of infinite order, the characteristic of the ring is 0.

Proof:

Suppose the order of 1 is n. Then n is the least positive integer such that n.1 = 0.

(ie), 1+1+...1 (n times) = 0 Now, let a ∈ R.

Then na = a+a+...+a (n times)

= 1.a + 1.a + ... + 1.a

= (1+1...+1) a

= 0.a

= 0

Thus na = 0 for all a ∈ R.

Hence the characteristic of the ring is n.

If 1 is of finite order then

no positive integer. n such that $n \cdot 1 = 0$

Hence the characteristic of the ring is 0.

Theorem: 4.15

The characteristic of an integral domain D is either 0 or a prime number.

Proof:

If the characteristic of D is 0 then there is nothing to prove. If not be the characteristic of D be n.

If n is not prime. Let $n = pq$. Where $1 < p < n$ and $1 < q < n$

Since characteristic of D is n we have $n \cdot 1 = 0$.

Hence $n \cdot 1 = pq \cdot 1$

$= (p \cdot 1)(q \cdot 1)$

$= 0$.

Since p is an integral domain either

$p \cdot 1 = 0$ or $q \cdot 1 = 0$

Since p, q are both less than n, this contradicts the definition of the characteristic of D.

Hence n is a prime number.

Theorem: 4.16

In an integral domain D of characteristic p, the order of every element in the additive group is p

Proof:

Let $a \neq 0$ be any non-zero element.

Let the order of a be n. Then n is the least positive integer such that $na = 0$.

Now, by the definition of the characteristic of D. we have $pa = 0$.

Hence $n \mid p$. Now, since p is prime, $n = 1$ or $n = p$.

If $n = 1$, $na = a = 0$ which is a contradiction

Hence $n = p$. Thus the order of a is p.

Subring definition

A non-empty subset S of a ring $(R, +, \cdot)$ is called a subring if S itself is a ring under the same operation as in R.

Examples:

(i) $2\mathbb{Z}$ is a subgroup of $\mathbb{Z}$.

Theorem 4.17

A non-empty subset S of a ring R is a subring iff $a, b \in S \Rightarrow a - b \in S$ and $ab \in S$

Proof:

Let S be a subring of R.

Then $(S, +)$ is an subgroup of $(R, +)$.

Hence $a, b \in S \Rightarrow a - b \in S$.

Also since S itself is a ring $ab \in S$.

Conversely let S be a non-empty subset of R such that $a, b \in S \Rightarrow a - b \in S$ and $ab \in S$.

Then $(S, +)$ is a subgroup of $(R, +)$.

Also S is closed under multiplication.

Then associative and distributive

Laws in S are consequence of the corresponding laws in R.

Hence S is a subring.

Solved Problems:

problem: 1

Let X be any set and let F be the set of all finite subsets of X. Then F is a subring of $(\mathcal{P}(X), \Delta, \cap)$

soln:

Let $A, B \in F$. Then A and B are finite sets.

Hence $(A-B) \cup (B-A) = A \Delta B$ is a finite set so that $A \Delta B \in F$.

Similarly $A \cap B \in F$. Thus F is a subring.

Problem: 2

Let R be a ring with identity

Then $S = \{n \cdot 1 / n \in Z\}$ is a subring of R.

soln:

Let $a, b \in S$. Then $a = n \cdot 1$ and $b = m \cdot 1$ for some $n, m \in Z$.

Hence $a - b = n \cdot 1 - m \cdot 1 = (n-m) \cdot 1 \in S$.

$Z/ZP = \{PZ, PZ+1 \cdots PZ+(P-1)\}$. It is easy to see that the ring $\frac{Z}{PZ} \cong ZP$. Here Z is an integral domain that not a field where as Z/PZ is a field

UNIT - V

Maximal and prime ideals:

Definition : maximal ideal

Let R be a ring. An ideal $M \neq R$ is said to be a maximal ring. Ideal of R if whenever U is an ideal of R such that $M \subseteq U \subseteq R$. then either $U = M$ (or) $U = R$. That is no proper ideal of R property containing M.

Examples:

I. (2) is a maximal ideal in Z.

For Let, U be an ideal property. containing (2)

$\therefore$ U contains an odd integer say $2n+1$

$\therefore 1 = (2n+1) - 2n \in U$.

$\therefore U = Z$ (by theorem 4.20)

Thus there is no proper ideal of $\mathbb{Z}$

property containing (2).

Hence (2) is a maximal ideal of $\mathbb{Z}$.

Theorem: 4.24

Let R be a ~~containing~~ commutative ring with identity. An ideal M of R is maximal iff R/M is a field.

Proof: Part - I

Assume that: Let M be a maximal ideal in R.

Prove that: R/M is a field.

Since R is a commutative ring with identity and $M \neq R$, R/M is also a commutative ring with identity.

Now, Let $M+a$ be a non-zero element in R/M that $a \notin M$. We shall now prove that $M+a$ has multiplicative inverse in R/M.

Let $U = \{ ra + m / r \in R \text{ and } m \in N \}$.

We claim that U in an ideal of R.

$(r_1 a + m_1) - (r_2 a + m_2) = (r_1 - r_2)a + (m_1 - m_2) \in$

2020.12.11 14:15

Also. $r(r_1 a + m_1) = (rr_1)a + rm \in U$ [since $rm_1 \in M$].

$\therefore U$ is an ideal of R.

Now. Let $m \in N$. Then $m = 0a + m \in U$.

$\therefore M \neq U$.

$\therefore U$ is an ideal of R. property containing M. But M is a maximal of R.

$\therefore U = R$. Hence $1 \in U$.

$\therefore 1 = ba + m$ for some $b \in R$.

Now,

$$M+1 = M+ba+m = M+ba \quad [\text{since } m \in M)$$

$$= (M+b)(M+a).$$

Hence $M+b$ is the inverse of $M+a$.

thus every non-zero element of R/M has inverse.

Hence R/M is field.

Conversely,

part-(ii) Assume that Suppose R/M is a field.

prove that. Let M be a maximal ideal in R.

Let U be any ideal of R property containing.

$\therefore$ There exists an element

$\therefore M+a$ is a non-zero element of R/M.

Since R/M is a field $M+a$ has an inverse say $M+b$.

$\therefore (M+a)(M+b) = M+1$

$\therefore M+ab = M+1$.

$\because 1-ab \in M$

But $M \subseteq U$. Hence $1-ab \in U$.

Also $a \in U \Rightarrow ab \in U$.

$\therefore 1 = (1-ab) + ab \in U$. Thus $1 \in U$.

$U = R$. Thus there is no proper ideal of R.

Property containing M. Hence M is a maximal ideal in R.

Definition: prime ideal

Let R be a commutative ring. An ideal $P \neq R$ is called a prime ideal if $ab \in P \Rightarrow$ either $a \in P$ or $b \in P$.

Examples:

Let R be an integral domain. Then (0) is a prime ideal of R.

For, $ab \in (0) \Rightarrow ab = 0$.

$\Rightarrow a = 0$ (or) $b = 0$ (since R in an I.D)

$\Rightarrow a \in (0)$ (or) $b \in (0)$.

theorem: 9.25

Let R be any commutative ring with identity. Let p be an ideal of R. then p is a prime ideal $\Leftrightarrow$ R/p is an integral domain.

proof:

Let p be a prime ideal.

since R is a commutative ring with identity R/p is also commutative ring with identity.

Now, $(p+a)(p+b) = p+0$.

$\Rightarrow p + ab = p$. (Integral domain) $ab = 0$

$\Rightarrow ab \in p$

$\Rightarrow a \in p$ (or) $b \in p$ (since p is a prime ideal)

$\Rightarrow p+a = p$ (or) $p+b = p$.

Thus R/p is integral domain.

Conversely, suppose R/p is an integral domain.

We claim that p is a prime ideal

Let $ab \in P$. Then $P + ab = P$

$\therefore (P+a)(P+b) = P$.

$\therefore P+a = P$ (or) $P+b = P$. (since R/P has no zero divisors)

$\therefore a \in P$ or $b \in P$.

$\therefore P$ is a prime ideal of R.

Corollary:

Let R be a commutative ring with identity. Then every maximal ideal of R is a Prime ideal of R.

proof:

Let M be a maximal ideal of R.

$\therefore R/M$ is a field. (by theorem 4.24)

$\therefore R/M$ is an integral domain (by theorem 4.8)

$\therefore M$ is a prime ideal. (by theorem 4.25)

Homomorphism of rings:

Definition: homomorphism

Let R and R' be rings. A function

$f: R \to R'$ is called a homomorphism if

(i) $f(a+b) = fa + fb$ and

(ii) $f(ab) = f(a)f(b)$ for all $a, b \in R$.

monomorphism:

If f is 1-1, then f is called a monomorphism.

epimorphism:

If f is onto, then f is called an epimorphism.

endomorphism:

A homomorphism of a ring onto itself is called an endomorphism.

Examples:

1. Let R be any ring $f: R \times R \to R$ given by $f(x, y) = x$ is a ring homomorphism.

For,

$$f[(a, b) + (c, d)] = f(a+c, b+d) = a+c.$$

$$= f(a, b) + f(c, d).$$

Also

$$f[(a, b)(c, d)] = f(ac, bd) = ac.$$

2020.12.11 14:14

$= f(a,b)\, F(c,d)$.

Definition: Natural homomorphism

Let R be a ring and I be an ideal of R. Then $\phi : R \to R/I$. defined by $\phi(x) = I + x$. is a ring homomorphism ϕ is called the natural homomorphism.

$$\phi(x+y) = I + (x+y).$$

$$= (I+x) + (I+y).$$

$$= \phi(x) + \phi(y).$$

$$\phi(xy) = I + xy.$$

$$= (I+x)(I+y).$$

$$= \phi(x)\,\phi(y).$$

Hence ϕ is a ring homomorphism.

Theorem: 4.26

Let R and R' be rings and $f : R \to R'$ be a homomorphisms. Then

(i) $f(0) = 0'$.

(ii) $f(-a) = -f(a)$ for all $a \in R$.

(iii) If S is a subring of R, then $f(S)$ is a subring of R'. In particular $f(R)$ is a subring of R'.

(iv) If S is an ideal of R, Then $f(S)$ is an Ideal of $f(R)$.

(v) If S' is a subring of R' then $f^{-1}(S)$ is a subring of R.

(vi) If S' is an ideal of $f(R)$. then $f^{-1}(S')$ is an ideal of R.

(vii) If R is a ring with identity 1 and $f(1) \neq 0$ then $f(1) = 1'$ is the identity of $f(R)$.

(viii) If R is a commutative ring then $f(R)$ is also commutative.

Proof:

Since f is a homomorphism of the group $(R,+)$ to $(R',+)$ the results (i) and (ii) follow from theorem 3.55.

(iii) Since S is a subring of R, $(S,+)$ is a subgroup of $(R,+)$ and hence $f(S)$ is a subgroup of $(R',+)$.

Now Let $a', b' \in f(S)$.

Then $a' = f(a)$ and $b' = f(b)$ for some $a, b \in S$.

$\therefore a'b' = f(a) f(b) = f(ab) \in f(S)$.

Hence $f(S)$ is a subring of R'.

(iv) Let S be an ideal of R.

To prove that $f(S)$ is an ideal of $f(R)$ it is enough if we prove that $r' \in f(R)$ and

$a' \in f(S) \Rightarrow r'a'$ and $a'r' \in f(S)$.

Let $r' = f(r)$ and $a' = f(a)$ where $r \in R$.

and $a \in S$.

Now, since S is an ideal of R, ra and $ar \in S$.

Hence $f(ra) = f(r) f(a) = r'a' \in f(S)$.

Similarly $a'r' \in f(S)$.

Hence $f(S)$ is an ideal of $f(R)$.

(v) Let S' be a subring of R'. Since $(S', +)$ is a subgroup of $(R', +)$, $f^{-1}(S')$ is a subgroup of $(R, +)$.

Now, Let $a, b \in f^{-1}(S')$.

Then $f(a), f(b) \in S'$.

$\therefore f(ab) = f(a) f(b) \in S'$. (since S' is a subring of R')

$\therefore ab \in f^{-1}(S')$.

Hence $f^{-1}(S')$ is a subring of R.

(vi) Proof is similar to that of (v).

(vii) Let R be a ring with identity 1.

Let $a' \in f(R)$.

Then $a' = f(a)$ for some $a \in R$.

Now, $a' f(1) = f(a) f(1) = f(a1) = f(a) = a'$.

Similarly $f(1) a' = a'$. Also $f(1) \neq 0$.

Hence $f(1)$ is the identity of $f(R)$.

(viii) proof is left to the reader.

Definition: kernal

The kernal K of a homomorphism f of a ring R to a ring R' is defined by

$\{ a / a \in R \text{ and } f(a) = 0 \}$.

Theorem: 4.27

Let $f: R \to R'$ be a homomorphism.

Let K' be the kernal of f. Then $R/K \cong R'$.

Proof:

By definition $K = f^{-1}\{0\}$.

since $\{0\}$ as an ideal of $f(R)$. by (vi)

of theorem 4.26, K in an ideal of R.

Theorem: 4.28

Let R and R' be rings and $f: R \to R'$ be an epimorphism let K be the kernel of f.

Then $R/K \approx R'$

Proof:

Define $\phi: R/K \to R'$ by $\phi(K+a) = f(a)$.

i) ϕ is well defined, For let $K+b = K+a$

Then $b \in K+a$.

$\therefore b = k+a$ where $k \in K$.

$\therefore f(b) = f(k+a) = f(k) + f(a)$.

$= 0 + f(a) = f(a)$.

$\therefore \phi(K+b) = f(b) = f(a) = \phi(K+a)$.

(ii) ϕ in 1-1

For. $\phi(K+a) = \phi(K+b) \Rightarrow f(a) = f(b)$

$\Rightarrow f(a) - f(b) = 0$.

$\Rightarrow f(a) + f(-b) = 0$.

$\Rightarrow f(a-b) = 0$

$\Rightarrow a - b \in K.$

$\Rightarrow a \in K + b.$

$\Rightarrow K + a = K + b.$

(iii) ϕ is onto

For. Let $a' \in R'$.

Since f is onto, there exists $a \in R$ such that $f(a) = a'$.

Hence $\phi(K+a) = f(a) = a'$.

(iv) ϕ is homomorphism.

For.

$$\phi[(K+a)+(K+b)] = \phi[K+(a+b)].$$

$$= f(a+b).$$

$$= f(a) + f(b) \quad \text{(since f is a homomorphism)}.$$

$$= \phi(K+a) + \phi(K+b).$$

and $\phi[(K+a)(K+b)] = \phi[(K+ab)]$.

$$= f(ab)$$

$$= f(a) f(b) \quad \text{(since f is a homomorphism)}$$

$$= \phi(K+a)\phi(K+b).$$

Hence ϕ is an isomorphism.

Hence $R/k \cong R'$.

Solved problems:

Problem: 1

The homomorphism image of an integral domain need not be an integral domain.

Soln:

$f: Z \to Z_4$. defined by $f(a) = r$. Where $a = 4q+r$, $0 \leq r < 4$. is a homomorphism of Z onto Z_4.

Hence Here Z is an integral domain and Z_4 is not an integral domain since $2 \otimes 2 = 0$.

Problem: 2

Any homomorphism of a field to itself is either one-one or maps every element to 0.

soln:

Let F be a field. and $f: F \to F$ be a homomorphism. Let k be the kernal of F. Then k is an ideal of F. By theorem 4.21

$k = \{0\}$ or $k = F$.

If $K = \{0\}$. then f is 1-1.

If $K = F$. then $f(a) = 0$ for all $a \in F$.

Field of quotient of an integral domain:

state and prove embedded theorem

statement:

(i) Specify the elements of F.

(ii) Define addition and multiplication in F.

(iii) Show that F is a field under these operations.

(iv) D can be embedded in F.

stage (i)

Let D be an integral domain.

Let $S = \{(a,b) / a, b \in D \text{ and } b \neq 0\}$.

We are going to think of the ordered pair (a, b) as one representing a formal quotient a/b.

For example . $1+D = 2$, the pair $(1, 2)$ will eventual represent the fraction $1/2$.

Definition:

Two elements (a,b) and $(c,d) \in S$ are defined to be equivalent iff $ab = d($ [illegible] (c,b)

is equivalent to (c, d) we write $(a, b) \sim (c, d)$.

Lemma : 1

$\sim$ is an equivalence relation in S.

Proof:

Let $(a, b) \in S$.

$(a, b) \sim (a, b)$ since $ab = ba = ab$.

Hence $\sim$ is reflexive.

Now, $(a, b) \sim (c, d) \Rightarrow ad = bc$.

$\Rightarrow cb = da$

$\Rightarrow (c, d) \sim (a, b)$.

Hence $\sim$ is symmetric.

Now, Let $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$.

Now to prove that $(a, b) \sim (e, f)$ we must prove that $af = be$.

Case (i)

Let $c = 0$. Now $ad = bc$ and $cf = de$.

$\therefore ad = 0$ and $de = 0$

But $d \neq 0$. Hence $a = 0$ and $c = 0$.

$\therefore af = e = 0$.

2020.12.11 14:12

Case (ii)

Let $c \neq 0$.

we have $ad = bc$ and $cf = de$.

$\therefore adcf = bcde$

$\therefore af = be$ (by cancellation Law)

$\therefore \sim$ is transitive.

Hence $\sim$ is an equivalence relation on S.

Consider the equivalence class containing (a, b).

Let it denoted by a/b. Let $F = \{a/b \mid (a,b) \in S\}$.

Stage (ii)

Let $a/b, c/d \in F$. we now define

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \text{ and } \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Since D is an integral domain and $b, d \neq 0$ we have $bd \neq 0$.

$\therefore \frac{ad+bc}{bd}$ and $\frac{ac}{bd} \in F$.

Lemma : 2

Addition and multiplication defined above are well defined.

Proof:

Let $(a_1, b_1) \in a/b$ and $(c_1, d_1) \in c/d$.

$\therefore a_1 b = b_1 a$ and $c_1 d = d_1 c \longrightarrow (1)$.

$\therefore a_1 b d b_1 = b_1 a d d_1$ and $c_1 d b b_1 = d_1 c b b_1$.

$\therefore (a_1 d_1 + b_1 c_1) bd = (ad + bc) b_1 d_1$.

$$\therefore \frac{ad + bc}{bd} = \frac{a_1 b_1 + b_1 c_1}{b_1 d_1}$$

$$\therefore \frac{a}{b} + \frac{c}{d} = \frac{a_1}{b_1} + \frac{c_1}{d_1}$$

Multiplication is well defined.

Lemma : 3

Stage (iii)

F is a field with the addition and multiplication defined above.

Proof:

If can easily be verified that addition is commutative and associative.

$0/1$ is the zero of F and $-\frac{a}{b}$ is the additive inverse of a/b.

$\therefore (F, +)$ is an abelian group.

clearly multiplication is commutative and associative. $\frac{1}{1}$ is the identity of F.

If a/b is a non-zero element of F, then $a \neq 0$.

$\therefore b/a \in F$ and is the inverse of a/b.

Now, $\frac{a}{b}\left(\frac{c}{d} + \frac{e}{f}\right) = \frac{a}{b}\left(\frac{cf + de}{df}\right)$

$$= \frac{acf + ade}{bdf}$$

$$= \frac{acfb + adeb}{bd + fb}.$$

$$= \frac{ac}{bd} + \frac{ae}{bf}$$

$$= \frac{a}{b}\frac{c}{d} + \frac{a}{b}\frac{e}{f}.$$

Stage (iv)

The field F contains a subring R which is isomorphic to D.

Lemma: 4

The map $f: D \to F$. given by $f(a) = \frac{a}{1}$

Euclidean domain

Definition: Euclidean domain (or) Euclidean ring

Let R be a commutative ring without zero-divisors. R is called an Euclidean domain or an Euclidean ring if for every non-zero element $a \in R$ there is defined a non-negative integer $d(a)$ satisfying the following conditions.

(i) For any two non-zero elements $a, b \in R$. $d(a) \leq d(ab)$.

(ii) For any two non-zero elements $a, b \in R$ there exists $q, r \in R$ such that $a = qb + r$ where either $r = 0$ (or) $d(r) < d(b)$.

Examples:

1) $\mathbb{Z}$ is an Euclidean domain where $d(a) = |a|$.

Proof:

$d(ab) = |ab| = |a||b| \geq |a| = d(a)$.

Let a, b be two non-zero elements of $\mathbb{Z}$. Let q be the quotient and r be the remainder when a is divided by b.

Then $a = qb + r$ and $0 \leq r < |b|$.

Hence $\mathbb{Z}$ is an Euclidean domain.

2) Any field F is an Euclidean domain where $d(a) = 1$ for all $a \in F - \{0\}$.

Proof:

$d(a) = d(ab) = 1$ for all $a \in F - \{0\}$.

Hence $d(a) \leq d(ab)$.

Also, $a = (ab^{-1})b + 0$ so that $q = ab^{-1}$ and $r = 0$.

∴ condition (ii) is satisfied.

Hence F is an Euclidean domain.

3) The ring of Gaussian integers $R = \{a + bi \mid a, b \in \mathbb{Z}\}$ is an Euclidean domain where we define $d(a+ib) = a^2 + b^2$.

Proof:

Let $x = a + ib$ and $y = c + id$ be two non-zero elements in R. Then

$$d(xy) = d[(a+ib)(c+id)]$$

$= d[(ac-bd) + i(ad+bc)]$

$= (ac-bd)^2 + (ad+bc)^2$

$= (a^2+b^2)(c^2+d^2)$

$\geq a^2+b^2$

$= d(x)$

$\therefore d(xy) \geq d(x)$

Now, to prove condition (ii), let

$$\frac{a+bi}{c+di} = p+iq$$

Then $p = \frac{ac+bd}{c^2+d^2}$ and $q = \frac{bc-ad}{c^2+d^2}$ and

Hence $p, q \in \mathbb{Q}$

Now, Let $m, n \in \mathbb{Z}$ be such that

$|p-m| \leq \frac{1}{2}$ and $|q-n| \leq \frac{1}{2}$.

Let $p-m = \alpha$ and $q-n = \beta$ so that

$|\alpha| \leq \frac{1}{2}$ and $|\beta| \leq \frac{1}{2}$

Now,

$a+bi = (c+di)(p+qi)$

$= (c+di)[(\alpha+m)+(\beta+n)i]$

$= (c+di)(m+ni) + r$

where $r = (c+di)(\alpha+\beta i)$.

Now,

$a+bi$, $c+di$, $m+ni \in R$ and

hence $r \in R$.

If $r \neq 0$, then

$$d(r) = (c^2+d^2)(\alpha^2+\beta^2)$$

$$\leq (c^2+d^2)(1/4 + 1/4)$$

$$< c^2+d^2$$

$$= d(y).$$

$\therefore d(r) < d(y)$.

$\therefore R$ is an Euclidean domain.

Theorem: 4.36

Let R be an Euclidean domain and I be an ideal of R. Then there exists element $a \in I$ such that $I = aR$ ie) Every Ideal of an Euclidean domain is a principal ideal.

2020.12.11 14:10

If $I = \{0\}$. Then we take $a = 0$.

Hence we assume that $I \neq \{0\}$.

Let $a \in I$ be a non-zero element such that $d(a)$ is minimum.

[This is possible since d takes only non-negative Integer values].

Now, we claim that $I = aR$.

Let $x \in I$. Then there exists $q, r \in R$ such that $x = qa + r$ where $r = 0$ (or) $d(r) < d(a)$.

$\therefore$ Now, $a \in I \Rightarrow qa \in I$ (since I is an ideal)

Also $x \in I$.

Hence $r = x - qa \in I$

Now, Suppose $r \neq 0$. Then $d(r) < d(a)$

$\therefore r$ is an element of I such that $d(r) < d(a)$ which is a contradiction to the choice of a and hence $r = 0$.

$\therefore x = qa$ and hence $I = aR$.

Theorem 4.37 :

Any Euclidean domain R has an identity element.

Since R is an ideal of R, there exists $c \in R$ such that $R = cR$.

$\therefore$ Every element of R is a multiple of C.

In particular $c = ec$ for some $e \in R$.

Now, let $x \in R$. Then $x = cy$ for some $y \in R$.

$\therefore ex = e(cy) = (ec)y = cy = x$.

$\therefore$ e is the required identity element.

Theorem: 4.38

Any Euclidean domain R is a Principal ideal domain.

proof:

By definition of Euclidean domain

R is a commutative ring without zero divisors. By theorem 4.37 R has an identity element. Hence R is an integral domain. Also every ideal of R is a principal ideal. Hence R is a principal ideal domain.

Theorem : 4.39

Let R be an Euclidean domain. Let a and b be two non-zero elements of R. Then

(i) b is not a unit in R $\Rightarrow d(a) < d(ab)$

(ii) b is a unit in R $\Rightarrow d(a) = d(ab)$.

Proof:

(i) Suppose b is not a unit in R.

By definition of Euclidean domain there exists element $q, r \in R$ such that

$$a = q(ab) + r \longrightarrow (1).$$

where either $r = 0$ or $d(r) < d(ab)$

Now,

Suppose $r = 0$ then $a = q(ab)$.

$\therefore a - q(ab) = 0.$

$\therefore a(1 - qb) = 0.$

Now, R has no zero-divisors and $a \neq 0$.

$\therefore 1 - qb = 0$. Hence $qb = 1$.

$\therefore b$ is a unit R which is a contradi-ction.

$\therefore r \neq 0$. Hence $d(r) < d(ab) \longrightarrow (2)$.

Now,

$r = a(1 - qb)$ (by 1).

$\therefore d(r) = d\left[a(1 - bq)\right] \geq d(a) \longrightarrow (3)$

$\therefore d(a) \leq d(r) < d(ab)$ [by (2) and (3)].

$\therefore d(a) < d(ab)$.

(ii) Suppose b is a unit in R.

Now, $d(a) \leq d(ab)$.

Also $d(a) = d\left[(ab)b^{-1}\right] \geq d(ab)$.

$\therefore d(a) \geq d(ab)$.

$\therefore d(a) = d(ab)$.

Theorem: 4.40

Let a be a non-zero element of Euclidean domain in R. Then a is a unit in R iff $d(a) = d(1)$.

Proof:

Suppose a is a unit in R.

$d(a) = d(aa^{-1})$ (by theorem 4.9)

$= d(1)$.

Conversely: Let $d(a) = d(1)$.

suppose a is not a unit in R.

Then $d(a) > d(1)$ (by theorem 4.39)

$\therefore d(a) > d(1)$ which is a contradiction

$\therefore a$ is a unit.

Theorem: 4.41

Let a be a non-zero element of an Euclidean domain R. If $d(a) = 0$, then a is a unit in R.

Proof:

suppose a is a not a unit in R.

Then $d(1) < d(1a)$ (By theorem 4.39).

2020.12.11 14:09

$\therefore d(1) \leq d(a) = 0$.

Hence $d(1) < 0$ which is a contradiction since d takes only non-negative values.

Theorem: 4.42

Let R be an Euclidean domain. Then any two elements $a, b \in R$ have a g.c.d and it is of the form $ax + by$ where $x, y \in R$.

Proof:

Let $A = \{ ax + by \mid x, y \in R \}$.

We claim that A is an ideal of R.

Let $u, v \in A$. Then $u = ax_1 + by_1$ and

$v = ax_2 + by_2$.

$\therefore u - v = a(x_1 - x_2) + b(y_1 - y_2) \in A$.

Now, Let $c \in R$. Then

$uc = (ax_1 + by_1) + c$.

$= a(x_1 c) + b(y_1 c) \in A$.

A is an ideal of R.

2020.12.11 14:09

Now, since R is an Euclidean domain it is a principal ideal domain.

Hence A is a principal ideal of R.

Now, Let $d \in A$ be such that $A = (d)$.

$\therefore d = ra + sb$ where $r, s \in R$.

Now, $a = 1a + 0b \in A$. and $b = 0a + 1b \in A$.

$\therefore a = da_1$ and $b = db_1$ for some $a_1, b_1 \in R$.

$\therefore d/a$ and d/b.

Now, suppose $l \in R$ and l/a and l/b

Then $l/(ra + sb)$ so that l/d.

d is the required g.c.d of a and b

Definition: relatively prime

Two elements a and b of an Euclidean domain R are said to be relative prime if their g.c.d is unit in R.

Theorem: 4.43

Let R be an Euclidean domain. Let $a, b, c \in R$. Then a/bc and $(a, b) = 1 \Rightarrow a/c$.

Proof

Since $(a, b) = 1$, there exists $x, y \in R$ such that $ax + by = 1$.

$\therefore acx + bcy = c$.

Now, $a \mid acx$. Also $a \mid bc \Rightarrow a \mid bcy$.

$\therefore a \mid (acx + bcy)$. Hence $a \mid c$.

Theorem 4.44

Let p be a prime element in an Euclidean domain in R. Let $a, b \in R$. Then $p \mid ab \Rightarrow p \mid a$ (or) $p \mid b$.

Proof:

Suppose p does not divide a.

Then $(p, a) = 1$ (since p is prime).

$\therefore$ By Theorem 4.43 we have $p \mid b$.

Corollary:

Let p be a prime element in Euclidean domain R.

Let $a_1, a_2, \ldots, a_n \in R$.

then $p \mid a_1 \cdot a_2 \cdots a_n \Rightarrow p$ divides at least one a_i.

theorem: 4.45

Any Euclidean domain R is a U.F.D

Proof

First we shall prove that any element a in R. is either a unit or can be expressed as the product of a finite number of prime elements of R.

We prove this by induction on $d(a)$

If $d(a) = d(1)$ then a is a unit in R.

(by theorem 4.44)

Hence the assertion is true Now, we assume that the result is true for all $x \in R$ such that $d(x) < d(a)$ and prove that the result is true for a.

If a is a prime there is nothing to Prove.

If not, $a = bc$ where neither b or c is a unit in R.

$\therefore d(b) < d(a)$ and $d(c) < d(a)$.

(by theorem 4.29)

Now by Induction hypothesis b and c can be written as the product of a finite number of prime elements.

Hence a can be expressed as a product of a finite number of prime elements.

We show prove that uniqueness

Let $a = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$ .where p_i s and q_i s are prime elements of R.

$\therefore p_1 \mid q_1 q_2 \cdots q_s$.

$p_1 \mid q_i$ for some i without loss of

generality we assume that $p_1 \mid q_1$. since p_1 and q_1 are both prime elements of R, p_1 and q_1 must be associates.

$\therefore q_1 = u_1 p_1$ where u_1 is a unit in R.

$\therefore p_1 p_2 \cdots p_r = u_1 p_1 q_2 q_3 \cdots q_s$.

$\therefore p_2 p_3 \ldots p_r = u_1 q_2 q_3 \cdots q_s$.

Now, if $r < s$, repeating the above argument r times the left side becomes 1 and the right side contains a product of some prime elements which is impossible

Hence $r \geq s$.

similarly $s \geq r$ and hence $r = s$.

Further we have shown that every p_i is an associate of some q_j and conversely.

Hence the theorem.

Solved problems:

Problem: 1

Show that $1+i$ is a prime element in the ring R of Gaussian integers.

Soln:

Suppose $(a+bi) \mid (1+i)$

Then there exist an element $c+id \in R$. such that $(a+bi)(c+di) = 1+i$.

$\therefore d[(a+bi)(c+di)] = d(1+i)$.

$\therefore (a^2+b^2)(c^2+d^2) = 2$ and $a, b, c, d \in Z$.

$\therefore a^2+b^2 = 1$ (or) $c^2+d^2 = 1$.

$\therefore d(a+ib) = d(1)$ (or) $d(c+id) = d(1)$.

$\therefore$ Either $a+ib$ (or) $c+id$ is a unit in R (by theorem 4.40).

Hence $1+i$ is a prime element of R.

Problem: 2

Prove that 5 is not prime element in the ring K of Gaussian integers.

Soln:

$5 = (2+i)(2-i)$

and $d(2+i) = d(2-i) = 5 > d(1)$.

Hence neither $2+i$ nor $2-i$ is a unit in R.

Hence 5 is not a prime element of R.

problem: 3

Find the ring g.c.d of $16+7i$ and $10-5i$ in the ring K of Gaussian integers.

Soln:

Let $a = 16+7i$ and $b = 10-5i$