Ex. 7. *Prove that the mapping* $\phi : D \to F$ *defined by* $\phi(a) = [a, 1]$ *is an isomorphism of* D *into* F.

Ex. 8. *Let* D *be an integral domain;* $a, b \in D$. *Suppose that* $a^n = b^n$ *and* $a^m = b^m$ *for two relatively prime integers* m *and* n. *Prove that* $a = b$.

[D.U., 2000, 1995]

Solution. Let $a = 0$. Then $a^n = 0$ and so $b^n = 0$ ($\because$ $a^n = b^n$).

Now $b^n = 0 \Rightarrow b.b...b$ (n times) $= 0$.

Thus $b = 0$, since D is an integral domain.

$\therefore$ $a = b$. Similarly, if $b = 0$, then $a = 0$ and so $a = b$.

We now consider the case when $a \neq 0$ and $b \neq 0$.

Since D is an integral domain, D can be imbedded in a field F.

Let $f : D \to F$ be an isomorphism. We have

$$\begin{aligned}\{f(a)\}^n &= f(a) \cdot f(a) \ldots f(a) \ (n \text{ times}) \\ &= f(a \cdot a \ldots a), \quad \text{since } f \text{ is a homomorphism} \\ &= f(a^n) = f(b^n), \text{ since } a^n = b^n \\ &= f(b \cdot b \ldots b) \\ &= f(b) \cdot f(b) \ldots f(b) \ (n \text{ times}), \text{ as } f \text{ is a homo.}\end{aligned}$$

$$\therefore \qquad \{f(a)\}^n = \{f(b)\}^n. \qquad \ldots(1)$$

Similarly, $\{f(a)\}^m = \{f(b)\}^m$. $\qquad \ldots(2)$

Since n and m are relatively prime integers, there exist two integers p and q such that $np + mq = 1$. Now

$$\begin{aligned}f(a) = \{f(a)\}^{np+mq} &= [\{f(a)\}^n]^p \cdot [\{f(a)\}^m]^q \\ &= [\{f(b)\}^n]^p \cdot [\{f(b)\}^m]^q, \text{ by (1) and (2)} \\ &= \{f(b)\}^{np} \cdot \{f(b)\}^{mq} = \{f(b)\}^{np+mq} = f(b).\end{aligned}$$

$$\therefore \qquad f(a) = f(b) \Rightarrow a = b, \text{ since } f \text{ is one-to-one.}$$

Remark 1. In the relation $np + mq = 1$, one of the integers p and q is necessarily negative. If p is negative, then $p = -l$, for some postive integer l. Consequently, $a^p = (a^{-1})^l$, which may not exist in D. However, F being a field,

$$\{f(a)\}^p = [\{f(a)\}^{-1}]^l \in F, \quad \text{as } f(a) \neq 0 \in F.$$

Remark 2. *The conclusion of the above problem may not hold, if* D *is not an integral domain.*

The ring $\mathbf{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$ of integers modulo 8 is not an integral domain, since $2 \neq 0$ and $4 \neq 0$, but $2 \otimes_8 4 = 0 \in \mathbf{Z}_8$.

We take $a = 2$, $b = 4 \in \mathbf{Z}_8$, $m = 3$, $n = 4$.

Then m and n are relatively prime integers satisfying

$a^m = 2^3 = 0$ in $\mathbf{Z}_8$, $b^m = 4^3 = 0$ in $\mathbf{Z}_8$;

$a^n = 2^4 = 0$ in $\mathbf{Z}_8$, $b^n = 4^4 = 0$ in $\mathbf{Z}_8$.

$a^m = b^m$ and $a^n = b^n$, $(n, m) = 1$, but $a \neq b$.

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

$\Rightarrow \quad f(ad) = f(bc)$, since f is a homomorphism

$\Rightarrow \quad ad = bc$, since f is one-to-one

$\Rightarrow \quad [a, b] = [c, d]$

$\Rightarrow \phi$ is one-to-one.

Thirdly, we prove that ϕ is onto.

Let $[\alpha, \beta] \in F_2$ be arbitrary. Then $\alpha, \beta \in D_2$ and $\beta \neq 0$.

Since $f: D_1 \to D_2$ is onto, there exist two elements $a_1, b_1 \in D_1$ such that $f(a_1) = \alpha, f(b_1) = \beta$.

As shown above, $\beta \neq 0 \Rightarrow f(b_1) \neq 0 \Rightarrow b_1 \neq 0 \in D_1$.

$\therefore \quad [\alpha, \beta] = [f(a_1), f(b_1)] = \phi\{[a_1, b_1]\}$, by (1) and $[a_1, b_1] \in F_1$.

Thus ϕ is onto.

Finally, we prove that ϕ is a homomorphism.

Let $[a, b], [c, d] \in F_1$.

Then $[a, b] + [c, d] = [ad + bc, bd]$ and $[a, b]\,[c, d] = [ac, bd]$.

Using (1), we have

$$\begin{aligned}\phi\{[a, b] + [c, d]\} &= [f(ad + bc), f(bd)] \\ &= [f(ad) + f(bc), f(bd)], \text{ as } f \text{ is a homomorphism} \\ &= [f(a)f(d) + f(b)f(c), f(b)f(d)], \\ &\qquad \text{as } f \text{ is a homomorphism} \\ &= [f(a), f(b)] + [f(c), f(d)] \\ &= \phi\{[a, b]\} + \phi\{[c, d]\}, \text{ by (1).}\end{aligned}$$

$$\begin{aligned}\text{Again } \phi\{[a, b]\,[c, d]\} &= \phi\{[ac, bd]\} = [f(ac), f(bd)], \text{ by (1)} \\ &= [f(a)f(c), f(b)f(d)], \text{ as } f \text{ is a homomorphism} \\ &= [f(a), f(b)]\,[f(c), f(d)] \\ &= \phi\{[a, b]\}\,\phi\{[c, d]\}, \text{ by (1).}\end{aligned}$$

Thus ϕ is a homomorphism, one-to-one and onto and so $F_1 \approx F_2$.

Hence F_1 and F_2 are isomorphic.

Remark. *The converse of the above theorem may not be true i.e.,* if the quotient fields F_1 and F_2 of two integral domains D_1 and D_2, respectively, are isomorphic; then D_1 and D_2 may not be isomorhpic.

Let $D_1 = \mathbf{Z}$ (all integers) and $D_2 = \mathbf{E}$ (all even integers).

Then D_1 and D_2 are two non-isomorphic integral domains (*e.g.*, you cannot set up a one-to-one correspondence between D_1 and D_2). However, their quotient fields are each $\mathbf{Q}$ (all rationals) and $\mathbf{Q} \approx \mathbf{Q}$.

Ex. 1. *Give examples of two non-isomorphic integral domains having isomorphic quotient fields.* [D.U., 1988, 94]

Ex. 2. *Show that the converse of Theorem 2.5.8 is not true by considering the integral domains* $\mathbf{Z}$ *and* $5\mathbf{Z}$. [D.U., 1997]

Hint. $\mathbf{Z} = \{\ldots -3, -2, -1, 0, 1, 2, 3, \ldots\}$,
$5\mathbf{Z} = \{\ldots, -10, -5, 0, 5, 10, \ldots\}$.

Then $\mathbf{Z}$ and $5\mathbf{Z}$ are non-isomorphic integral domains, since we cannot establish a one-to-one correspondence between $\mathbf{Z}$ and $5\mathbf{Z}$. However, their quotient fields are each $\mathbf{Q}$ and $\mathbf{Q} \approx \mathbf{Q}$.

2.6 Maximal and Prime Ideals

Definition (Maximal Ideal)

An ideal $M \neq R$ of a ring R is called a **maximal ideal** *of R, if for any ideal U of R such that*

$$M \subset U \subset R, \text{ then either } M = U \text{ or } U = R.$$

In other words, an ideal $M \neq R$ is a **maximal ideal** *of R, if there does not exist any proper ideal between M and R.*

Illustrations

1. $\{0, 2\}$ is a maximal ideal of the ring $\mathbf{Z}_4 = \{0, 1, 2, 3\}$ modulo 4.
2. $\{0, 3\}$ and $\{0, 2, 4, 6\}$ are maximal ideals of the ring
$\mathbf{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$ modulo 8.

Notice that you cannot find a proper ideal between $\{0, 3\}$ and $\mathbf{Z}_8$. Further, $\{0, 4\}$ is an ideal of $\mathbf{Z}_8$, but is not a maximal ideal of $\mathbf{Z}_8$, since

$$\{0, 4\} \subset \{0, 2, 4, 6\} \subset \mathbf{Z}_8.$$

EXAMPLES

Example 2.6.1. *Find the maximal ideals of $\mathbf{Z}_6$, the ring of integers modulo 6.* [D.U., 1996]

Solution. The proper ideals of $\mathbf{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ are $(3) = \{0, 3\}$, $(2) = \{0, 2, 4\}$.

Since there does not exist any proper ideal between (3) and $\mathbf{Z}_6$, $(3) = \{0, 3\}$ is a maximal ideal of $\mathbf{Z}_6$.

Similarly, $(2) = \{0, 2, 4\}$ is also a maximal ideal of $\mathbf{Z}_6$.

Example 2.6.2. *Find the maximal ideals of $\mathbf{Z}_{12}$, the ring of integers modulo 12.*

Solution. We know $\mathbf{Z}_{12} = \{0, 1, 2, \ldots, 11\}$.

The proper ideals of $\mathbf{Z}_{12}$ are

$$(2) = \{0, 2, 4, 6, 8, 10\}\ (3) = \{0, 3, 6, 9\},$$

$$(4) = \{0, 4, 8\},\ (6) = \{0, 6\}.$$

Since there does not exist any proper ideal between (3) and $\mathbf{Z}_{12}$, $\{0, 3, 6, 9\}$ is a maximal ideal of $\mathbf{Z}_{12}$. It may be observed that $(2) = \{0, 2, 4, 6, 8, 10\}$ is also a maximal ideal of $\mathbf{Z}_{12}$. However, (4) and (6) are not maximal ideals of $\mathbf{Z}_{12}$, since $(4) \subset (2) \subset \mathbf{Z}_{12}$ and $(6) \subset (3) \subset \mathbf{Z}_{12}$.

Example 2.6.3. *Show that* $\{0\}$ *is the only maximal ideal of a field* F.

Solution. We know that a field F has only two ideals F and $\{0\}$. Since $\{0\} \neq F$ ($\because 1 \in F$ and $1 \neq 0$), $\{0\}$ is the only maximal ideal of F.

Example 2.6.4. *Show that* $(4) = \{\ldots -8, -4, 0, 4, 8, \ldots\}$ *is a maximal ideal of the ring* **E** *of even integers.*

Solution. Since $2 \notin (4)$, $(4) \neq \mathbf{E}$. Let U be any ideal of **E** such that $(4) \subset U \subset \mathbf{E}$, $(4) \neq U$. Then there exists some $x \in U$ such that $x \notin (4) \Rightarrow x$ is an even integer not divisible by 4

$\Rightarrow x = 4n + 2$ for some integer $n \Rightarrow 2 = x - 4n$, where $x - 4n \in U$

$\Rightarrow 2 \in U \Rightarrow (2) \subseteq U \Rightarrow \mathbf{E} = U$.

Hence (4) is a maximal ideal of **E**.

Example 2.6.5. *Show that* $M = (n_0)$ *is a maximal ideal of* **Z** *iff* n_0 *is a prime number.*

Solution. Let n_0 be a prime number. We shall prove that $M = (n_0)$ is a maximal ideal of **Z**.

Let $U = (n) = \{nx : x \in \mathbf{Z}\}$ be any ideal of **Z** such that $M \subset U \subset \mathbf{Z}$.

Since $n_0 \in M$, $n_0 \in U \Rightarrow n_0 = nx$, for some $x \in \mathbf{Z}$. Since n_0 is prime, either $n = 1$ or $n = n_0$. If $n = 1$, then $U = (1) = \mathbf{Z}$. If $n = n_0$, then $U = M$. Hence $M = (n_0)$ is a maximal ideal of **Z**.

Conversely, let $N = (n_0)$ be a maximal ideal of **Z**. We shall prove that n_0 is a prime number.

Let $n_0 = ab$, where a and b are positive integers. Let $U = (a)$. Suppose x is an artbitrary element of M. Then $x = n_0 r$ for some $r \in \mathbf{Z} \Rightarrow x = (ab)r$

$\Rightarrow x = a(br) \Rightarrow x \in U$. Thus $M \subset U \subset \mathbf{Z}$.

Since M is a maximal ideal of **Z**, either $M = U$ or $U = \mathbf{Z}$.

If $U = \mathbf{Z}$, then $1 \in U = (a) \Rightarrow 1 = ay$, for some $y \in \mathbf{Z}$. So $a = 1$.

If $M = U$, then $a \in U \Rightarrow a \in M \Rightarrow a = n_0 . t$, for some $t \in \mathbf{Z}$

$\Rightarrow a = (ab)\, t = a\,(bt) \quad \Rightarrow bt = 1 \Rightarrow b = 1$.

Thus $a = 1$ or $b = 1$ (and $n_0 = ab$). Hence n_0 is a prime number

Remark. It may be noticed that (2), (3), (5), (7) etc. are prime ideals of **Z**, where $(2) = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$, $(3) = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$ etc.

Example 2.6.6. *Let* R *be the ring of all the real-valued continuous functions on the closed unit interval. Show that*

$$M = \{f \in R : f(\tfrac{1}{3}) = 0\}$$

is a maximal ideal of R. [D.U, 1994]

Solution. Let **R** denote the set of all real numbers.

The given ring is

$$R = \{f \mid f : [0, 1] \to \mathbf{R} \text{ is continuous on } [0,1]\}.$$

Notice that R is a ring w.r.t. the compositions :

$$\left.\begin{aligned}(f+g)(x) &= f(x)+g(x)\\ (fg)(x) &= f(x)\,.\,g(x)\end{aligned}\right\}\ \forall\ x\in[0,1] \text{ and } f,g\in R.$$

We proceed to show that M is an ideal of R.

Let $f, g \in M$. Then $f(\frac{1}{3}) = 0 = g(\frac{1}{3})$. We have

$$(f-g)(\tfrac{1}{3}) = f(\tfrac{1}{3}) - g(\tfrac{1}{3}) = 0 \text{ and so } f-g\in M.$$

Let $f\in M$ and $h\in R$. Then $f(\frac{1}{3}) = 0$ and

$$(fh)(\tfrac{1}{3}) = f(\tfrac{1}{3})\,h(\tfrac{1}{3}) = 0\,.\,h(\tfrac{1}{3}) = 0 \Rightarrow fh\in M.$$

Similarly, $hf\in M$ and so M is an ideal of R. Finally, we show that M is a maximal ideal of R. Let U be any ideal of R such that

$$M\subset U\subset R \quad\text{and}\quad M\neq U.$$

We need to show that $U = R$.

Since $M\subset U$ and $M\neq U$, there exists a function $g\in U$ such that $g\notin M$, *i.e.*, $g(\frac{1}{3})\neq 0$

i.e., $\alpha\neq 0$, where $\alpha = g(\frac{1}{3})$. ...(1)

[Notice that $g(\frac{1}{3}) = 0 \Rightarrow g\in M$, a contradiction]

We define a function $h : [0, 1] \to \mathbf{R}$ as

$$h(x) = g(x) - \alpha,\quad \forall\quad x\in[0,1] \qquad ...(2)$$

$$\Rightarrow\qquad h(\tfrac{1}{3}) = g(\tfrac{1}{3}) - \alpha = 0, \text{ using (1)}$$

$\Rightarrow h\in M \Rightarrow h\in U$, since $M\subset U$.

Since U is an ideal of R, therefore

$$g\in U \text{ and } h\in U \Rightarrow g-h\in U \Rightarrow \alpha\in U, \text{ by (2)}$$

Since $\alpha\neq 0$, $\alpha^{-1}\in\mathbf{R}$ exists. The constant function

$$\alpha^{-1} : [0,1]\to\mathbf{R} \text{ defined as } \alpha^{-1}(x) = \alpha^{-1}\ \forall\ x\in[0,1]$$

is a continuous function on [0, 1] and as such $\alpha^{-1}\in R$.

Since U is an ideal of R, so

$$\alpha\in U \text{ and } \alpha^{-1}\in R \Rightarrow \alpha\alpha^{-1}\in U \Rightarrow 1\in U$$

$$\Rightarrow\qquad 1\,.\,f\in U\ \forall\ f\in R \Rightarrow f\in U\ \forall\ f\in R \Rightarrow R = U.$$

Hence M is a maximal ideal of R.

Example 2.6.7. *Let R be the ring of all real-valued continuous functions on the closed unit interval. Show that*

(*i*) $M_1 = \{f\in R : f(\frac{1}{5}) = 0\}$ [D.U., 1995]

(*ii*) $M_2 = \{f\in R : f(\frac{2}{3}) = 0\}$ [D.U., 1992]

are maximal ideals of R.

Hint. Similar to Example 2.6.6.

Example 2.6.8. *If γ is a real number such that $0 \le \gamma \le 1$, show that*

$$M_\gamma = \{f \in R : f(\gamma) = 0\}$$

is a maximal ideal of R, where R is the ring of all real-valued continuous functions on the closed unit interval.

Theorem 2.6.1. *If R is a commutative ring with unity, then an ideal M of R is maximal if and only if R/M is a field.* [D.U., 1996]

Proof. *Condition is necessary*

Let M be a maximal ideal of R. Since R is a commutative ring with unity 1, so R/M is also a commutative ring with unity $1 + M$. Thus R/M becomes a field, if we show that each non-zero element of R/M has its multiplicative inverse in R/M. Let $a + M$ be any non-zero element of R/M

$\Rightarrow a + M \in R/M$ and $a + M \neq M$ *i.e.*, $a \notin M$.

Let $S = \{m + ax : m \in M, x \in R;\ a \text{ is fixed}\}$.

We proceed to show that S is an ideal of R. Obviously, S is non-empty, since $0 + a.0 = 0 \in S$.

Let $\alpha, \beta \in S$. Then $\alpha = m_1 + ax_1$, $\beta = m_2 + ax_2$, where $m_1, m_2 \in M$ and $x_1, x_2 \in R$. We have

$$\alpha - \beta = (m_1 + ax_1) - (m_2 + ax_2) = (m_1 - m_2) + a(x_1 - x_2).$$

Since M is an ideal of R, so $m_1, m_2 \in M \Rightarrow m_1 - m_2 \in M$.

Further $x_1, x_2 \in R \Rightarrow x_1 - x_2 \in R$.

Consequently, $\alpha - \beta \in S$. For any $r \in r$ and $\alpha \in S$, we see that

$$\alpha r = (m_1 + ax_1) r = m_1 r + a(x_1 r),$$

where $x_1 r \in R$ and $m_1 r \in M$ (since M is an ideal of R)

$\therefore$ $\alpha r \in S$ and so $r\alpha = \alpha r \in S$, as R is commutative.

Thus S is an ideal of R such that $M \subseteq S \subseteq R$

[Notice that for any $m \in M$, $m = m + a \,.\, 0 \in S$]

Since M is a maximal ideal of R, either $M = S$ or $S = R$.

If $M = S$, then $a = 0 + 1 \,.\, a \Rightarrow a \in S \Rightarrow a \in M$, which is a contradiction. Thus we have $S = R$. It follows that

$$1 \in R \Rightarrow 1 \in S \Rightarrow 1 = m_0 + ab, \text{ for some } m_0 \in M \text{ and } b \in R.$$

$\therefore$ $1 + M = (m_0 + ab) + M = ab + m_0 + M = ab + M,$

since $m_0 \in M \Rightarrow m_0 + M = M$

$\Rightarrow$ $1 + M = (a + M)(b + M) = (b + M)(a + M),$

since R/M is commutative

$\Rightarrow (a + M)^{-1} = b + M \in R/M.$

Hence R/M is a field.

Condition is sufficient

Let M be an ideal of R such that R/M is a field. We shall prove that M is a maximal ideal of R. Let U be any ideal of R such that $M \subset U \subset R, M \neq U$. We shall prove that $U = R$. Since $M \subset U$ and $M \neq U$, there exists some $p \in U$ such that $p \notin M$ *i.e.*, $p + M \neq M$ (since $p + M = M \Rightarrow p \in M$). Since R/M is a field and $p + M \neq M \in R/M$, $(p + M)^{-1}$ exists.

Let $(p + M)^{-1} = q + M \in R/M$. Then

$$1 + M = (p + M)(q + M) = pq + M$$

$$\Rightarrow \quad 1 - pq \in M \subset U \Rightarrow 1 - pq \in U.$$

Since U is an ideal of R, so $p \in U$ and $q \in R \Rightarrow pq \in U$. Also $1 - pq \in U$. Consequently,

$$1 - pq + pq \in U \in U \Rightarrow 1 \in U.$$

For each $x \in R$ and $1 \in U \Rightarrow x \,.\, 1 \in U \Rightarrow x \in U \; \forall \; x \in R$

$\Rightarrow \quad R \subset U$ and $U \subset R \Rightarrow U = R$.

Hence M is a maximal ideal of R.

Corollary. *For each prime number p, $\mathbf{Z}/(p)$ is a field.*

Proof. We know $\mathbf{Z}$ (all integers) is a commutative ring with unity and for any prime number p, the set

$$(p) = \{px : x \in \mathbf{Z}\} \text{ is a maximal ideal of } \mathbf{Z}.$$

Hence by the above theorem, $\mathbf{Z}/(p)$ is a field.

Remarks :

1. It is interesting to note that

$$\frac{\mathbf{Z}}{(2)} = \{(2), 1 + (2)\},$$

$$\frac{\mathbf{Z}}{(3)} = \{(3), 1 + (3), 2 + (3)\},$$

$$\frac{\mathbf{Z}}{(5)} = \{(5), 1 + (5), 2 + (5), 3 + (5), 4 + (5)\} \text{ etc.}$$

are all finite fields.

2. From the *sufficient condition* of Theorem 2.6.1., we notice that

If R/M is a field (R **not** necessarily a commutative ring with unity), *then M is a maximal ideal of R.*

Theorem 2.6.2. *Let R be a ring with unity. Prove that an ideal M of R is maximal if and only if $M + (a) = R \; \forall \; a \notin M$.* [D.U., 1998]

Proof. We know $(a) = \{ax : x \in R\} = aR, a \in R$.

Condition is necessary

Let M be a maximal ideal of R and let $a \notin M$.

Since the sum of two ideals of R is an ideal of R, $M+(a)$ is an ideal of R such that

$$M \subset M+(a) \subset R \quad \ldots(1)$$

Clearly, $$M \neq M+(a), \quad \ldots(2)$$

for if $M = M+(a)$, then

$$a = 0 + a \,.\, 1 \Rightarrow a \in M+(a) \Rightarrow a \in M,$$

which is a contradiction

Since M is a maximal ideal of R, so by (1) and (2),

$$M+(a) = R.$$

Condition is sufficient

Let M be an ideal of R such that $M+(a) = R \ \forall\ a \notin M$. We shall prove that M is a maximal ideal of R. Let U be any ideal of R such that $M \subset U \subset R, M \neq U$. We shall prove that $U = R$.

Since $M \subset U$ and $M \neq U$, there exists some $a \in U$ such that $a \notin M$.

Since $1 \in R = M+(a)$, we can write

$1 = m + ax$, for some $m \in M$ and $x \in R$.

Since U is an ideal of R, so $a \in U$ and $x \in R \Rightarrow ax \in U$

Further $m \in M \subset U \Rightarrow m \in U$.

Thus $m + ax \in U \Rightarrow 1 \in U \Rightarrow 1 \,.\, r \in U \ \forall\ r \in R$, since U is an ideal of $R \Rightarrow r \in U \ \forall\ r \in R \Rightarrow R = U$.

Hence M is a maximal ideal of R.

EXAMPLES

Example 2.6.9. *Show that in the ring*

$$R = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : a, b \in \mathbf{Q} \right\},$$

the set

$$M = \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} : b \in \mathbf{Q} \right\},$$

is a maximal ideal of R.

Solution. It is easy to verify that M is an ideal of R and further

$$S = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \in \mathbf{Q} \right\}$$

is a subfield of R in which $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ is the unity and the multiplicative inverse of $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$ is $\begin{pmatrix} a^{-1} & 0 \\ 0 & 0 \end{pmatrix}$, for each $a \neq 0$.

The mapping $\theta : R \to S$ defined as

$$\theta\left\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}\right\} = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$$

is an onto homomorphism (verify !) and

$$Ker\,\theta = \left\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \in R : \theta\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\right\}$$

$$= \left\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : \theta\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} i.e., a = 0\right\}$$

$$= \left\{\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}, b \in \mathbf{Q}\right\} = M.$$

By Fundamental theorem of homomorphism of rings, $\frac{R}{M} \approx S$ or $S \approx \frac{R}{M}$. Since S is a field, so $\frac{R}{M}$ is a field.

Hence M is a maximal ideal of R. [Theorem 2.6.1.]

Example 2.6.10. *Give an example of a non-commutative ring R and an ideal I or R such that R/I is a field.*

Solution. Let $R = \left\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}; a, b \in \mathbf{Q}\right\}$, $I = \left\{\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} : b \in \mathbf{Q}\right\}$.

By Example 2.6.9, I is an ideal of R, which is a non-commutative ring and $\frac{R}{I}$ is field.

Example 2.6.11. *If f is a homomorphism from a ring R onto a field F, prove that Ker f is a maximal ideal of R.*

Solution. Since $f : R \to F$ is an onto homomorphism, so by Fundamental theorem of homomorphism,

$$\frac{R}{Ker f} \approx F \quad \text{or} \quad F \approx \frac{R}{Ker f}.$$

Since isomorphic image of a field is a field, therefore

$\frac{R}{Ker f}$ is a field, where $Ker f$ is an ideal of R.

Hence $Ker f$ is a maximal ideal of R.

[See Remark 2 of Theorem 2.6.1.]

Example 2.6.12. *Let $f : R \to R'$ be an onto ring homomorphism. State the theorem that establishes a correspondence between the ideals of R' and the ideals of R.*

Use this theorem to find all the ideals of $\mathbf{Z}/12\,\mathbf{Z}$. Identify the maximal ones and establish the maximality of any one them. [D.U., 1998]

Solution. The statement of the theorem is as follows :

If $f : R \to R'$ is an onto homomorphism with kernel U, then R' is isomorphic to R/U. Further there is a one-to-one correspondence between the set of ideals of R' and the set of ideals of R which contain U.

We see that $U = 12\mathbf{Z} = \{\ldots, -36, -24, -12, 0, 12, 24, 36, \ldots\}$.

The mapping $f : \mathbf{Z} \to \mathbf{Z}/U$ defined by $f(n) = n + U \; \forall \; n \in \mathbf{Z}$ is an onto homomorphism. By the above correspondence theorem, there is a one-to-one correspondence between the ideals of $\mathbf{Z}/U$ and the ideals of $\mathbf{Z}$ which contain U. The only ideals of $\mathbf{Z}$ which contain U are $\mathbf{Z}$, and $12\mathbf{Z}$ and

$$2\mathbf{Z} = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$$
$$3\mathbf{Z} = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$$
$$4\mathbf{Z} = \{\ldots, -8, -4, 0, 4, 8, \ldots\}$$
$$6\mathbf{Z} = \{\ldots, -12, -6, 0, 6, 12, \ldots\}.$$

Hence all the ideals of $\mathbf{Z}/U$ are $\mathbf{Z}/U = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \bar{11}\}$, $U/U = \{\bar{0} = U\}$, $2\mathbf{Z}/U = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \bar{10}\}$, $3\mathbf{Z}/U = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}\}$, $4\mathbf{Z}/U = \{\bar{0}, \bar{4}, \bar{8}\}$, $6\mathbf{Z}/U = \{\bar{0}, \bar{6}\}$ (Here $\bar{n} = n + U$).

Out of these, the maximal ideals are $2\mathbf{Z}/U$ and $3\mathbf{Z}/U$ *i.e.*, $2\mathbf{Z}/12\mathbf{Z}$ and $3\mathbf{Z}/12\mathbf{Z}$, since, for example, there does not exist any proper ideal between $3\mathbf{Z}/12\mathbf{Z}$ and $\mathbf{Z}/12\mathbf{Z}$.

Example 2.6.13. *Is the ideal $M = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}\}$ a maximal ideal of $\mathbf{Z}/(12)$, the ring of integers modulo 12 ? Justify your answer.* [D.U., 199

Solution. As shown in the above example, all the proper ideals of $\mathbf{Z}/(12)$ are

$$\{\bar{0}\}, \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \bar{10}\}, \{\bar{0}, \bar{3}, \bar{6}, \bar{9}\}, \{\bar{0}, \bar{4}, \bar{8}\}, \{\bar{0}, \bar{6}\}, \{\bar{0}, \bar{1}, \bar{2}, \ldots, \bar{11}\}.$$

Since there does not exist any proper ideal between $M = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}\}$ and $\mathbf{Z}/(12) = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \bar{11}\}$, M is a maximal ideal of $\mathbf{Z}/(12)$. Notice that $\{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \bar{10}\}$ is also a maximal ideal of $\mathbf{Z}/(12)$.

However, $\{\bar{0}\}$, $\{\bar{0}, \bar{4}, \bar{8}\}$, $\{\bar{0}, \bar{6}\}$ are not maximal ideals of $\mathbf{Z}/(12)$, since for example, $\{\bar{0}, \bar{6}\} \subset \{\bar{0}, \bar{3}, \bar{6}, \bar{9}\} \subset \mathbf{Z}/(12)$.

Example 2.6.14. *Let M be a proper ideal in a Boolean ring R with unity. Prove that (i) R/M is a Boolean ring and (ii) $R/M \approx \mathbf{Z}/(2)$ if and only if M is a maximal ideal of R.*

Solution. (*i*) For any $x + M \in R/M$, we have

$$(x + M)^2 = (x + M)(x + M) = x^2 + M = x + M, \qquad \ldots(1)$$

since $x^2 = x \; \forall \; x \in R$. ($\because$ R is a Boolean ring)

Hence R/M is a Boolean ring.

(*ii*) Let $R/M \approx \mathbf{Z}/(2)$. Since 2 is prime, $\mathbf{Z}/(2)$ is a field [See corollary of Theorem 2.6.1.] and so R/M is a field. Hence M is a maximal ideal of R [Theorem 2.6.1.]

Conversely, let M be a maximal ideal of R.

Then R/M is a field [Theorem 2.6.1.]. From (1), we have

$$(x+M)^2 = (x+M)(1+M) \quad \forall \quad x \in R \qquad (\because 1 \in R)$$

$$\Rightarrow (x+M)[(x+M)-(1+M)] = \bar{0},\ \bar{0} = M \in R/M$$

$$\Rightarrow \quad x+M = \bar{0} \text{ or } (x+M)-(1+M) = \bar{0},$$

since R/M is a field implies R/M is an integral domain.

$$\therefore \quad x+M = M \quad \text{or} \quad x+M = 1+M, \ \forall \ x \in R.$$

This shows that R/M has only two elements *viz.* M and $1+M$. The mapping $f: R/M \to \mathbf{R}/(2)$ defined by $f(M) = (2)$ and $f(1+M) = 1+(2)$ is homomorphism, 1-1 and onto. Hence $\frac{R}{M} \approx \frac{Z}{(2)}$.

Prime Ideal

Definition. *An ideal P of a ring R is called a* **prime ideal,** *if for any $a \in R, b \in R$;*

$$ab \in P \Rightarrow \textit{either } a \in P \textit{ or } b \in P.$$

Illustrations

1. *The ideal $\{0\}$ in $\mathbf{Z}$ (ring of integers) is a prime ideal.*
   Let $a, b \in \mathbf{Z}$ be such that $ab \in \{0\} \Rightarrow ab = 0 \Rightarrow a = 0$ or $b = 0$
   $\Rightarrow \quad a \in \{0\}$ or $b \in \{0\}$.
2. *For any prime number p, $(p) = \{px : x \in \mathbf{Z}\}$ is a prime ideal of $\mathbf{Z}$.*
   Let $a, b \in \mathbf{Z}$ be such that $ab \in (p) \Rightarrow ab = px$ for some $x \in \mathbf{Z}$
   $\Rightarrow p \mid ab \Rightarrow p \mid a$ or $p \mid b$ (since is prime) $\Rightarrow a = py$ or $b = pz$,
   for some $y, z \in \mathbf{Z} \Rightarrow a \in (p)$ or $b \in (p)$.
   In particular, the ideals
   $$(2) = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$$
   $$(3) = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$$
   $$(5) = \{\ldots, -10, -5, 0, 5, 10, \ldots\} \text{ etc.}$$
   are prime ideals of $\mathbf{Z}$.
3. The ideal $(4) = \{.., -12, -8, -4, 0, 4, 8, 12, \ldots\}$ is **not** a prime ideal of $\mathbf{Z}$, since $2.6 = 12 \in (4)$, but $2 \notin (4)$ and $6 \notin (4)$.

Theorem 2.6.3. *Let R be a commutative ring. Prove that an ideal P of R is a prime ideal if and only if R/P is an integral domain.* [D.U., 2000, 1997]

Proof. *Condition is necessary*

Let P be a prime ideal of R. We shall prove that $\frac{R}{P} = \{a+P : a \in R\}$ is an integral domain. Since R is a commutative ring, so is R/P. In order to show that R/P is an integral domain, we need to prove that R/P is without zero divisors. Let $X = a+P$, $Y = b+P \in R/P$ be such that

$$XY = \bar{0} \text{ (zero of } R/P) \textit{ i.e.,} (a+P)(b+P) = P$$

$$\Rightarrow \quad ab+P = P \Rightarrow ab \in P \Rightarrow a \in P \text{ or } b \in P,$$

since P is a prime ideal of R.

$a \in P$ or $b \in P \Rightarrow a + P = P$ or $b + P = P$

Now $\Rightarrow \bar{1} = \bar{0}$ or $\bar{1} = \bar{0}$ $(\bar{0} = P \in R/P)$ $\Rightarrow$ R/P has no zero divi

$\Rightarrow$ Hence R/P is an integral domain.

Condition is sufficient

Let R be an integral domain. We have to show that P is a p

ideal of R. Let $a, b \in R$ be such that $ab \in P$. Then

$$ab + P = P \Rightarrow (a + P)(b + P) = \bar{0}\ (\bar{0} = P \in R/P)$$

$\Rightarrow a + P = \bar{0}$ or $b + P = \bar{0}$, since R/P has no zero divisors.

Consequently, $a + P = P$ or $b + P = P \Rightarrow a \in P$ or $b \in P$.

Hence P is a prime ideal of R.

Corollary 1. *If R be a commutative ring with unity, then every maxi*

ideal of R is a prime ideal of R. [D.U., 1

Proof. Let M be a maximal ideal of R. By Theorem 2.6.1, $\frac{R}{M}$ is a

$\Rightarrow \frac{R}{M}$ is an integral domain [Theorem 1.5.4]

$\Rightarrow M$ is a prime ideal of R.

Remark. *The converse of the above corollary may not be true i.e.*

prime ideal of R may not be a maximal ideal of R.

For example, (0) is a prime ideal of $\mathbf{Z}$. But (0) is not a maximal i

of $\mathbf{Z}$, since $(0) \subset (2) \subset \mathbf{Z}$, where $(2) = \{..., -4, -2, 0, 2, 4, ...\}$

The converse is true, if R happens to be a finite commutative ri

proved below :

Corollary 2. *If R is a finite commutative ring with unity, then e*

prime ideal of R is a maximal ideal of R. [D.U., 19

Proof. Let P be a prime ideal of R. Then R/P is an integral dom

[Theorem 2.6.3]. Since R is finite, R/P is a finite integral domain and

R/P is a field [Theorem 1.5.5]. Hence P is a maximal ideal of

[Theorem 2.6.1].

Ex. *If R is a finite commutative ring with unity, deduce that an ide*

is maximal if and only if it is a prime ideal in R. [D.U., 19

Hint. See Cor. 2 for the sufficient condition and Cor. 1 for t

necessary condition (although we do not need that R is finite in this par

Theorem 2.6.4. *Let R be a commutative ring and P an ideal of*

Then P is a prime ideal of R if and only if for any two ideals A and B

R, the following condition is satisfied :

$$AB \subseteq P \Rightarrow A \subseteq P \text{ or } B \subseteq P.$$

Proof. *Condition is necessary*

Let P be a prime ideal of R. Let A, B be and two ideals of R such t

Now $a \in P$ or $b \in P \Rightarrow a+P=P$ or $b+P=P$

$\Rightarrow \quad X=\bar{0}$ or $Y=\bar{0}\ (\bar{0}=P \in R/P) \Rightarrow R/P$ has no zero divisors.

Hence R/P is an integral domain.

Condition is sufficient

Let R/P be an integral domain. We have to show that P is a prime ideal of R. Let $a, b \in R$ be such that $ab \in P$. Then

$$ab+P=P \Rightarrow (a+P)(b+P)=\bar{0}\ (\bar{0}=P \in R/P)$$

$\Rightarrow a+P=\bar{0}$ or $b+P=\bar{0}$, since R/P has no zero divisiors.

Consequently, $a+P=P$ or $b+P=P \Rightarrow a \in P$ or $b \in P$.

Hence P is a prime ideal of R.

Corollary 1. *If R be a commutative ring with unity, then every maximal ideal of R is a prime ideal of R.* [D.U., 1995]

Proof. Let M be a maximal ideal of R. By Theorem 2.6.1, $\frac{R}{M}$ is a field.

$\Rightarrow \frac{R}{M}$ is an integral domain [Theorem 1.5.4]

$\Rightarrow M$ is a prime ideal of R.

Remark. *The converse of the above corollary may not be true i.e., a prime ideal of R may not be a maximal ideal of R.*

For example, (0) is a prime ideal of $\mathbf{Z}$. But (0) is not a maximal ideal of $\mathbf{Z}$, since $(0) \subset (2) \subset \mathbf{Z}$, where $(2) = \{..., -4, -2, 0, 2, 4, ...\}$

The converse is true, if R happens to be a finite commutative ring as proved below :

Corollary 2. *If R is a finite commutative ring with unity, then every prime ideal of R is a maximal ideal of R.* [D.U., 1996]

Proof. Let P be a prime ideal of R. Then R/P is an integral domain [Theorem 2.6.3]. Since R is finite, R/P is a finite integral domain and so R/P is a field [Theorem 1.5.5]. Hence P is a maximal ideal of R [Theorem 2.6.1].

Ex. *If R is a finite commutative ring with unity, deduce that an ideal is maximal if and only if it is a prime ideal in R.* [D.U., 1997]

Hint. See Cor. 2 for the sufficient condition and Cor. 1 for the necessary condition (although we do not need that R is finite in this part).

Theorem 2.6.4. *Let R be a commutative ring and P an ideal of R. Then P is a prime ideal of R if and only if for any two ideals A and B of R, the following condition is satisfied :*

$$AB \subseteq P \Rightarrow A \subseteq P \text{ or } B \subseteq P.$$

Proof. *Condition is necessary*

Let P be a prime ideal of R. Let A, B be and two ideals of R such that

$$AB \subseteq P.$$

We shall prove that either $A \subseteq P$ or $B \subseteq P$.

Let $A \not\subseteq P$. Then there exists some element $a \in A$ such that $a \notin P$.

Consequently,

$$ab \in AB \quad \forall \quad b \in B \quad \Rightarrow \quad ab \in P, \text{ by (1)}$$

$\Rightarrow a \in P$ or $b \in P$, since P is a prime ideal of R

$\Rightarrow b \in P \; \forall \; b \in B$, since $a \notin P$

$\Rightarrow B \subseteq P$.

Similarly, we can show if $B \not\subseteq P$, then $A \subseteq P$.

Condition is sufficient

Suppose $AB \subseteq P \Rightarrow A \subseteq P$ or $B \subseteq P$, ...(1)

where A and B are any two ideals of R. We shall prove that P is a prime ideal of R. Let $ab \in P$; where $a, b \in R$. Let A and B be the ideals generated by a and b, respectively. Then A and B are the smallest ideals of R containing a and b, respectively *i.e.*,

$$A = (a) = \{ar : r \in R\} \text{ and } B = (b) = \{br : r \in R\}. \quad ...(2)$$

Now A and B being two ideals of R imply that AB is an ideal of R.

Let x be any element of AB. Then

$$x = a_1 b_1 + a_2 b_2 + \ldots + a_n b_n \text{ ; where } a_i \in A, b_i \in B, 1 \le i \le n \quad ...(3)$$

Using (2), $a_i \in A \Rightarrow a_i = ar_i$; $r_i \in R$, $1 \le i \le n$

and $b_i \in B \Rightarrow b_i = bs_i$; $s_i \in R$, $1 \le i \le n$.

Putting in (3), we get

$$x = (ar_1)(bs_1) + (ar_2)(bs_2) + \ldots + (ar_n)(bs_n)$$

$$= ab(r_1 s_1) + ab(r_2 s_2) + \ldots + ab(r_n s_n), \text{ since } R \text{ is commutative}$$

$$= ab(r_1 s_1 + r_2 s_2 + \ldots + r_n s_n)$$

$$= ab\, r^*, \text{ where } r^* = r_1 s_1 + \ldots + r_n s_n \in R.$$

Thus $x \in P$, since $ab \in P$, $r^* \in R$ and P is an ideal of R.

Now $x \in P \quad \forall \quad x \in AB \Rightarrow AB \subseteq P$

$\Rightarrow A \subseteq P$ or $B \subseteq P$, using (1)

$\Rightarrow a \in P$ or $b \in P$.

Hence P is a prime ideal of R.

EXAMPLES

Example 2.6.15. *Give an example of a finite commutative ring which has a maximal ideal which is not a prime ideal.* [D.U., 2000]

Solution. Consider the ring $R = \{0, 2, 4, 6\}$ under addition and multiplication modulo 8. Then R is a finite commutative ring *without* unity. Let $M = \{0, 4\}$. Then M is an ideal of R, which is not prime ($\because 2 \otimes_8 6 = 4 \in M$, but $2 \notin M$ and $6 \notin M$). It is easy to verify that all the ideals of R are (0), M and R. Since there does not exist any proper ideal between (0) and M, M is the maximal ideal of R.

Example 2.6.16. *Let P_1, P_2 be prime ideals of a ring R. Show that if $P_1 \cap P_2$ is a prime ideal of R, then either $P_1 \subseteq P_2$ or $P_2 \subseteq P_1$.* [D.U., 1999]

Solution. We know $P_1 P_2 \subseteq P_1 \cap P_2$. Since $P_1 \cap P_2$ is a prime ideal of R, so by the necessary condition of Theorem 2.6.4, either $P_1 \subseteq P_1 \cap P_2$ or $P_2 \subseteq P_1 \cap P_2$. Hence either $P_1 \subseteq P_2$ or $P_2 \subseteq P_1$.

Example 2.6.17. *Let R be a commutative ring. Let I be an ideal of R and P a prime ideal of I. Show that P is an ideal of R.*

Solution. Obviously, $a, b \in P \Rightarrow a - b \in P$.

Let $a \in P$ and $r \in R$ be arbitrary. We have to show that $ar \in P$. Since $P \subseteq I$, $a \in I$. Consequently, $ar \in I$, since I is an ideal of R

$\Rightarrow$ $(ar)\, r = ar^2 \in I$, since I is an ideal of R.

Now $a \in P$ and $ar^2 \in I \Rightarrow a(ar^2) \in P \Rightarrow a^2 r^2 \in P$, since P is an ideal of I. Using the commutativity of R, we see that

$$a^2 r^2 = (ar)\,(ar) \in P, \text{ where } ar \in I$$

$\Rightarrow$ $ar \in P$, since P is a prime ideal of I

Also $ra = ar \in P$. Hence P is an ideal of R.

Note. We have seen in Ex. 9 of section 1.9 of Chapter 1 :

If A and B are two ideals of a ring R such that A is an ideal of B and B is an ideal of R, then A need not be an ideal of R. In the above example, we have shown that if A is a prime ideal of B and B is an ideal of a commutative ring R, then A is an ideal of R.

Example 2.6.18. (*i*) *Show that the intersection of two prime ideals of a ring R may not be a prime ideal of R.*

(*ii*) *Show that the intersection of two maximal ideals of a ring R may not be a maximal ideal of R.*

Solution. Let $A = (2) = \{\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots\}$,

$B = (3) = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$.

Then A and B are two prime (maximal ideals) of $\mathbf{Z}$. We have

$$A \cap B = \{\ldots, -12, -6, 0, 6, 12, \ldots\}.$$

It follows that $A \cap B$ is not a prime ideal of $\mathbf{Z}$, since, for example, $3.8 = 24 \in A \cap B$, but $3 \notin A \cap B$ and $8 \notin A \cap B$.

Also $A \cap B$ is not a maximal ideal of $\mathbf{Z}$, since $A \cap B \subset A \subset \mathbf{Z}$.

Example 2.6.19. *Show that a commutative ring R is an integral domain iff $\{0\}$ is a prime ideal.*

Solution. Let R be an integral domain. Then $\{0\}$ is a prime ideal of R since $ab \in \{0\} \Rightarrow ab = 0 \Rightarrow a = 0$ or $b = 0 \Rightarrow a \in \{0\}$ or $b \in \{0\}$.

Conversely, let $\{0\}$ be a prime ideal of R. We shall prove that R is an integral domain *i.e.*, R has no zero divisors. Let $a, b \in R$ be such that $ab = 0$. Then $ab \in \{0\} \Rightarrow a \in \{0\}$ or $b \in \{0\}$, since $\{0\}$ is a prime ideal of R. So $a = 0$ or $b = 0$. Hence R is an integral domain.

Example 2.6.20. *Let R denote the ring of all real-valued continuous functions on the closed interval* [0, 1]. *Is* (0) *a prime ideal of R ? Justify.* [D.U.; 1992]

Solution. We know that R is a commutative ring with unity.

It may be remarked that R is *not* an integral domain as shown below :

Let $f(x) = \begin{cases} x, & \text{if } x \le 0 \\ 0, & \text{if } x > 0 \end{cases}$ and $g(x) = \begin{cases} 0, & \text{if } x \le 0 \\ x, & \text{if } x > 0. \end{cases}$

Then $f \in R$ and $g \in R$, where $f \neq 0$, and $g \neq 0$, but $fg = 0$.

Let, if possible, (0) be a prime ideal of R.

Let $f, g \in R$ be such that $fg = 0$. Then $fg \in (0)$ and so $f \in (0)$ or $g \in (0)$, since (0) is a prime ideal of R. Thus $f = 0$ or $g = 0$, which means that R is an integral domain, a contradiction Hence (0) is not a prime ideal of R.

Example 2.6.21. *In $\mathbf{Z}/(8)$, the ring of integers modulo* 8, *is the ideal generated by $\bar{2} = 2 + (8)$ a prime ideal ? Is it also maximal ?* [D.U., 1995]

Solution. Let $R = \mathbf{Z}/8 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}\}$.

Then R is a commutative ring with unity. The ideal $(\bar{2}) = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}\}$ is a maximal ideal of R, since there does not exist any proper ideal between $(\bar{2})$ and R. Since $(\bar{2})$ is a maximal ideal of R, a commutative ring with unity, $(\bar{2})$ is also a prime ideal of R.

[See Cor. 1 of Theorem 2.6.3]

Example 2.6.22. *Show that in a boolean ring R, every prime ideal $P \neq R$ is maximal.* [D.U., 1994, 93]

Solution. Let U be any ideal of R such that

$$P \subset U \subset R, \text{ where } P \neq U.$$

We shall prove that $U = R$.

Since $P \subset U$ and $P \neq U$, there exists some $x \in U$ such that $x \notin P$. Since R is a boolean ring, so $x^2 = x \Rightarrow x^2 r = xr \quad \forall \ r \in R$

$\Rightarrow \quad x(xr - r) = 0 \in P$, since P is an ideal of R.

Now $x(xr - r) \in P$

$\Rightarrow x \in P$ or $xr - r \in P$, since P is a prime ideal of R

$\Rightarrow xr - r \in P$, since $x \notin P$.

Let $xr - r = p$, where $p \in P$. Then $r = xr - p$.

Since U is an ideal of R, so $x \in U$ and $r \in R \Rightarrow xr \in U$.

Also $p \in P \subset U \Rightarrow p \in U \Rightarrow xr - p \in U$, since U is an ideal of R

$\Rightarrow \quad r \in U \; \forall \, r \in R \Rightarrow R \subseteq U \Rightarrow U = R$.

Hence P is a maximal ideal of R.

Example 2.6.23. *Let R be commutative ring with unit element in which every ideal is a prime ideal. Prove that R is a field.* [D.U., 1993]

Solution. Firstly, we show that R is an integral domain.

Let $a, b \in R$ be such that $ab = 0 \Rightarrow ab \in (0) \Rightarrow a \in (0)$ or $b \in (0)$, since (0) being an ideal of R is a prime ideal. Thus $a = 0$ or $b = 0$ and so R is an integral domain. Since R is a commutative ring with unit element $1 \in R$, R becomes a field if each non-zero element of R has its multiplicative inverse in R. Let $a \neq 0 \in R$ be arbitrary.

Let $\quad a^2R = \{a^2x : x \in R\}$.

We proceed to show that $a^2 R$ is an ideal of R.

Let $\alpha, \beta \in a^2 R$. Then $\alpha = a^2x$, $\beta = a^2y$; for some $x, y \in R$.

$\therefore \quad \alpha - \beta = a^2x - a^2y = a^2 (x - y) \in a^2 R$, since $x - y \in R$.

For any $r \in R$ and $\alpha \in a^2 R$, we see that

$$\alpha r = (a^2 x)\, r = a^2 (xr) \in a^2 R, \text{ since } xr \in R.$$

$\Rightarrow \quad r\alpha = \alpha r \in a^2 R$, since R is commutative.

Thus a^2R is an ideal of R and so by the given hypothesis, $a^2 R$ is a prim ideal of R. We have

$$1 \in R \Rightarrow a^2 . 1 \in a^2 R \Rightarrow a^2 \in a^2 R \Rightarrow a . a \in a^2 R$$
$$\Rightarrow a \in a^2 R, \text{ since } a^2R \text{ is a prime ideal of } R$$
$$\Rightarrow a = a^2 b, \text{ for some } b \in R$$
$$\Rightarrow a . 1 - a . ab = 0 \Rightarrow a (1 - ab) = 0$$
$$\Rightarrow 1 - ab = 0, \text{ since } a \neq 0 \text{ and } R \text{ in an integral doma}$$
$$\Rightarrow 1 = ab = ba, \text{ since } R \text{ is commutative}$$
$$\Rightarrow a^{-1} = b \in R.$$

Hence R is a field.

Example 2.6.24. *Let R be a commutative ring with unity and let M a maximal ideal of R such that $M^2 = \{0\}$. Show that if N is any other maxim ideal of R, then $N = M$.*

Solution. We have $\quad M^2 = \{ab : a \in M, b \in M\}$.

Since N is a maximal ideal of a commutative ring R with unity, R/N a field $\Rightarrow R/N$ is an integral domain $\Rightarrow N$ is a prime ideal of R.

[See Theorem 2.6

Let $m \in M$ be arbitrary. Then $m^2 = m \,.\, m \in M^2 = \{0\}$

$\Rightarrow m^2 = 0 \Rightarrow m^2 \in N$, since N is an ideal of R

$\Rightarrow m \,.\, m \in N \Rightarrow m \in N$, since N is a prime ideal of R

Thus $M \subseteq N \subseteq R$.

Since M is a maximal ideal of R, either $N = M$ or $N = R$.

But $N \neq R$, as N is a maximal ideal of R.

Hence $N = M$.

Example 2.6.25. *Let A and B be two prime ideals of a commutative ring R. Show that $x^2 \in A \cap B \Rightarrow x \in A \cap B$, for all $x \in R$.*

Solution. For any $x \in R$, $x^2 \in A \cap B \Rightarrow x^2 \in A$ and $x^2 \in B$.

Since A is a prime ideal of R, $x^2 = x \,.\, x \in A \Rightarrow x \in A$.

Similarly, $x^2 = x \,.\, x \in B \Rightarrow x \in B$. Hence $x \in A \cap B$.

Definition. *An ideal A of a commutative ring R is called a* **semi-prime ideal**, *if for each $a \in R$, $a^2 \in A \Rightarrow a \in A$.*

In the light of this definition, the above example may be restated as : *The intersection of two prime ideals of a commutative ring R is a semi-prime ideal of R.*

2.7 Divisibility in Rings, Prime and Irreducible Elements

Definition 1. *Let R be a commutative ring and $a \neq 0 \in R$, $b \in R$. We say that 'a divides b', denoted as $a \mid b$, if there exists some $c \in R$ such that $b = ac$.*

The following properties are easy to verify :

(*i*) $a \mid b$ and $b \mid c \Rightarrow a \mid c$.

(*ii*) $a \mid b$ and $a \mid c \Rightarrow a \mid (b + c)$ and $a \mid (b - c)$.

(*iii*) $a \mid b \Rightarrow a \mid bx$ for all $x \in r$.

In order to verify (*ii*), we proceed as follows :

$a \mid b \Rightarrow b = ax$, for some $x \in R$ and $a \mid c \Rightarrow c = ay$, for some $y \in R$.

$\therefore\ b \pm c = a(x \pm y)$, where $x \pm y \in R$.

Hence $a \mid (b \pm c)$.

Definition 2. (H.C.F.)

Let R be a commutative ring and a, b be any two non-zero elements of R. A non-zero element $d \in R$ is called a **highest common factor (h.c.f.)** *or a* **greatest common divisor (g.c.d.)** *of a and b, if*

(*i*) *$d \mid a$ and $d \mid b$.*

(*ii*) *Whenever $c \neq 0 \in R$ is such that $c \mid a$ and $c \mid b$, then $c \mid d$.*

We write $d = (a, b)$ to denote that d is a g.c.d. of a and b.

Definition 3. (L.C.M.)

Let R be a commutative ring and a, b be any two non-zero elements of R. A non-zero element $c \in R$ is called a **least common multiple (l.c.m.)** *of a and b, if*

(i) $a \mid c$ and $b \mid c$.

(ii) Whenever $x \neq 0 \in R$ is such that $a \mid x$ and $b \mid x$, then $c \mid x$.

We write $c = [a, b]$ to denote that c is a l.c.m. of a and b.

Remark. *Any two non-zero elements of a ring may or may not have a g.c.d. (l.c.m.). They may even have more than one g.c.d. (l.c.m.). See the following illustrations.*

Illustrations

1. In **Z**, 2 is a g.c.d. of 4 and 6. Also -2 is a g.c.d. of 4 and 6. Further 12 is an l.c.m. of 4 and 6. Similarly, -12 is also an l.c.m. of 4 and 6.
2. In the ring **E** of even integers, 4 and 6 do not have a g.c.d., Notice that $2 \in \mathbf{E}$ is **not** a g.c.d. of 4 and 6, since $2.2 = 4 \Rightarrow 2 \mid 2$ in **E**, but $2.3 = 6$

   $\Rightarrow 2 \nmid 6$. $(\because 3 \notin \mathbf{E})$

   Similarly, 4 and 6 do not have a l.c.m.

   Notice that $12 \in \mathbf{E}$ is **not** a l.c.m of 4 and 6, since $4 \nmid 12$ in **E** $(\because 12 = 4.3$ and $3 \notin \mathbf{E})$.

3. Consider the ring :

$$\mathbf{Z}/(12) = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9}, \overline{10}, \overline{11}\}.$$

We shall show that $\bar{2}$ is a g.c.d. of $\bar{6}$ and $\bar{8}$.

Since $\bar{6} = \bar{3} \,.\, \bar{2}$ and $\bar{8} = \bar{4} \,.\, \bar{2}$, so $\bar{2} \mid \bar{6}$ and $\bar{2} \mid \bar{8}$.

Let $\bar{x} \neq \bar{0} \in \mathbf{Z}/(12)$ be such that $\bar{x} \mid \bar{6}$ and $\bar{x} \mid \bar{8}$.

Then $\bar{x} \mid (\bar{8} - \bar{6})$ *i.e.*, $\bar{x} \mid \bar{2}$ and so $\bar{2}$ is a g.c.d. of $\bar{6}$ and $\bar{8}$.

Again $\bar{6} = \overline{10} \,.\, \bar{3}$ and $\bar{8} = \overline{10} \,.\, \bar{2} \Rightarrow \overline{10} \mid \bar{6}$ and $\overline{10} \mid \bar{8}$.

Let $\bar{x} \neq \bar{0} \in \mathbf{Z}/(12)$ be such that $\bar{x} \mid \bar{6}$ and $\bar{x} \mid \bar{8}$. Then

$$\bar{x} \mid (\bar{2} \,.\, \bar{8} - \bar{6}) \text{ } i.e., \bar{x} \mid \overline{10}.$$

Thus $\overline{10}$ is also a g.c.d of $\bar{6}$ and $\bar{8}$.

Now we show that $\bar{6}$ and $\bar{8}$ have no l.c.m.

Let $\bar{x}$ be an l.c.m. of $\bar{6}$ and $\bar{8}$. Then $\bar{6} \mid \bar{x}$ and $\bar{8} \mid \bar{x}$.

Now $\bar{6} \mid \bar{x} \Rightarrow \bar{x} = \bar{6} \,.\, \bar{y}$, for some $\bar{y} \in \mathbf{Z}/(12) \Rightarrow \bar{x} = \bar{0}$ or $\bar{6} \Rightarrow \bar{x} = \bar{6}$, since l.c.m. is never zero. It follows that $\bar{8} \mid \bar{6}$ and so $\bar{6} = \bar{8} \,.\, \bar{z}$, for some $\bar{z} \in \mathbf{Z}/(12)$. We see that $\bar{8} \,.\, \bar{x} = \bar{0}$ or $\bar{4}$ or $\bar{8}$ $\forall\, \bar{x} \in \mathbf{Z}/(12)$.

Consequently, $\bar{6} = \bar{8} \,.\, \bar{z}$ is impossible. Hence $\bar{6}$ and $\bar{8}$ have no l.c.m. in $\mathbf{Z}/(12)$.

Ex. 1. *In the ring* $\mathbf{Z}/(8) = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}\}$, *show that*

(i) $g.c.d.\ (\bar{4}, \bar{6}) = \bar{2}$ *and* $\bar{6}$.

(ii) $l.c.m.\ (\bar{4}, \bar{6}) = \bar{4}$.

(iii) $l.c.m.\ (\bar{3}, \bar{6}) = \bar{2}$ *and* $\bar{6}$.

Ex. 2. *Show that in* $\mathbf{Z}/(20)$, $g.c.d.\ (\bar{9}, \overline{18}) = \bar{9}$ *and* $l.c.m.\ (\bar{9}, \overline{18}) = \overline{18}$.

Definition 4. (Unit)

Let R be a commutative ring with unity. An element $0 \neq u \in R$ *is called a* **unit** *if and only if u divides* 1. *In other words,* $u \neq 0 \in R$ *is called a* **unit** *iff there exists some element* $c \in R$ *such that* $1 = uc = cu$ *i.e.,* $u \neq 0 \in R$ *is a* **unit** *iff* $u^{-1} \in R$.

Illustrations

1. ± 1 are the units in $\mathbf{Z}$ (all integers).
2. $\pm 1, \pm i$ are the units in $\mathbf{Z}[i] = \{m + ni : m, n \in \mathbf{Z}\}$. Here $i = \sqrt{-1}$.
   Notice that $(i)(-i) = 1, (-1)(-1) = 1$ etc.
3. The units in the ring $\mathbf{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$ modulo 8 are 1, 3, 5 and 7, since $1 \otimes_8 1 = 1, 3 \otimes_8 3 = 1, 5 \otimes_8 5 = 1, 7 \otimes_8 7 = 1$.

Definition 5. (Associates)

Let R be a commutative ring with unity. Two elements $a, b \in R$ *are called* **associates**, *if there exists a unit* $u \in R$ *such that* $b = ua$.

We write the associates a and b as $a \sim b$.

Remark. Since u is a unit in R, $u^{-1} \in R$. Thus $b = ua \Rightarrow a = u^{-1} b$, where u^{-1} is a unit in R. *It follows that if* $a, b \in R$ *are associates, then* $b = u_1 a$ *or* $a = u_2 b$, *for some units* u_1, u_2 *in R.*

Illustrations

1. 1 and $-i$ are associates in $\mathbf{Z}[i]$, since $1 = (-i)(i)$, i being a unit in $\mathbf{Z}[i]$.
2. $2 + 3i$ and $2i - 3$ are associates, since $2i - 3 = (2 + 3i)\, i$, i being a unit in $\mathbf{Z}[i]$.

Definition 6. (Irreducible Element)

Let R be a commutative ring with unity. A non-zero, non-unit element $p \in R$ *is called an* **irreducible element**, *if* $p = ab$ *implies that either a or b is a unit ;* $a, b \in R$.

Remark 1. *It may be observed that* $p \in R$ *is* **not** *irreducible, if there exists a pair of elements* $a, b \in R$ *such that* $p = ab$, *where a and b are both* **non-unit** *elements of R.*

Definition 7. (Prime Element)

Let R be a commutative ring with unity. A non-zero, non-unit element $p \in R$ *is called a* **prime element,** *if* $p \mid ab$ $(a, b \in R)$ *implies that either* $p \mid a$ *or* $p \mid b$.

Remark 2. *It may be observed that $p \in R$ is* **not** *prime, if there exists a pair of elements, $a, b \in R$ such that $p \mid ab$, but $p \nmid a$ and $p \nmid b$.*

Ramark 3. *Irreducible and prime elements in a commutative ring with unity are always non-zero and non-unit elements.*

Remark 4. *In the ring $\mathbf{Z}$ of integers, every prime number is both a prime element and irreducible element.*

EXAMPLES

Example 2.7.1. *In a commutative ring R with unit element, prove that the relation 'a is an associate of b' is an equivalence relation.*

Solution. Let $a, b, c \in R$.

(*i*) *Reflexive.* $a \sim a$, since $a = a.1$ and $1 \in R$ is a unit.

(*ii*) *Symmetric.* Let $a \sim b$. Then $b = ua$, where $u \in R$ is a unit

$\Rightarrow a = u^{-1} b$, where $u^{-1} \in R$ is also a unit

$\Rightarrow b \sim a$.

(*iii*) *Transitive.* Let $a \sim b$ and $b \sim c$. Then $b = u_1 a$ and $c = u_2 b$, for some units u_1 and u_2 in R. It follows that $c = u_2 (u_1 a) = (u_2 u_1) a$. ...(1)

We have $u_1 u_1^{-1} = 1$ and $u_2 u_2^{-1} = 1 \Rightarrow u_2 u_2^{-1} (u_1 u_1^{-1}) = 1$

$\Rightarrow (u_2 u_1) (u_1^{-1} u_2^{-1}) = 1$, since R is commutative

$\Rightarrow (u_2 u_1) (u_2 u_1)^{-1} = 1 \Rightarrow u_2 u_1 \in R$ is a unit and so by (1), $a \sim c$. Hence '$a \sim b$' is an equivalence relation.

Example 2.7.2. *Prove that if an ideal U of a ring R contains a unit of R, then $U = R$.*

Solution. Let u be a unit of R such that $u \in U$.

We have $uu^{-1} = 1$. Since U is an ideal of R, so $u \in U$ and $u^{-1} \in R \Rightarrow uu^{-1} \in U \Rightarrow 1 \in U$.

$\Rightarrow 1 . r \in U \; \forall \; r \in R \Rightarrow r \in U \quad \forall \quad r \in R \Rightarrow U = R$.

Example 2.7.3. *Prove that the units in a commutative ring R with a unit element form an abelian group.*

Solution. Let G be the set of all units of R. Then G is non-empty, since $1 \in R$ is a unit and so $1 \in G$. Further G is closed, since $u_1 \in G$ and $u_2 \in G \Rightarrow u_1$ and u_2 are units in $R \Rightarrow u_1 u_2$ is a unit in $R \Rightarrow u_1 u_2 \in G$.

[See Example 2.7.1]

Obviously, $1 \in G$ is the identity of G and for each $u \in G$, $uu^{-1} = u^{-1} u = 1 \Rightarrow u^{-1} \in G$. Since R is commutative, so G is commutative. Hence G is an abelian group.

Example 2.7.4. *Let R be an integral domain with unity and a, b be any two non-zero elements of R. Show that a and b are associates iff $a \mid b$ and $b \mid a$.*

Solution. Let $a \sim b$. Then $b = au$, for some unit u in R. It follows that $a = bu^{-1}$, where $u^{-1} \in R$ is a unit.

Now $b = au \Rightarrow a \mid b$ and $a = bu^{-1} \Rightarrow b \mid a$.

Conversely, let $a \mid b$ and $b \mid a$. Then $b = ax$ and $a = by$, for some $x, y \in R$. We have $a = (ax)\, y$ or $a \,.\, 1 = a\,(xy)$. This implies $1 = xy$, since $a \neq 0$ and R is an integral domain. It follows that $x \mid 1$ *i.e.*, x is a unit in R. Hence $b = ax \Rightarrow a$ and b are associates.

Example 2.7.5. *In the ring* $\mathbf{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$, *show that* $\bar{2}$ *is a prime element but not irreducible.*

Solution. The only unit in $\mathbf{Z}_6$ is $\bar{1}$. Thus $\bar{2} \in \mathbf{Z}_8$ is a non-zero and non-unit element. Let $\bar{2} \mid \bar{a}\,\bar{b}$, where $\bar{a}, \bar{b} \in \mathbf{Z}_6$. Then $ab - 2$ is divisible by 6 and so $ab - 2 = 6x$, for some $x \in \mathbf{Z}$. We have $ab = 2\,(1 + 3x) \Rightarrow 2 \mid ab \Rightarrow 2 \mid a$ or $2 \mid b \Rightarrow \bar{2} \mid \bar{a}$ or $\bar{2} \mid \bar{b}$.

Hence $\bar{2}$ is a prime element of $\mathbf{Z}_6$.

We have $\bar{2} = \bar{2} \otimes_6 \bar{4}$, where neither $\bar{2}$ nor $\bar{4}$ is a unit.

Hence $\bar{2}$ is not an irreducible element of $\mathbf{Z}_6$.

Example 2.7.6. *Prove that in* $\mathbf{Z}_8$, $\bar{2}$ *is a prime element but not irreducible.*

Hint. Similar to Example 2.7.5.

Example 2.7.7. *Show that* $1 + i$ *is an irreducible element in* $\mathbf{Z}[i]$. [D.U., 1999]

Solution. Clearly, $1 + i$ is a non-zero and non-unit element of $\mathbf{Z}[i]$. Notice that the units in $\mathbf{Z}[i]$ are $\pm 1, \pm i$.

Let $(1 + i) = (a + bi)\,(c + di)$, where $a + bi, c + di \in \mathbf{Z}[i]$.

Taking conjugates on both sides, we get

$$(1 - i) = (a - bi)\,(c - di).$$

On multiplying the respective sides of the above equations, we get

$$2 = (a^2 + b^2)\,(c^2 + d^2) \quad (\because\ i^2 = -1).$$

The above equation yields the following cases :

Case I. $a^2 + b^2 = 1$ and $c^2 + d^2 = 2$.

Case II. $a^2 + b^2 = 2$ and $c^2 + d^2 = 1$.

In case I, $a^2 + b^2 = 1 \Rightarrow (a + bi)\,(a - bi) = 1 \Rightarrow a + bi$ is a unit.

In case II, $c^2 + d^2 = 1 \Rightarrow c + di$ is a unit.

Hence $1 + i$ is an irreducible element of $\mathbf{Z}[i]$.

Example 2.7.8. *Show that* $1-i$ *is an irreducible element of* $\mathbf{Z}[i]$.

Hint. Proceed like Example 2.7.7.

Example 2.7.9. *Show that* 3 *is not a prime element of* $\mathbf{Z}[\sqrt{-5}]$.

Solution. We know

$\mathbf{Z}[\sqrt{-5}] = \{a + b\sqrt{5}\, i : a, b \text{ are integers and } i = \sqrt{-1}\}$ is an integral domain with unity. We see that $2+\sqrt{5}\, i$ and $2-\sqrt{5}\, i \in \mathbf{Z}[\sqrt{-5}]$ and

$$(2+\sqrt{5}\, i)(2-\sqrt{5}\, i) = 9.$$

Obviously, 3 divides $(2+\sqrt{5}\, i)(2-\sqrt{5}i) = 9$, but 3 does not divide $2+\sqrt{5}\, i$ and $2-\sqrt{5}\, i$, for if 3 divides $2+\sqrt{5}\, i$, then $2+\sqrt{5}\, i = 3(a+b\sqrt{5}\, i)$, for some $a, b \in \mathbf{Z}$. Consequently, $3a = 2$ $(a \in \mathbf{Z})$, which is impossible. Similarly, 3 does not divide $2-\sqrt{5}\, i$. Hence 3 is not prime in $\mathbf{Z}[\sqrt{-5}]$.

Example 2.7.10. *Show that* $\sqrt{-5}$ *is a prime element of* $\mathbf{Z}[\sqrt{-5}]$.

Solution. Obviously, $\sqrt{-5} \neq 0$. Let, if possible, $\sqrt{-5}$ be a unit element of $\mathbf{Z}[\sqrt{-5}]$. Then $\sqrt{-5}$ divides 1 and so $1 = \sqrt{-5}\,(a+b\sqrt{-5})$, for some $a, b \in \mathbf{Z} \Rightarrow 1 = -5b$, which is impossible in $\mathbf{Z}$. Thus $\sqrt{-5}$ is not a unit. Suppose that $\sqrt{-5}$ divides $(a+b\sqrt{-5})(c+d\sqrt{-5})$; $a, b, c, d \in \mathbf{Z}$.

Then $(a+b\sqrt{-5})(c+d\sqrt{-5}) = \sqrt{-5}\,(x+y\sqrt{-5})$, for some $x, y \in \mathbf{Z}$.

Comparing the real parts on both the sides, we get

$$-5y = ac - 5bd \Rightarrow 5(bd-y) = ac$$

$$\Rightarrow 5 \mid ac \Rightarrow 5 \mid a \text{ or } 5 \mid c, \text{ since 5 is prime in } \mathbf{Z}.$$

If $5 \mid a$, then $-5 \mid a \Rightarrow (\sqrt{-5})(\sqrt{-5}) \mid a \Rightarrow \sqrt{-5} \mid a$.

Also $\sqrt{-5} \mid b\sqrt{-5}$.

$\therefore$ $\sqrt{-5} \mid (a+b\sqrt{-5})$.

Similarly, if $5 \mid c$, then $\sqrt{-5} \mid (c+d\sqrt{-5})$.

Hence $\sqrt{-5}$ is a prime element of $\mathbf{Z}[\sqrt{-5}]$.

Example 2.7.11. *Show that* $\sqrt{-3}$ *is a prime element of* $\mathbf{Z}[\sqrt{-3}]$.

Please try yourself.

Example 2.7.12. *Show that* 3 *is an irreducible element of* $\mathbf{Z}[\sqrt{-5}]$.

Solution. Let $3 = (a+b\sqrt{5}\, i)(c+d\sqrt{5}\, i)$; $a, b, c\, d \in \mathbf{Z}$.

Taking conjugates on both the sides, we get

$$3 = (a-b\sqrt{5}\, i)(c-d\sqrt{5}\, i).$$

On multiplying the respective sides of the above equations, we get

$$9 = (a^2+5b^2)(c^2+5d^2).$$

Both the sides of the above equation are positive integers.

Consequently, we have the following cases :

Case I. $a^2+5b^2 = 1$ and $c^2+5d^2 = 9$.

Case II. $a^2+5b^2 = 9$ and $c^2+5d^2 = 1$.

Case III. $a^2+5b^2 = 3$ and $c^2+5d^2 = 3$.

It is clear that case III is not possible in $\mathbf{Z}$. Case I is possible when $a = \pm 1, b = 0 \Rightarrow a+b\sqrt{5}\, i = \pm 1$, which are units in $\mathbf{Z}[\sqrt{-5}]$.

Similarly, case II yields that $c + d\sqrt{5}\, i = \pm 1$, which are units in $\mathbf{Z}[\sqrt{-5}]$. Hence 3 is an irreducible element of $\mathbf{Z}[\sqrt{-5}]$.

Example 2.7.13. *Give an example to show that in an integral domain, every irreducible element need not be prime.*

Hint. See Examples 2.7.9 and 2.7.12.

Example 2.7.14. *Prove that $2 + \sqrt{-5}$ is irreducible but not prime in $\mathbf{Z}[\sqrt{-5}]$.*

Hint. Let $2 + \sqrt{5}\, i = (a + b\sqrt{5}\, i)\,(c + d\sqrt{5}\, i)$; $a, b, c, d \in \mathbf{Z}$.

Then $2 - \sqrt{5}\, i = (a - b\sqrt{5}\, i)\,(c - d\sqrt{5}\, i)$, and so

$$9 = (a^2 + 5b^2)\,(c^2 + 5d^2).$$

As discussed in Example 2.7.12, $2 + \sqrt{-5}$ is an irreducible element of $\mathbf{Z}[\sqrt{-5}]$.

Further $2 + \sqrt{-5}$ divides $3 \cdot 3 = 9 = (2 + \sqrt{-5})\,(2 - \sqrt{-5})$, but $2 + \sqrt{-5}$ does not divide 3. Hence $2 + \sqrt{-5}$ is not a prime element of $\mathbf{Z}[\sqrt{-5}]$.

Example 2.7.15. *Prove that $2 - \sqrt{-5}$ is irreducible but not prime in $\mathbf{Z}[\sqrt{-5}]$.*

Example 2.7.16. *Prove that $1 + \sqrt{-3}$ is irreducible but not prime in $\mathbf{Z}[\sqrt{-5}]$.*

Example 2.7.17. *Prove that 5 is irreducible but not prime in $\mathbf{Z}[\sqrt{-6}]$.*

Example 2.7.18. *Prove that 2, $1 \pm \sqrt{-3}$ are irreducible elements of $\mathbf{Z}[\sqrt{-3}]$.*

Please try yourself.

Example 2.7.19. *Prove that 2 is an irreducible but not a prime element of $\mathbf{Z}[\sqrt{-3}]$.*

Hint. $4 = (1 + \sqrt{-3})\,(1 - \sqrt{-3})$, 2 divides 4 but 2 does not divide both $1 + \sqrt{-3}$ and $1 - \sqrt{-3}$.

Example 2.7.20. *If p, q are prime elements in an integral domain R with unity such that $p \mid q$, then show that p and q are associates.* [D.U., 1994]

Solution. By definition, p and q are non-zero and non-units. Since $p \mid q$, $q = ap$, for some $a \in R$. Since $q = q \cdot 1$, $q \mid q \Rightarrow q \mid ap \Rightarrow q \mid a$ or $q \mid p$, since q is prime.

If $q \mid a$, then $a = qx$, for some $x \in R$. Thus $q = ap = qxp$ or $q \cdot 1 = qxp$ or $1 = xp$ ($\because$ $q \neq 0$ and R is an I.D.) $\Rightarrow p \mid 1 \Rightarrow p$ is a unit, a contradiction.

Thus $q \mid p \Rightarrow p = qy$, for some $y \in R$.

$\therefore$ $q = ap \Rightarrow q \cdot 1 = aqy \Rightarrow q \cdot 1 = q \cdot ay \Rightarrow 1 = ay \Rightarrow a \mid 1$

$\Rightarrow a$ is a unit, where $q = ap$. Hence p and q are associates.

Theorem 2.7.1. *Let R be an integral domain with unity. Show that every prime element of R is irreducible. However, the converse need not be true.*

Proof. Let p be any prime element of R. Then $p \neq 0$ and p is not a unit. We have to show that p is irreducible. Let $p = ab$, where $a, b \in R$. We shall prove that either a or b is a unit. We have

$$p \,.\, 1 = ab \Rightarrow p \mid ab \Rightarrow p \mid a \text{ or } p \mid b, \text{ since } p \text{ is prime.}$$

Let $p \mid a$. Then $a = pr$, for some $r \in R$ and so

$$\begin{aligned} p = ab &\Rightarrow p = (pr)\, b \Rightarrow p \,.\, 1 - p\,(rb) = 0 \\ &\Rightarrow p\,(1 - rb) = 0 \Rightarrow 1 - rb = 0, \text{ as } p \neq 0 \\ &\Rightarrow rb = 1 \Rightarrow b \mid 1 \Rightarrow b \text{ is a unit.} \end{aligned}$$

Similarly, we can show that if $p \mid b$, then a is a unit. Hence p is an irreducible element.

However, the converse need not be true *i.e.*, an irreducible element in an integral domain may not be prime. For example, *3 is an irreducible element of* $\mathbf{Z}[\sqrt{-5}]$, *but is not a prime element of* $\mathbf{Z}[\sqrt{-5}]$.

[See Examples 2.7.9 and 2.7.12]

Ex. *Show that* $\sqrt{-5}$ *is an irreducible element of* $\mathbf{Z}[\sqrt{-5}]$.

Hint. Refer to Example 2.7.10 and Theorem 2.7.1.

2.8 Principal Ideal Domain

We first introduce the notion of a *principal ideal* of a ring.

Definition. (Principal ideal)

Let a be any element of a commutative ring R. The smallest ideal of R which contains a is called the **principal ideal** *generated by a.*

It is denoted by $\langle a \rangle$ or (a).

In other words, (a) is a principal ideal of R if for any ideal A of R which contains a, then $(a) \subseteq A$.

We characterize a principal ideal (a) in a commutative ring R in the following :

Theorem 2.8.1. *If R be a commutative ring and $a \in R$, then*

$$(a) = \{ar + na : r \in R, n \in \mathbf{Z}\}.$$

Proof. Let $S = \{ar + na : r \in R, n \in \mathbf{Z}\}$.

We shall prove that S is the smallest ideal of R which contains a.

We see that

$$a = a \,.\, 0 + 1 \,.\, a \;(0 \in R \text{ and } 1 \in \mathbf{Z}) \text{ and so } a \in S.$$

Let $\alpha, \beta \in S$. Then $\alpha = ar + na$, $\beta = as + ma$; where $r, s \in R$ and $n, m \in \mathbf{Z}$. We have

$$\alpha - \beta = (ar + na) - (as + ma) = a\,(r - s) + (n - m)\, a \in S.$$

For any $x \in R$ and $\alpha \in S$, we have

$$\alpha x = (ar + na)\, x = a\,(rx) + a\,(nx)$$

or

$$\alpha x = a\,(rx + nx) + 0a\;(0 \in \mathbf{Z}) \Rightarrow \alpha x \in S.$$

Since R is commutative, $x\alpha = \alpha x \in S$.

Thus S is an ideal of R which contains a.

Let T be *any* other ideal of R which contains a.

We shall prove that $S \subseteq T$.

Since $a \in T$ and T is an ideal of R, $ar \in T \; \forall \; r \in R$.

Also $na = a + a + ... + a$ (n times) $\Rightarrow na \in T \; \forall \; n \in \mathbf{Z}$.

Thus $ar + na \in T \; \forall \; r \in R$ and $\forall \; n \in \mathbf{Z}$ and so $S \subseteq T$. Hence S is the smallest ideal of R which contains a *i.e.*,

$$(a) = S = \{ar + na : r \in R, n \in \mathbf{Z}\}.$$

Corollary. *If R is a commutative ring with unity and $a \in R$, then*

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

Proof. Since $1 \in R$, so $n \,.\, 1 = 1 + 1 + 1 ... + 1$ (n times)

$\Rightarrow n \,.\, 1 \in R \; \forall \; n \in \mathbf{Z}$.

Let $x \in (a)$ be arbitrary. Then $x = ar + na$, for some $r \in R$ and $n \in \mathbf{Z}$. We have

$$x = ar + na = a(r + n \,.\, 1) = at, \text{ where } t = r + n \,.\, 1 \in R$$

$\Rightarrow \quad (a) \subseteq aR$.

Conversely, let $y \in aR$ be arbitrary. Then

$$y = ar_0, \text{ for some } r_0 \in R \Rightarrow y = ar_0 + 0 \,.\, a \; (0 \in \mathbf{Z})$$

$\Rightarrow \quad y \in (a) \Rightarrow aR \subseteq (a)$.

Hence $(a) = aR = \{ar : r \in R\}$.

Definition. (Principal Ideal Domain)

An integral domain R with unity is called a **principal ideal domain** **(P.I.D.)**, *if each ideal A of R is a principal ideal i.e.,*

$$A = (a) = \{ar : r \in R\}, \textit{ for some } a \in A.$$

EXAMPLES

Example 2.8.1. *Show that* $\mathbf{Z}$ *(all integers) is a P.I.D.*

Solution. We know $\mathbf{Z}$ is an integral domain with unity. Let A be any ideal of $\mathbf{Z}$. If $A = (0)$, there is nothing to prove. Suppose $A \neq (0)$. Let n be the smallest positive integer in A. (Notice that A does contain positive integers). We shall show that $A = (n)$. Let $x \in (n)$ be arbitrary. Then $x = nk$, for some $k \in \mathbf{Z}$. Since A is an ideal of $\mathbf{Z}$, so $n \in A$ and $k \in \mathbf{Z} \Rightarrow nk \in A \Rightarrow x \in A \Rightarrow (n) \subseteq A$. Conversely, let m be any integer in A. By the division algorithm in $\mathbf{Z}$, there exist integers q and r such that $m = qn + r$, where $r = 0$ or $0 < r < n$. If $0 < r < n$, then $r = m - qn \in A$ ($\because \; m, n \in A$), which contradicts the fact that n is the least positive integer that belongs to A. Thus $r = 0$ and so $m = nq$, which implies that $A \subseteq (n)$. Hence $A = (n)$ and so $\mathbf{Z}$ is a P.I.D.

Example 2.8.2. *Prove that every field is a P.I.D. Is the converse true ? Justify your answer.* [D.U., 1999]

Solution. We know that the only ideals of a field F are (0) and F itself. For any $x \in F$, $x = 1 \,.\, x$ implies that $x \in (1)$ *i.e.*, $F = (1)$. Hence the only ideals of a field F are (0) and (1), which are principal ideals. Hence F is a P.I.D.. *The converse, however, is not true.* For example, $\mathbf{Z}$ (all integers) is a P.I.D., which is not a field.

Example 2.8.3. *For any prime p, the ring* $\mathbf{Z}_p$ *of integers modulo p, is a P.I.D.*

Solution. For any prime p, we know

$$\mathbf{Z}_p = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{p-1}\}$$

is a field and so by Example 2.8.2, $\mathbf{Z}_p$ is a P.I.D.

Example 2.8.4. *If A, B, C are non-zero ideals of a P.I.D. R, show that*

(*a*) $A(B \cap C) = AB \cap AC$.

(*b*) $A = \langle a \rangle$ *and* $B = \langle b \rangle \Rightarrow AB = \langle ab \rangle$.

Solution. (*a*) We suppose that

$A = \langle a \rangle, B = \langle b \rangle, C = \langle c \rangle, B \cap C = \langle d \rangle$; where $a \in A, b \in B, c \in C$ and $d \in B \cap C$. Moreover a, b, c are all non-zero elements of R.

Let $x \in AB \cap AC$ be arbitrary. Then $x \in AB$ and $x \in AC$

$\Rightarrow x = a_1 b_1 + a_2 b_2 + \ldots + a_m b_m$ and $x = \alpha_1 \beta_1 + \alpha_2 \beta_2 + \ldots + \alpha_n \beta_n$; where $a_i \in A$, $b_i \in B$, $\alpha_i \in A$ and $\beta_i \in C$ *i.e.*, $a_i = ar_i$, $b_i = bs_i$, $\alpha_i = at_i$ and $\beta_i = ck_i$ for each i. Here r_i, s_i, t_i and $k_i \in R$.

$\therefore \quad x = ar_1 bs_1 + \ldots + ar_m bs_m = ab(r_1 s_1 + \ldots + r_m s_m)$, ...(1)

and $\quad x = at_1 ck_1 + \ldots + at_n ck_n = ac(t_1 k_1 + \ldots t_n k_n)$.

Clearly, $ab(r_1 s_1 + \ldots + r_m s_m) = ac(t_1 k_1 + \ldots + t_n k_n)$.

Since $a \neq 0$, it follows that

$$b(r_1 s_1 + \ldots + r_m s_m) = c(t_1 k_1 + \ldots + t_n k_n) = y, \text{ say}$$

$\Rightarrow \quad y \in B$ and $y \in C \Rightarrow y \in B \cap C$,

and $\quad x = ab(r_1 s_1 + \ldots + r_m s_m) \Rightarrow x = ay \Rightarrow x \in A(B \cap C)$.

$\therefore \quad AB \cap AC \subseteq A(B \cap C)$. ...(2)

Conversely, let $x \in A(B \cap C)$. Then

$$x = p_1 q_1 + \ldots + p_l q_l, \text{ where } p_i \in A, q_i \in B \cap C$$

i.e., $\quad p_i = a z_i$ and $q_i = d\pi_i$; $z_i, \pi_i \in R$.

$\therefore \quad x = az_1 d\pi_1 + \ldots + az_l d\pi_l = ad(z_1 \pi_1 + \ldots + z_l \pi_l)$.

It follows that $d(z_1 \pi_1 + \ldots + z_l \pi_l) \in B$. $(\because d \in B, z_1 \pi_1 + \ldots + z_l \pi_l \in R)$

Similarly, $\quad d(z_1 \pi_1 + \ldots + z_l \pi_l) \in C$. $(\because d \in C)$

$\therefore \quad x = ad(z_1 \pi_1 + \ldots + z_l \pi_l) \Rightarrow x \in AB$ and $x \in AC$

$\Rightarrow x \in AB \cap AC$.

$\therefore \quad A(B \cap C) \subseteq AB \cap AC$. ...(3)

From (2) and (3), $\quad A(B \cap C) = AB \cap AC$.

(*b*) Let $A = \langle a \rangle$ and $B = \langle b \rangle$.

Let $x \in AB$. Then $x = ab(r_1 s_1 + \ldots + r_m s_m)$, by (1)

$\Rightarrow x \in \langle ab \rangle \Rightarrow AB \subseteq \langle ab \rangle$

Conversely, let $y \in \langle ab \rangle$. Then $y = (ab)\, r$, for some $r \in R$

$\Rightarrow \quad y = a\,(br)$, where $a \in A$ and $br \in B$, as $B = \langle b \rangle$.

Thus $y \in AB$ *i.e.*, $\langle ab \rangle \subseteq AB$.

Hence $AB = \langle ab \rangle$.

Example 2.8.5. *If A, B, C are ideals in a P.I.D. R, prove that*

(i) $A \cap (B + C) = A \cap B + A \cap C$.

(ii) $A + (B \cap C) = (A + B) \cap (A + C)$.

Hint. Take $A = \langle a \rangle$, $B = \langle b \rangle$, $C = \langle c \rangle$. Verify that $A + B = \langle a + b \rangle$, $B + C = \langle b + c \rangle$, $A + C = \langle a + c \rangle$.

Take $A \cap B = \langle l \rangle$, $B \cap C = \langle m \rangle$, $A \cap C = \langle n \rangle$.

Theorem 2.8.2. *Prove that any two non-zero elements a, b in a P.I.D. R have a g.c.d. Further if $d \in R$ is a g.c.d. of a and b, then $d = \lambda a + \mu b$; for some $\lambda, \mu \in R$.* [D.U., 1999, 97]

Proof. Let $A = \{xa + yb : x, y \in R\}$. ...(1)

We shall prove that A is an ideal of R. Clearly, A is non-empty, since $0 = 0 \,.\, a + 0 \,.\, b \in A$. Let $\alpha, \beta \in A$. Then

$$\alpha = x_1 a + y_1 b,\ \beta = x_2 a + y_2 b \ ; \quad \text{where} \quad x_1, y_1, x_2, y_2 \in R.$$

We have

$$\alpha - \beta = (x_1 a + y_1 b) - (x_2 a + y_2 b) = (x_1 - x_2)\, a + (y_1 - y_2)\, b,$$

where $x_1 - x_2 \in R,\ y_1 - y_2 \in R$.

Thus $\alpha - \beta \in A$. For any $r \in R$ and $\alpha \in A$, we have

$$\alpha r = (x_1 a + y_1 b)\, r = r\,(x_1 a + y_1 b), \text{ since } R \text{ is commutative}$$

$$= (rx_1)\, a + (ry_1)\, b \in A, \text{ since } rx_1 \in R,\ ry_1 \in R$$

Since R is commutative, $r\alpha = \alpha r \in A$.

Thus A is an ideal of R. Since R is a P.I.D., so

$$A = (d), \text{ for some } d \in A. \qquad ...(2)$$

Since $d \in A$, so by virtue of (1), we can write

$$d = \lambda a + \mu b \text{ for some } \lambda, \mu \in R. \qquad ...(3)$$

We now proceed to show that d is g.c.d. of a and b. We have

$$a = 1 \,.\, a + 0 \,.\, b \quad \text{and} \quad b = 0 \,.\, a + 1 \,.\, b.$$

$\Rightarrow a \in A$ and $b \in A$, by (1).

Using (2), $a = dx$ and $b = dy$; for some $x, y \in R$

$\Rightarrow d \mid a$ and $d \mid b$.

Let $c \in R$ be such that $c \mid a$ and $c \mid b$. Then

$$c \mid \lambda a \text{ and } c \mid \mu b \Rightarrow c \mid (\lambda a + \mu b) \Rightarrow c \mid d, \text{ by (3).}$$

Hence d is a g.c:d. of a and b and $d = \lambda a + \mu b$; $\lambda, \mu \in R$.

EXAMPLES

Example 2.8.6. *Let R be an integral domain with unity and a, b be any two non-zero elements of R. Show that*

(i) $a \mid b$ *and* $b \mid a$ *iff* $(a) = (b)$.

(ii) *a and b are associates iff* $(a) = (b)$.

Solution. (*i*) Let $a \mid b$ so that $b = ac$, for some $c \in R$.

Let $x \in (b)$ be arbitrary. Then $x = br$, for some $r \in R$

or $x = (ac)\, r = a\,(cr)$, where $cr \in R$

$\Rightarrow$ $x \in (a)\ \forall\ x \in (b)$.

Thus $a \mid b \Rightarrow (b) \subseteq (a)$.

Similarly, $b \mid a \Rightarrow (a) \subseteq (b)$.

Hence $a \mid b$ and $b \mid a \Rightarrow (a) = (b)$.

Conversely, $(a) = (b) \Rightarrow a \in (b) \Rightarrow a = bs$, for some $s \in R$

$\Rightarrow b \mid a$.

Again $(a) = (b) \Rightarrow b \in (a) \Rightarrow b = at$, for some $t \in R \Rightarrow a \mid b$.

Hence $(a) = (b) \Rightarrow a \mid b$ and $b \mid a$.

(*ii*) By Example 2.7.4, a and b are associates $\Leftrightarrow a \mid b$ and $b \mid a$.

By part (*i*), $a \mid b$ and $b \mid a \Leftrightarrow (a) = (b)$. Hence the result follows.

Example 2.8.7. *In a P.I.D., prove that any two greatest common divisors of a and b are associates.*

Solution. By Theorem 2.8.2, any two non-zero elements a and b in a P.I.D. R have a g.c.d. Let d_1 and $d_2 \in R$ be any two greatest common divisors of a and b. Then $d_1 \mid a$ and $d_1 \mid b$; $d_2 \mid a$ and $d_2 \mid b$.

Since d_1 is a g.c.d. of a and b, so $d_2 \mid a$ and $d_2 \mid b \Rightarrow d_2 \mid d_1$.

Since d_2 is a g.c.d. of a and b, so $d_1 \mid a$ and $d_1 \mid b \Rightarrow d_1 \mid d_2$.

Hence $d_1 \mid d_2$ and $d_2 \mid d_1 \Rightarrow d_1$ and d_2 are associates, by Example 2.8.6.

Example 2.8.8. *In a P.I.D., prove that any associate of a g.c.d. is a g.c.d.*

Solution. Let R be a P.I.D. and $d_1 \in R$ be a g.c.d. of $a, b \in R$.

Let $d_2 \in R$ be an associate of d_1. Then $d_1 = ud_2$, for some unit $u \in R$.

It follows that $d_2 \mid d_1$, where $d_1 \mid a$ and $d_1 \mid b$.

Consequently, $d_2 \mid a$ and $d_2 \mid b$. ...(1)

Let $x \in R$ be such that $x \mid a$ and $x \mid b$. ...(2)

Then $x \mid d_1$, since d_1 is g.c,d. of a and b.

We have $d_1 = ud_2 \Rightarrow d_2 = u^{-1} d_1 \Rightarrow d_1 \mid d_2$ ...(3)

Hence $x \mid d_1$ and $d_1 \mid d_2 \Rightarrow x \mid d_2$

From (1), (2) and (3) ; d_2 is also a g.c.d. of a and b.

Example 2.8.9. *Let R be a P.I.D. Let $d_1 \in R$ be a g.c.d. of $a, b \in R$. Show that $d_2 \in R$ is a g.c.d. of a and b if and only if d_1 and d_2 are associates.*

Solution. Refer to Examples 2.8.7, 2.8.8.

Definition. (Co-prime Elements)

Two non-zero elements of a principal ideal domain R are said to be **relatively prime** *or* **co-prime,** *if their greatest common divisor is a unit of R.*

Lemma 2.8.3. *Two elements a and b of a P.I.D. R are relatively prime iff* $(a, b) = 1$.

Proof. Let x be any unit in R. then $x\,x^{-1} = 1$, where x^{-1} is a unit in R. It follows that 1 and x are associates. Thus 1 is an associate of any unit. Since a and b are relatively prime, g.c.d. of a and b is a unit, say u *i.e.*, $u = (a, b)$. Since any associate of a g.c.d. is a g.c.d., 1 is g.c.d. of a and b. Hence $1 = (a, b)$. [See Example 2.8.8]

Conversely, $(a, b) = 1 \Rightarrow a$ and b are relatively prime, since 1 is a unit in R.

Lemma 2.8.4. *Two elements a and b of a P.I.D. R are co-prime if and only if there exist x and y in R such that* $ax + by = 1$. [D.U., 1997]

Proof. By Lemma 2.8.3 ; a and b are co-prime $\Rightarrow 1 = (a, b)$.

By Theorem 2.8.2, there exist $x, y \in R$ such that $ax + by = 1$.

Conversely, let $ax + by = 1$, for some $x, y \in R$.

Let $d \in R$ be a g.c.d of a and b. Then $d \mid a$ and $d \mid b$

$\Rightarrow d \mid ax$ and $d \mid by$

$\Rightarrow d \mid (ax + by) \Rightarrow d \mid 1 \Rightarrow d \mid 1 \Rightarrow d$ is a unit. Hence a and b are co-prime.

Lemma 2.8.5. *Let R be a principal ideal domain and* $a, b, c \in R$. *If* $a \mid bc$ *and* $(a, b) = 1$, *then* $a \mid c$.

Proof. Since $(a, b) = 1$, there exist $x, y \in R$ such that $ax + by = 1$ (Theorem 2.8.2). It follows that $cax + cby = c \cdot 1$ or $acx + bcy = c$.

Now $a \mid a \Rightarrow a \mid acx$ and $a \mid bc \Rightarrow a \mid bcy$.

$\therefore \quad a \mid (acx + bcy) \Rightarrow a \mid c$.

Theorem 2.8.6. *Prove that any two non-zero elements a and b in a P.I.D. R have a l.c.m.*

Proof. Let $A = (a)$ and $B = (b)$ be two ideals of R generated by a and b, respectively. It follows that $A \cap B$ is an ideal of R. Since R is a P.I.D., $A \cap B$ must be a principal ideal *i.e.*,

$$A \cap B = (l), \text{ for some } l \in A \cap B.$$

We shall show that l is l.c.m. of a and b.

$$l \in A \cap B \Rightarrow l \in A = (a) \text{ and } l \in B = (b)$$

$\Rightarrow l = ax$ and $l = by$, for some $x, y \in R$

$\Rightarrow a \mid l$ and $b \mid l$. ...(1)

Let $x \in R$ be such that $a \mid x$ and $b \mid x$. ...(2)

Then $x = ar$ and $x = bs$, for some $r, s \in R$

$\Rightarrow \quad x \in A = (a)$ and $x \in B = (b)$

$\Rightarrow \quad x \in A \cap B = (l) \Rightarrow x = lt$, for some $t \in R$

$\Rightarrow \quad l \mid x$. ...(3)

From (1), (2), (3) ; it follows that l is l.c.m. of a and b.

Theorem 2.8.7. *Prove that if R is a P.I.D. and a, b are two non-zero elements of R, then $[a, b]\,(a, b) = abu$, for some unit $u \in R$.*

Solution. Since R is a P.I.D., a and b possess g.c.d. and l.c.m.

We suppose that

$$d = (a, b) = \text{g.c.d. of } a \text{ and } b,$$
$$l = [a, b] = \text{l.c.m. of } a \text{ and } b.$$

By definition of l.c.m., $a \mid l$ and $b \mid l$

$\Rightarrow \quad l = ax,\ l = by$, for some $x, y \in R$. ...(1)

Since d is g.c.d. of a and b, there exist λ and $\mu \in R$ such that

$$d = \lambda a + \mu b \Rightarrow l(\lambda a + \mu b) = ld$$
$$\Rightarrow \quad ld = l\lambda a + \lambda\mu b \Rightarrow ld = by\lambda a + ax\mu b$$
$$\Rightarrow \quad ld = ab(\mu x + \lambda y) \Rightarrow ab \mid ld. \qquad ...(2)$$

By definition of g.c.d., $d \mid a$ and $d \mid b$

$\Rightarrow \quad a = dr$ and $b = ds$, for some $r, s \in R$

$\Rightarrow \quad ab = drds = (drs)\,d.$ ...(3)

Now $a = dr$ and $dr \mid drs \Rightarrow a \mid drs$, $b = ds$ and $ds \mid drs \Rightarrow b \mid drs$.

$\therefore \quad a \mid drs$ and $b \mid drs$ ...(4)

From (1) and (4), $l \mid drs$ and so $drs = lt$, for some $t \in R$.

Putting in (3) gives $\quad ab = ltd = (ld)\,t \quad \Rightarrow \quad ld \mid ab.$ ...(5)

From (2) and (5), ab and ld are associates. [See Example 2.7.4]

Consequently, $ld = uab$, for some unit $u \in R$.

Hence $\quad [a, b]\,(a, b) = abu$, for some unit $u \in R$.

Example 2.8.10. *Let R be a P.I.D. Let $l_1 \in R$ be l.c.m. of $a, b \in R$. Show that $l_2 \in R$ is l.c.m. of a and b if and only if l_1 and l_2 are associates.*

Solution. By Theorem 2.8.6, any two non-zero elements a and b in R have a l.c.m. Let l_1 and l_2 be two least common multiples of a and b. Then $a \mid l_1$ and $b \mid l_1$; $a \mid l_2$ and $b \mid l_2$. Since l_1 is l.c.m. of a and b, so $a \mid l_2$ and $b \mid l_2 \Rightarrow l_1 \mid l_2$. Since l_2 is l.c.m. of a and b, so $a \mid l_1$ and $b \mid l_1 \Rightarrow l_2 \mid l_1$.

Hence $l_1 \mid l_2$ and $l_2 \mid l_1 \Rightarrow l_1$ and l_2 are associates.

Conversely, let l_1 be l.c.m. of a and b and l_2 be an associate of l_1.

We shall prove that l_2 is l.c.m. of a and b.

Since l_1 and l_2 are associates, $l_2 = ul_1$, for some unit $u \in R$

$\Rightarrow \quad l_1 \mid l_2$, where $a \mid l_1$ and $b \mid l_1$ ...(1)

$\Rightarrow \quad a \mid l_2$ and $b \mid l_2$. ...(2)

Let $x \in R$ be such that $a \mid x$ and $b \mid x$.

Since l_1 is l.c.m. of a and b, so $a \mid x$ and $b \mid x \Rightarrow l_1 \mid x$.

Since u is a unit in R, so $l_2 = ul_1 \Rightarrow l_1 = u^{-1} l_2 \Rightarrow l_2 \mid l_1$. ...(3)

Now $\quad l_2 \mid l_1$ and $l_1 \mid x \quad \Rightarrow \quad l_2 \mid x$.

From (1), (2) and (3) ; l_2 is l.c.m. of a and b.

Theorem 2.8.8. *In a P.I.D. an element is prime if and only if it is irreducible.*

Proof. Let R be a P.I.D. Since R is an integral domain, by Theorem 2.7.1, every prime element of R is irreducible. Now we shall show that every irreducible element of R is prime. Let p be any irreducible element of R. Then $p \neq 0$ and p is not a unit. We shall prove that p is prime. Let $p \mid ab$, where $a, b \in R$. Let $p \dagger a$. We shall prove that $p \mid b$. Since (p) and (b) are ideals of R, so $(p)+(b)$ is also an ideal of R. Since R is a P.I.D., $(p)+(b)$ must be a principal ideal *i.e.*,

$$(p)+(b)=(d), \text{ for some } d \in R. \qquad \ldots(1)$$

From (1), $(p) \subseteq (d)$

$$\Rightarrow \quad p \in (d) \Rightarrow p = dx, \text{ for some } x \in R. \qquad \ldots(2)$$

Since p is irreducible, either d or x is a unit. Suppose d is a unit. Then $d^{-1} \in R$ and $dd^{-1}=1 \Rightarrow 1 \in (d) \Rightarrow 1 \in (p)+(b)$, by (1)

$$\Rightarrow \quad 1 = pr + bs, \text{ for some } r, s \in R \qquad \ldots(3)$$

$$\Rightarrow \quad a = a.1 = apr + abs.$$

Now $p \mid p \Rightarrow p \mid apr$ and $p \mid ab \Rightarrow p \mid abs$.

Thus $p \mid (apr + abs)$ and so $p \mid a$, by (3).

But $p \mid a$ is contrary to our assumption and so d can not be a unit. It follows that x is a unit *i.e.*, $x^{-1} \in R$. From (2), $d = px^{-1}$. Let $\alpha \in (d)$. Then $\alpha = dy$, for some $y \in R$

$$\Rightarrow \quad \alpha = (px^{-1})\, y = p\,(x^{-1} y),\ x^{-1} y \in R$$

$$\Rightarrow \quad \alpha \in (p)\ \forall\ \alpha \in (d) \ \Rightarrow\ (d) \subseteq (p).$$

As shown above, $(p) \subseteq (d)$

$\therefore$ $(d)=(p)$. Using in (1), we get

$$(p)+(b)=(p) \Rightarrow (b) \subseteq (p) \Rightarrow b \in (p) \quad \Rightarrow b = pt, \text{ for some } t \in R$$

$\Rightarrow p \mid b$. Hence p is prime.

Ex. 1. *Show that* $\mathbf{Z}[\sqrt{-5}]$ *is not a P.I.D.*

Solution. If $\mathbf{Z}[\sqrt{-5}]$ is a P.I.D., then every irreducible element of $\mathbf{Z}[\sqrt{-5}]$ must be prime. By Examples 2.7.9 and 2.7.12, $3 \in \mathbf{Z}[\sqrt{-5}]$ is irreducible but not prime. Hence we arrive at a contradiction and so $\mathbf{Z}[\sqrt{-5}]$ is not a P.I.D.

Ex. 2. *Show that* $\mathbf{Z}[\sqrt{-6}]$ *is not a P.I.D.*

[Hint. See Example 2.7.17]

Theorem 2.8.9. *Let R be a P.I.D., which is not a field. Prove that an ideal $A=(a)$ is a maximal ideal if and only if a is an irreducible element of R.* [D.U., 2000, 1996, 95]

Proof. Since R is not a field, there exists an element $p \neq 0 \in R$ such that p^{-1} does not exist *i.e.*, p is not a unit.

Condition is necessary

Let $A=(a)$ be a maximum ideal of R. We shall prove that a is an irreducible element of R. We observe that $a \neq 0$, for if $a=0$, then

$(0) \subset (p) \subset R$ and so $(a) = (0)$ is not a maximum ideal of R, which is contrary to the given hypothesis. Further, $A \neq R \Rightarrow a$ is not a unit, for if a is a unit, then $a^{-1} \in R$ and so $a \in A$ and $a^{-1} \in R \Rightarrow 1 = aa^{-1} \in A \Rightarrow A = R$, which is a contradiction. Thus $a \neq 0$ and a is not a unit. Suppose that

$$a = bc, \text{ for some } b, c \in R.$$

Let $B = (b)$. Let $r \in A = (a)$ be arbitrary. Then $r = ax$, for some $x \in R$ or $r = (bc)\, x = b\,(cx) \Rightarrow r \in B \Rightarrow A \subseteq B \subseteq R$. Since A is a maximal ideal of R, either $A = B$ or $B = R$.

Let $B = R$. Then $1 \in R \Rightarrow 1 \in B = (b) \Rightarrow 1 = by$, for some $y \in R$.

$\therefore\ b \mid 1 \Rightarrow b$ is a unit.

Let $A = B$. Then $b \in B \Rightarrow b \in A = (a) \Rightarrow b = az$, for $z \in R$

$\Rightarrow\quad b = (bc)\, z \Rightarrow cz = 1 \Rightarrow c \mid 1 \Rightarrow c$ is a unit.

It follows that $a = bc \Rightarrow$ either b or c is a unit.

Hence a is an irreducible element of R.

Condition is sufficient

Let $A = (a)$, where a is an irreducible element of R. We shall show that A is a maximal ideal of R. Let I be any ideal of R such that $A \subseteq I \subseteq R$.

Since R is a P.I.D., $I = (d)$, for some $d \in R$.

Case I. Let $d \in A = (a)$. Then $d = ax$ for some $x \in R$. For any $r \in I = (d)$, $r = dy$, for some $y \in R \Rightarrow r = (ax)\, y = a\,(xy) \Rightarrow r \in A \Rightarrow I \subseteq A$.

Also $A \subseteq I$. Thus $A = I$.

Case II. Let $d \notin A$. Since $a \in A$ and $A \subseteq I = (d)$, so $a = dt$, for some $t \in R$. Since a is irreducible, either d or t is a unit.

If t is a unit, then $t^{-1} \in R$ and so $d = at^{-1}$. Since $a \in A$ and $t^{-1} \in R$, $at^{-1} \in A$, as A is an ideal of R. Thus $d \in A$, which is a contradiction. Consequently, d must be a unit *i.e.*, $d^{-1} \in R$.

Now $\quad d \in I$ and $d^{-1} \in R \Rightarrow 1 = dd^{-1} \in I \Rightarrow I = R$.

Hence $A \subseteq I \subseteq R \Rightarrow A = I$ or $I = R$ and so A is a maximal ideal of R.

Theorem 2.8.10. *Let R be a principal ideal domain. Show that any non-zero ideal $P \neq R$ is prime if and only if it is maximal.*

Proof. Let $P \neq R$ be a non-zero prime ideal of R. Since R is a P.I.D., $P = (a)$, for some $0 \neq a \in P$. We shall prove that P is a maximal ideal of R.

Let M be any ideal of R such that $P \subseteq M \subseteq R$. We can write $M = (b)$, for some $b \in M$. Since $a \in P$ and $P \subseteq M$, $a \in M \Rightarrow a = bx$, for some $x \in R$. Since P is a prime ideal of R and $a \in P$, either $b \in P$ or $x \in P$. If $b \in P$, then $(b) \subseteq P \Rightarrow M \subseteq P \Rightarrow P = M$.

If $x \in P = (a)$, then $x = ay$, for some $y \in R$. Consequently,

$$a = bx \Rightarrow a = bay \Rightarrow a \,.\, 1 = a \,.\, by \Rightarrow by = 1 \Rightarrow b \text{ is a unit.}$$

Since M is an ideal of R containing a unit b, $M = R$.

[See Example 2.7.2]

Hence P is a maximal ideal of R.

Conversely, every maximal ideal of R (being a commutative ring with unity) is a prime ideal of R. [See Theorem 2.6.3.]

Theorem 2.8.11. *Let R be a P.I.D. Show that every ascending chain of ideals*

$$(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \ldots \subseteq (a_n) \subseteq \ldots. \qquad \ldots(1)$$

is finite. [D.U., 1998]

Proof. Suppose the above chain of ideals is not finite.

Let $$A = \bigcup_{i=1}^{\infty} (a_i). \qquad \ldots(2)$$

We proceed to show that A is an ideal of R.

Let $x, y \in A$ be arbitrary. Then, by (2), $x \in (a_m), y \in (a_n)$;

for some positive integers m, n. We may assume that $m \leq n$.

Using (1), we get

$$(a_m) \subseteq (a_n) \Rightarrow x, y \in (a_n)$$

$$\Rightarrow \quad x - y \in (a_n) \Rightarrow x - y \in A, \text{ by (1).}$$

Again for any $r \in R$ and $x \in A$, we see that

$$x \in (a_m) \text{ and so } rx \in (a_m) \Rightarrow rx \in A \Rightarrow xr = rx \in A.$$

Thus A is an ideal of R and so A must be a principal ideal, as R is a P.I.D.

Let $A = (a)$, for some $a \in A$ ...(3)

Using (2), $a \in A \Rightarrow a \in (a_k)$, for some positive integer k

$$\Rightarrow \quad (a) \subseteq (a_k) \Rightarrow A \subseteq (a_k), \text{ by (3)}$$

$$\Rightarrow \bigcup_{i=1}^{\infty} (a_i) \subseteq (a_k), \text{ by (2)}$$

$$\Rightarrow \quad (a_i) \subseteq (a_k), \text{ for } i = 1, 2, 3, \ldots \qquad \ldots(4)$$

From (1), $(a_k) \subseteq (a_{k+1}) \subseteq (a_{k+2}) \subseteq \ldots.$ ...(5)

From (4), $(a_{k+1}) \subseteq (a_k), (a_{k+2}) \subseteq (a_k)$ and so on. ...(6)

From (5) and (6), we obtain

$$(a_k) = (a_{k+1}) = (a_{k+2}) = \ldots$$

Hence the given ascending chain of ideals is finite *i.e.*,

$$(a_1) \subseteq (a_2) \subseteq \ldots \subseteq (a_k).$$

3

Euclidean and Polynomial Rings

This chapter is devoted to the study of *Polynomial Rings, Euclidean* and *Unique factorization domains*. We shall prove that

E.D. $\Rightarrow$ P.I.D. $\Rightarrow$ U.F.D.

Primitive and *Irreducible polynomials* and *Eisenstein Criterion of Irreducibility of Polynomials over the rationals* have been discussed. At the end of the chapter, we prove a major theorem :

R is a U.F.D. $\Rightarrow$ *R [x] is a U.F.D.*

3.1 Euclidean Domain (E.D.)

Definition. *An integral domain R is called a* **Euclidean domain** (*or* **Euclidean ring**), *if for each* $a \neq 0 \in R$, *there is associated a non-negative integer, denoted by* $d(a)$, *such that*

(E.1) $d(a) \leq d(ab)$, $\forall\ a \neq 0, b \neq 0 \in R$.

(E.2) *For each pair* $a \neq 0 \in R, b \neq 0 \in R$, *there exist* $t, r \in R$ *such that* $a = tb + r$, *where either* $r = 0$ *or* $d(r) < d(b)$.

Remark. The function d is called *Euclidean valuation* on R. It may be observed that condition **(E.1)** also implies that $d(b) \leq d(ab)$.

EXAMPLES

Example 3.1.1. *The ring* **Z** *of integers is a Euclidean domain.*

Solution. We take $d(a) = |a|$, $\forall\ a \neq 0 \in \mathbf{Z}$.

Let $a \neq 0, b \neq 0 \in \mathbf{Z}$. Then $|a| \leq |ab| \Rightarrow d(a) \leq d(ab)$. On dividing a by b, we get integers t and r such that $a = tb + r$, where either $r = 0$ or $|r| < |b|$ *i.e.*, $d(r) < d(b)$. Hence **Z** is a Euclidean domain.

Example 3.1.2. *Every field F is a Euclidean domain.*

Solution. We take $d(a) = 1$, $\forall\ a \neq 0 \in F$.

Let $a \neq 0$, $b \neq 0 \in F$. Then $ab \neq 0$, since every field is an integral domain. Consequently,

$$d(a) = 1 \text{ and } d(ab) = 1 \Rightarrow d(a) = d(ab).$$

Also $b \neq 0 \in F \Rightarrow b^{-1} \in F$ and so $a = (ab^{-1})\, b + 0 = tb + r$,

where $t = ab^{-1} \in F$ and $r = 0 \in F$.

Hence F is a Euclidean domain.

Example 3.1.3. *The field* **Q** *of rational numbers with* $d(a) = 1$ *for all* $a \neq 0 \in \mathbf{Q}$ *is a Euclidean domain. However,* **Q** *with* $d(a) = |a|$ *for all* $a \neq 0 \in \mathbf{Q}$, *is* **not** *a Euclidean domain.*

Solution. If $d(a) = 1 \ \forall \ a \neq 0 \in \mathbf{Q}$, then $\mathbf{Q}$ is a Euclidean domain. (See Example 3.1.2).

However, $\mathbf{Q}$ with $d(a) = |a| \ \forall \ a \neq 0 \in \mathbf{Q}$ is not a Euclidean domain, for otherwise, on taking $a = b = \frac{3}{2}$;

$$\frac{3}{2} = \left|\frac{3}{2}\right| < \left|\frac{3}{2} \cdot \frac{3}{2}\right| = 1, \text{ a contradiction.}$$

Example 3.1.4. *Define a Euclidean ring and give two examples.* [D.U., 1996]

Example 3.1.5. *Show that* $\mathbf{Z}[i] = \{m + ni : m, n \in \mathbf{Z}, i = \sqrt{-1}\}$ *is a Euclidean domain.* [D.U., 2000, 1998, 95]

{$\mathbf{Z}[i]$ is called the Ring of Gaussian integers}

Solution. It is easy to verify that $\mathbf{Z}[i]$ is an integral domain with unity $1 = 1 + 0i$.

Let $a = m + ni \neq 0, \ b = m_1 + n_1 i \neq 0 \in \mathbf{Z}[i]$.

We define $d(a) = d(m + ni) = m^2 + n^2$. ...(1)

Obviously, $d(a)$ is a positive integer, for each $a \neq 0 \in \mathbf{Z}[i]$.

Indeed $d(a) \geq 1, \ \forall \ a \neq 0 \in \mathbf{Z}[i]$. ...(2)

We have

$$ab = (m + ni)(m_1 + n_1 i) = (mm_1 - nn_1) + (mn_1 + m_1 n)\, i$$

$$\therefore \quad d(ab) = (mm_1 - nn_1)^2 + (mn_1 + m_1 n)^2$$

$$= m^2 m_1^2 + n^2 n_1^2 + m^2 n_1^2 + m_1^2 n^2$$

$$= (m^2 + n^2)(m_1^2 + n_1^2) = d(a)\, d(b).$$

Thus $d(ab) = d(a)\, d(b), \ \forall \ a \neq 0, \ b \neq 0 \in \mathbf{Z}[i]$. ...(3)

We notice that $d(a) = d(a) \cdot 1$

$$\leq d(a)\, d(b), \qquad [\because \ d(b) \geq 1, \text{ by (2)}]$$

$$= d(ab), \text{ by (3)}$$

$$\therefore \quad d(a) \leq d(ab), \ \forall \ a \neq 0, \ b \neq 0 \in \mathbf{Z}[i]$$

Now we shall verify the second condition (E.2) of Euclidean domain.

We have

$$\frac{a}{b} = \frac{m + ni}{m_1 + n_1 i} = \frac{(m + ni)(m_1 - n_1 i)}{(m_1 + n_1 i)(m_1 - n_1 i)}$$

or

$$\frac{a}{b} = \left(\frac{mm_1 + nn_1}{m_1^2 + n_1^2}\right) + \left(\frac{m_1 n - mn_1}{m_1^2 + n_1^2}\right) i = p + qi \text{ (say)},$$

where p and q are rational numbers.

Corresponding to the rational numbers p and q, we can find suitable integers p' and q' such that ...(4)

$$|p' - p| \leq \frac{1}{2} \quad \text{and} \quad |q' - q| \leq \frac{1}{2}.$$

Let $t = p' + q'i$. Then $t \in \mathbf{Z}[i]$.

We have $\frac{a}{b} = \lambda$, where $\lambda = p + qi$

or $a = \lambda b = (\lambda - t)\, b + tb = tb + r$, where $r = (\lambda - t)\, b$.

Now $a, b, t \in \mathbf{Z}[i] \Rightarrow a - tb \in \mathbf{Z}[i] \Rightarrow r \in \mathbf{Z}[i]$.

Thus there exist $t, r \in \mathbf{Z}[i]$ such that

$a = tb + r$, where either $r = 0$ or

$$d(r) = d\{(\lambda - t)\, b\} = d\{(p - p') + (q - q')\, i\}\, d(b)$$

$$= [(p - p')^2 + (q - q')^2]\, d(b)$$

$$\leq \left[\frac{1}{4} + \frac{1}{4}\right] d(b), \text{ by (4)}$$

$$= \frac{1}{2} d(b)$$

$$< d(b).$$

Hence $\mathbf{Z}[i]$ is a Euclidean domain.

Example 3.1.6. *Shows that* $\mathbf{Z}[\sqrt{2}] = \{m + n\sqrt{2} : m, n \in \mathbf{Z}\}$ *is a Euclidean domain.* [D.U., 1989]

Solution. It is easy to verify that $\mathbf{Z}[\sqrt{2}]$ is an integral domain with unity $1 = 1 + \sqrt{2}\,.\,0$.

Let $a = m + n\sqrt{2} \neq 0,\ b = m_1 + n_1\sqrt{2} \neq 0 \in \mathbf{Z}\sqrt{2}$.

We define

$$d(a) = d(m + n\sqrt{2}) = |m^2 - 2n^2|. \quad \ldots(1)$$

Obviously, $d(a)$ is a positive integer, for each $a \neq 0 \in \mathbf{Z}[\sqrt{2}]$.

Indeed $d(a) \geq 1,\ \forall\ a \neq 0 \in \mathbf{Z}[\sqrt{2}]$. $\quad \ldots(2)$

We have

$$ab = (mm_1 + 2nn_1) + (mn_1 + m_1 n)\sqrt{2}$$

and

$$d(ab) = |(mm_1 + 2nn_1)^2 - 2(mn_1 + m_1 n)^2|, \text{ by (1)}$$

$$= |m^2 m_1^2 + 4n^2 n_1^2 - 2(m^2 n_1^2 + m_1^2 n^2)|$$

$$= |(m^2 - 2n^2)(m_1^2 - 2n_1^2)|$$

$$= |m^2 - 2n^2|\,|m_1^2 - 2n_1^2| = d(a)\, d(b). \quad \ldots(3)$$

Thus $d(ab) = d(a)\, d(b),\ \forall\ a \neq 0, b \neq 0 \in \mathbf{Z}[\sqrt{2}]$.

We notice that

$$d(a) = d(a) \,.\, 1$$

$$\leq d(a)\, d(b) \qquad [\because\ d(b) \geq 1, \text{ by (2)}]$$

$$= d(ab), \text{ by (3)}$$

$\therefore\ d(a) \leq d(ab),\ \forall\ a \neq 0, b \neq 0 \in \mathbf{Z}[\sqrt{2}]$.

Now we shall verify the second condition **(E.2)** of Euclidean domain.

We have

$$\frac{a}{b}=\frac{m+n\sqrt{2}}{m_1+n_1\sqrt{2}}=\frac{(m+n\sqrt{2})\,(m_1-n_1\sqrt{2})}{(m_1+n_1\sqrt{2})\,(m_1-n_1\sqrt{2})}$$

$$=\left(\frac{mm_1-2nn_1}{m_1^2-2n_1^2}\right)+\left(\frac{m_1n-mn_1}{m_1^2-2n_1^2}\right)\sqrt{2}=p+q\sqrt{2},$$

where p and q are rational numbers. We can find two integers p' and q' such that

$$|p'-p|\le\tfrac{1}{2} \text{ and } |q'-q|\le\tfrac{1}{2}. \qquad ...(4)$$

Let $t=p'+q'\sqrt{2}$. Then $t\in \mathbf{Z}\sqrt{2}]$.

We have $\frac{a}{b}=\lambda$, where $\lambda=p+q\sqrt{2}$

or $a=\lambda b=(\lambda-t)\,b+tb=tb+r$, where $r=(\lambda-t)\,b$.

Now $a, b, t\in \mathbf{Z}[\sqrt{2}] \Rightarrow a-tb\in \mathbf{Z}[\sqrt{2}] \Rightarrow r\in \mathbf{Z}[\sqrt{2}]$.

Thus there exist $t, r\in \mathbf{Z}[\sqrt{2}]$ such that

$$a=tb+r, \text{ where either } r=0$$

or
$$d(r)=d\{(\lambda-t)\,b\}=d\{(p-p')+(q-q')\sqrt{2}\}\,d(b)$$
$$=|(p-p')^2-2(q-q')^2|\,d(b)$$
$$\le|(p-p')^2+2(q-q')^2|\,d(b)$$
$$\le\left(\frac{1}{4}+\frac{2}{4}\right)d(b), \text{ by (4)}$$
$$=\frac{3}{4}d(b)$$
$$<d(b).$$

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

Example 3.1.7. *Show that* $\mathbf{Z}[\sqrt{3}]=\{m+n\sqrt{3} \ \because\ m, n\in \mathbf{Z}\}$ *is a Euclidean domain.* [D.U., 1992]

Hint. Take $d(m+n\sqrt{3})=|m^2-3n^2|$.

Theorem 3.1.1. *Every Euclidean domain is a principal ideal domain i.e.,*

$$E.D. \Rightarrow P.I.D.$$ [D.U., 2000, 1996, 93]

Proof. Let R be a Euclidean domain. Firstly, we show that every ideal of R is a principal ideal. Let A be any ideal of R. If $A=(0)$, there is nothing to prove. If $A\neq(0)$, we can choose some element $a_0\neq 0\in A$ such that $d(a_0)$ is minimal *i.e.*, $d(a_0)\le d(x)$, $\forall\ x\neq 0\in A$. ...(1)

Let $x\in A$ be arbitrary. If $x=0$, then $x\in(a_0)$.

For $x\neq 0$ and $a_0\neq 0\in R$, there exist $t, r\in R$ such that

$$x=ta_0+r, \text{ where either } r=0 \text{ or } d(r)<d(a_0).$$

Now $a_0 \in A$ and $t \in R \Rightarrow ta_0 \in A$, since A is an ideal of R. Further $a \in A$ and $ta_0 \in A \Rightarrow a - ta_0 \in A \Rightarrow r \in A$.

If $r \neq 0$, then $d(r) < d(a_0)$ and $r \in A$, which contradicts (1).

$\therefore$ $r = 0$ and so $x = ta_0 \Rightarrow x \in (a_0)\ \forall\ x \in A \Rightarrow A \subseteq (a_0)$.

Conversely, if $x \in (a_0)$, then $x = sa_0$, for some $s \in R$.

Since A is an ideal of R, $a_0 \in A$ and $s \in R \Rightarrow sa_0 \in A \Rightarrow x \in A$

$\Rightarrow (a_0) \subseteq A$. Hence $A = (a_0)$.

Finally, we show that R has unity. Since R is an ideal of R and as proved above, R is a principal ideal. Let $R = (r_0)$, for some $r_0 \in R$.

It follows that $r_0 = r_0 c$, for some $c \in R$.

Let $x \in R$ be arbitrary. Then $x = r_0 a$, for some $a \in R$.

We have $xc = (r_0 a)\, c = r_0 (ac) = r_0 (ca) = (r_0 c)\, a = r_0 a = x$

$\therefore$ $xc = cx = x\ \forall\ x \in R$, since R is commutative

$\Rightarrow c$ is the unity of R. Hence R is a P.I.D.

Corollary. $\mathbf{Z}[i]$, $\mathbf{Z}[\sqrt{2}]$ *are principal ideal domains.*

Proof. Since $\mathbf{Z}[i]$ and $\mathbf{Z}[\sqrt{2}]$ are Euclidean domains, the result follows.

Remarks.

1. In the definition of Euclidean domain, we do not explicitly mention that it has unity, but in fact *Every Euclidean domain has unity.* (See Theorem 3.1.1).
2. Every ideal M of a Euclidean domain is of the form $M = (m)$, for some $m \in M$ and $d(m)$ is minimal.
3. *The converse of Theorem* 3.1.1 *is not true* i.e., a principal ideal domain need not be a Euclidean domain. For example, the ring

$$R = \left\{ a + b\left(\frac{1 + \sqrt{-19}}{2} \right) : a, b \in \mathbf{Z} \right\}$$

is a principal ideal domain, but not a Euclidean domain.

The proof is beyond the scope of the book.

Since E.D. $\Rightarrow$ P.I.D., the following theorems proved for a principal ideal domain also hold for a Euclidean domain.

Theorem 3.1.2. *Let R be a Euclidean domain. Then any two non-zero elements a and b in R have a greatest common divisor d ; where*

$$d = \lambda a + \mu b, \text{ for some } \lambda, \mu \in R.$$

Proof. See Theorem 2.8.2. and use the fact E.D. $\Rightarrow$ P.I.D.

Theorem 3.1.3. *Any two non-zero elements in a Euclidean domain have a least common multiple.*

Proof. See Theorems 2.8.6 and use the fact E.D. $\Rightarrow$ P.I.D.

Theorem 3.1.4. *In a Euclidean domain, an element is prime if and only if it is irreducible.*

Proof. See Theorem 2.8.8 and use the fact E.D. $\Rightarrow$ P.I.D.

Theorem 3.1.5. *The ideal $A = (a_0)$ is a maximal ideal of a Euclidean domain R if and only if a_0 is an irreducible (prime) element of R.*

Proof. See Theorem 2.8.9 and use the fact E.D. $\Rightarrow$ P.I.D.

EXAMPLES

Example 3.1.8. *Show that* $\mathbf{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbf{Z}\}$ *is not a Euclidean domain.*

Solution. Let, if possible, $\mathbf{Z}[\sqrt{-5}]$ be a Euclidean domain. Consequently, an element in $\mathbf{Z}[\sqrt{-5}]$ is prime if and only if it is irreducible [Theorem 3.1.4]. We have seen that $3 \in \mathbf{Z}[\sqrt{-5}]$ is irreducible but not prime [See Examples 2.7.9. and 2.7.12. of chapter 2].

Hence $\mathbf{Z}[\sqrt{-5}]$ is not a Euclidean domain.

Example 3.1.9. Show that $\mathbf{Z}[\sqrt{-6}] = \{a + b\sqrt{-6} : a, b \in \mathbf{Z}\}$ *is not a Euclidean domain.*

Hint. See Example 2.7.17. $5 \in \mathbf{Z}[\sqrt{-6}]$ is irreducible but not prime.

Example 3.1.10. *In a Euclidean ring prove that any two greatest common divisors of a and b associates.* [D.U., 1995]

Hint. See Example 2.8.7, and use the fact E.D. $\Rightarrow$ P.I.D.

Example 3.1.11. *State and prove a necessary and sufficient condition for an element of a Euclidean ring R to be a unit of R.* [D.U., 1999, 92]

Or

Prove that a necessary and sufficient condition that an element a in the Euclidean ring R be a unit is that $d(a) = d(1)$. [D.U., 1996]

Solution. Since R is a Euclidean domain, $1 \in R$ and by condition **(E.1)** of the definition of E.D., $d(1) \leq d(1 \cdot x)\ \forall\ x \neq 0 \in R$

$$\therefore \quad d(1) \leq d(x) \quad \forall\ x \neq 0 \in R. \qquad \ldots(1)$$

Condition is necessary

Let $a \in R$ be a unit in R. Then $a \mid 1$ *i.e.*, there exists some $b \in R$ such that $ab = 1$. By condition **(E.2)** of E.D.,

$$d(a) \leq d(ab) \text{ or } d(a) \leq d(1).$$

From (1), $\quad d(1) \leq d(a)$. Hence $\quad d(a) = d(1)$.

Condition is sufficient

Let $d(a) = d(1)$. We shall prove that a is unit. By definition of E.D., for $1, a \in R$, there exist $t, r \in R$ such that $1 = at + r$, where either $r = 0$ or $d(r) < d(a)$.

If $r \neq 0$, then $d(r) < d(a) \Rightarrow d(r) < d(1)$, which contradicts (1).

$\therefore r = 0$ and so $1 = at \Rightarrow a \mid 1 \Rightarrow a$ is unit.

Remark. As a consequence of the above result, it follows that

The only units of $\mathbf{Z}[i]$ *are* $\pm 1, \pm i$.

Notice that $\quad d(i) = d(-i) = d(-1) = d(1) = 1.$

$$[\because\ d(a + bi) = a^2 + b^2]$$

Example 3.1.12. *Let a and b be two non-zero elements of a Euclidean domain R. Prove that b is not a unit in R if and only if $d(a) < d(ab)$.* [D.U., 1993]

Proof. By condition **(E.1)** of Euclidean domain, $d(a) \leq d(ab)$. ...(1)

Consider the ideal $A = (a) = \{xa : x \in R\}$ of R.

We know $a \neq 0 \in A$ and $d(a)$ is minimal.

[See Remark 2 of Theorem 3.1.1]

Since $a \in A$ and $b \in R$, $ab \in A$ (as A is an ideal of R). Let, if possible, $d(a) = d(ab)$. By the minimality of $d(a) = d(ab)$, we conclude that $A = (ab)$. Since $a \in A$ and $A = (ab)$, $a = abx$, for some $x \in R$

$\Rightarrow a \cdot 1 = abx \Rightarrow 1 = bx$, since $a \neq 0$ and R is an integral domain.

$\Rightarrow b \mid 1 \Rightarrow b$ is a unit in R, which is a contradiction.

$\therefore d(a) \neq d(ab)$ and so by (1), $d(a) < d(ab)$.

Conversely, let $d(ab) > d(a)$. We have to show that b is not a unit in R. Let, if possible, b be a unit in R. Then $b^{-1} \in R$ and $bb^{-1} = 1$.

We have $d(a) = d(a \cdot 1) = d(a \cdot bb^{-1}) = d(ab \cdot b^{-1}) \geq d(ab)$, by def.

$\therefore \quad d(a) \geq d(ab)$.

Again, by definition of E.D., $d(ab) \geq d(a)$.

$\therefore \quad d(a) = d(ab)$, which is contrary to the given hypothesis.

Hence b is not a unit in R.

Example 3.1.13. *Let D be a Euclidean domain with unit element 1. Let x be a non-unit in D. Show that $d(1) < d(x)$, under usual notations. Deduce that x is a unit in D iff $d(x) = d(1)$.* [D.U., 1994]

Solution. (*i*) Since x is a non-unit in D, so $d(a) < d(ax)$, $\forall\ a \neq 0 \in D$.

[See Example 3.1.12.]

In particular, $d(1) < d(1 \cdot x)$ (Take $a = 1 \in R$).

$\therefore \quad d(1) < d(x)$.

(*ii*) Let $d(x) = d(1)$. Then x must be a unit in D, for otherwise, $d(1) < d(x)$ [By part (*i*)], which is contrary to the given hypothesis.

Conversely, let x be a unit. Then $x \mid 1$ or $1 = xy$, for some $y \in R$. Thus $d(1) = d(xy) \geq d(x)$, by definition of E.D. ...(1)

$\therefore \quad d(1) \geq d(x)$.

Since $1 \in R$, by definition of E.D., ...(2)

$d(1 \cdot x) \geq d(1)$ *i.e.*, $d(x) \geq d(1)$.

From (1) and (2), $d(x) = d(1)$.

Example 3.1.14. *Let R be a Euclidean domain and $a, b, c \in R$. If $a \mid bc$ and $(a, b) = 1$, prove that $a \mid c$.*

Solution. Since E.D. $\Rightarrow$ P.I.D., the result follows by Lemma 2.8.5.

Example 3.1.15. *Let R be a Euclidean domain. Prove that*

(*i*) $d(a) = d(-a)\ \forall\ a \neq 0 \in R$.

(*ii*) *If $d(a) = 0$ for $a \neq 0 \in R$, then a is unit in R.*

Solution. (*i*) Since $1 \in R$, we see that

$a \mid -a$ and $-a \mid a \Rightarrow -a = ax$ and $a = -ay$, for some $x, y \in R$.

Now $-a = ax \Rightarrow d(-a) = d(ax) \geq d(a)$, since R is E.D.

$\therefore\ d(-a) \geq d(a)$

Again $a = -ay \Rightarrow d(a) = d(-ay) \geq d(-a) \Rightarrow d(a) \geq d(-a)$.

Hence $d(a) = d(-a)\ \forall\ a \neq 0 \in R$.

(*ii*) For $1 \in R$, $a \neq 0 \in R$, there exist $t, r \in R$ such that

$1 = at + r$, where $r = 0$ or $d(r) < d(a)$.

If $r \neq 0$, then $d(r) < d(a)$ or $d(r) < 0$ ($\because\ d(a) = 0$), which is impossible, as $d(r)$ is a non-negative integer. Thus $r = 0$ and so $1 = at \Rightarrow a \mid 1 \Rightarrow a$ is unit.

Example 3.1.16. *Let a, b be two non-zero elements of a Euclidean domain R. Prove that*

(i) If a and b are associates, then $d(a) = d(b)$.

However, the converse need not be true.

Or

Show by an example that it is possible to find two elements a and b in a Euclidean domain such that $d(a) = d(b)$, but a, b are not associates.

[D.U., 1994]

(ii) If $a \mid b$ and $d(a) = d(b)$, then a and b are associates.

(iii) $d(a) = d(ab)$ iff b is a unit.

Solution. (*i*) Since a and b are associates, $a \mid b$ and $b \mid a$.

(See Example 2.7.4 of chapter 2)

Now $a \mid b \Rightarrow b = ax$, for some $x \in R$

$\Rightarrow d(b) = d(ax) \geq d(a)$, by definition of E.D.

$\Rightarrow d(a) \leq d(b)$

Similarly, $b \mid a \Rightarrow d(b) \leq d(a)$. Hence $d(a) = d(b)$.

However, the converse is not true as shown below :

We know $\mathbf{Z}[i] = \{m + ni : m, n \in \mathbf{Z}\}$ is a E.D., where

$d(m + ni) = m^2 + n^2$.

Let $a = 3 + 4i$, $b = 3 - 4i \in \mathbf{Z}[i]$. Then

$d(a) = d(b) = 9 + 16 = 25$.

If a and b are associates, then $a = ub$ for some unit $u \in \mathbf{Z}[i]$ *i.e.*, $u = \pm 1, \pm i$.

[We know that the units of $\mathbf{Z}[i]$ are $\pm 1, \pm i$.]

Consequently, we have

$3 + 4i = 1(3 - 4i)$ or $3 + 4i = -1(3 - 4i)$

or $3 + 4i = i(3 - 4i)$ or $3 + 4i = -i(3 - 4i)$

The above relations give us

$3 + 4i = 3 - 4i$ or $3 + 4i = -3 + 4i$

or $3 + 4i = 4 + 3i$ or $3 + 4i = -4 - 3i$.

None of these relations is possible. Hence $d(a) = d(b)$, but a and b are not associates.

(*ii*) Consider the ideal $A = (a) = \{ax : x \in R\}$ of R.

We know $a \neq 0 \in A$ and $d(a)$ is minimal.

[See Remark 2 of Theorem 3.1.1]

Since $a \mid b$, $b = ax$, for some $x \in R$.

Since $a \in A$ and A is an ideal of R, $b = ax \in A$.

Since $b \in A$ and $d(b) = d(a)$, so by the minimality of $d(a) = d(b)$, $A = (b)$. Now $a \in A \Rightarrow a \in (b) \Rightarrow a = by$, for some $y \in R \Rightarrow b \mid a$.

Hence $a \mid b$ and $b \mid a \Rightarrow a$ and b are associates.

(*iii*) Let $d(a) = d(ab)$. Then b must be a unit in R, for otherwise, $d(a) < d(ab)$ [see Example 3.1.12], which is contrary to the given hypothesis.

Conversely, let b be a unit in R.

Then $b \mid 1 \Rightarrow 1 = bc$, for some $c \in R$

$\Rightarrow a \,.\, 1 = a(bc)$, since $a \neq 0$ and R is an integral domain

$\Rightarrow a = ab \,.\, c \Rightarrow d(a) = d(ab \,.\, c) \geq d(ab)$, by def. of E.D.

$\Rightarrow d(ab) \leq d(a)$.

By definition of E.D., $d(a) \leq d(ab)$. Hence $d(a) = d(ab)$.

Example 3.1.17. *If $a + bi$ is not a unit of $\mathbf{Z}[i]$, prove that $a^2 + b^2 > 1$.* [D.U., 2000, 1995, 91]

Solution. For each $a + bi \neq 0 \in \mathbf{Z}[i]$, we know

$$d(a + bi) = a^2 + b^2 \geq 1.$$

We know that the only units of $\mathbf{Z}[i]$ are $\pm 1, \pm i$ and

$$d(u) = 1 \ \forall \ u \in \{1, -1, i, -i\} \subset \mathbf{Z}[i].$$

Consequently, $d(x) > 1$ for all non-units $x \in \mathbf{Z}[i]$.

Since $a + bi$ is not a unit, $d(a + bi) > 1$.

Hence $a^2 + b^2 > 1$

Example 3.1.18. *Prove that in a Euclidean ring R, (a, b) can be found as follows :*

$$b = q_0 a + r_1, \text{ where } d(r_1) < d(a)$$

$$a_1 = q_1 r_1 + r_2, \text{ where } d(r_2) < d(r_1)$$

$$r_1 = q_2 r_2 + r_3, \text{ where } d(r_3) < d(r_2)$$

$$\vdots \qquad\qquad \vdots$$

$$r_{n-1} = q_n r_n,$$

and $$r_n = (a, b).$$

Solution. It is clear that a and b are both non-zero elements of R. By definition of E.D., there exist q_0 and $r_1 \in R$, such that

$$b = q_0 a + r_1, \text{ where either } r_1 = 0 \text{ or } d(r_1) < d(a).$$

If $r_1 \neq 0$, then $b = bq + r_1$, where $d(r_1) < d(a)$.

It follows that $(a, b) = (a, r_1)$.

For $a \neq 0$, $r_1 \neq 0 \in R$, there exist $q_2, r_2 \in R$ such that

$a = q_2 r_1 + r_2$, where $d(r_2) < d(r_1)$ (of course, $r_2 \neq 0$).

It follows that $(a, b) = (a, r_1) = (r_2, r_1)$.

For $r_1 \neq 0$, $r_2 \neq 0 \in R$, there exist $q_3, r_3 \in R$ such that

$r_1 = q_3 r_2 + r_3$, where $d(r_3) < d(r_2)$.

It follows that $(a, b) = (a, r_1) = (r_2, r_1) = (r_3, r_2)$ and so on.

Proceeding in a similar manner, we shall obtain

$r_{n-1} = q_n r_n + r_{n+1}$, where $r_{n+1} = 0$.

Consequently, $r_{n-1} = q_n r_n$, where $r_n = (r_{n-1}, r_n)$.

Hence $r_n = (r_{n-1}, r_n) = \ldots = (r_2, r_1) = (a, r_1) = (a, b)$.

Remark. *The technique of this example helps us to find g.c.d. of two elements in Z [i], as explained in the following examples*

Example 3.1.19. *Let $a = 3 + 2i$ and $b = 1 + 3i \in Z[i]$. Find $q, r \in Z[i]$ such that $a = bq + r$, where $d(r) < d(b)$.*

Solution. We have

$$\frac{a}{b} = \frac{3+2i}{1+3i} = \frac{(3+2i)(1-3i)}{(1+3i)(1-3i)} = \frac{9-7i}{10} = \frac{9}{10} - \frac{7}{10}i$$

$$= (1-i) + \frac{1}{10} + \frac{3}{10}i.$$

$$\therefore \quad a = (1-i)(1+3i) + \left(-\frac{1}{10} + \frac{3i}{10}\right)(1+3i)$$

or $$a = (1-i)(1+3i) + (-1).$$

Hence $a = bq + r$, where $q = 1 - i \in Z[i]$, $r = -1 \in Z[i]$ and $d(r) < d(b)$. [$\because d(r) = 1, d(b) = 1 + 9 = 10$]

Example 3.1.20. *If possible, find g.c.d. and l.c.m. of $10 + 11i$ and $8 + i$ in Z [i].* [D.U., 1998]

Solution. We have

$$\frac{10+11i}{8+i} = \frac{(10+11i)(8-i)}{(8+i)(8-i)} = \frac{91+78i}{65} = \frac{7}{5} + \frac{6}{5}i$$

or $$\frac{10+11i}{8+i} = (1+i) + \left(\frac{2}{5} + \frac{1}{5}i\right)$$

or $$10 + 11i = (1+i)(8+i) + \left(\frac{2}{5} + \frac{1}{5}i\right)(8+i)$$

or $$10 + 11i = (1+i)(8+i) + (3+2i), \text{ where } d(3+2i) < d(8+i)$$

or [$\because d(3+2i) = 13, d(8+i) = 65$]

If $r_1 \neq 0$, then $b = q_0 a + r_1$, where $d(r_1) < d(a)$.

It follows that $(a, b) = (a, r_1)$.

For $a \neq 0$, $r_1 \neq 0 \in R$, there exist $q_1, r_2 \in R$ such that

$a = q_1 r_1 + r_2$, where $d(r_2) < d(r_1)$ (of course, $r_2 \neq 0$)

It follows that $(a, b) = (a, r_1) = (r_1, r_2)$.

For $r_1 \neq 0$, $r_2 \neq 0 \in R$, there exist $q_2, r_3 \in R$ such that

$r_1 = q_2 r_2 + r_3$, where $d(r_3) < d(r_2)$.

It follows that $(a, b) = (a, r_1) = (r_1, r_2) = (r_2, r_3)$ and so on.

Proceeding in a similar manner, we shall obtain

$r_{n-1} = q_n r_n + r_{n+1}$, where $r_{n+1} = 0$.

Consequently, $r_{n-1} = q_n r_n$, where $r_n = (r_{n-1}, r_n)$.

Hence $r_n = (r_{n-1}, r_n) = \ldots = (r_1, r_2) = (a, r_1) = (a, b)$.

Remark. *The technique of this example helps us to find g.c.d. of two elements in* $\mathbf{Z}[i]$, *as explained in the following examples*

Example 3.1.19. *Let* $a = 3 + 2i$ *and* $b = 1 + 3i \in \mathbf{Z}[i]$. *Find* $q, r \in \mathbf{Z}[i]$ *such that* $a = bq + r$, *where* $d(r) < d(b)$.

Solution. We have

$$\frac{a}{b} = \frac{3+2i}{1+3i} = \frac{(3+2i)(1-3i)}{(1+3i)(1-3i)} = \frac{9-7i}{10} = \frac{9}{10} - \frac{7}{10}i$$

$$= (1-i) \mathcal{T} \frac{1}{10} + \frac{3}{10}i.$$

$$\therefore \quad a = (1-i)(1+3i) + \left(-\frac{1}{10} + \frac{3i}{10}\right)(1+3i)$$

or $$a = (1-i)(1+3i) + (-1).$$

Hence $a = bq + r$, where $q = 1 - i \in \mathbf{Z}[i]$, $r = -1 \in \mathbf{Z}[i]$ and $d(r) < d(b)$. [$\because d(r) = 1, d(b) = 1 + 9 = 10$]

Example 3.1.20. *If possible, find g.c.d. and l.c.m. of* $10 + 11i$ *and* $8 + i$ *in* $\mathbf{Z}[i]$. [D.U., 1998]

Solution. We have

$$\frac{10+11i}{8+i} = \frac{(10+11i)(8-i)}{(8+i)(8-i)} = \frac{91+78i}{65} = \frac{7}{5} + \frac{6}{5}i$$

or $$\frac{10+11i}{8+i} = (1+i) + \left(\frac{2}{5} + \frac{1}{5}i\right)$$

or $$10 + 11i = (1+i)(8+i) + \left(\frac{2}{5} + \frac{1}{5}i\right)(8+i)$$

or $$10 + 11i = (1+i)(8+i) + (3+2i), \text{ where } d(3+2i) < d(8+i)$$

[$\because d(3+2i) = 13, d(8+i) = 65$]

Now we consider

$$\frac{8+i}{3+2i}=\frac{(8+i)(3-2i)}{(3+2i)(3-2i)}=\frac{26-13i}{13}=2-i$$

or $(8+i)=(2-i)(3+2i)$

Hence $3+2i$ is the g.c.d. of $10+11i$ and $8+i$.

If (a, b) and $[a, b]$, respectively, denote g.c.d. and l.c.m. of a and b in $\mathbf{Z}[i]$, then

$$[a, b]=\frac{ab}{(a, b)}.$$ [See Theorem 2.8.7. Take $u=1$]

Hence l.c.m. of $a=10+11i$, $b=8+i$ is

$$=\frac{(10+11i)(8+i)}{3+2i}=\frac{(69+98i)(3-2i)}{(3+2i)(3-2i)}$$

$$=\frac{403+156i}{13}=31+12i.$$

Example 3.1.21. *Show that* $3+4i$ *and* $4-3i$ *are associates in* $\mathbf{Z}[i]$.

Solution. Clearly, $3+4i=i(4-3i)$, where i is a unit in $\mathbf{Z}[i]$.

By definition, $3+4i$ and $4-3i$ are associates.

It may be noted that g.c.d of $3+4i$ and $4-3i$ is **not** i. Indeed g.c.d. of $3+4i$ and $4-3i$ is $3+4i$ or $4-3i$ (both non-units in $\mathbf{Z}[i]$). Hence $3+4i$ and $4-3i$ **are not co-prime** in $\mathbf{Z}[i]$.

Example 3.1.22. *Find the g.c.d. in* $\mathbf{Z}[i]$ *of* 2 *and* $3+5i$.

[D.U., 1994]

Solution. We have

$$\frac{3+5i}{2}=\frac{3}{2}+\frac{5i}{2}=(1+2i)+\left(\frac{1}{2}+\frac{1}{2}i\right)$$

or $(3+5i)=(1+2i)\,2+(1+i)$, where $d(1+i)<d(2)$.

Now $$\frac{2}{1+i}=\frac{2(1-i)}{(1+i)(1-i)}=\frac{2-2i}{2}=1-i$$

i.e., $2=(1+i)(1-i)$.

Hence $1+i$ is the g.c.d. of 2 and $3+5i$.

Example 3.1.23. *Find the g.c.d. of* $11+7i$ *and* $18-i$ *in* $\mathbf{Z}[i]$.

[D.U., 2000, 1996]

Solution. We have

$$\frac{18-i}{11+7i}=\frac{(18-i)(11-7i)}{(11+7i)(11-7i)}=\frac{191-137i}{170}$$

$$=(1-i)+\left(\frac{21}{170}+\frac{33}{170}i\right).$$

$\therefore$ $$(18-i)=(1-i)(11+7i)+\left(\frac{21}{170}+\frac{33i}{170}\right)(11+7i)$$

or $(18-i)=(1-i)(11+7i)+3i$, where $d(3i)<d(11+7i)$.

Now we consider

$$\frac{11+7i}{3i}=\frac{7}{3}+\frac{11}{3i}=\frac{7}{3}-\frac{11}{3}i=(2-3i)+\left(\frac{1}{3}-\frac{2}{3}i\right)$$

or $$11+7i=(2-3i)\,3i+\left(\frac{1}{3}-\frac{2}{3}i\right)(3i)$$

or $$11+7i=(2-3i)\,3i+(2+i),\ \text{where } d(2+i)<d(3i).$$

Again $$\frac{3i}{2+i}=\frac{3i(2-i)}{(2+i)(2-i)}=\frac{3+6i}{5}=(1+2i)+\left(-\frac{2}{5}-\frac{4}{5}i\right)$$

or $$3i=(1+2i)(2+i)+\left(-\frac{2}{5}-\frac{4}{5}i\right)(2+i)$$

or $$3i=(1+2i)(2+i)-2i,\ \text{where } d(-2i)<d(2+i).$$

Further $$\frac{2+i}{-2i}=-\frac{1}{i}-\frac{1}{2}=-\frac{1}{2}+i$$

or $$2+i=i(-2i)+i,\ \text{where } d(i)<d(-2i).$$

Finally, $$-\frac{2i}{i}=-2 \text{ or } -2i=(-2)\,i.$$

Thus i is the g.c.d. of $11+7i$ and $18-i$, where i is a unit in $\mathbf{Z}[i]$. Hence $11+7i$ and $18-i$ are co-prime elements in $\mathbf{Z}[i]$.

EXERCISES

1. If $a=1+2i$ and $b=3+i\in\mathbf{Z}[i]$, find $t, r\in\mathbf{Z}[i]$ such that $a=tb+r$, where $d(r)<d(b)$. **[Ans.** $t=1, r=-2-2i$**]**
2. Find the g.c.d. of $3+2i$ and $2-3i$ in $\mathbf{Z}[i]$. **[Ans.** i**]**
3. Find the g.c.d. of $3+4i$ and $7-i$ in $\mathbf{Z}[i]$. **[Ans. 1]**
4. Find the g.c.d. of 3 and $4+5i$ in $\mathbf{Z}[i]$. **[Ans.** i**]**

[Hint. Similar to Example 3.1.22**]**

5. Show that $\mathbf{Z}[\sqrt{-2}]=\{m+n\sqrt{-2}: m, n\in\mathbf{Z}\}$ is a Euclidean domain.

[Hint. Take $d(m+n\sqrt{-2})=m^2+2n^2$.**]**

6. Let $a, b, c\in R$, R being a Euclidean domain. If $a\mid c$ and $b\mid c$ and $(a, b)=1$, prove that $ab\mid c$.

[Hint. Let $c=ar_1$, $c=br_2$ and $ax+by=1$. Then

$$c=acx+bcy=abr_2x+abr_1y=ab(r_2x+r_1y).$$ Hence $ab\mid c$.**]**

7. Let R be a Euclidean domain with valuation d. If $a, b\in R$ and $a\mid b$, then a and b are associates if and only if $d(a)=d(b)$. **[D.U., 1993]**

[Hint. See Example 3.1.16 (i, ii)**]**

8. Let R be a Euclidean domain and $a, b\in R$. Prove that a is non-unit in R if and only if $d(ab)>d(b)$. **[D.U., 1993]**

[Hint. See Example 3.1.12.**]**

9. Let R be a Euclidean domain. Show that every non-zero prime ideal $P \neq R$ is a maximal ideal of R. [D.U., 1971]

[**Hint.** See Theorem 2.8.10 and use the fact E.D. $\Rightarrow$ P.I.D.]

10. Let R be a Euclidean ring. Let a and b be two non-zero elements in R. Prove that

(*i*) If b is a unit in R, then $d(ab) = d(a)$.

(*ii*) If b is not a unit in R, then $d(ab) > d(a)$.

[**Hint.** See Examples 3.1.12 and 3.1.16 (*iii*)]

3.2 Polynomial Rings

Let R be a ring. The **ring of polynomials** *in the indeterminate x, denoted as $R[x]$, is defined as the set*

$$R[x] = \{a_0 + a_1x + a_2x^2 + \ldots + a_nx^n : a_i \in R \text{ and } n \geq 0 \in \mathbf{Z}\}.$$

We shall give $R[x]$ a *ring structure* as follows :

Let $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n \in R[x]$,

and $g(x) = b_0 + b_1x + b_2x^2 + \ldots + b_mx^m \in R[x]$.

We define :

Equality. $f(x) = g(x)$ iff $a_i = b_i$ for each i.

Sum. $f(x) + g(x) = c_0 + c_1x + c_2x^2 + \ldots + c_ix^i + \ldots,$ ...(A)

where $c_i = a_i + b_i$, for each i.

Product. $f(x)\,g(x) = c_0 + c_1x + c_2x^2 + \ldots + c_ix^i + \ldots,$ ...(B)

where $c_0 = a_0b_0$, $c_1 = a_0b_1 + a_1b_0$, $c_2 = a_0b_2 + a_1b_1 + a_2b_0, \ldots,$

$$c_i = a_0b_i + a_1b_{i-1} + a_2b_{i-2} + \ldots + a_{i-1}b_1 + a_ib_0.$$

(Notice that the sum of the suffixes of each term of the above expression is i).

It is easy to verify that $R[x]$ *is a ring w.r.t. the compositions given by* (A) *and* (B), where the additive identity is $0 = 0 + 0x + 0x^2 + \ldots$, the additive inverse of $f(x)$ is $-f(x) = -a_0 - a_1x - a_2x^2 - \ldots - a_nx^n$.

The ring $R[x]$ is also called the *ring of polynomials over R* and the elements of $R[x]$ are called *polynomials over R*. It is easy to verify that

(*i*) *If R is commutative, then $R[x]$ is also commutative.*

(*ii*) *If R has unity 1, then $R[x]$ also has unity 1, where* $1 = 1 + 0x + 0x^2 + \ldots$

(*iii*) *If F is a field, then $F[x]$ is a commutative ring with unity. However, $F[x]$ is not a field.*

For example, $f(x) = 1 \,.\, x \in F[x]$ has no multiplicative inverse in $F[x]$, for if $g(x) = b_0 + b_1x + b_2x^2 + \ldots + b_mx^m \in F[x]$ is the multiplicative inverse of $f(x)$, then

$$f(x)\,g(x) = 1 \text{ } i.e., \; c_0 + c_1x + c_2x^2 + \ldots = 1 + 0x + 0x^2 + \ldots$$

$\Rightarrow \quad c_0 = 1, c_1 = 0, c_2 = 0, \ldots$

$\Rightarrow a_0 b_0 = 1 \Rightarrow 0 \,.\, b_0 = 1 \Rightarrow 0 = 1$, *a contradiction.*

Indeed $F[x]$ *is an integral domain.* [See Cor. 4 of Theorem 3.2.1]

Definition. (Degree of a Polynomial)

Let $f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n \in R[x]$.

We say that $f(x)$ is a *non-zero polynomial*, if at least one of the coefficients $a_0, a_1, \ldots, a_n$ is not zero.

We say that $f(x)$ *has degree* n, if $a_n \neq 0$.

We write it as $deg\, f(x) = n$ or $deg\, f = n$.

In other words, the **degree** *of* $f(x)$ *is the largest integer* i *for which the* i*th coefficient of* $f(x)$ *is not zero. Consequently, if* $deg\, f(x) = n$, *then*

$$a_n \neq 0 \text{ and } a_i = 0 \text{ for } i > n.$$

We say that *degree of* $f(x)$ *is zero, if* $a_0 \neq 0$ and $a_i = 0$ for $i > 0$.

In this case, $f(x)$ is called a **constant polynomial.** Thus a polynomial of the form $f(x) = a_0$, where $a_0 \neq 0 \in R$; is a *constant polynomial* in $R[x]$. *We do not define the degree of the zero polynomial.* From the above discussion, we conclude that

If $f(x) \neq 0 \in R[x]$, *then the degree of* $f(x)$ *is a non-negative integer.*

Theorem 3.2.1. *Let* $f(x)$ *and* $g(x)$ *be two non-zero polynomials in* $R[x]$, R *being any ring.*

(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*

$$deg\,(f(x)\, g(x)) = deg\, f(x) + deg\, g(x).$$

Proof. Let $f(x) = a_0 + a_1 x + \ldots + a_n x^n \in R[x], a_n \neq 0$

and $g(x) = b_0 + b_1 x + \ldots + b_m x^m \in R[x], b_m \neq 0.$

Then $deg\, f(x) = n,\ deg\ g(x) = m.$

Further $a_i = 0$, for $i > n$ and $b_j > 0$, for $j > m$ ...(1)

(*i*) We have $f(x) + g(x) = c_0 + c_1 x + \ldots + c_i x^i + \ldots,$

where $c_i = a_i + b_i$, for each i

For $i > \max\,(deg\, f(x), deg\, g(x)) = \max\,(n, m)$, we have

$i > n$ and $i > m$. So by (1), $a_i = 0$ and $b_i = 0$

$\Rightarrow c_i = 0$, for $i > \max\,(n, m)$.

Hence $deg\,(f(x) + g(x)) \leq \max\,(n, m) = \max\,(deg\, f(x), deg\, g(x))$.

(*ii*) We have $f(x)\, g(x) = c_0 + c_1 x + \ldots + c_i \,.\, x^i + \ldots,$ where

$$c_i = a_0 b_i + a_1 b_{i-1} + \ldots + a_i b_0 = \sum_{p+q=i} a_p b_q \,.$$

If $i > n+m$, then for any two non-negative integers p and q satisfying $p+q=i$, either $p>n$ or $q>m$. So by (1), either $a_p=0$ or $b_q=0$. In each case, we have $a_p b_q = 0$

$$\Rightarrow \quad c_i = \sum_{p+q=i} a_p b_q = 0, \text{ for } i > n+m.$$

Hence $deg\,(f(x)\,g(x)) \le n+m = deg\,f(x) + deg\,g(x)$.

(iii) Since R is an integral domain, so $a_n \neq 0,\ b_m \neq 0 \in R \Rightarrow a_n b_m \neq 0$

$\Rightarrow c_{n+m} = a_n b_m \neq 0$

$\Rightarrow deg\,(f(x))\,g(x)) \ge n+m.$

By part *(ii)*, $deg\,(f(x)\,g(x)) \le n+m.$

Hence $deg\,(f(x)\,g(x)) = n+m = deg\,f(x) + deg\,g(x)$.

Corollary 1. *If $f(x), g(x)$ are two non-zero polynomials in $F[x]$ (F being a field), then*

$$deg\,(f(x)\,g(x)) = deg\,f(x) + deg\,g(x).$$

Proof. Since every field is an integral domain, the result follows by part *(iii)*.

Corollary 2. *If $f(x), g(x)$ are two non-zero polynomials in $F[x]$ (F being a field), then*

(i) $deg\,f(x) \le deg\,(f(x)\,g(x))$, *(ii)* $deg\,g(x) \le deg\,(f(x)\,g(x))$.

Proof. By corollary 1, we have

$$deg\,(f(x)\,g(x)) = deg\,f(x) + deg\,g(x)$$
$$\ge deg\,f(x), \text{ since } deg\,g(x) \ge 0.$$

$\therefore \quad deg\,f(x) \le deg\,(f(x)\,g(x))$.

Similarly, $deg\,g(x) \le deg\,(f(x)\,g(x))$.

Corollary 3. *If R is an integral domain, then $R[x]$ is an integral domain.*

Proof. Since R is commutative, $R[x]$ is a commutative ring. Now we show that $R[x]$ has no zero divisors. Let $f(x) \neq 0,\ g(x) \neq 0 \in R[x]$; where $f(x) = a_0 + a_1x + ... + a_nx^n,\ g(x) = b_0 + b_1x + ... + b_mx^m$; $a_n \neq 0,\ b_m \neq 0 \in R$.

Then $f(x)\,g(x) = c_0 + c_1x + ... + c_{n+m}x^{n+m}$, where

$c_{n+m} = a_n b_m \neq 0$, since R is an integral domain.

Thus $f(x)\,g(x) \neq 0 \in R[x]$ and so $R[x]$ is an integral domain.

Corollary 4. *If F is a field, $F[x]$ is an integral domain .*

Proof. Since every field is an integral domain, the result follows by Cor. 3.

Theorem 3.2.2. *If R is an integral domain with unity, then units of R and $R[x]$ are same.*

Solution. Let a_0 be a unit of R. Then $a_0 \mid 1$ *i.e.*, there exists some $b_0 \in R$ such that $a_0 b_0 = 1$

Let $f(x) = a_0 + 0x + 0x^2 + \ldots$, $g(x) = b_0 + 0x + 0x^2 + \ldots$

Then $f(x), g(x) \in R[x]$ and $f(x)\,g(x) = a_0 b_0 + 0x + 0x^2 + \ldots$

or $f(x)\,g(x) = 1 \Rightarrow f(x) \mid 1$ in $R[x] \Rightarrow f(x)$ is a unit in $R[x]$.

Hence $a_0 = f(x)$ is a unit in $R[x]$.

Conversely, let $f(x)$ be a unit of $R[x]$. Then there exists some $g(x) \in R[x]$ such that $f(x)\,g(x) = 1 = 1 + 0x + 0x^2 + \ldots$ ...(1)

$\Rightarrow deg\,(f(x)\,g(x)) = deg\,(1 + 0x + 0x^2 + \ldots) = 0$

$\Rightarrow deg\,f(x) + deg\,g(x) = 0$, since R is an I.D. [Theorem 3.2.1 (*iii*)]

$\Rightarrow deg\,f(x) = 0$ and $deg\,g(x) = 0$

$\Rightarrow f(x)$ and $g(x)$ are constant polynomials, say

$f(x) = \alpha\ (\alpha \neq 0 \in R)$, $g(x) = \beta\ (\beta \neq 0 \in R)$

$\Rightarrow \alpha\beta = 1$, by (1)

$\Rightarrow \alpha \mid 1$ in R.

Hence $f(x) = \alpha$ is a unit of R.

Ex. *Let R be an integral domain with unity. Show that units in $R[x]$ are units in R. Find out the units of $\mathbf{Z}[x]$, where $\mathbf{Z}$ is the ring of integers.* [D.U., 1997]

Solution. The units in $R[x]$ are units in R. [See the converse part of Theorem 3.2.2]. It follows that the units of $\mathbf{Z}[x]$ are ± 1, since the units of $\mathbf{Z}$ are ± 1.

Theorem 3.2.3. *If R is an integral domain with unity, then any irreducible element of R is an irreducible element of $R[x]$.*

Proof. Let a be any irreducible element of R. Let, if possible, a be not an irreducible element of $R[x]$. Then we can write

$a = f(x)\,g(x)$, where $f(x), g(x) \in R[x]$ ...(1)

and $f(x), g(x)$ are both non-unit elements of $R[x]$. Since units of R and $R[x]$ are same [Theorem 3.2.2.], both $f(x)$ and $g(x)$ cannot be in R, for otherwise a will not be an irreducible element of R, a contradiction. We suppose that $f(x) \notin R$. From (1), we have

$deg\,a = deg\,(f(x)\,g(x) = deg\,f(x) + deg\,g(x)$,

since R is an integral domain

$\Rightarrow 0 = deg\,f(x) + deg\,g(x)$ $(\because a \in R \Rightarrow deg\,a = 0)$

$\Rightarrow deg\,f(x) = 0$ and $deg\,g(x) = 0$

Now $deg\,f(x) = 0 \Rightarrow f(x)$ is a constant polynomial of the form $f(x) = \alpha$, where $\alpha \neq 0 \in R \Rightarrow f(x) \in R$, which is a contradiction. Hence a is an irreducible element of $R[x]$.

EXAMPLES

Example 3.2.1. *Give examples of two polynomials $f(x), g(x)$ in $R[x]$ such that*

(*i*) $deg\,(f(x) + g(x)) < max\,(deg\,f(x), deg\,g(x))$.

(*ii*) $deg\,(f(x)\,g(x)) < deg\,f(x) + deg\,g(x)$.

Solution. (*i*) Let

$$f(x) = 2 + 3x + 4x^2 \in \mathbf{Z}[x],\ g(x) = 1 + 2x - 4x^2 \in \mathbf{Z}[x].$$

Then $deg\, f(x) = deg\, g(x) = 2 \Rightarrow \max(deg\, f(x), deg\, g(x)) = 2.$

We have $f(x) + g(x) = 3 + 5x \Rightarrow deg\,(f(x) + g(x)) = 1.$

Hence $deg\,(f(x) + g(x)) < \max(deg\, f(x), deg\, g(x))$.

(*ii*) Let $R = \mathbf{Z}_4 = \{0, 1, 2, 3\}$ be the ring of integers modulo 4.

Let $f(x) = 1 + 2x^2,\ g(x) = 3 + x + 2x^3 \in R[x]$.

Then $deg\, f(x) = 2$ and $deg\, g(x) = 3$. We have

$$f(x)\, g(x) = 3 + x + 6x^2 + 4x^3 + 4x^5 = 3 + x + 2x^2 + 0x^3 + 0x^5$$

$$= 3 + x + 2x^2 \Rightarrow deg\,(f(x)\, g(x)) = 2.$$

Hence $deg\,(f(x)\, g(x)) < deg\, f(x) + deg\, g(x) = 5$.

Note that $\mathbf{Z}_4$ is not an integral domain.

Example 3.2.2. *Find the sum and product of the polynomials*

$$f(x) = 4x - 5,\ g(x) = 2x^2 - 4x + 2 \text{ in } \mathbf{Z}_8[x].$$ [D.U., 2000]

Solution. We know $\mathbf{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$ is the ring of integers modulo 8. We have

$$f(x) + g(x) = 4x - 5 + 2x^2 - 4x + 2 = 2x^2 - 3,$$

and $$f(x)\, g(x) = (-5 + 4x)(2 - 4x + 2x^2), \text{ where}$$

$$a_0 = -5,\ a_1 = 4,\ b_0 = 2,\ b_1 = -4,\ b_2 = 2.$$

$\therefore$ $c_0 = a_0 b_0 = -10 = -2$ in $\mathbf{Z}_8$

$c_1 = a_0 b_1 + a_1 b_0 = 20 + 8 = 28 = 4$ in $\mathbf{Z}_8$

$c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0 = -10 - 16 + 0 = -26 = -2$ in $\mathbf{Z}_8$

$c_3 = a_0 b_3 + a_1 b_2 + a_2 b_1 + a_3 b_0 = a_1 b_2 = 8 = 0$ in $\mathbf{Z}_8$.

Hence $f(x)\, g(x) = c_0 + c_1 x + c_2 x^2 + c_3 x^3 = -2 + 4x - 2x^2$.

Example 3.2.3. *Find the sum and product of the polynomials:*

$$f(x) = 1 + 3x,\ g(x) = 4 + 5x + 2x^3 \text{ in } \mathbf{Z}_6[x].$$

Please try yourself.

[**Ans.** Sum $= 5 + 2x + 2x^3$, Product $= 4 + 5x + 3x^2 + 2x^3$]

Example 3.2.4. *Show that every ring R can be imbedded in the polynomial ring R [x].*

Or

Show that every ring R is isomorphic to a subring of R [x].

Solution. Define a mapping $\theta : R \to R[x]$ as

$$\theta(a) = a + 0x + 0x^2 + \ldots,\ \forall\ a \in R.$$

Then θ is one-to-one, since for any $a, b \in R$,

$$\theta(a) = \theta(b) \Rightarrow a + 0x + 0x^2 + \ldots = b + 0x + 0x^2 + \ldots \Rightarrow a = b.$$

Now we show that θ is a homomorphism. We have

$$\theta(a+b) = (a+b) + 0x + 0x^2 + \ldots$$
$$= (a + 0x + 0x^2 + \ldots) + (b + 0x + 0x^2 + \ldots)$$
$$= \theta(a) + \theta(b)$$

and
$$\theta(ab) = ab + 0x + 0x^2 + \ldots$$
$$= (a + 0x + 0x^2 + \ldots)(b + 0x + 0x^2 + \ldots) = \theta(a)\,\theta(b).$$

Hence θ is an isomorphism of R into $R[x]$ *i.e.*, R is imbedded in $R[x]$. It follows that

$\theta : R \to \theta(R)$ is an onto isomorphism, when $\theta(R)$ is a subring of $R[x]$. Hence R is isomorphic to a subring of $R[x]$.

Example 3.2.5. *Show that a ring R is an integral domain if and only if $R[x]$ is an integral domain.*

Solution. R is an I.D. $\Rightarrow R[x]$ is an I.D. [Cor. 3 of Theorem 3.2.1]

Conversely, let $R[x]$ be an integral domain. By Example 3.2.4, $R \approx \theta(R)$, where $\theta(R)$ is a subring of $R[x]$. It follows that $\theta(R) \approx R$. Since subring of an integral domain is an integral domain, $\theta(R)$ is an integral domain. Since isomorphic image of an integral domain is an integral domain, so $\theta(R) \approx R$ implies that R is an integral domain.

Example 3.2.6. *If a ring R has no proper zero divisors, then prove that $R[x]$ has no proper zero divisors.* [D.U., 1999]

Solution. Let $f(x) = a_0 + a_1x + \ldots + a_nx^n \neq 0 \in R[x]$, $a_n \neq 0 \in R$

and
$$g(x) = b_0 + b_1x + \ldots + b_mx^m \neq 0 \in R[x],\ b_m \neq 0 \in R.$$

$\therefore$ $\deg f(x) = n$, $\deg g(x) = m$;

and
$$a_i = 0, \text{ for each } i \geq n+1 \text{ and } b_j = 0, \text{ for each } j \geq m+1. \quad \ldots(1)$$

We have $f(x)\,g(x) = c_0 + c_1x + c_2x^2 + \ldots$,

where
$$c_{n+m} = a_0\,b_{m+n} + a_1\,b_{m+n-1} + \ldots + a_{n-1}\,b_{m+1} + a_n\,b_m$$
$$+ a_{n+1}\,b_{m-1} + \ldots + a_{n+m}\,b_0 = a_n\,b_m, \text{ by (1)}$$

$\therefore$ $c_{n+m} = a_n\,b_m \neq 0$, since R has no proper zero divisors.

Hence $f(x)\,g(x) \neq 0$ and so $R[x]$ has no proper zero divisors.

Example 3.2.7. *Let R be a commutative ring with no non-zero nilpotent elements. If $f(x) = a_0 + a_1x + \ldots + a_m x^m$ in $R[x]$ is a zero divisor, prove that there is an element $b \neq 0$ in R such that*

$$ba_0 = ba_1 = \ldots = ba_m = 0.$$

Solution. Since R has no non-zero nilpotent elements, so for all positive integers n, $a^n = 0 \Rightarrow a = 0\ \forall\ a \in R$. ...(1)

Since $f(x) \in R[x]$ is a zero divisor, there exists some $g(x) \in R[x]$ such that

$$f(x)\,g(x) = 0.$$

Let
$$g(x) = b_0 + b_1x + \ldots + b_nx^n \in R[x].$$

We may suppose that $a_m \neq 0$ and $b_n \neq 0 \in R$. We have

$$(a_0 + a_1x + ... + a_{m-1}x^{m-1} + a_mx^m)(b_0 + b_1x + ... + b_{n-1}x^{n-1} + b_nx^n) = 0 + 0x + 0x^2 + ...$$

It follows that

$$a_mb_n = 0,\ a_{m-1}b_n + a_mb_{n-1} = 0,\ ...,\ a_0b_1 + a_1b_0 = 0,\ a_0b_0 = 0$$

We have $(a_{m-1}b_n + a_mb_{n-1})\,b_n = 0 \,.\, b_n = 0$

or $a_{m-1}b_n^2 = 0$, since R is commutative and $a_mb_n = 0$.

Similarly, $a_{m-2}b_n^3 = 0$, ..., $a_1b_n^m = 0$ and $a_0b_n^{m+1} = 0$.

Let $b = b_n^{m+1}$. Then $b \neq 0 \in R$, for $b = 0 \Rightarrow b_n^{m+1} = 0 \Rightarrow b_n = 0$ (by (1)), which is a contradiction.

We have $a_0b = 0$.

Now $a_1b = a_1b_n^{m+1} = (a_1b_n^m)\,b_n = 0 \,.\, b_n = 0$,

.....

$$a_{m-1}b = a_{m-1}b_n^{m+1} = (a_{m-1}b_n^2)(b_n^{m-1}) = 0 \,.\, b_n^{m-1} = 0,$$

$$a_mb = a_mb_n^{m+1} = (a_mb_n)(b_n^m) = 0 \,.\, b_n^m = 0.$$

$\therefore$ $a_0b = a_1b = ... = a_mb = 0$

Hence $ba_0 = ba_1 = ... = ba_m = 0$, since R is commutative.

Remark. *The above problem can also be done by dropping the assumption that R has no non-zero nilpotent elements as proved below:*

Example 3.2.8. *Let R be a commutative ring. If $f(x) = a_0 + a_1x + ... + a_mx^m$ in $R[x]$ is a zero divisor, prove that there is an element $b \neq 0$ in R such that*

$$ba_0 = ba_1 = ... = ba_m = 0.$$

Solution. Since $f(x) \in R[x]$ is a zero divisor, there exists some $g(x) \in R[x]$ of *least positive degree* such that ...(1)

$$f(x)\,g(x) = 0.$$

It means that for all polynomials $h(x) \in R[x]$ with $\deg h(x) < \deg g(x)$ and satisfying $f(x)\,h(x) = 0$, then $h(x) = 0$. ...(2)

Let $g(x) = b_0 + b_1x + ... + b_nx^n \in R[x]$.

We may suppose that $a_m \neq 0$ and $b_n \neq 0 \in R$. We have

$$(a_0 + a_1x + ... + a_{m-1}x^{m-1} + a_mx^m)(b_0 + b_1x + ... + b_{n-1}x^{n-1} + b_nx^n) = 0 + 0x + 0x^2 + ... \quad ...(2)$$

Let $h(x) = a_m\,g(x) = a_mb_0 + a_mb_1x + ... + a_mb_{n-1}x^{n-1}$ $(\because a_mb_n = 0)$

$\Rightarrow$ $\deg h(x) \leq n - 1 < \deg g(x)$ and $f(x)\,h(x) = f(x)\,(a_m\,g(x))$

i.e., $f(x)\,h(x) = a_m\,(f(x)\,g(x))$, since R is commutative.

$\therefore$ $f(x)\, h(x) = 0$, (by (1)) and $deg\, h(x) < deg\, g(x) = n$.

In view of (2), it follows that, $h(x) = 0$ *i.e.*, $a_m\, g(x) = 0$.

From (2), $a_{m-1}\, b_n + a_m\, b_{n-1} = 0$

$\Rightarrow (a_{m-1}\, b_n + a_m\, b_{n-1})\, g(x) = 0\, .\, g(x)$

$\Rightarrow b_n\, (a_{m-1}\, g(x)) + b_{n-1}\, (a_m\, g(x)) = 0$, since R is commutative

$\Rightarrow b_n\, (a_{m-1}\, g(x)) = 0$, as $a_m\, g(x) = 0$

$\Rightarrow a_{m-1}\, g(x) = 0$, since $b_n \neq 0$. Again, from (2), we obtain

$$a_{m-2}\, b_n + a_{m-1}\, b_{n-1} + a_m\, b_{n-2} = 0 \Rightarrow a_{m-2}\, g(x) = 0,$$

since $a_m\, g(x) = 0$ and $a_{m-1}\, g(x) = 0$.

Proceeding in the similar manner, we obtain

$$a_m\, g(x) = 0,\ a_{m-1}\, g(x) = 0,\ \ldots,\ a_1\, g(x) = 0,\ a_0\, g(x) = 0.$$

In particular,

$$a_m\, b_n = 0,\ a_{m-1}\, b_n = 0,\ \ldots,\ a_1 b_n = 0,\ a_0\, b_n = 0\ ;\ \text{where } b_n \neq 0.$$

Taking $b = b_n \neq 0 \in R$, and since R is commutative, we get

$$ba_0 = ba_1 = \ldots = ba_m = 0.$$

Theorem 3.2.4. (Division Algorithm)

If $f(x)$ and $g(x)$ are two non-zero polynomials in $F[x]$ (F being a field), then there exist two polynomials $t(x)$ and $r(x)$ in $F[x]$ such that

$$f(x) = t(x)\, g(x) + r(x),$$

where $r(x) = 0$ or $deg\, r(x) < deg\, g(x)$.

Proof. Suppose that $deg\, f(x) < deg\, g(x)$.

Taking $t(x) = 0$ and $r(x) = f(x)$, we obtain

$$f(x) = t(x)\, g(x) + r(x), \text{ where } deg\, r(x) < deg\, g(x).$$

Hence the result is true in this case.

We now discuss the case when $deg\, f(x) \geq deg\, g(x)$.

Let $$f(x) = a_0 + a_1 x + \ldots + a_m x^m \in F[x],\ a_m \neq 0 \in F$$

and $$g(x) = b_0 + b_1 x + \ldots + b_n x^n \in F[x],\ b_n \neq 0 \in F.$$

Then $deg\, f(x) = m$, $deg\, g(x) = n$ and $m \geq n$.

We shall prove the result by induction on $m = deg\, f(x)$.

If $m = 0$ (and of course $n = 0$), then $f(x) = a_0$ and $g(x) = b_0$, where $a_0 \neq 0 \in F$ and $b_0 \neq 0 \in F$. We can write

$$a_0 = (a_0\, b_0^{-1})\, b_0 \text{ } i.e., f(x) = t(x)\, g(x) + r(x),$$

where $$t(x) = a_0\, b_0^{-1} \text{ and } r(x) = 0.$$

Thus the result is true for $m = 0$. Suppose that the result is true for all non-zero polynomials in $F[x]$ of degree less than m (Induction Hypothesis).

Let $$f_1(x) = f(x) - a_m\, b_n^{-1}\, x^{m-n}\, g(x). \qquad \ldots(1)$$

[Notice that $b_n \neq 0 \in F \Rightarrow b_n^{-1} \in F$ and $m \geq n \Rightarrow m - n \geq 0$]

We have $f_1(x) = (a_0 + a_1 x + \ldots + a_{m-1} x^{m-1} + a_m x^m)$
$- a_m b_n^{-1} x^{m-n} (b_0 + b_1 x + \ldots + b_{n-1} x^{n-1} + b_n x^n)$
$= (a_0 + a_1 x + \ldots + a_{m-1} x^{m-1} + a_m x^m)$
$- (a_m b_n^{-1} b_0 x^{m-n} + \ldots + a_m b_n^{-1} b_{n-1} x^{m-1} + a_m x^m)$

It follows that $deg\, f_1(x) \leq m - 1 < m$.

By induction hypothesis, there exist polynomials $t_1(x)$ and $r(x)$ in $F[x]$ such that

$$f_1(x) = t_1(x)\, g(x) + r(x), \quad \ldots(2)$$

where $r(x) = 0$ or $deg\, r(x) < deg\, g(x)$.

Using (1) in (2), we get

$$f(x) - a_m b_n^{-1} x^{m-n} g(x) = t_1(x)\, g(x) + r(x)$$

or $$f(x) = \{t_1(x) + a_m b_n^{-1} x^{m-n}\}\, g(x) + r(x).$$

Hence $f(x) = t(x)\, g(x) + r(x)$, where

$$t(x) = t_1(x) + a_m b_n^{-1} x^{m-n} \in F[x]$$

and $r(x) = 0$ or $deg\, r(x) < deg\, g(x)$.

This completes the induction and the result is proved.

Theorem 3.2.5. *If F is a field, then $F[x]$ is a Euclidean domain.* [D.U., 1994]

Proof. Since every field is an integral domain, F is an integral domain and so $F[x]$ is an integral domain. [Cor. 3 of Theorem 3.2.1].

Further for any two non-zero polynomials $f(x)$ and $g(x)$ in $R[x]$, we have

$deg\,(f(x)\, g(x)) = deg\, f(x) + deg\, g(x) \geq deg\, f(x)$, since $deg\, g(x) \geq 0$. (See Cor. 1 of Theorem 3.2.1)

$$\therefore \quad deg\, f(x) \leq deg\,(f(x)\, g(x)). \quad \ldots(1)$$

We define the Euclidean valuation d on $F[x]$ as follows :

$$d(f) \equiv d(f(x)) = deg\, f(x), \ \forall\, f(x) \neq 0 \in F[x]. \quad \ldots(2)$$

Then $d(f)$ is a non-negative integer, since $deg\, f(x)$ is so.

From (1) and (2), we see that

$$d(f) \leq d(fg)\ \forall\, f \neq 0,\ g \neq 0 \in F[x].$$

By Theorem 3.2.4, for $f(x) \neq 0$, $g(x) \neq 0 \in F[x]$, there exist $t(x)$, $r(x)$ in $F[x]$ such that $f(x) = t(x)\, g(x) + r(x)$, where

$$r(x) = 0 \text{ or } deg\, r(x) < deg\, g(x).$$

$$\therefore \quad f = tg + r, \text{ where } r = 0 \text{ or } d(r) < d(g).$$

Hence $F[x]$ is a Euclidean domain.

Theorem 3.2.6. *If F is a field, $F[x]$ is a principal ideal domain.*

Proof. Since $F[x]$ is a Euclidean domain and further every Euclidean domain is a principal ideal domain, $F[x]$ is a P.I.D.

Remark. It may be observed that any ideal A of $F[x]$ is expressible as $A = \langle p(x) \rangle$, for some $p(x) \in A$ *i.e.*,

$$A = \langle p(x) \rangle = \{p(x) f(x) : f(x) \in F[x]\}.$$

In particular, $\langle x \rangle = \{x f(x) : f(x) \in F[x]\}$.

Theorem 3.2.7. *The ideal $A = \langle p(x) \rangle$ in $F[x]$ is a maximal ideal if and only if $p(x)$ is an irreducible element of $F[x]$.*

Proof. The result follows by Theorem 3.2.6 and Theorem 2.8.9.

Corollary. $\dfrac{F[x]}{\langle p(x) \rangle}$ *is a field if and only if $p(x)$ is an irreducible element of $F[x]$.*

Proof. Since $F[x]$ is a commutative ring with unity, the corollary follows by Theorem 3.2.7. and Theorem 2.6.1.

EXAMPLES

Example 3.2.9. *Show that $\langle x+2 \rangle$ is a maximal ideal of $\mathbf{Q}[x]$ and hence $\dfrac{\mathbf{Q}[x]}{\langle x+2 \rangle}$ is a field.*

Solution. By Theorem 3.2.6, $\mathbf{Q}[x]$ is a P.I.D. We have $\langle x+2 \rangle = \{(x+2) f(x) : f(x) \in \mathbf{Q}[x]\}$. By virtue of Theorem 3.2.7, $\langle x+2 \rangle$ is a maximal ideal of $\mathbf{Q}[x]$, if we prove that $x+2$ is an irreducible element of $\mathbf{Q}[x]$. Let $x+2 = f(x)\, g(x)$, where $f(x), g(x) \in \mathbf{Q}[x]$. ...(1)

Then $deg\,(f(x)\, g(x)) = deg\,(x+2) = 1$

or $deg\, f(x) + deg\, g(x) = 1$.

[See Cor. 1 of Theorem 3.2.1.]

This gives us two cases.

Case I. $deg\, f(x) = 0$ and $deg\, g(x) = 1$.

Case II. $deg\, f(x) = 1$ and $deg\, g(x) = 0$.

In case I, we may take

$$f(x) = a_0 \neq 0 \in \mathbf{Q} \text{ and } g(x) = b_0 + b_1 x\,;\, b_0 \in \mathbf{Q},\, b_1 \neq 0 \in \mathbf{Q}.$$

Putting in (1), we get

$$x+2 = a_0 (b_0 + b_1 x)$$

$$\Rightarrow \quad a_0 b_0 = 2 \text{ and } a_0 b_1 = 1,\ a_0 \neq 0,\ b_1 \neq 0 \in \mathbf{Q}.$$

Now $a_0 b_1 = 1 \Rightarrow a_0 \mid 1 \Rightarrow f(x) = a_0$ is a unit.

Thus $x+2$ is an irreducible element of $\mathbf{Q}[x]$.

Similarly, in case II we can prove that $g(x)$ is a unit and so $x+2$ is an irreducible element of $\mathbf{Q}[x]$. Hence $\langle x+2 \rangle$ is a maximal ideal of $\mathbf{Q}[x]$. Since $\mathbf{Q}[x]$ is a commutative ring with unity, $\dfrac{\mathbf{Q}[x]}{\langle x+2 \rangle}$ is a field.

[Theorem 2.6.1.]

Example 3.2.10. *Show that* $\langle x+1 \rangle$ *is a maximal ideal of* $Q[x]$ *and that* $\dfrac{Q[x]}{\langle x+1 \rangle}$ *is a field.*

Please try yourself.

Example 3.2.11. *If* R *is a ring, prove that* $\dfrac{R[x]}{\langle x \rangle} \approx R$, $\langle x \rangle$ *is the ideal generated by* x. [D.U., 1997]

Solution. We have

$$\langle x \rangle = \{x\, p(x) : p(x) \in R[x]\}.$$

We define a mapping

$$\theta : R[x] \to R \text{ as } \theta(f(x)) = \theta(a_0 + a_1 x + \ldots + a_n x^n) = a_0. \quad \ldots(1)$$

Obviously, θ is onto. Now we show that θ is a homomorphism.

Let $f(x) = a_0 + a_1 x + \ldots + a_n x^n \in R[x]$,

and $g(x) = b_0 + b_1 x + \ldots + b_m x^m \in R[x]$.

Then $f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + \ldots$,

and $f(x)\, g(x) = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + \ldots$

From (1), we have

$$\theta(f(x) + g(x)) = a_0 + b_0 = \theta(f(x)) + \theta(g(x)),$$

$$\theta(f(x)\, g(x)) = a_0 b_0 = \theta(f(x))\, \theta(g(x)).$$

Thus θ is a homomorphism of $R[x]$ onto R.

By Fundamental theorem of homomorphism, we can write

$$\frac{R[x]}{Ker\,\theta} \approx R. \quad \ldots(2)$$

Let $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ be an arbitrary element of $Ker\,\theta$.

Then $f(x) \in Ker\,\theta \Leftrightarrow \theta(f(x)) = 0 \Leftrightarrow a_0 = 0$

$\Leftrightarrow f(x) = a_1 x + a_2 x^2 + \ldots + a_n x^n$

$\Leftrightarrow f(x) = x(a_1 + a_2 x + \ldots + a_n x^{n-1})$.

$\Leftrightarrow f(x) \in \langle x \rangle \Leftrightarrow Ker\,\theta = \langle x \rangle$.

Putting in (2), we get $\dfrac{R[x]}{\langle x \rangle} \approx R$.

Example 3.2.12. *If* R *is a commutative ring with unity and* A *is an ideal of* R, *prove that*

$$\frac{R[x]}{A[x]} \approx \frac{R}{A}[x].$$

Deduce that if A *is a prime ideal of* R, *then* $A[x]$ *is a prime ideal of* $R[x]$. [D.U., 1992]

Solution. Since A is an ideal of R, the quotient ring R/A is a commutative ring with unity, where

$$\frac{R}{A} = \{\bar{r} = r + A : r \in R\}.$$

It follows that $\frac{R}{A}[x]$ is also a commutative ring with unity.

We define a mapping

$$\theta : R[x] \to \frac{R}{A}[x] \text{ as}$$

$$\theta(f(x)) = \theta(r_0 + r_1 x + \ldots + r_n x^n) = \bar{r}_0 + \bar{r}_1 x + \ldots + \bar{r}_n x^n. \quad \ldots(1)$$

(Here $\bar{r}_i = r_i + A,\ r_i \in R$)

We shall prove that θ is a homomorphism.

Let $f(x) = r_0 + r_1 x + \ldots + r_n x^n \in R[x]$,

and $g(x) = s_0 + s_1 x + s_m x^m \in R[x]$.

Then $f(x) + g(x) = r_0 + s_0 + (r_1 + s_1)x + \ldots$,

$f(x)\, g(x) = r_0 s_0 + (r_0 s_1 + r_1 s_0)x + \ldots$

From (1), we have

$$\theta(f(x) + g(x)) = \overline{r_0 + s_0} + (\overline{r_1 + s_1})x + \ldots \quad \ldots(2)$$

$$\theta(f(x)\, g(x)) = \overline{r_0 s_0} + (\overline{r_0 s_1 + r_1 s_0})x + \ldots \quad \ldots(3)$$

We see that

$$\overline{r_i + s_i} = r_i + s_i + A = (r_i + A) + (s_i + A) = \bar{r}_i + \bar{s}_i, \text{ for each } i.$$

Again $\overline{r_i s_j} = r_i s_j + A = (r_i + A)(s_j + A) = \bar{r}_i \bar{s}_j$, for each i and j

Using these results in (2) and (3), we get

$$\theta(f(x) + g(x)) = \bar{r}_0 + \bar{s}_0 + (\bar{r}_1 + \bar{s}_1)x + \ldots$$
$$= (\bar{r}_0 + \bar{r}_1 x + \ldots) + (\bar{s}_0 + \bar{s}_1 x + \ldots)$$
$$= \theta(f(x)) + \theta(g(x)), \text{ by (1)}$$

$$\theta(f(x)\, g(x)) = (\bar{r}_0 \bar{s}_0) + (\bar{r}_0 \bar{s}_1 + \bar{r}_1 \bar{s}_0)x + \ldots$$
$$= (\bar{r}_0 + \bar{r}_1 x + \ldots.)(\bar{s}_0 + \bar{s}_1 x + \ldots)$$
$$= \theta(f(x))\, \theta(g(x)), \text{ by (1).}$$

Thus θ is a homomorphism. Also θ is onto, for any $p(x) \in \frac{R}{A}[x] \Rightarrow$ $p(x) = \bar{t}_0 + \bar{t}_1 x + \ldots + \bar{t}_k x^k$, where $\bar{t}_i = t_i + A\ (t_i \in R) \Rightarrow \theta(q(x)) = p(x)$, where $q(x) = t_0 + t_1 x + \ldots + t_k x^k \in R[x]$.

By Fundamental theorem of homomorphism, we obtain

$$\frac{R[x]}{Ker\,\theta} \approx \frac{R}{A}[x]. \quad \ldots(4)$$

Let $f(x) = r_0 + r_1 x + ... + r_n x^n \in Ker\,\theta$ be arbitrary.

$\Leftrightarrow \theta(f(x)) = \bar{0} \in \frac{R}{A}[x]$ $(\bar{0} = A)$

$\Leftrightarrow \bar{r}_0 + \bar{r}_1 x + ... + \bar{r}_n x^n = \bar{0} + \bar{0}\,x + ... + \bar{0}\,x^n$, by (1)

$\Leftrightarrow \bar{r}_i = \bar{0}$, for each i

$\Leftrightarrow r_i + A = A$, for each i

$\Leftrightarrow r_i \in A$, for each i

$\Leftrightarrow f(x) = r_0 + r_1 x + ... + r_n x^n \in A[x]$

$\Leftrightarrow Ker\,\theta = A[x]$.

Putting in (4), we get

$$\frac{R[x]}{A[x]} \approx \frac{R}{A}[x]. \qquad ...(5)$$

(*ii*) Let A be a prime ideal of R.

Then $\frac{R}{A}$ is an integral domain. [Theorem 2.6.3]

$\Rightarrow \frac{R}{A}[x]$ is an integral domain. [Cor. 3 of Theorem 3.2.1]

$\Rightarrow \frac{R[x]}{A[x]}$ is an integral domain, by (5)

$\Rightarrow A[x]$ is a prime ideal of $R[x]$. [Theorem 2.6.3]

Example 3.2.13. *Prove that the ideal* $\langle x^4 + 4 \rangle$ *is not a prime ideal of* $\mathbf{Q}[x]$, $\mathbf{Q}$ *being the field of rational numbers.*

Solution. We have $\langle x^4 + 4 \rangle = \{(x^4 + 4) f(x) : f(x) \in \mathbf{Q}[x]\}$

and $(x^2 + 2 + 2x)(x^2 + 2 - 2x) = (x^2 + 2)^2 - 4x^2 = x^4 + 4$.

Thus $(x^2 + 2x + 2)(x^2 - 2x + 2) \in \langle x^4 + 4 \rangle$, but

$x^2 + 2x + 2 \notin \langle x^4 + 4 \rangle$ and $x^2 - 2x + 2 \notin \langle x^4 + 4 \rangle$.

Hence $\langle x^4 + 4 \rangle$ is not a prime ideal of $\mathbf{Q}[x]$.

Theorem 3.2.8. *An integral domain R with unity is a field if and only if $R[x]$ is a principal ideal domain.* [D.U., 1997]

Proof. *Condition is necessary*

Let R be a field. Then $R[x]$ is a Euclidean domain. [Theorem 3.2.5]

Hence $R[x]$ is a principal ideal domain [E.D. $\Rightarrow$ P.I.D.]

Condition is sufficient

Let $R[x]$ be a principal ideal domain.

We shall prove that R is a field. By Example 3.2.11, we have

$$\frac{R[x]}{\langle x \rangle} \approx R. \qquad ...(1)$$

We now proceed to show that

$$\langle x \rangle = \{x p(x) : p(x) \in R[x]\}$$

is a maximal ideal of $R[x]$. Let M be any ideal of $R[x]$ such that

$$\langle x \rangle \subseteq M \subseteq R[x].$$

Since $R[x]$ is a P.I.D., M is a principal ideal of $R[x]$. ...(2)

Let $M = \langle f(x) \rangle$, for some $f(x) \in M$.

We have $x = x \cdot 1$ and so $x \in \langle x \rangle$ ...(3)

$\Rightarrow x \in M$, by (2)

$\Rightarrow x = f(x)\, g(x)$, for some $g(x) \in R[x]$, by (3).

This gives rise to the following cases :

Case I. $f(x) = 1$ and $g(x) = x$.

Case II. $f(x) = x$ and $g(x) = 1$.

In case I, $M = \langle 1 \rangle = R[x]$.

In case II, $\langle f(x) \rangle = \langle x \rangle \Rightarrow M = \langle x \rangle$.

It follows that $\langle x \rangle$ is a maximal ideal of $R[x]$, where $R[x]$ is a commutative ring with unity. Hence $\dfrac{R[x]}{\langle x \rangle}$ is a field [Theorem 2.6.1.] and so by (1), R is a field.

Corollary 1. $\mathbf{Z}[x]$ *is not a P.I.D.*

Proof. Let, if possible, $\mathbf{Z}[x]$ be a P.I.D., where $\mathbf{Z}$ is an integral domain with unity. By Theorem 3.2.8, $\mathbf{Z}$ is a field, which is impossible. Hence $\mathbf{Z}[x]$ is not a P.I.D.

Corollary 2. *If F is a field, then $F[x, y]$ is not a P.I.D.*

Proof. $F[x, y]$ is a polynomial ring (over F) in two indeterminates x and y. A typical element of $F[x, y]$ is of the form

$$a_0 + a_1 x + a_2 y + b_1 x^2 + b_2 xy + b_3 y^2 + \ldots + \alpha_1 x^{n-1} + \alpha_2 x^{n-1} y + \ldots + \alpha_n y^n,$$

where $a_i, b_i, \ldots, \alpha_i \in F$ and n is a non-negative integer.

It is easy to verify that

$$F[x, y] = F_1[y], \text{ where } F_1 = F[x].$$

Let, if possible, $F[x, y]$ be a P.I.D. $\Rightarrow F_1[y]$ is a P.I.D.,

where $F_1 = F[x]$ is an integral domain with unity

$\Rightarrow F_1$ is a field. [See Theorem 3.2.8.]

$\Rightarrow F[x]$ is a field, which is not true as x is not invertible.

Hence $F[x, y]$ is not a P.I.D.

Remark. *For an independent proof of Corollary 2, see Example* 3.2.21.

EXAMPLES

Example 3.2.14. *R is a ring such that $R[x]$ is a P.I.D. Show that R is a field.* [D.U., 1991]

Solution. Since $R[x]$ is a P.I.D., $R[x]$ is an integral domain with unity (by definition). Consequently, R is an integral domain with unity [See Example 3.2.5]. The result follows by the sufficient condition of Theorem 3.2.8.

Example 3.2.15. *Prove that if R is an integral domain with unity that is not a field, then $R[x]$ is not a P.I.D.*

Solution. Let, if possible, $R[x]$ be a P.I.D. By Theorem 3.2.8, R is a field, which is a contradiction. Hence $R[x]$ is not a P.I.D.

Example 3.2.16. *Prove that if D is an integral domain with unity that is not a field, then $D[x]$ is not a Euclidean domain.*

Solution. Let, if possible, $D[x]$ be a Euclidean domain. Then $D[x]$ is a P.I.D. and so by Theorem 3.2.8, D is a field, which is a contradiction. Hence $D[x]$ is not a Euclidean domain.

Example 3.2.17. *Show that*

$$A = \{x f(x) + 2g(x) : f(x), g(x) \in \mathbf{Z}[x]\}$$

is not a principal ideal of $\mathbf{Z}[x]$ and so $\mathbf{Z}[x]$ is not a P.I.D.

Solution. Firstly, we show that A is an ideal of $\mathbf{Z}[x]$. Let $h(x), k(x) \in A$. Then

$$h(x) = x f_1(x) + 2 g_1(x), k(x) = x f_2(x) + 2 g_2(x),$$

for some $f_1(x), f_2(x), g_1(x), g_2(x)$ in $\mathbf{Z}[x]$. We have

$$h(x) - k(x) = x(f_1(x) - f_2(x)) + 2(g_1(x) - g_2(x)) \in A.$$

For any $h(x) \in A$ and $r(x) \in \mathbf{Z}[x]$, we have

$$h(x) r(x) = x f_1(x) r(x) + 2 g_1(x) r(x) \in \mathbf{Z}[x].$$

Thus A is an ideal of $\mathbf{Z}[x]$. Now we show that A is not a principal ideal of $\mathbf{Z}[x]$. Let, if possible, $A = \langle p(x) \rangle$, for some $p(x) \in A$. We can write

$$x = x(1 + 0x + 0x^2 + \ldots) + 2(0 + 0x + 0x^2 + \ldots) \text{ and so } x \in A.$$

$$\therefore \quad x \in \langle p(x) \rangle \Rightarrow x = p(x)\, s(x), \text{ for some } s(x) \in \mathbf{Z}[x].$$

Similarly, $2 \in A = \langle p(x) \rangle \Rightarrow 2 = p(x)\, t(x)$, for some $t(x) \in \mathbf{Z}[x]$. ...(1)

From the above relations, we get

$$2x = 2p(x)\, s(x) \text{ and } 2x = xp(x)\, t(x)$$

$$\Rightarrow \quad 2p(x)\, s(x) = x\, p(x)\, t(x)$$

$$\Rightarrow \quad x\, t(x) = 2s(x)$$

$\Rightarrow$ each coefficient of $x\, t(x)$ and hence that of $t(x)$ is an even integer.

Let $t(x) = 2r(x)$, for some $r(x) \in \mathbf{Z}[x]$. ...(2)

From (1) and (2), we obtain

$$p(x)\, r(x) = 1 \Rightarrow 1 \in A = \langle p(x) \rangle$$

$$\Rightarrow 1 \in \{x f(x) + 2g(x) : f(x), g(x) \in \mathbf{Z}[x]\}$$

$$\Rightarrow 1 = x(a_0 + a_1 x + \ldots) + 2(b_0 + b_1 x + \ldots) \text{ ; for some } a_i, b_i \in \mathbf{Z}$$

$\Rightarrow 1 = 2b_0$ ($b_0 \in \mathbf{Z}$), which is impossible.

Hence A is not a principal ideal of $\mathbf{Z}[x]$. Consequently, $\mathbf{Z}[x]$ is not a P.I.D.

Example 3.2.18. *Prove that the ideal $\langle x \rangle$ of $\mathbf{Z}[x]$ is a prime ideal but not a maximal ideal of $\mathbf{Z}[x]$.*

Solution. We have $\langle x \rangle = \{x\,p(x) : p(x) \in \mathbf{Z}[x]\}$.

Let $f(x) = a_0 + a_1x + \ldots + a_m x^m$ and $g(x) = b_0 + b_1x + \ldots + b_nx^n$ be two polynomials in $\mathbf{Z}[x]$ such that $f(x)\,g(x) \in \langle x \rangle$. Then

$f(x)\,g(x) = x\,p(x)$, for some $p(x) = c_0 + c_1x + \ldots + c_rx^r \in \mathbf{Z}[x]$.

We have

$$(a_0 + a_1x + \ldots)(b_0 + b_1x + \ldots) = x(c_0 + c_1x + \ldots).$$

Comparing the constant term on both the sides, we get

$$a_0b_0 = 0 \Rightarrow a_0 = 0 \text{ or } b_0 = 0. \qquad (\because a_0, b_0 \in \mathbf{Z})$$

If $a_0 = 0$, then $f(x) = a_1x + a_2x^2 + \ldots + a_m x^m$

$$= x(a_1 + a_2x + \ldots + a_m x^{m-1}) \in \langle x \rangle.$$

Similarly, $b_0 = 0 \Rightarrow g(x) \in \langle x \rangle$.

Hence $\langle x \rangle$ is a prime ideal of $Z[x]$.

However, $\langle x \rangle$ is not a maximal ideal of $\mathbf{Z}[x]$, since

$$A = \{x f(x) + 2g(x) : f(x), g(x) \in \mathbf{Z}[x]\}$$

is a proper ideal of $\mathbf{Z}[x]$ such that

$$\langle x \rangle \subset A \subset \mathbf{Z}[x].$$

Notice that $2 \in A$ but $2 \notin \langle x \rangle$ and $1 \in \mathbf{Z}[x]$ but $1 \notin A$.

[By Example 3.2.17, $1 \in A \Rightarrow 1 = 2b_0$ $(b_0 \in \mathbf{Z})$, a contradiction].

Example 3.2.19. *Show that greatest common divisor of 2 and x in $\mathbf{Z}[x]$ ($\mathbf{Z}$ = ring of integers) cannot be written as $2r(x) + xs(x)$, where $r(x), s(x) \in \mathbf{Z}[x]$. Hence show that $\mathbf{Z}[x]$ is not a P.I.D..* [D.U., 1991]

Solution. Let $f(x)$ be a g.c.d. of 2 and x in $\mathbf{Z}[x]$ [g.c.d. of any two non-zero elements exists in $\mathbf{Z}[x]$, since $\mathbf{Z}[x]$ is a unique factorization domain. [See Theorem 3.3.4.]

Let, if possible, $f(x) = 2r(x) + xs(x)$, ...(1)

where $r(x), s(x) \in \mathbf{Z}[x]$ and $f(x) = (2, x)$.

By definition of g.c.d., $f(x) \mid 2$ and $f(x) \mid x$

$\Rightarrow$ $2 = f(x)\,g(x)$ and $x = f(x)\,h(x)$, for some $g(x), h(x) \in \mathbf{Z}[x]$.

We have $deg\,(f(x)\,g(x)) = deg\,2 = 0$

$\Rightarrow deg\,f(x) + deg\,g(x) = 0$, since $\mathbf{Z}$ is an I.D.

$\Rightarrow deg\,f(x) = 0 \Rightarrow f(x)$ is a constant polynomial.

Let $f(x) = \alpha$, where $\alpha \neq 0 \in \mathbf{Z}$.

$\therefore$ $x = \alpha\,h(x) \Rightarrow deg\,h(x) = 1$.

Let $h(x) = \beta x + \gamma$, where $\beta \neq 0 \in \mathbf{Z}$, $\gamma \in \mathbf{Z}$.

We have $x = \alpha(\beta x + \gamma) = \alpha\beta x + \alpha\gamma \Rightarrow \alpha\beta = 1 \Rightarrow 1 = f(x)\,\beta$.

Using (1), $1 = [2r(x) + xs(x)]\,\beta$.

Comparing the constant term on both the sides, we get

$$1 = 2a_0 \beta,$$

where $r(x) = a_0 + a_1 x + \ldots \in \mathbf{Z}[x]$, $a_0 \neq 0 \in \mathbf{Z}$. ...(2)

Notice that if $a_0 = 0$, then by (2), $1 = 0$, a contradiction.

The equation (2) is impossible in $\mathbf{Z}$, since a_0 and $\beta \in \mathbf{Z}$. Hence $f(x)$ cannot be written as $2r(x) + xs(x)$, where $f(x) = (2, x)$.

(*ii*) Let, if possible, $\mathbf{Z}[x]$ be a P.I.D.

Then the ideal $A = \{2r(x) + xs(x) : r(x), s(x) \in \mathbf{Z}[x]\}$ of $\mathbf{Z}[x]$ is principal and so $A = \langle p(x) \rangle$, for some $p(x) \in A$.

It follows that $p(x) = 2r(x) + xs(x)$, for some $r(x), s(x) \in \mathbf{Z}[x]$.

The above relation implies that $p(x)$ is g.c d of 2 and x. But this is impossible, as proved above.

Hence A is not a principal ideal of $\mathbf{Z}[x]$ and so $\mathbf{Z}[x]$ is not a P.I.D.

Example 3.2.20. *Show that the ideal*

$$A = \{xf(x) + 2g(x) : f(x), g(x) \in \mathbf{Z}[x]\}$$

is a maximal ideal of $\mathbf{Z}[x]$

Solution. Let M be any ideal of $\mathbf{Z}[x]$ such that

$$A \subset M \subset \mathbf{Z}[x], A \neq M.$$

Then there exists some $p(x) \in M$ such that $p(x) \notin A$.

Let $p(x) = a_0 + a_1 x + \ldots + a_m x^m \in \mathbf{Z}[x]$

If a_0 is even, then $a_0 = 2k$, for some $k \in \mathbf{Z}$.

$\therefore$ $p(x) = x(a_1 + a_2 x + \ldots + a_m x^{m-1}) + 2k \in A$,

which is a contradiction. Thus a_0 is an odd integer, say $a_0 = 2a + 1, a \in \mathbf{Z}$.

$\therefore$ $p(x) = 2a + 1 + a_1 x + \ldots + a_m x^m = q(x) + 1$,

where $q(x) = 2a + a_1 x + \ldots + a_m x^m$

$= x(a_1 + a_2 x + \ldots + a_m x^{m-1}) + 2a \in A \subset M$.

Now $p(x) \in M$ and $q(x) \in M \Rightarrow p(x) - q(x) \in M$, since M is an ideal of $\mathbf{Z}[x] \Rightarrow 1 \in M \Rightarrow M = \mathbf{Z}[x]$.

Hence A is a maximal ideal of $\mathbf{Z}[x]$.

Example 3.2.21. *Show that* $F[x, y]$ *is not a P.I.D., F being a field.*

Solution. It is clear that $(x) = \{xf(x, y) : f(x, y) \in F[x, y]\}$ is an ideal of $F[x, y]$. Similarly, (y) is an ideal of $F[x, y]$. Consequently, $(x) + (y)$ is also an ideal of $F[x, y]$. Let, if possible,

$$(x) + (y) = \langle f(x, y) \rangle, \text{ for some } f(x, y) \in F[x, y].$$

Clearly, $x = x + 0 \in (x) + (y)$. Thus $x = af(x, y)$, for some $a \neq 0 \in F$.

Similarly, $y = bf(x, y)$, for some $b \neq 0 \in F$.

The above relations imply $xa^{-1} = yb^{-1} \Rightarrow bx - ay = 0$, which is absurd, as x and y are independent variables over F. Hence $F[x, y]$ is not a P.I.D.

3.3 Unique Factorization Domain (U.F.D.)

Definition 1. *An integral domain R with unity is called a* **unique factorization domain (U.F.D.)**, *if it satisfies the following conditions :*

(i) Each non-zero element of R is either a unit or can be expressed as a product of finite number of irreducible elements of R.

(ii) The above decomposition is unique upto the order and associates of the irreducible elements. It means if a non-zero, non-unit element $a \in R$ is expressible as

$$a = p_1 p_2 \dots p_r \text{ and } a = q_1 q_2 \dots q_s ,$$

where p_i's and q_j's are irreducible elements of R, then there exists a one-to-one correspondence between p_i's and q_j's such that the corresponding elements are associates. In particular, $r = s$.

Illustrations

1. *Every field F is a U.F.D.*

   Notice that each non-zero element $a \in F$ is a unit *i.e.*,

   $aa^{-1} = 1 \Rightarrow a \mid 1$.

2. *The ring $\mathbf{Z}$ of integers is a U.F.D.*

   Notice that the units in $\mathbf{Z}$ are ± 1 and any integer different from ± 1 and 0 is expressible as a product of finite number of prime (irreducible) numbers and this expression is unique upto order and associates of irreducible elements. For example, the expressions

   $$210 = 2 \times 3 \times 5 \times 7 \quad \text{and} \quad 210 = 3 \times (-2) \times 7 \times (-5)$$

   are unique except for order and sign.

   Notice that 2 and -2, 5 and -5 are associates in $\mathbf{Z}$.

3. *Every Euclidean domain is a U.F.D.* [See Theorem 3.3.1].

   In particular, $\mathbf{Z}[i]$, $\mathbf{Z}[\sqrt{2}]$, $F[x]$ (F being a field) are U.F.Ds.

Ex. *Define a unique factorization domain and give two examples of it.*

Theorem 3.3.1. *Let R be a Euclidean ring. Prove that every element in R is either a unit in R or can be uniquely written (upto associates) as a product of prime elements of R.* [D.U., 1996]

Or

Show that every Euclidean domain is a unique factorization domain.

Proof. By Theorem 3.1.4, an element in a Euclidean domain R is prime if and only if it is irreducible.

Firstly we show that every element in R is either a unit or can be written as a product of irreducible elements of R. We shall prove this result by induction on $d(a)$, since $d(a)$ is a non-negative integer for each $a \neq 0 \in R$. If $d(a) = 0$, then a is a unit in R [See Example 3.1.15 (*ii*)].

Thus the result is true in this case. Suppose that the result is true for all $r \neq 0 \in R$ such that $d(r) < d(a)$. We shall prove the result for $r = a \in R$.

If a is irreducible (prime), there is nothing to prove. If a is not irreducible, then we can write $a = bc$, where neither b nor c is a unit in R. By Example 3.1.12, it follows that

$$d(b) < d(bc) = d(a) \quad \text{and} \quad d(c) < d(bc) = d(a)$$

i.e., $$d(b) < d(a) \quad \text{and} \quad d(c) < d(a).$$

By induction hypothesis, we can write

$$b = x_1 x_2, \ldots x_m \quad \text{and} \quad c = y_1 y_2 \ldots y_n,$$

where each x_i and y_j is an irreducible (prime) element of R.

Hence $a = bc = x_1 x_2 \ldots x_m y_1 y_2 \ldots y_n$,

which is a product of finite number of irreducible (prime) elements of R.

Uniqueness. We consider two representations of a as products of finite number of irreducible (prime) elements of R as follow :

$$a = p_1 p_2 \ldots p_m, \; a = q_1 q_2 \ldots q_n.$$

Then $p_1 p_1 \ldots p_m = q_1 q_2 \ldots q_n$. ...(1)

It is clear that $p_1 \mid p_1 p_2 \ldots p_m$ and so $p_1 \mid q_1 q_2 \ldots q_n$.

Since every irreducible element of R is prime, so

$$p_1 \mid q_1 q_2 \ldots q_n \Rightarrow p_1 \mid q_j, \text{ for some } j, 1 \le j \le n.$$

Without any loss of generality, we may assume that $p_1 \mid q_1$ (p_1 and q_1 are both prime). Consequently, p_1 and q_1 are associates [See Example 2.7.20] or $q_1 = u_1 p_1$, where u_1 is a unit in R. Thus, by (1), we have

$$p_1 p_2 \ldots p_m = u_1 p_1 q_2 \ldots q_n$$

or $$p_2 p_3 \ldots p_m = u_1 q_2 \ldots q_n. \qquad (\because p_1 \neq 0 \in R) \quad ...(2)$$

Since $p_2 \mid p_2 p_3 \ldots p_m$, we may take $p_2 \mid q_2$ and so p_2 and q_2 are associates.

[Notice that $p_2 \dagger u_1$, for otherwise, $p_2 \mid u_1$ and $u_1 \mid 1 \Rightarrow p_2 \mid 1 \Rightarrow p_2$ is a unit, a contradiction]

We can write $p_2 = u_2 q_2$. Putting this in (2) and cancelling out p_2 on both sides, we get

$$p_3 p_4 \ldots p_m = u_1 u_2 q_3 q_4 \ldots q_n \text{ and so on.}$$

After m steps all p_i's are cancelled out and the L.H.S. becomes 1, but the R.H.S. contains some q_j's. It means that

$$\text{number of } p_i\text{'s} \le \text{number of } q_j\text{'s } \textit{i.e.}, \; m \le n.$$

Repeating the above procedure with $q_1 \mid q_1 q_2 \ldots q_n \Rightarrow q_1 \mid p_1 p_2 \ldots p_m$ $\Rightarrow q_1 \mid p_1$ etc., we get $n \le m$. Thus $m = n$ and in this process we have also proved that p_i and q_i are associates for each i, $1 \le i \le m$. Hence R is a U.F.D.

Remark. Since $\mathbf{Z}[i]$, $\mathbf{Z}[\sqrt{2}]$, $F[x]$ (F being a field) etc. are all Euclidean domains, so $\mathbf{Z}[i]$, $\mathbf{Z}[\sqrt{2}]$, $F[x]$ etc. are also unique factorization domains.

Theorem 3.3.2. *If R is an integral domain with unity in which every non-zero, non-unit element is a finite product of irreducible elements and every irreducible element is prime, then R is a unique factorization domain.*

Proof. By the given hypothesis, R becomes a U.F.D. if we verify the second condition (uniqueness upto associates) of the definition of U.F.D. Let a be any non-zero, non-unit element of R such that

$$a = p_1 p_2 \dots p_m, \; a = q_1 q_2 \dots q_n ,$$

where each p_i and each q_j is an irreducible element of R. By the given hypothesis, each p_i and each q_j is a prime element of R. Imitating the proof of 'uniqueness part' of Theorem 3.3.1, the second condition of the definition of U.F.D. is verified. Hence R is a U.F.D.

Remark 1. The statement of Theorem 3.3.2 can be taken as the second definition of U.F.D.

Definition 2. (U.F.D.)

An integral domain R with unity is called a **U.F.D.**, *if it satisfies the following conditions :*

(*i*) *Every non-zero, non-unit element of R is expressible as a finite product of irreducible elements of R.*

(*ii*) *Every irreducible element of R is prime.*

Remark 2. *The two definitions of U.F.D. are equivalent.*

In Theorem 3.3.2, we have proved that Definition 2 $\Rightarrow$ Definition 1.

Also Definition 1 $\Rightarrow$ Definition 2, since every irreducible element of a U.F.D. is prime, by Theorem 3.3.3 given below.

Hence Definition 1 $\Leftrightarrow$ Definition 2.

Ex.1. *Give two different definitions a U.F.D. and use any one of them to prove that $\mathbf{Z}[\sqrt{-5}]$ is not a UFD.* [D.U., 1998]

Hint. $3 = 3 + \sqrt{-5} \, . \, 0 \in \mathbf{Z}[\sqrt{-5}]$ is irreducible but not prime [See Examples 2.7.9 and 2.7.12]. By second definition, $\mathbf{Z}[\sqrt{-5}]$ is not a UFD. Also see Example 3.3.1 ahead.

Ex.2. *Give two different definitions of a U.F.D. and establish their equivalence.*

Hint. See Remark 2 above.

Ex. 3. *Prove that an integral domain R with unity is a U.F.D. if and only if every non-zero, non-unit element of R is a finite product of irreducible elements of R and every irreducible element of R is prime.*

Hint. Prove that Definition 1 $\Leftrightarrow$ Definition 2.

Theorem 3.3.3. *An element in a U.F.D. is prime if and only if it is irreducible.* [D.U., 2000, 1997, 94]

Proof. Let R be a U.F.D.

Condition is necessary

Let $p \in R$ be prime. Then $p \neq 0$ and p is not a unit.

Let $p = ab$, for some $a, b \in R$. Since $p = p.1$, $p \mid p$ *i.e.*, $p \mid ab \Rightarrow p \mid a$ or $p \mid b$, since p is prime.

Theorem 3.3.2. *If R is an integral domain with unity in which every non-zero, non-unit element is a finite product of irreducible elements and every irreducible element is prime, then R is a unique factorization domain.*

Proof. By the given hypothesis, R becomes a U.F.D. if we verify the second condition (uniqueness upto associates) of the definition of U.F.D. Let a be any non-zero, non-unit element of R such that

$$a = p_1 p_2 \dots p_m,\ a = q_1 q_2 \dots q_n ,$$

where each p_i and each q_j is an irreducible element of R. By the given hypothesis, each p_i and each q_j is a prime element of R. Imitating the proof of 'uniqueness part' of Theorem 3.3.1, the second condition of the definition of U.F.D. is verified. Hence R is a U.F.D.

Remark 1. The statement of Theorem 3.3.2 can be taken as the second definition of U.F.D.

Definition 2. (U.F.D.)

An integral domain R with unity is called a **U.F.D.**, *if it satisfies the following conditions :*

(*i*) *Every non-zero, non-unit element of R is expressible as a finite product of irreducible elements of R.*

(*ii*) *Every irreducible element of R is prime.*

Remark 2. *The two definitions of U.F.D. are equivalent.*

In Theorem 3.3.2, we have proved that Definition 2 $\Rightarrow$ Definition 1.

Also Definition 1 $\Rightarrow$ Definition 2, since every irreducible element of a U.F.D. is prime, by Theorem 3.3.3 given below.

Hence Definition 1 $\Leftrightarrow$ Definition 2.

Ex.1. *Give two different definitions a U.F.D. and use any one of them to prove that $\mathbf{Z}[\sqrt{-5}]$ is not a UFD.* [D.U., 1998]

Hint. $3 = 3 + \sqrt{-5}\,.\,0 \in \mathbf{Z}[\sqrt{-5}]$ is irreducible but not prime [See Examples 2.7.9 and 2.7.12]. By second definition, $\mathbf{Z}[\sqrt{-5}]$ is not a UFD. Also see Example 3.3.1 ahead.

Ex.2. *Give two different definitions of a U.F.D. and establish their equivalence.*

Hint. See Remark 2 above.

Ex. 3. *Prove that an integral domain R with unity is a U.F.D. if and only if every non-zero, non-unit element of R is a finite product of irreducible elements of R and every irreducible element of R is prime.*

Hint. Prove that Definition 1 $\Leftrightarrow$ Definition 2.

Theorem 3.3.3. *An element in a U.F.D. is prime if and only if it is irreducible.* [D.U., 2000, 1997, 94]

Proof. Let R be a U.F.D.

Condition is necessary

Let $p \in R$ be prime. Then $p \neq 0$ and p is not a unit.

Let $p = ab$, for some $a, b \in R$. Since $p = p.1$, $p \mid p$ *i.e.*, $p \mid ab \Rightarrow p \mid a$ or $p \mid b$, since p is prime.

Let $p \mid a$. Then $a = pc$, for some $c \in R$.

$\therefore \quad p = ab \Rightarrow p \cdot 1 = p(cb) \Rightarrow cb = 1 \Rightarrow b \mid 1 \Rightarrow b$ is a unit.

Similarly, $p \mid b \Rightarrow a$ is a unit.

Hence $p = ab \Rightarrow$ either a or b is a unit and so p is irreducible.

Condition is sufficient

Let $p \in R$ be irreducible. Then $p \neq 0$ and p is not a unit.

Let $p \mid ab$, for some $a, b \in R$. Then $ab = cp$, for some $c \in R$. It is clear that both a and b cannot be units, for otherwise, $a \mid 1$ and $b \mid 1 \Rightarrow ab \mid 1$ and since $p \mid ab$, so $p \mid 1 \Rightarrow p$ is a unit, a contradiction. Thus at least one of a or b is a non-unit.

Case I. *Suppose a is a unit.*

Then $a^{-1} \in R$ exists and $ab = cp \Rightarrow b = a^{-1} c\, p \Rightarrow p \mid b$.

Similarly, if b is a unit, then $p \mid a$. Hence p is prime in this case.

Case II. *Suppose a and b are both non-units in R.*

Since R is a U.F.D., by definition,

$$a = p_1 p_2 \dots p_n, \; b = q_1 q_2 \dots q_m, \qquad \dots(1)$$

where each p_i and each q_j is an irreducible element of R. If c is a unit, then $ab = cp \Rightarrow ab$ is an associate of p and p is irreducible. Since associate of an irreducible element is irreducible, so ab is irreducible $\Rightarrow$ either a is a unit or b is a unit, which is contrary to our assumption. Thus c is a non-unit element of R and so by definition of U.F.D., we can write

$$c = r_1 r_2 \dots r_k, \qquad \dots(2)$$

where each r_i is an irreducible element in R.

Putting (1) and (2) in $ab = cp$, we get

$$p_1 p_2 \dots p_n q_1 q_2 \dots q_m = p\, r_1 r_2 \dots r_k.$$

By condition (*ii*) of the definition of U.F.D., p is an associate of some p_i or $q_j \Rightarrow p \mid p_i \; (1 \le i \le n)$ or $p \mid q_j \; (1 \le j \le m) \Rightarrow p \mid p_1 p_2 \dots p_n$ or $p \mid q_1 q_2 \dots q_m \Rightarrow p \mid a$ or $p \mid b$, by (1).

Hence p is prime.

EXAMPLES

Example 3.3.1. *Prove that* $\mathbf{Z}[\sqrt{-5}]$ *is not a U.F.D.* [D.U., 1998]

Solution. We notice that $9 = 9 + 0\sqrt{-5} \in \mathbf{Z}[\sqrt{-5}]$, where

$$9 = 3.3 \text{ and } 9 = (2 + \sqrt{-5})(2 - \sqrt{-5}).$$

By Examples 2.7.12, 2.7.14 (Chapter 2), 3, $2 \pm \sqrt{-5}$ are irreducible elements of $\mathbf{Z}[\sqrt{-5}]$. We see that $9 \in \mathbf{Z}[\sqrt{-5}]$ has two distinct expressions as products of irreducible elements of $\mathbf{Z}[\sqrt{-5}]$. Hence $\mathbf{Z}[\sqrt{-5}]$ is not a U.F.D., by Definition 1.

Example 3.3.2. *Prove* $J[\sqrt{-3}]$ *is not a U.F.D., J being the ring of integers.* [D.U., 1996]

Solution. We see that $4 = 4 + 0\sqrt{-3} \in J[\sqrt{-3}]$ and

$$4 = 2.2 \quad \text{and} \quad 4 = (1+\sqrt{-3})(1-\sqrt{-3}). \qquad ...(1)$$

We shall prove that $2, 1 \pm \sqrt{-3}$ are irreducible elements of $J[\sqrt{-3}]$. Let $2 = (a + b\sqrt{3}\,i)(c + d\sqrt{3}\,i)$ and so $2 = \bar{2} = (a - b\sqrt{3}\,i)(c - d\sqrt{3}\,i)$

(Here a, b, c, d are all integers)

$\Rightarrow 4 = (a^2 + 3b^2)(c^2 + 3d^2)$, which gives the following possibilities :

(*i*) $a^2 + 3b^2 = 1$ and $c^2 + 3d^2 = 4$;

(*ii*) $a^2 + 3b^2 = 4$ and $c^2 + 5d^2 = 1$;

(*iii*) $a^2 + 3b^2 = 2$ and $c^2 + 3d^2 = 2$, which is impossible in J.

The first two possibilities imply

$$[a = \pm 1, b = 0] \text{ or } [c = \pm 1, d = 0]$$

$\Rightarrow a + b\sqrt{3}\,i = \pm 1$ or $c + d\sqrt{3}\,i = \pm 1$ (± 1 being units in $J[\sqrt{-3}]$.

Hence 2 is irreducible in $J[\sqrt{-3}]$.

Let $1 + \sqrt{-3} = (a + b\sqrt{-3})(c + d\sqrt{-3})$; $a, b, c, d \in J$

$\Rightarrow \quad 1 - \sqrt{-3} = (a - b\sqrt{-3})(c - d\sqrt{-3})$.

On multiplying the respective sides of the above equations, we get

$$4 = (a^2 + 3b^2)(c^2 + 3d^2).$$

As argued above, it follows that $1 \pm \sqrt{-3}$ are irreducible elements of $J[\sqrt{-3}]$. From (1), we see that $4 \in J[\sqrt{-3}]$ has two distinct expressions as products of irreducible elements of $J[\sqrt{-3}]$. Hence $J[\sqrt{-3}]$ is not a U.F.D.

Example 3.3.3. *Show that* $\mathbf{Z}[\sqrt{-6}]$ *is not a U.F.D.*

Hint. $10 = 2.5$, $10 = (2 + \sqrt{-6})(2 - \sqrt{-6})$; where $2, 5, 2 \pm \sqrt{-6}$ are distinct irreducible elements of $\mathbf{Z}[\sqrt{-6}]$.

Example 3.3.4. *Show that* $\mathbf{Z}[\sqrt{-7}]$ *is not a U.F.D.*

Hint. $16 = 2 \,.\, 2 \,.\, 2 \,.\, 2$, $16 = (3 + \sqrt{-7})(3 - \sqrt{-7})$; where $2, 3 \pm \sqrt{-7}$ are distinct irreducible elements of $\mathbf{Z}[\sqrt{-7}]$.

Theorem 3.3.4. *In a U.F.D. every pair of non-zero elements have a g.c.d. and l.c.m.* [D.U., 1992]

Proof. Let R be a U.F.D. and a, b be any two non-zero elements of R.

Case I. *Suppose one of* a *and* b (*say* a) *is a unit.*

Then a^{-1} exists and $aa^{-1} = 1 \Rightarrow 1 \,.\, b = (aa^{-1})\, b$

$\Rightarrow \quad b = a\,(a^{-1}\, b) \Rightarrow a \mid b$. Also $a = a \,.\, 1 \Rightarrow a \mid a$.

If $c \in R$ is such that $c \mid a$ and $c \mid b$, then $c \mid a$ implies that a is g.c.d. of a and b.

Again $a \mid b$ and $b \mid b \Rightarrow b \mid x$ (where $a \mid x$ and $b \mid x$). Thus b is l.c.m. of a and b.

Similarly, we can show that if b is a unit, then b is g.c.d. of a and b and a is l.c.m. of a and b.

Case II. *Suppose a and b are both non-units in R.*

Since R is a U.F.D, we can write

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n},$$

$$b = p_1^{\beta_1} p_2^{\beta_2} \dots p_n^{\beta_n},$$

where p_i are irreducible elements in R ; α_i and β_i are non-negative integers, and by p_i^0 we mean a unit.

[For example in $\mathbf{Z}$; $48 = 2^4 . 3^1 . 5^0$ and $75 = 2^0 . 3^1 . 5^2$]

Let $\lambda_i = \min(\alpha_i, \beta_i)$, $i = 1, 2, \dots, n$

and $c = p_1^{\lambda_1} p_2^{\lambda_2} \dots p_n^{\lambda_n} \in R.$

Since $\lambda_i \le \alpha_i$ and $\lambda_i \le \beta_i$, $p_i^{\lambda_i} \mid p_i^{\alpha_i}$ and $p_i^{\lambda_i} \mid p_i^{\beta_i}$ for each i.

Consequently, $c \mid a$ and $c \mid b$.

Further, let $d \in R$ be such that $d \mid a$ and $d \mid b$.

If d is a unit, then $dd^{-1} = 1 \Rightarrow c = c(dd^{-1})$

$\Rightarrow \quad c = d(cd^{-1}) \Rightarrow d \mid c \Rightarrow c$ is g.c.d. of a and b.

If d is not a unit in R, we can write

$$d = p_1^{\gamma_1} p_2^{\gamma_2} \dots p_n^{\gamma_n} \quad (\gamma_i \text{ being non-negative integers})$$

Since $d \mid a$ and $d \mid b$, $\gamma_i \le \alpha_i$ and $\gamma_i \le \beta_i$, for each i

$\Rightarrow \gamma_i \le \min(\alpha_i, \beta_i) = \lambda_i$, for each i

$\Rightarrow p_1^{\gamma_1} p_2^{\gamma_2} \dots p_n^{\gamma_n} \mid p_1^{\lambda_1} p_2^{\lambda_2} \dots p_n^{\lambda_n} \Rightarrow d \mid c.$

Hence c is g.c.d. of a and b.

Similarly, we can prove that if $\mu_i = \max(\alpha_i, \beta_i)$ for each i, then $x = p_1^{\mu_1} p_2^{\mu_2} \dots p_n^{\mu_m} \in R$ is l.c.m. of a and b.

Corollary. *Any finite number of non-zero elements $a_1, a_2, \dots, a_n$ of a U.F.D. have a g.c.d. and l.c.m.*

Theorem 3.3.5. *Every principal ideal domain is a unique factorization domain i.e., P.I.D. $\Rightarrow$ U.F.D.*

Lemma. *Let R be a P.I.D. Then every ascending chain of ideals in R :*

$$(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \dots \subseteq (a_n) \subseteq \dots \text{ is finite.}$$

For the proof of the Lemma, see Theorem 2.8.11 (Chapter 2).

Proof of the Theorem. Let R be a P.I.D. Let a be any non-zero, non-unit element of R. We proceed to show that a is expressible as a finite product of irreducible elements of R. If a is irreducible, there is nothing to prove.

If a is not irreducible, then $a = a_1 a_1'$, where a_1 and a_1' are both non-units in R. We notice that $a = a_1 a_1' \Rightarrow a_1 \mid a \Rightarrow (a) \subset (a_1)$ and $(a) \neq (a_1)$, for $(a) = (a_1) \Rightarrow a$ and a_1 are associates $\Rightarrow a_1'$ is a unit, a contradiction.

[Refer to Example 2.8.6, Chapter 2]

If in the expression $a = a_1 a_1'$, both a_1 and a_1' are irreducible, the result is proved. Otherwise, we may suppose that a_1 is not irreducible. Then $a_1 = a_2 a_2'$, where a_2 and a_2' are both non-units in R and as argued above,

$$(a_1) \subset (a_2) \text{ with } (a_1) \neq (a_2).$$

Thus we have $a = a_2 a_2' a_1'$. If a_2, a_2', a_1' are all irreducible elements in R, the result is proved. Otherwise, proceeding in a similar manner, we obtain an ascending chain of ideals :

$$(a) \subset (a_1) \subset (a_2) \subset \ldots,$$

where no two of these ideals are equal. By the above lemma, such a chain of ascending ideals in a P.I.D. must be finite *i.e.*, $(a) \subset (a_1) \subset (a_2) \subset \ldots. \subset (a_m)$, for some positive integer m. Consequently, after a finite number of steps, we arrive at an expression of a as a product of finite number of irreducible elements of R of the form

$$a = p_1 p_2 \ldots p_m, \text{ where each } p_i \text{ is irreducible.}$$

Uniqueness. The above expression is unique upto the order and associates of the irreducible elements. The proof of this fact is exactly similar to the uniqueness part as proved in Theorem 3.3.1. [Notice that in a P.I.D, an element in prime iff it is irreducible]

Corollary. *Every Euclidean domain is a U.F.D.*

Proof. We know

E.D. $\Rightarrow$ P.I.D. [Theorem 3.3.1.]

and P.I.D. $\Rightarrow$ U.F.D. [Theorem 3.3.5]

Hence E.D. $\Rightarrow$ U.F.D.

3.4 Primitive and Irreducible Polynomials

Let a and b be any two non-zero elements of R, R being a U.F.D. They have a g.c.d. (Theorem 3.3.4). Further, any two greatest common divisors d_1 and d_2 of a and b are associates (See Example 2.8.7) *i.e.*, $d_1 = ud_2$, where u is a unit in R. By virtue of this relation, *we say that g.c.d. of a and b is unique within units of R.* The uniquely determined (within an arbitrary unit) g.c.d. of a and b is denoted by (a, b). With this observation, we give the following :

Definition. (Content of a Polynomial)

Let R be a U.F.D. and let $f(x) = a_0 + a_1 x + \ldots + a_m x^n$ be any non-zero polynomial in $R[x]$. The **content** *of $f(x)$ is defined as the greatest common divisor of $a_0, a_1, \ldots, a_m$. It is denoted by $c(f)$.*

It is unique within units of R.

Definition. *A polynomial in $R[x]$ (R being a U.F.D.) is said to be* **primitive,** *if its content is a unit.*

Illustrations

1. The content of $f(x) = 4 + 2x + 6x^2 \in \mathbf{Z}[x]$ is 2, since g.c.d. of 4, 2 and 6 is 2.
2. $f(x) = 1 + 2x + 6x^2 \in \mathbf{Z}[x]$ is primitive, since g.c.d. of 1, 2 and 6 is 1, a unit in **Z**.
3. $f(x) = 3 + 9x + 6x \in \mathbf{Z}[x]$ is not primitive.

Notice that $f(x) = 3(1 + 3x + 2x^3)$, where $c(f) = 3$ and $1 + 3x + 2x^3$ is primitive. We generalize this property in the following :

Lemma 3.4.1. *Let R be a U.F.D. and $0 \neq f(x) \in R[x]$. Then $f(x) = a f_1(x)$, where $a = c(f)$ and $f_1(x) \in R[x]$ is primitive.*

Proof. Let $f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n \in R[x]$

Let a = g.c.d. of $a_0, a_1, \ldots, a_n$. Then for each i, $1 \leq i \leq n$,

$$a \mid a_i \Rightarrow a_i = ab_i, \text{ for some } b_i \in R.$$

$$\therefore \quad f(x) = ab_0 + ab_1 x + ab_2 x^2 + \ldots + ab_n x^n$$

$$= a(b_0 + b_1 x + b_2 x^2 + \ldots + b_n x^n), \; a = c(f)$$

$$= a f_1(x), \text{ where } f_1(x) = b_0 + b_1 x + \ldots + b_n x^n \in R[x].$$

Since a is g.c.d. of $a_0, a_1, \ldots, a_n$, g.c.d. of $b_0, b_1, \ldots, b_n$ is 1 and so $f_1(x)$ is primitive. This proves the Lemma.

Ex. *In* **Z**$[x]$, *show that* $8x^3 + 6x + 3$ *is a primitive polynomial whereas* $8x^3 + 6x^2 + 2$ *is not.* [D.U., 1994]

Theorem 3.4.2. (Gauss Lemma)

If R is a U.F.D., then the product of two primitive polynomials in $R[x]$ is a primitive polynomial in $R[x]$. [D.U., 1999, 98, 93]

Proof. Let $f(x)$ and $g(x)$ be two primitive polynomials in $R[x]$, where

$$f(x) = a_0 + a_1 x + \ldots + a_n x^n, \; g(x) = b_0 + b_1 x + \ldots + b_m x^m.$$

Then

$$f(x)\, g(x) = c_0 + c_1 x + c_2 x^2 + \ldots + c_k x^k + \ldots,$$

where $$c_k = a_0 b_k + a_1 b_{k-1} + a_2 b_{k-2} + \ldots + a_k b_0. \qquad \ldots(1)$$

Let, if possible, $f(x)\, g(x)$ be not a primitive polynomial. Then g.c.d. of $c_0, c_1, c_2, \ldots$ is a non-unit in R, say r.

Since R is a U.F.D., we can write

$$r = p_1 p_2 \ldots p_t, \text{ where each } p_i \text{ is irreducible}$$

$$\Rightarrow \quad p_i \mid r \text{ and } r \mid c_k \;\; \forall \;\; k \Rightarrow p_i \mid c_k \;\; \forall \;\; k$$

Thus there exists some irreducible element $p \in R$ such that

$$p \mid c_k \;\; \forall \;\; k. \qquad \ldots(2)$$

Since p is irreducible, p is non-zero and non-unit. Since $f(x)$ is a primitive polynomial, g.c.d. of $a_0, a_1, \ldots, a_n$ is a unit. Since p is a non-unit,

p does not divide some a_k. Let a_i be the first coefficient of $f(x)$, which is not divisible by p. It means

$$p \mid a_0, p \mid a_1, p \mid a_2 \ldots, p \mid a_{i-1} \text{ but } p \nmid a_i. \quad \ldots(3)$$

Similarly, let b_j be the first coefficient of $g(x)$, which is not divisible by p. It means

$$p \mid b_0, p \mid b_1, p \mid b_2, \ldots, p \mid b_{j-1} \text{ but } p \nmid b_j. \quad \ldots(4)$$

From (1), we obtain

$$c_{i+j} = (a_0 b_{i+j} + a_1 b_{i+j-1} + \ldots + a_{i-1} b_{j+1}) + a_i b_j + (a_{i+1} b_{j-1} + a_{i+2} b_{j-2} + \ldots + a_{i+j} b_0) \quad \ldots(5)$$

From (3) and (4), we see that

$$p \mid (a_0 b_{i+j} + a_1 b_{i+j-1} + \ldots + a_{i-1} b_{j+1}), \quad \ldots(6)$$

and

$$p \mid (a_{i+1} b_{j-1} + a_{i+2} b_{j-2} + \ldots + a_{i+j} b_0). \quad \ldots(7)$$

From (2), $p \mid c_{i+j}$. $\quad \ldots(8)$

Using (6), (7) and (8) in (5), we obtain

$$p \mid a_i b_j \Rightarrow p \mid a_i \text{ or } b \mid b_j,$$

since every irreducible element of R is prime.

Thus we arrive at a contradiction, since $p \nmid a_i$ and $p \nmid b_j$. Hence $f(x)\, g(x)$ is a primitive polynomial.

Corollary 1. *If R is a U.F.D. and $f(x), g(x) \in R[x]$, then*

$$c(fg) = c(f)\, c(g).$$

Proof. By Lemma 3.4.1, we can write

$f(x) = a f_1(x)$, where $a = c(f)$ and $f_1(x) \in R[x]$ is primitive,

$g(x) = b g_1(x)$, where $b = c(g)$ and $g_1(x) \in R[x]$ is primitive.

$$\therefore \quad f(x)\, g(x) = ab f_1(x)\, g_1(x). \quad \ldots(1)$$

Since the product of two primitive polynomials is primitive, $f_1(x)\, g_1(x)$ is primitive. Using this property in (1), we observe that

$$c(fg) = ab = c(f)\, c(g).$$

The converse of Gauss's Lemma is also true as shown below :

Corollary 2. *Let R be a U.F.D. and $f(x), g(x) \in R[x]$.*

If $f(x)\, g(x)$ is a primitive polynomial, then $f(x)$ and $g(x)$ are also primitive polynomials.

Proof. Since $f(x)\, g(x)$ is primitive, $c(fg)$ is a unit. By Cor. 1, $c(f)\, c(g)$ is a unit $\Rightarrow ab$ is a unit, where $a = c(f)$, $b = c(g)$.

$\therefore (ab)^{-1} \in R \Rightarrow b^{-1} a^{-1} \in R \Rightarrow a^{-1} \in R$ and $b^{-1} \in R \Rightarrow a$ and b are units in $R \Rightarrow c(f)$ and $c(g)$ are units $\Rightarrow f(x)$ and $g(x)$ are primitive polynomials.

Theorem 3.4.3. *Let D be a Euclidean domain, F its field of quotients. If the primitive polynomial $f(x) \in D[x]$ can be factored as the product of two polynomials in $F[x]$, then $f(x)$ can be factored as the product of two polynomials in $D[x]$.*

Proof. Let $f(x) = g(x)\, h(x)$, where $g(x), h(x) \in F[x]$.

Let $g(x) = \alpha_0 + \alpha_1 x + \ldots + \alpha_n x^n \in F[x], \alpha_i \in F.$

Since F is field of quotients of D, we can write

$$\alpha_i = \frac{b_i}{a_i}\ ; a_i, b_i \in D \text{ and } a_i \neq 0.$$

$$\therefore \quad g(x) = \frac{b_0}{a_0} + \frac{b_1}{a_1} x + \ldots + \frac{b_n}{a_n} x^n$$

$$= \frac{1}{a}\left(b_0 a_1 \ldots a_n + b_1 a_0 a_2 \ldots a_n x + \ldots + b_n a_0 a_1 \ldots a_{n-1} x^n \right),$$

where $a = a_0 a_1 \ldots a_n \in D.$

Thus $g(x) \in F[x]$ is expressible as

$$g(x) = \frac{1}{a} g_0(x), \text{ where } a \neq 0 \in D,\ g_0(x) \in D[x]. \qquad \ldots(1)$$

Similarly, $h(x) = \frac{1}{b} h_0(x)$, where $b \neq 0 \in D,\ h_0(x) \in D[x]$. $\ldots(2)$

By Lemma 3.4.1, $g_0(x) \in D[x]$ can be written as

$g_0(x) = r\, g_1(x)$, where $r = c(g_0)$ and $g_1(x) \in D[x]$ is primitive $\ldots(3)$

Similarly,

$h_0(x) = s\, h_1(x)$, where $s = c(h_0)$ and $h_1(x) \in D[x]$ is primitive $\ldots(4)$

From (1) and (3), we obtain

$$g(x) = \frac{r}{a} g_1(x).$$

From (2) and (4), we obtain

$$h(x) = \frac{s}{b} h_1(x).$$

$$\therefore \quad f(x) = g(x)\, h(x) = \frac{rs}{ab} g_1(x)\, h_1(x)$$

or $$ab\, f(x) = rs\, g_1(x)\, h_1(x). \qquad \ldots(5)$$

Since the product of two primitive polynomials is primitive, $g_1(x)\, h_1(x)$ is primitive in $D[x]$. Consequently,

$$c \text{ (R.H.S. of (5))} = rs.$$

Since $f(x)$ is given to be primitive in $D[x]$, so

$$c \text{ (L.H.S. of (5))} = rs.$$

It follows that $ab = rs$ and so by (5), we obtain

$$f(x) = g_1(x)\, h_1(x), \quad \text{where } g_1(x) \in D[x],\ h_1(x) \in D[x].$$

This proves the theorem.

Corollary. *If a primitive polynomial $f(x) \in \mathbf{Z}[x]$ can be factored as the product of two polynomials having rational coefficients, then $f(x)$ can be factored as the product of two polynomials having integer coefficients.*

Proof. We are given $f(x) \in \mathbf{Z}[x]$, where the field of quotients of $\mathbf{Z}$ is $\mathbf{Q}$ (all rationals). Taking $D = \mathbf{Z}$ and $F = \mathbf{Q}$ in the above theorem, we see that

$$f(x) = g(x)\, h(x), \quad \text{where} \quad g(x),\ h(x) \in \mathbf{Q}[x]$$

$$\Rightarrow \quad f(x) = g_1(x)\, h_1(x), \text{ where } g_1(x),\ h_1(x) \in \mathbf{Z}[x].$$

Definition. (Irreducible Polynomial)

Let R be an integral domain with unity. A polynomial $f(x) \in R[x]$ is said to be **irreducible** *over R, if whenever*

$$f(x) = g(x)\, h(x), \text{ where } g(x),\ h(x) \in R[x],$$

then either deg $g(x) = 0$ or deg $h(x) = 0$ i.e., either $g(x)$ or $h(x)$ is a constant polynomial.

Further, $f(x) \in R[x]$ is said to be **reducible** *over R, if it is not irreducible over R i.e., $f(x)$ can be written as $f(x) = g(x)\, h(x)$, for some $g(x),\ h(x) \in R[x]$; where deg $g(x) > 0$ and deg $h(x) > 0$*

Illustrations

1. The polynomial $x^2 + 1$ is irreducible over the field of real numbers, but not over the field of complex numbers, since
$$x^2 + 1 = (x + i)(x - i),\ i^2 = -1$$
2. The polynomial $x^2 - 2$ is irreducible over $\mathbf{Q}$ (all rationals), but not over $\mathbf{R}$ (all reals), since
$$x^2 - 2 = (x + \sqrt{2})(x - \sqrt{2}).$$
3. The polynomial $f(x) = 1 + x + x^3 + x^4$ is not irreducible over any field F, since
$$f(x) = (1 + x)(1 + x^3).$$

Remark. We recall that : *A non-zero, non-unit element p of an integral domain R with unity is called an* **irreducible element**, *if*

$$p = ab\ (a, b \in R) \Rightarrow \text{either } a \text{ is a unit or } b \text{ is a unit.}$$

We shall frequently use the following results :

(*i*) *If R is an integral domain with unity, then units of R and $R[x]$ are the same.* [See Theorem 3.2.2.]

(*ii*) *Any irreducible element of R is an irreducible element of $R[x]$.* [See Theorem 3.2.3.]

We study the relationship between irreducible elements and irreducible polynomials in $R[x]$ in the following :

Theorem 3.4.4. *Let R be an integral domain with unity. Every irreducible element in $R[x]$ is an irreducible polynomial. The converse, however, need not be true.*

Proof. Let $f(x)$ be any irreducible element of $R[x]$. We want to show that $f(x)$ is an irreducible polynomial over R. Suppose this is false. Then we can write

$$f(x) = g(x)\,h(x), \text{ where } g(x), h(x) \in R[x];$$

and $\quad deg\ g(x) > 0 \quad \text{and} \quad deg\ h(x) > 0$

$\Rightarrow g(x), h(x)$ are not constant polynomials and so $g(x) \notin R$, $h(x) \notin R$

$\Rightarrow g(x)$ and $h(x)$ cannot be units in R

$\Rightarrow g(x)$ and $h(x)$ cannot be units in $R[x]$,

since units of R and $R[x]$ are the same

$\Rightarrow f(x)$ is not an irreducible element of $R[x]$, which is a contradiction.

Hence $f(x)$ is an irreducible polynomial over R.

However, the converse is not true i.e., an irreducible polynomial in $R[x]$ may not be an irreducible element of $R[x]$. For example, $f(x) = 3x^2 + 3 = 3(x^2 + 1) \in \mathbf{Z}[x]$ is an irreducible polynomial over $\mathbf{Z}$ (all integers), but is not an irreducible element of $\mathbf{Z}[x]$, since the units of $\mathbf{Z}[x]$ are ± 1 and in this case $3 \neq \pm 1$ and $x^2 + 1 \neq \pm 1$.

Theorem 3.4.5. *Let F be a field and $f(x)$ a non-zero polynomial in $F[x]$. Then $f(x)$ is an irreducible element if and only if $f(x)$ is an irreducible polynomial.*

Proof. By Theorem 3.4.4, $f(x)$ is an irreducible element implies that $f(x)$ is an irreducible polynomial.

Conversely, let $f(x)$ be an irreducible polynomial of $F[x]$. We shall prove that $f(x)$ is an irreducible element. Let $f(x) = g(x)\,h(x)$, where $g(x)$, $h(x) \in F[x]$. Since $f(x)$ is an irreducible polynomial, either $deg\ g(x) = 0$ or $deg\ h(x) = 0$ *i.e.*, either $g(x)$ or $h(x)$ is a constant polynomial. Let $g(x) = \alpha$, $\alpha \neq 0 \in F$. Since F is a field, $\alpha^{-1} \in F \Rightarrow \alpha$ is a unit in $F \Rightarrow g(x)$ is a unit in $F[x]$, since units of F and $F[x]$ are same.

Hence $f(x)$ is an irreducible element of $F[x]$.

Theorem 3.4.6. *Let F be a field. The ideal*

$$A = \langle p(x) \rangle = \{p(x) f(x) : f(x) \in F[x]\}$$

in $F[x]$ is a maximal ideal if and only if $p(x)$ is an irreducible polynomial over F.

Further $\dfrac{F[x]}{\langle p(x) \rangle}$ is a field.

Proof. Since $F[x]$ is a Euclidean domain, the first part of the theorem follows by Theorem 3.1.5 and Theorem 3.4.5.

(*ii*) Since $\langle p(x) \rangle$ is a maximal ideal of $F[x]$, therefore

$$\frac{F[x]}{\langle p(x) \rangle} \text{ is a field.} \qquad \text{[Theorem 2.6.1]}$$

Theorem 3.4.7. *If R is a U.F.D., then any $f(x) \in R[x]$ is an irreducible element of $R[x]$ if and only if either $f(x)$ is an irreducible element of R or $f(x)$ is an irreducible primitive polynomial of $R[x]$.*

Proof. *Condition is necessary*

Let $f(x)$ be an irreducible element of $R[x]$. If $f(x) \in R$, then $f(x)$ is an irreducible element of R. Suppose $f(x) \notin R$. We shall show that $f(x)$ is an irreducible primitive polynomial of $R[x]$. Let $f(x) = g(x)\, h(x)$, where $g(x), h(x) \in R[x]$. Since $f(x)$ is an irreducible element of $R[x]$, one of $g(x)$ or $h(x)$ must be a unit of $R[x]$ *i.e.*, one of $g(x)$ or $h(x)$ must be a unit of R, since units of R and $R[x]$ are same. Consequently, $deg\ g(x) = 0$ or $deg\ h(x) = 0$. This show that $f(x)$ is an irreducible polynomial of $R[x]$. Next we show that $f(x)$ is primitive. By Lemma 3.4.1, we have

$$f(x) = a f_1(x), \text{ where } a = c(f) \in R \text{ and } f_1(x) \text{ is primitive.}$$

It follows that

$$deg\ f_1(x) = deg\ f(x) > 0 \Rightarrow f_1(x) \notin R$$

$\Rightarrow f_1(x)$ is not a unit of R ...(1)

$\Rightarrow f_1(x)$ is not a unit of $R[x]$

Since $f(x)$ is an irreducible element of $R[x]$, so

$$f(x) = a f_1(x) \Rightarrow a = c(f) \text{ must be a unit, using (1).}$$

Hence $f(x)$ is a primitive polynomial.

Condition is sufficient

Conversely, if $f(x)$ is an irreducible element of R, then $f(x)$ is an irreducible element of $R[x]$. [See Theorem 3.2.3]

Suppose now $f(x)$ is an irreducible, primitive polynomial of $R[x]$. Let

$$f(x) = g(x)\, h(x), \text{ where } g(x), h(x) \in R[x]. \quad ...(2)$$

Since $f(x)$ is an irreducible polynomial,

$$\text{either } deg\ g(x) = 0 \quad \text{or} \quad deg\ h(x) = 0.$$

Let $deg\ g(x) = 0 \Rightarrow g(x)$ is a constant polynomial.

Let $g(x) = \alpha \neq 0 \in R$. We have

$$c(f) = c(g)\, c(h) = \alpha\beta,$$

where $c(g) = c(\alpha) = \alpha$, as $\alpha \in R$ and $c(h) = \beta \in R$, say.

Since $f(x)$ is a primitive polynomial, $c(f)$ is a unit of R.

Let $c(f) = u \in R$, where $u \mid 1$.

$\therefore \quad u = \alpha\beta \Rightarrow \alpha \mid u$ and $u \mid 1 \Rightarrow \alpha \mid 1$

$\Rightarrow \quad g(x) = \alpha$ is a unit of R

$\Rightarrow g(x)$ is a unit of $R[x]$, since units of R and $R[x]$ are the same.

Hence, by (2), $f(x)$ is an irreducible element of $R[x]$.

We now investigate as to when a polynomial with integer coefficients is irreducible over $\mathbf{Q}$ (field of rational numbers) in the following :

Theorem 3.4.8. (Eisenstein Criterion of Irreducibility over Q) *Let* $f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_{n-1} x^{n-1} + a_n x^n$ *be a polynomial with integer coefficients. Let p be a prime number such that*

$$p \mid a_0,\ p \mid a_1, \ldots, p \mid a_{n-1};\ p \nmid a_n \text{ and } p^2 \nmid a_0.$$

Then $f(x)$ *is irreducible over* $\mathbf{Q}$, *the field of rational numbers.*

Proof. Case I. *Let* $f(x)$ *be primitive in* $\mathbf{Z}[x]$.

Suppose $f(x)$ is not irreducible over $\mathbf{Q}$. Then $f(x)$ can be factored as a product of two polynomials having rational coefficients. Since $f(x)$ is primitive in $\mathbf{Z}[x]$, $f(x)$ can be factored as a product of two polynomials having integer coefficients. [See Corollary of Theorem 3.4.3]

Let $f(x) = g(x)\, h(x)$, where $g(x), h(x) \in \mathbf{Z}[x]$;

and $\deg g(x) > 0, \deg h(x) > 0.$

Let $g(x) = b_0 + b_1 x + \ldots + b_r x^r,\ h(x) = c_0 + c_1 x + \ldots + c_s x^s,$

where b_i's and c_i's are integers and $r > 0, s > 0$.

The relation $f(x) = g(x)\, h(x)$ implies

$$a_0 + a_1 x + \ldots + a_n x^n = (b_0 + b_1 x + \ldots + b_r x^r)(c_0 + c_1 x + \ldots + c_s x^s) \quad \ldots(1)$$

Comparing the constants on both the sides of (1), we get

$$a_0 = b_0 c_0.$$

Since $p \mid a_0$, $p \mid b_0 c_0 \Rightarrow p \mid b_0$ or $p \mid c_0$, as p is prime. Further p cannot divide both b_0 and c_0, for otherwise, $p^2 \mid b_0 c_0$ *i.e.*, $p^2 \mid a_0$, a contradiction.

Let us take $p \mid b_0$ and $p \nmid c_0$.

It is clear that p does not divide all the coefficients of $g(x)$, for then by (1), p will divide all the coefficients of $f(x)$, which is impossible, as p does not divide a_n. Let b_k be the **first** coefficient of $g(x)$ which is not divisible by p, $k \leq r < n$. It means

$$p \mid b_0,\ p \mid b_1, \ldots, p \mid b_{k-1}, p \nmid b_k.$$

Comparing the coefficients of x^k on both the sides of (1), we get

$$a_k = b_0 c_k + b_1 c_{k-1} + \ldots + b_{k-1} c_1 + b_k c_0. \quad \ldots(2)$$

Since $k < n$, $p \mid a_k$ (by the given hypothesis).

Since $p \mid b_0,\ p \mid b_1, \ldots, p \mid b_{k-1}$; so

$$p \mid (b_0 c_k + b_1 c_{k-1} + \ldots + b_{k-1} c_1).$$

It follows that

$p \mid [a_k - (b_0 c_k + b_1 c_{k-1} + \ldots + b_{k-1} c_1)$ *i.e.*, $p \mid b_k c_0$, by (2)

$\Rightarrow$ $p \mid b_k$ or $p \mid c_0$, as p is prime.

Since p does not divide both b_k and c_0, we arrive at a contradiction.

Hence $f(x)$ is irreducible over $\mathbf{Q}$.

Case II. *Suppose $f(x)$ is not primitive in $\mathbf{Z}[x]$.*

We can write $f(x) = a f_1(x)$, where $a = c(f) \in \mathbf{Z}$ and $f_1(x)$ is primitive in $\mathbf{Z}[x]$.

Let $f_1(x) = b_0 + b_1 x + \ldots + b_n x^n \in \mathbf{Z}[x]$. Then

$$f(x) = a f_1(x) \Rightarrow a_0 = ab_0, a_1 = ab_1, \ldots, a_n = ab_n.$$

Since $p \dagger a_n$, so $p \dagger ab_n \Rightarrow p \dagger a$ and $p \dagger b_n$, as p is prime.

Since $p \dagger a$ and p divides $a_0, a_1, \ldots, a_{n-1}$, so $p \mid b_0, p \mid b_1, \ldots, p \mid b_{n-1}$.

Also $p \dagger b_n$ and $p^2 \dagger b_0$.

The above conditions together with the primitivity of $f_1(x) \in \mathbf{Z}[x]$ imply that $f_1(x)$ is irreducible over $\mathbf{Q}$. [Apply case I]

Hence $f(x) = a f_1(x)$ is irreducible over $\mathbf{Q}$.

Remark. *Eisenstein's criterion is not necessary for the irreducibility of any polynomial in $\mathbf{Z}[x]$ over $\mathbf{Q}$.* For example, $x^2 + 1 \in \mathbf{Z}[x]$ is irreducible over $\mathbf{Q}$, but there is no prime number p such that p divides 1.

Ex. *State and prove Eisenstein Criterion of irreducibility of a polynomial with integral coefficients over the field of rational numbers. Is this criterion necessary ? Explain.* [D.U., 1993]

EXAMPLES

Example 3.4.1. *Show that $x^3 - 2$ is irreducible over $\mathbf{Q}$.*

Solution. We have $x^3 - 2 = -2 + 0x + 0x^2 + 1 \cdot x^3$.

We write $a_0 = -2$, $a_1 = a_2 = 0$ and $a_3 = 1$.

Then $p = 2$ divides a_0, a_1, a_2 and $p \dagger a_3$, $p^2 \dagger a_0$.

Hence $x^3 - 2$ is irreducible over $\mathbf{Q}$.

Example 3.4.2. *If p is a prime number, prove that the polynomial $x^n - p$ is irreducible over the rationals.* [D.U., 1995]

Solution. Let $f(x) = x^n - p = -p + 0x + 0x^2 + \ldots + 0x^{n-1} + 1 \cdot x^n$.

We write $a_0 = -p, a_1 = a_2 = \ldots = a_{n-1} = 0, a_n = 1$.

Then p divides $a_0, a_1, \ldots, a_{n-1}$; but $p \dagger a_n$ and $p^2 \dagger a_0$. Hence $x^n - p$ is irreducible over the rationals.

Example 3.4.3. *Show that $x^3 - 6x + 2$ is irreducible over the rationals.* [D.U., 1997]

Solution. $x^3 - 6x + 2 = 2 - 6x + 0x^2 + 1 \cdot x^3$.

We write $a_0 = 2,\ a_1 = -6,\ a_2 = 0,\ a_3 = 1$.

Then $p = 2$ divides a_0, a_1, a_2 ; but $p \nmid a_3$ and $p^2 \nmid a_0$.

Hence $x^3 - 6x + 2$ is irreducible over the rationals.

Example 3.4.4. *Prove that the polynomial $x^4 + 2x + 2$ is irreducible over the field of rational numbers.*

Please try yourself.

Example 3.4.5. *Prove that the polynomial $1 + x + x^2 + \ldots + x^{p-1}$, where p is a prime number, is irreducible over the field of rational numbers.* [D.U., 1990]

Solution. Notice that we cannot directly apply Eisenstein criterion to prove that the given polynomial is irreducible over **Q**. We now proceed as follows :

Let $$f(x) = 1 + x + x^2 + \ldots + x^{p-1} = \frac{x^p - 1}{x - 1}.$$

Replacing x by $x + 1$, we get

$$f(x+1) = \frac{(1+x)^p - 1}{x}$$

$$= \frac{1}{x}\left[1 + p_{c_1} x + p_{c_2} x^2 + \ldots + p_{c_{p-1}} x^{p-1} + x^p - 1\right]$$

$$= p + \frac{1}{2} p\,(p-1)\,x + \ldots + p\,x^{p-2} + 1 \cdot x^{p-1}.$$

We write $a_0 = p,\ a_1 = \frac{1}{2} p\,(p-1),\ \ldots,\ a_{p-1} = p,\ a_p = 1$.

Then p divides $a_0, a_1, \ldots, a_{p-1}$; but p does not divide a_p and p^2 does not divide a_0. By Eisenstein criterion of irreducibility, $f(x+1)$ is irreducible over **Q**. Now we show that $f(x)$ is irreducible over **Q**. Suppose this is false. Then we can write

$$f(x) = g(x)\,h(x), \quad \text{where} \quad g(x), h(x) \in \mathbf{Q}[x]\ ;$$

and $$deg\ g(x) > 0 \quad \text{and} \quad deg\ h(x) > 0.$$

$$\therefore \quad f(x+1) = g(x+1)\,h(x+1),$$

where $g(x+1), h(x+1) \in \mathbf{Q}[x]$; $deg\ g(x+1) > 0$ and $deg\ h(x+1) > 0$. It means that $f(x+1)$ is not irreducible over **Q**, a contradiction. Hence $f(x)$ is irreducible over **Q**.

Example 3.4.6. *Show that $x^4 + x^3 + x^2 + x + 1$ is irreducible over the rationals.*

Solution. Taking $p = 5$ in Example 3.4.5, the given polynomial is irreducible over **Q**. However, we give an independent proof.

Let $f(x) = x^4 + x^3 + x^2 + x + 1 = \dfrac{x^5 - 1}{x - 1}$

$\therefore\ f(x+1) = \dfrac{(1+x)^5 - 1}{x}$

$$= \frac{1}{x}\left(1 + 5_{c_1}x + 5_{c_2}x^2 + 5_{c_3}x^3 + 5_{c_4}x^4 + x^5 - 1\right)$$

$$= 5 + 10x + 10x^2 + 5x^3 + 1\,.\,x^4.$$

We write $a_0 = 5, a_1 = 10,\ a_2 = 10, a_3 = 5,\ a_4 = 1$. Then $p = 5$ divides a_0, a_1, a_2, a_3 but $p \nmid a_4$ and $p^2 \nmid a_0$. Hence $f(x+1)$ is irreducible over $\mathbf{Q}$. As argued in Example 3.4.5., $f(x)$ is also irreducible over $\mathbf{Q}$.

Example 3.4.7. *Discuss the irreducibility of* $f(x) = x^4 + 1$, *over rationals.* [D.U., 1999]

Solution. We have $f(x-1) = (x-1)^4 + 1$

or $$f(x-1) = (x^4 - 4x^3 + 6x^2 - 4x + 1) + 1$$

$$= 2 - 4x + 6x^2 - 4x^3 + x^4.$$

We write $a_0 = 2,\ a_1 = -4,\ a_2 = 6,\ a_3 = -4,\ a_4 = 1.$

Then $p = 2$ divides a_0, a_1, a_2, a_3 ; but $p \nmid a_4$ and $p^2 \nmid a_0$. By Eisenstein criterion of irreducibility, $f(x-1)$ is irreducible over $\mathbf{Q}$. Hence $f(x) = x^4 + 1$ is irreducible over $\mathbf{Q}$, for otherwise

$$f(x) = g(x)\,h(x)\ ;\ g(x), h(x) \in \mathbf{Q}[x],$$

and $deg\ g(x) > 0$ and $deg\ h(x) > 0$ imply that

$$f(x-1) = g(x-1)\,h(x-1),$$

where $g(x-1), h(x-1) \in \mathbf{Q}[x]$ are both of positive degree and so $f(x-1)$ is reducible over $\mathbf{Q}$, a contradiction.

Example 3.4.8. *Using Eisenstein Criterion, show that* $8x^3 - 6x - 1$ *is an irreducible polynomial over rationals.* [D.U., 1991]

Solution. Let $f(x) = 8x^3 - 6x - 1$. Then

$$f(x-1) = 8(x-1)^3 - 6(x-1) - 1$$

$$= 8(x^3 - 3x^2 + 3x - 1) - 6x + 5$$

$$= -3 + 18x - 24x^2 + 8x^3.$$

We write $a_0 = -3,\ a_1 = 18,\ a_2 = -24,\ a_3 = 8.$

Then $p = 3$ divides a_0, a_1, a_2 ; but $p \nmid a_3$ and $p^2 \nmid a_0$. By Eisenstein criterion of irreducibility, $f(x-1)$ is irreducible over $\mathbf{Q}$. Hence $f(x)$ is irreducible over $\mathbf{Q}$.

Example 3.4.9. *Show that* $f(x) = x^3 + x^2 - 2x - 1$ *is irreducible over rationals.*

Solution. We have

$$f(x+2) = (x+2)^3 + (x+2)^2 - 2(x+2) - 1$$

$$= (x^3 + 6x^2 + 12x + 8) + (x^2 + 4x + 4) - 2x - 5$$
$$= 7 + 14x + 7x^2 + x^3$$

We write $a_0 = 7,\ a_1 = 14,\ a_2 = 7,\ a_3 = 1.$

Then $p = 7$ divides a_0, a_1, a_2 ; but $p \nmid a_3$ and $p^2 \nmid a_0$.

By Eisenstein criterion of irreducibility, $f(x+2)$ is irreducible over $\mathbf{Q}$. Hence $f(x)$ is irreducible over $\mathbf{Q}$.

Remark. If may be verified that the polynomials $f(x-1), f(x+1)$ fail to satisfy the conditions of Eisenstein criterion for the given $f(x)$.

Example 3.4.10. *Find out if* $x^3 + 3x + 1$ *is irreducible over* $\mathbf{Q}$? [D.U., 1999]

Solution. Let $f(x) = x^3 + 3x + 1.$

$$\therefore \quad f(x+2) = (x+2)^3 + 3(x+2) + 1 = 15 + 15x + 6x^2 + x^3.$$

We write $a_0 = 15,\ a_1 = 15,\ a_2 = 6,\ a_3 = 1.$

Then $p = 3$ divides a_0, a_1, a_2 ; but $p \nmid a_3$ and $p^2 \nmid a_0$.

By Eisenstein Criterion $f(x+2)$ is irreducible over $\mathbf{Q}$. Hence $f(x)$ is irreducible over $\mathbf{Q}$.

In the following examples, we discuss the irreducibility of polynomials over fields other than the field $\mathbf{Q}$ of rational numbers.

Example 3.4.11. *Show that* $x^2 + 1$ *is irreducible over the integers mod* 7.

Solution. We have $F = \mathbf{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$.

Let $$x^2 + 1 = (x+a)(x+b),\ a, b \in F.$$

Comparing the coefficients of x and constants on both the sides, we get

$$0 = a + b, \qquad \ldots(1)$$
$$1 = ab. \qquad \ldots(2)$$

(1) is satisfied when $(a, b) = (0, 0), (1, 6), (2, 5), (3, 4), (4, 3), (5, 2), (6, 1)$. For these values of a and b, $ab = 0, 6, 3, 5, 5, 3, 6$.

Thus (2) is not satisfied and so $x^2 + 1$ is irreducible over F.

Aliter. Since $f(x) = x^2 + 1$ is not satisfied by the elements of F (i.e. $f(\alpha) \neq 0\ \forall\ \alpha \in F$), $f(x)$ has no linear factors in $F[x]$. This shows that $f(x) = x^2 + 1$ is irreducible over $F = \mathbf{Z}_7$.

Example 3.4.12. *Factorize* $x^2 + x + 5$ *in* $F[x]$, *where* F *is the field of integers mod* 11. [D.U., 1997]

Solution. We have $F = \mathbf{Z}_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.

Let $$x^2 + x + 5 = (x+a)(x+b),\ a, b \in F.$$

Comparing the coefficients of x and constant terms on both the sides we get

$$1 = a + b, \quad \ldots(1)$$
$$5 = ab. \quad \ldots(2)$$

(1) is satisfied when $(a, b) = (1, 0), (2, 10), (3, 9), (4, 8), (5, 7), (6, 6)$.

Consequently, $ab = 0, 9, 5, 10, 2, 3$.

We see that (1) and (2) are both satisfied when $a = 3, b = 9$.

Hence $x^2 + x + 5 = (x + 3)(x + 9)$ in $\mathbf{Z}_{11}$.

Example 3.4.13. *Factorize $x^2 + 3x + 1$ in $F[x]$, where F is the field of integer mod 11.* [Ans. $(x + 5)(x + 9)$]

Please try yourself.

Example 3.4.14. *Prove that $x^3 - 9$ is reducible over the integers mod 11.*

Solution. $F = \mathbf{Z}_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.

Since $9 + 2 = 0$ in $\mathbf{Z}_{11}$, so $-9 = 2$ in $\mathbf{Z}_{11}$.

Let $x^3 - 9 = x^3 + 2 = (x + a)(x^2 + bx + c)$, where $a, b, c \in F$.

Comparing the coefficients of x^2, x and constant terms on both sides, we get

$$0 = a + b,$$
$$0 = ab + c,$$
$$2 = ac.$$

The above equations are all satisfied if $a = 7, b = 4$ and $c = 5 \in F$.

Hence $x^3 - 9$ is reducible over $\mathbf{Z}_{11}$ and

$$x^3 - 9 = x^3 + 2 = (x + 7)(x^2 + 4x + 5).$$

Example 3.4.15. *Factorize $x^3 + 9$ over the field of integers mod 11.* [Ans. $(x + 4)(x^2 + 7x + 5)$]

Please try yourself.

Example 3.4.16. *Factorize $x^3 + 2x + 2$ over the field of integers mod 5.* [Ans. $(x + 2)(x^2 + 3x + 1)$]

Please try yourself.

Example 3.4.17. *Prove that $x^2 + x + 1$ is irreducible over the field of integers mod 2.*

Hint. $x^2 + x + 1 = (x + a)(x + b)$; $a, b \in F = \{0, 1\}$

Then $1 = a + b$ and $1 = ab$ are both not satisfied in F.

Example 3.4.18. *Let F be the field of integers modulo 5. Show that the polynomial $x^2 + 2x + 3$ is irreducible over F. Use this to construct a field containing 25 elements.* [D.U., 1992]

Solution. We have $F = \mathbf{Z}_5 = \{0, 1, 2, 3, 4\}$.

Let $x^2 + 2x + 3 = (x + a)(x + b)$; $a, b \in F$.

Comparing the coefficients of x and constants on both the sides, we get

$$2 = a + b, \quad \text{...(1)}$$

$$3 = ab. \quad \text{...(2)}$$

(1) is satisfied for $(a, b) = (0, 2), (1, 1), (3, 4), (2, 0), (4, 3)$. For these values of a and b, $ab = 0, 1, 2, 0, 2$ *i.e.*, (2) is never satisfied. Consequently, $x^2 + 2x + 3$ is irreducible over F. Hence, by Theorem 3.4.6, $\dfrac{F[x]}{\langle x^2 + 2x + 3 \rangle}$ is a field. Any element of this field is $f(x) + A$, where $f(x) \in F[x]$, $A = \langle x^2 + 2x + 3 \rangle$. By Division algorithm in $F[x]$, for $f(x) \in F[x]$, $x^2 + 2x + 3 \in F[x]$, there exist $t(x), r(x) \in F[x]$ such that

$$f(x) = (x^2 + 2x + 3)\, t(x) + r(x), \quad \text{...(1)}$$

where $r(x) = 0$ or $deg\ r(x) < deg\ (x^2 + 2x + 3) = 2$.

We may take $r(x) = \alpha x + \beta$, where $\alpha, \beta \in F$.

$\therefore$ $f(x) + A = r(x) + (x^2 + 2x + 3)\, t(x) + A$, by (1)

or $f(x) + A = r(x) + A = \alpha x + \beta + A$, ...(2)

since $(x^2 + 2x + 3)\, t(x) \in A = \langle x^2 + 2x + 3 \rangle$.

In (2), we see that $\alpha, \beta \in F = Z_5$ and $o(Z_5) = 5$. Consequently, each of α and β can be selected in 5 ways. Hence, by (2), the number of elements of the field $\dfrac{F[x]}{\langle x^2 + 2x + 3 \rangle}$ is $5^2 = 25$.

Example 3.4.19. *Prove that $x^2 + x + 4$ is irreducible over F, the field of integers mod 11. Also prove that $\dfrac{F[x]}{\langle x^2 + x + 4 \rangle}$ is a field having 121 elements.*

Solution. We have

$$F = Z_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}.$$

We can prove the irreducibility of $x^2 + x + 4$ over F by the method as described in Example 3.4.18. However, another convenient method is given below :

We observe that $f(x) = x^2 + x + 4$ is not satisfied by the elements of F (*i.e.*, $f(\alpha) \neq 0$ for each $\alpha \in F$). Consequently, $x^2 + x + 4$ is not expressible as a product of two linear factors in $F[x]$. Hence $x^2 + x + 4$ is irreducible over F. By Theorem 3.4.6., $\dfrac{F[x]}{\langle x^2 + x + 4 \rangle}$ is a field. Any element of this field is of the form $f(x) + \langle x^2 + x + 4 \rangle$, where $f(x) \in F[x]$.

By Division algorithm in $F[x]$, there exist $t(x), r(x) \in F[x]$ such that

$$f(x) = t(x)(x^2 + x + 4) + r(x), \text{ where}$$

$$r(x) = 0 \text{ or } deg\ r(x) < deg\ (x^2 + x + 4) = 2.$$

We may take $r(x) = \alpha x + \beta \in F[x]$.

Since $t(x)(x^2+x+4) \in \langle x^2+x+4 \rangle$, therefore

$$f(x) + \langle x^2+x+4 \rangle = r(x) + \langle x^2+x+4 \rangle$$
$$= \alpha x + \beta + \langle x^2+x+4 \rangle. \quad \ldots(1)$$

In the above expression $\alpha, \beta \in F = \mathbf{Z}_{11}$ and $o(\mathbf{Z})_{11} = 11$. Consequently, each of α and β can be selected in 11 ways. Hence, by (1), the number of elements of the field $\frac{F[x]}{\langle x^2+x+4 \rangle}$ is $11^2 = 121$.

Example 3.4.20. *Prove that x^2+1 is irreducible over the field F of integers mod 11. Also prove that $\frac{F[x]}{\langle x^2+1 \rangle}$ is a field having 121 elements.*

Hint. Similar to Example 3.4.19.

Example 3.4.21. *Construct a field having 121 elements.*

Hint. Show that x^2+1 is an irreducible polynomial over $F = \mathbf{Z}_{11}$. Hence $\frac{F[x]}{\langle x^2+1 \rangle}$ is a field having 121 elements.

Example 3.4.22. *Find a polynomial of degree 3 irreducible over the ring of integers J_3, mod 3. Use it to construct a field having 27 elements.*

Solution. Let us consider $f(x) = x^3+2x+1 \in F[x]$, where $F = J_3 = \{0, 1, 2\}$. Since this polynomial is not satisfied by the elements of F (*i.e.*, $f(\alpha) \neq 0 \ \forall \ \alpha \in F$), $f(x)$ has no linear factor in $F[x]$. Hence x^2+2x+1 is irreducible over F. By Theorem 3.4.6., $\frac{F[x]}{\langle x^3+2x+1 \rangle}$ is a field. Any element of this field is of the form $f(x) + \langle x^3+2x+1 \rangle$, $f(x) \in F[x]$.

By Division algorithm in $F[x]$, there exist $t(x), r(x) \in F[x]$ such that $f(x) = t(x)(x^3+2x+1) + r(x)$, where

$r(x) = 0$ or $deg\, r(x) < deg\,(x^3+2x+1) = 3$. We may take $r(x) = \alpha + \beta x + \gamma x^2 \in F[x]$. Since $t(x)(x^3+2x+1) \in \langle x^3+2x+1 \rangle$, so

$$f(x) + \langle x^3+2x+1 \rangle = r(x) + \langle x^3+2x+1 \rangle$$
$$= \alpha + \beta x + \gamma x^3 + \langle x^3+2x+1 \rangle. \quad \ldots(1)$$

Since $o(F) = 3$, each of α, β, γ can be selected in 3 ways. Hence, by (1), the number of elements of the field $\frac{F[x]}{\langle x^3+2x+1 \rangle}$ is $3^3 = 27$.

Example 3.4.23. *Show that x^4+x+3 is reducible over the field $\mathbf{Z}_5$ of integers modulo 5.*

Solution. Let $x^4+x+3 = (x^2+ax+b)(x^2+cx+d)$,

where $a, b, c, d \in F \in \mathbf{Z}_5 = \{0, 1, 2, 3, 4\}$.

Comparing the coefficients of x^3, x^2, x and constant terms on both the sides, we get

$$0 = a + c$$
$$0 = ac + b + d$$
$$1 = ad + bc$$
$$3 = bd.$$

The above four equations are satisfied by the values :

$$a = 3,\ c = 2,\ b = 1 \text{ and } d = 3.$$

Hence $x^4 + x + 3 = (x^2 + 3x + 1)(x^2 + 2x + 3)$.

Example 3.4.24. *Construct a field having 625 elements.*

Hint. Construct an irreducible polynomial of degree 4 over the field F of integers modulo 5, $F = \mathbf{Z}_5 = \{0, 1, 2, 3, 4\}$. As explained in Example 3.4.23, verify that $x^4 + x + 4$ is irreducible of degree 4 over F. Hence $\dfrac{F[x]}{\langle x^4 + x + 4 \rangle}$ is a field having $5^4 = 625$ elements.

Example 3.4.25. *If $f(x)$ is in $F[x]$, where F is the field of integers mod p, p a prime, and $f(x)$ is irreducible over F of degree n, prove that $\dfrac{F[x]}{\langle f(x) \rangle}$ is a field with p^n elements.*

Solution. Since $f(x)$ is irreducible over $F = \mathbf{Z}_p$, $\dfrac{F[x]}{\langle f(x) \rangle}$ is a field. [Theorem 3.4.6]

Any element of this field is $a(x) + \langle f(x) \rangle$, where $a(x) \in F[x]$.

By Division algorithm in $F[x]$, there exist $t(x), r(x) \in F[x]$ such that

$$a(x) = f(x)\, t(x) + r(x), \qquad \ldots(1)$$

where $r(x) = 0$ or $\deg r(x) < \deg f(x) = n$.

We take $r(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_{n-1} x^{n-1} \in F[x]$

From (1), $a(x) + \langle f(x) \rangle = r(x) + \langle f(x) \rangle$, since $f(x)\, t(x) \in \langle f(x) \rangle$.

$\therefore$ $a(x) + \langle f(x) \rangle = a_0 + a_1 x + \ldots + a_{n-1} x^{n-1} + \langle f(x) \rangle$ ...(1)

where $a_0, a_1, \ldots, a_{n-1} \in F = \mathbf{Z}_p$, $o(\mathbf{Z}_p) = p$.

Since each of $a_0, a_1, \ldots, a_{n-1}$ (which are n in number) can be selected in p ways, so by (1), the number of elements of $\dfrac{F[x]}{\langle f(x) \rangle}$ is p^n.

Example 3.4.26. *Find out if $x^3 + 3x + 1$ is irreducible over $\mathbf{Q}$. Write an element of $\mathbf{Q}[x]/\langle x^3 + 3x + 1 \rangle$.*

Is $\mathbf{Q} \subseteq \mathbf{Q}[x]/\langle x^3 + 3x + 1 \rangle$? [D.U., 1998]

Solution. By Example 3.4.10, $x^3 + 3x + 1$ is irreducible over $\mathbf{Q}$.

It follows, by Theorem 3.4.6, that

$$\frac{\mathbf{Q}[x]}{\langle x^3+3x+1\rangle} \text{ is a field.}$$

Any element of $\dfrac{\mathbf{Q}[x]}{\langle x^3+3x+1\rangle}$ is of the form

$$f(x)+\langle x^3+3x+1\rangle, \quad \text{where } f(x)\in \mathbf{Q}[x].$$

By Division algorithm in $\mathbf{Q}[x]$, for $f(x)\in \mathbf{Q}[x]$ and $x^3+3x+1\in \mathbf{Q}[x]$, there exist $t(x)$ and $r(x)\in \mathbf{Q}[x]$ such that

$$f(x)=t(x)(x^3+3x+1)+r(x), \qquad ...(1)$$

where $\deg r(x) < \deg (x^3+3x+1)=3.$

We may choose $r(x)=a_0+a_1x+a_2x^2\in \mathbf{Q}[x]$.

By (1), $f(x)+A=r(x)+t(x)(x^3+3x+1)+A,$

where $A=\langle x^3+3x+1\rangle=\{(x^3+3x+1)g(x): g(x)\in \mathbf{Q}[x]\}.$

$\therefore$ $f(x)+A=r(x)+A$, since $t(x)(x^3+3x+1)\in A$.

Hence $f(x)+\langle x^3+3x+1\rangle=a_0+a_1x+a_2x^2+\langle x^3+3x+1\rangle$, ...(2)

where $a_0, a_1, a_2\in \mathbf{Q}$.

From (2), it is clear that $\mathbf{Q}$ is not contained in $\dfrac{\mathbf{Q}[x]}{\langle x^3+3x+1\rangle}$.

EXERCISES

1. Show that the following polynomials are irreducible over $\mathbf{Q}$:
   (*i*) $x^3-5x+10$ (*ii*) $2x^4-3x^2+3$
   (*iii*) $5x^4+3x^3-6x^2+15x+6$ (*iv*) x^2+x+1.
   [**Hint of (*iv*).** Verify that $f(x+1)$ is irreducible over $\mathbf{Q}$.]
2. Show that x^3+3x+2 is irreducible over the field of integers mod 7.
3. Show that x^2+1 is reducible over the field of integers mod 5. [**Ans.** $(x+2)(x+3)$]
4. Construct a field having 25 elements.
   [**Hint.** Verify that x^2+2 is irreducible over $F=\mathbf{Z}_5$.]
5. Show that x^3-2 is irreducible over $\mathbf{Q}$, the field of rational numbers. Write down an element of $\mathbf{Q}[x]/\langle x^3-2\rangle$.
6. Let F be the field of real numbers. Prove that $F[x]/\langle x^2+1\rangle$ is a field isomorphic to the field of complex numbers.
   [**Hint.** x^2+1 is irreducible over F and so $F[x]/\langle x^2+1\rangle$ is a field. Any element of this field is a_0+a_1x+A ; where $a_i\in F$ and $A=\langle x^2+1\rangle$.
   We have $a_0+a_1x+A=a_0+a_1t$, where
   $t=x+A$ and $t^2+1=x^2+A+1=x^2+1+A=A=\bar{0}\in F[x]/A$

The mapping $\theta : \mathbf{C} \to F[x]/A$ defined by

$$\theta(a+ib) = a+bt,\ t = x+A$$

is homomorphism, onto and 1 – 1.]

7. Show that x^2+1 and x^2+x+4 are irreducible over F, the field of integers modulo 11. Prove also that $\dfrac{F[x]}{\langle x^2+1\rangle}$ and $\dfrac{F[x]}{\langle x^2+x+4\rangle}$ are isomorphic fields, each having 121 elements.

[**Hint.** Refer to Examples 3.4.19, 3.4.20. Verify that the mapping

$$\theta : \frac{F[x]}{\langle x^2+1\rangle} \to \frac{F[x]}{\langle x^2+x+4\rangle} \text{ defined by}$$

$$\theta[\alpha x+\beta+\langle x^2+1\rangle] = \alpha x+(\beta-5\alpha)+\langle x^2+x+4\rangle$$

is a ring homomorphism. Further θ is an isomorphism, since homomorphism of a field is either an isomorphism or takes each element into zero. Since the two fields have the same number of elements, θ is onto.]

8. Show that the polynomial x^3-x+1 is irreducible over $\mathbf{Q}$, even though Eisenstein Criterion is not applicable.

[**Hint.** Let, if possible, x^3-x+1 be reducible over $\mathbf{Q}$. Then it has a root $\alpha \in \mathbf{Q}$. Let $\alpha = m/n$, where $m, n \in \mathbf{Z}$, $n \neq 0$, $(m, n) = 1$. We have

$$\frac{m^3}{n^3} - \frac{m}{n} + 1 = 0 \Rightarrow m^3 - mn^2 + n^3 = 0 \Rightarrow m^3 = n^2(m-n)$$

$\Rightarrow \quad n^2 \mid m^3 \Rightarrow n \mid m^3 \Rightarrow n = \pm 1$, as $(m, n) = 1$

$\therefore \quad m^3 = n^2(m-n)$ becomes $m^3 = m \pm 1 \Rightarrow m(m^2-1) = \pm 1$,

which is impossible for all integral values of m. Hence x^3-x+1 is irreducible over $\mathbf{Q}$. Eisenstein criterion is not applicable, since there does not exist any prime p such that $p \mid 1$.]

9. Show that the polynomial x^3-x-1 is irreducible over $\mathbf{Q}$.

[**Hint.** Similar to Ex. 8 above]

10. Let F be a field and $f(x) \in F[x]$ be a polynomial of degree > 1. If $f(\alpha) = 0$ for some $\alpha \in F$, then $f(x)$ is reducible over F.

Solution. Since $\alpha \in F$, $x-\alpha \in F[x]$. Also $f(x) \in F[x]$. By Division algorithm in $F[x]$, there exist $t(x), r(x) \in F[x]$ such that $f(x) = (x-\alpha)\,t(x) + r(x)$, where $r(x) = 0$ or $\deg r(x) < \deg(x-\alpha) = 1$ *i.e.*, $\deg r(x) = 0$ *i.e.*, $r(x)$ is a constant polynomial. We write $r(x) = r \in F$. We have $f(\alpha) = 0 + r$ *i.e.*, $r = 0$ and so

$$f(x) = (x-\alpha)\,t(x), \text{ where } \deg t(x) = \deg f(x) - 1 > 0.$$

Hence $f(x)$ is reducible over F.

11. Give an example of a polynomial, which is

(*i*) primitive and irreducible.

[**Hint.** $x^3 - 6x + 3 \in \mathbf{Q}[x]$]

(*ii*) primitive and reducible.

[**Hint.** $x^3 - 5x + 6$ is primitive and reducible over $\mathbf{Z}$. Notice that $x^2 - 5x + 6 = (x-2)(x-3)$.]

(*iii*) not primitive but irreducible.

[**Hint.** $2x^2 - 4 \in \mathbf{Z}[x]$ is not primitive but irreducible over $\mathbf{Z}$.]

(*iv*) not primitive but reducible.

[**Hint.** $2x^2 - 8 \in \mathbf{Z}$ is not primitive but reducible over $\mathbf{Z}$, since $2x^2 - 8 = (2x-4)(x+2)$.]

12. Examine whether the polynomial $x^3 + 3x^2 + x - 4$ is irreducible over (*i*) the field of integers modulo 5, (*ii*) the field of integers modulo 7.

[**Ans.** (*i*) irreducible over $\mathbf{Z}_5$ (*ii*) reducible over $\mathbf{Z}_7$.]

13. Let R be a U.F.D. Show that every prime element in R generates a prime ideal.

[**Hint.** Let p be a prime element of $R \Rightarrow p$ is an irreducible element of $R \Rightarrow \langle p \rangle$ is a maximal ideal of $R \Rightarrow \langle p \rangle$ is a prime ideal of R, since every maximal ideal of a commutative ring with unity is a prime ideal.]

14. Prove that the ideal $\langle x^3 + x + 1 \rangle$ in the polynomial ring $\mathbf{Z}_2[x]$ is a prime ideal.

[**Hint.** Since $x^3 + x + 1$ is not satisfied by the elements of $\mathbf{Z}_2 = \{0, 1\}$, $x^3 + x + 1$ is an irreducible polynomial in $\mathbf{Z}_2[x]$. Hence $\langle x^3 + x + 1 \rangle$ is a maximal ideal of $\mathbf{Z}_2[x] \Rightarrow \langle x^3 + x + 1 \rangle$ is a prime ideal of $\mathbf{Z}_2[x]$.]

15. Prove that the ideal $\langle x^3 - x - 1 \rangle$ is a prime ideal of the polynomial ring $\mathbf{Z}_3[x]$.

3.5 $R[x]$ as U.F.D.

In this section we shall prove a major theorem which states :

R is a U.F.D. $\Rightarrow$ $R[x]$ is a U.F.D.

To establish this result we need the following lemmas. Let R be a U.F.D. Since R is an integral domain, R has a field of quotients F (say). We can consider $R[x]$ to be a subring of $F[x]$.

Lemma 3.5.1. *Let R be a U.F.D. and F its field of quotients. Then any $f(x) \in F[x]$ can be written as $f(x) = \dfrac{f_0(x)}{a}$, where $a \in R$ and $f_0(x) \in R[x]$.*

Proof. Let $f(x) = \alpha_0 + \alpha_1 x + \ldots + \alpha_n x^n \in F[x]$, $\alpha_i \in F$.

Since F is a quotient field of R, we can write

$$\alpha_i = \frac{b_i}{a_i};\ b_i \in R,\ a_i \neq 0 \in R,\ 1 \leq i \leq n.$$

Lemma 3.5.2. If $f(x) \in R[x]$ is both primitive and irreducible polynomial in $R[x]$, then $f(x)$ is an irreducible polynomial in $F[x]$.

Proof. Let, if possible, $f(x)$ be a reducible polynomial in $F[x]$, then

$$f(x) = g(x)\, h(x),$$

where $g(x), h(x) \in F[x]$, $\deg g(x) > 0$, and $\deg h(x) > 0$.

By Lemma 3.5.1, we can write

$$g(x) = \frac{g_0(x)}{a}, \quad h(x) = \frac{h_0(x)}{b},$$

where $a, b \in R$ and $g_0(x) \in R[x]$, $h_0(x) \in R[x]$.

By Lemma 3.4.1, we can write

$$g_0(x) = a\, g_1(x), \; h_0(x) = b\, h_1(x),$$

where $a = c(g_0)$, $b = c(h_0)$; $g_1(x)$ and $h_1(x)$ are primitive in $R[x]$.

From (1), (2), (3), we obtain

$$f(x) = \frac{ab}{\alpha\beta}\, g_1(x)\, h_1(x) \quad \text{or} \quad ab\, f(x) = \alpha\beta\, g_1(x)\, h_1(x).$$

Since $f(x)$ is primitive in $R[x]$,

$$c(\text{L.H.S. of (4)}) = ab.$$

Since $g_1(x)\, h_1(x)$ is primitive in $R[x]$ (by Gauss's Lemma),

$$c(\text{R.H.S. of (4)}) = \alpha\beta.$$

It follows that $ab = \alpha\beta$ and so by (4), we have

$$f(x) = g_1(x)\, h_1(x).$$

where $g_1(x), h_1(x) \in R[x]$ and

$$\deg g_0 = \deg g > 0 \text{ and } \deg h_1 = \deg h_0 = \deg h > 0.$$

$f(x)$ is reducible in $R[x]$, which is contrary to
polynomial in $F[x]$
itive polynomial in $R[x]$
irreducible polynomial

(*ii*) primitive and reducible.

[**Hint.** $x^3 - 5x + 6$ is primitive and reducible over $\mathbf{Z}$. Notice that $x^2 - 5x + 6 = (x-2)(x-3)$.]

(*iii*) not primitive but irreducible.

[**Hint.** $2x^2 - 4 \in \mathbf{Z}[x]$ is not primitive but irreducible over $\mathbf{Z}$.]

(*iv*) not primitive but reducible.

[**Hint.** $2x^2 - 8 \in \mathbf{Z}$ is not primitive but reducible over $\mathbf{Z}$, since $2x^2 - 8 = (2x-4)(x+2)$.]

12. Examine whether the polynomial $x^3 + 3x^2 + x - 4$ is irreducible over (*i*) the field of integers modulo 5, (*ii*) the field of integers modulo 7.

[**Ans.** (*i*) irreducible over $\mathbf{Z}_5$ (*ii*) reducible over $\mathbf{Z}_7$.]

13. Let R be a U.F.D. Show that every prime element in R generates a prime ideal.

[**Hint.** Let p be a prime element of $R \Rightarrow p$ is an irreducible element of $R \Rightarrow \langle p \rangle$ is a maximal ideal of $R \Rightarrow \langle p \rangle$ is a prime ideal of R, since every maximal ideal of a commutative ring with unity is a prime ideal.]

14. Prove that the ideal $\langle x^3 + x + 1 \rangle$ in the polynomial ring $\mathbf{Z}_2[x]$ is a prime ideal.

[**Hint.** Since $x^3 + x + 1$ is not satisfied by the elements of $\mathbf{Z}_2 = \{0, 1\}$, $x^3 + x + 1$ is an irreducible polynomial in $\mathbf{Z}_2[x]$. Hence $\langle x^3 + x + 1 \rangle$ is a maximal ideal of $\mathbf{Z}_2[x] \Rightarrow \langle x^3 + x + 1 \rangle$ is a prime ideal of $\mathbf{Z}_2[x]$.]

15. Prove that the ideal $\langle x^3 - x - 1 \rangle$ is a prime ideal of the polynomial ring $\mathbf{Z}_3[x]$.

3.5 $R[x]$ as U.F.D.

In this section we shall prove a major theorem which states :

R is a U.F.D. $\Rightarrow$ $R[x]$ is a U.F.D.

To establish this result we need the following lemmas. Let R be a U.F.D. Since R is an integral domain, R has a field of quotients F (say). We can consider $R[x]$ to be a subring of $F[x]$.

Lemma 3.5.1. *Let R be a U.F.D. and F its field of quotients. Then any $f(x) \in F[x]$ can be written as $f(x) = \dfrac{f_0(x)}{a}$, where $a \in R$ and $f_0(x) \in R[x]$.*

Proof. Let $f(x) = \alpha_0 + \alpha_1 x + \ldots + \alpha_n x^n \in F[x]$, $\alpha_i \in F$.

Since F is a quotient field of R, we can write

$$\alpha_i = \frac{b_i}{a_i}\,;\ b_i \in R,\ a_i \neq 0 \in R,\ 1 \leq i \leq n.$$

$$\therefore \quad f(x) = \frac{b_0}{a_0} + \frac{b_1}{a_1} x + \ldots + \frac{b_n}{a_n} x^n$$

$$= \frac{1}{a} (b_0 a_1 \ldots a_n + b_1 a_0 a_2 \ldots a_n x + b_n a_0 a_1 \ldots a_{n-1} x^n),$$

where $a = a_0 a_1 \ldots a_n \neq 0 \in R$.

Hence $f(x) = \dfrac{f_0(x)}{a}$, where $a \in R$ and

$$f_0(x) = b_0 a_1 \ldots a_n + \ldots + b_n a_0 a_1 \ldots a_{n-1} x^n \in R[x].$$

Lemma 3.5.2. *If $f(x) \in R[x]$ is both primitive and irreducible polynomial in $R[x]$, then $f(x)$ is an irreducible polynomial in $F[x]$.*

Proof. Let, if possible, $f(x)$ be a reducible polynomial in $F[x]$. Then

$$f(x) = g(x)\, h(x), \qquad \ldots(1)$$

where $g(x), h(x) \in F[x]$, $deg\ g(x) > 0$ and $deg\ h(x) > 0$.

By Lemma 3.5.1, we can write

$$g(x) = \frac{g_0(x)}{a}, \; h(x) = \frac{h_0(x)}{b}, \qquad \ldots(2)$$

where $a, b \in R$ and $g_0(x) \in R[x]$, $h_0(x) \in R[x]$.

By Lemma 3.4.1, we can write

$$g_0(x) = \alpha\, g_1(x),\ h_0(x) = \beta\, h_1(x), \qquad \ldots(3)$$

where $\alpha = c(g_0)$, $\beta = c(h_0)$; $g_1(x)$ and $h_1(x)$ are primitive in $R[x]$.

From (1), (2), (3) , we obtain

$$f(x) = \frac{\alpha\beta}{ab}\, g_1(x)\, h_1(x) \text{ or } ab\, f(x) = \alpha\beta\, g_1(x)\, h_1(x). \qquad \ldots(4)$$

Since $f(x)$ is primitive in $R[x]$,

$$c \text{ (L.H.S. of (4))} = ab.$$

Since $g_1(x)\, h_1(x)$ is primitive in $R[x]$ (by Gauss's Lemma),

$$c \text{ (R.H.S. of (4))} = \alpha\beta.$$

It follows that $ab = \alpha\beta$ and so by (4), we have

$$f(x) = g_1(x)\, h_1(x),$$

where $g_1(x), h_1(x) \in R[x]$ and

$$deg\ g_1 = deg\ g_0 = deg\ g > 0 \text{ and } deg\ h_1 = deg\ h_0 = deg\ h > 0.$$

This means that $f(x)$ is reducible in $R[x]$, which is contrary to the given hypothesis.

Hence $f(x)$ is an irreducible polynomial in $F[x]$.

Lemma 3.5.3. *Let $f(x) \in R[x]$ be a primitive polynomial in $R[x]$ and an irreducible polynomial in $F[x]$. Then $f(x)$ is an irreducible polynomial in $R[x]$.*

Proof. Let $f(x) = g(x)\,h(x)\,;\ g(x)\,h(x) \in R[x]$.

$\therefore$ $f(x) = g(x)\,h(x)\,;\ g(x), h(x) \in F[x]$; ...(1)

as $R[x]$ is a subring of $F[x]$.

Since $f(x)$ is an irreducible polynomial in $F[x]$, so, by (1),

either $deg\ g(x) = 0$ or $deg\ h(x) = 0$.

Let $deg\ g(x) = 0$. Then $g(x)$ is a constant polynomial *i.e.*, $g(x) = \alpha$, for some $\alpha \neq 0 \in R$. Consequently, $f(x) = \alpha\,h(x)$. Since $f(x)$ is primitive in $R[x]$, $c(f)$ is a unit in $R \Rightarrow c(\alpha\,h)$ is a unit in $R \Rightarrow c(\alpha)\,c(h)$ is a unit in $R \Rightarrow \alpha\,\beta$ is a unit in R, where $\beta = c(h) \in R$. Let $\alpha\,\beta = u$, where u is a unit in $R \Rightarrow \alpha \mid u$ and $u \mid 1 \Rightarrow \alpha \mid 1 \Rightarrow \alpha$ is a unit in $R \Rightarrow \alpha$ is a unit in $R[x]$ $\Rightarrow g(x)$ is a unit in $R[x] \Rightarrow f(x)$ is an irreducible element of $R[x]$.

Hence $f(x)$ is an irreducible polynomial in $R[x]$.

[See Theorem 3.4.4.]

Theorem 3.5.4. *If R is a U.F.D. and if $p(x)$ is a primitive polynomial in $R[x]$, then $p(x)$ can be factored in a unique way as the product of irreducible elements (polynomials) in $R[x]$.* [D.U., 1995]

Proof. Let F be a quotient field of R. We can consider $R[x]$ to be a subring of $F[x]$ and so $p(x) \in F[x]$. Since F is a field, $F[x]$ is a Euclidean domain $\Rightarrow F[x]$ is a U.F.D. Consequently, $p(x) \in F[x]$ can be written as

$$p(x) = p_1(x)\,p_2(x) \ldots p_n(x), \qquad \ldots(1)$$

where each $p_i(x) \in F[x]$ is an irreducible polynomial over F. By Lemma 3.5.1., for each i, $1 \leq i \leq n$, we can write

$$p_i(x) = \frac{f_i(x)}{a_i}\ ;\ a_i \in R, f_i(x) \in R[x]. \qquad \ldots(2)$$

By Lemma 3.4.1, we can write

$$f_i(x) = b_i\,q_i(x)\ ; \qquad \ldots(3)$$

where $b_i = c(f_i)$ and $q_i(x) \in R[x]$ is primitive in $R[x]$.

From (1), (2) and (3), we obtain

$$p(x) = \frac{1}{a_1\,a_2 \ldots a_n} f_1(x)\,f_2(x) \ldots f_n(x)$$

$$= \frac{b_1\,b_2 \ldots b_n}{a_1\,a_2 \ldots a_n}\,q_1(x)\,q_2(x) \ldots q_n(x).$$

$\therefore$ $a_1\,a_2 \ldots a_n\,p(x) = b_1\,b_2 \ldots b_n\,q_1(x)\,q_2(x) \ldots q_n(x)$. ...(4)

Since $p(x)$ is primitive in $R[x]$,

$$c(\text{L.H.S. of (4)}) = a_1\,a_2 \ldots a_n.$$

By Gauss's Lemma, $q_1(x)\,q_2(x) \ldots q_n(x)$ is primitive in $R[x]$ and so

$$c(\text{R.H.S. of (4)}) = b_1\,b_2 \ldots b_n.$$

It follows that $a_1 a_2 \ldots a_n = b_1\,b_2 \ldots b_n$.

Hence, by (4), $p(x) = q_1(x)\,q_2(x) \ldots q_n(x)$. ...(5)

We now show that each $q_i(x)$ in (5) is irreducible in $R[x]$. Since $p(x)$ is primitive in $R[x]$, so by (1), each $p_i(x)$ is necessarily primitive in $R[x]$. Further each $p_i(x) \in F[x]$ is an irreducible polynomial in $F[x]$. By Lemma 3.5.3, each $p_i(x)$ is an irreducible polynomial in $R[x] \Rightarrow$ each $f_i(x)$ is irreducible in $R[x]$, by (2).

Thus each $q_i(x)$ is irreducible in $R[x]$.

Lastly, we prove the uniqueness of (5).

Let $$p(x) = t_1(x)\, t_2(x) \ldots t_m(x), \qquad \ldots(6)$$

where each $t_i(x)$ is irreducible in $R[x]$.

Since $p(x)$ is primitive in $R[x]$, each $t_i(x)$ is necessarily primitive in $R[x]$. By Lemma 3.5.2, each $t_i(x)$ is irreducible in $F[x]$. Similarly, in (5), each $q_i(x)$ is irreducible in $F[x]$. Since $F[x]$ is a U.F.D., $m = n$ and $q_i(x)$, $t_i(x)$ are associates in $F[x]$ for each i.

$$\therefore \qquad q_i(x) = u_i\, t_i(x), \qquad \ldots(7)$$

where u_i is a unit in $F[x]$ *i.e.*, u_i is a unit in F. Let $u_i = \dfrac{a_i}{b_i}$, $a_i, b_i \neq 0 \in R$.

$$\therefore \qquad b_i\, q_i(x) = a_i\, t_i(x). \qquad \ldots(8)$$

Since $q_i(x)$ and $t_i(x)$ are primitive in $R[x]$, therefore

$$c\,(\text{L.H.S. of (8)}) = b_i, \quad c\,(\text{R.H.S. of (8)}) = a_i\,.$$

Since the content of a polynomial is unique upto associates, so a_i and b_i are associates in R *i.e.*, $b_i = u\, a_i$, for some unit $u \in R$

$$\Rightarrow \frac{a_i}{b_i} = u^{-1} \quad \Rightarrow \quad u_i = u^{-1},\ u^{-1} \text{ is a unit in } R.$$

Putting in (7), $q_i(x) = u^{-1}\, t_i(x)$, u^{-1} is a unit in R and hence in $R[x]$.

This shows that $q_i(x)$ and $t_i(x)$ are associates in $R[x]$ for each i and $m = n$. Hence $p(x)$ has a unique factorization as a product of irreducible polynomials in $R[x]$.

Theorem 3.5.5. *If R is a U.F.D., then $R[x]$ is a U.F.D.*

Proof. Let $f(x)$ be any non-zero, non-unit element of $R[x]$. By Lemma 3.4.1, we have

$$f(x) = a\, f_1(x), \qquad \ldots(1)$$

where $a = c(f)$ and $f_1(x)$ is primitive in $R[x]$. By Theorem 3.5.4, we can write

$$f_1(x) = q_1(x)\, q_2(x) \ldots q_n(x), \qquad \ldots(2)$$

where each $q_i(x)$ is irreducible in $R[x]$ and further this representation is unique upto associates.

Since $a \in R$ and R is a U.F.D, we can write a in a unique way as a finite product of irreducible elements of R, say

$$a = d_1\, d_2 \ldots d_m. \qquad \ldots(3)$$

Since R is a U.F.D., any irreducible element of R is an irreducible element of $R[x]$. So each d_i is an irreducible element of $R[x]$.

From (1), (2), (3) ; we see that

$$f(x) = d_1 d_2 \ldots d_m q_1(x) q_2(x) \ldots q_n(x),$$

which is a unique representation of $f(x)$ as a product of irreducible elements in $R[x]$.

Hence $R[x]$ is a U.F.D.

Remark 1. *It is interesting to note that* $\mathbf{Z}[x]$ *is a U.F.D. since* $\mathbf{Z}$ *is a U.F.D. Similarly,* $F[x]$ *is a U.F.D., if* F *is a field.*

Corollary 1. *If* R *is a U.F.D., then* $R[x, y]$ *is a U.F.D.*

Proof. Since R is a U.F.D., $R_1 = R[x]$ is a U.F.D.

Now R_1 is a U.F.D. $\Rightarrow$ $R_1[y]$ is a U.F.D.

$\Rightarrow$ $R[x, y]$ is a U.F.D.

Corollary 2. *If* F *is a field, then* $F[x, y]$ *is a U.F.D.*

Proof. Since F is a field, F is a Euclidean domain $\Rightarrow$ F is a U.F.D. $\Rightarrow F[x, y]$ is a U.F.D., by Cor. 1.

Remark 2. The above results can be generalized as follow :

(*a*) If R is a U.F.D., then $R[x_1, x_2, .., x_n]$ is a U.F.D.

(*b*) If F is a field, then $F[x_1, x_2, \ldots, x_n]$ is a U.F.D.

(*c*) $\mathbf{Z}[x_1, x_2, \ldots, x_n]$ is a U.F.D., $\mathbf{Z}$ being the ring of integers.

Ex.1. *Prove that every P.I.D. is U.F.D. Show by an example that the converse is not true.*

[**Hint.** $\mathbf{Z}[x]$ is a U.F.D. (See Remark 1 above), but $\mathbf{Z}[x]$ is not a P.I.D. (See Cor. 1 of Theorem 3.2.8.)]

Ex.2. *Show that* $F[x, y]$ *is a U.F.D., which is not a P.I.D. ;* F *being any field.*

[**Hint.** See Cor. 2 above and Example 3.2.21.]

Ex.3. *Show that* $\mathbf{Z}_5[x]$ *is a U.F.D. Is* $x^2 + 2x + 3$ *reducible over* $\mathbf{Z}_5[x]$?

Solution. Since 5 is prime, $\mathbf{Z}_5 = \{0, 1, 2, 3, 4\}$ is a field $\Rightarrow$ $\mathbf{Z}_5$ is a U.F.D. $\Rightarrow$ $\mathbf{Z}_5[x]$ is a U.F.D.

Since $f(x) = x^2 + 2x + 3$ is not satisfied by the elements of $\mathbf{Z}_5$ *i.e.*, $f(\alpha) \neq 0 \ \forall \ \alpha \in \mathbf{Z}_5$, $f(x)$ has no linear factors in $\mathbf{Z}_5[x]$.

Hence $x^2 + 2x + 3$ is irreducible over $\mathbf{Z}_5[x]$.

Ex.4. *Show that* $\mathbf{Z}_{11}[x]$ *is a U.F.D. Is* $x^3 + 2$ *reducible over* $\mathbf{Z}_{11}[x]$?

[**Ans.** Yes]

4

Extension Fields

4.1 Extension Fields

Definition 1. *If K is a field and F a subfield of K, then K is called an* **extension** *of F.*

Remark. Since $F \subseteq K$, we observe that

I. $(K, +)$ is an abelian group.

II. For any $\alpha \in F$ and $a \in K$, $\alpha a \in K$ such that for all $\alpha, \beta \in F$ and $a, b \in K$; the following properties hold :

1. $\alpha (a + b) = \alpha a + \alpha b$
2. $(\alpha + \beta) a = \alpha a + \beta a$
3. $\alpha (\beta a) = (\alpha \beta) a$
4. $1a = a$, where $1 \in F$.

It follows that K is a vector space over F.

As a vector space, we may discuss linear independence of elements, dimension, basis etc. in K relative to F.

Definition 2. *If K is an extension of F, then the* **degree** *of K over F is defined as the dimension of K as a vector space over F. It is denoted by $[K : F]$. Thus $[K : F] = dim_F K$.*

Definition 3. *If $[K : F]$ is finite i.e., if K is a finite-dimensional vector space over F, we say that K is a* **finite extension** *of F.*

Let V be a vector space over a field F.

1. A set $\{v_1, v_2, \ldots, v_n\}$ of elements of V is called *linearly independent* over F, if $\alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_n v_n = 0 \Rightarrow \alpha_i = 0$, for each i $(\alpha_i \in F)$.

   A set of vectors in V is called *linearly dependent* over F, if it is not linearly independent over F.
2. A subset S of a vector space V over a field F is called a *basis* of V over F, if (i) S consists of linearly independent elements and (ii) $V = L(S)$, linear span of S. It means each $v \in V$ can be written as $v = \alpha_1 s_1 + \alpha_2 s_2 + \ldots + \alpha_m s_m$, where $\alpha_i \in F$ and $s_i \in S$, $1 \leq i \leq m$.
3. The *dimension* of V over F is the number of elements in any basis of V over F.

Illustrations

1. Let $\mathbf{R}$ and $\mathbf{C}$ be the fields of real and complex numbers, respectively. Then $\mathbf{C}$ is an extension of $\mathbf{R}$ and $[\mathbf{C} : \mathbf{R}] = 2$, since $\{1, i\}$ is a basis of $\mathbf{C}$ over $\mathbf{R}$.

...Every field F is an extension of F and $[F : F] = 1$, since $\{1\}$ is a basis of F over F.

...Let $K = \{a + b\sqrt{2} : a, b \in \mathbf{Q}$ (all rationals)$\}$. Then K is an extension field of $\mathbf{Q}$ and $[K : \mathbf{Q}] = 2$, since $\{1, \sqrt{2}\}$ is a basis of K over $\mathbf{Q}$.

Ex. 1. *If* $[K : F] = 1$, *prove that* $K = F$.

Solution. Since K is an extension of F, $F \subseteq K$.

Since $[K : F] = 1$, let $\{e\}$ be a basis of K over F.

$\therefore \quad 1 \in K \Rightarrow 1 = \alpha e$, for some $\alpha \neq 0 \in F$

$\Rightarrow \quad e = \alpha^{-1} . 1 = \alpha^{-1} \Rightarrow e \in F.$

For any $a \in K$, we have $a = \beta e$, for some $\beta \in F$

Since $\beta \in F$ and $e \in F$, $\beta e \in F \Rightarrow a \in F$.

$\therefore \quad K \subseteq F$. Hence $K = F$.

Ex. 2. *If* K *is an extension of* F, *prove that* $K = F$ *if and only if* $[K : F] = 1$.

Hint. See Ex. 1. By Illustration 2, $K = F \Rightarrow [K : F] = [F : F] = 1$.

Theorem 4.1.1. *Let* K *be a finite extension of* F *and* L *a finite extension of* K. *Then* L *is a finite extension of* F *and*

$$[L : F] = [L : K]\,[K : F].$$ [D.U., 1995]

Proof. Let $[L : K] = m$ and $[K : F] = n$

$\Rightarrow \quad dim_K L = m$ and $dim_F K = n.$

Let $\mathcal{B}_1 = \{a_1, a_2, \ldots, a_m\}$ be a basis of L over K

and $\mathcal{B}_2 = \{b_1, b_2, \ldots, b_n\}$ be a basis of K over F.

We shall prove that $\mathcal{B} = \{a_i b_j : 1 \le i \le m, 1 \le j \le n\}$ is a basis of L over F.

Since $K \subseteq L$, $b_j \in L$. Also $a_i \in L \Rightarrow a_i b_j \in L$, for each i and j.

First of all we show that $\mathcal{B}$ is a linearly independent subset of L over F.

Let $\sum_{i=1}^{m} \sum_{j=1}^{n} \alpha_{ij} a_i b_j = 0$, where $\alpha_{ij} \in F$ ...(1)

$$\Rightarrow \quad \sum_{i=1}^{m} \left(\sum_{j=1}^{n} \alpha_{ij} b_j \right) a_i = 0,$$

where $\sum_{j=1}^{n} \alpha_{ij} b_j \in K$ and $\alpha_{ij} \in F$. (In L, $a_i b_j = b_j a_i$)

Since $\mathcal{B}_1$ is linearly independent over K, so by (1),

$$\sum_{j=1}^{n} \alpha_{ij} b_j = 0 \quad \text{for each} \quad i,\ 1 \le i \le m. \qquad \ldots(2)$$

Since $\mathcal{B}_2$ is linearly independent over F, so by (2),

$\alpha_{ij} = 0$ for each j, $1 \le j \le n$ and for each i, $1 \le i \le m$.

This shows that $\mathcal{B}$ is a linearly independent subset of L over F. Finally we show that $\mathcal{B}$ spans L over F. Let $a \in L$ be arbitrary. Since $\mathcal{B}_1$ is a basis of L over K, we have

$$a = \alpha_1 a_1 + \alpha_2 a_2 + \ldots + \alpha_m a_m, \quad \text{where} \quad \alpha_i \in K$$

or
$$a = \sum_{i=1}^{m} \alpha_i a_i . \qquad \ldots(3)$$

Since $\mathcal{B}_2$ is a basis of K over F, so $\alpha_i \in K$ can be written as

$$\alpha_i = \beta_{i1} b_1 + \beta_{i2} b_2 + \ldots + \beta_{in} b_n , \beta_{ij} \in F$$

or
$$\alpha_i = \sum_{j=1}^{n} \beta_{ij} b_j . \qquad \ldots(4)$$

From (3) and (4), $$a = \sum_{i=1}^{m} \left(\sum_{j=1}^{n} \beta_{ij} b_j \right) a_i .$$

$$\therefore \qquad a = \sum_{i=1}^{m} \sum_{j=1}^{n} \beta_{ij} a_i b_j, \quad \beta_{ij} \in F.$$

This shows that $\mathcal{B}$ spans L over F and so $\mathcal{B}$ is a basis of L over F and

$$dim_F L = mn.$$

Consequently, L is a finite extension of F and

$$[L : F] = dim_F L = mn = [L : K]\,[K : F].$$

Hence $[L : F] = [L : K]\,[K : F]$.

Corollary 1. *Let L be a finite extension of F and K a subfield of L which contains F. Then $[K : F]$ divides $[L : F]$.* [D.U., 2000]

Proof. We are given $F \subseteq K \subseteq L$. Let $[L : F] = n$ (finite).

Let $\mathcal{B} = \{a_1, a_2, \ldots, a_n\}$ be a basis of L over F.

Let $a \in L$ be arbitrary. Then

$$a = \alpha_1 a_1 + \alpha_2 a_2 + \ldots + \alpha_n a_n, \alpha_i \in F. \qquad \ldots(1)$$

Since $F \subseteq K$, $\alpha_i \in K$. Using in (1), we see that $\mathcal{B}$ spans L over K. Consequently, L is a finite dimensional vector space over K *i.e.*, $[L : K]$ is finite. Since subspace of a finite dimensional vector space is finite dimensional, so $[L : F]$ is finite implies $[K : F]$ is finite. Thus each one of $[L : K]$, $[L : F]$ and $[K : F]$ is finite and so by Theorem 4.1.1, we have

$$[L : F] = [L : K]\,[K : F].$$

Hence $[K : F]$ divides $[L : F]$

Corollary 2. *If K is an extension of F and $[K : F]$ is a prime number p, there is no field L such that $F \subset L \subset K$.*

Proof. Suppose there exists a field L such that $F \subset L \subset K$. Then

$$p = [K : F] = [K : L]\,[L : F], \text{ by Theorem 4.1.1.}$$

Thus implies either $[K : L] = 1$ or $[L : F] = 1$

$\Rightarrow$ $K = L$ or $L = F$, a contradiction.

Hence the result.

4.2 Field Adjunctions

Let K be an extension of F and $a \in K$. Let $\mathcal{A}$ be the collection of all subfields of K which contain both F and a. Then $\mathcal{A}$ is non-empty, since $K \in \mathcal{A}$. We know that the intersection of any number of subfields of K is a subfield of K. Let $F(a)$ denote the intersection of all those subfields of K which are members of $\mathcal{A}$. Then $F(a)$ is a subfield of K and $F(a)$ contains both F and a, since each member of $\mathcal{A}$ contains both F and a. Thus $F(a) \in \mathcal{A}$. By definition of intersection, every subfield of K in $\mathcal{A}$ contains $F(a)$. *Hence $F(a)$ is the smallest subfield of K containing both F and a. We call $F(a)$ the subfield obtained by adjoining a to F.*

Definition. *Let K be an extension of a field F and $a \in K$. Then $F(a)$ means the smallest field containing F and a.*

An extension K of F is called a **simple extension** *of F, if $K = F(a)$, for some $a \in K$.*

Let K be an extension of F and $a, b \in K$. Let $T = F(a)$. Then T is a subfield of K and so K is an extension of T. As argued earlier, $T(b)$ is the smallest subfield of K containing $T = F(a)$ and b. We write

$$T(b) = (F(a))(b) \text{ as } F(a, b).$$

Hence $F(a, b)$ *is the smallest subfield containing F, a and b.* We call $F(a, b)$ the subfield obtained by adjoining both a and b to F.

Similarly, if $a_1, a_2, \ldots, a_n \in K$, then $F(a_1, a_2, \ldots, a_n)$ is the smallest subfield of K containing F and the elements $a_1, a_2, \ldots, a_n$.

EXAMPLES

Example 4.2.1. *Show that* $[\mathbf{Q}(\sqrt{2}) : \mathbf{Q}] = 2$.

Solution. We know $\mathbf{Q}(\sqrt{2})$ is the smallest field containing $\mathbf{Q}$ and $\sqrt{2}$ and so $\mathbf{Q}(\sqrt{2})$ is an extension of $\mathbf{Q}$. Further $\{1, \sqrt{2}\}$ is a basis of $\mathbf{Q}(\sqrt{2})$ over $\mathbf{Q}$. Hence $[\mathbf{Q}(\sqrt{2}) : \mathbf{Q}] = 2$.

Example 4.2.2. *Find a basis of* $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ *over* $\mathbf{Q}$. *Hence find* $[\mathbf{Q}(\sqrt{2}, \sqrt{3}) : \mathbf{Q}]$.

Solution. $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ is the smallest field containing $\mathbf{Q}$, $\sqrt{2}$ and $\sqrt{3}$.

Any element of $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ is of the form

$$a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\sqrt{3}, \text{ where } a, b, c, d \in \mathbf{Q}.$$

It follows that $\{1, \sqrt{2}, \sqrt{3}, \sqrt{2}\sqrt{3}\}$ is a basis of $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbf{Q}$.

Hence $[\mathbf{Q}(\sqrt{2}, \sqrt{3}) : \mathbf{Q}] = 4$.

Example 4.2.3. *What is a basis of* $\mathbf{Q}(\sqrt{3}, \sqrt{5})$ *over* $\mathbf{Q}$? [D.U., 1995]

[Ans. $\{1, \sqrt{3}, \sqrt{5}, \sqrt{15}\}$**]**

Please try yourself.

Example 4.2.4. *Prove that* $\mathbf{Q}(\sqrt{2}, \sqrt{3}) = \mathbf{Q}(\sqrt{2} + \sqrt{3})$. [D.U., 2000]

Solution. $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ is the smallest field containing $\mathbf{Q}$, $\sqrt{2}$ and $\sqrt{3}$.

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

$\Rightarrow$ $Q(\sqrt{2}+\sqrt{3}) \subseteq Q(\sqrt{2}, \sqrt{3})$. ...(1)

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

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

Since $5, 2 \in Q \subseteq Q(\sqrt{2}+\sqrt{3})$, so

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

$\Rightarrow$ $\frac{1}{2}(2\sqrt{2}\sqrt{3}) = \sqrt{2}\sqrt{3} \in Q(\sqrt{2}+\sqrt{3})$.

Since $\sqrt{2}+\sqrt{3}$ and $\sqrt{2}\sqrt{3}$ both belong to $Q(\sqrt{2}+\sqrt{3})$,

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

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

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

From (2) and (3), we see that

$3\sqrt{2}+3\sqrt{3}-2\sqrt{3}-3\sqrt{2} = \sqrt{3} \in Q(\sqrt{2}+\sqrt{3})$.

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

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

We know $Q(\sqrt{2}, \sqrt{3}) = \{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{2}\sqrt{3} : a, b, c, d \in Q\}$.

$\therefore$ $Q(\sqrt{2}, \sqrt{3}) \subseteq Q(\sqrt{2}+\sqrt{3})$. ...(4)

From (1) and (4), $Q(\sqrt{2}, \sqrt{3}) = Q(\sqrt{2}+\sqrt{3})$.

Example 4.2.5. *Prove that* $Q(\sqrt{3}, \sqrt{5}) = Q(\sqrt{3}+\sqrt{5})$.

Please try yourself.

4.3 Algebraic Elements and Algebraic Extensions

Definition (Algebraic Element)

Let K be an extension of a field F. An element $a \in K$ is said to be **algebraic** *over F, if there exists a non-zero polynomial $f(x) \in F[x]$ such that $f(a) = 0$. Otherwise, a is called a* **transcendental element.**

Illustrations

1. $\sqrt{2} \in Q(\sqrt{2})$ is algebraic over Q, since $\sqrt{2}$ satisfies the polynomial $f(x) = x^2 - 2 \in Q[x]$.
2. $\sqrt{2}+\sqrt{3}$ *is algebraic over* Q.

   Let $a = \sqrt{2}+\sqrt{3}$. Then $a^2 = 5+2\sqrt{6}$ and

   $a^4 = 49+20\sqrt{6} = 10(5+2\sqrt{6}) - 1 = 10a^2 - 1$

   i.e., $a^4 - 10a^2 + 1 = 0$. Thus $a = \sqrt{2}+\sqrt{3}$ satisfies the polynomial $x^4 - 10x^2 + 1 \in Q[x]$ and so $\sqrt{2}+\sqrt{3}$ is algebraic over Q.
3. π and $e \in R$ are not algebraic over Q.

Definition (Algebraic Extension)

An extension K of a field F is called an **algebraic extension,** *if every element of K is algebraic over F.*

Illustrations

1. $Q(\sqrt{2})$ is an algebraic extension of **Q**, since $[Q(\sqrt{2}) : Q] = 2$ (finite) and every finite extension is algebraic. [Theorem 4.3.1]
2. The field **C** of complex numbers is an algebraic extension of the field **R** of real numbers.
3. $Q(\sqrt{2}, \sqrt{3})$ is an algebraic extension of **Q**.
4. **R** is not an algebraic extension of **Q**, since $\pi, e \in \mathbf{R}$ are not algebraic over **Q**.

Theorem 4.3.1. *Every finite extension of a field F is an algebraic extension. However, the converse is not true.* [D.U., 1994]

Proof. Let K be a finite extension of F. Let $[K : F] = n$ *i.e.*, $dim_F K = n$. Let $a \in K$ be arbitrary. Since $dim_F K = n$, so $(n+1)$ elements of K viz. $1, a, a^2, \ldots, a^n$ are linearly dependent over F. Consequently, there exist $\alpha_0, \alpha_1, \ldots, \alpha_n \in F$, not all zero, such that

$$\alpha_0 . 1 + \alpha_1 a + \alpha_2 a^2 + \ldots + \alpha_n a^n = 0. \qquad \ldots(1)$$

Let $f(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \ldots + \alpha_n x^n \in F[x]$.

Then $f(x)$ is a non-zero polynomial in $F[x]$ such that $f(a) = 0$, by (1).

This shows that a is algebraic over F, where $a \in K$ is arbitrary. Hence K is an algebraic extension of F.

However, the converse is not true i.e., an algebraic extension of F may not be a finite extension of F.

For the counter-example, see Example 4.3.8. ahead.

Definition. *A non-zero polynomial $f(x) \in F[x]$ is said to be a* **monic polynomial** *over F, if the coefficient of the highest power of x in $f(x)$ is equal to* 1.

Theorem 4.3.2. *Let K be an extension of F and let $a \in K$ be algebraic over F. Then*

(*i*) *There exists a unique monic irreducible polynomial $p(x) \in F[x]$ of least positive degree such that $p(a) = 0$.*

(*ii*) *If $g(x) \in F[x]$ is such that $g(a) = 0$, then $p(x)$ divides $g(x)$.* [D.U., 1997]

Proof. (*i*) Since $a \in K$ is algebraic over F, a satisfies some non-zero polynomial over F. Let $f(x)$ be a non-zero polynomial (over F) of *least positive degree*, n, such that $f(a) = 0$. ...(1)

We take $f(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \ldots + \alpha_n x^n \in F[x], \alpha_n \neq 0 \in F$.

Let $p(x) = x^n + \alpha_n^{-1} \alpha_{n-1} x^{n-1} + \ldots + \alpha_n^{-1} \alpha_1 x + \alpha_n^{-1} \alpha_0 = \alpha_n^{-1} f(x)$.

Then $p(a) = \alpha_n^{-1} f(a) = \alpha_n^{-1} . 0 = 0$, where $deg\ p(x) = n = deg\ f(x)$.

Thus we see that $p(x)$ is a monic polynomial in $F[x]$ of least positive degree such that $p(a) = 0$. Now we show that $p(x)$ is irreducible over F. Let, if possible, $p(x)$ be not irreducible over F. Then we can write

Since $a \in K$ is algebraic over F, by Theorem 4.3.2, there exists a unique monic irreducible polynomial $p(x) \in F[x]$ of least positive degree such that $p(a) = 0$. Further $g(a) = 0 \Rightarrow g(x)$ divides $p(x) \Rightarrow g(x) = p(x) h(x)$, for some $h(x) \in F[x]$. Since this is true for all $g(x) \neq 0 \in M$, $M = (p(x))$. Since $p(x)$ is irreducible over F, M is a maximal ideal of $F[x]$. Consequently,

$$\frac{F[x]}{M} \text{ is a field and so } F[a] \text{ is a field, by (2).}$$

Since $F(a)$ is the smallest field containing F and a,

$$F(a) \subseteq F[a]. \qquad \ldots(3)$$

From (1) and (3), $F[a] = F(a)$.

Theorem 4.3.4. *Let K be an extension of a field F. An element $a \in K$ is algebraic over F if and only if $[F(a) : F]$ is finite.*

[D.U., 1999, 96]

Proof. *Sufficient condition*

Let $[F(a) : F] = n$ (finite). Then $dim_F F(a) = n$.

Since $F(a)$ is the smallest field containing F and a ; so $(n + 1)$ elements of $F(a)$ *viz.* $1, a, a^2, \ldots, a^n$ must be linearly dependent over F.

There exist elements $\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_n$ in F, not all zero, such that

$$\alpha_0 \cdot 1 + \alpha_1 a + \alpha_2 a^2 + \ldots + \alpha_n a^n = 0. \qquad \ldots(1)$$

Let $f(x) = \alpha_0 + \alpha_1 x + \ldots + \alpha_n x^n \in F[x]$.

Then $f(x)$ is a non-zero polynomial in $F[x]$ such that $f(a) = 0$, by (1). Hence a is algebraic over F.

Necessary condition

Let $a \in K$ be algebraic over F. By Theorem 4.3.2, there exists a unique monic irreducible polynomial $p(x) \in F[x]$ of lowest positive degree such that $p(a) = 0$. Let $deg\, p(x) = n$. Since $a \in K$ is algebraic over F, $F(a) = F[a] = \{f(a) : f(x) \in F[x]\}$. [Theorem 4.3.3]

Let $0 \neq f(a) \in F[a]$. Then $f(x) \in F[x]$

Since $f(x)$, $p(x) \in F[x]$, by Division algorithm, there exist $t(x)$, $r(x) \in F[x]$ such that

$$f(x) = p(x)\, t(x) + r(x), \qquad \ldots(2)$$

where $r(x) = 0$ or $deg\, r(x) < deg\, p(x) < n$.

If $r(x) = 0$, then $f(x) = p(x)\, t(x) \Rightarrow f(a) = p(a)\, t(a) = 0$ $(\because p(a) = 0)$. But $f(a) = 0$ is contrary to the given assumption. Thus $r(x) \neq 0$ and so we may take $r(x) = \alpha_0 + \alpha_1 x + \ldots + \alpha_{n-1} x^{n-1} \in F[x]$.

From (2), $f(a) = r(a)$

$(\because p(a) = 0)$

i.e., $f(a) = \alpha_0 \cdot 1 + \alpha_1 \cdot a + \ldots + \alpha_{n-1} \cdot a^{n-1}$ $\forall f(a) \neq 0 \in F[a]$.

This shows that the set $S = \{1, a, a^2, \ldots, a^{n-1}\}$ spans $F[a]$ over F. Further S is a linearly independent set, for otherwise, there exist $\beta_0, \beta_1, \ldots, \beta_{n-1} \in F$, not all zero, such that

$$\beta_0 \cdot 1 + \beta_1 a + \ldots + \beta_{n-1} a^{n-1} = 0$$

i.e., a satisfies the non-zero polynomial $\beta_0 + \beta_1 x + \ldots + \beta_{n-1} x^{n-1} \in F[x]$ of degree $< n$ = degree of the minimal polynomial $p(x)$, which is a contradiction. Hence $S = \{1, a, a^2, \ldots, a^{n-1}\}$ is a basis of $F[a] = F(a)$ over F i.e.,

$$[F(a) : F] = n \text{ (finite)}.$$

Remark. *If $a \in K$ is algebraic over F, then $[F(a) : F]$ = degree of the unique monic irreducible polynomial over F satisfied by a.*

This result will be treated as a formula in several examples on splitting fields of polynomials.

Ex. 1. *Let K be an extension of a field F and $a \in K$ be algebraic of degree n over F. Then $[F(a) : F] = n$.*

Hint. See the necessary condition of Theorem 4.3.4.

Ex. 2. *Show that* $[\mathbf{Q}(\sqrt{2}) : \mathbf{Q}] = 2$.

Solution. $\sqrt{2}$ satisfies the irreducible monic polynomial $x^2 - 2 \in \mathbf{Q}[x]$, which is of degree 2. Thus $\sqrt{2}$ is algebraic of degree 2 over $\mathbf{Q}$ and so $[\mathbf{Q}(\sqrt{2}) : \mathbf{Q}] = 2$.

Ex. 3. *Show that* $[\mathbf{Q}(\sqrt[3]{2}) : \mathbf{Q}] = 3$.

Theorem 4.3.5. *Let K be an extension of a field F. If $a, b \in K$ are algebraic over F, then $a \pm b$, ab, ab^{-1} $(b \neq 0)$ are algebraic over F. In other words, the elements of K which are algebraic over F form a subfield of K.*

Proof. Since $a \in K$ is algebraic over F, $[F(a) : F]$ is finite.

[Theorem 4.3.4]

Since $b \in K$ is algebraic over F, $f(b) = 0$ for some non-zero polynomial $f(x)$ over $F \subseteq F(a)$. Consequently, b is algebraic over $F(a)$ and so

$[(F(a))(b) : F(a)]$ is finite. [Theorem 4.3.4]

$\therefore$ $[F(a,b) : F(a)]$ is finite.

Hence $[F(a, b) : F] = [F(a, b) : F(a)]\,[F(a) : F]$ is finite.

Notice that $F \subset F(a) \subset F(a, b)$.

We have proved that $F(a, b)$ is a finite extension of F and so $F(a, b)$ is an algebraic extension of F, since every finite extension is algebraic [Theorem 4.3.1]. It follows that every element of $F(a, b)$ is algebraic over F. Since $F(a, b)$ is the smallest field containing F, a and b, so $a \pm b$, ab, ab^{-1} $(b \neq 0)$ all belong to $F(a, b)$. Hence $a \pm b$, ab, ab^{-1} $(b \neq 0)$ are algebraic over F. In other words, the elements of K which are algebraic over F form a subfield of K.

Theorem 4.3.6. *Let K be an extension of a field F. If $a_1, a_2, \ldots, a_n \in K$ are algebraic over F, then $F(a_1, a_2, \ldots, a_n)$ is a finite extension of F and so is algebraic over F.*

Proof. We shall prove the result by induction on n. If $n = 1$, $\alpha_1 \in K$ is algebraic over F implies that $[F(\alpha_1) : F]$ is finite, by (1), 4.3.4. Thus the result is true for $n = 1$. Suppose that the result is true for positive integers less than n. Since α_n is algebraic over F, so α_n is a some non-zero polynomial over $F \subset F(\alpha_1, \alpha_2, \ldots, \alpha_{n-1}) = F_{n-1}$, say

$\Rightarrow [F_{n-1}(\alpha_n) : F_{n-1}]$ is finite (Theorem 4.3.4)

$\Rightarrow [(F(\alpha_1, \alpha_2, \ldots, \alpha_{n-1}))(\alpha_n) : F(\alpha_1, \alpha_2, \ldots, \alpha_{n-1})]$ is finite

$\Rightarrow [F(\alpha_1, \alpha_2, \ldots, \alpha_{n-1}, \alpha_n) : F(\alpha_1, \alpha_2, \ldots, \alpha_{n-1})]$ is finite.

By induction hypothesis,

$$[F(\alpha_1, \alpha_2, \ldots, \alpha_{n-1}) : F] \text{ is finite.}$$

We have $[F(\alpha_1, \alpha_2, \ldots, \alpha_n) : F]$

$= [F(\alpha_1, \alpha_2, \ldots, \alpha_n) : F(\alpha_1, \alpha_2, \ldots, \alpha_{n-1})][F(\alpha_1, \alpha_2, \ldots, \alpha_{n-1}) : F]$

= finite, by (1) and (2).

This completes the induction. Hence $F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ is a finite e sion of F and so is algebraic over F, since every finite extension is alge

Theorem 4.3.7. *If L is an algebraic extension of K and K algebraic extension of F, then L is an algebraic extension of F.*

Proof. Let $a \in L$ be arbitrary. We shall prove that a is algebraic F. Since L is an algebraic extension of K, a is algebraic over K $f(a) = 0$, for some $0 \neq f(x) \in K[x]$.

Let $$f(x) = \alpha_0 + \alpha_1 x + \ldots + \alpha_n x^n \in K[x].$$

Since $\alpha_0, \alpha_1, \ldots, \alpha_n \in K$ are algebraic over F ($\because K$ is an alge extension of F), $[F(\alpha_0, \alpha_1, \ldots, \alpha_n) : F]$ is finite *i.e.*, $[M : F]$ is finite where $M = F(\alpha_0, \alpha_1, \ldots, \alpha_n)$. [See Theorem 4.

It follows that $f(x) \in M[x]$ ($\because \alpha_i$'s $\in M$) and $f(a) = 0$. This mea is algebraic over M and so $[M(a) : M]$ is finite. [See Theorem 4.

We have $[M(a) : F] = [M(a) : M][M : F]$ = finite

$\Rightarrow M(a)$ is a finite extension of F

$\Rightarrow M(a)$ is an algebraic extension of F

$\Rightarrow a \in M(a)$ is algebraic over F.

Thus a is algebraic over F for each $a \in L$ and so it follows that L an algebraic extension of F.

EXAMPLES

Example 4.3.1. (*a*) *Show that $\sqrt{2}$ and $\sqrt{3}$ are both algebraic over $\mathbf{Q}$. Exhibit a polynomial of degree 4 over $\mathbf{Q}$ satisfied by $\sqrt{2} + \sqrt{3}$.*

(*b*) *What is the degree of $\sqrt{2} + \sqrt{3}$ over $\mathbf{Q}$?*

(*c*) *What is the degree of $\sqrt{2}\sqrt{3}$ over $\mathbf{Q}$?*

Proof. We shall prove the result by induction on n. If $n = 1$, then $a_1 \in K$ is algebraic over F implies that $[F(a_1) : F]$ is finite, by Theorem 4.3.4. Thus the result is true for $n = 1$. Suppose that the result is true for all positive integers less than n. Since a_n is algebraic over F, so a_n satisfies some non-zero polynomial over $F \subset F(a_1, a_2, \ldots, a_{n-1}) = F_1$, say

$\Rightarrow [F_1(a_n) : F_1]$ is finite (Theorem 4.3.4)

$\Rightarrow [(F(a_1, a_2, \ldots, a_{n-1}))(a_n) : F(a_1, a_2, \ldots, a_{n-1})]$ is finite

$\Rightarrow [F(a_1, a_2, \ldots, a_{n-1}, a_n) : F(a_1, a_2, \ldots, a_{n-1})]$ is finite. ...(1)

By induction hypothesis,

$[F(a_1, a_2, \ldots, a_{n-1}) : F]$ is finite. ...(2)

We have $[F(a_1, a_2, \ldots, a_n) : F]$

$= [F(a_1, a_2, \ldots, a_n) : F(a_1, a_2, \ldots, a_{n-1})]\,[F(a_1, a_2, \ldots, a_{n-1}) : F]$

= finite, by (1) and (2).

This completes the induction. Hence $F(a_1, a_2, \ldots, a_n)$ is a finite extension of F and so is algebraic over F, since every finite extension is algebraic.

Theorem 4.3.7. *If L is an algebraic extension of K and K is an algebraic extension of F, then L is an algebraic extension of F.*

[D.U., 1999]

Proof. Let $a \in L$ be arbitrary. We shall prove that a is algebraic over F. Since L is an algebraic extension of K, a is algebraic over K *i.e.*, $f(a) = 0$, for some $0 \neq f(x) \in K[x]$.

Let $f(x) = \alpha_0 + \alpha_1 x + \ldots + \alpha_n x^n \in K[x]$.

Since $\alpha_0, \alpha_1, \ldots, \alpha_n \in K$ are algebraic over F ($\because$ K is an algebraic extension of F), $[F(\alpha_0, \alpha_1, \ldots, \alpha_n) : F]$ is finite *i.e.*, $[M : F]$ is finite where $M = F(\alpha_0, \alpha_1, \ldots, \alpha_n)$. [See Theorem 4.3.6]

It follows that $f(x) \in M[x]$ ($\because$ α_i's $\in M$) and $f(a) = 0$. This means a is algebraic over M and so $[M(a) : M]$ is finite. [See Theorem 4.3.4]

We have $[M(a) : F] = [M(a) : M]\,[M : F]$ = finite

$\Rightarrow M(a)$ is a finite extension of F

$\Rightarrow M(a)$ is an algebraic extension of F

$\Rightarrow a \in M(a)$ is algebraic over F.

Thus a is algebraic over F for each $a \in L$ and so it follows that L is an algebraic extension of F.

EXAMPLES

Example 4.3.1. (*a*) *Show that $\sqrt{2}$ and $\sqrt{3}$ are both algebraic over $\mathbf{Q}$. Exhibit a polynomial of degree 4 over $\mathbf{Q}$ satisfied by $\sqrt{2} + \sqrt{3}$.*

(*b*) *What is the degree of $\sqrt{2} + \sqrt{3}$ over $\mathbf{Q}$?*

(*c*) *What is the degree of $\sqrt{2}\sqrt{3}$ over $\mathbf{Q}$?*

Solution. (*a*) $\sqrt{2}$ and $\sqrt{3}$ satisfy the polynomials x^2-2 and x^2-3, respectively, over **Q**. Hence $\sqrt{2}$ and $\sqrt{3}$ are both algebraic over **Q**.

Let $a=\sqrt{2}+\sqrt{3}$. Then $a^2=5+2\sqrt{6}$ and $a^4=49+20\sqrt{6}$ $=10(5+2\sqrt{6})-1=10a^2-1$ *i.e.*, $a^4-10a^2+1=0$. Hence $\sqrt{2}+\sqrt{3}$ satisfies the polynomial x^4-10x^2+1 of degree 4 over **Q**.

(*b*) We know $\mathbf{Q}(\sqrt{2},\sqrt{3})=\mathbf{Q}(\sqrt{2}+\sqrt{3})$. [See Example 4.2.4]

Since x^2-2 is an irreducible monic polynomial of least degree 2 over **Q** satisfied by $\sqrt{2}$, so $[\mathbf{Q}(\sqrt{2}):\mathbf{Q}]=2$.

Again x^2-3 is an irreducible monic polynomial of least degree 2 over $\mathbf{Q}\subset\mathbf{Q}(\sqrt{2})$ satisfied by $\sqrt{3}$. Consequently,

$$[(\mathbf{Q}(\sqrt{2}))(\sqrt{3}):\mathbf{Q}(\sqrt{2})]=2 \text{ or } [\mathbf{Q}(\sqrt{2},\sqrt{3}):\mathbf{Q}(\sqrt{2})]=2.$$

We have $\mathbf{Q}\subset\mathbf{Q}(\sqrt{2})\subset\mathbf{Q}(\sqrt{2},\sqrt{3})$ and

$$[\mathbf{Q}(\sqrt{2},\sqrt{3}):\mathbf{Q}]=[\mathbf{Q}(\sqrt{2},\sqrt{3}):\mathbf{Q}(\sqrt{2})]\,[\mathbf{Q}(\sqrt{2}):\mathbf{Q}]=2\times2=4.$$

$\therefore\ [\mathbf{Q}(\sqrt{2}+\sqrt{3}):\mathbf{Q}]=[\mathbf{Q}(\sqrt{2},\sqrt{3}):\mathbf{Q}]=4.$

Hence the degree of $\sqrt{2}+\sqrt{3}$ over **Q** is 4.

(*c*) Since $\sqrt{2}\,.\,\sqrt{3}=\sqrt{6}$ satisfies x^2-6 over **Q**. By Eisenstein criterion, x^2-6 is irreducible over **Q** and so x^2-6 is the minimal polynomial of $\sqrt{2}\,\sqrt{3}$ over **Q** of degree 2. Hence the degree of $\sqrt{2}\,\sqrt{3}$ over **Q** is 2.

Example 4.3.2. (*i*) *Prove that* $\sqrt{3}$ *and* $\sqrt{5}$ *are both algebraic over* **Q**.

(*ii*) *What is the degree of* $\sqrt{3}+\sqrt{5}$ *over* **Q** ?

(*iii*) *What is a basis of* $\mathbf{Q}(\sqrt{3},\sqrt{5})$ *over* **Q** ? [D.U., 1995]

Solution. (*i*) $\sqrt{3}$ and $\sqrt{5}$ are both algebraic over **Q**, since they satisfy the polynomials x^2-3 and x^2-5, respectively, over **Q**.

(*ii*) As explained in Example 4.3.1., we see that

$$[\mathbf{Q}(\sqrt{3}):\mathbf{Q}]=deg\,(x^2-3)=2,$$

and $[(\mathbf{Q}(\sqrt{3}))(\sqrt{5}),\mathbf{Q}(\sqrt{3})]=[\mathbf{Q}(\sqrt{3},\sqrt{5}):\mathbf{Q}(\sqrt{3})]=deg\,(x^2-5)=2.$

$\therefore\ [\mathbf{Q}(\sqrt{3},\sqrt{5}):\mathbf{Q}]=[\mathbf{Q}(\sqrt{3},\sqrt{5}):\mathbf{Q}(\sqrt{3})]\,[\mathbf{Q}(\sqrt{3}):\mathbf{Q}]=2\times2=4$

or $[\mathbf{Q}(\sqrt{3}+\sqrt{5}):\mathbf{Q}]=4$, since $\mathbf{Q}(\sqrt{3},\sqrt{5})=\mathbf{Q}(\sqrt{3}+\sqrt{5})$. (Verify)

Hence the degree of $\sqrt{3}+\sqrt{5}$ over **Q** is 4.

(*iii*) $\mathbf{Q}(\sqrt{3},\sqrt{5})$ is the smallest field containing **Q**, $\sqrt{3}$ and $\sqrt{5}$.

Any element of $\mathbf{Q}(\sqrt{3},\sqrt{5})$ is of the form :

$$a+b\sqrt{3}+c\sqrt{5}+d\sqrt{3}\sqrt{5}:a,b,c,d\in\mathbf{Q}.$$

Hence $\{1,\sqrt{3},\sqrt{5},\sqrt{3}\sqrt{5}\}$ is a basis of $\mathbf{Q}(\sqrt{3},\sqrt{5})$ over **Q**.

Example 4.3.3. *Show that* $\mathbf{Q}(\sqrt{2},\sqrt[3]{5})=\mathbf{Q}(\sqrt{2}+\sqrt[3]{5})$.

Solution. Since $\mathbf{Q}(\sqrt{2},\sqrt[3]{5})$ is the smallest field containing **Q**, $\sqrt{2}$ and $\sqrt[3]{5}$; $\sqrt{2}+\sqrt[3]{5}\in\mathbf{Q}(\sqrt{2},\sqrt[3]{5})$. Consequently,

$$\mathbf{Q}(\sqrt{2}+\sqrt[3]{5})\subseteq\mathbf{Q}(\sqrt{2},\sqrt[3]{5}). \qquad ...(1)$$