189/35 BEHIND RAILWAY STATION, VAISH COLLEGE ROAD, ROHTAK PIN-124001 (HARYANA)
E-mail us on - jrinstituterohtak@gmail.com, balwanmudgil54@gmail.com Mob. 8607383607, 9802177766

1.1 Definitions and Examples

Def. Ring : A non-empty set R is said to be a ring with respect to two operations denoted by ' + ' and ' $\cdot$ ' called addition and multiplication respectively if it satisfies the following axioms :

(i) Addition is closed : $a+b \in R$ for all $a,\ b \in R$.

(ii) Addition is associative : $(a+b)+c = a+(b+c)$ for all $a, b, c \in R$.

(iii) Existence of additive identity : There exists an element denoted by $0 \in R$ such that $a+0 = a = 0+a$ for all $a \in R$. This element 0 is known as additive identity or zero element in R.

(iv) Existence of additive inverse : For each $a \in R$, there exists an element $b \in R$ such that $a+b = 0 = b+a$. This element b is called additive inverse or negative of a and is denoted by $-a$.

(v) Addition is commutative : $a+b = b+a$ for all $a, b \in R$.

(vi) Multiplication is closed : $a \cdot b \in R$ for all $a,\ b \in R$.

(vii) Multiplication is associative : $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a,\ b,\ c \in R$.

(viii) Multiplication is distributive over addition : For all $a, b, c \in R$

$$a \cdot (b+c) = a \cdot b + a \cdot c \qquad \text{[Left distributivity]}$$

$$(a+b) \cdot c = a \cdot c + b \cdot c \qquad \text{[Right distributivity]}$$

Then we write that $(R, +, \cdot)$ is a ring.

Remarks :

(i) Out of eight properties of ring, it should be noted that first five properties are of addition , next two are of multiplication and last one is common i.e., it includes addition and multiplication both.

(ii) First five properties of above definition of a ring says that every ring R is an abelian group under addition or additive abelian group.

(iii) We usually denote $a \cdot b$ by ab.

(iv) The ring $R = \{0\}$ is called the trivial ring.

Def. Zero ring : Let $(R, +)$ be an additive abelian group. We define multiplication in R by $a \cdot b = 0$ for all $a, b \in R$, then $(R, +, \cdot)$ becomes a ring which is called zero ring. Therefore, by an abelian group we can always form a ring.

Def. Commutative ring : A ring in which $a \cdot b = b \cdot a$ for all $a, b \in R$ is called a commutative ring i.e., a ring is said to be commutative if it is commutative w.r.t. multiplication.

Def. Ring with unity : A ring $R \neq \{0\}$ is said to be a ring with unity if it contains multiplicative identity i.e., there exists an element denoted by $1 \in R$ such that $a \cdot 1 = a = 1 \cdot a$ for all $a \in R$.

Def. Division ring or Skew-field : A ring R is said to be a division ring or skew-field if

(i) R is with unity i.e. $1 \in R$.

(ii) Every non-zero element of R has a multiplicative inverse i.e., for every non-zero element $a \in R$ there exists an element $b \in R$ such that $a \cdot b = b \cdot a = 1$. We usually denote multiplicative inverse of a by a^{-1}.

Def. Field : A commutative division ring is called a field. In other words, a commutative ring with unity in which every non-zero element has a multiplicative inverse is called a field.

Remarks :

(i) It should be noted that a field has total eleven properties , out of which five are of addition , five are of multiplication and one property is common.

(ii) A field is an abelian group under addition and non-zero elements of a field form an abelian group under multiplication.

(iii) Sometimes we write CRU in place of commutative ring with unity.

(iv) A field has atleast two elements.

Def. Zero divisor : A non-zero element 'a' of a ring R is called an zero divisor if there exists a non-zero element $b \in R$ such that $a\,b = 0$ or $b\,a = 0$.

Def. Ring with zero divisors : A ring which contains zero divisors is called a ring with zero divisors.

Def. Ring without zero divisors : A ring in which no zero divisor exists is called a ring without zero divisors.

OR

A ring R is said to be without zero divisors if $ab = 0 \Rightarrow a = 0$ or $b = 0$

OR

A ring is called without zero divisors if product of any two non - zero elements is always non- zero.

Def . Integral Domain : A commutative ring with unity and without zero divisors is called an integral domain.

Remark : Some authors do not take unity in the definition of integral domain. For instance, Joseph A. Gallian takes unity in the definition of integral domain, while I.N. Herstein does not take unity in the definition of integral domain.

Results : If R is a ring then for all $a, b, c \in R$, we have

1. $a + b = a + c \Rightarrow b = c$
2. $-(-a) = a$
3. The zero element of R is unique.
4. The additive inverse of any element in R is unique.

189/35 BEHIND RAILWAY STATION, VAISH COLLEGE ROAD, ROHTAK PIN-124001 (HARYANA)
E-mail us on - jrinstituterohtak@gmail.com, balwanmudgil54@gmail.com Mob. 8607383607, 9802177766

5. $a \cdot 0 = 0 \cdot a = 0$
6. $a(-b) = -(ab)$
7. $(-a)b = -(ab)$
8. $(-a)(-b) = ab$
9. $a(b-c) = ab - ac$
10. $(b-c)a = ba - ca$
11. If n is an integer then $n(-a) = -(na)$
12. If n is an integer then $n(ab) = (na)b = a(nb)$
13. If m and n are two integers then $(ma)(nb) = (mn)(ab)$

    Further, if R has a unity element 1, then
14. $(-1)a = -a$
15. $(-1)(-1) = 1$
16. Unity is unique.
17. Multiplicative inverse of a non-zero element, if exists, is unique.

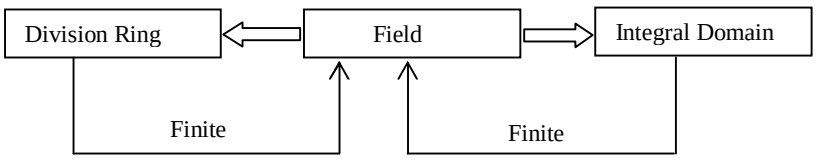
Results :

1. A commutative ring R with unity is an integral domain iff cancellation laws holds in R.
2. A division ring is always without zero divisors.
3. A field is always without zero divisors.
4. A field is always an integral domain.
5. A ring with zero divisors cannot be an integral domain and field.
6. **Wedderburn's theorem :**

(i) Every finite commutative ring without zero divisors is a field.

(ii) Every finite integral domain is a field. But an infinite integral domain may or may not be a field.

(iii) Every finite division ring is a field. But an infinite divison ring may or may not be a field.



Def. Unit : Let $(R,+,\cdot)$ be a ring with unity and $a \in R$. Then, a is said to be unit element of R if there exists $b \in R$ such that $a \cdot b = b \cdot a = 1$. In other words, a non zero element of a ring which has multiplicative inverse is called a unit.

Remark : Unity is always a unit but every unit is not a unity.

Def. U(R) : The set of all units of a ring R is denoted by $U(R)$.

Def. Idempotent element : An element 'a' of a ring $(R,+,\cdot)$ is said to be idempotent if $a \cdot a = a$ i.e., $a^2 = a$.

Def. Boolean Ring : A ring $(R,+,\cdot)$ in which every element is an idempotent is called a Boolean ring.

Def. Nilpotent element : An element a of a ring $(R,+,\cdot)$ is said to be nilpotent if there exists a positive integer n such that $a^n = 0$.

Def. Additive order of an element : Let R be a ring and $a \in R$ be any element. The additive order of a is defined to be the smallest positive integer n (if exists) such that $n \cdot a = 0$. If no such positive integer exist then order of a is defined to be infinity.

Def. Characteristic of a ring : The smallest positive integer n such that $n \cdot a = 0$ for all $a \in R$ is called the characteristic of a ring R. If no such positive integer exist then characteristic of R is said to be zero .

Def. Direct product of rings : Let $R_1, R_2, ..., R_n$ be any rings then their direct product $R_1 \times R_2 \times ..... \times R_n = \{(a_1, a_2, ..., a_n) : a_i \in R_i\}$ is a ring under componentwise addition and multiplication.

Def. Polynomial Ring : Let R be a ring then the set $R[x] = \{a_0 + a_1 x + a_2 x^2 + ... + a_n x^n : a_i \in R$ and n is a non – negative integer$\}$ forms a ring with respect to addition and multiplication of polynomials.

Def. Polynomial ring in two variables : Let R be a ring then the set $R[x,y] = R[x][y] = \{a_0 + a_1 y + a_2 y^2 + ... + a_n y^n : a_i \in R[x]$ and n is a non – negative integer$\}$ forms a ring with respect to addition and multiplication of polynomials.

Results : Let R be a ring and $R[x]$ be its polynomial ring then the following results hold :

1. If R is with unity then the polynomial ring $R[x]$ is also with unity.
2. If R is commutative, then the polynomial ring $R[x]$ is also commutative.
3. If R is without zero divisors then the polynomial ring $R[x]$ is also without zero divisors.
4. If R is with zero divisors then the polynomial ring $R[x]$ is also with zero divisors.
5. If R is an integral domain then the polynomial ring $R[x]$ is also an integral domain.

189/35 BEHIND RAILWAY STATION, VAISH COLLEGE ROAD, ROHTAK PIN-124001 (HARYANA)
E-mail us on - jrinstituterohtak@gmail.com, balwanmudgil54@gmail.com Mob. 8607383607, 9802177766

6. If R is a field then the polynomial ring $R[x]$ is never a field.

7. The polynomial rings $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$, $\mathbb{Z}_p[x]$ all are integral domain but not a field.

Results on commutative ring :

1. If R is commutative ring then $(xy)^2 = x^2y^2 \ \forall\ x, y \in R$ but the converse may not be true.

   e.g., Let $R = \left\{\begin{bmatrix} 0 & a \\ 0 & b \end{bmatrix} : a, b \in \mathbb{Z}\right\}$, then $(R, +, \cdot)$ is a non-commutative ring but $(xy)^2 = x^2y^2 \ \forall\ x, y \in R$

2. If R is a ring with unity and $(xy)^2 = x^2y^2 \ \forall\ x, y \in R$, then R is commutative.
3. Any ring of prime order is commutative.
4. A ring with unity and of order p^2, where p is prime, is commutative.
5. A Boolean ring is always commutative.

Results on characteristic of a ring :

1. $\text{Ch}(\mathbb{Z}_n) = n$.
2. $\text{Ch}(M_m(\mathbb{Z}_n)) = n$
3. $\text{Ch}(\mathbb{Z}_m \times \mathbb{Z}_n) = \text{lcm}(m, n)$
4. The additive order of each non zero element of an integral domain is same and is equal to the characteristic.
5. Let R be a ring with unity 1. If additive order of 1 is infinity then characteristic of R is 0 and if additive order of 1 is n then characteristic of R is n.
6. Characteristic of a finite ring is always non-zero.
7. Characteristic of an infinite ring may be zero or non zero. e.g. $\text{Ch}(\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}) = 0$, $\text{Ch}(\mathbb{Z}_n[x]) = n$
8. If characteristic of a ring is zero then the ring is infinite.
9. If characteristic of a ring is non zero then the ring may be finite or infinite. e.g., $\mathbb{Z}_n$ and $\mathbb{Z}_n[x]$.
10. Characteristic of any integral domain (and hence of a field) is either zero or a prime number.
11. Characteristic of a non-zero Boolean ring is always 2.

Results :

1. If F is a field then $U(F) = F - \{0\} = F^*$
2. $U(\mathbb{Z}_m \times \mathbb{Z}_n) = U(\mathbb{Z}_m) \times U(\mathbb{Z}_n)$
3. In an integral domain there are only two idempotent elements 0 and 1 and one nilpotent element 0.

4. If a is an idempotent element in $\mathbb{Z}_n$ then $1-a$ is also an idempotent element.

5. If n is composite then $\mathbb{Z}_n$ is with zero divisors and therefore not an integral domain and hence not a field.

6. $\mathbb{Z}_p$ is a field iff p is prime.

7. If $d>1$ is a positive integer such that d is not a perfect square, then $\mathbb{Z}(\sqrt{d})=\left\{a+b\sqrt{d}:a,b\in\mathbb{Z}\right\}$ is an integral domain but not a field.

8. If $d>1$ is a positive integer which is not a perfect square then $\mathbb{Q}(\sqrt{d})=\left\{a+b\sqrt{d}:a,b\in\mathbb{Q}\right\}$ is a field.

9. If p is prime then $\mathbb{Q}(\sqrt{p})$ is a field.

10. $\mathbb{Z}_p[i]$ is a field iff p is a prime of the form $4k+3$, where k is a non-negative integer.

11. In a finite CRU every non-zero element is either a unit or a zero divisor.

12. If $n=p_1^{k_1}\cdot p_2^{k_2}\cdots p_r^{k_r}$ then the number of idempotent elements in $\mathbb{Z}_n$ is 2^r where r is the number of distinct prime factors of n.

13. If $n=p_1^{k_1}\cdot p_2^{k_2}\cdots p_r^{k_r}$ then the number of nilpotent elements in $\mathbb{Z}_n$ is $p_1^{k_1-1}\cdot p_2^{k_2-1}\cdots\cdots p_r^{k_r-1}$ or $\dfrac{n}{p_1\cdot p_2\cdots p_r}$.

Exercise 1.1

1. Which of the following are rings. Which of them are commutative, with unity, integral domain, division ring, field under usual addition and multiplication. Also find their units, characteristic, idempotent and nilpotent elements :

   (i) $\mathbb{Z}$ (ii) $\mathbb{Q}$ (iii) $\mathbb{R}$ (iv) $\mathbb{C}$ (v) $2\mathbb{Z}$

   (vi) $\mathbb{Z}(i)$ (vii) $\mathbb{Z}\left(\sqrt{2}\right)$ (viii) $\mathbb{Q}\left(\sqrt{2}\right)$ (ix) $\mathbb{Q}(i)$

2. Which of the following are rings. Which of them are commutative, with unity, integral domain, division ring, field under modulo addition and multiplication. Also find their units, characteristic, idempotent and nilpotent elements :

   (i) $\mathbb{Z}_6$ (ii) $\mathbb{Z}_7$ (iii) $\mathbb{Z}_8$ (iv) $\mathbb{Z}_{11}$ (v) $\mathbb{Z}_2[i]$ (vi) $\mathbb{Z}_3[i]$

3. Which of the following are rings. Which of them are commutative, with unity, integral domain, division ring, field under matrix addition and multiplication.

   (i) $M_2(\mathbb{Z})$ (ii) $M_2(2\mathbb{Z})$ (iii) $M_2(\mathbb{Q})$ (iv) $M_2(\mathbb{R})$ (v) $M_2(\mathbb{C})$

   (vi) $M_2(\mathbb{Z}_2)$ (vii) $M_2(\mathbb{Z}_3)$ (viii) $\left\{A\in M_2(\mathbb{R}):|A|=1\right\}$

   (ix) $\left\{A\in M_2(\mathbb{R}):|A|\text{ is a rational number}\right\}$

189/35 BEHIND RAILWAY STATION, VAISH COLLEGE ROAD, ROHTAK PIN-124001 (HARYANA)
E-mail us on - jrinstituterohtak@gmail.com, balwanmudgil54@gmail.com Mob. 8607383607, 9802177766

4. Which of the following are rings. Which of them are commutative, with unity, integral domain, division ring, field under usual addition and multiplication. Also find their units, characteristic, idempotent and nilpotent elements :

   (i) $\mathbb{Z}[x]$ (ii) $\mathbb{Q}[x]$ (iii) $\mathbb{R}[x]$ (iv) $\mathbb{C}[x]$ (v) $\mathbb{Z}_2[x]$ (vi) $\mathbb{Z}_4[x]$

   (vii) $\mathbb{Z}[x,y]$ (viii) $\mathbb{Q}[x,y]$ (ix) $\mathbb{R}[x,y]$ (x) $\mathbb{C}[x,y]$ (xi) $\mathbb{Z}_2[x,y]$ (xii) $\mathbb{Z}_4[x,y]$

5. Which of the following are rings. Which of them are commutative, with unity, integral domain, division ring, field under usual addition and multiplication. Also find their units, characteristic, idempotent and nilpotent elements :

   (i) $\mathbb{Z}\times\mathbb{Z}$ (ii) $\mathbb{Z}\times\mathbb{Q}$ (iii) $\mathbb{Q}\times\mathbb{Q}$ (iv) $\mathbb{Z}_2\times\mathbb{Z}_3$

6. Let X be a non empty set and $\mathbb{R}^X$ denotes the set of all functions $f : X \to \mathbb{R}$, then $\mathbb{R}^X$ is a ring under addition and multiplication of functions defined by $(f+g)(x) = f(x)+g(x)$ and $(f\cdot g)(x) = f(x)\cdot g(x)$.

7. What are the units in the ring $\mathbb{R}^{\mathbb{R}}$.

8. Let $C[a,b]$ denote the set of all real valued continuous function defined on $[a,b]$. Show that $C[a,b]$ is a commutative ring, with unity and with zero divisors w.r.t. usual addition and multiplication of functions. What are the units, idempotents and nilpotents of this ring.

9. Let $H(\mathbb{C})$ denotes the set of all entire functions defined on the complex plane $\mathbb{C}$, then show that $H(\mathbb{C})$ is an integral domain w.r.t. ordinary addition and multiplication of functions. Further show that units of $H(\mathbb{C})$ are nowhere vanishing entire functions.

10. Which of the following functions $f : \mathbb{C} \to \mathbb{C}$ are units in the ring $H(\mathbb{C})$:

    (i) $f(z) = k,\ k \neq 0$ (ii) $f(z) = z$ (iii) $f(z) = \sin z$

    (iv) $f(z) = e^z$ (v) $f(z) = e^{\sin z}$ (vi) $f(z) = e^{z^2}$

11. Let $R = \left\{ \begin{bmatrix} z_1 & z_2 \\ -\overline{z}_2 & \overline{z}_1 \end{bmatrix} : z_1, z_2 \in \mathbb{C} \right\}$ then show that R is a division ring but not a field.

12. Let $R = \{a+bi+cj+dk : a,b,c,d \in \mathbb{R}\}$ where the symbols i, j, k are connected by the relations $i^2 = j^2 = k^2 = ijk = -1$, $ij = k$, $jk = i$, $ki = j$, $ji = -k$, $kj = -i$, $ik = -j$. Show that R is a division ring but not a field under formal addition and multiplication.

This ring is known as the **ring of quaternions**.

13. Let $R=\{a+bi+cj+dk : a,b,c,d \in \mathbb{Z}_3\}$ where the symbols i, j, k are connected by the relations $i^2=j^2=k^2=ijk=-1$, $ij=k$, $jk=i$, $ki=j$, $ji=-k$, $kj=-i$, $ik=-j$. Show that R is not an integral domain under formal addition and multiplication modulo 3.
14. Show that $R=\left\{\begin{bmatrix} a & a \\ a & a \end{bmatrix} : a \in \mathbb{R}\right\}$ is a field under usual matrix addition and multiplication.
15. Show that $R=\left\{\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} : a \in \mathbb{R}\right\}$ is a field under usual matrix addition and multiplication.
16. Show that $R=\left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} : a,b,c,d \in \mathbb{Z}\right\}$ is a ring under matrix addition and componentwise matrix multiplication. What are the units of this ring.
17. Let a be a non-zero element of a ring R then prove that a cannot be both unit and zero divisor. Give an example of a ring in which there exist elements which are neither unit nor zero divisors.
18. Let R be finite CRU. Prove that every non-zero element of R is either a zero divisor or a unit. What happens if we drop the finiteness condition on R.
19. List all zero divisors in $\mathbb{Z}_{20}$. Can you see a relationship between the zero divisors of $\mathbb{Z}_{20}$ and the units of $\mathbb{Z}_{20}$?
20. Find a non-zero element in a ring that is neither a zero-divisor nor a unit.
21. Describe all zero-divisors and units of $\mathbb{Z}\times\mathbb{Q}\times\mathbb{Z}$.
22. Give an example of a commutative ring without zero-divisors that is not an integral domain.
23. Find two elements a and b in a ring such that both a and b are zero-divisors, $a+b\neq 0$ and $a+b$ is not a zero divisor.
24. Determine all elements of a ring that are both units and idempotents.
25. Find the characteristic of $\mathbb{Z}_4\times 4\mathbb{Z}$.
26. Let $X=\{a,b,c\}$ and $P(X)$ denotes the power set of X. Prove that $(P(X), \cap, \Delta)$ is not a ring.
27. Let $X=\{a,b,c\}$ and $P(X)$ denotes the power set of X. Prove that $(P(X), \Delta, \cap)$ is a Boolean ring. What are the units of this ring.
28. Let R be a CRU, then all the units of R form an abelian group with respect to multiplication of R.
29. Let $R=\{0,3,6\}$ then show that $(R, +_9, \times_9)$ is a zero ring.
30. What is the number of zero divisors in the rings $\mathbb{Z}_{49}$ and $\mathbb{Z}_7\times\mathbb{Z}_7$.

Answers

1. (i) Commutative ring with unity, integral domain, not a division ring, not a field, $U(\mathbb{Z})=\{1,-1\}$, idempotent elements $=\{0,1\}$, nilpotent element $=\{0\}$, $\mathrm{Ch}(\mathbb{Z})=0$.

   (ii) Commutative ring with unity, integral domain, division ring, field, $U(\mathbb{Q})=\mathbb{Q}^*=\mathbb{Q}-\{0\}$, idempotent elements $=\{0,1\}$, nilpotent element $=\{0\}$, $\mathrm{Ch}(\mathbb{Q})=0$.

   (iii) Commutative ring with unity, integral domain, division ring, field, $U(\mathbb{R})=\mathbb{R}-\{0\}$, idempotent elements $=\{0,1\}$, nilpotent element $=\{0\}$, $\mathrm{Ch}(\mathbb{R})=0$.

   (iv) Commutative ring with unity, integral domain, division ring, field, $U(\mathbb{C})=\mathbb{C}-\{0\}$, idempotent elements $=\{0,1\}$, nilpotent element $=\{0\}$, $\mathrm{Ch}(\mathbb{C})=0$.

   (v) Commutative ring without unity, not an integral domain, not a division ring, not a field, $U(2\mathbb{Z})=\phi$, idempotent element $=\{0\}$, nilpotent element $=\{0\}$, $\mathrm{Ch}(2\mathbb{Z})=0$.

   (vi) Commutative ring with unity, integral domain, not a division ring, not a field, $U(\mathbb{Z}(i))=\{1,-1,i,-i\}$, idempotent elements $=\{0,1\}$, nilpotent element $=\{0\}$, $\mathrm{Ch}(\mathbb{Z}(i))=0$.

   (vii) Commutative ring with unity, integral domain,not a division ring, not a field, $U\left(\mathbb{Z}\left(\sqrt{2}\right)\right)=\left\{a+b\sqrt{2}:a^2-2b^2=\pm 1,\ a,b\in\mathbb{Z}\right\}$, idempotent elements $=\{0,1\}$, nilpotent element $=\{0\}$, $\mathrm{Ch}\left(\mathbb{Z}\left(\sqrt{2}\right)\right)=0$.

   (viii) Commutative ring with unity, integral domain, division ring, field, $U\left(\mathbb{Q}\left(\sqrt{2}\right)\right)=\mathbb{Q}\left(\sqrt{2}\right)-\{0\}$, idempotent elements $=\{0,1\}$, nilpotent element $=\{0\}$, $\mathrm{Ch}\left(\mathbb{Q}\left(\sqrt{2}\right)\right)=0$.

   (ix) Commutative ring with unity, integral domain, division ring , field, $U(\mathbb{Q}(i))=\mathbb{Q}(i)-\{0\}$, idempotent elements $=\{0,1\}$, nilpotent element $=\{0\}$, $\mathrm{Ch}(\mathbb{Q}(i))=0$.

2. (i) Commutaive ring with unity, not an integral domain, not a division ring, not a field, $U(\mathbb{Z}_6)=\{1,5\}$, idempotent elements $=\{0,1,3,4\}$, nilpotent element $=\{0\}$, $\mathrm{Ch}(\mathbb{Z}_6)=6$.

   (ii) Commutiative ring with unity, integral domain, division ring, field, $U(\mathbb{Z}_7)=\mathbb{Z}_7-\{0\}$, idempotent elements $=\{0,1\}$, nilpotent element $=\{0\}$, $\mathrm{Ch}(\mathbb{Z}_7)=7$.

   (iii) Commutative ring with unity, not an integral domain, not a division ring, not a field,

$U(\mathbb{Z}_8)=\{1,3,5,7\}$, idempotent elements $=\{0,1\}$, nilpotent element $=\{0,2,4,6\}$, $\text{Ch}(\mathbb{Z}_8)=8$.

(iv) Commutative ring with unity, integral domain, division ring, field, $U(\mathbb{Z}_{11})=\mathbb{Z}_{11}-\{0\}$,

idempotent elements $=\{0,1\}$, nilpotent element $=\{0\}$, $\text{Ch}(\mathbb{Z}_{11})=11$

(v) Commutative ring with unity, not an integral domain, not a division ring, not a field,

$U(\mathbb{Z}_2[i])=\{1,i\}$, idempotent elements $=\{0,1\}$, nilpotent element $=\{0,1+i\}$, $\text{Ch}(\mathbb{Z}_2[i])=2$.

(vi) Commutative ring with unity, integral domain, division ring, field, $U(\mathbb{Z}_3[i])=\mathbb{Z}_3[i]-\{0\}$,

idempotent elements $=\{0,1\}$, nilpotent element $=\{0\}$, $\text{Ch}(\mathbb{Z}_3[i])=3$.

3. (i) Non-commutative ring with unity, not an integral domain, not a division ring, not a field.

(ii) Non-commutative ring without unity, not an integral domain, not a division ring, not a field.

(iii) Non-commutative ring with unity, not an integral domain, not a division ring, not a field.

(iv) Non-commutative ring with unity, not an integral domain, not a division ring, not a field.

(v) Non-commutative ring with unity, not an integral domain, not a division ring, not a field.

(vi) Non-commutative ring with unity, not an integral domain, not a division ring, not a field.

(vii) Non-commutative ring with unity, not an integral domain, not a division ring, not a field.

(viii) Not a ring.

(ix) Not a ring.

4. (i) Commutative ring with unity, integral domain, not a division ring, not a field,

$U(\mathbb{Z}[x])=\{1,-1\}$, idempotent elements $=\{0,1\}$, nilpotent element $=\{0\}$, $\text{Ch}(\mathbb{Z}[x])=0$.

(ii) Commutative ring with unity, integral domain, not a division ring, not a field,

$U(\mathbb{Q}[x])=\mathbb{Q}-\{0\}$, idempotent elements $=\{0,1\}$, nilpotent element $=\{0\}$, $\text{Ch}(\mathbb{Q}[x])=0$.

(iii) Commutative ring with unity, integral domain, not a division ring, not a field,

$U(\mathbb{R}[x])=\mathbb{R}-\{0\}$, idempotent elements $=\{0,1\}$, nilpotent element $=\{0\}$, $\text{Ch}(\mathbb{R}[x])=0$.

(iv) Commutative ring, integral domain, not a division ring, not a field, $U(\mathbb{C}[x])=\mathbb{C}-\{0\}$,

idempotent elements $=\{0,1\}$, nilpotent element $=\{0\}$, $\text{Ch}(\mathbb{C}[x])=0$.

(v) Commutative ring with unity, integral domain, not a division ring, not a field, $U(\mathbb{Z}_2[x])=\{1\}$,

idempotent elements $=\{0,1\}$, nilpotent element $=\{0\}$, $\text{Ch}(\mathbb{Z}_2[x])=2$.

(vi) Commutative ring with unity, not an integral domain, not a division ring, not a field,

$U(\mathbb{Z}_4[x])=\{1,3\}$, idempotent elements $=\{0,1\}$, nilpotent elements $=\{0,2\}$, $\text{Ch}(\mathbb{Z}_4[x])=4$.

5. (i) Commutative ring with unity, not an integral domain, not a division ring, not a field,

$U(\mathbb{Z}\times\mathbb{Z})=\{(1,1),(1,-1),(-1,1),(-1,-1)\}$, idempotent elements $=\{(0,0),(1,1),(0,1),(1,0)\}$,

nilpotent element $=\{(0,0)\}$, $\mathrm{Ch}(\mathbb{Z}\times\mathbb{Z})=0$.

(ii) Commutative ring with unity, not an integral domain, not a division ring, not a field,

$U(\mathbb{Z}\times\mathbb{Q})=\{(m,n):m=\pm1,n\in\mathbb{Q}\}$, idempotent elements $=\{(0,0),(1,0),(0,1),(1,1)\}$,

nilpotent element $=\{(0,0)\}$, $\mathrm{Ch}(\mathbb{Z}\times\mathbb{Q})=0$.

(iii) Commutative ring with unity, not an integral domain, not a division ring, not a field,

$U(\mathbb{Q}\times\mathbb{Q})=\{(m,n):m,n\neq0,\ m,n\in\mathbb{Q}\}$, idempotent elements $=\{(0,0),(1,0),(0,1),(1,1)\}$,

nilpotent element $=\{(0,0)\}$, $\mathrm{Ch}(\mathbb{Q}\times\mathbb{Q})=0$.

(iv) Commutative ring with unity, not an integral domain, not a division ring, not a field,

$U(\mathbb{Z}_2\times\mathbb{Z}_3)=\{(1,1),(1,2)\}$, idempotent elements $=\{(0,0),(1,0),(0,1),(1,1)\}$,

nilpotent element $=\{(0,0)\}$, $\mathrm{Ch}(\mathbb{Z}_2\times\mathbb{Z}_3)=6$

19. $\{2,4,5,6,8,10,12,14,15,16,18\}$ are the zero divisors in $\mathbb{Z}_{20}$ and every non zero element not in this list is a unit. Thus, zero divisors in $\mathbb{Z}_{20}$ are the non zero non units.

20. In $2\mathbb{Z}$, every element is neither a zero-divisor nor a unit.

21. (a,b,c) (at least one of a,b and c is zero and not all zero) are zero divisors and $(\pm1,b,\pm1),b\neq0$ are units.

22. $2\mathbb{Z}$ 23. In $\mathbb{Z}_6$, $a=2$ and $b=3$ 24. $a=1$ 25. 0

1.2 Subrings and Ideals

Def. Subring : Let R be a ring. A non-empty subset S of R is said to be a subring of R if S itself is a ring under the same binary operations as in R.

Any subring S of R is said to be a proper subring of R if $S\neq R$. Also, $\{0\}$ is known as trivial subring.

Result : A non-empty subset S of a ring R is a subring of R if and only if

(i) $a-b\in S$ for all $a,b\in S$ i.e. S is an additive subgroup of R.

(ii) $ab\in S$ for all $a,b\in S$.

Def. Left ideal : A non – empty subset S of a ring R is called a left ideal of R if

(i) $a-b\in S$ for all $a,b\in S$

(ii) $ra\in S$ for all $a\in S$, $r\in R$.

Def. Right ideal : A non – empty subset S of a ring R is called a right ideal of R if

(i) $a-b \in S$ for all $a,b \in S$

(ii) $ar \in S$ for all $a \in S$, $r \in R$.

Def. Ideal : A non-empty subset S of a ring R is called a both-sided ideal or simply, an ideal of R if it is left ideal as well as right ideal of R.

Equivalently, A non-empty subset S of a ring R is called an ideal of R if

(i) $a-b \in S$ for all $a,b \in S$

(ii) $ar \in S$ and $ra \in S$ for all $a \in S$, $r \in R$.

Remarks :

1. In a commutative ring every left ideal or right ideal is a both-sided ideal.
2. An ideal A of a ring R is called a proper ideal if $A \neq R$. Further , zero ideal $\{0\}$ is also called trivial ideal or zero ideal.
3. Every left ideal, right ideal and ideal is always a subring.
4. Every subring need not be an ideal.

Def. Sum of two ideals : Let A and B are two ideals of a ring R then their sum is defined as

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

Def. Ideal generated by a subset : Let S be any subset of a ring R. Then ideal generated by S is denoted by $\langle S \rangle$ and is defined to be the smallest ideal containing S

or

An ideal I of a ring is said to be generated by a subset S if

(i) $S \subseteq I$

(ii) If A is any ideal of R such that $S \subseteq A$, then $I \subseteq A$. Then we write $I=\langle S \rangle$.

Def. Product of two ideals : If A and B are two ideals of a ring R then their product is denoted by AB and is defined as $AB=\left\{\sum_{\text{finite}} a_i b_i \ : \ a_i \in A, b_i \in B\right\}$ i.e. AB contains the finite sums of the products of the pairs of elements taken first from A and second from B.

Def. Co maximal ideals : Two ideals A and B of R are said to be co-maximal if $A+B=R$.

Def. Centre of a ring : Let R be a ring then its centre denoted by $Z(R)$ and is defined as

$$Z(R)=\{r \in R : xr=rx \text{ for all } x \in R\}$$

Def. Right annihilator of an element : Let R be a ring and $a \in R$ be any element. Then, right annihilator of 'a' is denoted by $r(a)$, and is defined as

$$r(a)=\{r \in R : ar=0\}$$

189/35 BEHIND RAILWAY STATION, VAISH COLLEGE ROAD, ROHTAK PIN-124001 (HARYANA)
E-mail us on - jrinstituterohtak@gmail.com, balwanmudgil54@gmail.com Mob. 8607383607, 9802177766

In words , we can say that right annihilator of 'a' is the collection of all those elements of ring which when multiplied with 'a' on the right hand side gives zero.

Def. Left annihilator of an element : Let R be a ring and $a \in R$ be any element. Then, left annihilator of 'a' is denoted by $l(a)$, and is defined as

$$l(a) = \{r \in R : ra = 0\}$$

In words , we can say that left annihilator of 'a' is the collection of all those elements of ring which when multiplied with 'a' on the left hand side gives zero.

Results (A) : Algebra of ideals :

1. The intersection of any two left ideals of a ring is a left ideal of the ring.
2. An arbitrary intersection of left ideals of a ring is again a left ideal of the ring.
3. If A is a left ideal and B is a right ideal then $A \cap B$ is neither a left nor a right ideal, in general.
4. If A and B are two ideals of a ring R then $A \cup B$ is an ideal of R if and only if either $A \subseteq B$ or $B \subseteq A$.
5. If A and B are two ideals of a ring R then $A + B$ is also an ideal of R.
6. If A and B are two ideals of a ring R then A is an ideal of $A + B$.
7. If A and B are two ideals of a ring R then $A \cap B$ is an ideal of A, B and R.
8. Let R be a ring and $a \in R$ be any element then the ideal generated by a is denoted by $\langle a \rangle$ and is given by $\langle a \rangle = \left\{ \sum_{\text{finite sum}} r_i a s_i + ra + as + na : r, s, r_i, s_i \in R \text{ and } n \in \mathbb{Z} \right\}$.

   Sometimes this is denoted by $\langle a \rangle = RaR + Ra + aR + a\mathbb{Z}$.
9. If R is a ring with unity then $\langle a \rangle = RaR$.
10. If R is a commutative ring then $\langle a \rangle = Ra + a\mathbb{Z} = aR + a\mathbb{Z}$.
11. If R is a CRU then $\langle a \rangle = aR = Ra$.
12. If A and B are two ideals of a ring R then $A + B = \langle A \cup B \rangle$ i.e. $A + B$ is the smallest ideal containing $A \cup B$.
13. If A and B are two ideals of a ring R then their product AB is also an ideal of R.
14. If A is a left ideal and B is a right ideal of a ring R, then
    (i) AB is a two – sided ideal of R.
    (ii) BA need not be even a single sided ideal of R.

15. If A and B are two ideals of a ring R then $AB \subseteq A \cap B$ and $AB \subseteq A + B$.

16. Let A and B are two ideals of a CRU R such that $A + B = R$ then $AB = A \cap B$.

or

If A and B are co-maximal ideals of a commutative ring with unity then $AB = A \cap B$.

17. For the illustration of above result we can consider $2\mathbb{Z}$ and $3\mathbb{Z}$ in $\mathbb{Z}$. We see that $2\mathbb{Z} + 3\mathbb{Z} = \mathbb{Z}$ and $2\mathbb{Z} \cap 3\mathbb{Z} = (2\mathbb{Z})(3\mathbb{Z}) = 6\mathbb{Z}$.

Results (B) : Ideals in division rings and fields :

1. If U is an ideal of a ring R with unity such that $1 \in U$ then $U = R$. In words, if an ideal contains unity, then it is equal to the whole ring. We can also say that a proper ideal of a ring with unity cannot contain the unity element.
2. If U is an ideal of a ring R with unity such that U contains an unit of R then $U = R$. In words, if an ideal contains unit, then it is equal to the whole ring. We can also say that a proper ideal of a ring with unity cannot contain the unit element.

Def. Simple ring : A ring R is said to be a simple ring if it has no non-trivial proper ideals i.e., the only ideals of R are $\{0\}$ and R.

3. Let F be any field then $\{0\}$ and F are only ideals of F. In words, a field has no non-trivial proper ideals i.e., a field is always a simple ring.
4. Let R be a commutative ring with unity whose only ideals are $\{0\}$ and R then R is a field. In words, a commutative ring with unity which has no non-trivial proper ideals is a field. We can also say that a simple CRU is a field.
5. A commutative ring R with unity is a field iff it has no non-trivial proper ideals i.e., a CRU is a field iff it is a simple ring.
6. A division ring has no non-trivial proper ideals i.e., a division ring is always a simple ring.
7. Let R be a ring with unity such that R has no right ideals except $\{0\}$ and R, then R is a division ring.

Results (C) : Ideals in $\mathbb{Z}$ and $\mathbb{Z}_n$:

1. Ideals of $\mathbb{Z}$: Every ideal of $\mathbb{Z}$ is of the form $n\mathbb{Z}$ where n is an integer. In other words, $n\mathbb{Z}$, where n is an integer, are the only ideals of $\mathbb{Z}$.
2. The ideal $n\mathbb{Z}$ is the smallest ideal containing n, so we can also denote it by $\langle n \rangle$ i.e., $n\mathbb{Z} = \langle n \rangle$.
3. Subrings and ideals of $\mathbb{Z}$ are same.

189/35 BEHIND RAILWAY STATION, VAISH COLLEGE ROAD, ROHTAK PIN-124001 (HARYANA)
E-mail us on - jrinstituterohtak@gmail.com, balwanmudgil54@gmail.com Mob. 8607383607, 9802177766

4. If m and n are two distinct integers then

   (i) $m\mathbb{Z}+n\mathbb{Z}=\left[\text{g.c.d.}(m,n)\right]\cdot\mathbb{Z}$ (ii) $(m\mathbb{Z})\cap(n\mathbb{Z})=\left[\text{l.c.m.}(m,n)\right]\cdot\mathbb{Z}$

   (iii) $(m\mathbb{Z})\cdot(n\mathbb{Z})=mn\mathbb{Z}$ (iv) $m\mathbb{Z}\subseteq n\mathbb{Z}$ iff n divides m

5. Ideals of $\mathbb{Z}_n$: We know that $\mathbb{Z}_n$ is a cyclic group w.r.t. addition. Also we know that every subgroup of a cyclic group is cyclic. If we consider $\mathbb{Z}_n$ as a ring, then all cyclic subgroups of $\mathbb{Z}_n$ are the only subrings and ideals.

Results (D) : Unity and characteristic of subrings :

1. Subring of a ring with unity may be without unity. e.g., take $R=\mathbb{Z}$ and $S=2\mathbb{Z}$
2. Let S be a subring of a ring R with unity such that S is also with unity then the unity of S may or may not be same as that of R. e.g. consider $R=\mathbb{Q}$, $S=\mathbb{Z}$ and $R=\mathbb{Z}_6$, $S=\{0,2,4\}$.
3. If characteristic of ring is non-zero then characteristic of its subring is also non-zero.
4. Let S be a subring of ring R with unity and $\text{ch}(R)\neq 0$ then

   (i) If unity of S is same as that of R then $\text{ch}(S)=\text{ch}(\text{R})$

   (ii) If unity of S is either different from that of R or it does not exist then $\text{ch}(S)$ divides $\text{ch}(R)$.
5. Subring of a commutative ring is always commutative . However, subring of a non-commutative ring may or may not be commutative.

Exercise 1.2

1. Prove that the set of even integers is a subring and ideal of $(\mathbb{Z},+,\cdot)$.
2. Prove that $\{0,2,4\}$ is a subring and ideal of the ring $(\mathbb{Z}_6,+_6,\times_6)$.
3. Prove that $\{0,3,6,9\}$ is a subring and ideal of the ring $(\mathbb{Z}_{12},+_{12},\times_{12})$.
4. Prove that the set of Gaussian integers $\mathbb{Z}[i]=\{a+bi:a,b\in\mathbb{Z}\}$ is a subring but not an ideal of the ring of all complex numbers $\mathbb{C}$.
5. Describe all the subrings and ideals of the ring of integers.
6. Show that $2\mathbb{Z}\cup 3\mathbb{Z}$ is not a subring of $\mathbb{Z}$.

7. Determine the smallest subring of $\mathbb{Q}$ that contains $\frac{1}{2}$.

8. Determine the smallest subring of $\mathbb{Q}$ that contains $\frac{2}{3}$.

9. Prove that centre of a ring is always a subring of R.

10. Prove that $\mathbb{Z}$ is subring of $\mathbb{Q},\mathbb{R}$ and $\mathbb{C}$ but not an ideal, $\mathbb{Q}$ is a subring of $\mathbb{R}$ and $\mathbb{C}$ but not an ideal, $\mathbb{R}$ is subring of $\mathbb{C}$ but not an ideal.

11. Find a subring of $\mathbb{Z}\times\mathbb{Z}$ that is not an ideal of $\mathbb{Z}\times\mathbb{Z}$.

12. Let $S=\{a+bi : a,b\in\mathbb{Z}, b \text{ is even}\}$. Show that S is a subring of $\mathbb{Z}[i]$, but not an ideal of $\mathbb{Z}[i]$.

13. List all the ideals of the rings $\mathbb{Z}_{12},\mathbb{Z}_{15},\mathbb{Z}_{20}$ and $\mathbb{Z}_{24}$.

14. In the ring of integers, find a positive integer a such that

(i) $\langle a\rangle=\langle 2\rangle+\langle 3\rangle$ (ii) $\langle a\rangle=\langle 3\rangle+\langle 6\rangle$ (iii) $\langle a\rangle=\langle m\rangle+\langle n\rangle$

15. In the ring of integers, find a positive integer a such that

(i) $\langle a\rangle=\langle 3\rangle\langle 4\rangle$ (ii) $\langle a\rangle=\langle 6\rangle\langle 8\rangle$ (iii) $\langle a\rangle=\langle m\rangle\langle n\rangle$

16. Let R be any ring and $a\in R$ be any element. Prove that

(i) the set $Ra=\{ra : r\in R\}$ is a left ideal of R.

(ii) the set $aR=\{ar : r\in R\}$ is a right ideal of R.

17. Show that right annihilator of an element of a ring is a right ideal of ring.

18. Show that left annihilator of an element of a ring is a left ideal of ring.

19. Let R be a ring of all real valued continuous functions defined on $[0,1]$. Prove that the sets

$S_1=\left\{f\in R : f\left(\frac{1}{2}\right)=0\right\}$ and $S_2=\left\{f\in R : f\left(\frac{1}{2}\right)=f\left(\frac{1}{3}\right)=0\right\}$ are ideals of R.

20. Let $\mathbb{R}$ be the ring of continuous functions from $\mathbb{R}$ to $\mathbb{R}$. Let $A=\{f\in\mathbb{R} : f(0) \text{ is an even integer}\}$. Show that A is a subring of $\mathbb{R}$, but not an ideal of $\mathbb{R}$.

21. Let $R=\left\{\begin{bmatrix}a & b\\ c & d\end{bmatrix} : a,b,c,d\in\mathbb{Z}\right\}$ and $S=\left\{\begin{bmatrix}a & 0\\ b & 0\end{bmatrix} : a,b\in\mathbb{Z}\right\}$. Show that S is an left ideal of R but not right ideal.

22. Let $R=\left\{\begin{bmatrix}a & b\\ c & d\end{bmatrix} : a,b,c,d\in\mathbb{Z}\right\}$ and $S=\left\{\begin{bmatrix}a & b\\ 0 & 0\end{bmatrix} : a,b\in\mathbb{Z}\right\}$. Show that S is a right ideal of R but not a left ideal.

23. Let $R=\left\{\begin{bmatrix}a & b\\ c & d\end{bmatrix} : a,b,c,d\in\mathbb{Z}\right\}$ and $S=\left\{\begin{bmatrix}a & 0\\ 0 & b\end{bmatrix} : a,b\in\mathbb{Z}\right\}$. Show that S is a subring of R

189/35 BEHIND RAILWAY STATION, VAISH COLLEGE ROAD, ROHTAK PIN-124001 (HARYANA)
E-mail us on - jrinstituterohtak@gmail.com, balwanmudgil54@gmail.com Mob. 8607383607, 9802177766

but S is neither a left nor a right ideal of R.

24. Let $R=\left\{\begin{bmatrix} a & b & c \\ d & e & f \\ 0 & 0 & g \end{bmatrix} : a,b,c,d,e,f,g \in \mathbb{Z}\right\}$ be a ring and $A=\left\{\begin{bmatrix} 0 & 0 & a \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} : a \in \mathbb{Z}\right\}$,

$B=\left\{\begin{bmatrix} 0 & 0 & a \\ 0 & 0 & b \\ 0 & 0 & 0 \end{bmatrix} : a,b \in \mathbb{Z}\right\}$. Show that A is an ideal of B, B is an ideal of R but A is not an ideal of R.

25. Let $R=\left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} : a,b,c,d \in \mathbb{Z}\right\}$ be a ring. Prove that $Z(R)$ is neither a left nor a right ideal of R.

26. Let $R=\left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} : a,b,c,d \in \mathbb{Z}\right\}$ and $S=\left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} : a,b,c,d \in 2\mathbb{Z}\right\}$, then prove that S is an ideal of R and therefore R is not a simple ring.

27. Prove that $M_n(k\mathbb{Z})$ is ideal of $M_n(\mathbb{Z})$ $\forall\ k \in \mathbb{Z}$ and hence $M_n(\mathbb{Z})$ is not a simple ring.

28. Show that $R=\left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} : a,b,c,d \in \mathbb{Q}\right\}$ is a simple ring.

29. If $\mathbb{Q}$ is replaced by $\mathbb{R}$ or $\mathbb{C}$ in above ring R then show that it is also a simple ring.

30. Let $R=\left\{\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} : a,b \in \mathbb{R}\right\}$ and $S_1=\left\{\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} : a \in \mathbb{R}\right\}$, $S_2=\left\{\begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix} : a \in \mathbb{R}\right\}$, show that S_1 is a left ideal of R but not right ideal and S_2 is an ideal of R. Hence R is not a simple ring.

31. Let $R=\left\{\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} : a,b \in \mathbb{R}\right\}$ and $S=\left\{\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} : a \in \mathbb{R}\right\}$, then show that S is a subring of R but not an ideal of R. Show that R is non commutative, without unity and with zero divisors but S is a field.

32. Let $R=\left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} : a,b,c,d \in \mathbb{R}\right\}$ and $S=\left\{\begin{bmatrix} a & a \\ a & a \end{bmatrix} : a \in \mathbb{R}\right\}$, then show that S is a subring of R but not an ideal of R. Show that R is non commutative, with unity and with zero divisors but S is a field. Further unities of R and S are different.

33. Show that $\mathbb{Z}\times 2\mathbb{Z}$ is a subring of $\mathbb{Z}\times\mathbb{Z}$. Is it an ideal ?

34. Show that $\mathbb{Z}\times\{0\}$ is a subring of $\mathbb{Z}\times 2\mathbb{Z}$. Also show that $\mathbb{Z}\times\{0\}$ is with unity but $\mathbb{Z}\times 2\mathbb{Z}$ is without unity.

35. Show that $m\mathbb{Z}$ is an ideal of $n\mathbb{Z}$ iff n divides m.

36. Show that $m\mathbb{Z}[i]$ is an ideal of $\mathbb{Z}[i]$ for every integer m.

37. Consider the ring $(P(\mathbb{N}), \Delta, \cap)$. Let A be any subset of $\mathbb{N}$ then show that $P(A)$ is an ideal of $P(\mathbb{N})$ and therefore $P(\mathbb{N})$ is not a simple ring.

Answers

5. $n\mathbb{Z}$

7. $\left\{\frac{m}{2^n} : m \in \mathbb{Z}, n \in \mathbb{N} \cup \{0\}\right\}$

8. $\left\{\frac{2m}{3^n} : m \in \mathbb{Z}, n \in \mathbb{N} \cup \{0\}\right\}$

11. $\{(a,a) : a \in \mathbb{Z}\}$

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

$\langle 1\rangle = \mathbb{Z}_{15}, \langle 3\rangle = \{0,3,6,9,12\}, \langle 5\rangle = \{0,5,10\}, \langle 15\rangle = \{0\}$.

$\langle 1\rangle = \mathbb{Z}_{20}, \langle 2\rangle = \{0,2,4,6,8,10,12,14,16,18\}, \langle 4\rangle = \{0,4,8,12,16\}$,

$\langle 5\rangle = \{0,5,10,15\}, \langle 10\rangle = \{0,10\}, \langle 20\rangle = \{0\}$.

$\langle 1\rangle = \mathbb{Z}_{24}, \langle 2\rangle = \{0,2,4,6,8,10,12,14,16,18,20,22\}, \langle 3\rangle = \{0,3,6,9,12,15,18,21\}$,

$\langle 4\rangle = \{0,4,8,12,16,20\}, \langle 6\rangle = \{0,6,12,18\}, \langle 8\rangle = \{0,8,16\}, \langle 12\rangle = \{0,12\}, \langle 24\rangle = \{0\}$.

14. (i) 1 (ii) 3 (iii) g.c.d. (m,n)

15. (i) 12 (ii) 48 (iii) mn

---------- S C Q ----------

1. The ring M of 2×2 matrices with elements in $\mathbb{R}$ is
   1. Commutative ring with zero divisors, without unity.
   2. Non-commutative ring with zero divisors, with unity.
   3. Commutative ring with unity.
   4. Field.

2. The set of all matrices of the form $\left\{\begin{pmatrix} 0 & x \\ 0 & y \end{pmatrix} : x, y \in \mathbb{Q}\right\}$ under the two operations matrix addition and matrix multiplication is
   1. A ring with unity
   2. Commutative ring
   3. Non-commutative ring with zero divisors
   4. A ring without zero divisors but with unity.

3. Which of the following is not a ring ?
   1. Set of all 2×2 matrices whose elements are in $\mathbb{Q}$.
   2. Set of all 2×2 matrices whose elements are in $\mathbb{C}$.
   3. Set of all 2×2 matrices whose elements are in $\mathbb{Z}$.
   4. All 2×2 matrices whose elements are in $\mathbb{R}^+$ and determinant of the matrices is zero.

4. The integral domain of which cardinality is not possible
   1. 5 2. 6
   3. 7 4. 8

5. Let R be an integral domain with unity '1' in which $20\cdot 1 = 0$ and $12\cdot 1 = 0$. Then, characteristics of R is
   1. 2 2. 4
   3. 20 4. 12

6. In $\mathbb{Z}_8$, all the nilpotent elements are
   1. 2,4 and 6 2. 2 and 4
   3. 4 4. 0,2,4 and 6

7. A subring S of R has the following axioms :
   1. S is not closed under addition and multiplication.
   2. S is closed under addition only.
   3. S is closed under multiplication only.
   4. S is a ring under the operation defined in R .

8. Which of the following is not a subring of the given ring
   1. $(\mathbb{Z},+,\cdot)$ of the ring $(\mathbb{R},+,\cdot)$
   2. $(E,+,\cdot)$ of $(\mathbb{Z},+,\cdot)$; (E is the set of even integers.)
   3. $(\mathbb{Q},+,\cdot)$ of $(\mathbb{R},+,\cdot)$
   4. $(\mathrm{O},+,\cdot)$ of $(\mathbb{Z},+,\cdot)$; (O stands for odd integers.)

9. What is the characteristic of the ring of even integers $2\mathbb{Z}$?
   1. 2 2. 1
   3. 0 4. none of these

10. The number of nilpotent element in the ring $(\mathbb{Z}_{30},+_{30},\times_{30})$ is
    1. 0 2. 1
    3. 2 4. 3

11. The number of idempotent and nilpotent elements in $\mathbb{Z}_4$ respectively are
    1. 1, 3 2. 3, 1
    3. 2, 2 4. 0, 1

12. If F is a field with characteristic 3, then for all $a,b\in F$; $(a+b)^3$ is equal to
    1. $a+b$ 2. a^3+b^3
    3. $a+b+ab$ 4. 0

13. The characteristic of the ring $\mathbb{Z}_2\times\mathbb{Z}_4\times\mathbb{Z}_6$ is
    1. 2 2. 4
    3. 6 4. 12

14. The set $R=\left\{\left(a_{ij}\right)_{2\times2}:a_{ij}\in\mathbb{Z}\right\}$ is a ring w.r.t. '+' and '$\cdot$' defined by
$\left(a_{ij}\right)_{2\times2}+\left(b_{ij}\right)_{2\times2}=\left(a_{ij}+b_{ij}\right)_{2\times2}$ and
$\left(a_{ij}\right)_{2\times2}\cdot\left(b_{ij}\right)_{2\times2}=\left(a_{ij}\cdot b_{ij}\right)_{2\times2}$
Then, the number of units in R is
1. 2 2. 4
3. 16 4. 8

15. Let $(D,+,\cdot)$ be a division ring containing q elements. Then
1. $a^q=0$ for all $a\in D$
2. $a^q=a$ for all $a\in D$
3. $a^q=a-1$ for all $a\in D$
4. None of these

16. Which of the following rings is not a simple ring.
1. $R=\left\{\begin{bmatrix}a & b\\ c & d\end{bmatrix}:a,b,c,d\in\mathbb{Z}\right\}$
2. $R=\left\{\begin{bmatrix}a & b\\ c & d\end{bmatrix}:a,b,c,d\in\mathbb{Q}\right\}$
3. $R=\left\{\begin{bmatrix}a & b\\ c & d\end{bmatrix}:a,b,c,d\in\mathbb{R}\right\}$
4. $R=\left\{\begin{bmatrix}a & b\\ c & d\end{bmatrix}:a,b,c,d\in\mathbb{C}\right\}$

17. If U is an ideal of ring R and $1\in U$, then
1. U is a proper subset of R.
2. U is equal to R.
3. U is a superset of R.
4. $U=\phi$.

18. Consider $S=C[x^5]$, complex polynomials in x^5, as a subset of $T=C[x]$, the ring of all complex polynomials. Then,
1. S is neither an ideal nor a subring of T.
2. S is an ideal, but not a subring of T.
3. S is a subring, but not an ideal of T.
4. S is both a subring and an ideal of T.
(GATE 2004)

19. The characteristic of $\mathbb{Z}_{12}\times\mathbb{Z}$ is
1. 12 2. 0
3. 4 4. none of these

20. Every non –zero nilpotent element of ring R is
1. zero divisor 2. non-zero divisor
3. unity 4. none of these

21. If I is the set of integers and define $a\oplus b=a+b+1$ and $a\odot b=a+b+ab$. Then, the ring $\{I,\oplus,\odot\}$ is
1. commutative ring
2. Integral Domain
3. Field
4. None of these

22. Let D be the set of tuples $(w_1,....,w_{10})$, where $w_i\in\{1,2,3\},1\le i\le10$ and w_i+w_{i+1} is an even number for each i with $1\le i\le9$. Then, the number of elements in D is
1. $2^{11}+1$ 2. $2^{10}+1$
3. $3^{10}+1$ 4. $3^{11}+1$
(CSIR NET June 2015)

23. Which one of the following is false ?
1. Every field is also a ring.
2. Multiplication in a field is commutative.
3. Every ring with unity has at least 2 units.
4. Any ring containing $\mathbb{Z}$ as a subset must have characteristic equal to zero.

24. Let $M_3(\mathbb{R})$ be the ring of all 3×3 real matrices. If $I,J\subseteq M_3(\mathbb{R})$ are defined as
$I=\left\{\begin{bmatrix}a & b & c\\ 0 & 0 & 0\\ 0 & 0 & 0\end{bmatrix}:a,b,c\in\mathbb{R}\right\}$,
$J=\left\{\begin{bmatrix}a & 0 & 0\\ b & 0 & 0\\ c & 0 & 0\end{bmatrix}:a,b,c\in\mathbb{R}\right\}$, then
1. I is a right ideal and J is a left ideal.
2. I and J both are left ideals.
3. I and J both are right ideals.
4. I is a left ideal and J is a right ideal.
(GATE 2006)

25. Let
$R=\{\alpha_0+\alpha_1 i+\alpha_2 j+\alpha_3 k:\alpha_0,\alpha_1,\alpha_2,\alpha_3\in\mathbb{Z}_3\}$
be the ring of quaternions over $\mathbb{Z}_3$, where

$i^2 = j^2 = k^2 = ijk = -1;$
$ij = -ji = k;\ jk = -kj = i;\ \ ki = -ik = j$. Then

1. R is a field.
2. R is a division ring.
3. R has zero divisors.
4. None of these.

(GATE 2006)

26. The number of units in the ring $\mathbb{Z}_{10} \times \mathbb{Z}_{12}$ is
    1. 120 2. 60
    3. 16 4. 10

---------- M C Q ----------

1. Let $(R,+,\cdot)$ be a ring such that $a^2 = a$, $\forall\ a \in R$. Then
   1. R is commutative
   2. R is not commutative
   3. $a + a = 0\ \forall\ a \in R$
   4. $a + a \neq 0\ \forall\ a \in R$

2. Which of the following is/are not an integral domain ?
   1. $\mathbb{Z}_6$ 2. $\mathbb{Z}_7$
   3. $M_n(\mathbb{Z})$ 4. none of these

3. Let $\mathbb{Z}_6 = \{0,1,2,3,4,5\}$ is a ring of integers modulo 6, then the following is/are true
   1. $\mathbb{Z}_6$ is a ring without zero divisor.
   2. $\mathbb{Z}_6$ is a ring with zero divisor.
   3. 3 is an idempotent element in $\mathbb{Z}_6$,
   4. $\mathbb{Z}_6$ is an Integral Domain.

4. Which of the following is/are true ?
   1. Every integral domain is a field.
   2. A field has no zero divisors.
   3. Every finite integral domain is a field.
   4. A skew-field has zero divisors.

5. Which of the following is/are field ?
   1. $(\mathbb{Z},+,\cdot)$ 2. $(\mathbb{Q},+,\cdot)$
   3. $(\mathbb{Z}_5,+,\cdot)$ 4. $(\mathbb{Z}_6,+,\cdot)$

6. If S is any ideal of a ring R and T be any subring of R, then
   1. $S+T$ is a subring of R.
   2. $S+T$ is an ideal of R.
   3. S is a subring of $S+T$.
   4. S is an ideal of $S+T$.

7. Let I_1 and I_2 are two ideals of a ring R, which of the following is/are correct ?
   1. $I_1 \cup I_2$ is an ideal of R.
   2. $I_1 \cap I_2$ is an ideal of R.
   3. $I_1 + I_2$ is an ideal of R.
   4. $I_1 I_2$ is an ideal of R.

8. Let R denotes the ring of all 2×2 matrices with integer entries and $M = \left\{\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} : a,b \in \mathbb{Z}\right\}$, then which of the following is / are true :
   1. M is left ideal in R.
   2. M is right ideal in R.
   3. M is left ideal but not right ideal in R.
   4. M is right ideal but not left ideal in R.

9. Which of the following is true ?
   1. Every integral domain of the characteristic zero is infinite.
   2. The characteristic of $\mathbb{Z}_n$ is n.
   3. If r is a non zero element of a ring R, then either r is a unit or r is a zero divisor
   4. If A is a 2×2 matrix with $\det(A) = 0$, then A is a zero divisor in $M_2(\mathbb{R})$.

10. Let R be a non-zero ring with identity such that $a^2 = a$ for all $a \in R$. Which of the following statements are true ?
    1. There is no such ring
    2. $2a = 0$ for all $a \in R$
    3. $3a = 0$ for all $a \in R$
    4. $\mathbb{Z}/2\mathbb{Z}$ is a subring of R

(CSIR NET June 2017)

Assignment Key

SCQ

1. 2
2. 3
3. 4
4. 2
5. 1
6. 4
7. 4
8. 4
9. 3
10. 2
11. 3
12. 2
13. 4
14. 3
15. 2
16. 1
17. 2
18. 3
19. 2
20. 1
21. 2
22. 2
23. 3
24. 1
25. 3
26. 3

MCQ

1. 1,3
2. 1,3
3. 2,3
4. 2,3
5. 2,3
6. 1,3,4
7. 2,3,4
8. 1,3
9. 1,2,4
10. 2,4

189/35 BEHIND RAILWAY STATION, VAISH COLLEGE ROAD, ROHTAK PIN-124001 (HARYANA)
E-mail us on - jrinstituterohtak@gmail.com, balwanmudgil54@gmail.com Mob. 8607383607, 9802177766

2.1 Factorisation of Polynomials

Def. Irreducible Polynomial : Let R be an integral domain. A polynomial $f(x) \in R[x]$ of positive degree is said to be an irreducible polynomial over R if it cannot be expressed as product of two polynomials of positive degree. i.e., if $f(x) = g(x)h(x)$ where $g(x), h(x) \in R[x]$ then either $\deg(g(x)) = 0$ or $\deg(h(x)) = 0$.

Def. Reducible Polynomial : A polynomial of positive degree which is not irreducible over R is called reducible polynomial over R. i.e., $f(x)$ can be expressed as $f(x) = g(x)h(x)$ for some $g(x), h(x) \in R[x]$ where $\deg(g(x)) > 0$ and $\deg(h(x)) > 0$.

Results :

1. Let R be a ring and $f(x)$, $g(x)$ be two non-zero polynomials over R, then
   (i) If $f(x) + g(x) \neq 0$, then $\deg(f(x) + g(x)) \leq \max\{\deg f(x), \deg g(x)\}$.
   (ii) If $f(x).g(x) \neq 0$, then $\deg(f(x).g(x)) \leq \deg f(x) + \deg g(x)$
   (iii) If R is an integral domain, then $\deg(f(x).g(x)) = \deg f(x) + \deg g(x)$.
2. Division algorithm : Let $f(x)$ and $g(x)(\neq 0)$ be two elements of $F[x]$ where F is a field, then there exist unique polynomials $q(x)$ and $r(x)$ in $F[x]$ such that $f(x) = g(x) \cdot q(x) + r(x)$ where $r(x) = 0$ or $\deg r(x) < \deg g(x)$.
3. Division algorithm does not hold in the polynomial ring $\mathbb{Z}[x]$. e.g., consider $f(x) = 3x + 4$ and $g(x) = 2x + 3$.
4. Remainder theorem : Let F be an arbitrary field. If a polynomial $f(x) \in F[x]$ is divided by $x - a$, then the remainder is $f(a)$.
5. Factor theorem : A polynomial $f(x) \in F[x]$ is divisible by $x - a$ iff $f(a) = 0$.
6. A polynomial of degree one is always irreducible.
7. Let F be a field and $f(x) \in F[x]$ be a polynomial of degree 2 or 3 then $f(x)$ is reducible over F if and only if $f(x)$ has a zero in F.

8. Let F be a field and $f(x) \in F[x]$ be a polynomial of degree 4 or more, then

   (i) if $f(x)$ has a zero a in F then $x-a$ is a factor of $f(x)$ and so $f(x)$ is reducible over F.

   (ii) if $f(x)$ has no zero in F then $f(x)$ may or may not be reducible over F.

9. Let $f(x) \in \mathbb{Z}[x]$. If $f(x)$ is reducible over $\mathbb{Q}$, then it is reducible over $\mathbb{Z}$. In other words, a polynomial with integer coefficients is reducible (irreducible) over $\mathbb{Q}$ iff it is reducible(irreducible) over $\mathbb{Z}$. For instance, consider the factorization $6x^2 + x - 2 = \left(3x - \frac{3}{2}\right)\left(2x + \frac{4}{3}\right)$.

10. Mod p Irreducibility Test : Let p be a prime and suppose that $f(x) \in \mathbb{Z}[x]$ with $\deg f(x) \geq 1$. Let $\overline{f}(x)$ be the polynomial in $\mathbb{Z}_p[x]$ obtained from $f(x)$ by reducing all the coefficients of $f(x)$ modulo p. If $\deg \overline{f}(x) = \deg f(x)$ and $\overline{f}(x)$ is irreducible over $\mathbb{Z}_p$ then $f(x)$ is irreducible over $\mathbb{Q}$.

11. Eisenstein's criterion of irreducibility over $\mathbb{Q}$: Let $f(x) = a_0 + a_1 x + a_2 x^2 + ... + a_n x^n$ be a polynomial in $\mathbb{Z}[x]$. If p is a prime such that $p \mid a_0, p \mid a_1, ..., p \mid a_{n-1}$, $p \nmid a_n, p^2 \nmid a_0$ then $f(x)$ is an irreducible polynomial over $\mathbb{Q}$.

12. Shifting result : Let $f(x) \in \mathbb{Z}[x]$ be any polynomial and k be any integer then $f(x \pm k)$ is irreducible over $\mathbb{Q}$ iff $f(x)$ irreducible over $\mathbb{Q}$.

13. Irreducibility of p^{th} cyclotomic polynomial : For any prime p, the p^{th} cyclotomic polynomial $g_p(x) = x^{p-1} + x^{p-2} + ... + x + 1$ is irreducible over $\mathbb{Q}$.

14. If $g_p(x)$ is the p^{th} cyclotomic polynomial then $g_p\left(x^{p^{n-1}}\right)$ is irreducible over $\mathbb{Q}$ for every positive integer n.

15. A real polynomial of degree ≥ 3 is always reducible over $\mathbb{R}$, but it may or may not have a root in $\mathbb{R}$.

16. A real polynomial of degree 2 may or may not be irreducible over $\mathbb{R}$. e.g., consider the polynomials $x^2 + 1$ and $x^2 - 2$.

17. Let p be a prime, then the number of reducible polynomial over $\mathbb{Z}_p$ of the form $x^2 + ax + b$ is $\frac{p(p+1)}{2}$.

18. Let p be a prime, then the number of irreducible polynomial over $\mathbb{Z}_p$ of the form $x^2 + ax + b$ is $\frac{p(p-1)}{2}$.

Exercise 2.1

Which of the following polynomials are irreducible or reducible over the field $\mathbb{Z}_2$. Whenever a polynomial is reducible then reduce it into irreducible factors.

1. x^2+1 2. x^2+x+1 3. x^3+1 4. x^3+x+1
5. x^3+x^2+1 6. x^3+x^2+x+1 7. $x^4+3x^3-9x^2+7x+27$
8. x^4+x^2+1 9. x^4+1 10. x^4+x+1 11. x^4+x^2+x+1
12. x^4+x^3+1 13. x^4+x^3+x+1 14. $x^4+x^3+x^2+1$ 15. $x^4+x^3+x^2+x+1$
16. $x^5+x^4+x^3+x^2+1$ 17. $x^5+x^4+x^3+x+1$ 18. $x^5+x^4+x^3+x^2+x+1$ 19. $x^5+x^3+x^2+x+1$
20. $x^5+x^4+x^2+1$ 21. $x^5+x^3+x^2+1$ 22. x^5+x^2+x+1

Which of the following polynomials are irreducible or reducible over the field $\mathbb{Z}_3$. Whenever a polynomial is reducible then reduce it into irreducible factors.

23. x^2+x+1 24. x^2+x+2 25. x^2+2x+1
26. x^2+2x+2 27. $2x^2+x+2$ 28. x^3+2x+2
29. x^3+x^2+1 30. x^3+2x^2+2x+1 31. x^3+2x^2+2x+2
32. $x^4+3x^3-9x^2+7x+27$ 33. x^4+2x^2+1 34. x^4+x^3+x+1
35. $x^4+x^3+x^2+x+1$ 36. $x^4+x^3+2x^2+2x+1$ 37. x^4+2x^3+x+1
38. $x^4+2x^3+x^2+1$ 39. $x^4+2x^3+x^2+2x+1$ 40. $x^4+2x^3+2x^2+x+1$
41. x^5+2x^3+1 42. x^5+x^2+2 43. $x^5+x^4+x^3+x^2+x+2$
44. $x^5+x^4+2x^3+x^2+2x+1$ 45. $2x^5+x^2+2$ 46. x^5+2x+1
47. x^5+x^4+2 48. $x^5+x^3+x^2+2$

Which of the following polynomials are irreducible or reducible over the field $\mathbb{Z}_5$. Whenever a polynomial is reducible then reduce it into irreducible factors.

49. x^2+x+4 50. x^2+2x+4 51. x^2+3x+4
52. x^2+4x+4 53. x^3+4x^2+4x+1 54. x^3+4x^2+4x+2
55. x^3+4x^2+4x+3 56. x^3+4x^2+4x+4 57. $x^4+3x^3+2x^2+x+1$
58. $x^4+3x^3+3x^2+x+1$ 59. $x^4+3x^3+4x^2+4x+1$ 60. $x^4+4x^3+x^2+4x+1$
61. $x^4+4x^3+4x^2+1$ 62. $x^4+4x^3+4x^2+3x+1$

Which of the following polynomials are irreducible or reducible over the field $\mathbb{Z}_7$. Whenever a polynomial is reducible then reduce it into irreducible factors.

63. x^2+4x+4 64. x^2+6x+5 65. x^3+2x^2+x+1 66. x^3+6

Which of the following polynomials are irreducible or reducible over the field $\mathbb{Z}_{11}$. Whenever a polynomial is reducible then reduce it into irreducible factors.

67. $x^2+10x+9$ 68. x^2+7x+4 69. x^2+x+4 70. x^3+1

Which of the following polynomials are irreducible or reducible over $\mathbb{Z}$.

71. $21x^3-3x^2+2x+8$ 72. $x^4+x^3+x^2+x+1$ 73. $x^4+3x^3-9x^2+7x+27$

74. $5x^4-6x^3+9x^2-15x+12$ 75. $1+(x+1)+(x+1)^2+(x+1)^3+(x+1)^4$

Which of the following polynomials are irreducible or reducible over $\mathbb{Q}$.

76. $2x^2+4$ 77. x^2-2 78. x^2+1

79. $6x^2+x-2$ 80. x^2-5 81. x^3+2x^2+x-1

82. $8x^3-6x+1$ 83. x^3+x^2+x+1 84. x^3+3x^2-6x+3

85. x^3+2x^2+x+1 86. $x^3-312312x+123123$ 87. $\frac{3}{7}x^4-\frac{2}{7}x^2+\frac{9}{35}x+\frac{3}{5}$

88. x^4+1 89. x^4+x+1 90. x^4+3x^2+3

91. $1+x+x^2+x^3+x^4$ 92. $x^4-x^3+14x^2+5x+16$ 93. $x^5+3x^4+9x+15$

94. x^5+2x+4 95. $3x^5+15x^4-20x^3+10x+20$

96. $x^5+9x^4+12x^2+6$ 97. x^5+5x^2+1 98. $\frac{5}{2}x^5+\frac{9}{2}x^4+15x^3+\frac{3}{7}x^2+6x+\frac{3}{14}$

Which of the following polynomials are irreducible or reducible over $\mathbb{R}$.

99. x^3+2x^2+x-1 100. x^4+1 101. $x^5-3x^4+2x^3-5x+8$

Which of the following polynomials are irreducible or reducible over $\mathbb{Q}$.

102. x^3+x^2+x+1 103. x^3+x^2+x-1 104. x^3+x^2-x+1

105. x^3+x^2-x-1 106. x^3-x^2+x+1 107. x^3-x^2+x-1

108. x^3-x^2-x+1 109. x^3-x^2-x-1

Which of the following polynomials are irreducible or reducible over $\mathbb{Z}$.

110. x^4+4 111. x^4+64 112. x^4+16

113. x^4+36 114. x^4-1

115. For what values of *k* the polynomial x^4+k is reducible over $\mathbb{Z}$.

Which of the following polynomials are irreducible or reducible over $\mathbb{Z}$.

116. x^4+x^2+1 117. x^4-7x^2+1 118. x^4+10x^2+1

119. x^4+16x^2+1 120. x^4+7x^2+1

121. For what values of k the polynomial x^4+kx^2+1 is reducible over $\mathbb{Z}$.

Answers

1. reducible ; $x^2+1=(x+1)^2$
2. irreducible
3. reducible ; $x^3+1=(x+1)(x^2+x+1)$
4. irreducible
5. irreducible
6. reducible ; $x^3+x^2+x+1=(x+1)^3$
7. irreducible
8. reducible ; $x^4+x^2+1=(x^2+x+1)^2$
9. reducible ; $x^4+1=(x+1)^4$
10. irreducible
11. reducible ; $x^4+x^2+x+1=(x+1)(x^3+x^2+1)$
12. irreducible
13. reducible ; $x^4+x^3+x+1=(x+1)^2(x^2+x+1)$
14. reducible ; $x^4+x^3+x^2+1=(x+1)(x^3+x+1)$
15. irreducible
16. irreducible
17. irreducible
18. reducible ; $x^5+x^4+x^3+x^2+x+1=(x+1)(x^2+x+1)^2$
19. irreducible
20. reducible ; $x^5+x^4+x^2+1=(x+1)(x^4+x+1)$
21. reducible ; $x^5+x^3+x^2+1=(x+1)^3(x^2+x+1)$
22. reducible ; $x^5+x^2+x+1=(x+1)^2(x^3+x+1)$
23. reducible ; $x^2+x+1=(x+2)^2$
24. irreducible
25. reducible ; $x^2+2x+1=(x+1)^2$
26. irreducible
27. reducible ; $2x^2+x+2=2(x+1)^2$
28. irreducible
29. reducible ; $x^3+x^2+1=(x+2)(x^2+2x+2)$
30. reducible ; $x^3+2x^2+2x+1=(x+1)(x+2)^2$
31. irreducible
32. reducible ; $x^4+3x^3-9x^2+7x+27=x^4+x=x(x+1)^3$
33. reducible ; $x^4+2x^2+1=(x^2+1)^2$
34. reducible ; $x^4+x^3+x+1=(x+1)^4$
35. irreducible
36. reducible ; $x^4+x^3+2x^2+2x+1=(x^2+2x+2)^2$

37. irreducible 38. irreducible 39. irreducible

40. reducible ; $x^4+2x^3+2x^2+x+1=\left(x^2+x+2\right)^2$

41. reducible ; $x^5+2x^3+1=\left(x^2+2x+2\right)\left(x^3+x^2+x+2\right)$

42. reducible ; $x^5+x^2+2=\left(x^2+2x+2\right)\left(x^3+x^2+2x+1\right)$

43. reducible ; $x^5+x^4+x^3+x^2+x+2=\left(x^2+2x+2\right)\left(x^3+2x^2+x+1\right)$

44. irreducible 45. reducible ; $2x^5+x^2+2=\left(x^2+x+2\right)\left(2x^3+x^2+x+1\right)$

46. irreducible 47. irreducible 48. irreducible

49. reducible ; $x^2+x+4=\left(x+3\right)^2$ 50. irreducible 51. irreducible

52. reducible ; $x^2+4x+4=\left(x+2\right)^2$ 53. reducible ; $x^3+4x^2+4x+1=\left(x+1\right)\left(x+4\right)^2$

54. irreducible 55. reducible ; $x^3+4x^2+4x+3=\left(x+3\right)\left(x^2+x+1\right)$

56. irreducible 57. reducible ; $x^4+3x^3+2x^2+x+1=\left(x+1\right)\left(x^3+2x^2+1\right)$

58. reducible ; $x^4+3x^3+3x^2+x+1=\left(x+3\right)\left(x^3+3x+2\right)$

59. reducible ; $x^4+3x^3+4x^2+4x+1=\left(x+3\right)\left(x^3+4x+2\right)$

60. reducible ; $x^4+4x^3+x^2+4x+1=\left(x+1\right)^4$

61. reducible ; $x^4+4x^3+4x^2+1=\left(x+3\right)\left(x+4\right)\left(x^2+2x+3\right)$

62. reducible ; $x^4+4x^3+4x^2+3x+1=\left(x+2\right)\left(x^3+2x^2+3\right)$

63. reducible ; $x^2+4x+4=\left(x+2\right)^2$ 64. reducible ; $x^2+6x+5=\left(x+1\right)\left(x+5\right)$

65. reducible ; $x^3+2x^2+x+1=\left(x+4\right)\left(x^2+5x+2\right)$ 66. reducible ; $x^3+6=\left(x+3\right)\left(x+5\right)\left(x+6\right)$

67. reducible ; $x^2+10x+9=\left(x+1\right)\left(x+9\right)$ 68. reducible ; $x^2+7x+4=\left(x+9\right)^2$

69. reducible ; $x^2+x+4=\left(x+4\right)\left(x+8\right)$ 70. reducible ; $x^3+1=\left(x+1\right)\left(x^2+10x+1\right)$

71. irreducible	72. irreducible	73. irreducible	74. irreducible
75. irreducible	76. irreducible	77. irreducible	78. irreducible
79. irreducible	80. irreducible	81. irreducible	82. irreducible
83. reducible	84. irreducible	85. irreducible	86. irreducible
87. irreducible	88. irreducible	89. irreducible	90. irreducible

91. irreducible 92. irreducible 93. irreducible 94. irreducible
95. irreducible 96. irreducible 97. irreducible 98. irreducible
99. reducible 100. reducible 101. reducible

2.2 Maximal and Prime Ideal

Def. Maximal Ideal : An ideal $M(\neq R)$ of a ring R is said to be maximal ideal of R if there does not exist any ideal K of R such that $M \subsetneqq K \subsetneqq R$.

In words, there must not be any ideal of R which properly contains M and is properly contained in R. Roughly speaking, there does not exist any ideal between M and R.

or

An ideal $M(\neq R)$ of a ring R is said to be maximal ideal of R if whenever K is an ideal of R such that $M \subseteq K \subseteq R$, then either $K = M$ or $K = R$.

Remark : Negation of the above definition : An ideal $M \neq R$ is not a maximal ideal of R if there exists an ideal K of R such that $M \subsetneqq K \subsetneqq R$.

Examples :

(i) $2\mathbb{Z}$ is a maximal ideal of $\mathbb{Z}$, because there exists no ideal between $2\mathbb{Z}$ and $\mathbb{Z}$. However $6\mathbb{Z}$ is not a maximal ideal of $\mathbb{Z}$ because $6\mathbb{Z} \subset 3\mathbb{Z} \subset \mathbb{Z}$. In fact, $p\mathbb{Z}$, where p is a prime number, is always a maximal ideal of $\mathbb{Z}$.

(ii) $2\mathbb{Z} \times \mathbb{Z}$ is a maximal ideal of $\mathbb{Z} \times \mathbb{Z}$.

Def. Prime Ideal : An ideal $P \neq R$ of a ring R is said to be prime ideal if $ab \in P \Rightarrow a \in P$ or $b \in P$. In words, an ideal $P \neq R$ of a ring R is said to be prime ideal if , whenever product of two elements of R is in P then at least one of those elements must belong to P.

or

An ideal $P \neq R$ of a ring R is said to be prime ideal if $a \notin P, b \notin P \Rightarrow ab \notin P$. In words, an ideal $P \neq R$ is said to be a prime ideal if, whenever two elements of the ring are not in P then there product is also not in P.

Remark : Negation of the above definition : An ideal $P \neq R$ is not a prime ideal of R if there exist two elements $a, b \in R$ such that $a \notin P$, $b \notin P$ but $ab \in P$.

Examples :

(1) In the ring of integers $\mathbb{Z}$, $\{0\}$ is a prime ideal.

(2) $4\mathbb{Z} = \{4n : n \in \mathbb{Z}\}$ is not a prime ideal of $\mathbb{Z}$ as $2.2 = 4 \in 4\mathbb{Z}$ but $2 \notin 4\mathbb{Z}$.

(3) $5\mathbb{Z} = \{5n : n \in \mathbb{Z}\}$ is a prime ideal of $\mathbb{Z}$. We see that if a and b are any two integers such that $ab \in 5\mathbb{Z}$, then $5 \mid ab \Rightarrow 5 \mid a$ or $5 \mid b \Rightarrow a \in 5\mathbb{Z}$ or $b \in 5\mathbb{Z}$.

In fact each ideal of $\mathbb{Z}$ generated by some prime integer is a prime ideal.

Results :

1. **M P 1 Result :** In a ring R, a maximal ideal need not be a prime ideal and a prime ideal need not be a maximal ideal. e.g., $\{0\}$ is a prime ideal of $\mathbb{Z}$ but not a maximal ideal and $4\mathbb{Z}$ is a maximal ideal of $2\mathbb{Z}$ but not a prime ideal.
2. **M P 2 Result :** In a CRU every maximal ideal is prime ideal, but the converse need not be true.
3. **M P 3 Result :** In a finite CRU an ideal is maximal iff it is a prime ideal.
4. **Zero ideal Result :**
   (i) A ring R is without zero divisors iff $\{0\}$ is a prime ideal of R.
   (ii) A ring R is with zero divisor iff $\{0\}$ is not a prime ideal of R.
   (iii) A ring R has no non-trivial proper ideals iff $\{0\}$ is a maximal ideal of R.
   (iv) A ring R has non-trivial proper ideals iff $\{0\}$ is not a maximal ideal of R.
5. Let R be a commutative ring with unity, then R is a field iff $\{0\}$ is a maximal ideal of R.
6. Maximal and prime ideals of $\mathbb{Z}$:
   (i) The ideal $\{0\}$ is a prime ideal of $\mathbb{Z}$ but not a maximal ideal.
   (ii) An ideal generated by a composite number in $\mathbb{Z}$ is neither a prime nor a maximal ideal of $\mathbb{Z}$.
   (iii) An ideal of ring of integers $\mathbb{Z}$ is maximal if and only if it is generated by some prime integer i.e., every maximal ideal of $\mathbb{Z}$ is of the form $p\mathbb{Z}$, where p is a prime.
   (iv) Every non–zero ideal of $\mathbb{Z}$ is maximal iff it is prime ideal.
7. Maximal and prime ideals of $\mathbb{Z}_n$:
   (i) If n is prime then the only ideals of $\mathbb{Z}_n$ are $\{0\}$ and $\mathbb{Z}_n$. $\{0\}$ is maximal as well as prime ideal.
   (ii) If n is composite then $\mathbb{Z}_n$ has $\tau(n)$ ideals where $\tau(n)$ is the number of divisors of n.
   (iii) If n is composite then the ideals generated by prime divisors of n are maximal as well as prime ideals of $\mathbb{Z}_n$.
   (iv) If n is composite then the ideals generated by composite divisors of n are neither maximal nor prime ideals of $\mathbb{Z}_n$.

(v) If n is composite then $\{0\}$ is neither a maximal nor a prime ideal of $\mathbb{Z}_n$.

(vi) As $\mathbb{Z}_n$ is a finite CRU, so by M P 3 Result, an ideal of $\mathbb{Z}_n$ is maximal iff it is a prime ideal.

8. Four Important ideals of $\mathbb{Z}[x]$:

(i) $A = < x > = \{ x f(x) : f(x) \in \mathbb{Z}[x] \}$ is a prime ideal but not a maximal ideal.

(ii) $B = < 2, x > = \{ 2f(x) + xg(x) : f(x), g(x) \in \mathbb{Z}[x] \}$ is both maximal and prime ideal.

(iii) $C = < x^2 + 1 > = \{ (x^2 + 1) f(x) : f(x) \in \mathbb{Z}[x] \}$ is a prime ideal but not a maximal ideal.

(iv) $D = < 2, x^2 + 1 > = \{ 2f(x) + (x^2 + 1) g(x) : f(x), g(x) \in \mathbb{Z}[x] \}$ is neither a prime ideal nor a maximal ideal.

Remark : Ideal A contains all polynomials of $\mathbb{Z}[x]$ whose constant term is zero and ideal B contains all polynomials in $\mathbb{Z}[x]$ whose constant term is an even integer.

9. Maximal and prime ideals in $\mathbb{Z}[x]$:

(i) The ideal $\{0\}$ is a prime ideal but not a maximal ideal in $\mathbb{Z}[x]$.

(ii) Let $f(x) \in \mathbb{Z}[x]$ be a reducible polynomial then $\langle f(x) \rangle$ is neither a prime ideal nor a maximal ideal.

(iii) Let $f(x) \in \mathbb{Z}[x]$ be any irreducible polynomial, then $\langle f(x) \rangle$ is always a prime ideal but not a maximal ideal.

(iv) Every maximal ideal of $\mathbb{Z}[x]$ is of the form $\langle p, f(x) \rangle$, where p is prime and $f(x)$ is an irreducible polynomial over $\mathbb{Z}_p[x]$.

(v) A non-zero prime ideal of $\mathbb{Z}[x]$ may or may not be a maximal ideal.

10. Maximal and prime ideals in $\mathbb{Q}[x]$:

(i) The ideal $\{0\}$ is a prime ideal but not a maximal ideal in $\mathbb{Q}[x]$.

(ii) Let $f(x) \in \mathbb{Q}[x]$ be a reducible polynomial then $\langle f(x) \rangle$ is neither a prime ideal nor a maximal ideal.

(iii) Let $f(x) \in \mathbb{Q}[x]$ be any polynomial, then $\langle f(x) \rangle$ is a maximal ideal iff $f(x)$ is an

irreducible polynomial in $\mathbb{Q}[x]$.

(iv) Every non-zero ideal in $\mathbb{Q}[x]$ is maximal iff it is prime ideal.

11. Maximal and prime ideals in $F[x]$, where F is a field :

(i) The ideal $\{0\}$ is a prime ideal but not a maximal ideal in $F[x]$.

(ii) Let $f(x) \in F[x]$ be a reducible polynomial then $\langle f(x) \rangle$ is neither a prime ideal nor a maximal ideal.

(iii) Let $f(x) \in F[x]$ be any polynomial, then $\langle f(x) \rangle$ is a maximal ideal iff $f(x)$ is an irreducible polynomial in $F[x]$.

(iv) Every non-zero ideal in $F[x]$ is maximal iff it is prime ideal.

12. Maximal and prime ideals of the ring of Gaussian integers $\mathbb{Z}[i]$:

(i) The ideal $\{0\}$ is a prime ideal but not a maximal ideal in $\mathbb{Z}[i]$.

(ii) In the ring of Gaussian integers $\mathbb{Z}[i]$ an ideal $\langle a+ib \rangle$ is a maximal ideal iff either a^2+b^2 is a prime or it is square of a prime of the form $4k+3$.

(iii) If a^2+b^2 is neither a prime nor a square of a prime of the form $4k+3$ then $\langle a+ib \rangle$ is neither a prime nor a maximal ideal of $\mathbb{Z}[i]$.

(iv) Every non-zero ideal of $\mathbb{Z}[i]$ is maximal iff it is a prime ideal.

13. Let R be the ring of all real valued continuous functions on the interval $[0,1]$, then

(i) $S = \left\{ f(x) \in R \ : f\left(\frac{1}{2}\right) = 0 \right\}$ is a maximal ideal of R.

(ii) $S = \left\{ f(x) \in R \ : f\left(\frac{1}{2}\right) = f\left(\frac{1}{3}\right) = 0 \right\}$ is neither a prime ideal nor a maximal ideal of R.

14. Maximal and prime ideals in the ring $(P(\mathbb{N}), \Delta, \cap)$:

(i) If $A = \{2,3,4,5,.....\}$ then $P(A)$ is a maximal as well as prime ideal of $P(\mathbb{N})$.

(ii) If $B = \{3,4,5,6,.....\}$ then $P(B)$ is neither a maximal nor a prime ideal of $P(\mathbb{N})$.

15. **P F 1 Result :** Let R be a commutative ring with unity. If every ideal of R is prime , then R is a field.

16. The intersection of two prime (maximal) ideals of a ring R may not be prime (maximal) ideals of R.

17. The sum of two prime (maximal) ideals of a ring R may not be prime (maximal) ideals of R.

189/35 BEHIND RAILWAY STATION, VAISH COLLEGE ROAD, ROHTAK PIN-124001 (HARYANA)
E-mail us on - jrinstituterohtak@gmail.com, balwanmudgil54@gmail.com Mob. 8607383607, 9802177766

18. If $A_1, A_2, ..., A_r$ are maximal ideals of $\mathbb{Z}_m$ and $B_1, B_2, ..., B_s$ are maximal ideals of $\mathbb{Z}_n$, then $A_1 \times \mathbb{Z}_n, A_2 \times \mathbb{Z}_n, ..., A_r \times \mathbb{Z}_n, \mathbb{Z}_m \times B_1, \mathbb{Z}_m \times B_2, ..., \mathbb{Z}_m \times B_s$ are maximal ideals of $\mathbb{Z}_m \times \mathbb{Z}_n$. Here $A_1 \times B_1$ is not a maximal ideal of $\mathbb{Z}_m \times \mathbb{Z}_n$ because $A_1 \times B_1 \subsetneqq \mathbb{Z}_m \times B_1 \subsetneqq \mathbb{Z}_m \times \mathbb{Z}_n$.
19. The number of maximal ideals of $\mathbb{Z}_m \times \mathbb{Z}_n$ = (number of maximal ideals of $\mathbb{Z}_m$) + (number of maximal ideals of $\mathbb{Z}_n$).
20. Let *I* be an ideal of a CRU *R* such that every element of *R* which is not in *I* is a unit then *I* is the unique maximal ideal of *R*.

Exercise 2.2

1. Give an example of a finite commutative ring in which every maximal ideal need not be a prime ideal.
2. Find all maximal and prime ideals of $\mathbb{Z}$, $\mathbb{Z}_{10}$, $\mathbb{Z}_{11}$ and $\mathbb{Z}_{20}$.
3. In $\mathbb{Z} \times \mathbb{Z}$, let $I = \{(a,0) : a \in \mathbb{Z}\}$. Show that *I* is a prime ideal but not a maximal ideal.
4. Prove that $I = \langle 2 + 2i \rangle$ is not a prime ideal of $\mathbb{Z}[i]$.
5. Let *p* be a prime. Show that $A = \{(px, y) : x, y \in \mathbb{Z}\}$ is a maximal ideal of $\mathbb{Z} \times \mathbb{Z}$.
6. Let $A = \{a + bi : a, b \in \mathbb{Z}, a = b \bmod 2\}$. Show that *A* is a maximal ideal of $\mathbb{Z}[i]$.
7. Find all prime ideals and all maximal ideals of $\mathbb{Z}_2 \times \mathbb{Z}_2$.
8. Find a maximal ideal of $\mathbb{Z} \times \mathbb{Z}$.
9. Find a non trivial proper ideal of $\mathbb{Z} \times \mathbb{Z}$ that is not prime.
10. Show that $< x^2 + 1 >$ is not a prime ideal of $\mathbb{Z}_2[x]$.
11. Show that $\langle x \rangle$ is a not a prime ideal in $\mathbb{Z}_6[x]$, $\langle x \rangle$ is a prime ideal but not maximal ideal in $\mathbb{Z}[x]$ and $\langle x \rangle$ is a maximal ideal in $\mathbb{Q}[x]$.

Answers

1. $R = \{0, 2, 4, 6\}$ be a finite commutative ring under the operation modulo 8 and $A = \{0, 4\}$ is a maximal ideal but not a prime ideal.
2. $p\mathbb{Z}$, *p* is prime, is a maximal ideal of $\mathbb{Z}$ and $\{0\}$, $p\mathbb{Z}$, *p* is prime, are prime ideals of $\mathbb{Z}$.

$\langle 2\rangle = \{0,2,4,6,8\}$, $\langle 5\rangle = \{0,5\}$ are maximal and prime ideals of $\mathbb{Z}_{10}$. $\{0\}$ is maximal and prime ideal of $\mathbb{Z}_{11}$. $\langle 2\rangle = \{0,2,4,6,8\}$, $\langle 5\rangle = \{0,5\}$ are maximal and prime ideals of $\mathbb{Z}_{20}$.

7. $\{(0,0),(1,0)\}$ and $\{(0,0),(0,1)\}$ are both prime and maximal ideals.

8. $2\mathbb{Z}\times\mathbb{Z}$ 9. $4\mathbb{Z}\times\{0\}$

2.3 Quotient Ring

Def. Let R be a ring and U be an ideal of R, then we know that U is an abelian group under addition. Since the group $(R,+)$ is abelian so U is a normal subgroup of R. Let R/U denotes the set of all distinct cosets of U in R. i.e., $R/U = \{a+U : a \in R\}$

We define addition and multiplication in R/U as follows :

$$(a+U)+(b+U)=(a+b)+U$$

$$(a+U)\cdot(b+U)=a\cdot b+U \text{ for } a+U, b+U \in R/U$$

Then, R/U is a ring under these operations. This ring is known as *Quotient Ring* of R w.r.t. U.

Results :

Let U be an ideal of a ring R and R/U be the quotient ring of R w.r.t. ideal U, then

1. If R is commutative then R/U is also commutative, but converse may not be true.
2. If R has unity '1', then R/U has unity given by $1+U$.
3. If R is an integral domain then R/U may or may not be an integral domain.e.g. consider $\mathbb{Z}, 5\mathbb{Z}, 6\mathbb{Z}$
4. If R/U is an integral domain then R may or may not be an integral domain.
5. $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$
6. If n is composite then $\mathbb{Z}/n\mathbb{Z}$ is with zero divisors and not an integral domain and hence not a field.
7. $\mathbb{Z}/n\mathbb{Z}$ is a field iff n is prime.
8. If R is a ring with unity and U be an ideal of R then characteristic of R/U is either 0 or it divides characteristic of R. e.g., consider $R=\mathbb{Z}_6$ and $U=\{0,2,4\}$
9. The subrings of R/U are of the form J/U where J is a subring of R containing U.
10. The ideals of R/U are of the form J/U where J is an ideal of R containing U.
11. An ideal $M \neq R$ is a maximal ideal of R iff R/M is a simple ring.
12. **F M Result :** Let R be a CRU and M be an ideal of R. Then ideal M is maximal iff R/M is a field.
13. **I P Result :** Let R be a CRU and P be an ideal of R. Then ideal P is prime iff R/P is an integral domain.

14. The number of elements in $\frac{\mathbb{Z}[i]}{\langle a+ib\rangle}=a^2+b^2$.

15. Let $a+ib\in\mathbb{Z}[i]$ be any element, then $\frac{\mathbb{Z}[i]}{\langle a+ib\rangle}$ is a field iff a^2+b^2 is either a prime or square of a prime of the form $4k+3$. Further if $a+ib$ does not satisfy any of the above condition then $\frac{\mathbb{Z}[i]}{\langle a+ib\rangle}$ is not even an integral domain.

16. $\frac{\mathbb{Z}[i]}{\langle a+ib\rangle}\cong\begin{cases}\mathbb{Z}_{a^2+b^2} & \text{if } \gcd(a,b)=1\\ \mathbb{Z}_d[i]\times\mathbb{Z}_{\left(\frac{a}{d}\right)^2+\left(\frac{b}{d}\right)^2} & \text{if } \gcd(a,b)=d\end{cases}$, where $a\neq 0, b\neq 0$

17. $\frac{\mathbb{Z}[i]}{\langle a\rangle}\cong\mathbb{Z}_a[i]$, $a\neq 0$

18. Let F be a field and $f(x)$ is an irreducible polynomial over F then $\frac{F[x]}{\langle f(x)\rangle}$ is a field.

19. Construction of finite fields : Let p be a prime and $f(x)\in\mathbb{Z}_p[x]$ be an irreducible polynomial of degree n then $\frac{\mathbb{Z}_p[x]}{\langle f(x)\rangle}$ is a field of order p^n. If $f(x)$ is a reducible polynomial then $\frac{\mathbb{Z}_p[x]}{\langle f(x)\rangle}$ is a finite CRU of order p^n but it is not an integral domain and hence not a field.

20. Let p be a prime then $\mathbb{Z}[x]/\langle p\rangle\cong\mathbb{Z}_p[x]$.

21. Let p be a prime and $f(x)\in\mathbb{Z}[x]$ be an irreducible polynomial of degree n over $\mathbb{Z}_p$ then $\langle p, f(x)\rangle$ is a maximal ideal of $\mathbb{Z}[x]$ and $\mathbb{Z}[x]/\langle p, f(x)\rangle$ is a field of order p^n. If $f(x)$ is a reducible polynomial then $\mathbb{Z}[x]/\langle p, f(x)\rangle$ is a finite CRU of order p^n but it is not an integral domain and hence not a field.

22. By above result, we can say that every finite field can be obtained by taking a quotient ring of $\mathbb{Z}[x]$.

23. Order of a finite field is always p^n, where p is a prime and n is a positive integer.

24. Let F be a field and $p(x), a(x), b(x) \in F[x]$. If $p(x)$ is irreducible over F and $p(x) \mid a(x) \cdot b(x)$, then $p(x) \mid a(x)$ or $p(x) \mid b(x)$.

25. The number of distinct ideals of $\dfrac{\mathbb{Q}[x]}{\langle f(x) \rangle}$ is equal to the number of distinct factors of $f(x)$.

26. The number of distinct prime ideals of $\dfrac{\mathbb{Q}[x]}{\langle f(x) \rangle}$ is equal to the number of distinct irreducible factors of $f(x)$.

Exercise 2.3

Construct the following quotient rings. Which of them are CRU, Integral domain and field. Also find characteristic in each case.

1. $\mathbb{Z}/5\mathbb{Z}$
2. $\mathbb{Z}/6\mathbb{Z}$
3. $\dfrac{\mathbb{Z}[i]}{\langle 2-i \rangle}$
4. $\dfrac{\mathbb{Z}[i]}{\langle 3+i \rangle}$
5. $\dfrac{\mathbb{Z}[i]}{\langle 1-i \rangle}$
6. $\dfrac{\mathbb{Z}[i]}{\langle 2+i \rangle}$
7. $\dfrac{\mathbb{Z}[i]}{\langle 2+2i \rangle}$
8. $\dfrac{\mathbb{Z}[i]}{\langle 1+i \rangle}$
9. $\dfrac{\mathbb{Z}[i]}{\langle 7 \rangle}$
10. $\dfrac{\mathbb{Z}[i]}{\langle 11i \rangle}$
11. $\dfrac{\mathbb{Z}[i]}{\langle 3+4i \rangle}$
12. $\dfrac{\mathbb{Z}[i]}{\langle 3+3i \rangle}$
13. $\dfrac{\mathbb{Z}[x]}{\langle x \rangle}$
14. $\dfrac{\mathbb{Z}[x]}{\langle 2, x \rangle}$
15. $\dfrac{\mathbb{Z}[x]}{\langle x^2+x+2 \rangle}$
16. $\dfrac{\mathbb{Z}[x]}{\langle x^2+1 \rangle}$
17. $\dfrac{\mathbb{Z}[x]}{\langle 2, x^2+1 \rangle}$
18. $\dfrac{\mathbb{Q}[x]}{\langle x \rangle}$
19. $\dfrac{\mathbb{Q}[x]}{\langle x^2+1 \rangle}$
20. $\dfrac{\mathbb{Z}_5[i]}{\langle 1+i \rangle}$
21. $\dfrac{\mathbb{Z}_6[x]}{\langle 2x+4 \rangle}$
22. R/S where $R = \left\{ \left[a_{ij} \right]_{3\times 3} : a_{ij} \in \mathbb{Z} \right\}$ and $S = \left\{ \left[a_{ij} \right]_{3\times 3} : a_{ij} \in 2\mathbb{Z} \right\}$
23. R/S where $R = \left\{ \left[a_{ij} \right]_{n\times n} : a_{ij} \in \mathbb{Z} \right\}$ and $S = \left\{ \left[a_{ij} \right]_{n\times n} : a_{ij} \in m\mathbb{Z} \right\}$.
24. R/S where $R = \left\{ \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} : a, b \in \mathbb{R} \right\}$ and $U = \left\{ \begin{bmatrix} 0 & c \\ 0 & 0 \end{bmatrix} : c \in \mathbb{R} \right\}$.
25. Construct the finite fields of following order :
    (i) 8 (ii) 9 (iii) 16 (iv) 25 (v) 27
26. How many numbers are there from 2 to 100 which can be the order of a finite field ?
27. Find the number of ideals and the number of prime ideals in the following quotient rings :
    (i) $\dfrac{\mathbb{Q}[x]}{\langle x^3 \rangle}$ (ii) $\dfrac{\mathbb{Q}[x]}{\langle x^3-1 \rangle}$ (iii) $\dfrac{\mathbb{Q}[x]}{\langle x^4-1 \rangle}$ (iv) $\dfrac{\mathbb{Q}[x]}{\langle x^5-1 \rangle}$

28. Give an example of a ring R and its ideal U such that R is non commutative, without unity and with zero divisors but R/U is a field.

Answers

1. $\{5\mathbb{Z}, 1+5\mathbb{Z}, 2+5\mathbb{Z}, 3+5\mathbb{Z}, 4+5\mathbb{Z}\}$
2. $\{6\mathbb{Z}, 1+6\mathbb{Z}, 2+6\mathbb{Z}, 3+6\mathbb{Z}, 4+6\mathbb{Z}, 5+6\mathbb{Z}\}$
3. $\{I, 1+I, 2+I, 3+I, 4+I\}$, $I=\langle 2-i\rangle$
4. $\{I, 1+I, 2+I, 3+I, 4+I, 5+I, 6+I, 7+I, 8+I, 9+I\}$, $I=\langle 3+i\rangle$
5. $\{I, 1+I\}$, $I=\langle 1-i\rangle$
6. $\{I, 1+I, 2+I, 3+I, 4+I\}$, $I=\langle 2+i\rangle$
7. $\{I, 1+I, 2+I, 3+I, i+I, 1+i+I, 2+i+I, 3+i+I\}$, $I=\langle 2+2i\rangle$
8. $\{I, 1+I\}$, $I=\langle 1+i\rangle$
13. $\{....,-3+I,-2+I,-1+I,I,1+I,2+I,3+I,....\}$, $I=\langle x\rangle$
14. $\{I, 1+I\}$, $I=\langle 2,x\rangle$ = B
15. $\{a+bx+I : a,b\in\mathbb{Z}\}$, $I=\langle x^2+x+2\rangle$
16. $\{ax+b+I : a,b\in\mathbb{Z}\}$, $I=\langle x^2+1\rangle = C$
17. $\{ax+b+I : a,b\in\mathbb{Z}_2\}$, $I=\langle 2, x^2+1\rangle = D$
18. $\left\{....,-\frac{3}{2}+I,-\frac{1}{2}+I,I,\frac{1}{2}+I,\frac{3}{2}+I,....\right\}$, $I=\langle x\rangle$
19. $\{a+bx+I : a,b\in\mathbb{Q}\}$, $I=\langle x^2+1\rangle$
20. $\{I, 1+I\}$, $I=\langle 1+i\rangle$

2.4 Ring Homomorphism

Def. Homomorphism : Let $(R, +, \cdot)$ and $(R', +, \cdot)$ be two rings. A mapping $f : R \to R'$ is called a ring homomorphism if it satisfies the following properties:

(i) $f(a+b) = f(a) + f(b)$

(ii) $f(a \cdot b) = f(a) \cdot f(b)$ for all $a, b \in R$.

Remark : It should be noted that '+' and '$\cdot$' on the left hand side of above two properties are of R and those on the right hand side are of R'. So if binary operations in anyone of R and R' are denoted by some other symbols, then they are to be used in above definition accordingly.

Def. A mapping f of a ring R into a ring R' is called

(i) an isomorphism if f is homomorphism, one – one and onto.

(ii) a monomorphism if f is homomorphism and one – one.

(iii) an epimorphism if f is homomorphism and onto.

Def. Isomorphic rings : Two rings R and R' are said to be isomorphic if there exists an isomorphism $f : R \to R'$.

Def. Kernel of a ring homomorphism : Let $f : R \to R'$ be a ring homomorphism , then

Ker $f = \{r \in R : f(r) = 0\}$.

Results :

1. Let $f : R \to R'$ be a ring homomorphism , then
   (i) $f(0) = 0'$, where 0 and $0'$ are additive identities of the rings R and R' respectively.
   (ii) $f(-a) = -f(a)$ for all $a \in R$.
   (iii) For any $r \in R$ and any positive integer n, $f(nr) = n f(r)$.
   (iv) For any $r \in R$ and any positive integer n, $f(r^n) = (f(r))^n$.
2. Let $f : R \to R'$ be a ring homomorphism and A is a subring of R, then $f(A) = \{f(a) : a \in A\}$ is a subring of R'. In words, homomorphic image of a subring is also a subring.
3. Let $f : R \to R'$ be a ring homomorphism and B is a subring of R', then $f^{-1}(B) = \{r \in R : f(r) \in B\}$ is a subring of R. In words, inverse image of a subring is also a subring.
4. Let $f : R \to R'$ be a ring homomorphism and A is an ideal of R then $f(A)$ is an ideal of $f(R)$. Here $f(A)$ need not be an ideal of R'. Further if f is onto then $f(A)$ is an ideal of R'.

189/35 BEHIND RAILWAY STATION, VAISH COLLEGE ROAD, ROHTAK PIN-124001 (HARYANA)
E-mail us on - jrinstituterohtak@gmail.com, balwanmudgil54@gmail.com Mob. 8607383607, 9802177766

5. Let $f: R \to R'$ be a ring homomorphism and B is an ideal of R', then $f^{-1}(B) = \{r \in R: f(r) \in B\}$ is an ideal of R. In words, inverse image of an ideal is also an ideal.
6. Let $f: R \to R'$ be a ring homomorphism and if R is commutative, then $f(R)$ is commutative. Further if f is onto then R' is commutative. In words, image of a commutative ring is also commutative.
7. Let $f: R \to R'$ be a ring homomorphism and $1 \in R$ be the unity of R, then $f(1)$ is the unity of $f(R)$. Further if f is onto then $f(1)$ is the unity of R'.
8. If $f: R \to R'$ be a ring homomorphism , then Ker f is an ideal of R.
9. Let $f: R \to R'$ be a ring homomorphism , then f is one –one iff Ker $f = \{0\}$.
10. Any homomorphism of a field is either a monomorphism or takes each element into '0'.
11. Let $f: R \to R'$ be a ring homomorphism and $1 \in R$ be the unity of R, then $f(1)$ is an idempotent element of R' i.e., image of unity is always an idempotent element.
12. If $f: \mathbb{Z}_m \to \mathbb{Z}_n$ be a ring homomorphism, then the image of 1 i.e., $f(1)$ must be an idempotent element and additive order of $f(1)$ must divide m.
13. If n divides m and a is an idempotent of $\mathbb{Z}_n$, then the mapping $f(x) = ax$ is a ring homomorphism from $\mathbb{Z}_m$ to $\mathbb{Z}_n$.
14. The number of ring homomorphisms from $\mathbb{Z}_m$ to $\mathbb{Z}_n$ is $2^{w(n)-w\left(\frac{n}{\gcd(m,n)}\right)}$, where $w(a)$ is the number of distinct prime factors of a.
15. Let $f: R \to R'$ be a ring isomorphism then f^{-1} is an isomorphism from R' onto R.
16. Fundamental Theorem of Ring Homomorphism :

    Let $f: R \to R'$ be homomorphism , then $R/\text{Ker}\, f \cong f(R)$

    or

    Every homomorphic image of a ring is isomorphic to some quotient ring .
17. If $f: R \to R'$ is onto homomorphism , then $f(R) = R'$ and so above theorem takes the form $R/\text{Ker}\, f \cong R'$.
18. Let R be a ring with unity e. Show that the mapping $\phi: \mathbb{Z} \to R$ given by $\phi(n) = ne$ is a ring

homomorphism.

19. If R is a ring with unity and the characteristic of R is $n>0$, then R contains a subring isomorphic to $\mathbb{Z}_n$. If the characteristic of R is zero, then R contains a subring isomorphic to $\mathbb{Z}$.
20. If R is CRU then $R[x]/\langle x\rangle \cong R$ and $R[x]/\langle x+a\rangle \cong R$ where $a \in R$.
21. If R is a CRU then $R[x]/\langle x^2+1\rangle \cong R[i]$.
22. If R is a CRU then $R[x,y]/\langle y+a\rangle \cong R[x]$.
23. First theorem of isomorphism : Let R be a ring and S, T are ideals of R such that $S \subseteq T$ then $R/T \cong \dfrac{R/S}{T/S}$.
24. Second theorem of isomorphism : Let R be a ring and S,T are ideals of R then $(S+T)/S \cong T/(S \cap T)$.
25. If F is a finite field of characteristic p then the function $f : F \to F$ defined by $f(a)=a^p$ is an isomorphism.
26. Let $n>1$ be a positive integer then there are atleast two non isomorphic rings of order n. e.g. $(\mathbb{Z}_n,+_n,\times_n)$ and $(\mathbb{Z}_n,+_n,\cdot)$ where $a\cdot b=0$ for all $a,b \in \mathbb{Z}_n$.
27. There are eleven non isomorphic rings of order 4.

Exercise 2.4

1. Show that the mapping $f : \mathbb{C} \to \mathbb{C}$ defined by $f(a+ib)=a-ib$ is a homomorphism.
2. Let $R=\{a+\sqrt{5}b : a,b \in \mathbb{Z}\}$ be a ring under usual addition and multiplication of real numbers. Define $\phi : R \to R$ by $\phi(a+\sqrt{5}b)=a-\sqrt{5}b$. Show that ϕ is a homomorphism of R onto R' and its kernel consists of 0 only i.e. $\operatorname{Ker}\phi=\{0\}$.
3. Determine all ring homomorphisms from $\mathbb{R}$ to $\mathbb{R}$.
4. Show that the mapping $\phi : \mathbb{Z} \to \mathbb{Z}_m$ given by $\phi(x)=x \bmod m$, where m is any positive integer, is a ring homomorphism.
5. Describe all ring homomorphisms from $\mathbb{Z}_6$ to $\mathbb{Z}_6$. Determine all ring homomorphisms from $\mathbb{Z}_{20}$ to $\mathbb{Z}_{30}$.
6. Determine all ring homomorphisms from $\mathbb{Z}$ to $\mathbb{Z}$.
7. Determine all ring homomorphisms from $\mathbb{Q}$ to $\mathbb{Q}$.
8. Determine all ring homomorphisms from $\mathbb{Z}\times\mathbb{Z}$ to $\mathbb{Z}$.

9. Let $R=\left\{\begin{bmatrix} a & b \\ b & a \end{bmatrix} : a,b \in \mathbb{Z}\right\}$ and let ϕ be the mapping that takes $\begin{bmatrix} a & b \\ b & a \end{bmatrix}$ to $a-b$.

   (i) Show that ϕ is a homomorphism

   (ii) Determine the kernel of ϕ.

   (iii) Show that $R/\text{Ker}\,\phi$ is isomorphic to $\mathbb{Z}$.

   (iv) Is Ker ϕ a prime ideal ?

   (v) Is Ker ϕ a maximal ideal ?

Answers

3. The zero map and the identity map.

5. $f(x)=ax,\ a\in\{0,1,3,4\}$; $f(x)=ax,\ a\in\{0,6,15,21\}$

6. The zero map and the identity map.

7. The zero map and the identity map.

8. $f(a,b)=x,\ x\in\{0,a,b\}$

9. (ii) $\text{Ker}\,\phi=\left\{\begin{bmatrix} a & a \\ a & a \end{bmatrix} : a\in\mathbb{Z}\right\}$ (iv) yes (v) no

2.5 Embedding of rings and quotient fields

Def. Imbedding of a ring into another ring : A ring R is said to be imbedded in a ring R' if there exists a mapping $f : \mathrm{R}\to\mathrm{R}'$ such that

(i) f is homomorphism

(ii) f is one – one

We then say that R' is an extension ring or over ring of R .

Remark : Since $f : \mathrm{R}\to\mathrm{R}'$ is a homomorphism and one – one mapping , if we consider $f : \mathrm{R}\to f(\mathrm{R})$ then it obviously becomes an isomorphism . Thus R is isomorphic to $f(\mathrm{R})$ and f (R) is a subring of R .

Results :

1. A ring without unity can be imbedded into a ring with unity. Let R be a ring without unity.

Consider the set $R\times\mathbb{Z}$ where $\mathbb{Z}$ is the ring of integers. Define '+' and '.' on $R\times\mathbb{Z}$ as :

$$(r,n)+(s,m) = (r+s,n+m)$$

$$(r,n).(s,m) = (rs+ns+mr,mn)$$

Then it can be proved that $R\times\mathbb{Z}$ is a ring under these two operations.

Now we claim that $R' = R\times\mathbb{Z}$ is a ring with unity.

Let 0 be zero element of R then $(0\ ,\ 1)\in R\times\mathbb{Z}$, where $1\in\mathbb{Z}$

Let $(a,m)\in R'$, then we have

$$(0\ ,\ 1)(a,m) = (0.a+0.m+1.a,1.m) = (a,m)$$

$$(a,m)(0,1) = (a.0+a.1+m.0,m.1) = (a,m)$$

$\Rightarrow$ $(0\ ,\ 1)$ is a unity of R' . So R' is a ring with unity.

Now , we claim that R can be imbedded into R'.

Define a mapping $f : R\to R'$ by setting $f(r) = (r,0)$ for all $r\in R$

(i) f is homomorphism : Let r , $s\in R$ be any two elements, then

$$f(r+s) = (r+s\ ,\ 0)$$

$$= (r,0)+(s,0) = f(r)+f(s)$$

and $$f(rs) = (rs,0) = (rs+0.s+r.0,0)$$

$$= (r,0).(s,0) = f(r).f(s)\ .$$

(ii) f is one – one : Let r and s be any two elements of R such that

$$f(r) = f(s) \quad\Rightarrow\quad (r,0) = (s,0)$$

$$\Rightarrow\quad r = s$$

So f is one – one homomorphism.

Hence , R is imbedded into R'.

2. Every integral domain can be imbedded into a field.

Proof : Let D be an integral domain with at least two elements and let

$$D_0 = \{x\in D : x\neq 0\} = D-\{0\}$$

Consider the set , $D\times D_0 = \{(a,b) : a\in D\ ,\ b\in D_0\}$

Define a relation '~' on $D\times D_0$ as $(a,b)\sim(c,d)$ iff $ad = bc$

We claim that '~' is an equivalence relation.

(i) Reflexivity : Let $(a\ ,\ b)\in D\times D_0$. Since D is commutative , so

$$ab = ba \quad \Rightarrow \quad (a,b) \sim (a,b).$$

(ii) Symmetry : Let $(a,b) \sim (c,d) \quad \Rightarrow \quad ad = bc$

$$\Rightarrow \quad cb = da \quad \Rightarrow \quad (c,d) \sim (a,b).$$

(iii) Transitivity : Let $(a,b) \sim (c,d)$ and $(c,d) \sim (e,f)$

$$\Rightarrow \quad ad = bc \quad \text{and} \quad cf = de$$

Now $ad = bc \quad \Rightarrow \quad adf = bcf \quad \Rightarrow \quad adf = bde$ [Since $cf = de$]

$$\Rightarrow \quad daf = dbe$$

$$\Rightarrow \quad d(af - be) = 0$$

But $d \neq 0$ and D is without zero divisors, so $af - be = 0 \quad \Rightarrow \quad af = be$

$$\Rightarrow \quad (a,b) \sim (e,f)$$

Hence , '~' is an equivalence relation on $D \times D_0$ .Therefore it partitions the set $D \times D_0$ into equivalence classes and let $\frac{a}{b}$ denotes the equivalence class to which (a,b) belongs

$$\text{i.e.} \quad \frac{a}{b} = \{(x,y) \in D \times D_0 : (a,b) \sim (x,y)\}$$

Let F be the set of all equivalence classes defined above , i.e.

$$F = \left\{ \frac{a}{b} : a \in D, b \in D_0 \right\}$$

Let us define two operations '+' and '.' on F as

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \quad \text{and} \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

We show that addition and multiplication in F are well defined.

(i) Addition is well defined : Let $\frac{a}{b} = \frac{a'}{b'}$ and $\frac{c}{d} = \frac{c'}{d'}$

$$\Rightarrow \quad ab' = ba' \quad \text{and} \quad cd' = c'd$$

$$\Rightarrow \quad ab'dd' = ba'dd' \quad \text{and} \quad bb'cd' = bb'dc'$$

$$\Rightarrow \quad ab'dd' + bb'cd' = ba'dd' + bb'dc'$$

$$\Rightarrow \quad adb'd' + bcb'd' = a'd'bd + b'c'bd$$

$$\Rightarrow \quad (ad + bc)b'd' = (a'd' + b'c')bd$$

$$\Rightarrow \quad \frac{ad + bc}{bd} = \frac{a'd' + b'c'}{b'd'}$$

$$\Rightarrow \qquad \frac{a}{b}+\frac{c}{d}=\frac{a'}{b'}+\frac{c'}{d'}.$$

(ii) Multiplication is well defined : Let $\frac{a}{b} = \frac{a'}{b'}$ and $\frac{c}{d} = \frac{c'}{d'}$

$$\Rightarrow \qquad ab' = ba' \quad \text{and} \quad cd' = dc'$$

$$\Rightarrow \qquad ab'cd' = ba'dc'$$

$$\Rightarrow \qquad (ac)(b'd') = (a'c')(bd)$$

$$\Rightarrow \qquad \frac{ac}{bd} = \frac{a'c'}{b'd'}$$

$$\Rightarrow \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{a'}{b'} \cdot \frac{c'}{d'}$$

Now , we claim that F is a field.

(1) F is closed under addition : Let $\frac{a}{b}$, $\frac{c}{d} \in$ F, then $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$

Now, since $a,b,c,d \in$ D $\Rightarrow$ $ad+bc \in$ D

Also $b \neq 0$, $d \neq 0$ $\Rightarrow$ $bd \neq 0$, since D is an integral domain. Hence $\frac{ad+bc}{bd} \in$ F.

(2) Addition is associative : Let $\frac{a}{b}$, $\frac{c}{d}$, $\frac{e}{f} \in$ F, then

$$\frac{a}{b} + \left(\frac{c}{d}+\frac{e}{f}\right) = \frac{a}{b} + \left(\frac{cf+de}{df}\right)$$

$$= \frac{adf+b(cf+de)}{b(df)}$$

$$= \frac{adf+bcf+bde}{bdf}$$

$$= \frac{(ad+bc)f+(bd)e}{(bd)f}$$

$$= \left(\frac{ad+bc}{bd}\right)+\frac{e}{f} = \left(\frac{a}{b}+\frac{c}{d}\right)+\frac{e}{f}.$$

(3) Existence of additive identity : Let $\frac{a}{b} \in$ F. For $k(\neq 0) \in$ D . Consider $\frac{0}{k} \in$ F

Now , $\frac{a}{b}+\frac{0}{k} = \frac{ak+0.b}{b.k} = \frac{a}{b}$

and $\frac{0}{k}+\frac{a}{b} = \frac{0.b+a.k}{k.b} = \frac{a}{b}$

Hence, $\frac{0}{k}$ is additive identity of F.

(4) Existence of additive inverse : Let $\frac{a}{b} \in F$, then $a \in D \Rightarrow -a \in D$

Consider the element $\frac{-a}{b} \in F$, then we have ,

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

and $$\frac{-a}{b} + \frac{a}{b} = \frac{-ab+ab}{b^2} = \frac{0}{b^2}$$

So , $\frac{-a}{b}$ is additive inverse of $\frac{a}{b}$.

(5) Addition is commutative :

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} = \frac{cb+da}{db} = \frac{c}{d} + \frac{a}{b}$$

(6) F is closed under multiplication : Let $\frac{a}{b}, \frac{c}{d} \in F$, then $\frac{a}{b} . \frac{c}{d} = \frac{ac}{bd}$

Now, since $a, c \in D \Rightarrow ac \in D$

Also $b \neq 0$, $d \neq 0 \Rightarrow bd \neq 0$, since D is an integral domain. Hence $\frac{ac}{bd} \in F$.

(7) Multiplication is Associative : Let $\frac{a}{b}$, $\frac{c}{d}$, $\frac{e}{f} \in$ F, then

$$\frac{a}{b}\left(\frac{c}{d}.\frac{e}{f}\right) = \frac{a}{b}\left(\frac{ce}{df}\right) = \frac{a(ce)}{b(df)} = \frac{(ac)e}{(bd)f} = \frac{ac}{bd}.\frac{e}{f} = \left(\frac{a}{b}.\frac{c}{d}\right).\frac{e}{f}$$

(8) Multiplication is distributive over addition : Let $\frac{a}{b}$, $\frac{c}{d}$, $\frac{e}{f} \in$ F

Then we have ,

$$\frac{a}{b}.\left(\frac{c}{d}+\frac{e}{f}\right) = \frac{a}{b}.\left(\frac{cf+de}{df}\right) = \frac{a(cf+de)}{b(df)} = \frac{acf+ade}{bdf}$$

Also , $$\frac{a}{b}.\frac{c}{d} + \frac{a}{b}.\frac{e}{f} = \frac{ac}{bd} + \frac{ae}{bf} = \frac{acbf+aebd}{bdbf} = \frac{(acf+ade)b}{(bdf)b} = \frac{acf+ade}{bdf}$$

Thus $\frac{a}{b}.\left(\frac{c}{d}+\frac{e}{f}\right) = \frac{a}{b}.\frac{c}{d}+\frac{a}{b}.\frac{e}{f}$. So multiplication is left distributive over addition .

Similarly , we can prove that multiplication is right distributive over addition .

(9) Existence of unity : Let $\frac{a}{b} \in$ F. For $k(\neq 0) \in$ D , $\frac{k}{k} \in$ F

Now , $\frac{a}{b}.\frac{k}{k} = \frac{ak}{bk} = \frac{a}{b}$ and $\frac{k}{k}.\frac{a}{b} = \frac{ka}{kb} = \frac{a}{b}$

Hence $\frac{k}{k}$ is multiplicative identity of F.

(10) Existence of multiplicative inverse : Let $\frac{a}{b}$ be any non – zero element of F i.e. $\frac{a}{b} \neq \frac{0}{k}$

$(k \neq 0)$, then $a \neq 0$. Take $\frac{b}{a} \in$ F , then

$\frac{a}{b}.\frac{b}{a} = \frac{ab}{ba} = \frac{ab}{ab}$ and $\frac{b}{a}.\frac{a}{b} = \frac{ba}{ab} = \frac{ab}{ab}$

Hence $\frac{b}{a}$ is multiplicative inverse of $\frac{a}{b}$.

(11) Multiplication is commutative : Let $\frac{a}{b}$, $\frac{c}{d} \in$ F

then $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} = \frac{ca}{db} = \frac{c}{d}.\frac{a}{b}$.

Hence F is a field. This field is called the field of quotients or quotient field of the integral domain D. We shall prove that F is the field we are searching i.e. D is imbedded in F . Before doing so we first notice that if $b \neq 0$, $c \neq 0$ in D then $\frac{ab}{b} = \frac{ac}{c}$ because $(ab)c = b(ac)$ i.e. $(ab,b) \sim (ac,c)$. Let us denote $\frac{ab}{b}$ or $\frac{ac}{c}$ by $\frac{a}{1}$.

Now we define ϕ : D $\to$ F by setting $\phi(a) = \frac{a}{1}$ for all $a \in$ D.

(i) ϕ is homomorphism : We have,

$$\phi(a+b) = \frac{a+b}{1} = \frac{a.1+b.1}{1.1} = \frac{a}{1}+\frac{b}{1} = \phi(a)+\phi(b)$$

and $\phi(ab) = \frac{ab}{1} = \frac{a}{1}.\frac{b}{1} = \phi(a).\phi(b)$

Hence ϕ is homomorphism

(ii) ϕ is one – one : Let a and b be two elements of D such that

189/35 BEHIND RAILWAY STATION, VAISH COLLEGE ROAD, ROHTAK PIN-124001 (HARYANA)
E-mail us on - jrinstituterohtak@gmail.com, balwanmudgil54@gmail.com Mob. 8607383607, 9802177766

$$\phi(a) = \phi(b)$$

$$\Rightarrow \quad \frac{a}{1} = \frac{b}{1}$$

$$\Rightarrow \quad a = b. \text{ So } \phi \text{ is one – one}$$

Hence D is imbedded into F .

Def. Quotient Field : The quotient field F of an integral domain D is defined as

$$\text{F} = \left\{ \frac{a}{b} \ : \ a, b \in \text{D} \text{ and } b \neq 0 \right\} .$$

3. Let D_1 and D_2 be two isomorphic integral domains and let F_1 and F_2 be their respective fields of quotients , then show that F_1 and F_2 are also isomorphic.

Proof : Let D_1 and D_2 be isomorphic integral domains so that there exists a mapping $\phi : D_1 \to D_2$ which is ring isomorphism.

Now F_1 and F_2 are quotient fields of D_1 and D_2 respectively so by definition of quotient field, we have

$$F_1 = \left\{ \frac{a}{b} \ : \ a, b \in D_1 \text{ and } b \neq 0 \right\}$$

$$F_2 = \left\{ \frac{x}{y} \ : \ x, y \in D_2 \text{ and } y \neq 0 \right\}$$

We define a mapping $\psi : F_1 \to F_2$ by setting $\psi\left(\frac{a}{b}\right) = \frac{\phi(a)}{\phi(b)}$.

(i) ψ is homomorphism : Let $\frac{a}{b}$ and $\frac{c}{d}$ be any two elements of F_1 , then we have

$$\psi\left(\frac{a}{b} + \frac{c}{d}\right) = \psi\left(\frac{ad + bc}{bd}\right)$$

$$= \frac{\phi(ad + bc)}{\phi(bd)}$$

$$= \frac{\phi(a)\phi(d) + \phi(b)\phi(c)}{\phi(b)\phi(d)} \qquad [\text{Since } \phi \text{ is homomorphism}]$$

$$= \frac{\phi(a)}{\phi(b)} + \frac{\phi(c)}{\phi(d)} = \psi\left(\frac{a}{b}\right) + \psi\left(\frac{c}{d}\right)$$

Also , $\psi\left(\frac{a}{b} . \frac{c}{d}\right) = \psi\left(\frac{ac}{bd}\right)$

$$= \frac{\phi(ac)}{\phi(bd)} = \frac{\phi(a)\phi(c)}{\phi(b)\phi(d)} = \frac{\phi(a)}{\phi(b)} \cdot \frac{\phi(c)}{\phi(d)} = \psi\left(\frac{a}{b}\right)\psi\left(\frac{c}{d}\right)$$

$\Rightarrow$ ψ is a homomorphism.

(ii) ψ is one – one : Let $\frac{a}{b}$ and $\frac{c}{d}$ be any two elements of F_1 such that

$$\psi\left(\frac{a}{b}\right) = \psi\left(\frac{c}{d}\right)$$

$$\Rightarrow \quad \frac{\phi(a)}{\phi(b)} = \frac{\phi(c)}{\phi(d)}$$

$$\Rightarrow \quad \phi(a)\ \phi(d) = \phi(b)\phi(c)$$

$$\Rightarrow \quad \phi(ad) = \phi(bc) \qquad \text{[Since } \phi \text{ is homomorphism]}$$

$$\Rightarrow \quad ad = bc \qquad \text{[Since } \phi \text{ is one – one]}$$

$$\Rightarrow \quad \frac{a}{b} = \frac{c}{d}$$

So, ψ is one – one.

(iii) ψ is onto : Let $\frac{x}{y} \in F_2$ be any arbitrary element , then $x, y \in D_2$ and $y \neq 0$.

Since ϕ is onto , so there exist $a, b \in D_1$ such that

$$\phi(a) = x \quad \text{and} \quad \phi(b) = y, \quad b \neq 0$$

$$\Rightarrow \quad \frac{a}{b} \in F_1 \text{ and } \psi\left(\frac{a}{b}\right) = \frac{\phi(a)}{\phi(b)} = \frac{x}{y}$$

Thus $\frac{a}{b}$ is pre-image of $\frac{x}{y}$ under ψ and so ψ is onto.

Hence F_1 is isomorphic to F_2.

4. Field of quotients of an integral domain is unique upto isomorphism. In other words, if F_1 and F_2 are two field of quotients of an integral domain D , then $F_1 \cong F_2$.

Proof : Let F_1 and F_2 be two field of quotients of an integral domain D , then since $D \cong D$

So , by last theorem , $F_1 \cong F_2$.

Hence field of quotients is unique upto isomorphism.

5. The field of quotients of the integral domain $\mathbb{Z}$ is $\mathbb{Q}$.

6. The field of quotients of the integral domain $\mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z}\}$ is $\mathbb{Q}[i]$.

7. The field of quotients of an integral domain *D* is the smallest field containing *D*.

8. The field of quotients of a field is equal to itself.

189/35 BEHIND RAILWAY STATION, VAISH COLLEGE ROAD, ROHTAK PIN-124001 (HARYANA)
E-mail us on - jrinstituterohtak@gmail.com, balwanmudgil54@gmail.com Mob. 8607383607, 9802177766

---------- S C Q ----------

1. The number of prime ideals of $\mathbb{Z}_{10}$ is
   1. 1 2. 0
   3. 2 4. 5

2. The number of prime ideals of $\mathbb{Z}_{10^5}$ is
   1. 2 2. 5
   3. 10 4. 10000

3. Let *R* be a ring and *M* is an ideal of *R*, then
   1. If *M* is maximal ideal then it is prime ideal.
   2. If *M* is prime ideal then it is maximal ideal.
   3. Both (a) and (b).
   4. Neither (a) nor (b).

4. The number of homomorphism $\phi:\mathbb{Z}_5\to\mathbb{Z}_{20}$ is
   1. 1 2. 2
   3. 4 4. 5

5. If $f:\mathbb{R}[x]\to\mathbb{C}$ as $f\left(p(x)\right)=p(i)$, where $\mathbb{R}[x]$ is a polynomial ring over $\mathbb{R}$, then
   1. f is not homomorphism
   2. f is homomorphism and Ker $f=\langle x-1\rangle$
   3. f is homomorphism and Ker $f=\langle x^2+1\rangle$
   4. f is homomorphism and Ker $f=\langle x^2-1\rangle$

6. Let $(E,+,\cdot)$ be the ring of even integers and $A=\{4n:n\in\mathbb{Z}\}$, then which is/are correct
   I. *A* is an ideal.
   II. *A* is prime ideal.
   III. *A* is maximal ideal.
   1. I only 2. I and II
   3. I and III only 4. I, II and III

7. The number of elements in the field $\dfrac{\mathbb{Z}[i]}{\langle 2+i\rangle}$ is
   1. 2 2. 3
   3. 5 4. ∞

8. Let *F* be a finite field. If $f:F\to F$, given by $f(x)=x^3$ is a ring homomorphism, then
   1. $F=\dfrac{\mathbb{Z}}{3\mathbb{Z}}$.
   2. $F=\dfrac{\mathbb{Z}}{2\mathbb{Z}}$ or characteristic of $F=3$.
   3. $F=\dfrac{\mathbb{Z}}{2\mathbb{Z}}$ or $\dfrac{\mathbb{Z}}{3\mathbb{Z}}$.
   4. characteristic of *F* is 3.

9. Let $\mathbb{R}[x]$ be the polynomial ring in *x* over $\mathbb{R}$ and let $I=\langle x^2+1\rangle$ be the ideal generated by the polynomial x^2+1 in $\mathbb{R}[x]$. Then
   1. *I* is a maximal ideal.
   2. *I* is a prime ideal but not a maximal ideal.
   3. *I* is not a prime ideal.
   4. $\mathbb{R}[x]/I$ has zero divisors.

   (GATE 2007)

10. If *S* is a finite commutative ring with unity 1, then
    1. each prime ideal is a maximal ideal.
    2. *S* may have a prime ideal which is not maximal.
    3. *S* has no non-trivial maximal ideals.
    4. *S* is a field.

11. Let $I_1=\langle x^2-3\rangle$ and $I_2=\{f(x)\in\mathbb{Z}_{11}[x]:f(2)=0\}$ be two ideals of $\mathbb{Z}_{11}[x]$. Then
    1. I_1 and I_2 both are maximal.
    2. I_1 is maximal but I_2 is not.
    3. I_2 is maximal but I_1 is not.
    4. I_1 and I_2 both are not maximal.

12. Let $f(x)=x^3-9x^2+9x+3$. Then, $f(x)$ is
    1. irreducible over $\mathbb{Q}$ but reducible over $\mathbb{Z}_2$.

2. irreducible over both $\mathbb{Q}$ and $\mathbb{Z}_2$.
3. reducible over $\mathbb{Q}$ but irreducible over $\mathbb{Z}_2$.
4. reducible over both $\mathbb{Q}$ and $\mathbb{Z}_2$.

13. Let $f(x)=x^5+4x^4+4x^3+4x^2+x+1$. Then, the zeros of $f(x)$ over $\mathbb{Z}_5$ are 1 and 3 with respective multiplicity
1. 1 and 4 2. 2 and 3
3. 2 and 2 4. 1 and 2

(GATE 2007)

14. Let $f:\mathbb{C}\to\mathbb{R}$ such that $f(x+iy)=x$. Then, Ker f is
1. $\{x:x\in\mathbb{R}\}$
2. $\{0\}$
3. $\{iy:y\in\mathbb{R}\}$
4. $\{x+iy:x \text{ and } y \text{ are nonzero}\}$

15. Let $R=\left\{\frac{a}{b}:a,b\in\mathbb{Z},b \text{ is odd}\right\}$. Then, R is a ring such that
1. R has unique maximal ideal $I=\left\{\frac{a}{b}\in R:a \text{ is even}\right\}$.
2. R has infinitely many maximal ideals.
3. R has finitely many but more than one maximal ideals.
4. R has no maximal ideal.

16. The field of quotients of the integral domain $\mathbb{Z}$ is :
1. $\mathbb{Z}$ 2. $\mathbb{Q}$
3. $\mathbb{R}$ 4. $\mathbb{C}$

17. Let $I=\langle x^4+x^3+x^2+x+1\rangle$ be the ideal in $\mathbb{Z}_2[x]$ and $F=\mathbb{Z}_2[x]/I$. Then,
1. F is an infinite field.
2. F is a finite field of 4 elements.
3. F is a finite field of 8 elements.
4. F is a finite field of 16 elements.

18. Let the set $\mathbb{Z}/n\mathbb{Z}$ denote the ring of integers modulo n under addition and multiplication modulo n. Then, $\mathbb{Z}/9\mathbb{Z}$ is not a subring of $\mathbb{Z}/12\mathbb{Z}$ because
1. $\mathbb{Z}/9\mathbb{Z}$ is not a subset of $\mathbb{Z}/12\mathbb{Z}$.
2. G.C.D.$(9, 12)=3\neq 1$
3. 12 is not a power of 3.
4. 9 does not divide 12.

(GATE 2005)

19. The number of elements in $\frac{\mathbb{Z}_{11}[x]}{\langle x^2+1\rangle}$ is
1. 11 2. 121
3. 1331 4. None of these

20. If p is a prime and $\mathbb{Z}_{p^4}$ denote the ring of integers modulo p^4, then the number of maximal ideals in $\mathbb{Z}_{p^4}$ is
1. 4 2. 2
3. 3 4. 1

(GATE 2001)

21. The polynomial $f(x)=x^5+5$ is
1. irreducible over $\mathbb{C}$
2. irreducible over $\mathbb{R}$
3. irreducible over $\mathbb{Q}$
4. not irreducible over $\mathbb{Q}$

(GATE 2001)

22. Which of the following is not a prime ideal of $\mathbb{Z}$
1. $2\mathbb{Z}$ 2. $4\mathbb{Z}$
3. $5\mathbb{Z}$ 4. $7\mathbb{Z}$

23. Which of the following is not a field ?
1. $\mathbb{Z}/2\mathbb{Z}$ 2. $\mathbb{Z}/3\mathbb{Z}$
3. $\mathbb{Z}/4\mathbb{Z}$ 4. $\mathbb{Z}/5\mathbb{Z}$

24. Let $R=\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}$ and $I=\mathbb{Z}\times\mathbb{Z}\times\{0\}$. Then, which of the following statement is correct ?
1. I is a maximal ideal but not prime ideal of R.
2. I is a prime ideal but not a maximal ideal of R.
3. I is both maximal as well as prime ideal of R.
4. I is neither a maximal ideal nor a prime ideal of R.

(GATE 2012)

25. Let m and n be coprime natural numbers. Then, the kernel of the ring homomorphism $\phi:\mathbb{Z}\to\mathbb{Z}_m\times\mathbb{Z}_n$, defined by $\phi(x)=(\overline{x},\overline{x})$, is
    1. $m\mathbb{Z}$ 2. $mn\mathbb{Z}$
    3. $n\mathbb{Z}$ 4. $\mathbb{Z}$

    (GATE 2002)

26. Let $C[0,1]$ be the set of all continuous functions defined on the interval $[0,1]$. On this set, define addition and multiplication pointwise. Then, $C[0,1]$ is
    1. group but not a ring.
    2. a ring but not an integral domain.
    3. a field.
    4. an integral domain but not a field.

    (GATE 2003)

27. Set of multiples of 4 forms an ideal in $\mathbb{Z}$, the ring of integers under usual addition and multiplication. This ideal is
    1. a prime ideal but not a maximal ideal.
    2. a maximal ideal but not a prime ideal.
    3. both a prime ideal and a maximal ideal.
    4. neither a prime ideal nor a maximal ideal.

    (GATE 2003)

28. Let $S=\left\{\begin{bmatrix}a & b\\ 0 & c\end{bmatrix}: a,b,c\in\mathbb{R}\right\}$ be the ring under matrix addition and multiplication. Then, the subset $\left\{\begin{bmatrix}0 & p\\ 0 & 0\end{bmatrix}: p\in\mathbb{R}\right\}$ is
    1. not an ideal of S.
    2. an ideal but not a prime ideal of S.
    3. is a prime ideal but not a maximal ideal of S.
    4. is a maximal ideal of S.

    (GATE 2004)

29. Which of the following is a maximal ideal of the ring $(P(\mathbb{N}),\Delta,\cap)$
    1. $P(A)$ where $A=\{5,6,7,8,....\}$
    2. $P(A)$ where $A=\{4,5,6,7,....\}$
    3. $P(A)$ where $A=\{3,4,5,6,....\}$
    4. $P(A)$ where $A=\{2,3,4,5,....\}$

30. Which one of the following ideals of the ring $\mathbb{Z}[i]$ of Gaussian integers is not maximal ?
    1. $\langle 1+i\rangle$ 2. $\langle 1-i\rangle$
    3. $\langle 2+i\rangle$ 4. $\langle 3+i\rangle$

    (GATE 2009)

31. Consider the polynomial ring $\mathbb{Q}[x]$. The ideal of $\mathbb{Q}[x]$ generated by x^2-3 is
    1. maximal but not prime.
    2. prime but not maximal.
    3. both maximal and prime.
    4. neither maximal nor prime.

    (GATE 2010)

32. For the rings $L=\dfrac{\mathbb{R}[x]}{\langle x^2-x+1\rangle}$; $M=\dfrac{\mathbb{R}[x]}{\langle x^2+x+1\rangle}$; $N=\dfrac{\mathbb{R}[x]}{\langle x^2+2x+1\rangle}$. Which one of the following is true ?
    1. L is isomorphic to M ; L is not isomorphic to N ; M is not isomorphic to N.
    2. M is isomorphic to N ; M is not isomorphic to L ; N is not isomorphic to L.
    3. L is isomorphic to M ; M is isomorphic to N.
    4. L is not isomorphic to M ; L is not isomorphic to N ; M is not isomorphic to N.

    (GATE 2011)

33. If $\mathbb{Z}[i]$ is the ring of Gaussian integers , the quotient $\dfrac{\mathbb{Z}[i]}{\langle 3-i\rangle}$ is isomorphic to
    1. $\mathbb{Z}$ 2. $\dfrac{\mathbb{Z}}{3\mathbb{Z}}$
    3. $\dfrac{\mathbb{Z}}{4\mathbb{Z}}$ 4. $\dfrac{\mathbb{Z}}{10\mathbb{Z}}$

34. The number of maximal ideals in $\mathbb{Z}_{27}$ is
1. 0 2. 1
3. 2 4. 3

(GATE 2008)

35. Let $f(x)=x^3+2x^2+1$ and $g(x)=2x^2+x+2$. Then over $\mathbb{Z}_{(3)}$
1. $f(x)$ and $g(x)$ are irreducible.
2. $f(x)$ is irreducible, but $g(x)$ is not.
3. $g(x)$ is irreducible, but $f(x)$ is not.
4. neither $f(x)$ nor $g(x)$ is irreducible.

(CSIR NET June 2012)

36. The number of non trivial ring homomorphisms from $\mathbb{Z}_{(12)}$ to $\mathbb{Z}_{(28)}$ is
1. 1 2. 3 3. 4 4. 7

(CSIR NET June 2012)

37. Let R be the ring $\mathbb{Z}[x]/\left(\left(x^2+x+1\right)\left(x^3+x+1\right)\right)$ and I be the ideal generated by 2 in R. What is the cardinality of the ring R/I ?
1. 27 2. 32
3. 64 4. Infinite

(CSIR NET June 2015)

38. Which of the following is an irreducible factor of $x^{12}-1$ over $\mathbb{Q}$?
1. x^8+x^4+1
2. x^4+1
3. x^4-x^2+1
4. $x^5-x^4+x^3-x^2+x-1$

(CSIR NET Dec 2015)

39. How many elements does the set $\{z\in\mathbb{C}\,|\,z^{60}=-1,\ z^k\neq -1 \text{ for } 0<k<60\}$ have ?
1. 24 2. 30
3. 32 4. 45

(CSIR NET June 2015)

40. What is the cardinality of the set $\left\{z\in\mathbb{C}\,|\,z^{98}=1 \text{ and } z^n\neq 1 \text{ for any } 0<n<98\right\}$?
1. 0 2. 12
3. 42 4. 49

(CSIR NET Dec 2015)

41. Let p be a prime number. How many distinct sub-rings (with unity) of cardinality p does the field F_{p^2} have?
1. 0 2. 1
3. p 4. p^2

(CSIR NET June 2016)

42. Consider the ideal $I=\left(x^2+1, y\right)$ in the polynomial ring $\mathbb{C}[x,y]$. Which of the following statements is true ?
1. I is a maximal ideal
2. I is a prime ideal but not a maximal ideal
3. I is a maximal ideal but not a prime ideal
4. I is neither a prime ideal nor a maximal ideal

(CSIR NET June 2017)

43. If R is a finite field of characteristic p, then given any $b\in R$, $\exists\ a\in R$ such that
1. $a^p=b$ 2. $a^p=b-1$
3. $a^p=b^{-1}$ 4. None of these

---------- M C Q ----------

1. If S and T are two ideals of a ring R, then
1. $\frac{S+T}{S}\cong\frac{S}{S\cap T}$
2. $\frac{S+T}{S}\cong\frac{T}{S\cap T}$
3. $\frac{S+T}{T}\cong\frac{T}{S\cap T}$
4. $\frac{R}{S}\cong\frac{R/T}{S/T}$ if $T\subseteq S$

2. Which of the following is/are correct ?
1. Field of quotient of a finite integral domain D is D itself.
2. The quotient field F of an integral domain D is the largest field containing D.
3. Quotient field of the integral domain $\mathbb{Z}_5=\{0,1,2,3,4\}$ is $\mathbb{Z}_5$.
4. The field of quotient of the integral domain $\mathbb{Z}$ of integers is $\mathbb{R}$.

3. If R is a commutative ring with unity and I be any ideal of R, then
   1. If I is maximal, then R/I is a field.
   2. If I is maximal, then R/I is an integral domain.
   3. If I is prime ideal, then R/I is an integral domain.
   4. If I is prime ideal, then R/I is a field.

4. Let R be a commutative ring with unity. If every ideal of R is prime, then
   1. R is an Integral Domain.
   2. R is not an Integral Domain.
   3. R is a field.
   4. R is not a field.

5. Which of the following is maximal ideal ?
   1. $\left\{ f \in C[0,1] : f\left(\frac{1}{2}\right) = 0 \right\}$
   2. $\left\{ f \in C[0,1] : f\left(\frac{1}{3}\right) = 0 \right\}$
   3. $\left\{ f \in C[0,1] : f\left(\frac{1}{2}\right) = 0 = f\left(\frac{1}{3}\right) \right\}$
   4. $\left\{ f \in C[0,1] : f\left(\frac{1}{2}\right) \neq f\left(\frac{1}{3}\right) \right\}$

6. Let $f : F \to R$ be a homomorphism of a field F into a ring R, then
   1. f is one one.
   2. f is trivial homomorphism.
   3. either f is one one or it is the trivial homomorphism.
   4. f is a non trivial homomorphism.

7. Let $< p(x) >$ denote the ideal generated by the polynomial $p(x)$ in $\mathbb{Q}[x]$. If $f(x) = x^3 + x^2 + x + 1$ and $g(x) = x^3 - x^2 + x - 1$, then
   1. $< f(x) > + < g(x) > = < x^3 + x >$
   2. $< f(x) > + < g(x) > = < f(x) \cdot g(x) >$
   3. $< f(x) > + < g(x) > = < x^2 + 1 >$
   4. $< f(x) > + < g(x) > = < x^4 - 1 >$

(CSIR NET June 2011)

8. Let I_1 be the ideal generated by $x^2 + 1$ and I_2 be the ideal generated by $x^3 - x^2 + x - 1$ in $\mathbb{Q}[x]$. If $R_1 = \mathbb{Q}[x]/I_1$ and $R_2 = \mathbb{Q}[x]/I_2$, then
   1. R_1 and R_2 are fields.
   2. R_1 is a field and R_2 is not a field.
   3. R_1 is an integral domain, but R_2 is not an integral domain.
   4. R_1 and R_2 are not integral domains.

(CSIR NET June 2011)

9. Let $\mathbb{Z}[i]$ denote the ring of Gaussian integers. For which of the following values of n is the quotient ring $\mathbb{Z}[i]/n\mathbb{Z}[i]$ an integral domain ?
   1. 2 2. 13 3. 19 4. 7

(CSIR NET Dec 2011)

10. Let $R = \mathbb{Q}[x]/I$ where I is the ideal generated by $1 + x^2$. Let y to the coset of x in R . Then
    1. $y^2 + 1$ is irreducible over R
    2. $y^2 + y + 1$ is irreducible over R
    3. $y^2 - y + 1$ is irreducible over R
    4. $y^3 + y^2 + y + 1$ is irreducible over R

(CSIR NET June 2012)

11. Let $f(x) = x^3 + x^2 + x + 1$ and $g(x) = x^3 + 1$. Then in $\mathbb{Q}[x]$,
    1. g.c.d. $(f(x), g(x)) = x + 1$
    2. g.c.d. $(f(x), g(x)) = x^2 - 1$
    3. l.c.m. $(f(x), g(x)) = x^5 + x^3 + x^2 + 1$
    4. l.c.m. $(f(x), g(x)) = x^5 + x^4 + x^3 + x^2 + 1$

(CSIR NET June 2012)

12. For a positive integer n, let $f_n(x) = x^{n-1} + x^{n-2} + \ldots + x + 1$. Then

1. $f_n(x)$ is an irreducible polynomial in $\mathbb{Q}[x]$ for every positive integer *n*.
2. $f_p(x)$ is an irreducible polynomial in $\mathbb{Q}[x]$ for every prime number *p*.
3. $f_{p^e}(x)$ is an irreducible polynomial in $\mathbb{Q}[x]$ for every prime number *p* and every positive integer *e*.
4. $f_p\left(x^{p^{e-1}}\right)$ is an irreducible polynomial in $\mathbb{Q}[x]$ for every prime number *p* and every positive integer *e*.

(CSIR NET Dec 2012)

13. Consider the polynomial $f(x)=x^4-x^3+14x^2+5x+16$. Also for a prime number *p*, let $\mathbb{F}_p$ denote the field with *p* elements. Which of the following are always true ?
    1. Considering *f* as a polynomial with coefficients in $\mathbb{F}_3$, it has no roots in $\mathbb{F}_3$.
    2. Considering *f* as a polynomial with coefficients in $\mathbb{F}_3$, it is a product of two irreducible factors of degree 2 over $\mathbb{F}_3$.
    3. Considering *f* as a polynomial with coefficients in $\mathbb{F}_7$, it has an irreducible factor of degree 3 over $\mathbb{F}_7$.
    4. *f* is a product of two polynomials of degree 2 over $\mathbb{Z}$.

(CSIR NET Dec 2012)

14. For a positive integer *m*, let a_m denote the number of distinct prime ideals of the ring $\frac{\mathbb{Q}[x]}{\langle x^m-1\rangle}$. Then
    1. $a_4=2$
    2. $a_4=3$
    3. $a_5=2$
    4. $a_5=3$

(CSIR NET Dec 2012)

15. Which of the polynomials are irreducible over the given rings ?
    1. $x^5+3x^4+9x+15$ over $\mathbb{Q}$, the field of rationals
    2. x^3+2x^2+x+1 over $\mathbb{Z}/7\mathbb{Z}$, the ring of integers modulo 7
    3. x^3+x^2+x+1 over $\mathbb{Z}$, the ring of integers
    4. $x^4+x^3+x^2+x+1$ over $\mathbb{Z}$, the ring of integers

(CSIR NET June 2013)

16. Let $\mathbb{R}$ be a non zero commutative ring with unity $1_{\mathbb{R}}$. Define the characteristic of $\mathbb{R}$ to be order of $1_{\mathbb{R}}$ in $(\mathbb{R},+)$ if it is finite and to be 0 if the order of $1_{\mathbb{R}}$ in $(\mathbb{R},+)$ is infinite. We denote the characteristic of $\mathbb{R}$ by char($\mathbb{R}$). In the following, let $\mathbb{R}$ and *S* be non zero commutative rings with unity. Then
    1. char($\mathbb{R}$) is always a prime number.
    2. If *S* is a quotient ring of $\mathbb{R}$, then either char(*S*) divides char($\mathbb{R}$), or char(*S*) = 0.
    3. If *S* is a subring of $\mathbb{R}$ containing $1_{\mathbb{R}}$ then char(*S*) = char($\mathbb{R}$).
    4. If char($\mathbb{R}$) is a prime number, then $\mathbb{R}$ is a field.

(CSIR NET Dec 2013)

17. Let $f(x)=x^3+2x^2+x-1$. Determine in which of the following cases *f* is irreducible over the field *k*.
    1. $k=\mathbb{Q}$, the field of rational numbers.
    2. $k=\mathbb{R}$, the field or real numbers.
    3. $k=\mathbb{F}_2$, the finite field of 2 elements.
    4. $k=\mathbb{F}_3$, the finite field of 3 elements.

(CSIR NET Dec 2013)

18. Let $f(x)=x^4+3x^3-9x^2+7x+27$ and let *p* be a prime. Let $f_p(x)$ denote the corresponding polynomial with coefficients in $\mathbb{Z}/p\mathbb{Z}$. Then
    1. $f_2(x)$ is irreducible over $\mathbb{Z}/2\mathbb{Z}$.
    2. $f(x)$ is irreducible over $\mathbb{Q}$.
    3. $f_3(x)$ is irreducible over $\mathbb{Z}/3\mathbb{Z}$.
    4. $f(x)$ is irreducible over $\mathbb{Z}$.

(CSIR NET June 2014)

19. Let $\mathbb{R}[x]$ be the polynomial ring over $\mathbb{R}$ in one variable. Let $I \subseteq \mathbb{R}[x]$ be an ideal. Then
    1. I is a maximal ideal iff I is a non zero prime ideal
    2. I is a maximal ideal iff the quotient ring $\mathbb{R}[x]/I$ is isomorphic to $\mathbb{R}$
    3. I is a maximal ideal iff $I = (f(x))$, where $f(x)$ is a non constant irreducible polynomial over $\mathbb{R}$
    4. I is a maximal ideal iff there exists a non constant polynomial $f(x) \in I$ of degree ≤ 2

    (CSIR NET Dec 2014)

20. Let $C([0,1])$ be the ring of all real valued continuous functions on $[0,1]$. Which of the following statements are true ?
    1. $C([0,1])$ is an integral domain.
    2. The set of all functions vanishing at 0 is a maximal ideal.
    3. The set of all functions vanishing at both 0 and 1 is a prime ideal.
    4. If $f \in C([0,1])$ is such that $(f(x))^n = 0$ for all $x \in [0,1]$ for some $n > 1$, then $f(x) = 0$ for all $x \in [0,1]$.

    (CSIR NET June 2015)

21. Which of the following polynomials are irreducible in the ring $\mathbb{Z}[x]$ of polynomials in one variable with integer coefficients ?
    1. $x^2 - 5$
    2. $1 + (x+1) + (x+1)^2 + (x+1)^3 + (x+1)^4$
    3. $1 + x + x^2 + x^3 + x^4$
    4. $1 + x + x^2 + x^3$

    (CSIR NET June 2015)

22. Determine which of the following polynomials are irreducible over the indicated rings.
    1. $x^5 - 3x^4 + 2x^3 - 5x + 8$ over $\mathbb{R}$
    2. $x^3 + 2x^2 + x + 1$ over $\mathbb{Q}$
    3. $x^3 + 3x^2 - 6x + 3$ over $\mathbb{Z}$
    4. $x^4 + x^2 + 1$ over $\mathbb{Z}/2\mathbb{Z}$

    (CSIR NET June 2015)

23. Let A denote the quotient ring $\mathbb{Q}[X]/(X^3)$. Then
    1. There are exactly three distinct proper ideals in A.
    2. There is only one prime ideal in A.
    3. A is an integral domain.
    4. Let f, g be in $\mathbb{Q}[X]$ such that $\overline{f} \cdot \overline{g} = 0$ in A. Here $\overline{f}$ and $\overline{g}$ denote the image of f and g respectively in A. Then $f(0) \cdot g(0) = 0$.

    (CSIR NET Dec 2015)

24. Which of the following quotient rings are fields ?
    1. $\mathbb{F}_3[X]/(X^2 + X + 1)$, where $\mathbb{F}_3$ is the finite field with 3 elements.
    2. $\mathbb{Z}[X]/(X - 3)$
    3. $\mathbb{Q}[X]/(X^2 + X + 1)$
    4. $\mathbb{F}_2[X]/(X^2 + X + 1)$ where $\mathbb{F}_2$ is the finite field with 2 elements.

    (CSIR NET Dec 2015)

25. Let $f(x) \in \mathbb{Z}[x]$ be a polynomial of degree ≥ 2. Pick each correct statement from below :
    1. If $f(x)$ is irreducible in $\mathbb{Z}[x]$, then it is irreducible in $\mathbb{Q}[x]$.
    2. If $f(x)$ is irreducible in $\mathbb{Q}[x]$, then it is irreducible in $\mathbb{Z}[x]$.
    3. If $f(x)$ is irreducible in $\mathbb{Z}[x]$, then for all primes p the reduction $\overline{f(x)}$ of $f(x)$ modulo p is irreducible in $\mathbb{F}_p[x]$.
    4. If $f(x)$ is irreducible in $\mathbb{Z}[x]$, then it is

irreducible in $\mathbb{R}[x]$.

(CSIR NET June 2016)

26. Let R be a finite non-zero commutative ring with unity. Then which of the following statements are necessarily true ?
    1. Any non-zero element of R is either a unit or a zero divisor.
    2. There may exist a non-zero element of R which is neither a unit nor a zero divisor.
    3. Every prime ideal of R is maximal.
    4. If R has no zero divisors then order of any additive subgroup of R is a prime power.

(CSIR NET Dec 2016)

27. Let $R = \{ f : \{1,2,...,10\} \to \mathbb{Z}_2 \}$ be the set of all $\mathbb{Z}_2$-valued functions on the set $\{1,2,...,10\}$ of the first ten positive integers. Then R is commutative ring with pointwise addition and pointwise multiplication of functions. Which of the following statements are correct ?
    1. R has a unique maximal ideal.
    2. Every prime ideal of R is also maximal.
    3. Number of proper ideals of R is 511.
    4. Every element of R is idempotent.

(CSIR NET June 2017)

28. Which of the following polynomials are irreducible in $\mathbb{Z}[x]$?
    1. $x^4 + 10x + 5$
    2. $x^3 - 2x + 1$
    3. $x^4 + x^2 + 1$
    4. $x^3 + x + 1$

(CSIR NET June 2017)

29. Let $z = e^{\frac{2\pi i}{7}}$ and let $\theta = z + z^2 + z^4$. Then
    1. $\theta \in \mathbb{Q}$
    2. $\theta \in \mathbb{Q}\left(\sqrt{D}\right)$ for some $D > 0$
    3. $\theta \in \mathbb{Q}\left(\sqrt{D}\right)$ for some $D < 0$
    4. $\theta \in i\mathbb{R}$

(CSIR NET Dec 2017)

Assignment Key

SCQ

1. 3
2. 1
3. 4
4. 2
5. 3
6. 3
7. 3
8. 4
9. 1
10. 1
11. 3
12. 1
13. 4
14. 3
15. 1
16. 2
17. 4
18. 1
19. 2
20. 4
21. 3
22. 2
23. 3
24. 2
25. 2
26. 2
27. 4
28. 2
29. 4
30. 4
31. 3
32. 1
33. 4
34. 2
35. 2
36. 1
37. 2
38. 3
39. 3
40. 3
41. 2
42. 4
43. 1

MCQ

1. 2,4
2. 1,3
3. 1,2,3
4. 1,3
5. 1,2
6. 3
7. 3
8. 2,3
9. 3,4
10. 2,3
11. 1,3
12. 2,4
13. 3
14. 2,3
15. 1,4
16. 2,3
17. 1,3
18. 1,2,4
19. 1,3
20. 2,4
21. 1,2,3
22. 2,3
23. 1,2,4
24. 3,4
25. 1,2
26. 1,3,4
27. 2,4
28. 1,4
29. 3

189/35 BEHIND RAILWAY STATION, VAISH COLLEGE ROAD, ROHTAK PIN-124001 (HARYANA)
E-mail us on - jrinstituterohtak@gmail.com, balwanmudgil54@gmail.com Mob. 8607383607, 9802177766

3.1 Principal Ideal Domain (P.I.D)

Def. Ideal generated by a set : Let S be any subset of a ring R. An ideal A of ring R is said to be generated by S if it is the smallest ideal containing S. We denote this fact by $A=\langle S\rangle$ or (S).

Def. Principal Ideal : If we take $S=\{a\}$ in above definition then we denote $\langle S\rangle$ by $\langle a\rangle$ or (a) and such an ideal is called a principal ideal. In other words, an ideal A of R is said to be principal ideal if it is generated by a single element of R i.e. $A=\langle a\rangle$ for some $a\in R$.

Def. Principal ideal ring (P.I.R.) : A ring R is said to be a principal ideal ring if every ideal of R is a principal ideal.

Def. Principal Ideal Domain (P.I.D.) : An integral domain R is called a principal ideal domain if Every ideal of R is a principal ideal.

Remark : An integral domain R is not a P.I.D. if there exists an ideal I of R which is not a principal ideal i.e., I is not generated by a single element.

Results :

1. Every simple ring with unity is a P.I.R.
2. $\mathbb{Z}\times\mathbb{Z}$ is not a principal ideal ring as $\mathbb{Z}\times\mathbb{Z}$ itself is not generated by a single element.
2. $\mathbb{Z}$ is a P.I.D. : Since all the ideals of $\mathbb{Z}$ is of the form $n\mathbb{Z}$ which is generated by n i.e., $n\mathbb{Z}=\langle n\rangle$.
3. Every division ring is a P.I.R.
4. Every field is a P.I.D. : Since the only ideal of F (field) is $\{0\}$ and F and $\{0\}=\langle 0\rangle$ and $F=\langle 1\rangle$.
5. $\mathbb{Z}[x]$ is not a P.I.D.

First Proof : It is sufficient to show that there exist at least one ideal in $\mathbb{Z}[x]$ which is not a principal ideal.

Consider the ideal $B=<2,x>=\{2f(x)+xg(x):f(x),g(x)\in\mathbb{Z}[x]\}$

We claim that B is not a principal ideal , but first we prove that $B\neq\mathbb{Z}[x]$.

Let , if possible , let $B=\mathbb{Z}[x]$ the since $1\in\mathbb{Z}[x]$ so $1\in B$

$\Rightarrow \quad 1=xf(x)+2g(x)$

$\Rightarrow \quad 1=x(a_0+a_1x+.....+a_mx^m)+2(b_0+b_1x+.....+b_nx^n)$

$\Rightarrow \quad 1=2b_0$ which is not possible for any integer b_0.

Hence $B \neq \mathbb{Z}[x]$. .....(1)

Now let , if possible, let B be a principal ideal generated by $k(x)$ where $k(x) \in \mathbb{Z}[x]$

Clearly, $x, 2 \in B = \langle k(x) \rangle$

$\Rightarrow$ $x = k(x)h(x)$ for some $h(x) \in \mathbb{Z}[x]$ .....(2)

and $2 = k(x)t(x)$ for some $t(x) \in \mathbb{Z}[x]$ .....(3)

Multiplying (2) and (3) , we get $x\,k(x)t(x) = 2k(x)h(x)$

$\Rightarrow$ $xt(x) = 2h(x)$

$\Rightarrow$ Each co-efficient of $t(x)$ is an even integer.

$\Rightarrow$ $t(x) = 2r(x)$ for some $r(x) \in \mathbb{Z}[x]$

So by (3), we have $2 = 2k(x)r(x)$

$\Rightarrow$ $1 = k(x)r(x)$

$\Rightarrow$ $1 \in \langle k(x) \rangle = B$

$\Rightarrow$ $B = \mathbb{Z}[x]$, which is a contradiction to (1).

Thus , our supposition is wrong. Hence $Z[x]$ is not principal ideal domain.

6. If F is a field then $F[x]$ is a P.I.D. e.g. $\mathbb{Q}[x], \mathbb{R}[x], \mathbb{C}[x], \mathbb{Z}_p[x]$ are P.I.D.
7. **M P 4 Result :** In a PID, every non zero ideal is maximal iff it is a prime ideal.
8. Converse of above result is not true i.e., if every non zero ideal in a ring R is maximal iff it is prime, then it is not necessary that R is a P.I.D. e.g., consider the ring $P(\mathbb{N})$.
9. Second proof of the fact that $\mathbb{Z}[x]$ is not a P.I.D. : We know that the ideal $\langle x \rangle$ is a non-zero prime ideal of $\mathbb{Z}[x]$ but it is not a maximal ideal, so by M P 4 Result, $\mathbb{Z}[x]$ cannot be a P.I.D.
10. **P F 2 Result :** If R is a CRU such that $R[x]$ is a P.I.D. then R is a field.
11. Third proof of the fact that $\mathbb{Z}[x]$ is not a P.I.D. : We know that $\mathbb{Z}$ is a CRU and if $\mathbb{Z}[x]$ is a P.I.D. then by P F 2 Result, $\mathbb{Z}$ must be a field, which is a contradiction.
12. If F is a field then $F[x, y]$ is not a P.I.D.
13. If R is a P.I.D. and S be a subring of R containing unity then S may or may not be P.I.D. e.g., consider $\mathbb{Z}[x] \subseteq \mathbb{Q}[x]$ and $\mathbb{Z} \subseteq \mathbb{Q}$.
14. Let R be a P.I.D. and F be the quotient field of R. If K is a subring of R such that $R \subseteq K \subseteq F$ then K is a P.I.D.

189/35 BEHIND RAILWAY STATION, VAISH COLLEGE ROAD, ROHTAK PIN-124001 (HARYANA)
E-mail us on - jrinstituterohtak@gmail.com, balwanmudgil54@gmail.com Mob. 8607383607, 9802177766

15. Let R be a ring and let $I_1 \subseteq I_2 \subseteq .....I_n \subseteq .....$ be an ascending chain of ideals of R then $\bigcup_n I_n$ is an ideal of R.
16. Let R be a P.I.D. and let $I_1 \subseteq I_2 \subseteq .....I_n \subseteq .....$ be an ascending chain of ideals of R then there exists a positive integer r such that $I_r = I_{r+1} = I_{r+2} = ...$. In words we can say that in a P.I.D. every ascending chain of ideals becomes stationary after a finite number of steps.

Exercise 3.1

Which of the following are principal ideal domain? Justify your answers.

1. $\mathbb{Z}$ 2. $\mathbb{Q}$ 3. $\mathbb{R}[x]$ 4. $\mathbb{C}[x]$ 5. $\mathbb{Z}_{10}$
6. $\mathbb{Z}_2$ 7. $\mathbb{Z}_6$ 8. $F[x]$, where F is a field. 9. $F[x, y]$, where F is a field.

3.2 Divisibility

Def. Divisibility in a Commutative Ring : Let R be a commutative ring and $a, b \in R$ where $a \neq 0$. We say that a divides b if there exists $c \in R$ such that $b = ac$. We then write $a \mid b$. If there is no such element in R then we say that a does not divide b and write $a \nmid b$.

e.g. (i) In the ring of integers $(\mathbb{Z}, +, \cdot)$, $2 \mid 10$, since $\exists$ an integer 5 such that $10 = 2.5$.

(ii) In the ring of even integers , $2 \nmid 10$, since there is no even integer 'c' such that $10 = 2.c$

(iii) In $(\mathbb{Q}, +, .)$, $2 \mid 7$ since there exists $\frac{7}{2} \in \mathbb{Q}$ such that $7 = 2.\frac{7}{2}$.

Results :

1. In a field, a non-zero element divides every element.
2. In a commutative ring R, we have
   (i) If $a \mid b$, $b \mid c$ then $a \mid c$
   (ii) If $a \mid b$, $a \mid c$ then $a \mid (b \pm c)$
   (iii) If $a \mid b$ then $a \mid bx$ for all $x \in R$
   (iv) If R is a ring with unity '1' then $1 \mid x$ for all $x \in R$.

Def. Greatest Common Divisor : Let R be a commutative ring. An element $d \in R$ is said to be greatest common divisor of $a, b \in R$ if (i) $d \mid a$ and $d \mid b$, and (ii) if $c \in R$ such that $c \mid a$ and

$c \mid b$ then $c \mid d$. We , then write $d = (a,b)$ or g.c.d (a,b).

Def. Least Common Multiple : Let R be a commutative ring. An element $l \in R$ is said to be greatest common divisor of $a,b \in R$ if (i) $a \mid l$ and $b \mid l$, and (ii) if $c \in R$ such that $a \mid c$ and $b \mid c$ then $l \mid c$. We , then write $l = (a,b)$ or l.c.m. (a,b).

Remark : Any two elements in a commutative ring may or may not have a g.c.d. (l.c.m.) , they may have even more than one g.c.d. (l.c.m.). This is illustrated in the following examples .

Example 1. In the ring of even integers $2\mathbb{Z}$, 4 and 6 have no commom divisor. Clearly only divisor of 4 is 2 as $2.2 = 4$, but 6 has no divisor. Therfore 4 and 6 have no commom divisor and so no gcd.

Example 2. In the ring of integers $\mathbb{Z}$, 2 and -2 are g.c.d. of 4 and 6. Further , 12 and -12 are l.c.m. of 4 and 6.

Example 3. Consider the ring $(\mathbb{Z}_8, +_8, \times_8)$ where $\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$.

We have, $6 = 2 \times_8 3 \quad \Rightarrow \quad 2 \mid 6$ and $4 = 2 \times_8 2 \quad \Rightarrow \quad 2 \mid 4$

Also, if $c \mid 6$ and $c \mid 4$, then $c \mid (6-4)$ i.e. $c \mid 2$. So by definition, $\gcd(4,6) = 2$

Again, we have $6 = 6 \times_8 1 \quad \Rightarrow \quad 6 \mid 6$ and $4 = 6 \times_8 6 \quad \Rightarrow \quad 6 \mid 4$

Also, if $c \mid 6$ and $c \mid 4$, then as $c \mid 6$, so by definition, $\gcd(4,6) = 6$.

Hence there can be more than one gcd of two same elements of a ring.

Similarly , it can be checked that $\text{lcm}[3,6] = 2$ and 6.

Remark : In the above example we have seen that two elements of a commutative ring may not have a g.c.d. or l.c.m. But existence of g.c.d. and l.c.m. is assured if the ring R is a principal ideal domain.

Results :

1. Let R be a PID, then any two elements a and b in R have a greatest common divisor. Further if d is g.c.d. of a and b then $d = ma + nb$ for some $m,n \in R$.
2. Let R be a PID, then any two non-zero elements of R have a least common multiple.

Exercise 3.2

1. In $\mathbb{Z}_6$ show that $4 \mid 2$.
2. In $\mathbb{Z}_8$ show that $3 \mid 7$.
3. In $\mathbb{Z}_{15}$ show that $9 \mid 12$.

189/35 BEHIND RAILWAY STATION, VAISH COLLEGE ROAD, ROHTAK PIN-124001 (HARYANA)
E-mail us on - jrinstituterohtak@gmail.com, balwanmudgil54@gmail.com Mob. 8607383607, 9802177766

3.3 Prime Element, Irreducible Elements and Associativity

Def. Associates : Let R be a CRU, the elements $a,b \in R$ are called associates in R if $a = ub$ for some unit u.

Results :

1. The relation of associate in a ring R is an equivalence relation.
2. Let R be a ring and $a \in R$ be any non zero element then associates of a and units of R are always factors of a. Some authors call them improper factors.
3. In $\mathbb{Z}$ every non zero element has two associates.
4. In $\mathbb{Z}[i]$ every non zero element has four associates.
5. In an integral domain R the number of associates of a non zero element is equal to the number of units in R.

Def. Irreducible element : Let R be a CRU. An element $p \in R$ is said to be irreducible element of R if (i) $p \neq 0$ and p is not a unit (ii) For every a,b in R if $p = ab$ then either a or b is a unit. Roughly speaking, a non zero non unit element is an irreducible element if it can be factored only in a trivial way.

Remark : Negation of the above definition : A non-zero non-unit element p of a CRU R is not an irreducible element if there exist elements $a,b \in R$ such that $p = ab$ and neither a is a unit nor b is a unit.

Def. Prime Element : Let R be a CRU. An element $p \in R$ is said to be a prime element if (i) $p \neq 0$ and p is not a unit (ii) For every a,b in R if $p \mid ab$ then $p \mid a$ or $p \mid b$.

Remark : Negation of the above definition : A non-zero non-unit element p of a CRU R is not a prime element if there exist elements $a,b \in R$ such that $p \mid ab$ but $p \nmid a$ and $p \nmid b$.

Results :

1. Let R be an integral domain . If a, b are two non-zero elements of R, then a is associate of b iff $a \mid b$ and $b \mid a$.
2. In an integral domain R, any two gcd of same pair of elements of R are associates of each other.
3. **P I 1 Result :** In an integral domain R , every prime element is irreducible. However converse is not true.
4. **P I 2 Result :** In a PID , an element is irreducible iff it is prime.

5. **P I M Result :** Let R be a PID which is not a field. An ideal A of R is maximal iff it is generated by an irreducible element of R.
6. In $\mathbb{Z}$, every prime number and its negative are both irreducible and prime element.

Def. Norm in $\mathbb{Z}\left(\sqrt{d}\right)$: Let $\mathbb{Z}\left(\sqrt{d}\right)=\left\{a+b\sqrt{d} : a,b\in\mathbb{Z}\right\}$, where d is not a perfect square, then we define the norm of an element $x=a+b\sqrt{d}$ by $N\left(x\right)=\left|a^2-db^2\right|$.

7. Properties of norm :
   (i) $N\left(x\right)=0$ iff $x=0$
   (ii) $N\left(xy\right)=N\left(x\right)N\left(y\right)$ for all $x,y\in\mathbb{Z}\left(\sqrt{d}\right)$.
   (iii) x is a unit iff $N\left(x\right)=1$.
   (iv) If $N\left(x\right)$ is a prime number then x is an irreducible element in $\mathbb{Z}\left(\sqrt{d}\right)$.
8. Units of $\mathbb{Z}\left(\sqrt{-2}\right),\mathbb{Z}\left(\sqrt{-3}\right),\mathbb{Z}\left(\sqrt{-5}\right),\mathbb{Z}\left(\sqrt{-6}\right),$..... are only ±1.
9. Units of $\mathbb{Z}\left(\sqrt{2}\right),\mathbb{Z}\left(\sqrt{3}\right),\mathbb{Z}\left(\sqrt{5}\right)$..... are infinite in number.
10. Units of $\mathbb{Z}\left(i\right)$ are $1,-1,i,-i$.

Exercise 3.3

1. Find all associate classes in $\mathbb{Z}_{10}$.
2. Show that 2 and 5 are irreducible elements in $\mathbb{Z}$ but they are not irreducible elements in $\mathbb{Z}\left[i\right]$.
3. Show that 3 is an irreducible element in both $\mathbb{Z}$ and $\mathbb{Z}\left[i\right]$.
4. Show that $1-i$ is an irreducible element in $\mathbb{Z}\left[i\right]$.
5. In $\mathbb{Z}\left(\sqrt{-3}\right)$, prove that $1+\sqrt{-3}$ is an irreducible element but not a prime element.
6. In $\mathbb{Z}\left(\sqrt{-5}\right)$, prove that 3 and $1+3\sqrt{-5}$ are irreducible element but not a prime element.
7. In $\mathbb{Z}\left(\sqrt{5}\right)$, prove that 2 and $1+\sqrt{5}$ are irreducible but not prime element.
8. In $\mathbb{Z}\left(\sqrt{-6}\right)$, prove that 7 is an irreducible element or not.

189/35 BEHIND RAILWAY STATION, VAISH COLLEGE ROAD, ROHTAK PIN-124001 (HARYANA)
E-mail us on - jrinstituterohtak@gmail.com, balwanmudgil54@gmail.com Mob. 8607383607, 9802177766

3.4 Unique Factorization Domain

Def. Unique Factorization Domain : An integral domain R is said to be a unique factorization domain if

(i) Every non-zero non-unit element of R can be expressed as a product of finite number of irreducible elements of R, and

(ii) If $a \in R$ such that $a = p_1 \cdot p_2 \cdots p_m$ and $a = q_1 \cdot q_2 \cdots q_n$ are two factorizations of a, where p_i's and q_i's are irreducible elements in R then $m = n$ and each p_i is an associate of some q_j. In words, we can say that the factorization is unique upto order and associates.

Results :

1. $\mathbb{Z}$ is a UFD.
2. **P I 3 Result :** In a UFD, an element is prime element iff it is an irreducible element.
3. $\mathbb{Z}\left(\sqrt{-1}\right)$ and $\mathbb{Z}\left(\sqrt{-2}\right)$ are UFD.
4. $\mathbb{Z}\left(\sqrt{-3}\right), \mathbb{Z}\left(\sqrt{-5}\right), \mathbb{Z}\left(\sqrt{-6}\right)$..... are not UFD.
5. If R is a UFD then $R[x]$ is also a UFD.
6. Every PID is a UFD.

Exercise 3.4

1. In $\mathbb{Z}\left(\sqrt{-5}\right)$ factorise 21 and 46 into two different ways and hence conclude that $\mathbb{Z}\left(\sqrt{-5}\right)$ is not a UFD.
2. In $\mathbb{Z}\left(\sqrt{-6}\right)$ factorise 10 in two different ways and hence conclude that $\mathbb{Z}\left(\sqrt{-6}\right)$ is not a UFD.
3. Show that $\mathbb{Z}\left(\sqrt{5}\right)$ is not a UFD.
4. Show that $\mathbb{Z}\left(\sqrt{5}\right)$ has atleast one non principal ideal.

3.5 Euclidean Domain

Def. Euclidean domain : Let R be an integral domain. Then R is said to be Euclidean Domain , if to every non – zero element $a \in R$, we can assign a non-negative integer $d(a)$ s.t.

(i) For all $a,b \in R$ $(a \neq 0, b \neq 0)$, $d(ab) \geq d(a)$

(ii) For all $a,b \in R(b \neq 0)$, there exists q and r in R s.t. $a = bq + r$ where either $r = 0$ or $d(r) < d(b)$

Note : $d(a)$ is called d- value of 'a', $d(a)$ is not defined for $a = 0$. Second part of the definition called division algorithm.

Results :

1. The ring of integers $\mathbb{Z}$ is an ED.
2. Every field is an ED.
3. The field $\mathbb{Q}$ of rational numbers with $d(a) = 0$ for all $a \neq 0 \in \mathbb{Q}$ is a ED. However , $\mathbb{Q}$ with $d(a) = |a|$ for all $a \neq 0 \in \mathbb{Q}$ is not a ED.
4. The ring of Gaussian integers $\mathbb{Z}[i] = \{a + ib \ : \ a,b \in \mathbb{Z}\}$ is an ED with $d(a+ib) = a^2 + b^2$.
5. Every ED is a PID.
6. Let R be an ED and a , b be two non – zero elements of R , then
   (i) If b is a unit in R , then $d(ab) = d(a)$
   (ii) If b is not a unit in R , then $d(ab) > d(a)$.
7. An element 'a' in an ED is a unit iff $d(a) = d(1)$.
8. If F is a field , then $F[x]$ is an ED.
9. R is an integral domain iff $R[x]$ is an integral domain.
10. Field $\Rightarrow$ ED $\Rightarrow$ PID $\Rightarrow$ UFD $\Rightarrow$ ID $\Rightarrow$ CRU
11. Contrapositive : Not CRU $\Rightarrow$ Not ID $\Rightarrow$ Not UFD $\Rightarrow$ Not PID $\Rightarrow$ Not ED $\Rightarrow$ Not Field.
12. Let R be a E.D. and F be the quotient field of R. If K is a subring of R such that $R \subseteq K \subseteq F$ then K is a E.D.

Property Transfer Results :

P T R 1 : If R is a CRU then $R[x]$ is also a CRU.

P T R 2 : If R is an integral domain then $R[x]$ is also an integral domain.

P T R 3 : If R is a UFD then $R[x]$ is also a UFD.

P T R 4 : If R is a PID then $R[x]$ may or may not be a PID.

P T R 5 : If R is a ED then $R[x]$ may or may not be an ED.

P T R 6 : If R is a field then $R[x]$ is not a field.

P T R 7 : If R is a field then $R[x]$ is an ED with $d(f(x))=\text{degree}(f(x))$.

P T R 8 : If R is a CRU then $R[x,y]$ is also a CRU.

P T R 9 : If R is an integral domain then $R[x,y]$ is also an integral domain.

P T R 10 : If R is a UFD then $R[x,y]$ is also a UFD.

P T R 11 : If R is a PID then $R[x,y]$ is not a PID.

P T R 12 : If R is an ED then $R[x,y]$ is not an ED.

P T R 13 : If R is a field then $R[x,y]$ is not a field.

P T R 14 : If R is a field then $R[x,y]$ is a UFD but not a PID.

Table

S.No.	Structure	Field	E.D.	P.I.D.	U.F.D.	I.D.	CRU
1.	$\mathbb{Z}$	N	Y	Y	Y	Y	Y
2.	$\mathbb{Q}$	Y	Y	Y	Y	Y	Y
3.	$\mathbb{R}$	Y	Y	Y	Y	Y	Y
4.	$\mathbb{C}$	Y	Y	Y	Y	Y	Y
5.	$\mathbb{Z}_p$	Y	Y	Y	Y	Y	Y
6.	$\mathbb{Z}[x]$	N	N	N	Y	Y	Y
7.	$\mathbb{Q}[x]$	N	Y	Y	Y	Y	Y
8.	$\mathbb{R}[x]$	N	Y	Y	Y	Y	Y
9.	$\mathbb{C}[x]$	N	Y	Y	Y	Y	Y
10.	$\mathbb{Z}_p[x]$	N	Y	Y	Y	Y	Y
11.	$\mathbb{Z}[x,y]$	N	N	N	Y	Y	Y
12.	$\mathbb{Q}[x,y]$	N	N	N	Y	Y	Y

13.	$\mathbb{R}[x,y]$	N	N	N	Y	Y	Y
14.	$\mathbb{C}[x,y]$	N	N	N	Y	Y	Y
15.	$\mathbb{Z}_p[x,y]$	N	N	N	Y	Y	Y
16.	$\mathbb{Z}_p[i], p=4k+3$	Y	Y	Y	Y	Y	Y
17.	$\mathbb{Z}_p[i], p\neq 4k+3$	N	N	N	N	N	Y
18.	$\mathbb{Z}[i]$	N	Y	Y	Y	Y	Y
19.	$\mathbb{Z}\left(\sqrt{-2}\right)$	N	Y	Y	Y	Y	Y
20.	$\mathbb{Z}\left(\sqrt{-3}\right)$	N	N	N	N	Y	Y
21.	$\mathbb{Z}\left(\sqrt{-5}\right)$	N	N	N	N	Y	Y
22.	$\mathbb{Z}\left(\sqrt{2}\right)$	N	----	----	----	Y	Y
23.	$\mathbb{Z}\left(\sqrt{3}\right)$	N	----	----	----	Y	Y
24.	$\mathbb{Z}\left(\sqrt{5}\right)$	N	N	N	N	Y	Y
25.	$\mathbb{Q}\left(\sqrt{p}\right)$	Y	Y	Y	Y	Y	Y
26.	$\mathbb{Z}\left(\frac{1+\sqrt{-19}}{2}\right)$	N	N	Y	Y	Y	Y

---------- S C Q ----------

1. The polynomial ring $F[x]$ over a field F is a
   1. E.D. 2. U.F.D.
   3. P.I.D. 4. All of the above

2. Which of the following statement is true about $S = \mathbb{Z}[x]$?
   1. S is an E.D.
   2. S is a P.I.D.
   3. S is a U.F.D.
   4. S is not an integral domain.

3. Let $f(x) \in \mathbb{Q}[x]$, define $I = \left\{ f(x) \in \mathbb{Q}[x] : f\left(\frac{1}{2}\right) = 0 \right\}$, then
   1. I is not an ideal but subring of $\mathbb{Q}[x]$.
   2. I is an ideal but not principal ideal.
   3. I is principal ideal but not maximal ideal.
   4. I is principal as well as maximal ideal.

4. The number of associates of $2+3i$ in the Euclidean domain of Guassian integers is
   1. 1 2. 2
   3. 3 4. 4

5. Which of the following is true ?
   1. $UFD \Rightarrow ED \Rightarrow PID$
   2. $PID \Rightarrow ED \Rightarrow UFD$
   3. $ED \Rightarrow PID \Rightarrow UFD$
   4. $PID \Rightarrow UFD \Rightarrow ED$

6. Which one of the following is true ?
   1. Every PID is a Euclidean domain.
   2. Every UFD is a Euclidean domain.
   3. For any field F, $F[x]$ is a Euclidean domain.
   4. None

7. Which of the following rings is a PID ?
   1. $\mathbb{Q}[x,y]/(x)$
   2. $\mathbb{Z} \oplus \mathbb{Z}$
   3. $\mathbb{Z}[x]$
   4. $M_2(\mathbb{Z})$, the ring of 2×2 matrices with entries in $\mathbb{Z}$

   (CSIR NET June 2013)

8. Let R be a Euclidean domain such that R is not a field. Then the polynomial ring $R[X]$ is always
   1. a Euclidean domain.
   2. a principal ideal domain, but not a Euclidean domain.
   3. a unique factorization domain, but not a principal ideal domain.
   4. not a unique factorization domain.

   (CSIR NET Dec 2015)

9. Let R be a subring of $\mathbb{Q}$ containing 1. Then which of the following is necessarily true ?
   1. R is a principal ideal domain (PID)
   2. R contains infinitely many prime ideals
   3. R contains a prime ideal which is not a maximal ideal
   4. for every maximal ideal m in R, the residue field R/m is finite

   (CSIR NET Dec 2017)

---------- M C Q ----------

1. Which of the following is/are correct ?
   1. 3 is prime element in $\mathbb{Z}\left(\sqrt{-5}\right)$
   2. $1+\sqrt{-5}$ and $1-\sqrt{-5}$ both are not prime element in $\mathbb{Z}\left(\sqrt{-5}\right)$
   3. Every irreducible element in $\mathbb{Z}\left(\sqrt{-5}\right)$ need not be prime element.
   4. The gcd of 6 and $2\left(1+\sqrt{-5}\right)$ does not exists in $\mathbb{Z}\left(\sqrt{-5}\right)$.

2. Which of the following is NOT true ?
   1. $\mathbb{Z}[x]$ is a UFD
   2. Any two irreducibles in a UFD are associates.
   3. If D is a PID, then $D[x]$ is a PID.

4. A UFD is without zero divisors.

3. Which of the following integral domains are Euclidean domains ?
   1. $\mathbb{Z}\left[\sqrt{-3}\right]=\left\{a+b\sqrt{-3}: a,b\in\mathbb{Z}\right\}$
   2. $\mathbb{Z}[x]$
   3. $\mathbb{R}\left[x^2,x^3\right]=\left\{f=\sum_{i=0}^{n}a_i x^i\in\mathbb{R}[x]: a_1=0\right\}$
   4. $\left(\frac{\mathbb{Z}[x]}{\langle 2,x\rangle}\right)[y]$ where x, y are independent variables and $(2, x)$ is the ideal generated by 2 and x.

(CSIR NET Dec 2011)

4. Consider the ring $R=\mathbb{Z}\left[\sqrt{-5}\right]=\left\{a+b\sqrt{-5}: a,b\in\mathbb{Z}\right\}$ and the element $\alpha=3+\sqrt{-5}$ of R. Then
   1. α is prime
   2. α is irreducible
   3. R is not a unique factorization domain
   4. R is not an integral domain

(CSIR NET Dec 2012)

5. Let R be the ring obtained by taking the quotient of $(\mathbb{Z}/6\mathbb{Z})[X]$ by the principal ideal $(2X+4)$. Then
   1. R has infinitely many elements.
   2. R is a field.
   3. 5 is a unit in R.
   4. 4 is a unit in R.

(CSIR NET Dec 2013)

6. Let R be the ring of all entire functions, i.e. R is the ring of functions $f:\mathbb{C}\to\mathbb{C}$ that are analytic at every point of $\mathbb{C}$, with respect to pointwise addition and multiplication. Then
   1. The units in R are precisely the nowhere vanishing entire functions, i.e. $f:\mathbb{C}\to\mathbb{C}$ s.t. f is entire and $f(\alpha)\neq 0$ for all $\alpha\in\mathbb{C}$.
   2. The irreducible elements of R are, up to multiplication by a unit, linear polynomials of the form $z-\alpha$, where $\alpha\in\mathbb{C}$, i.e., if $f\in R$ is irreducible, then $f(z)=(z-\alpha)g(z)$ for all $z\in\mathbb{C}$, where g is a unit in R and $\alpha\in\mathbb{C}$.
   3. R is an integral domain.
   4. R is a unique factorization domain.

(CSIR NET June 2014)

7. Let R be a commutative ring with unity, such that $R[X]$ is a UFD. Denote the ideal (X) of $R[X]$ by I. Pick each correct statement from below :
   1. I is prime.
   2. If I is maximal, then $R[X]$ is a PID.
   3. If $R[X]$ is a Euclidean domain, then I is maximal.
   4. If $R[X]$ is a PID, then it is a Euclidean domain.

(CSIR NET June 2016)

8. Which of the following statements are true ?
   1. $\mathbb{Z}[x]$ is a principal ideal domain.
   2. $\mathbb{Z}[x,y]/\langle y+1\rangle$ is a unique factorization domain.
   3. If R is a principal ideal domain and ρ is a non-zero prime ideal, then R/ρ has finitely many prime ideals.
   4. If R is a principal ideal domain, then any subgring of R containing 1 is again a principal ideal domain.

(CSIR NET Dec 2016)

9. Let $\mathbb{F}_2$ be the finite field of order 2. Then which of the following statements are true ?
   1. $\mathbb{F}_2[x]$ has only finitely many irreducible elements.
   2. $\mathbb{F}_2[x]$ has exactly one irreducible polynomial of degree 2.
   3. $\mathbb{F}_2[x]/\langle x^2+1\rangle$ is a finite dimensional vector space over $\mathbb{F}_2$.
   4. Any irreducible polynomial in $\mathbb{F}_2[x]$ of degree 5 has distinct roots in any algebraic closure of $\mathbb{F}_2$.

(CSIR NET Dec 2016)

10. Which of the following rings are principal ideal domains (PID) ?
    1. $\mathbb{Q}[x]$
    2. $\mathbb{Z}[x]$
    3. $(\mathbb{Z}/6\mathbb{Z})[x]$
    4. $(\mathbb{Z}/7\mathbb{Z})[x]$

(CSIR NET June 2017)

11. Which of the following rings are principal ideal domains $(PIDs)$?
    1. $\mathbb{Z}[X]/\langle X^2+1\rangle$
    2. $\mathbb{Z}[X]$
    3. $\mathbb{C}[X,Y]$
    4. $\mathbb{R}[X,Y]/\langle X^2+1,Y\rangle$

(CSIR NET Dec 2017)

12. Which of the following statements are true ?
    1. A subring of an integral domain is an integral domain
    2. A subring of a unique factorization domain (UFD) is UFD
    3. A subring of a principal ideal domain (PID) is a PID
    4. A subring of an Euclidean domain is an Euclidean domain

(CSIR NET June 2018)

13. Let $f(x)\in\mathbb{Z}[x]$ be a monic polynomial.

    Then the roots of f
    1. can belong to $\mathbb{Z}$
    2. always belong to $(\mathbb{R}\setminus\mathbb{Q})\cup\mathbb{Z}$
    3. always belong to $(\mathbb{C}\setminus\mathbb{Q})\cup\mathbb{Z}$
    4. can belong to $(\mathbb{Q}\setminus\mathbb{Z})$

(CSIR NET June 2018)

Assignment Key

SCQ

1. 4
2. 3
3. 4
4. 4
5. 3
6. 3
7. 1
8. 3
9. 1

MCQ

1. 2,3,4
2. 2,3
3. 3,4
4. 2,3
5. 1,3
6. 1,2,3
7. 1,2,3,4
8. 2,3
9. 2,3,4
10. 1,4
11. 1,4
12. 1 or None
13. 1,3

4.1 Primitive Roots

Def . Primitive n^{th} root of unity : A number α (real or complex) is said to be primitive n^{th} root of unity if $\alpha^n = 1$ but $\alpha^k \neq 1$ for $k = 1,\ 2,\ .....,n-1$.

Results :

1. (i) The 'n' n^{th} roots of unity are given by $z = e^{\frac{2m\pi i}{n}}$, $m = 0,1,2,....,n-1.$

i.e, $z = 1,\ e^{\frac{2\pi i}{n}}, e^{\frac{4\pi i}{n}}, ..., e^{\frac{2(n-1)\pi i}{n}}$.

If we put $e^{\frac{2\pi i}{n}} = \alpha,$ then $z = 1, \alpha, \alpha^2, \alpha^3, ..., \alpha^{n-1}.$

(ii) n^{th} roots of -1 are given by $z = e^{\frac{(2m+1)\pi i}{n}}$, $m = 0,\ 1,\ 2,....,\ n-1.$

2. The primitive roots of unity are given by $z = e^{\frac{2m\pi i}{n}}$, where $\gcd(m,n) = 1$.
3. If α is the n^{th} primitive root of unity then $1 + \alpha + \alpha^2 + ... + \alpha^{n-1} = 0$.
4. The number of n^{th} primitive roots of unity is $\phi(n)$.
5. The number of n^{th} primitive roots of -1 is $\phi(2n)$.

Def . n^{th} cyclotomic polynomial : Let n be the positive integer and $\alpha_1, \alpha_2, ...\alpha_{\phi(n)}$ primitive n^{th} roots of unity. Then the polynomial $g_n(x) = (x-\alpha_1)(x-\alpha_2).....\left(x-\alpha_{\phi(n)}\right)$ is called n^{th} cyclotomic polynomial.

6. The polynomial $g_n(x)$ is the minimal polynomial of primitive n^{th} roots of unity over $\mathbb{Q}$.
7. $\deg\left(g_n(x)\right) = \phi(n)$.
8. The cyclotomic polynomial $g_n(x)$ can be calculated using the formula $x^n - 1 = \prod_{d/n} g_d(x)$.
9. Cyclotomic polynomial is always irreducible over $\mathbb{Q}$.
10. If n is a odd positive integer then $g_{2n}(x) = g_n(-x)$.
11. If n is an even positive integer then $g_{2n}(x) = g_n\left(x^2\right)$.

The cyclotomic polynomials $g_n(x)$ upto $n=15$.

n	$g_n(x)$
1.	$x-1$
2.	$x+1$
3.	x^2+x+1
4.	x^2+1
5.	$x^4+x^3+x^2+x+1$
6.	x^2-x+1
7.	$x^6+x^5+x^4+x^3+x^2+x+1$
8.	x^4+1
9.	x^6+x^3+1
10.	$x^4-x^3+x^2-x+1$
11.	$x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1$
12.	x^4-x^2+1
13.	$x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1$
14.	$x^6-x^5+x^4-x^3+x^2-x+1$
15.	$x^8-x^7+x^5-x^4+x^3-x+1$

Table of roots and primitive roots of unity

Sr. No.	Equations	Roots	Primitive Roots
1.	$x^2=1$	$1,\ -1$	-1
2.	$x^3=1$	$1,\omega,\omega^2$	ω,ω^2
3.	$x^4=1$	$1,-1,i,-i$	$i,-i$
4.	$x^5=1$	$1,\alpha,\alpha^2,\alpha^3,\alpha^4$ where $\alpha=e^{\frac{2\pi i}{5}}$	$\alpha,\alpha^2,\alpha^3,\alpha^4$
5.	$x^6=1$	$1,-1,\alpha,\alpha^2,\alpha^4,\alpha^5$ where $\alpha=e^{\frac{\pi i}{3}}$	α,α^5
6.	$x^7=1$	$1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6$ where $\alpha=e^{\frac{2\pi i}{7}}$	$\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6$
7.	$x^8=1$	$1,-1,i,-i,\alpha,\alpha^3,\alpha^5,\alpha^7$ where $\alpha=e^{\frac{\pi i}{4}}$	$\alpha,\alpha^3,\alpha^5,\alpha^7$

8.	$x^9=1$	$1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6,\alpha^7,\alpha^8$ where $\alpha=e^{\frac{2\pi i}{9}}$	$\alpha,\alpha^2,\alpha^4,\alpha^5,\alpha^7,\alpha^8$
9.	$x^{10}=1$	$1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6,\alpha^7,\alpha^8,\alpha^9$ where $\alpha=e^{\frac{2\pi i}{10}}$	$\alpha,\alpha^3,\alpha^7,\alpha^9$

Exercise 4.1

1. Solve the equations : (i) $x^3+1=0$ (ii) $x^4+1=0$
2. Construct the cyclotomic polynomial $g_{19}(x)$ and $g_{20}(x)$.

4.2 Field Extensions

Def . Field Extension : A field *K* is said to a field extension of a field *F* if *F* is a subfield of *K* or *F* is isomorphic to a subfield of *K*.

e.g., $\mathbb{C}/\mathbb{R}, \mathbb{C}/\mathbb{Q}, \mathbb{R}/\mathbb{Q}$ are field extension.

Remark : K/F is a field extension but not a quotient ring.

Def . Degree of an field extension : Let K/F be a field extension, then *K* is a vector space over *F* and therefore it must have a dimension. The dimension of *K* over *F* is called degree of *K* over *F* and it is denoted by $[K:F]$

Results : (i) $[\mathbb{C}:\mathbb{C}]=1$ (ii) $[\mathbb{R}:\mathbb{R}]=1$ (iii) $[\mathbb{C}:\mathbb{R}]=2$

(iv) $[\mathbb{R}:\mathbb{Q}]=\infty$ (v) $[\mathbb{C}:\mathbb{Q}]=\infty$ (vi) $[\mathbb{Q}:\mathbb{Q}]=1$

Def . Finite Extension : The extension K/F is said to be finite if its degree is finite.

Def . Infinite Extension : The extension K/F is said to be infinite if its degree is infinite.

Def . Algebraic Element : Let K/F be any field extension. An element $a \in K$ is said to be algebraic over *F* if '*a*' satisfies some polynomial over *F*.

Def . Algebraic Extension : An extension K/F is said to be algebraic extension if every element of *K* is algebraic over *F*.

Def . Non–Algebraic Extension : An extension K/F is said to be non–algebraic if there is atleast one element in *K* which is not algebraic over *F*.

Def . Minimal Polynomial of an element : Let K/F be any extension and $a \in K$ be any algebraic element. A polynomial $m(x) \in F[x]$ is said to be 'minimal polynomial' of a over *F* if

(i) $m(x)$ is monic (ii) $m(a)=0$ (iii) $m(x)$ is irreducible over *F*.

i.e, $m(x)$ is lowest degree monic polynomial which is satisfied by '*a*'.

Results :

1. Degree of minimal polynomial of any real number over $\mathbb{R}$ is 1 and any non-real complex number is 2.
2. The minimal polynomial of n^{th} primitive root of unity over $\mathbb{Q}$ is $g_n(x)$.

Sr. No	Element	Minimal Polynomial		
		over $\mathbb{Q}$	over $\mathbb{R}$	over $\mathbb{C}$
1.	$\frac{1}{2}$	$x-\frac{1}{2}$	$x-\frac{1}{2}$	$x-\frac{1}{2}$
2.	$\sqrt{2}$	x^2-2	$x-\sqrt{2}$	$x-\sqrt{2}$
3.	i	x^2+1	x^2+1	$x-i$
4.	ω	x^2+x+1	x^2+x+1	$x-\omega$
5.	$\sqrt[3]{2}$	x^3-2	$x-\sqrt[3]{2}$	$x-\sqrt[3]{2}$
6.	$1+\sqrt{2}$	x^2-2x-1	$x-1-\sqrt{2}$	$x-1-\sqrt{2}$
7.	$\sqrt{2}+\sqrt{3}$	x^4-10x^2+1	$x-\sqrt{2}-\sqrt{3}$	$x-\sqrt{2}-\sqrt{3}$
8.	$\sqrt{1+\sqrt[3]{2}}$	$x^6-3x^4+3x^2-3$	$x-\sqrt{1+\sqrt[3]{2}}$	$x-\sqrt{1+\sqrt[3]{2}}$
9.	$\sqrt{\sqrt[3]{2}-i}$	$x^{12}+3x^8-4x^6+3x^4+12x^2+5$	$x^2-2ax+\sqrt{1+2^{\frac{2}{3}}}$, where $a=\sqrt{\frac{1}{(2)^{\frac{2}{3}}}+\frac{1}{2}\sqrt{1+2^{\frac{2}{3}}}}$	$x-\sqrt{\sqrt[3]{2}-i}$
10	$\sqrt{3-\sqrt{6}}$	x^4-6x^2+3	$x-\sqrt{3-\sqrt{6}}$	$x-\sqrt{3-\sqrt{6}}$
11	$\sqrt{\frac{1}{3}+\sqrt{7}}$	$x^4-\frac{2x^2}{3}-\frac{62}{9}$	$x-\sqrt{\frac{1}{3}+\sqrt{7}}$	$x-\sqrt{\frac{1}{3}+\sqrt{7}}$
12	$\sqrt{\sqrt[3]{2}+i}$	$x^{12}+3x^8-4x^6+3x^4+12x^2+5$	$x^2-2ax+\sqrt{1+2^{\frac{2}{3}}}$, where $a=\sqrt{\frac{1}{(2)^{\frac{2}{3}}}+\frac{1}{2}\sqrt{1+2^{\frac{2}{3}}}}$	$x-\sqrt{\sqrt[3]{2}+i}$

13	$\sqrt[3]{2}+\sqrt[4]{3}$		$x-\sqrt[3]{2}-\sqrt[4]{3}$	$x-\sqrt[3]{2}-\sqrt[4]{3}$
14	$\sqrt[3]{2}+\sqrt[3]{4}$	x^3-6x-6	$x-\sqrt[3]{2}-\sqrt[3]{4}$	$x-\sqrt[3]{2}-\sqrt[3]{4}$
15	$\sqrt{-3}+\sqrt{2}$	x^4+2x^2+25	$x^2+2\sqrt{2}\,x+5$	$x-\sqrt{-3}-\sqrt{2}$
16	π	does not exist	$x-\pi$	$x-\pi$
17	e	does not exist	$x-e$	$x-e$
18	$e^{\frac{2\pi i}{1}}=1$	$g_1(x)=x-1$	$x-1$	$x-1$
19	$e^{\frac{2\pi i}{2}}=-1$	$g_2(x)=x+1$	$x+1$	$x+1$
20	$e^{\frac{2\pi i}{3}}=\omega$	$g_3(x)=x^2+x+1$	x^2+x+1	$x-\omega$
21	$e^{\frac{2\pi i}{4}}=i$	$g_4(x)=x^2+1$	x^2+1	$x-i$
22	$e^{\frac{2\pi i}{5}}$	$g_5(x)=x^4+x^3+x^2+x+1$	$x^2-2\cos\left(\frac{2\pi}{5}\right)x+1$	$x-e^{\frac{2\pi i}{5}}$
23	$e^{\frac{2\pi i}{6}}$	$g_6(x)=x^2-x+1$	$x^2-2\cos\left(\frac{\pi}{3}\right)x+1$	$x-e^{\frac{2\pi i}{6}}$
24	$e^{\frac{2\pi i}{7}}$	$g_7(x)=x^6+x^5+x^4+x^3+x^2+x+1$	$x^2-2\cos\left(\frac{2\pi}{7}\right)x+1$	$x-e^{\frac{2\pi i}{7}}$
25	$e^{\frac{2\pi i}{8}}$	$g_8(x)=x^4+1$	$x^2-2\cos\left(\frac{\pi}{4}\right)x+1$	$x-e^{\frac{2\pi i}{8}}$
26	$e^{\frac{2\pi i}{9}}$	$g_9(x)=x^6+x^3+1$	$x^2-2\cos\left(\frac{2\pi}{9}\right)x+1$	$x-e^{\frac{2\pi i}{9}}$
27	$e^{\frac{2\pi i}{10}}$	$g_{10}(x)=x^4-x^3+x^2-x+1$	$x^2-2\cos\left(\frac{\pi}{5}\right)x+1$	$x-e^{\frac{\pi i}{5}}$
28	$e^{\frac{2\pi i}{11}}$	$g_{11}(x)=x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1$	$x^2-2\cos\left(\frac{2\pi}{11}\right)x+1$	$x-e^{\frac{2\pi i}{11}}$
29.	$e^{\frac{2\pi i}{12}}$	$g_{12}(x)=x^4-x^2+1$	$x^2-2\cos\left(\frac{\pi}{6}\right)x+1$	$x-e^{\frac{\pi i}{6}}$

Results :

1. Every finite extension is algebraic but converse may not be true.
2. Finite extension of finite extension is finite.
3. Let K/E and E/F are two finite extension then K/F is also a finite extension and $[K:F]=[K:E][E:F]$. Further if $\{x_1, x_2, ..., x_m\}$ is a basis of K over E and $\{y_1, y_2, ..., y_n\}$ is a basis of E over F then $\{x_1y_1, x_1y_2, ..., x_1y_n, x_2y_1, x_2y_2, ..., x_2y_n, ..., x_my_1, x_my_2, ..., x_my_n\}$ is a basis of K over F.
4. Algebraic extension of algebraic extension is algebraic.
5. Let K/F be any extension. Suppose a and b are two algebraic element of K over F, then $a+b,\ a-b,\ ab,\ ab^{-1}(b\neq 0)$ are also algebraic over F.

Def. The smallest field containing F and a is denoted by $F(a)$. Similarly the smallest field containing F and $a_1, a_2, ...a_n$ is denoted by $F(a_1, a_2, ...a_n)$.

6. $\mathbb{Q}(\sqrt{p})=\{a+b\sqrt{p} : a,b\in\mathbb{Q}\}$
7. $\mathbb{Q}(i)=\{a+ib : a,b\in\mathbb{Q}\}$
8. **Single element result :** Let K/F be any extension and $a\in K$ be any algebraic element then
   (i) $[F(a):F]$ = degree of minimal polynomial of a over F.
   (ii) If $[F(a):F]=n$, then $\{1, a, a^2, ..., a^{n-1}\}$ is a basis of $F(a)$ over F.
9. Here p_i's and q_i's all are distinct primes.
   (i) $\left[\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, ...\sqrt{p_n}):\mathbb{Q}\right]=2^n$
   (ii) $\left[\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, ...\sqrt{p_n}):\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, ...\sqrt{p_m})\right]=2^{n-m}, 0\le m\le n$
   (iii) $\left[\mathbb{Q}(\sqrt[3]{p_1}, \sqrt[3]{p_2}, ..., \sqrt[3]{p_n}):\mathbb{Q}\right]=3^n$
   (iv) $\left[\mathbb{Q}(\sqrt[3]{p_1}, \sqrt[3]{p_2}, ..., \sqrt[3]{p_n}):\mathbb{Q}(\sqrt[3]{p_1}, \sqrt[3]{p_2}, ..., \sqrt[3]{p_m})\right]=3^{n-m}, 0\le m\le n$
   (v) $\left[\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, ...\sqrt{p_n}, \sqrt[3]{q_1}, \sqrt[3]{q_2}, ...\sqrt[3]{q_m}):\mathbb{Q}\right]=2^n3^m$
   (vi) $\left[\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, ..., \sqrt{p_n}, \sqrt[3]{q_1}, \sqrt[3]{q_2}, ..., \sqrt[3]{q_m}):\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, ..., \sqrt{p_r}, \sqrt[3]{q_1}, \sqrt[3]{q_2}, ..., \sqrt[3]{q_s})\right]=2^{n-r}\cdot 3^{m-s}$
   where $0\le r\le n, 0\le s\le m$

Remarks :

(i) The above six results are also true if some or all commas are replaced by plus (+) or minus (–).

(ii) i and ω behave as $\sqrt{p}$ because they are of degree 2.

10. If p and $q(\neq 0)$ are any integers then $e^{\frac{p\pi i}{q}}$, $\sin\left(\frac{p\pi}{q}\right)$ and $\cos\left(\frac{p\pi}{q}\right)$ are algebraic over $\mathbb{Q}$.

11. $\sin m^\circ$ and $\cos m^\circ$ are algebraic over $\mathbb{Q}$ where $m \in \mathbb{Q}$.

Exercise 4.2

1. Prove that $\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)=\mathbb{Q}\left(\sqrt{2}+\sqrt{3}\right)$.

2. Show that $\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)=\mathbb{Q}\left(\sqrt{2},\sqrt{6}\right)=\mathbb{Q}\left(\sqrt{3},\sqrt{6}\right)=\mathbb{Q}\left(\sqrt{2}+\sqrt{3}\right)=\mathbb{Q}\left(\sqrt{2}+\sqrt{6}\right)=\mathbb{Q}\left(\sqrt{3}+\sqrt{6}\right)$

   $=\mathbb{Q}\left(\sqrt{2},\sqrt{3},\sqrt{6}\right)=\left\{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} : a,b,c,d \in \mathbb{Q}\right\}$.

3. Show that $\mathbb{Q}\left(\sqrt[8]{2},\sqrt[4]{2},\sqrt{2}\right)=\mathbb{Q}\left(\sqrt[8]{2}\right)$.

4. If p_1 and p_2 are distinct primes then prove that $\mathbb{Q}\left(\sqrt{p_1},\sqrt{p_2}\right)=\mathbb{Q}\left(\sqrt{p_1}\pm\sqrt{p_2}\right)$

5. Find the following degrees and corresponding basis over $\mathbb{Q}$:

   (i) $\mathbb{Q}\left(\sqrt{2}\right)$ (ii) $\mathbb{Q}\left(\sqrt{2}+\sqrt{3}\right)$ (iii) $\mathbb{Q}(i)$

   (iv) $\mathbb{Q}(\omega)$ (v) $\mathbb{Q}(1+i)$ (vi) $\mathbb{Q}\left(\sqrt[3]{2}\right)$

   (vii) $\mathbb{Q}\left(\sqrt[5]{2}\right)$ (viii) $\mathbb{Q}(\alpha)$ where $\alpha=e^{\frac{2\pi i}{7}}$

6. Find the following degrees and corresponding basis over $\mathbb{R}$:

   (i) $\mathbb{R}\left(\sqrt{2}\right)$ (ii) $\mathbb{R}\left(\sqrt{2}+\sqrt{3}\right)$ (iii) $\mathbb{R}(i)$

   (iv) $\mathbb{R}(\omega)$ (v) $\mathbb{R}(1+i)$ (vi) $\mathbb{R}\left(\sqrt[3]{2}\right)$

   (vii) $\mathbb{R}\left(\sqrt[5]{2}\right)$ (viii) $\mathbb{R}(\alpha)$ where $\alpha=e^{\frac{2\pi i}{7}}$

7. Evaluate the following degrees and the corresponding basis :

   (i) $\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)$ over $\mathbb{Q}\left(\sqrt{2}\right)$ (ii) $\mathbb{Q}\left(\sqrt{2},\omega\right)$ over $\mathbb{Q}(\omega)$

   (iii) $\mathbb{Q}\left(\sqrt{2},\omega\right)$ over $\mathbb{Q}\left(\sqrt{2}\right)$ (iv) $\mathbb{Q}\left(\sqrt{2},i\right)$ over $\mathbb{Q}(i)$

   (v) $\mathbb{Q}\left(\sqrt{2},i\right)$ over $\mathbb{Q}\left(\sqrt{2}\right)$ (vi) $\mathbb{Q}\left(\sqrt[3]{2},\omega\right)$ over $\mathbb{Q}(\omega)$

   (vii) $\mathbb{Q}\left(\sqrt{2}+\sqrt{3}\right)$ over $\mathbb{Q}\left(\sqrt{2}\right)$ (viii) $\mathbb{Q}\left(\sqrt{2}+\omega\right)$ over $\mathbb{Q}\left(\sqrt{2}\right)$

   (ix) $\mathbb{Q}\left(\sqrt{2}+\sqrt[3]{2}\right)$ over $\mathbb{Q}\left(\sqrt{2}\right)$

8. Evaluate the following degrees and the corresponding basis :

(i) $\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)$ over $\mathbb{Q}$ (ii) $\mathbb{Q}\left(\sqrt{2},\omega\right)$ over $\mathbb{Q}$ (iii) $\mathbb{Q}\left(\sqrt{2},\omega\right)$ over $\mathbb{Q}$

(iv) $\mathbb{Q}\left(\sqrt{2},i\right)$ over $\mathbb{Q}$ (v) $\mathbb{Q}\left(\sqrt{2},i\right)$ over $\mathbb{Q}$ (vi) $\mathbb{Q}\left(\sqrt[3]{2},\omega\right)$ over $\mathbb{Q}$

(vii) $\mathbb{Q}\left(\sqrt{2}+\sqrt{3}\right)$ over $\mathbb{Q}$ (viii) $\mathbb{Q}\left(\sqrt{2}+\omega\right)$ over $\mathbb{Q}$ (ix) $\mathbb{Q}\left(\sqrt{2}+\sqrt[3]{2}\right)$ over $\mathbb{Q}$

Answers

5. (i) degree $=2$; basis $=\left\{1,\sqrt{2}\right\}$ (ii) degree $=4$; basis $=\left\{1,\sqrt{2},\sqrt{3},\sqrt{2}\sqrt{3}\right\}$

(iii) degree $=2$; basis $=\{1,i\}$ (iv) degree $=2$; basis $=\{1,\omega\}$

(v) degree $=2$; basis $=\{1,i\}$ (vi) degree $=3$; basis $=\left\{1,2^{\frac{1}{3}},2^{\frac{2}{3}}\right\}$

(vii) degree $=5$; basis $=\left\{1,2^{\frac{1}{5}},2^{\frac{2}{5}},2^{\frac{3}{5}},2^{\frac{4}{5}}\right\}$ (viii) degree $=6$; basis $=\left\{1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5\right\}$

6. (i) degree $=1$; basis $=\{1\}$ (ii) degree $=1$; basis $=\{1\}$

(iii) degree $=2$; basis $=\{1,i\}$ (iv) degree $=2$; basis $=\{1,\omega\}$

(v) degree $=2$; basis $=\{1,i\}$ (vi) degree $=1$; basis $=\{1\}$

(vii) degree $=1$; basis $=\{1\}$ (viii) degree $=2$; basis $=\{1,\alpha\}$

7. (i) degree $=2$; basis $=\left\{1,\sqrt{3}\right\}$ (ii) degree $=2$; basis $=\left\{1,\sqrt{2}\right\}$

(iii) degree $=2$; basis $=\{1,\omega\}$ (iv) degree $=2$; basis $=\left\{1,\sqrt{2}\right\}$

(v) degree $=2$; basis $=\{1,i\}$ (vi) degree $=3$; basis $=\left\{1,2^{\frac{1}{3}},2^{\frac{2}{3}}\right\}$

(vii) degree $=2$; basis $=\left\{1,\sqrt{3}\right\}$ (viii) degree $=2$; basis $=\{1,\omega\}$

(ix) degree $=3$; basis $=\left\{1,2^{\frac{1}{3}},2^{\frac{2}{3}}\right\}$

J.R. INSTITUTE OF MATHEMATICS

189/35 BEHIND RAILWAY STATION, VAISH COLLEGE ROAD, ROHTAK PIN-124001 (HARYANA)
E-mail us on - jrinstituterohtak@gmail.com, balwanmudgil54@gmail.com Mob. 8607383607, 9802177766

4.3 Splitting field and Multiple roots

Def. Splitting Field : Let $f(x) \in F[x]$ be any polynomial where F is a field. The splitting field of $f(x)$ over F is the smallest extension of F which contains all the roots of $f(x)$.

Results :

1. **Kronecker's Theorem :** Let F be a field and $f(x)$ a non constant polynomial $F[x]$. Then there is an extension field E of F in which $f(x)$ has a zero (roots).
2. Let F be a field and let $p(x) \in F[x]$ be irreducible over F. If 'a' is a zero of $p(x)$ in some extension E of F then $F(a)$ is isomorphic to $\frac{F[x]}{\langle p(x) \rangle}$ i.e, $F(a) \cong \frac{F[x]}{\langle p(x) \rangle}$. Furthermore, if $\deg p(x) = n$, then every member of $F(a)$ can be uniquely expressed in the form $c_{n-1}a^{n-1} + c_{n-2}a^{n-2} + ... + c_1 a + c_0$, where $c_0, c_1, ..., c_{n-1} \in F$.
3. Splitting Fields are unique i.e, isomorphic.
4. Criterion for multiple zeros : A polynomial $f(x)$ over a field F has a multiple zero in some extension E iff $f(x)$ and $f'(x)$ have a common factor of positive degree in $F[x]$ i.e., $\gcd(f(x), f'(x))$ is of positive degree.
5. Working Rule to find the splitting field over $\mathbb{Q}$:
   (i) Find out the roots of the given polynomial.
   (ii) Adjoin all the roots with $\mathbb{Q}$.
   (iii) Simplify to obtain splitting field.

Exercise 4.3

1. Find the splitting field, its degree and basis for the polynomial over $\mathbb{Q}$:

(i) $x^4 + 1$	(ii) $x^6 + 1$	(iii) $x^5 - 1$
(iv) $x^5 - 3x^3 + x^2 - 3$	(v) $x^4 + x^2 + 1$	(vi) $x^4 + 2$
(vii) $x^4 - 3$	(viii) $x^4 - 2$	(ix) $x^4 - 5x^2 + 6$

2. Show that $x^4 + x + 1$ over $\mathbb{Z}_2$ does not have any multiple zeros in any field extension of $\mathbb{Z}_2$.

3. Show that $x^{21}+2x^8+1$ does not have multiple zeros in any extension of $\mathbb{Z}_3$.

4. Show that $x^{21}+2x^9+1$ has multiple zeros in some extension of $\mathbb{Z}_3$.

Answers

1. (i) $\mathbb{Q}\left(\sqrt{2},i\right)$; degree $=4$; basis $=\left\{1,\sqrt{2},i,\sqrt{2}\,i\right\}$

   (ii) $\mathbb{Q}\left(\sqrt{3},i\right)$; degree $=4$; basis $=\left\{1,\sqrt{3},i,\sqrt{3}\,i\right\}$

   (iii) $\mathbb{Q}(\alpha)$, where $\alpha=e^{\frac{2\pi i}{5}}$; degree $=4$; basis $=\left\{1,\alpha,\alpha^2,\alpha^3\right\}$

   (iv) $\mathbb{Q}\left(\sqrt{3},i\right)$; degree $=4$; basis $=\left\{1,\sqrt{3},i,\sqrt{3}\,i\right\}$

   (v) $\mathbb{Q}\left(\sqrt{3}\,i\right)$; degree $=2$; basis $=\left\{1,\sqrt{3}\,i\right\}$

   (vi) $\mathbb{Q}\left(2^{\frac{1}{4}},i\right)$; degree $=8$; basis $=\left\{1,2^{\frac{1}{4}},2^{\frac{2}{4}},2^{\frac{3}{4}},i,2^{\frac{1}{4}}i,2^{\frac{2}{4}}i,2^{\frac{3}{4}}i\right\}$

   (vii) $\mathbb{Q}\left(3^{\frac{1}{4}},i\right)$; degree $=8$; basis $=\left\{1,3^{\frac{1}{4}},3^{\frac{2}{4}},3^{\frac{3}{4}},i,3^{\frac{1}{4}}i,3^{\frac{2}{4}}i,3^{\frac{3}{4}}i\right\}$

   (viii) $\mathbb{Q}\left(2^{\frac{1}{4}},i\right)$; degree $=8$; basis $=\left\{1,2^{\frac{1}{4}},2^{\frac{2}{4}},2^{\frac{3}{4}},i,2^{\frac{1}{4}}i,2^{\frac{2}{4}}i,2^{\frac{3}{4}}i\right\}$

   (ix) $\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)$; degree $=4$; basis $=\left\{1,\sqrt{2},\sqrt{3},\sqrt{2}\sqrt{3}\right\}$

4.4 Finite Fields

Results :

1. F is finite iff F^* is cyclic where $F^*=F-\{0\}$. OR F is infinite iff F^* is non cyclic.
2. $\mathbb{Q}^*,\mathbb{R}^*,\mathbb{C}^*$ are always abelian group w.r.t. multiplication but not cyclic as $\mathbb{Q},\mathbb{R}$ and $\mathbb{C}$ are field of infinite order.
3. $\mathbb{Z}_p^*$ is a cyclic group with respect to $\times_p$, where p is a prime number.
4. Characteristic of a integral domain is either zero or a prime number.

Def. Prime Field : A field having no proper subfield is called a prime field. In other words we can say that a field F is said to be a prime field if F is the only subfield of F.

5. Upto isomorphism there are only two prime fields namely $\mathbb{Q}$ and $\mathbb{Z}_p$.

6. $[\mathbb{R}:\mathbb{R}]=1$ and $[\mathbb{C}:\mathbb{R}]=2$, so there are no field between $\mathbb{R}$ and $\mathbb{C}$.

7. $[\mathbb{R}:\mathbb{Q}]=\infty$ and $[\mathbb{Q}:\mathbb{Q}]=1$, so there are infinite many fields between $\mathbb{Q}$ and $\mathbb{R}$.

8. The number of subfields of a field of order p^n is $\tau(n)$ i.e, number of divisors of *n*.

9. Let *F* be a field with $O(F)=p^n$ then it has a unique subfield of order p^m iff *m* divides *n*.

10. Let *K* be a field of order p^n and *F* be its subfield of order p^m, where *m* divides *n*, then K/F is a finite (and hence algebraic) extension and $[K:F]=\frac{n}{m}$.

Exercise 4.4

1. The number of subfields of a field of order 97^{97} is
   (a) 98 (b) 97 (c) 2 (d) 99
2. Which of the following number can be order of a subfield of a field of order 81
   (a) 1 (b) 3 (c) 9 (d) 27
3. The number of subfields of a field of order 43^{144} is
   (a) 9 (b) 12 (c) 10 (d) None of these
4. Let *F* be a field of order 16 and d_1, d_2, d_3 denotes the number of elements of multiplicative order 3, 5, 15 respectively, then which of the following is/ are
   (a) $d_1 < d_2 < d_3$ (b) $d_1 < 2d_2 = d_3$ (c) $d_1 \cdot d_2 = d_3$ (d) $d_1 + d_2 + d_3 \le 14$

---------- S C Q ----------

1. Degree of $\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)$ over $\mathbb{Q}$, where $\mathbb{Q}$ is the field of rational number is
   1. 4 2. 3
   3. 1 4. 2

2. Let I denote the ideal generated by $x^4+x^3+x^2+x+1$ in $Z_2[x]$ and $F=Z_2[x]/I$. Then,
   1. F is an infinite field.
   2. F is a finite field of 4 elements.
   3. F is a finite field of 8 elements.
   4. F is a finite field of 16 elements.

3. The no. of subfields of a field of order 97^{97} is
   (a) 98 (b) 97
   (c) 2 (d) 99

4. The number of subfields of a field of order 43^{144} is
   (a) 9 (b) 12
   (c) 10 (d) 15

5. Which of the following polynomial have multiple roots in some extension of the respective field.
   (a) $x^4+x^2+1\in Z_2[x]$
   (b) $x^{21}+28x^8+1\in Z_3[x]$
   (c) $x^3+x+1\in Z_2[x]$
   (d) $x^2+2x+2\in Z_3[x]$

6. The degree of the extension $\mathbb{Q}\left(\sqrt{2}+\sqrt[3]{2}\right)$ over the field $\mathbb{Q}\left(\sqrt{2}\right)$ is
   1. 1 2. 2
   3. 3 4. 6
   (CSIR NET June 2011)

7. For which of the following primes p, does the polynomial x^4+x+6 have a root of multiplicity >1 over a field of characteristic p ?
   1. $p=2$ 2. $p=3$
   3. $p=5$ 4. $p=7$
   (CSIR NET Dec 2011)

8. Let F be a field of 8 elements and $A=\{x\in F \mid x^7=1$ and $x^k\neq 1$ for all natural numbers $k<7\}$. Then the number of elements in A is
   1. 1 2. 2 3. 3 4. 6
   (CSIR NET June 2012)

9. Let ω be a complex number such that $\omega^3=1$ and $\omega\neq 1$. Suppose L is the field $\mathbb{Q}\left(\sqrt[3]{2},\omega\right)$ generated by $\sqrt[3]{2}$ and ω over the field $\mathbb{Q}$ of rational numbers. Then the number of subfields K of L s.t. $\mathbb{Q}\subseteq K\subseteq L$ is
   1. 2 2. 3 3. 4 4. 5
   (CSIR NET Dec 2012)

10. Let $F\subseteq\mathbb{C}$ be the splitting field of x^7-2 over $\mathbb{Q}$, and $z=e^{2\pi i/7}$ a primitive seventh root of unity.
    Let $\left[F:\mathbb{Q}(z)\right]=a$ and $\left[F:\sqrt[7]{2}\right]=b$. Then
    1. $a=b=7$ 2. $a=b=6$
    3. $a>b$ 4. $a<b$
    (CSIR NET June 2013)

11. Find the degree of the field extension $\mathbb{Q}\left(\sqrt{2},\sqrt[4]{2},\sqrt[8]{2}\right)$ over $\mathbb{Q}$.
    1. 4 2. 8 3. 14 4. 32
    (CSIR NET Dec 2014)

12. The number of subfields of a field of cardinality 2^{100} is
    1. 2 2. 4
    3. 9 4. 100
    (CSIR NET June 2015)

---------- M C Q ----------

1. Which of the following number can be order of a subfield of a field of order 81

   (a) 1 (b) 3

   (c) 9 (d) 27

2. Let F be a field of order 16 and d_1, d_2, d_3 denotes the number of elements of multiplicative order 3, 5, 15 respectively, then which of the following is/ are

   (a) $d_1 < d_2 < d_3$ (b) $d_1 < 2d_2 = d_3$

   (c) $d_1 \cdot d_2 = d_3$ (d) $d_1 + d_2 + d_3 \le 14$

3. Which of the following is true ?
   1. $\sin 7^0$ is algebraic over $\mathbb{Q}$.
   2. $\cos\frac{\pi}{17}$ is a algebraic over $\mathbb{Q}$.
   3. $\sin^{-1}1$ is algebraic over $\mathbb{Q}$.
   4. $\sqrt{2}+\sqrt{\pi}$ is algebraic over $\mathbb{Q}(\pi)$.

   (CSIR NET June 2012)

4. Let $F = F_3[x]/(x^3+2x-1)$, where F_3 is the field with 3 elements. Which of the following statements are true ?
   1. F is field with 27 elements
   2. F is a separable but not a normal extension of F_3
   3. The automorphism group of F is cyclic
   4. The automorphism group of F is abelian but not cyclic

   (CSIR NET June 2013)

5. Let F and F' be two finite fields of order q and q' respectively. Then :
   1. F' contains a subfield isomorphic to F if and only if $q \le q'$.
   2. F' contains a subfield isomorphic to F if and only if q divides q'.
   3. If the g.c.d of q and q' is not 1, then both are isomorphic to subfields of some finite field L.
   4. Both F and F' are quotient rings of the ring $\mathbb{Z}[X]$.

   (CSIR NET Dec 2013)

6. Which of the following is/are true ?
   1. Given any positive integer n, there exists a field extension of $\mathbb{Q}$ of degree n.
   2. Given a positive integer n, there exist fields F and K s.t. $F \subseteq K$ and K is Galois over F with $[K:F]=n$.
   3. Let K be a Galois extension of $\mathbb{Q}$ with $[K:\mathbb{Q}]=4$. Then there is a field L s.t. $K \supseteq L \supseteq \mathbb{Q}, [L:\mathbb{Q}]=2$ and L is a Galois extension of $\mathbb{Q}$.
   4. There is an algebraic extension K of $\mathbb{Q}$ such that $[K:\mathbb{Q}]$ is not finite.

   (CSIR NET Dec 2014)

7. Let $\omega = \cos\frac{2\pi}{10} + i\sin\frac{2\pi}{10}$. Let $K = \mathbb{Q}(\omega^2)$ and let $L = \mathbb{Q}(\omega)$. Then
   1. $[L:\mathbb{Q}]=10$ 2. $[L:K]=2$
   3. $[K:\mathbb{Q}]=4$ 4. $L=K$

   (CSIR NET Dec 2015)

8. Which of the following statements are true ?
   1. The multiplicative group of a finite field is always cyclic
   2. The additive group of a finite field is always cyclic
   3. There exists a finite field of any given order
   4. There exists at most one finite field (upto isomorphism) of any given order

   (CSIR NET June 2018)

189/35 BEHIND RAILWAY STATION, VAISH COLLEGE ROAD, ROHTAK PIN-124001 (HARYANA)
E-mail us on - jrinstituterohtak@gmail.com, balwanmudgil54@gmail.com Mob. 8607383607, 9802177766

Assignment Key
SCQ

1. 1
2. 4
3. 3
4. 4
5. 1
6. 3
7. 2
8. 4
9. 1
10. 3
11. 2
12. 3

MCQ

1. 2,3
2. 1,3,4
3. 1,2,4
4. 1,3
5. 3,4
6. ---
7. 3,4
8. 1,4