MATH305 (Theory of Rings And Fields) 15/01/2018

Course Outline

Structures of Integers

Preliminaries

Euclidean Algorithms and Greatest Common Divisor

Prime, Relative prime

Unique Factorization (Fundamental theorem of Arithmetic)

Rings

Quotient Rings & Fields

Modules

References

Course Book

Theory of Rings, Fields & Groups (Introduction of Abstract Algebra) by R.B.J.T Allenby & Edwards Arnold (1983).

STRUCTURES OF INTEGERS

Preliminaries

A set is any collection of well defined objects (elements)

The concept of set is fundamental to all branches of mathematics. Example of sets

$\mathbb{Z}$: set of integers, $\mathbb{N}$: set of Natural numbers

$\mathbb{Q}$: set of Rational numbers, $\mathbb{C}$: set of Complex numbers

$\mathbb{R}$: set of Real numbers.

MATH305 (Theory of Rings And Fields) 15/01/2018

Course Outline

1. Structures of Integers
2. Preliminaries
3. Euclidean Algorithms and Greatest Common Divisor
4. Prime, Relative Prime
5. Unique Factorization (Fundamental Theorem of Arith
6. Rings
7. Quotient Rings & Fields
8. Modules

References

1. Note Book
2. Theory of Rings, Fields & Groups (Introduction of Abstract Algebra) by R.B.J.T Allenby & Edwards Arnold (1993).

STRUCTURES OF INTEGERS

Preliminaries

- A set is any collection of well defined objects (elements)
- The concept of set is fundamental to all branches of mathematics. Example of sets
  - $\mathbb{Z}$: set of integers, $\mathbb{N}$: set of Natural numbers
  - $\mathbb{Q}$: set of Rational numbers, $\mathbb{C}$: set of Complex numbers
  - $\mathbb{R}$: set of Real numbers

$4-6 = 4+(-6)$ ✱

Integers are also called whole numbers (+ve or $\mathbb{Z}^-$ $\mathbb{Z}^+$
it is defined as $\mathbb{Z} = \{\ldots -3, -2, -1, 0, 1, 2, 3 \ldots\}$.
Addition and Multiplication are the Common binary operations
on the set of integers.

1.2 Properties of the two binary operation (+ & ×)

i) Closure property: $\forall a,b \in \mathbb{Z}$ $a+b \in \mathbb{Z}$ & $a.b \in \mathbb{Z}$

ii) Commutative: $\forall a,b \in \mathbb{Z}$, $a+b = b+a$ & $a.b = b.a$

iii) Existence of Identity: $\forall a \in \mathbb{Z}$ $\exists 0 \in \mathbb{Z}$ ∋ $a+0 = a$ & $\exists 1 \in \mathbb{Z}$ ∋ $a.1 = a$ $\forall a \in \mathbb{Z}$ {additive identity & Multiplicative identity}

iv) Difference of two integers: $a-b = a+(-b)$

1.3 Some Elementary Consequence of the properties

$\forall a,b,c \in \mathbb{Z}$ (i) If $a+b = a+c$ then $b=c$ } Cancellation
$a.b = a.c$ then $b=c$ } Law.

ii)* $a(b+c) = ab+ac$ Distributive Law

iii) $a.0 = 0$ $\forall a \in \mathbb{Z}$

iv) $a=b \Rightarrow -a = -b$

v)* $-(-a) = a$ (vi)* $-0 = 0$ (vii)* $-(a+b) = -a-b$

viii)* $(-a)(-b) = ab$ (ix) $ab = 0 \Rightarrow$ either $a=0$ or $b=0$

x)* $ab \neq 0 \Rightarrow$ ~~either~~ $a \neq 0$ and $b \neq 0$ Proof Exercise

xi) $a.0 = 0$

$a.0 = a.(0+0) = a.0 + a.0$

$a.0 + a.0 = a.0$ add $-a.0$ to both side

$a.0 + a.0 - a.0 = a.0 - a.0 \Rightarrow a.0 + 0 = 0$

$a.0 = 0$ ✓ proved.

Def: $a|b \Rightarrow \exists m \in \mathbb{Z} \ni b = am$ — ①

Again $b|c \Rightarrow \exists y \in \mathbb{Z} \ni c = by$ — ②

from ① & ② we have $c = (am)y = amy$

$c = a(my) \Rightarrow a|b$ ☐ 16/07/2012

1.4 DIVISIBILITY OF THE SET OF INTEGER

Given any two integers "a & b" we say "a" divides "b" written as $a|b$ if $\exists c \in \mathbb{Z} \ni b = ac$.

Otherwise, $a \nmid b$ (i.e a does not divides b). if a divide b, then 'a' is called the divisor or "a" is a factor of 'b' or b is a multiple of a eg. $2|12$, $3|9$ But $3 \nmid 11$, $7 \nmid 9$ etc.

For any $a \in \mathbb{Z}$, if $a \neq 0$ then $\pm 1 \& \pm a$ are improper divisors of a, other divisors are called proper divisors.

SOME ELEMENTARY PROPERTIES OF DIVISOR

i) if $a|b$ then either $b = 0$ or $|a| \leq |b|$.

ii) * $a|b \iff a|-b$ or $-a|b$, or $-a|-b$, or $|a||b|$.

$$|a| = \begin{cases} a & \text{if } a \geq 0 \\ -a & \text{if } a < 0 \end{cases}$$

iii) if $a|b$ and $b|c$ then $a|c$ ✓

iv) If $a|b$ and $b|a \Rightarrow a = \pm b$

v) if $a|b$ then $a|(b+c)$ iff $a|c$ ✓.

vi) $a|a$ reflexive (vii) $a|b$ and $a|c$ then $a|bc$ ✓

viii) if $a|b$ and $a|c$ $\exists$ $x, y \in \mathbb{Z} \ni a|(bx+cy)$

Proof exercise by using definition of divisibles

$a|b \Rightarrow b = am$ — ① & $a|c \Rightarrow c = an$ — ②

for ① & ② we have $bx = amx$ & $cy = any$ $\quad bx + cy = amx + any$

$bx + cy = a(mx + ny)$ $\quad \therefore a|bx+cy$ $\forall$ $am \in \mathbb{Z}$

1.5 DIVISION ALGORITHM (THEOREM)

If $a, b \in \mathbb{Z}$, $b \neq 0$ then $\exists$ unique q and $r \ni$ $a = bq + r$ where $0 \leq r < |b|$, b is called the dividend and r is the remainder.

Division algorithm is very important in Number Theory. Example: ① Given $20, 3 \in \mathbb{Z}$ Now, $20 = 3 \cdot 6 + 2$ where $q = 6$ & $r = 2$ $\therefore 2 < 3$

② $17, 4 \in \mathbb{Z}$, $17 = 4 \cdot 4 + 1$ $q = 4$ & $r = 1$ $1 < 4$

1.6 GREATEST COMMON DIVISOR (GCD) / (HCF)

Let $a, b \in \mathbb{Z}$ $\exists$ atleast one of a or $b \neq 0$. Then the gcd is a positive integer $d \ni$

i) $d \mid a$ and $d \mid b$

ii) $\exists c \in \mathbb{Z} \ni c \mid a$ and $c \mid b$ then $c \mid d$.

We write $d = (a, b)$

PROPERTIES OF GCD

Let $a, b \in \mathbb{Z}$ then

i) $(a, b) = (b, a)$

ii) if $d = (a, b)$, $d \geq 1$

iii) $(a, a) = a$

iv) $(a, b) = a \iff a \mid b$

v) $(a, 0) = |a|$

By extension $d = (a_1, a_2, a_3, \ldots, a_n)$. Also $d = (a, b)$ can be expressed as

from If $a|b$ & $a|c$ then $a|(b+c)$

$d = (a,b) = ax + by$, $x, y \in \mathbb{Z}$

every pairs $a, b \in \mathbb{Z}$ $\exists$ a unique d $\rightarrow d = ax+by$

is called Linear Combination of a & b

THEOREM 1.1 :: Let $a, b \in \mathbb{Z}$ & $b \neq 0$ and $a = bq + r$ $(0 \leq r < |b|)$ then $(a,b) = (b,r)$

Proof :: Suppose $d_1 = (a,b)$ and $d_2 = (b,r)$, we need to show that $d_1 = d_2$.

$(a,b) = d_1 \Rightarrow d_1 | a$ and $d_1 | b \Rightarrow d_1 | (a - bq)$ $q \in \mathbb{Z}$ from properties of divisors but $a = bq + r$

$\Rightarrow r = a - bq$ $\therefore d_1 | r$

But $d_1 | b$ and $d_1 | r \Rightarrow d_1 = (b,r)$.

Also $d_2 = (b,r)$ by defn $d_1 | d_2$ ---① Slow

Similarly $(b,r) = d_2$, we can also ~~write~~ $d_2 | d_1$ ---② from ① & ②

$\therefore d_1 = d_2$ ∎

20/01/2017

EUCLIDEAN ALGORITHM

By repeated use of division algorithm the gcd of any two or more integers can be obtained

Given any $a, b \in \mathbb{Z}$, where $q_1, q_2, \ldots, q_K \in \mathbb{Z}$ and $r_1, r_2, \ldots r_K \in \mathbb{Z}$, then

$a = bq_1 + r_1 \quad 0 \leq r_1 < b$ $\qquad r_{K-1} = r_K q_{K+1} + r_{K+1}$

$b = r_1 q_2 + r_2 \quad 0 \leq r_2 < r_1$ $\qquad 0 \leq r_{K+1} < r_K$

$r_1 = r_2 q_3 + r_3 \quad 0 \leq r_3 < r_2$

The process must terminate since $b > r_1 > \cdots$ and only finitely many integers lie between 0 and b.

If the process terminates at $(k-1)^{th}$ step i.e. $r_{k+1} = 0$ then we have $r_{k-1} = r_k q_{k+1} \Rightarrow r_{k+1} = (r_{k-1}, r_k) \Rightarrow r_k / r_{k-1}$

Consequences, we have

$(a,b) = (b,r_1) = (r_1, r_2) = (r_2, r_3) = \cdots = r_k$

Hence $r_k = (a,b)$.

Example 1) By prime factorization we can find the gcd of 21 and 27

Sol $27 = 3 \times 3 \times 3 \Rightarrow (21, 27) = 3$

$21 = 3 \times 7$

2) By prime factorization, find the gcd of (24356, 734) Not easy as the numbers?

* The gcd of $a, b \in \mathbb{Z}$ can be obtained by prime factorization but not easy when a & b are very large numbers.

Euclidean algorithm is first computational proof for calculating gcd of any two integers.

3) find the gcd of (1785, 546)

Sol $1785 = 3 \cdot (546) + 147$

$546 = 3 \cdot (147) + 105$

$441 = 2(105) + 42$

The (erst non-zero remainder is the gcd

sol) $1785 = (3)(546) + 147$

$546 = (3)(147) + 105$

$147 = (1)(105) + 42$

$105 = (2)(42) + 21$ Then $(1785, 546) = 21$

$42 = 21(2) + 0$

This process can be presented linear

4) find the gcd of (26, 118)

$118 = 26(4) + 14$

$26 = 14(1) + 12$ $(26, 118) = 2$

$14 = 12(1) + 2$

$12 = 2(6) + 0$

5) (888, 54)

$888 = 54(16) + 24$

$54 = 24(2) + 6$

$24 = 6(4) + 0$

Then $(888, 54) = 6$

Exercise 1 : find the gcd of the following

i) (238, 23) (ii) (4472, 312)

iii) (22, 447) (iv) (3418, 910)

EXTENDED EUCLIDEAN ALGORITHM

If $d = (a, b) \Rightarrow d = ax + by$ for $x, y \in \mathbb{Z}$ To find x & y we use extended euclidean. Extended euclidean algorithm is the

process of using method of backward substitution to obtained the linear combination of gcd

example: find the (65, 40) and express it in the form $d = 65x + 40y \quad \forall x, y \in \mathbb{Z}$

Sol (65, 40) $\qquad 5 = 65x + 40y$

$65 = 40(1) + 25 \quad 25 = 65 - 40(1)$

$40 = 25(1) + 15 \quad 15 = 40 - 25(1)$

$25 = 15(1) + 10 \quad 10 = 25 - 15(1)$

$15 = 10(1) + 5 \quad (65, 40) = 5$

$10 = 5(2) + 0$

Now, $5 = 15 - 10(1)$

$= 15 - [25 - 15(1)] = 15 - 25 + 15(1) = 15(2) - 25$

$= (2)[40 - 25(1)] - 25 = 40(2) - 25(2) - 25$

$= 40(2) - 25(3)$

$= 40(2) - [65 - 40(1)](3) = 40(2) - 65(3) + 40(3)$

$= 40(5) - 65(3)$

$5 = -65(3) + 40(5) = 65(-3) + 40(5)$

$d = 65x + 40y \Rightarrow x = -3 \text{ & } y = 5$ //

Exercise

2) find the gcd of $(138, 63) = (a, b)$ and express it the form of $d = ax + by$

Sol

$138 = 63(2) + 12$ $\quad 12 = 138 - 63(2)$

$63 = 12(5) + 3$ $\quad 3 = 63 - 12(5)$

$12 = 3(4) + 0$

Now, $3 = 63 - 12(5)$

$= 63 - [138 - 63(2)](5)$

$= 63 - 138(5) + 63(10)$

$= 63(11) - 135(5)$

$3 = 135(-5) + 63(11)$ ~~etc~~ $x = -5$ & $y = 11$

Exercise 2:- find integers x & y ~~?~~ (i) $15 = 21x + 15y$

ii) $10 = 165x + 17y$ (iii) $5 = 108x - 20y$

2) If $a = -1387$, $b = 510$ write $(a,b) = ax + by$

3) If $d = 308x + 136y$ find x & y and d

RELATIVELY PRIME INTEGERS 23/01/2018

Two integers a & b are said to be relatively prime if their gcd is One (1). [i.e $(a,b) = 1$]

Eg $(3,11) = 1$, $(2,21) = 1$

Theorem 1.2 :- Two a & b are relatively prime iff $\exists\ x, y \in \mathbb{Z}$? $ax + by = 1$

Proof :- Suppose a & b are relatively prime then $(a,b) = 1$. Hence, we have $ax + by = 1$ for some $x, y \in \mathbb{Z}$.

Suppose $ax + by = 1$ for $x, y \in \mathbb{Z}$, we need to show that $(a,b) = 1$:

Again, let $(a,b) = d \Rightarrow d/a \nmid d/b \Rightarrow d/ax+by$ for

$\Rightarrow d/1 \quad x, y \in \mathbb{Z}$

$\Rightarrow d = \pm 1$ but gcd is always positive

$\therefore d = 1$ □.

Theorem 1.3: If $(a,b) = 1$ and $(a,c) = 1$ then $(a, bc) = 1$

Proof: Given $(a,b) = 1 \Rightarrow \exists\, x_1, y_1 \in \mathbb{Z}$ such that

$ax_1 + by_1 = 1, \quad by_1 = 1 - ax_1 \quad \cdots (1)$

Similarly, $(a,c) = 1 \Rightarrow \exists\, x_2, y_2 \in \mathbb{Z}$ such that

$ax_2 + cy_2 = 1 \Rightarrow cy_2 = 1 - ax_2 \quad \cdots (2)$

Multiply (1) & (2) together, we have,

$(by_1)(cy_2) = (1 - ax_1)(1 - ax_2)$

$bcy_1y_2 = 1 - ax_2 - ax_1 + a^2x_1x_2$

$a(x_2 + x_1 - ax_1x_2) + bcy_1y_2 = 1$

$a[x_2 + x_1 - ax_1x_2] + bcy_1y_2 = 1$

$\therefore (a, bc) = 1$ where $x_1, x_2, y_2, y_1 \in \mathbb{Z}$

Let $x_3 = x_2 + x_1 - ax_1x_2$ & $y_1y_2 = y_3$

$ax_3 + bcy_3 = 1$

$\therefore (a, bc) = 1 \quad x_3, y_3 \in \mathbb{Z}$ □

Theorem 1.4: If two integers a & b are relatively prime that is $(a,b) = 1$, then $a/bc \Rightarrow a/c$

Proof: Suppose $(a,b) = 1 \Rightarrow ax + by = 1$

$\exists\, c \in \mathbb{Z}$ such that $cax + cby = c \quad \cdots (1)$

Also, given that $a/bc \Rightarrow bc = qa, q \in \mathbb{Z}$

In (i), $ca x + cay = c \Rightarrow c = a(cx + cy)$

$c = aq_1$ where $q_1 = cx + cy \in \mathbb{Z}$

$\Rightarrow a/c$ □

LEAST COMMON MULTIPLE (LCM)

Let $a, b \in \mathbb{Z}$, the lcm of a and b is the unique positive integer m s.t (i) a/m & b/m

(ii) if a/s and $b/s \Rightarrow m/s$

We write $m = [a, b]$.

Example: $[3, 7] = 21$

PROPERTIES OF LEAST COMMON MULTIPLE

i) $[a, b] = [-a, b] = [a, -b] = [-a, -b] = [|a|, |b|]$

ii) if $(a, b) = d$ and $[a, b] = m$, then $dm = |ab|$

iii) if $(a, b) = d$ and $[a, b] = m$, then d/m

PRIMES AND COMPOSITE INTEGER

A non-zero integer p is called a prime if it is less than 1 and its only divisors are 1 or -1 and itself.

* A non-zero integer p is called a prime if it is neither 1 or -1 and its only divisors are $1, -1, p$ and $-p$

Example: 2, 3, 5, 7, 11, 13... are all prime numbers.

If an integer a can be written as $a = bc$ then a is called Composite integer. where $b, c \in \mathbb{Z} \Rightarrow |b| > 1$ & $|c| > 1$

Example $21 = 3 \cdot 7$, $6 = 2 \cdot 3$, $\therefore$ 6, 21 are composite

29/01/2018

Recall that

~~A number $p \in \mathbb{Z}$ is called~~

1) A number $p > 1 \in \mathbb{Z}$ is called a prime number if its only divisors are 1 and p.

2) If the $\gcd(a, b) = 1$. Then we say that a and b are relatively prime. eg. $(2, 13) = 1$, $(3, 11) = 1$ etc

3) The number that are not prime are called composite. Eg. $12 = \pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12$ while $11 = \pm 1, \pm 11$.

EUCLID LEMMA: Let $a, b \in \mathbb{Z}$. If $p \mid ab$. then either $p \mid a$ or $p \mid b$ where p is a prime number.

Example $2, 12 \Rightarrow 2 \mid 12 \Rightarrow 2 \mid (3, 4) \xleftarrow{2 \nmid 3} 2 \mid 4$. 2 = prime.

$6 \mid 12 \Rightarrow 6 \mid (3, 4) \xleftarrow[6 \nmid 4 \times]{6 \nmid 3 \times}$ because 6 ≠ prime

Proof: Let p be prime

Let $a, b \in \mathbb{Z}$ & suppose $p \mid ab$

Suppose $p \nmid a$, we show that $p \mid b$,

If $p \nmid a \Rightarrow \gcd(p, a) = 1$

$\Rightarrow p$ and a are relatively prime

Since $(p, a) = 1$, $\exists\ x, y \in \mathbb{Z}$ ∋ $px + ay = 1$

$bpx + bay = b$ — (1)

Also, given $p/ab \Rightarrow ab = pq$ - (2) $q \in \mathbb{Z}$

from (1) & (2) we have $b = bpx + bqy$

but $ab = bq = pq$ $\quad b = bpx + pqy$

$b = p(bx + qy)$ $\quad$ let $q_1 = bx + qy$

Now $b = pq_1$ $\quad q_1$

Hence p/b

~~Theorem~~ Lemma 1.6 : In general if p is a prime and divides $a_1, a_2, a_3, \ldots, a_n$ of certain integers then p must divides atleast one of the $a_1, a_2, a_3, \ldots, a_n$.

Proof of $p/ab \Rightarrow p/a$ or p/b

$p/a_1, a_2, a_3, \ldots, a_n \Rightarrow p/a_1(a_2, a_3, \ldots, a_n)$

Theorem 1.7 : If a is a positive integer greater than 1, then a has a prime factor.

Proof : we use mathematical induction. Let $a=2$ least number greater than 1, $2 = 2 \cdot (1) \cdot 2$ has prime factor 2 $\Rightarrow$ the theorem is true for $a=2$.

We now assume that the result is true for all integers K such that, $1 < K < a$. - - - (1)

We now consider a, iff

If a is prime, then we don't have anything to prove.

Suppose a is not prime, then $\exists b, c \in \mathbb{Z}$

where
$1 < b < a$ and $1 < c < a$
$\Rightarrow a = bc$
By assumption from (1), then theorem is true for all integers $k \Rightarrow 1 < k < a$, now, since we have $1 < b < a$, b has a prime factor
Let p be the prime factor then $p \mid b$,
But $b \mid a$ because, $a = bc$.
By transitivity of division $p \mid a$ i.e a has a prime factor p. □

Theorem 1.8 : Fundamental Theorem of Arithmetic (or Unique factorization.) : Every positive integer $a > 1$ can be uniquely expressed as a product of positive primes.

Proof : We use mathematical induction on a
Let $a = 2$, since 2 is the least positive integer $> 1 \Rightarrow 2 = 2(1)$. The result is true for $a = 2$
we now assume that true for all positive integers
$k \Rightarrow 1 < k < a$ ---- (1)
we now consider a, If a is a prime, we are done, Suppose a is not a prime then $\Rightarrow a = bc$ where $1 < b < a$ and $1 < c < a$
By our assumption, (1), b and c can be

where $p_1, p_2, p_r, q_1, q_2, q_r$ are prime.

Let $b = p_1 p_2 \cdots p_r$ and $c = q_1 q_2 \cdots q_r$

$\therefore a = bc = (p_1 p_2 \cdots p_r)(q_1 q_2 \cdots q_r)$ where

Hence by mathematical induction every positive integer > 1 is expressed as product of prime.

Uniqueness: Suppose, another prime factorization of a is given as

$$a = (p_1' p_2' \cdots p_t')(q_1' q_2' \cdots q_s')$$

but $a = a$

$$p_1' p_2' \cdots p_t' = p_1 p_2 \cdots p_r q_1 q_2 \cdots q_r$$

Now $p_1' \mid (p_1' p_2' \cdots p_t') \Rightarrow p_1' \mid (p_1 p_2 \cdots p_r q_1 q_2 \cdots q_r)$

Without any loss of generality we assume

$\Rightarrow p_1' = p_1$ since p_1' and p_1 are prime

$\Rightarrow p_1 p_2' p_3' \cdots p_t = p_1 p_2 \cdots p_r q_1 q_2 \cdots q_r$

By Cancellation law

$$p_2' p_3' \cdots p_t = p_2 p_3 \cdots p_r q_1 \cdots q_r$$

Continue applying the same reasoning we have

$p_1' = p_1, p_2' = p_2 \ldots$ where $t = r+r$ □

Note:

Sum of the prime may be repeating, hence

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} \quad \text{--- (1)}$$

e.g. $20 = 2 \cdot 2 \cdot 5 = 2^2 \cdot 5^1$

where $p_1 < p_2 < p_3 < \cdots < p_r$ and $\alpha_1, \alpha_2, \ldots, \alpha_r \geq 1$

Then (1) is called prime factorization in canonical form.

Example: find the gcd and LCM of a = 50400 and b = 14850 by 1st expressed a & b in canonical form

Sol: a = 50400 = $2^5 \cdot 3^2 \cdot 5^2 \cdot 7^1$

b = 14850 = $2^1 \cdot 3^3 \cdot 5^2 \cdot 11^1$

gcd(50400, 14850) = $2^1 \cdot 3^2 \cdot 5^2 = 450$

LCM[50400, 14850] = $2^5 \cdot 3^3 \cdot 5^2 \cdot 7^1 \cdot 11^1 = 1663200$

RINGS AND FIELDS

30/01/2018

A non-empty set R together with two (2) binary operations, addition (+) and multiplication (·) that satisfy the following properties:

i) (R, +) is an abelian group.

ii) (R, ·) is closed ie for every $a, b \in R$ then $a \cdot b \in R$

iii) (R, ·) is associative ie for every $a, b, c \in R$ then

$$a(bc) = (ab)c$$

iv) $\forall a, b, c \in R \Rightarrow a(b+c) = ab + ac$ - Distributive

Zero (0) is called additive identity.

One (1) is called multiplicative identity

Example

(1) (Z, +, ·) where Z is set of integers

BASIC DEFINITIONS

- A commutative Ring is a ring R that satisfies additional properties that if $a, b \in R$ then $ab = ba$
- A ring with identity is a ring that contains an element One (1) if $a \in R$ then

$$1 \cdot a = a \cdot 1 = a.$$

Example: [Concrete]

Let $Z[x]$ be the set of all polynomials of the form

$$\sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

$(Z[x], +, \cdot)$ is a ring of polynomial over Z

Here $U(x) = 1$ is multiplicative identity

therefore $(Z[x], +, \cdot)$ is a ring with unity (identity).

(Hint: let $p(x) = \sum_{i=0}^{m} a_i x^i$ and $q(x) = \sum_{i=0}^{n} b_i x^i$

$p(x) + q(x) = \sum_{i=0}^{n} (a_i + b_i) x^i = \sum_{i=0}^{n} c_i x^i$ -- closed (+)

$p(x) q(x) = \sum_{k}^{} \sum_{i=0}^{m+n} (a_i x^i)(b_i x^i) = \sum_{k=0}^{n+m} c_k x^k$ -- closed (·)

$c_k = \sum_{i=0} a_i b_{k-j} = a_0 b_k + a_1 b_{k-1} + \cdots + a_k b_0$ }

2) The set of all odd integer with addition (+) and multiplication (·) is not a ring, since addition of two odd numbers is an even number.

3) Let $m(Z)$, $m(Q)$, $m(R)$, $m(C)$, $m(Z_n)$ denote respectively the 2×2 matrices with entries from integer, rational number, Real number, Comple

number and integer modulo n with usual matrix addition and multiplication are all rings with unity.

4) Let T be the set of all continuous functions from $\mathbb{R}$ to $\mathbb{R}$, where $\mathbb{R}$ is the set of real numbers. Then $(T, +, \cdot)$ is an commutative ring with unity. Since if f and g are continuous function $(f+g)x = f(x) + g(x)$ & $(fg)x = f(x)g(x)$. T is closed under $(+)$ and $(\cdot)$

5) Let $G = \{a + bi \mid a, b \in \mathbb{Z}, i = \sqrt{-1}\}$. Define addition and multiplication on G by

$(a+bi) + (c+di) = (a+c) + (b+d)i$

$(a+bi)(c+di) = (ac - bd) + (ad + bc)i$ then $(G, +, \cdot)$ is a commutative ring with unity

6) An example of a ring without unity is $(2\mathbb{Z}, +, \cdot)$.

Definition : Integral Domain

Is a Commutative ring R with identity that satisfies additional properties that $\forall a, b \in R$ if $ab = 0$ then either $a = 0$ or $b = 0$. a is called left zero divisor and b is called right zero divisor. Integral domain

(I) Ring (II) Commutative (III) it has unity (IV) it has no zero divisor

Division ring: (i) Ring (ii) Unity (iii) every non-zero element has a multiplicative inverse

Definition: A non-zero element of a ring R is called a **zero divisor**, if $\exists$ an element $b \neq 0 \in R$ $\ni$ $ab = 0$ or $ba = 0$

Definition: **Ring with zero divisor** is a ring in which $\exists$ non-zero elements $a \neq b$ $\ni$ $ab = 0$ otherwise called ring without zero divisor.

Example 1) Let $m(z)$ is a ring with zero divisors since $0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in m(z)$ is the zero element of $m(z)$. Let $A, B \in m(z)$ i.e

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

$$AB = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0 \Rightarrow A \neq 0 \text{ & } B \neq 0$$

2) A ring $(Z_n, +, \cdot)$ is a ring with zero divisors eg $(Z_6, +, \cdot)$ is a ring with

3) $(Z, +, \cdot)$ is a ring without zero divisors. Because product any two non-zero integers cannot be zero.

12/02/2018

Definition: A ring $(R, +, \cdot)$ is a **Division Ring** or **Skew Field**, if in addition $(R \setminus \{0\}, \cdot)$ is a group. i.e if every non-zero element $a \in R$ has a multiplicative inverse a^{-1} $\ni$ $a \cdot a^{-1} = 1$

Field :- (i) Ring (ii) Commutative (iii) unity
(iv) Every non-zero element has a multiplicative inverse

Definition :- A commutative Division Ring is called a Fields

Example :- ① $(\mathbb{Z}, +, \cdot)$ is an integral domain
② $(\mathbb{Z}_p, +, \cdot)$ is a integral domain
3) The set $\mathbb{R}, \mathbb{Q}, \mathbb{C}$ are all integral domain and fields with the usual addition and multiplication.
4) An example of a division Ring which is not a field is the Quaternion of Hamilton denoted by $(\bar{\mathbb{Q}}, +, \cdot)$, $\bar{\mathbb{Q}} = \{a + ib + cj + dk \mid a, b, c \in \mathbb{Q}\}$
where $ij = k$, $jk = i$, $ki = j$; $i^2 = j^2 = k^2 = -1$
$ji = -k$, $kj = -i$; $ik = -j$

Theorem 2.1 :- Let $(R, +, \cdot)$ be a ring then
i) $a0 = 0a = 0$ (ii) $(-a)b = a(-b) = -(ab)$
iii) $(-1)(-1) = 1$ (iv) $(-a)(-b) = ab$
v) $a(b-c) = ab - ac$ (vi) $(a-b)c = ac - bc$
vii) $1 \neq 0$ (viii) multiplicative identity is Unique

Proof vii) Suppose $1 = 0$ $\forall a \in R$
$a = a \cdot 1 = a \cdot 0 = 0$ Contradiction
i.e. every element in R is zero contradiction
hence $1 \neq 0$

viii) Suppose $1'$ is another multiplicative identity
we have $1 = 1 \cdot 1' = 1' \Rightarrow 1 = 1'$

Every finite integral domain is a field.

Wedderburn's theorem

Ques multiplicative identity is unique:

Theorem 2.2 :- Every field $(F, +, \cdot)$ is an integral domain

Proof :- A field is commutative ring with unity we simply show that F contains no zero divisor

Suppose $a, b \in F$ and $ab = 0$

If $a \neq 0$, we show that $b = 0$

If $a \neq 0$, $\exists\, a^{-1} \in F$ such that $a^{-1}a = 1$

$b = 1 \cdot b = a^{-1}ab = a^{-1}(ab) = a^{-1}0 = 0 \Rightarrow b = 0$

Similarly, if $b \neq 0$, then $\exists\, b^{-1} \in F$ such that $b \cdot b^{-1} =$

$a = a \cdot 1 = a \cdot bb^{-1} = (ab)b^{-1} = 0 \cdot b^{-1} = 0$

$\Rightarrow$ if $b \neq 0$ then $a = 0$

i.e., In field F $ab = 0 \Rightarrow a = 0$, or $b = 0$

Hence :- Field has no zero divisor. Hence Field $(F, +, \cdot)$ is an integral domain. □

Note :- Not every integral domain is a field. For example $(Z, +, \cdot)$.

Theorem 2.3 :- Every finite integral domain is a field

Proof :- Let $D = \{x_0, x_1, x_2, \ldots, x_n\}$ be a finite integral domain where x_0 is zero and $x_1 = 1$. To show, D is a field, we only show the existence of a multiplicative inverse for each element of D except x_0.

If x_i is not equal to zero, we show that
$x_i\Delta = \{x_i x_0, x_i x_1, x_i x_2, \ldots, x_i x_n\} = \Delta$
If $x_i x_j = x_i x_k$; then by cancellation law
$x_j = x_k$
Hence all element of $x_i\Delta$ are distinct and $x_i\Delta$ a subset of Δ with the same elements.
Therefore $x_i\Delta = \Delta$. There are some element x_j such that $x_i x_j = x_1 = 1$
Hence $x_j = x_i^{-1}$
Hence Δ is a field □

$Z_5 = \{0, 1, 2, 3, 4\}$ EXAMPLE

① Z_n is a finite integral domain and hence a field iff n is prime. But the set of integers Z, an infinite integral domain not a field.

2) Let $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \in \mathbb{R} \mid a, b \in \mathbb{Q}\}$. Then $(\mathbb{Q}(\sqrt{2}), +, \cdot)$ is a field.

Proof :- We first check that $(+)$ and $(\cdot)$ the binary operation is on $\mathbb{Q}(\sqrt{2})$.
Let $a, b, c, d \in \mathbb{Q}$
$(a + b\sqrt{2}) + (c + d\sqrt{2})$
$= (a + c) + (b + d)\sqrt{2}$
Since $a + c$ and $b + d \in \mathbb{Q}$. Then the

property is satisfied.

Also $(a+b\sqrt{2})(c+d\sqrt{2}) = ac + ad\sqrt{2} + cb\sqrt{2} + 2bd$

$= (ac + 2bd) + (ad+cb)\sqrt{2} \in \mathbb{Q}$

$\therefore$ $(\cdot)$ is a binary operation on $\mathbb{Q}(\sqrt{2})$

We observe that $\mathbb{Q}(\sqrt{2})$ is a subset of $\mathbb{R}$ hence the addition $(+)$ and multiplication $(\cdot)$ are the same as in $\mathbb{R}$.

We then check the axiom of commutative ring on $\mathbb{Q}(\sqrt{2})$.

⇒ Addition of real numbers is associative and Commutative

⇒ Existence of Zero : $0 = 0 + 0\sqrt{2}$

$\therefore 0 + 0\sqrt{2}$ is the additive identity

The additive inverse of $a+b\sqrt{2}$ is $-a+(-b)\sqrt{2}$

multiplication of real number is associative. So also in $\mathbb{Q}$. $\therefore \mathbb{Q}\sqrt{2}$ is Commutative ring with unity.

To show that $\mathbb{Q}\sqrt{2}$ is a field

Let $a+b\sqrt{2}$ be a non-zero element of $\mathbb{Q}(\sqrt{2})$

$$\frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{(a+b\sqrt{2})(a-b\sqrt{2})} = \frac{a-b\sqrt{2}}{a^2 - 2b^2}$$

$$= \left(\frac{a}{a^2-2b^2} + \left(\frac{-b\sqrt{2}}{a^2-2b^2}\right)\right) \in \mathbb{Q}\sqrt{2}$$

$\therefore \mathbb{Q}\sqrt{2}$ is a field

SUBRING

Definition: Let R be a ring. A non-empty subset S of the ring R (set R) is called a subring of R, if S is closed with respect to the operations of addition and multiplication in R and S itself is a ring under these operations.

Examples

1) $\{0, 2, 4\}$ and $\{0, 3\}$ are both subrings of $\mathbb{Z}$.
2) $\{0\}$ is a trivial subring of R and R is a subring of itself called improper subring.
3) The set, $2\mathbb{Z}$ of all even integers is a subring of the ring $\mathbb{Z}$ under the usual addition and multiplication.

Theorem 2-4 (Condition for a subring)
The necessary and sufficient condition for a subset S of a ring R to be a subring is
if $a, b \in S$ (i) $a - b \in S$
(ii) $a \cdot b \in S$

Proof :- Suppose $(S, +, \cdot)$ is a subring of $(R, +, \cdot)$
then $(S, +)$ is a subgroup of $(R, +)$
$\therefore \forall b \in S \Rightarrow -b \in S$
$\therefore \forall a \in S, -b \in S$

$a+(-b) \in S$, Closure property
Also S is closed with respect to multiplication
i.e $\forall a, b \in S$, $a.b \in S$.

Conversely, Suppose the two conditions, we show S is a subring

from (1) $a \in S \Rightarrow (a-a) \in S \Rightarrow 0 \in S$

Also, since $0 \in S$, $\forall a \in S$

from (1) $0 - a \in S \Rightarrow -a \in S$

i.e Every element of S has additive inverse.

Now, $\forall a, b \in S \Rightarrow -b \in S$;

from (1), $a-(-b) \in S \Rightarrow a+b \in S$. Closure pp.

Since S is a subset of R.

i.e $(S, +)$ is a subgroup of $(R, +)$

Then commutative & associative also hold. in S.

Hence $(S, +, \cdot)$ is a ring of $(R, +, \cdot)$

Theorem 2: The intersection of any two subrings of ring R is again a subring.

Proof: Let S_1 and S_2 be any two subrings of a ring R.

We want to show that $S_1 \cap S_2$ is a subring of R.

Let $a, b \in S_1 \cap S_2$,

$\Rightarrow a, b \in S_1$ and $a, b \in S_2$

Since S_1 is a subring then

$a-b \in S_1$ & $a-b \in S_2$

$a \cdot b \in S_1$ $a \cdot b \in S_2$

$\Rightarrow a-b \in S_1 \cap S_2$ also $a \cdot b \in S_1 \cap S_2$

$\Rightarrow S_1 \cap S_2$ is a subring of R.

Theorem 2-6: Finitely intersection of subrings of R is again is a subring of R.

Proof Hint Let $S = \bigcap_{i=1}^{n} S_i$

05/03/2018

SUBFIELD

Let F be a field. Let K be a non-empty subset of F. K is called a subfield of F, if K is closed with respect to addition and multiplication and K is itself is a field under these binary operation.

Examples

1. The field of real numbers is a subfield of Complex numbers
2. The field of rational numbers is a subfield real numbers.
3. **THEOREM**: NECESSARY AND SUFFICIENT CONDITION FOR A NON-EMPTY SUBSET K OF A FIELD F TO BE A SUBFIELD are as follows

i) $\forall a, b \in K$, $a-b \in K$.

ii) $a \in K$ $b \neq 0 \in K$ then $ab^{-1} \in K$.

Proof :- Suppose K is a subfield of the field F. Then K is a subgroup with respect to addition.

$\Rightarrow \forall\ b \in K \Rightarrow -b \in K$

Also, let $a, b \in K$.

$\Rightarrow a + (-b) \in K \Rightarrow a - b \in K$.

But K is closed with respect to multiplication.

then $\forall\ a \in K \quad b \neq 0 \quad ab^{-1} \in K$.

Conversely, suppose the two conditions are satisfied

then, from (i) $a\ (K, +)$ is an abelian group.

let $a \neq 0 \in K$ from (ii) $aa^{-1} \in K \Rightarrow 1 \in K$ (multiplicative identity)

Now, $1 \in K, a \neq 0 \in K \Rightarrow 1 a^{-1} \in K$ from (ii)

$1 \cdot a^{-1} \in K$

i.e each multiplication inverse in K (i.e non-zero elem. i.e each non-zero element of K possesses multiplication inverse.

Now, $b \neq 0 \in K \Rightarrow b^{-1} \in K$.

from (ii) $a(b^{-1})^{-1} \in K \Rightarrow ab \in K$.

Also if $b = 0$ then $ab = 0 \Rightarrow 0 \in K$

Since K is a subset of F. Then Associative Distributive rule hold in F, hence K is a sub-field of F.

Defn: If $(R, +, \cdot)$ is a ring then the centre of R, $C(R)$ is the set of elements in R which commute with all other elements for the multiplication operation

$$C(R) = \{a \in R / ab = ba \ \forall b \in R\}$$

Theorem 2.8: The centre of a ring R is a commutative subring of R. Proof

HOMOMORPHISM

Defn: Suppose $(R, +, \cdot)$ and $(S, \oplus, \odot)$ are rings then the mapping

$\theta : (R, +, \cdot) \longrightarrow (S, \oplus, \odot)$ is a ring homomorphism. If

i) $\theta(a+b) = \theta(a) \oplus \theta(b)$

ii) $\theta(a \cdot b) = \theta(a) \odot \theta(b) \quad \forall a, b \in R$.

i) If θ is bijective then θ is called Isomorphism

ii) If R & S are isomorphic then we write $R \cong S$

iii) If θ is a homomorphism and $R = S$ then θ is called endomorphism

iv) A bijective endomorphism is called an Automorphism.

Examples: Let $\theta : (Z, +, \cdot) \longrightarrow (Z_n, \oplus, \odot)$ be defined by $\theta(m) = \bar{m}$ where $\bar{m}$ represent

the equivalence class of m in $\mathbb{Z}_n$. Then θ is a ring homomorphism.

Proof $\theta(m+n) = \overline{m+n} = \bar{m} \oplus \bar{n} = \theta(m) \oplus \theta(n)$

$\theta(mn) = \overline{mn} = \bar{m} \odot \bar{n} = \theta(m) \odot \theta(n)$

But θ is not a ring homomorphism, since

$\theta(n+1) = \overline{n+1} = \bar{n} \oplus \bar{1} = \bar{0} \oplus \bar{1} = \bar{1} = \theta(1)$

because if it modulo n $\theta(n) = \bar{n} = \bar{0} = 0$

2) Let $\theta : (\mathbb{Z}, +, \cdot) \to (M_2(\mathbb{Z}), +, \times)$ be defined by $\theta(n) = \begin{pmatrix} n & 0 \\ 0 & n \end{pmatrix}$. Then θ is a ring homomorphism

Proof :- Let $m, n \in \mathbb{Z}$

i) $\theta(m+n) = \begin{pmatrix} m+n & 0 \\ 0 & m+n \end{pmatrix} = \begin{pmatrix} m & 0 \\ 0 & m \end{pmatrix} + \begin{pmatrix} n & 0 \\ 0 & n \end{pmatrix} =$

$= \theta(m) + \theta(n)$

ii) $\theta(mn) = \begin{pmatrix} mn & 0 \\ 0 & mn \end{pmatrix} = \begin{pmatrix} m & 0 \\ 0 & n \end{pmatrix}\begin{pmatrix} n & 0 \\ 0 & n \end{pmatrix} = \theta(m)\theta(n)$
$= \theta(m) \times \theta(n)$

3) Let θ Since the two conditions satisfied then θ is a ring homomorphism.

3) Let $\theta : (G, +, \times) \longrightarrow (M_2(\mathbb{Z}), +, \times)$ be defined by $\theta(m + ni) = \begin{pmatrix} m & n \\ -n & m \end{pmatrix}$ where $(G, +, \times)$ is called a ring of Gaussian integer is a ring homomorphism. Verify

Remark :- If $\theta : (R, +, \cdot) \to (S, \oplus, \odot)$ is a ring homomorphism. Then $\theta : (R, +) \to (S, \oplus)$ is a group homomorphism.

THEOREM 2.9 :- If $\theta : (R, +, \cdot) \to (S, +, \cdot)$ is a ring homomorphism. Then $\theta(R)$ is a subring of R.

Or Let $\theta : R \to R'$ be a homomorphic mapping of a ring R into a ring R'. Let S' be the homomorphic image of R in R'. Then S' is a subring of R'.

Proof : Let $\theta : R \to R'$ given

then $\theta(R) = S' \subseteq R'$

Let $a', b' \in S' \to \exists\, a, b \in R$ ∋

$\theta(a) = a'$ and $\theta(b) = b'$ since $\theta(R) = S'$

we need to show $a' - b' = \theta(a) - \theta(b) = \theta(a - b)$

since θ is a homomorphism. but $a - b \in R \Rightarrow a' - b' \in S'$

finally $a', b' \in S' \Rightarrow a'b' \in S'$

Since $\forall\, a', b' \in S'$ we have,

$a' - b' \in S'$ and $a'b' \in S'$

$\Rightarrow S'$ is a subring of R ∎

Theorem 2.10 : If θ is a homomorphism of a ring R into a ring R' then

(i) $\theta(0) = 0'$ (0 & $0'$ are additive identity in R & R' respectively)

ii) $\theta(-a) = -\theta(a)$

iii) if 1 is the multiplicative identity in R, then $1'$ is the multiplicative identity in R'.

iv) if a has multiplicative inverse $a^{-1} \in R$

then $\theta(a^{-1})$ is the multiplicative inverse of $\theta(a)$ in R'

Proof (i) Let $a \in R$, then $\theta(a) \in R'$

$\Rightarrow \theta(a) + 0' = \theta(a) = \theta(a+0) = \theta(a) + \theta(0)$

$\therefore \theta(0) = 0'$ from the remark (1) above.

ii) Let $a \in R$, then $-a \in R$

Now $0' = \theta(0) = \theta(a + (-a)) = \theta(a) + \theta(-a)$

$\Rightarrow \theta(-a)$ is the additive inverse of $\theta(a)$ $\therefore \theta(-a) = -\theta(a)$

iii) $\theta(1)\theta(a) = \theta(1 \cdot a) = \theta(a)$

$\Rightarrow \theta(1)$ is a multiplicative identity in $\theta(R)$

iv) $\theta(a) \cdot \theta(a^{-1}) = \theta(a \cdot a^{-1}) = \theta(1)$

$\therefore \theta(a^{-1})$ is the multiplicative inverse of $\theta(a)$.

KERNAL OF HOMOMORPHISM

Defn:- Let $\theta : R \to R'$ be a ring homomorphism. Then the set K of R that are mapped to the identity $0'$ in R' is called Kernal of the homomorphism θ. It is denoted by $\ker\theta$

$\ker\theta = \{ x \in R \mid \theta(x) = 0' \}$.

where $0'$ = identity in R'

Remark 2:- If $\theta : R \to R'$ is ring homomorphism and $r \in \ker\theta$. Then $x \cdot r, r \cdot x \in \ker\theta$ $\forall x \in R$

$\theta(x \cdot r) = \theta(x) \cdot \theta(r) = \theta(x) \cdot 0' = 0'$ where $\theta(r) = 0'$

IDEAL

Definition: A subring I of a ring R is called an **ideal** of R, if $x \cdot r \in I$, $r \in R$; $\forall x \in I$.

Remark 3: Ker θ of a ring homomorphism is an ideal in R.

i) An ideal I of R is called a proper ideal of R if I is a proper subring of R. ~~Otherwise called~~

ii) Both a ring R and the trivial subring $\{0\}$ are ideals of R. R is called improper ideal $\{0\}$ trivial ideal.

12/03/2018

The property $x \cdot r \in I$ and $r \cdot x \in I$ for $x \in I$ and $r \in R$ are called **left** and **Right** ideal in R respectively.

A subring S of R, that is both left and right ideal is called an **ideal of R**.

A ring that has no proper ideal is called **proper ring**.

Examples

① Let M be a set of all 2×2 matrices of the form $\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}$ $\forall a, b \in \mathbb{Z}$, M is a left ideal but not right ideal.

To show (1), Let $A=\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \in M$ & $B=\begin{pmatrix} c & 0 \\ d & 0 \end{pmatrix} \in M$

$A-B \in M$? Now $A-B=\begin{pmatrix} a-c & 0 \\ b-d & 0 \end{pmatrix} \in M$

$AB=\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}\begin{pmatrix} c & 0 \\ d & 0 \end{pmatrix}=\begin{pmatrix} ac+0 & 0+0 \\ bc+0 & 0+0 \end{pmatrix}=\begin{pmatrix} ac & 0 \\ bc & 0 \end{pmatrix} \in M.$

$\therefore M$ is a Subring of R

Now, for the Ideal, let $A=\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}$

then $r=\begin{pmatrix} x & y \\ w & z \end{pmatrix} \Rightarrow A \cdot r=\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}\begin{pmatrix} x & y \\ w & z \end{pmatrix}$

$A \cdot r=\begin{pmatrix} ax & ay \\ bx & by \end{pmatrix} \notin M \therefore M$ is not right ideal of R.

$r \cdot A=\begin{pmatrix} x & y \\ w & z \end{pmatrix}\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}=\begin{pmatrix} xa+yb & 0 \\ wa+zb & 0 \end{pmatrix} \in M$

$\therefore M$ is left ideal of R.

(2) Let M be a field integer, the set P of integer defined by $P=\{xm \mid x \in \mathbb{Z}\}$ is an ideal of the ring R of integers.

Sol Let $x, m \in P$ and $r \in R$ then

$r(xm)=(rx)m \in P$

Since $r \in R$ $rx \in R$ and Since $rx=rx$

$\forall x, r \in R$ then P is an ideal of R.

$5 \cdot 4 = 20 = 10 \times 2 \Rightarrow 5/10$ R the ring I

$5 \cdot 8 = 40 = 10 \times 4 \rightarrow 5/10$ R/I

$5 \times 2 \rightarrow 5/5$

$20 \times 2 \Rightarrow 5/20$

Exercise.

1.) Show the intersection of two ideals of R is again an ideal of R.

2.) Show that the set of integers is a subring but not an ideal of the ring of rational number.

Definition

Let K be a right ideal in ring R, K is called a principal right ideal in R if $K = \{a \cdot r \mid r \in R$ and a is some fixed element of R$\}$

Also $K = \{r \cdot a \mid r \in R$ and $r \in K\}$ is called principal ~~ideal~~ left ideal in R.

Definition: Let R be a commutative ring if every ideal in R is a principal ideal then R is called principal ideal ring.

Definition: An ideal I in a commutative ring R is called a prime ideal if for any arbitrary $r, s \in R$, then $r \cdot s \in I$

Implies that either $r \in I$ or $s \in I$

Example

In the ring of integer $\mathbb{Z}$ the ideal $I = \{5 \cdot r : r \in \mathbb{Z}\}$ also written as $\langle 5 \rangle$ is a prime ideal since ~~for~~ every

$12 \cdot 4 = 48 = 24 \times 8 \Rightarrow 12 \mid 24$

but $48 = 6 \times 8 \Rightarrow 12 \mid 8$ or $12 \nmid 8 \Rightarrow$

$\forall a, b \in I$ either $5 \mid a$ or $5 \mid b$

but $K = \{12 \cdot r \mid r \in \mathbb{Z}\}$ is not a prime ideal

Since $6 \times 8 = 48 \in K$ but $12 \mid 6$ or $12 \mid 8$.

$I = \{m \cdot r \mid r \in \mathbb{Z}, m \neq 0\}$ is a prime ideal if m is a prime number.

Definition: A proper ideal in a Commutative ring R is called Maximal if there exists no proper ideal in R that properly contains I.

Example: An ideal I of the ring of $\mathbb{Z}$ is maximal iff I is generated by some prime integer. for $I = (5)$ is a maximal ideal in $\mathbb{Z}$ since the only ideal in $\mathbb{Z}$ which properly contains I is $\mathbb{Z}$ itself.

27-03-2018

QUOTIENT RING

Let R be a ring and Let I be an ideal in R. Then $R/I = \{x + I \mid x \in R\}$ is called a QUOTIENT RING which is the set of all distinct elements cosets of I in R

EUCLIDEAN RING

Also Called euclidean domain

Let R be a Commutative ring without zero divisor. Ie R is an integral domain then R is called Euclidean ring. if for

every non-zero element $a \in R$, we can assign a non-negative integer $d(a)$ such that

i) $\forall a, b \in R$ (both non-zero)
$d(ab) \geq d(a)$

ii) for any $a, b \in R$ $b \neq 0$ $\exists q, r \in R$
$r = bq + r$ where $r = 0$ or
$d(r) < d(b)$

Note that: (ii) is called division algorithm

Example: Show that the ring of integers is an Euclidean ring.

Let $(\mathbb{Z}, +, \cdot)$ be the ring of integers
$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$
Let the function d on $\mathbb{Z}$ be defined by
$d(a) = |a|$ $\forall a \neq 0 \in \mathbb{Z}$ then
$|a|$ is a non-negative integer
Now for any $a, b \in \mathbb{Z}$
$|ab| = |a||b|$
$\Rightarrow |ab| \geq |a|$
$\Rightarrow d(ab) \geq d(a)$
finally, for $a, b \in \mathbb{Z}$ $b \neq 0$ $\exists q, r \in \mathbb{Z}$
$a = bq + r$ where $0 \leq r < |b|$
Therefore the ring of integers is

Euclidean ring.

MODULES

The concept of modules is generalization of a vector space. In vector-space the scalars are elements from field while in modules the scalars are elements from an arbitrary ring.

Defn: A non-empty set M is called left R-Module over a ring R if M is an abelian group under the operation of addition such that for any $r \in R$ $m \in M$ $\exists$ a unique element $rm \in M$ with the following conditions-

i) $r(a+b) = ra + rb$

ii) $(r+s)a = ra + sa$

iii) $r(sa) = (rs)a$ $\forall a, b \in M$ $r, s \in R$

Similarly Right Module is defined.

UNITAL R-MODULES

If the ring R with unity (1) then left R-module called unital module where

$1 \cdot m = m$ $\forall m \in M$

If R is a field then a Unital R-module is a vector space.

Examples

1) Every abelian group G is a module over the ring of integer $(\mathbb{Z})$.

2) Every ring R is an R-module over itself.

General properties of modules:

Let M be any R-module then

i) $r0 = 0 \quad \forall r \in M$

ii) $0a = 0 \quad \forall a \in M$

iii) $(-r)a = -(ra) = r(-a)$

iv) $(-r)(-a) = ra$

v) $r(a-b) = ra - rb$

vi) $(r-s)a = sa - sb \quad \forall r \in R, a, b \in M$ & $s \in R$.

SUB-MODULES

A non-empty subset S of R-module is called R-submodule of M if

i) S is an additive subgroup of M

ii) $r \in R$ & $a \in S \Rightarrow ra \in S$.

Note: (i) As usual if M is any R-module then M itself and $\{0\}$ are always submodule of M are called improper submodule.

ii) Others are called proper submodule.

Irreducible R-module:

Any R-module M is called

irreducible module, if its only submodule are M and {0} only.

Theorem 3.1 : If A and B are any two submodules of R-module M then $A \cap B$ is also a submodule of M.

proof :- Since A and B are submodules of R-module M, therefore A and B are additive subgroup of M.

Now, let $r \in R$ and $a \in A \cap B$

$\Rightarrow a \in A$ and $a \in B$.

$\Rightarrow ra \in A$ and $ra \in B$.

$\Rightarrow ra \in A \cap B$

Hence $A \cap B$ is submodules of M.

Theorem 3.2 : Arbitrary intersection of submodules of R-module M is again a submodule of M. Converse

SUBMODULE GENERATOR

Submodule generated by subset of module. Let S be non-empty subset of R-module M. If A is submodule of M containing S and A is contained in all submodules of M containing S then A is called submodule of M

generated by S, denoted (S) and (S) is the smallest submodule of M containing S.

Theorem 3-3 : The submodule of a unital R-module M generated by a subset S of M consists of all linear combinations of elements in S

Proof :- Let $L(S) = \{r_1 a_1 + r_2 a_2 + \cdots + r_n a_n$ any where $a_1, a_2, \ldots, a_n$ are arbitrary subsets of S and $r_1, r_2, \ldots r_n$ are arbitrary subset of the ring R.

We show that L(S) is a submodule of R.

Let $a' = r_1 + a_1', r$ and $b' = s_1 b_1 + s_2 b_2 + \cdots + s_n b_n$ be any two elements of L(S).

where $r_1^2, s_1^3 \in$.

Let $a^* = r_1 a_1^* + r_2 a_2^* + r_3 a_3^* + \cdots + r_n a_n^*$

$b^* = s_1 b_1^* + s_2 b_2^* + s_3 b_3^* + \cdots + s_n b_n^*$.

Now $a^* - b^* = r_1 a_1^* + r_2 a_2^* + \cdots + r_n a_n^* - (s_1 b_1^* + s_2 b_2^* + \cdots + s_n b_n)$

$a - b \in L(S)$ since it is a linear combination of some element of S.

for any $a^*, b^* \in (S)$, then $a^* - b^* \in L(S)$

Hence $L(S)$ is an additive subgroup of M

Also, let $r \in R$ and $a^* = r_1 a_1^* + r_2 a_2^* + \dots + r_n a_n^*$ then

$ra^* = r(r_1 a_1^* + r_2 a_2^* + \dots + r_n a_n^*)$

$= rr_1(a_1^*) + (rr_2)a_2^* + \dots + (rr_n)a_n^*$

Since $rr_1, rr_2, \dots, rr_n \in R$

ra^* is also a linear combination of some element of S.

for any $r \in R$ and $a^* \in L(S)$, $ra^* \in L(S)$

$\therefore L(S)$ is a submodule of M.

Each elements S belongs to $L(S)$, since for each $a_i \in S$ we have $a_i = 1 \cdot a_i$ where 1 is the unit element of R and $a_i \in S \Rightarrow a_i \in L(S)$

$\therefore L(S)$ is a submodule of M and S is contained in $L(S)$.

Finally, if N is any submodule of M containing S, then each element of $L(S)$ must be in N is closed under scalar multiplication and addition. Therefore, $L(S)$ will be contained in N hence $L(S) = (S)$

$\Rightarrow L(S)$ is the submodule of M generated by S.

Linear Sum of two submodules:

Let A and B be any submodules of an R-module M.

Then the linear sum of A and B is denoted by A+B and given by

$A+B = \{a+b \mid a \in A \text{ and } b \in B\}$

Theorem 3.4: If A and B are submodules of a R-module M then A+B is also a submodule of M

Proof: Given A and B as submodules of M then

$A+B = \{a+b \mid a \in A \text{ and } b \in B\}$

Let $c = a_1 + b_1$ and $d = a_2 + b_2 \in A+B$

Now $c - d = (a_1 + b_1) - (a_2 + b_2)$

$= (a_1 - a_2) + (b_1 - b_2)$

Since A is an additive subgroup (M), then $a_1, a_2 \in A$, $a_1 - a_2 \in A$, $b_1, b_2 \in B$, $b_1 - b_2 \in B$

$\Rightarrow c - d \in A+B$

Now, let $r \in R$ and $c = a_1 + b_1 \in A+B$

where we have $rc = r(a_1 + b_1) = ra_1 + rb_1$

Since A is a submodule, then $\forall a \in A$ and $r \in R$, then $ra_1 \in A$.

Similarly $rb_1 \in B$

$\therefore ra_1 + rb_2 \in A+B$

$\Rightarrow$ for $r \in R$ and $c = a+b \in A+B$, then $rc \in A+B$

Hence $A+B$ is a submodule of M □

DIRECT SUM OF SUBMODULES

Let M be an R-module and $M_1, M_2, M_3 \dots M_n$ be submodules of M. If every element $a \in M$ can be written uniquely as $a = a_1 + a_2 + a_3 + \dots + a_n$ where $a_1 \in M_1, a_2 \in M_2, \dots a_n \in M_n$, If M is a direct sum of M_1 and M_2 we write $M = M_1 \oplus M_2$

Theorem 3.5 :- The necessary and sufficient condition for a module M to be a direct sum of M_1 and M_2 are

i) $M = M_1 + M_2$

ii) $M_1 \cap M_2 = \{0\}$ (similar to that of vector space)

HOMOMORPHISM OF MODULE

Let M and N be any two module then the mapping $T: M \to N$ is called a homomorphism if (i) $T(m_1 + m_2) = T(m_1) + T(m_2)$

ii) $T(rm) = r(T(m))$ $\forall r \in R$ and $m \in M$

Note :- If T is a homomorphism of M onto N then N is called the homomorphic image of M

If the mapping is 1-1 then T is called isomorphism of M onto N

$T(m)$ image of $m \in M$ is also written as

Thm on mT

Note: If $T: M \to N$ is a homo. Then

(i) $T(0) = 0$ (ii) $T(-m) = -T(m)$

(iii) $T(m_1 - m_2) = T(m_1) - T(m_2)$ $\forall m_1, m_2 \in M$

KERNEL OF HOMOMORPHISM

Let T be a homomorphism of R-module M into R-module N.

Then the kernel of T written as $\text{Ker}(T)$ is defined as

$K(T) = \{m \in M / T(m) = 0\}$ where 0 is additive identity group.

Theorem 3.6: The Kernel of a homomorphism is a submodule.

Proof: Let $K(T)$ be the Kernel of the homomorphism T of M onto N i.e

$K(T) = \{m \in M / T(m) = 0\}$ we show that $K(T)$ is a submodule.

Let $m_1, m_2 \in K(T)$ then $T(m_1) = 0$ and $T(m_2) = 0$

$T(m_1 - m_2) = T(m_1) - T(m_2) = 0 - 0 = 0$

$\Rightarrow K(T)$ is an additive subgroup of M

finally $r \in R$ & $m \in K(T)$ then

$T(rm) = r(T(m)) = r \cdot 0 = 0$

Hence $K(T)$ is a subgroup of M

Theorem 3.7: Let T be a module homomorphism. Then T is an isomorphism iff $K(T) = 0$.

Proof Let $T: M \to N$

Suppose $K(T) = 0$, we show that T is an isomorphism. Let $m_1, m_2 \in M \Rightarrow T(m_1) = T(m_2)$

$T(m_1) - T(m_2) = 0 \Rightarrow T(m_1 - m_2) = 0$

$\Rightarrow m_1 - m_2 \in K(T) \Rightarrow m_1 - m_2 = 0$

$m_1 = m_2$ (1-1)

Conversely, suppose that T is an isomorphism then we show that $K(T) = 0$.

Let $T(m) = 0 = T(0)$ but T is 1-1

$T(m) = T(0) \Rightarrow m = 0$

Then $m \in K(T)$ Hence $K(T) = 0$.