Ring Theory

Sagar L. Khairnar

DEFINITION: Ring

A non-empty set R together with two binary operations '+' and '.' is said to be a ring if

1. (R, +) is an additive abelian group.
2. (R, .) is a semigroup.
3. a . (b + c) = a . b + a .c and
(a + b) . c = a . c + b .c for all a, b, c ∈R (the two distributive laws)

Examples

1. Each of Z, R, Q and C is a commutative ring.
2. Let n be a positive integer and let Z_n= {0, 1, . . . , n – 1} with addition and multiplication performed modulo n. Then Zn is a commutative ring.
3. The set Mn(Q) of all n × n matrices with rational entries is a ring under matrix addition and multiplication. If n ≥ 2, this ring is noncommutative. More generally, if R is a ring, then Mn(R) is also a ring (with the usual rules for matrix addition and multiplication).
4. For any ring R, we have the ring R[x] = $\{a_0+ a_1x + a_2x^2+ \cdots + a_nx^n | a_0, \ldots, a_n \in R, n \in W\}$, called the ring of polynomials with coefficients in R. Here x is an indeterminate (and addition and multiplication of polynomials is "formal").
5. If X is a nonempty set, then the set F(X, R) of real valued functions f : X → R is a commutative ring under pointwise addition and multiplication.
6. If $R_1, \ldots, R_n$ are rings, then their direct product is the cartesian product $R_1 \times \cdots \times R_n$ with the operations
$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1+ b_1, \ldots, a_n+ b_n)$,
$(a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n) = (a_1b_1, \ldots, a_nb_n)$.
7. The smallest ring is the zero ring R = {0}. A ring R is the zero ring if and only if $1_R = 0_R$

Question :Let R be a ring with unit element. Using its elements we define a ring R˜ by defining a ⊕b = a + b + 1, and a·b= ab+ a + b, where a, b ∈R and where the addition and multiplication on the right-hand side of these relations are those of R.

(a) Prove that R˜ is a ring under the operations ⊕and ·.
(b) What act as the zero-element of R˜?
(c) What acts as the unit-element of R˜?
(d) Prove that R is isomorphic to R˜

DEFINITION: Subring

A non-empty subset S of R is said to be a subring of R if

1. (S, +) is a subgroup of (R,+).
2. (S, .) is a subsemigroup of (R,.)

Examples

1. Z is a subring of Q, R & C
2. Q is a subring of R & C
3. R is a subring of C
4. $M_n(Z)$ is a subring of $M_n(Q)$

DEFINITION : Zero Divisor

Suppose R is a ring. A nonzero element r ∈R is said to be a zero divisor if there exists a nonzero s ∈R
such that rs= 0 or sr= 0.

DEFINITION : Integral Domain

A commutative ring without zero divisor is called integral domain.

DEFINITION : Unit element

A nonzero element u ∈ R is said to be unit if there exists nonzero element v∈ R such that u.v=1, where R is a ring with unity (not necessarily commutative)

DEFINITION : Division ring (Skew field)

If every nonzero element in a (not necessarily commutative) ring is a unit, then R is called a division ring (or skew field).

DEFINITION : Field

A commutative division ring is called field.

Examples

1. Z is integral domain but not a division ring
2. $M_n(R)$ is a ring which is not an integral domain for $n \geq 2$

3. Real quarternion is a ring which is a division ring but not a field.
4. Q, R, C are fields

Results

1. Every field is a division ring & integral domain but not conversely.
2. The ring Zn is a field if and only if n is a prime number.
3. Let R be a ring such that | R| = p, where p is a prime number. Then R is isomorphic to Z_p. Inparticular, R is a field.
4. Let R be a commutative ring. Then the following statements are equivalent:
   (a) R is an integral domain.
   (b) If ab= ac in R and a $\neq$ 0, then b = c.
5. If R is an integral domain and S is a subring of R, then S is an integral domain
6. Every finite integral domain is a field

DEFINITION : Ideal

Let R be a ring. A nonempty subset I of R is said to be theright (left) ideal of R if

1. I is a subgroup of R under addition.
2. For all r ∈R and s ∈I; rs∈I.(sr∈I).

I is called an ideal; if I is simultaneously both a right and a left ideal of R. If R isa commutative ring naturally the concept of right and left ideals coincide

Examples

1. nZ is an ideal of Z, where n=0,1,2,3,…
2. Z is not an ideal of Q

Properties

1. A+B={x+y / x ∈ A, y ∈B} is an ideal .
2. A.B={x.y / x ∈ A, y ∈B}={ $\sum_{i=0}^{finite} u_i v_i$ / $u_i \in A, v_i \in B$} is an ideal.
3. $A \cup B$ is an ideal if $A \subseteq B$ or $B \subseteq A$
4. A⋂ B is always an ideal.

Types

Minimal ideal : If I≠(0) is an ideal of a ring R. R is said to be a minimal ideal if there is an ideal J such that $(0) \subseteq J \subseteq I$ then either J=(0) or J=I.

Maximal Ideal : If I≠R is an ideal of a ring R. R is said to be a maximal ideal if there is an ideal J such that $I \subseteq J \subseteq R$ then either I=J or J=R

Prime ideal: If I is an ideal of a ring R. R is said to be a minimal ideal if x.y∈ I then either x∈I or y∈I.

Examples :

1. (0) & R are ideals of R
2. nZ is an ideal of Z where n=0,1,2,3…

Result

1. nZ is prime ideal of Z iff n is a prime
2. nZ is maximal ideal of Z iff n is a prime
3. Every maximal ideal is a prime ideal. Converse is true if R is a P.I.D.
4. Let I be an ideal of a ring R. Then
   1 ∈I. ⇔ I contains a unit. ⇔ I = R. ⇔ I contains an element which has a left inverse or a right inverse
5. The number of ideals of nZ is nothing but the total number of divisors of n
6. If R is a ring with 1 and I is an ideal in R such that $I \neq R$, then there is a maximal ideal M of the such that $I \subseteq M$.
7. LetRbe a ring with 1 . Then R is a division ring iff R has no proper ideals
8. LetR be a commutative ring with 1 . Then R is a field iff R has no proper ideals

Definition: Simple Ring

A Ring R is called as simple ring if R has no proper ideals.

Examples

1. Every Field is a simple ring.
2. Z is not a simple ring.
3. $M_n(R)$ is a simple ring.

Definition:Quotient Ring

Let I be an ideal of R. The set S={x+I / x∈ R} is a ring with the operations"+" and "." Defined as (a+I)+(b+I)=(a+b)+I & (a+I).(b+I)=(a.b+I) $\forall a, b \in R$. This ring is called as a Quotient Ring& denote by S=R/I

Properties

1. a+I = I for all a ∈I
2. a+I = b+Iiff a-b ∈I

Examples :

R=Z & I=4Z. Then R/I=Z/4Z={x+4Z /x∈ Z}=Z_4

Results

1. R/I = R if and only if I = (0) and R/I = (0) if and only if I = R.
2. R/I is commutative if R is commutative (but not conversely).
3. R/I is a ring with 1 if R is with 1 (but not conversely).
4. If $a \in R$is a unit, then a +I is a unit in R/I (but not conversely) .
5. $Z/nZ=Z_n$
6. R/I is an integral domain if and only if I is a prime ideal in R.
7. R/I is a field if and only if I is a maximal ideal in R.
8. Every prime ideal of a Boolean ring is maximal
9. A prime ideal in a finite commutative ring with 1 ismaximal.

Definition: Ring homomorphism

Let R and S be rings. A mapping $f : R \to S$ is called a ring homomorphism if it satisfies the following properties. $f(a + b) = f(a) + f(b)$,$f(ab) = f(a)f(b)$ for all $a,b \in R$

Properties:

$f(0_R) = f(0_R + 0_R) = f(0_R) + f(0_R) \Rightarrow f(0_R) = 0_S$,

$f(a) + f(-a) = f(a + (-a)) = f(0R) = 0S \Rightarrow f(-a) = -f(a)$

For every $m \in Z$ and $r \in R$, we have $f(mr) = mf(r)$.

For every $m \in N$ and $r \in R$, we have $f(r^m) = f(r)^m$.

If $u \in R^*$, then $f(u) \in S^*$and, for every $m \in Z$, we have $f(u^m) = f(u)^m$. In particular, $f(u^{-1}) = f(u)^{-1}$.

Types:

Monomorphismor Injective homomprphism if f is 1-1

Epimorphismor surjective homomorphism if f is onto

Isomprphismif f is 1-1 and onto

Endomorphism if f is homomorphism and R=S

Automorphismif f is homomorphism and R=S

Frobeniushomomorphism

Let R be a commutative ring with p = charRa prime number. Then the map
$f : R \to R$, $f(r) = r^p$is a ring homomorphism, called the Frobenius homomorphism

Examples

1. f :Z → Q such that f(x)=x. This is monomorphism
2. f :Z → Z_n such that f(x)=$\bar{x}$ where $\bar{x} \equiv x(mod\ n)$. f is epimorphism but not monomorphism
3. f :IR→ IR be a homomorphism then either f≡0 or f is identity.
4. f :ℂ→ ℂ such that f(z)=$\bar{z}$ is an isomorphism.

Definition: Kernel of a homomorphism

Let R and S be rings. Let f :R → S be a ring homomorphism. Then Kernel of a homomorphism is defined as Kerf={x ∈ R / f(x)=0_S}

Result:

1. Let f :R → S be a homomorphism of rings with I = Kerf. Then R/Kerf ≅ Im(f)
2. If I⊆ J are both ideals in R, then (R/I)/(J/I) ≅ R/J
3. Let R be a commtative ring with 1 and I and J be ideals coprime to each other (i.e., I +J = R) .Then I ⋂ J = IJ and R/IJ≅R/I× R/J
4. Z/nZ≅ $Z/nZ \cong Z/p_1^{r_1}Z) \times (Z/p_2^{r_2}Z) \times (Z/p_3^{r_3}Z) \times \ldots \times (Z/p_k^{r_k}Z)$where n= $p_1^{r_1}p_2^{r_2}\ldots p_k^{r_k}$
5. The number of homomorphism from Z_n to Z_m is equal to gcd(m,n)
6. If R is a simple ring &f :R → R be a homomorphism then either f≡0 or f is isomorphism.

Definition: Characteristic of a ring.

Given a ring R (commutative or not , with or without unity), the characteristic of R, denoted by Char(R), & Char(R)=n if there exists a least positive integer nsuch that na = 0 for all a∈ R otherwise, Char(R)=0.

Properties:

1. Char(R) = 1 iff R= (0)
2. Char(R) = 0 if and only if given any positive integer n, there is an a =a(n) (depending on n) such that na≠0
3. Char(R) = n ≠0 iffn.x=0, for all x∈ R and for any positive integer m <n, there is an a ∈ R such that ma≠0
4. Let S be a subring of a ring R. Then Char(S)≤ Char{R) and equality holds if both R and S have the same unity
5. If R and S are rings, then =Char(R × S) = $\begin{cases} 0, & if\ Char(R) or\ Char(S) is\ 0 \\ l, & Otherwise \end{cases}$

where*l* =lcm(Char(R),Char(S))

Result:

1. Suppose R is a ring with 1 such that the non-units in R form a subgroup of (R, +), then Char(R) is either 0 or else a power of a prime.
2. If a ring R has 1, then we have
   a. Char(R) = 0 if and only if the additive order of 1 in the abelian group (R, +) is infinite.
   b .Char(R) = n ≠0 if and only if the additive order of 1 in (R,+) is finite and is equal to n.
3. Let R be a ring with 1 .Let P = {n1 / n ∈ Z} be the smallest subring of R containing 1, called the prime subring of R. Then we have the following.
   a .Char(R) = 0 if and only if P is infiite.
   b. Char(R) = n ≠ 0 if and only if P is finite and has exactly n elements, or equivalently, n is the additive order of 1 .
4. The characteristic of an integral domain (in particular, of a division ring or a field) is either 0 or a prime number.
5. Char(Z)=Char(nZ)=0 but Char(Z/nZ)=n≠0 if n≠0
6. If $f : \underbrace{R\times R\times....\times R}_{n\ times} \to \underbrace{R\times R\times....\times R}_{m\ times}$ is a ring automorphism then m=n

Assume that R be a commutative integral domain with 1 and $R^* = R - \{0\}$.

Definition: *a divides b*

Let a,b∈ R, a≠0. We say that a divides b or a is a divisor (or factor) of b and written a|bif there exists c∈ R such that b =ac.

Associates: Two elements a and b in R* are said to be associates of each other if a|bandb|a

Irreducible element: A non-zero non-unit a∈R is said to be irreducible if a = bc, then either b or cis a unit, i.e., a cannot be written as a product of two non-units or equivalently, the only divisors of a are its associates or units.

Prime element: A non-zero non-unit a ∈ R is said to be a prime if a|bc, (b,c∈ R), then either a|b or a|c

Results:

1. Let a, b∈ R, a≠0. Then a|b if and only if (b) ⊆ (a).
2. Let a, b ∈ R*. Then a and b are associates of each other iff a= ubfor some unit u ∈ R iff (a) = (b) .
3. Every prime is irreducible but not conversely.
4. Let a be a non-zero non-unit in a commutative integral domain R. Then
   a) . The element a is irreducible in R if and only if the ideal (a) is maximal among all principal

ideals other than R, i. e., there is no principal ideal in R, other than R, properly containing (a).
b). The element a is prime in R if and only if the ideal (a) is a non-zero prime ideal in R.

Definition : Greatest Common Divisor (GCD)

Given a, b ∈ R* ,an element d ∈ R* is called a greatest common divisor of a and b if
1 . d|aand d|b, i.e., d is a common divisor of a and b and

2 .c|a and c| b then c|d, i.e., d is greatest among the common divisors of a and b.

Definition : Least Common Multiple (LCM)

Given a, b ∈ R* ,an element l∈ R* is called a least common multiple of a and b if
1 . a| l and b| l, i.e., l is a common multiple of a and b and

2 .a|m and b|m then l|m, i.e., l is least among the common multiples of a and b.

Properties:

1. Given a, b ∈ R*, if gcd {resp. lcm) of a and b exits, then it is unique upto associates and is denoted by gcd(a, b) (resp. lcm(a, b)) .
2. If the gcd(a,b)=1 then a& b are said to be coprime.
3. $LCM(a,b) = \frac{a.b}{GCD(a,b)}$

Definition : Euclidian Domain (E.D.)

A commutative integral domain R (withor without unity) is called a Euclidean domain if there is a map d: R*→Z^+such that

1. $\forall a,b \in R^*$, a|bthen d(a) ≤d(b) or equivalently, d(x) ≤d(xy) and
2. $\forall a \in R \, and \;\; \forall b \in R^*, \exists q, r \in R$ (depending on a and b) such that a =qb+ r with either r(a)=0 or else d(r) <d(b).

Examples

1. Every field is Euclidian Domain with the map d(a)=1
2. Z is Euclidian Domain with the map d(n)=|n|
3. Z(i) is Euclidean Domain with the map d(n+mi)=| n^2+ m^2 |
4. R[x]the polynomial ring in one variable over a field R is Euclidean Domain with the map d(p(x))=deg(p(x)).

Results:

1. Every Euclidean domain R has unity
2. The group of units of E.D. is given by U(R) = {a∈ R* /d(a) = d(1)}.

3. 2Z is not E.D since $1 \notin 2Z$.

Definition : Principal Ideal

Let I be an ideal of R. I is said to be principal ideal if I=(x) for some x∈ I.

Example :I=2Z is principal ideal of Z since I=(2)

Definition: Principal Ideal Domain(P.I.D.)

A commutative integral domain R is called a principal ideal domain (PID)if every ideal of R is principal i.e., generated by one element .

Results:

1. Every Euclidean domain is a PID
2. Let R be a PID (with1) . Then
   a .Every irreducible element is a prime in R.
   b. Every non-zero prime ideal is maximal in R.
3. For a commutative integral domain R with unity, the following are equivalent.
   a). R is a fild.
   b). R[X] is Euclidean.
   c). R[X] is a PID .
4. Let R be a PID with 1 and a, b ∈ R*. Then

. d = gcd(a, b) iff (d) =(a) + (b), (gcd(a,b)=1 if and only if $\exists x, y \in R$ such that 1 == ax + by)

l= lcm (a, b) iff (l) = (a) $\bigcap$ (b) .

5. a). R(m) is Euclidean iffm =-1 , ±2, ±3, 5, 6, ±7,±11, 13, 1 7, 19, 21 , 29, 33, 37, 41 , 57 or 73.
   b). Let m> 0. Then R(-m) is a PID iffm = 1, 2, 3, 7, 1 1 , 19,43, 67 or 163

   where$R(m) = \begin{cases} Z\left(\sqrt{m}\right) \ if\ m \equiv 2\ or\ 3(mod4) \\ Z\left(\frac{1+\sqrt{m}}{2}\right) \ if\ m \equiv 1(mod4) \end{cases}$ m be a non-zero square free integer(positive or negative)

Definition: Factorisation Domain (F.D.)

A commutative integra domain R (with 1) is called a factorisation domain (FD) if every non-zero elements inR can be written as a unit times a finite product of irreducible elements.

Results:

1. Every PID is a factorisation domain

2. If d is a positive integer, then the ring $Z[i\sqrt{d}]$ is a factorisation domain.

Definition: Unique Factorisation Domain(U.F.D.)

A domain R is called a unique factorisation domain (UFD) if

1) R is a factorisation domain, i.e., every non-zero element can be factored into a unit times a finite product of irreducibles and

2) the factorisation into irreducibles is unique upto order and associates, i.e. , if $x \in R^*$ is factored as $x = u.p_1p_2 a_3 \dots p_r = vq_1q_2q_3 \dots q_s$. where u, v are units and p_i's, q_i's are irreducibles, then r = s and each $p_i$is an associate of a q_j and vice-versa.

Result:

1. In a UFD, x is irreducible element iff x is a prime.
2. Every UFD is an UFD
3. A domain R is a UFO if and only if R is an FD in which every irreducible element is a prime.
4. A domain R is a UFD if and only if every non-zero non-unit in R can be factored into a finite product of primes.
5. Every PID is a UFD.
6. Let R be a UFD .Then show that R is a P I D if every prime (resp .maximal) ideal is principal.
7. In a UFD any two irreducible are associates of each other.

Definition : Polynomial Ring

Let R be any Ring. The set $R[x] = \{a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \mid a_0, \dots, a_n \in R, n \in W\}$, form a ring with the binary operations "+"& "."called as the ring of polynomials with coefficients in R. Here x is an indeterminate .

Let $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$, and $g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m \in R[x]$ $\quad n>m$

$f(x) + g(x) = (a_0 + a_1x + a_2x^2 + \cdots + a_nx^n) + (b_0 + b_1x + b_2x^2 + \cdots + b_mx^m)$

$= (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \cdots + (a_m + b_m)x^m + a_nx^n + \cdots a_nx^n$

$f(x).g(x) = C_0 + C_1x + C_2x^2 + C_3x^3 + \dots + C_kx^k + \dots + C_{n+m}x^{n+m}$ where $C_k = \sum_{i=0}^{k} a_i b_{k-i}$

Examples :

1. Z[x],
2. Q[x],
3. IR[x]
4. $Z_p[x]$

Results:

1. If R is ID then R[x] also an ID
2. If R is field then R[x] is an IDbut not a field
3. If R is commutative then R[x] also commutative
4. If R has unity then then R[x] aso commutative
5. R is a subring of R[x]
6. If R is field then R[x] is ED
7. If R is field then R[x] is PID
8. If R is field then R[x] is UFD
9. If R is UFD then R[x] is UFD
10. If R is field then units of R[x] are the nonzero elements of R

Definition: Content of polynomial:

Given a non-zero polynomial f(X) in R[X] , the gcd of the coefficients of f(X) is called the content of f(X) and is denoted by c(f(X)) or simply c(f).

Primitive polynomial:

A non-zero polynomial f(X) is called primitive if its content is 1 , i.e., its coefficients are collectively coprime.

Irreducible Polynomial: A non-zero non-unit $f(x) \in R[x]$ is said to be irreducible iff$f(x)= g(x)h(x)$, then either g(x)or h(x)is a unit, i.e., f(x)cannot be written as a product of two non-units or equivalently, the only divisors of f(x)are its associates or units.

Examples

1. The polynomial $f(x)=2x^2+4$ is irreducible over Q but reducible over Z.
   Since $f(x)=2(x^2+2)$ but 2 is unit in Q $\Rightarrow$ f(x) is irreducible over Q
   but 2 is not unit in Z $\Rightarrow$ f(x) is reducible over Z
2. The polynomial $f(x)=2x^2+4$ is irreducible over IR but reducible over $\mathbb{C}$.
3. The polynomial $f(x)=x^2-2$ is irreducible over Q but reducible over IR.
4. The polynomial $f(x)=x^2+1$ is irreducible over Z_3 but reducible over Z_5.

Reducibility Tests

1. Let R be a field . If $f(x) \in R[x]$ and $\deg f(x)=2$ or 3 then $f(x)$ is reducible over R iff $f(x)$ has a zero in R

2. Let $f(x) \in Z[x]$. If $f(x)$ is reducible over Q then it is reducible over Z
3. Let p be a prime and suppose that $f(x) \in Z[x]$ with deg $f(x) \geq 1$. Let $\tilde{f}(x)$ be the polynomial in $Z_p[x]$ obtained from $f(x)$ by reducing all the coefficients of $f(x)$ modulo p. If $\tilde{f}(x)$ is irreducible over Z_p and deg$f(x)$=deg$\tilde{f}(x)$ then $f(x)$ is irreducibile over Q
4. Let $f(x)=a_0+ a_1x + a_2x^2+ \cdots + a_nx^n \in Z[x]$. If there is a prime p such that p / a_n, p / a_{n-1}, … p/a_0 and p^2/ a_0 then f(x) is irreducible over Q
5. For any prime p the pthcyclotomic polynomial $\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x + 1$ is irreducible over Q
6. Let R be a field and let $p(x) \in R[x]$. Then $\langle p(x) \rangle$ is a maximal ideal in R[x] iff p(x) is irreducible over R
7. Let R be a field and let $p(x), a(x), b(x) \in R[x]$. If p(x) is irreducible over R and p(x) / a(x)b(x) then p(x) /a(x) or p(x)/b(x)
8. Suppose that $f(x) \in Z_p[x]$ and is irreducible over Z_p , where p is a prime . If deg$f(x)$=n then $Z_p[x]/\langle f(x) \rangle$ is a field with p^n elements.

Let K be a finite field with $|K| = p^n$. The multiplicative group $K^* = K\backslash\{0\}$ is cyclic
Every finite field contains at least one primitive element.More precisely there are exactly $\phi(q - 1)$ primitive elements.

Let K be a finite field with $|K| = q$ elements. There exist elements of orderk if and only if $k|(q - 1)$.

Let $f(x) \in K[x]$ be irreducible and let L be the splitting field of fover K.
Let $\alpha \& \beta$ be roots of f(x) over L.
We have $K(\alpha) \cong K(\beta)$

Let $f, g \in IF_q[x]$ be irreducible, of the same degree deg(f) = deg(g). Then their splitting fields are isomorphic.

Let n be prime. An irreducible binomial $f(x) = x^n + a_0$ of degree n over IF_qexists if and only if $n|q - 1$.

Consider the elements ,in the subring $\mathbb{Z}[x2, x3]$ of $\mathbb{Z}[x]$ consisting of all finite sums of the form $\sum aij(x2)\, i(x3)\, j$, $aij \in \mathbb{Z}$. We see that $x2$ and $x3$ are both common divisors of $x5$ and $x6$, but neither of $x2$ or $x3$ divides the other (in $\mathbb{Z}[x2, x3]$). Thus, the gcd of $x5$ and $x6$ in $\mathbb{Z}[x2, x3]$ does not exist.