Thus $1, \bar{x}, \bar{x}^2, \ldots, \bar{x}^{n-1}$ are L. I.

Further, let $\alpha \in E = F[x]/\langle p(x) \rangle$ then $\alpha = f(x) + I$ for some $f(x) \in F[x]$.

We can write

$$f(x) = p(x)\, q(x) + r(x)$$

Where r(x) = 0 or deg r(x) < deg p(x).

Then $\alpha = f(x) + I$

$= [p(x)\, q(x) + r(x)] + I$

$= [p(x)\, q(x) + I] + [r(x) + I]$

$= I + r(x) + I \quad [\because p(x)\, q(x) \in I = \langle p(x) \rangle]$

$= r(x) + I$

But deg r(x) < n, therefore

$\alpha = r(x) + I$

$= \gamma_0 + \gamma_1 x + \gamma_2 x^2 + \ldots + \gamma_{n-1} x^{n-1} + I$

$= \gamma_0 (1+I) + \gamma_1 (x+I) + \gamma_2 (x^2+I) + \ldots + \gamma_{n-1} (x^{n-1} + I)$

$= \gamma_0 \bar{I} + \gamma_1 \bar{x} + \gamma_2 \bar{x}^2 + \ldots + \gamma_{n-1} \bar{x}^{n-1}$

Thus $\{\bar{I}, \bar{x}, \bar{x}^2, \ldots, \bar{x}^{n-1}\}$ generated E and so it is a basis for E.

Hence [E : F] = n = deg p(x).



CHECK YOUR PROGRESS

Q 18: Let Q be the field of rationals. Then show that $Q(\sqrt{2}, \sqrt{3}) = Q(\sqrt{2} + \sqrt{3})$

Q 19: Find a basis of $Q(\sqrt{3}, \sqrt{5})$ over Q.

Q 20: Find the minimal polynomial for $\sqrt{2} + \sqrt{3}$ over Q.

Q 21: Show that $[Q[\sqrt{2}] : Q] = 2$

Q 22: Show that $x^3 - 2$ is the minimal polynomial of $\sqrt[3]{2}$ over Q.



12.13 LET US SUM UP

- Elements a and b of an integral domain D are called associates of a = ub, where u is a unit of D.

- A nonzero element a of an integral domain D is called irreducible if
  (i) a is not a unit and
  (ii) whenever b, $c \in D$ such that a = bc, then b or c is a unit.
- A nonzero element p of an integral domain D is called prime if
  (i) p is not a unit and
  (ii) p|ab implies p|a or p|b.
- In an integral domain, every prime is an irreducible.
- Let D be an integral domain with unity. Then D is called a PID if every ideal of D is a principal ideal.
- In a PID, an element is an irreducible if and only if it is a prime.
- An integral domain D is a unique factorization domain if
  (i) every nonzero element of D that is not a unit can be written as a product of irreducible of D;
  (ii) If $a = p_1^{n_1}. p_2^{n_2}. . . p_k^{n_k}$ and $a = q_1^{n_1}. q_2^{n_2}. . . q_k^{n_k}$ are two expression as product of irreducible elements, where no two of the p_i's are associates and no two of the q_j's are associates, then k = r and each p_i is an associate of one and only one q_j and $n_i = m_j$.
- In a UFD, every irreducible element is prime.
- If D is a UFD, then D[x] is also UFD.
- An integral domain D is called a Euclidean domain (ED) if there exists a function $\delta : D - \{0\} \to Z$
  such that (i) $\delta(a) \geq 0$ for all $a \in D - \{0\}$,
  (ii) $\delta(ab) \geq \delta(a)$ for all $a, b \in D - \{0\}$
  and (iii) for $a \in D$, $b \in D - \{0\}$ there exists $q, r \in D$ such that a = bq + r where r = 0 or $\delta(r) < \delta(b)$.
- Every ED is a PID and every PID is a UFD.
- Let K and F be any two fields and $\sigma : F \to K$ be a monomorphism. Then $F \cong \sigma(F) \subseteq K$ and (K, σ) is called an extension of field F. Since $F \cong \sigma(F)$ and $\sigma(F)$ is a subfield of K, so we may regard F as a subfield of K.
- The dimension K as a vector space over F is called degree of K|F i.e. degree of K|F is denoted by [K : F]
- Let K|F be any extension. If $\alpha \in K$ and α satisfies a polynomial over F,

i.e. f(α) = 0 where f(x) = $\lambda_0+\lambda_1 x+\lambda_2 x^2+\ldots+\lambda_n x^n$; $\lambda_i \in F$ for all i = 0, 1, 2, . . ., n. Then α is called algebraic over R.

- The extension K|F is called algebraic extension if every element of K is algebraic over F. Otherwise, K|F is said to be transcendental extension if at least one element is not algebraic over F.



12.14 FURTHER READINGS

1) Gallian, Joseph A. : Contemporary Abstract algebra (8th Ed, Cengage Learning India Private Ltd, Delhi 110092.

2) Khanna, V. K. and Bhambri, S. K. : A course in Abstract Algebra (2002), Vikas Publishing House Pvt. Ltd, New delhi 110014.

3) Singh, J. : Theory of Field Extensions, Maharshi Dayanand University Press, Rohtak-124001.



12.15 ANSWERS TO CHECK YOUR PROGRESS

Ans to Q No 1: Let a + ib $\in$ Z[i] be a unit. Then there exists c + id $\in$ Z[i] such that

(a+ib) (c+id) = 1 (I)

$\Rightarrow$ (a–ib) (c–id) = 1 (II)

From (i) and (ii), $(a^2+b^2)(c^2+d^2) = 1$

$\Rightarrow$ $a^2+b^2 = 1$, $c^2+d^2 = 1$ [$\because$ a, b, c, d $\in$ Z]

Now $a^2+b^2 = 1 \Rightarrow a^2 = 1, b^2 = 0$ or $a^2 = 0, b^2 = 1$

$\Rightarrow$ a = $\pm$ 1, b = 0 or a = 0, b = $\pm$ 1

The units of Z[i] are $\pm 1, \pm i$; i.e. 1, –1, i, –i.

Ans to Q No 2: Let $a+b\sqrt{-5}$ be a unit in Z [$\sqrt{-5}$].

Then there exists $c+d\sqrt{-5} \in Z[\sqrt{-5}]$ such that

$(a+b\sqrt{-5})(c+d\sqrt{-5}) = 1$ (I)

$\therefore (a-b\sqrt{-5})(c-d\sqrt{-5}) = 1$ (II)

From (I) and (II), $(a^2+5b^2)(c^2+5d^2) = 1$

$\Rightarrow a^2+5b^2 = 1,\ c^2+5d^2 = 1$ [$\because a, b, c, d \in Z$]

Now $a^2+5b^2 = 1$ implies $a = \pm 1,\ b = 0$

The units of $Z[\sqrt{-5}]$ are ± 1.

Ans to Q No 3: Since $\pm 1, \pm i$ are the units in Z[i], therefore $1+i \neq 0$ is not a unit.

Let $1+i = xy$, where $x, y \in Z[i]$

$= (a+ib)(c+id)$ where $x = a+ib,\ y = c+id$.

$\therefore 1 - i = (a - ib)(c-id)$

Thus $(1+i)(1-i) = (a+ib)(a-ib)(c+id)(c-id)$

$\Rightarrow 2 = (a^2+b^2)(c^2+d^2)$

$\Rightarrow a^2+b^2 = 1,\ c^2+d^2 = 2$ or $c^2+d^2 = 1,\ a^2+b^2 = 2$

If $a^2+b^2 = 1$, then $(a+ib)(a-ib) = 1$

$\Rightarrow a+ib$ is a unit.

If $c^2+d^2 = 1$, then $(c+ib)(c-ib) = 1$

$\Rightarrow c+ib$ is a unit.

Thus $1+i = (a+ib)(c+id)$

$\Rightarrow$ either $a+ib$ is a unit or $c+id$ is a unit.

Hence $1+i$ an irreducible element in Z[i].

Ans to Q No 4: We have to show 2 is a prime element but not irreducible in Z_6.

Let $2 \mid \bar{a}\bar{b}$

$\Rightarrow 6 \mid ab - 2$

$\Rightarrow ab - 2 = 6k$ for some $k \in Z$

$\Rightarrow ab = 2(1+3k)$

$\Rightarrow 2 \mid ab$

$\Rightarrow 2 \mid a$ or $2 \mid b$ [$\because$ 2 is prime in Z]

$\Rightarrow 2 \mid \bar{a}$ or $2 \mid \bar{b}$

$\Rightarrow \bar{2}$ is prime in Z_6.

We have $\bar{2} = \bar{2} \cdot \bar{4}$

Where neither $\bar{2}$ nor $\bar{4}$ is a unit, this gives us $\bar{2}$ is not an irreducible element.

Note that Z_6 is not an integral domain.

Ans to Q No 5: Consider the ideal A = {x f(x)+2g(x) : f(x), g(x)$\in$ Z[x]} of Z[x].

We have to prove A is not principal ideal. If possible, let A is a principal ideal generated by k(x), k(x)$\in$ Z[x].

Since x = x(1+0.x +0.x^2+ . . .) +2 (0+0.x+0x^2+ . . .)$\in$ A = $\langle$ k(x)$\rangle$.

Suppose x = k(x) h(x) for some h(x)$\in$ Z[x]

Also 2$\in\langle$ k(x)$\rangle$ $\Rightarrow$ 2=k(x) p(x) for some p(x)$\in$ Z[x]

$\Rightarrow$ 2x = x k(x) p(x)

$\Rightarrow$ 2k(x) h(x) = xk(x) p(x)

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

$\Rightarrow$ each coefficient of p(x) is an even integes

i.e p(x) = 2r(x) for some p(x)$\in$ Z[x]

$\Rightarrow$ k(x) p(x) = 2k(x) r(x)

$\Rightarrow$ 2 = 2k(x) r(x)

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

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

$\Rightarrow\langle$ k(x)$\rangle$ = Z[x]

Which is not true as A is proper ideal of Z[x]. Thus A is not a principal ideal and hence z[x] is not a PID.

Ans to Q No 6: Since Z is a PID which is not a field and in a PID every irreducible element is a prime and vice versa, therefore the proper ideal $\langle$ p$\rangle$ is maximal if and only if p is a prime number.

Ans to Q No 7: Since Q is a field, therefore Q[x] is a PID which is not a field. To show $\langle$ x+2$\rangle$ is maximal ideal of Q[x] it is enough to show x+2 is an irreducible element.

Let x+2 = f(x) g(x), where f(x), g(x)$\in$ Q[x]

Then deg (x+2) = deg f(x) + deg g(x)

$\Rightarrow$ deg f(x) + deg g(x) = 1

$\Rightarrow$ either deg f(x) = 1, deg g(x) = 0 or deg f(x) = 0, deg g(x) = 1

If deg f(x) = 1, deg g(x) = 0, then g(x) = $b_0(\neq 0)\in$ Q and there exists b_0' $\in$ Q such that b_0b_0' = 1, i.e. g(x) is a unit.

Similarly, if deg f(x) = 0, deg g(x) = 1, then f(x) is a unit.

Thus x+2 is an irreducible element of Q[x] and hence $\langle$ x+2$\rangle$ is a maximal ideal of Q[x].

Ans to Q No 8: Let R be a PID. First we have to show every pair of nonzero elements a and b of R have ged and LCM.

For a, $b \in R$, consider the ideal $\langle a \rangle + \langle b \rangle$. Then $\langle a \rangle + \langle b \rangle$ is an ideal containing $\langle a \rangle$ and $\langle b \rangle$. Since R is a PID, $\langle a \rangle + \langle b \rangle$ is a principal ideal and so $\exists\ d \in R$ such that $\langle a \rangle + \langle b \rangle = \langle d \rangle$. So

$\langle a \rangle \subseteq \langle d \rangle$ and $\langle b \rangle \subseteq \langle d \rangle$

$\Rightarrow a = a.1 \in \langle a \rangle \subseteq \langle d \rangle$ and $b = b.1 \in \langle b \rangle \subseteq \langle d \rangle$

$\Rightarrow a \in \langle d \rangle$ and $b \in \langle d \rangle$

$\Rightarrow a = dr$ and $b = dr'$ where $r, r' \in R$.

$\Rightarrow d|a$ and $d|b$

If $c \in R$ such that $c|a$ and $c|b$, then $a = ct$, $b = ct'$, $t, t' \in R$.

Since $\langle a \rangle + \langle b \rangle = \langle d \rangle$ and $d \in \langle d \rangle$ so there exists $x, y \in R$ such that

$d = ax + by$

$\Rightarrow d = ctx + ct'y$

$\Rightarrow d = c(tx + t'y)$

$\Rightarrow c|d$

Thus gcd of a and b is d.

Again, we consider the ideal $\langle a \rangle \cap \langle b \rangle$ of R. Since R is a PID, so $\langle a \rangle \cap \langle b \rangle$ is a principal ideal of R and there exists $m \in R$ such that $\langle a \rangle \cap \langle b \rangle = \langle m \rangle$.

We claim that LCM (a, b) = m.

We have $\langle a \rangle \cap \langle b \rangle = \langle m \rangle$

$\Rightarrow \langle m \rangle \subseteq \langle a \rangle$ and $\langle m \rangle \subseteq \langle b \rangle$

$\Rightarrow m = m.1 \in \langle m \rangle \subseteq \langle a \rangle$ and $m = m.1 \in \langle m \rangle \subseteq \langle b \rangle$

$\Rightarrow m \in \langle a \rangle$ and $m \in \langle b \rangle$

$\Rightarrow m = ar$ and $m = br'$ for some $r, r' \in R$

$\Rightarrow a|m$ and $b|m$

Next, let $c \in R$ such that a|c, b|c. We have to show m|c.

Now $a|c \Rightarrow c = as$ for some $s \in R$

$b|c \Rightarrow c = bs'$ for some $s' \in R$

$\therefore c \in \langle a \rangle \cap \langle b \rangle$

$\Rightarrow c \in \langle m \rangle$

$\Rightarrow c = mz$ for some $z \in R$

$\Rightarrow m|c$

Thus LCM (a. b) = m.

Ans to Q No 9: Let a, b be any two non zero elements of R. Suppose one of them (say a) is a unit. Then $aa^{-1} = 1$ and

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

$\Rightarrow a|b$

Also $a = 1.1 \Rightarrow a|a$

And if c|a and c|b, then as it means c|a.

We get a = gcd (a, b).

Similarly, if b is a unit, b = gcd (a, b).

Let a and b be non units. Since R is a UFD, so

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots . p_n^{\alpha_n}$$

$$b = p_1^{\beta_1} p_2^{\beta_2} \ldots . p_n^{\beta_n}$$

as product of irreducibles (Nore it is possible to express both a and b as product of same irreducibles by suitably choosing the powers).

Let $S_i = \min \{\alpha_i, \beta_i\}$. We want to show

$d = p_1^{s_1}.p_2^{s_2} \ldots . p_n^{s_n}$ is gcd (a, b).

Now, we can write,

$$a = \left(p_1^{s_1} p_2^{s_2} \ldots . p_n^{s_n}\right) \left(p_1^{\alpha_1 - s_1}.p_2^{\alpha_2 - s_2} \ldots . p_n^{\alpha_n - s_n}\right)$$

$$= d\left(p_1^{\alpha_1 - s_1}.p_2^{\alpha_2 - s_2} \ldots . p_n^{\alpha_n - s_n}\right)$$

$\therefore d|a$

Similarly d|b.

Let c|a and c|b. We have to show c|d.

If c is a unit, $d = 1.d = (cc^{-1})d = c(c^{-1}d)$

$\Rightarrow c|d$

If c is not a unit, we can write

$c = p_1^{r_1}.p_2^{r_2} \ldots p_n^{r_n}$ where $r_i \leq \alpha_i$ for all i as c|a

and $r_i \leq \beta_i$ for all i as c|b

Thus $r_i \leq \min \{\alpha_i, \beta_i\} = s_i$ for all i

Thus $d = p_1^{s_1}.p_2^{s_2} \ldots . p_n^{s_n} = \left(p_1^{\gamma_1}.p_2^{\gamma_2} \ldots . p_n^{\gamma_n}\right) \left(p_1^{s_1 - \gamma_1}.p_2^{s_2 - \gamma_2} \ldots . p_n^{s_n - \gamma_n}\right)$

$= c \left(p_1^{s_1 - \gamma_1}.p_2^{s_2 - \gamma_2} \ldots . p_n^{s_n - \gamma_n}\right)$

$\Rightarrow c|d$

Hence gcd (a, b) = d.

Ans to Q No 10: Let a and b be any two nonzero elements of R. Suppose a is a unit. Then there exists $a^{-1} \in R$ such that $aa^{-1} = 1$.

Now $b = 1.b = (aa^{-1})b = a(a^{-1}b)$

$\Rightarrow a|b$

$\Rightarrow$ lcm (a, b) = b

Simlarly, if b is a unit, then lcm (a, b) = a.

Let now a and b be non units. Since R is a UFD, we can express.

$a = p_1^{\alpha_1}.p_2^{\alpha_2}.\ldots.p_n^{\alpha_n}$

$b = p_1^{\beta_1}.p_2^{\beta_2}.\ldots.p_n^{\beta_n}$

as product of irreducibles (Note it is possible to express both a and b as product of same irreducibles by suitably choosing the powers.

Let $t_i = \max\{\alpha_i, \beta_i\}$ for each i. We claim that $m = p_1^{t_1}.p_2^{t_2}.\ldots.p_n^{t_n}$ = lcm (a, b).

Now $m = p_1^{t1}.p_2^{t2}.\ldots.p_n^{tn}$

$= \left(p_1^{\alpha_1}.p_2^{\alpha_2}.\ldots.p_n^{\alpha_n}\right)\left(p_1^{t_1-\alpha_1}.p_2^{t_2-\alpha_2}.\ldots.p_n^{t_n-\alpha_n}\right)$

$= a\left(p_1^{t_1-\alpha_1}.p_2^{t_2-\alpha_2}.\ldots.p_n^{t_n-\alpha_n}\right)$

$\Rightarrow a|m$

Similarly, b|m

Let a|c, b|c, we have to show m|c.

Since a|c, b|c, so $c = p_1^{r_1}.p_2^{r_2}.\ldots.p_n^{r_n}$, where

$r_i \geq \alpha_i$ for all i

$r_i \geq \beta_i$ for all i

$\therefore r_i \geq \max\{\alpha_i, \beta_i\} = t_i$ for all i.

Thus $c = p_1^{\gamma_1}.p_2^{\gamma_2}.\ldots.p_n^{\gamma_n}$

$= \left(p_1^{t_1}.p_2^{t_2}.\ldots.p_n^{t_n}\right)\left(p_1^{\gamma_1-t_1}.p_2^{\gamma_2-t_2}.\ldots.p_n^{\gamma_n-t_n}\right)$

$= m\left(p_1^{\gamma_1-t_1}.p_2^{\gamma_2-t_2}.\ldots.p_n^{\gamma_n-t_n}\right)$

$\Rightarrow m|c$

Thus lcm(a, b) = m

Ans to Q No 11: Let D be a UFD and $f, g \in D[x]$ be two nonzero polynomials. Let g.c.d of coefficients of f=d and gcd of coefficients of g = d'. Then $f = df_1$ and $g = d'g_1$

Where f_1, g_1 are primitive polynomials, c(f) = dD and c(g) = d′D. Then

fg = dd′ f_1g_1

Now as f_1g_1 is primitive, dd′ is gcd of the coefficients of fg. consequently

C(fg) = dd′D

= (dD) (d′D)

= c(f) c(g)

Ans to Q No 12: As Z is a UFD, Z[x] is a UFD. Next we claim that Z[x] is not a PID. To establish our claim we can follow the as answer to the Q. No. 5.

Ans to Q No 13: Since 5 is a prime, so Z_5 is a field.

$\Rightarrow Z_5$ is a UFD.

$\Rightarrow Z_5[x]$ is a UFD.

Again, x^2+2x+3 will be reducible over Z_5 if it has a root in Z_5. But none of the elements in Z_5 is a root of x^2+2x+3. Hence it is irreducible polynomial over Z_5.

Ans to Q No 14: Let a be a unit element of D. We have to prove $\delta(a) = \delta(1)$.

Since a is a unit element of D, so there exists $b \in D$ such that ab=1.

We have

$\delta(ab) \geq \delta(a)$

$\Rightarrow \delta(1) \geq \delta(a)$ (I)

Again $\Rightarrow \delta(a) = (a.1) \geq \delta(1)$

$\Rightarrow \delta(a) \geq \delta(1)$ (II)

From (I) and (II), we get $\delta(a) = \delta(1)$

Conversely, let $\delta(a) = \delta(1)$. We have to show a is a unit element of D.

If possible, let a is not a unit. Then

d(1) < d(1.a) Taking a = 1, b = a

$\Rightarrow$ d(1) < d(a), a contradiction.

Hence a is a unit element of D.

Ans to Q No 15: We know that Z[i] is an integral domain. We define a map

δ : Z[i] $\rightarrow$ Z by

$\delta(a+ib) = a^2+b^2$ where $a+ib \neq 0$

Then (i) $\delta(a+ib) > 0$ for all $a+ib \in Z[i] - \{0\}$

(ii) Let a+ib, c+id $\in$ Z[i] – {0}. Then

δ [(a+ib) (c+id)] = δ [(ac–bd)+ (ad+bc)i]

= $(ac–bd)^2 + (ad+bc)^2$

= $(a^2+b^2)(c^2+d^2) \geq a^2+b^2 = \delta$ (a+ib)

i.e. δ [(a+ib) (c+id)] $\geq \delta$ (a+ib).

(iii) Let a+ib $\in$ Z[i] and c+id ($\neq 0$) $\in$ Z[i]. Let

$\frac{a+ib}{c+id}$ = p+iq, where p, q $\in$ Q.

We can write p = [p]+Q, where [p] and θ are the integral part and fractional part of p respectively.

Then there exists m $\in$ Z such that $|p–m| \leq \frac{1}{2}$

Similarly, q = [q]+ θ' and there exists an integer n such that $|q–n| \leq \frac{1}{2}$.

Let p–m = α and q–n = β. Then

$|\alpha| \leq \frac{1}{2}$ and $|\beta| \leq \frac{1}{2}$

We have p+iq = $\frac{a+ib}{c+id}$

$\Rightarrow$ a+ib = (p+iq) (c+id)

= [(m+ α)+(n+ β) i] (c+id) [$\because$ p–m = α, q – n = β]

= [(m+in) (α+i β)] (c+id)

= (m+in) (c+id) + (α+i β) (c+id)

= (m+in) (c+id) + r

Where r = (α+i β) (c+id) $\in$ Z[i] and r = (α+i β)(c+id)

= (αc– β d)+i(β c+ αd)

If r $\neq$ 0, then δ (r) = (αc– β d)^2+(β c+ αd)^2

= (α^2+ β^2)(c^2+d^2)

$\leq \left(\frac{1}{4}+\frac{1}{4}\right)(c^2+d^2)$

= $\frac{1}{2}(c^2+d^2)$

< $c^2+d^2 = \delta$ (c+id)

i.e. (r) < δ (c+id).

Hence if a+ib $\in$ Z[i] , c+id ($\neq 0$) $\in$ Z[i], then there exists m+in $\in$ Z[i] such

that

$a+ib = (m+in)(c+id) + r$ where $r = 0$ or $\delta(r) < \delta(c+id)$.

Thus $Z[i]$ is an Euclidean domain.

Ans to Q No 16: (i) Let a and b are associates. Then

$a = bx$, where x is a unit in D

$\Rightarrow \delta(a) = \delta(bx) \geq \delta(b)$

$\Rightarrow \delta(a) \geq \delta(b)$ (I)

Also $a = bx$

$\Rightarrow b = ax^{-1}$

$\Rightarrow \delta(b) = \delta(ax^{-1}) \geq \delta(a)$

$\Rightarrow \delta(b) \geq \delta(a)$ (II)

From (i) and (ii), we get

$\delta(a) = \delta(b)$

(ii) Let $a|b$ and $\delta(a) = \delta(b)$. We have to prove a and b are associates.

First we show $b|a$. For $a \in D$, $b(\neq 0) \in D$, there exists $q, r \in D$ such that

$a = bq+r$ where $r = 0$ or $\delta(r) < \delta(b)$

If $r \neq 0$, then $\delta(r) < \delta(b)$. Since $a|b$, so

$b = ac$ for some $c \in D$.

Now $a = bq+r \Rightarrow a = acq+r$

$\Rightarrow r = a(1-cq)$

$\Rightarrow \delta(r) = \delta(a(1-cq)) \geq \delta(a) = \delta(b)$

$\Rightarrow \delta(r) \geq \delta(b)$, a contradiction.

Hence $r = 0$. Thus $a = bq \Rightarrow b|a$. So we get $a|b$ and $b|a$

$\Rightarrow$ a and b are associates since

$a|b \Rightarrow b = ac$ for some $c \in D$

$b|a \Rightarrow a = bd$, for some $d \in D$

$\Rightarrow a = acd$

$\Rightarrow cd = 1$

$\Rightarrow$ c is unit.

(iii) Let a be not a unit. We have to prove $\delta(ab) > \delta(b)$.

We have $b|ab$ and $\delta(ab) \geq \delta(b)$.

Let $\delta(ab) = \delta(b)$. Then

ab and b are associates

$\Rightarrow$ ab = bc, where c is a unit in D.

$\Rightarrow$ ab = cb

$\Rightarrow$ a = c

$\Rightarrow$ a is a unit, a contradiction

Hence S(ab)>S(b).

Conversely, let (ab) > (b). We have to prove that a is not a unit.

If possible, let a be a unit in D. Then there exists $a' \in D$ such that $aa' = 1$.

$\Rightarrow b(aa') = b$

$\Rightarrow (ab)a' = b$

$\Rightarrow \delta(b) = \delta((ab)a') \delta \geq \delta(ab)$

$\Rightarrow \delta(b) \geq \delta(ab)$, a contradiction.

Hence a is not a unit.

(iv) We know that Z[i] is a Euclidean domain.

We define : Z[i] is a Euclidean domain.

We define δ : Z[i] – {0} Z

$\delta(a+ib) = a^2+b^2$.

The units of Z[i] are $\pm 1, \pm i$.

We have $\delta(3+2i) = \delta(3-2i) = 13$ but 3+2i and 3–2i are not associates as associates of 3+2i are 3+2i, –3 – 2i, –2+3i and 2–3j.

Ans to Q No 17: Since $Z(\sqrt{2}) = \{a+b\sqrt{2} : a, b \in Z\}$ is an integral domin, so we define $\delta : Z[\sqrt{2}]-\{0\} \to Z$ by $\delta(a+b\sqrt{2}) = |a^2-2b^2|$.

(i) $\delta(a+b\sqrt{2}) = |a^2-2b^2| \geq 0$ for all $a+b\sqrt{2}$ $(\neq 0) \in Z[\sqrt{2}]$.

(ii) $\delta[(a+b\sqrt{2})(c+d\sqrt{2})] = \delta[(ac+2bd) + (bc+ad)\sqrt{2}]$

$= |(ac+2bd)^2 - 2(bc+ad)^2|$

$= |(a^2-2b^2)(c^2-2d^2)|$

$\geq |a^2 - 2b^21 = \delta(a+b\sqrt{2})$

i.e. $\delta[(a+b\sqrt{2})(c+d\sqrt{2})] \geq \delta(a+b\sqrt{2})$.

(iii) Let $a+b\sqrt{2}, c+d\sqrt{2} \in Z[\sqrt{2}]$, where $c+d\sqrt{2} \neq 0$.

Let $\frac{a+b\sqrt{2}}{c+d\sqrt{2}} = p+q\sqrt{2}$, where $p, q \in Q$.

Let $p = [p]+\theta$, where [p] and θ are the integral and fractional parts of p

respectively. Then there exists m such that $|p-m| \le \frac{1}{2}$.

Similarly, for q = [q]+ θ' where [q] and θ' are the integral and fractional parts of q respectively. Then there exists n such that $|q-n| \le \frac{1}{2}$.

Let p–m = α and q–n = β. Then $|\alpha| \le \frac{1}{2}$, $|\beta| \le \frac{1}{2}$.

Thus $\frac{a+b\sqrt{2}}{c+d\sqrt{2}} = p+q\sqrt{2}$

$\Rightarrow a+b\sqrt{2} = (c+d\sqrt{2})(p+q\sqrt{2})$

$\Rightarrow a+b\sqrt{2} = (c+d\sqrt{2})[(m+\alpha)+(n+\beta)\sqrt{2}]$

$\Rightarrow a+b\sqrt{2} = (c+d\sqrt{2})(m+n\sqrt{2}) + (c+d\sqrt{2})(\alpha+\beta\sqrt{2})$

$= (c+d\sqrt{2})(m+n\sqrt{2}) + r$

Where $r = (c+d\sqrt{2})(\alpha+\beta\sqrt{2}) \in Z[\sqrt{2}]$ and

$\delta(r) = \delta[(c+d\sqrt{2})(\alpha+\beta\sqrt{2})]$

$= \delta[(c\alpha+2d\beta) + (c\beta+d\alpha)\sqrt{2}]$

$= |(c\alpha+2d\beta)^2 - 2(c\beta+d\alpha)^2|$

$= |(\alpha^2-2\beta^2)-(c^2-2d^2)|$

$= |\alpha^2-2\beta^2|\,|c^2-2d^2|$

$\le (|\alpha|^2+2|\beta|^2)\,|c^2-2d^2|$

$\le \left(\frac{1}{4}+2.\frac{1}{4}\right)|c^2-2d^2| \qquad [\because |\alpha| \le \frac{1}{2}, |\beta| \le \frac{1}{2}]$

$= \frac{3}{4}|c^2-2d^2|$

$< |c^2-2d^2| = \delta(c^2+2d^2)$

Hence $Z[\sqrt{2}]$ is a Euclidean domain.

Ans to Q No 18: By definition, $\sqrt{2}, \sqrt{3} \in Q(\sqrt{2}, \sqrt{3})$

$\Rightarrow \sqrt{2}+\sqrt{3} \in Q(\sqrt{2}, \sqrt{3})$

$\Rightarrow Q(\sqrt{2}+\sqrt{3}) \subseteq Q(\sqrt{2}, \sqrt{3})$ (I)

We have $\sqrt{2}+\sqrt{3} \in Q(\sqrt{2}+\sqrt{3})$

$\Rightarrow (\sqrt{2}+\sqrt{3})^2 \in Q(\sqrt{2}+\sqrt{3})$

Also $5 \in Q(\sqrt{2}+\sqrt{3})$

Thus $(\sqrt{2}+\sqrt{3})^2 - 5 \in Q(\sqrt{2}+\sqrt{3})$

$$\Rightarrow 2\sqrt{2}\ \sqrt{3} \in Q\left(\sqrt{2}+\sqrt{3}\right)$$

Also $2 \in Q\left(\sqrt{2}+\sqrt{3}\right)$

$$\Rightarrow 2\times\frac{1}{2}\sqrt{2}\ \sqrt{3} \in Q\left(\sqrt{2}+\sqrt{3}\right)$$

$$\Rightarrow \sqrt{2}\ \sqrt{3} \in Q\left(\sqrt{2}+\sqrt{3}\right)$$

Now $\sqrt{2}+\sqrt{3} \in Q\left(\sqrt{2}+\sqrt{3}\right)$ and $\sqrt{2}\ \sqrt{3} \in Q\left(\sqrt{2}+\sqrt{3}\right)$

$$\Rightarrow \left(\sqrt{2}+\sqrt{3}\right)\sqrt{2}\ \sqrt{3} \in Q\left(\sqrt{2}+\sqrt{3}\right)$$

$$\Rightarrow 2\sqrt{3}+3\sqrt{2} \in Q\left(\sqrt{2}+\sqrt{3}\right)$$

Again $\sqrt{2}+\sqrt{3} \in Q\left(\sqrt{2}+\sqrt{3}\right)$

$$3\sqrt{2}+3\sqrt{3} \in Q\left(\sqrt{2}+\sqrt{3}\right)$$

Thus $\left(3\sqrt{2}+3\sqrt{3}\right)-\left(2\sqrt{3}+3\sqrt{2}\right) \in Q\left(\sqrt{2}+\sqrt{3}\right)$

$$\Rightarrow \sqrt{3} \in Q\left(\sqrt{2}+\sqrt{3}\right)$$

Similarly we can show $\sqrt{2} \in Q\left(\sqrt{2}+\sqrt{3}\right)$

Thus $Q\left(\sqrt{2}, \sqrt{3}\right) \subseteq Q\left(\sqrt{2}+\sqrt{3}\right)$ (II)

From (I) and (II), we get

$$Q\left(\sqrt{2}, \sqrt{3}\right) = Q\left(\sqrt{2}+\sqrt{3}\right)$$

Ans to Q No 19: We have $\left[Q\left(\sqrt{3}, \sqrt{5}\right): Q\right] = \left[Q\left(\sqrt{3}\right)\left(\sqrt{5}\right): Q\right]$

$$= \left[Q\left(\sqrt{3}\right)\left(\sqrt{5}\right): Q\left(\sqrt{3}\right)\right]\left[Q\left(\sqrt{3}\right): Q\right]$$

$$= \left[L\left(\sqrt{5}\right): L\right]\left[Q\left(\sqrt{3}\right): Q\right] \text{ where } L = Q\left(\sqrt{3}\right)$$

= deg I rr (L, $\sqrt{5}$) x deg Irr (Q, $\sqrt{3}$)

= deg (x^2–5) x deg (x^2–3)

= 2 x 2

= 4

Thus basis has 4 elements.

Also if [F(a) : F] = n, then 1, a, a^2, . . ., a^{n-1} is basis of F(a) over F.

Thus basis of L $\left(\sqrt{5}\right)$ over L is {1, $\sqrt{5}$ } and basis of Q $\left(\sqrt{3}\right)$ over Q is {1, $\sqrt{3}$).

Thus the basis of $\left[Q\left(\sqrt{3}, \sqrt{5}\right): Q\right] = \left[L\left(\sqrt{5}\right): L\right]\left[Q\left(\sqrt{3}\right): Q\right]$ is $\left\{1.1, 1.\sqrt{3}, 1.\sqrt{5}, \sqrt{3}.\sqrt{5}\right\} = \left\{1, \sqrt{3}, \sqrt{5}, \sqrt{5}\right\}$

Ans to Q No 20: $\left(\sqrt{2}+\sqrt{3}\right)^2 = 5+2\sqrt{6}$

$$\Rightarrow \left(\sqrt{2}+\sqrt{3}\right)^4 = 49+20\sqrt{6}$$

So $\left(\sqrt{2}+\sqrt{3}\right)^4-10\left(\sqrt{2}+\sqrt{3}\right)^2=-1$

$\Rightarrow \left(\sqrt{2}+\sqrt{3}\right)^4-10\left(\sqrt{2}+\sqrt{3}\right)^2+1=0$

Therefore $a=\sqrt{2}+\sqrt{3}$ satisfies $f(x)=x^4-10x^2+1$ Over Q. Let p(x) = Irr (Q, a).

Then $\sqrt{2}-\sqrt{3}$, $-\sqrt{2}+\sqrt{3}$, $-\sqrt{2}-\sqrt{3}$ are also roots of p(x). So degree of p(x) is al least 4.

But f(a) = 0 and $f(x)\in Q[x]$

$\Rightarrow$ p(x) |f(x)

$\Rightarrow$ p(x) = f(x)

So f(x) is the minimal polynomial for $\sqrt{2}+\sqrt{3}$ over Q.

Ans to Q No 21: Since $Q[\sqrt{2}]=\{a+b\sqrt{2} : a, b\in Q\}$ is field extension of Q. The subset $\{1, \sqrt{2}\}$ form a basis of $Q[\sqrt{2}]$ over Q. Consequently $[Q[\sqrt{2}] : Q] = 2$

Ans to Q No 22: x^3-2 is a monic polynomial satisfied by $3\sqrt{2}$. By Eisenstin's Criterion, x^3-2 is irreducible over Q, so no polynomial over Q of degree less than 3 can be satisfied by $3\sqrt{2}$. Thus x^3-2 is the minimal polynomial of $3\sqrt{2}$ over Q.



12.16 MODEL QUESTIONS

Q 1: Every ideal in a Euclidean domain is a principal ideal.

Q 2: Show that in a PID every nonzero prime ideal is maximal.

Q 3: Let a, b be two nonzero elements of a ED D. If b is not a unit in D, then $\delta(a) < \delta(ab)$.

Q 4: Let D be a PID and a, b be two nonzero elements of D. Show that lcm (a, b)(gcd (a, b) = abu, where u is a unit.

Q 5: Show that $Z[\sqrt{3}] = \{a+\sqrt{3}\, b : a, b\in Z\}$ is a ED.

Q 6: Let D be a commutative ring with unity such that D[x] is a PID. Show that D is a field.

Q 7: Show that an integral domain D with unity is a field if and only if D[x] is a PID.

Q 8: Show that Z[$\sqrt{-3}$] is not a UFD.

Q 9: Show that in Z_{12}, gcd ($\bar{6}$, $\bar{8}$) = $\bar{2}$ and $\overline{10}$. Also show that $\bar{6}$ and $\bar{8}$ have no lcm in Z_{12}.

Q 10: Show that Z[$\sqrt{5}$] is not a UFD.

Q 11: Prove that if a ∈ K is algebraic over F of an odd degree, then F(a) = F(a^2).

Q 12: Let K|F be a field extension. For any two elements a, b ∈ K, prove that F(a, b) = F(b, a).

Q 13: Find a basis and degree of Q($\sqrt{2}$, $\sqrt{3}$) over F.

Q 14: Find the minimal polynomial of $\sqrt[3]{2}+\sqrt[3]{4}$ over Q.

Q 15: Let E ba an extension field of F. Show that [E : F] finite if and only if E = F (a_1, a_2, . . ., a_n), where a_1, a_2, . . ., a_n are algebraic over F.

Q 16: If α and β are real numbers and α and β are transcendental over Q, show that either $\alpha\beta$ or $\alpha+\beta$ is also transcentental over Q.

Q 17: Let a and b belong to some extension field of F and let b be algebraic over F. Prove that [F(a, b) : F(a)] ≤ [F(a, b) : F].

Q 18: Let a, b ∈ Q. Show that $Q\left(\sqrt{a}, \sqrt{b}\right) = Q\left(\sqrt{a}+\sqrt{b}\right)$.

*** ***** ***