Unique factorization Domain (or Gaussian Domain):

Defn: Let R be an integral domain with unity then R is called a unique factorization domain (UFD) if

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

(ii) If $a = p_1 p_2 \cdots p_m$
$a = q_1 q_2 \cdots q_n$
where p_i and q_j are irreducible in R then $m=n$ and each p_i is an associate of some q_j. (i.e., each $p_i = u_i q_i$ where u_i is a unit in some order)

→ every field F is a UFD. as it contains no non-zero, non unit elements.
i.e, each non-zero element $a \in F$ is a unit.
i.e, $a a^{-1} = 1 \Rightarrow a|1$.

→ The ring of integers is a UFD

Sol: we know that it is an integral domain with unity. If $n \in \mathbb{Z}$ be any non-zero, non-unit element (i.e, $n \neq 0, \pm 1$) of $\mathbb{Z}$ then
If $n > 0$, we can write
$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$ where p_i are primes.

$\Rightarrow n = (p_1 p_1 p_1 \ldots p_1)(p_2 p_2 \ldots p_2) \ldots (p_m p_m \ldots p_m)$

i.e, n is the product of prime (thus irreducible) elements of Z. Again this Representation of n is unique.

In case $n<0$,

let $n = (-m)$ where $m>0$

then we can express m as product of primes (therefore, irreducibles) in Z.

say, $m = q_1 q_2 \ldots q_k$

then $-m = n = (-q_1)(q_2)\ldots(q_k)$

→ If $a \in R$ can be expressed as a product of irreducible elements, the expression need not be unique as the following example shows

Ex: $R = \{a + b\sqrt{-5} \mid a, b \in Z\}$.

We have seen that the only units in R are ± 1, and that $1+2\sqrt{-5}$ is an irreducible element.

Similarly we can show that 3 and 7 are irreducible elements.

Then $21 = 3 \cdot 7 = (1+2\sqrt{-5})(1-2\sqrt{-5})$.

The two factorizations of 21 as a product of irreducible elements, are distinct as $1 \pm 2\sqrt{-5}$ are not the associates of 3 or 7.

→ In a UFD R an element is prime iff it is irreducible.

Soln: Let $a \in R$ be a prime element, then since R is an integral domain with unity, a will be irreducible. (∵ in an Integral domain with unity, every prime element is irreducible)

Conversely, let $a \in R$ be irreducible.

Then a is non-zero, non-unit.

Let a/bc then $bc = ak$ for some k

Case(i): suppose b is a unit

then $c = ak b^{-1} = a(kb^{-1}) \Rightarrow a/c$.

Case(ii): suppose c is a unit then similarly, a/b

Case(iii): suppose b, c are non-units.

if k is a unit, then $bc = ak$

$\Rightarrow a = b(ck^{-1})$

Since a is irreducible, either b or ck^{-1} is a unit. But b is not a unit.

Thus ck^{-1} is a unit.

But that implies c is a unit, which is again not true. Hence k is not a unit.

we can thus express

$b = p_1 p_2 \ldots\ldots p_m$

$c = q_1 q_2 \ldots\ldots q_n$

$k = r_1 r_2 \cdots r_t$

as product of irreducibles. (by defn of UFD)

So $bc = ak$ becomes

$$p_1 p_2 \cdots p_m q_1 q_2 \cdots q_n = a r_1 r_2 \cdots r_t = x \quad (\text{say})$$

Then x is an element having two representations as product of irreducible elements.

By Defn. of UFD each element in one representation is an associate of some element in the other.

$\Rightarrow$ a is an associate of some p_i or some q_j.

$\Rightarrow$ $ua = p_i$ or $ua = q_j$ for some unit u.

$\Rightarrow$ a/p_i or a/q_j.

$\Rightarrow$ a/b or a/c. $(\because p_i/b, q_j/c)$

$\Rightarrow$ a is prime element.

→ 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 UFD.

proof: To show that R is a UFD we need prove that if $a \in R$ be a non-zero, non unit element and

$a = p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n$

where p_i and q_j are irreducible elements then $m=n$ and each p_i is an associate of some q_j.

we use induction on n.

Let $n=1$, then $a = p_1 p_2 \cdots p_m$ and as q_1 is irreducible some p_i is a unit.

But each p_i being irreducible cannot be a unit. Thus $m=1$.

$\therefore a = p_1 = q_1$, or that the result is true for $n=1$.

Let it be true for $n-1$.

Let now $a = p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n$

Then $p_1 p_2 \cdots p_m = q_1 (q_2 \cdots q_n)$

$\Rightarrow q_1 \mid p_1 p_2 \cdots p_m$

Since q_1 is irreducible, it is prime (given)

$\Rightarrow q_1 \mid p_i$ for some i.

Without loss of generality, we can take $i=1$

then $q_1 \mid p_1 \Rightarrow p_1 = q_1 u_1$

But p_1 irreducible $\Rightarrow q_1$ or u_1 is a unit.

As q_1 is not a unit (being irreducible), u_1 will be a unit and thus p_1, q_1 are associates.

Now $(q_1 u_1) p_2 p_3 \cdots p_m = q_1 q_2 \cdots q_n$

(or)

$(u_1 p_2) p_3 \cdots p_m = q_2 q_3 \cdots q_n$

$\Rightarrow p_2' p_3 \cdots p_m = q_2 q_3 \cdots q_n$

where $p_2' = u_1 p_2$ is irreducible.

R.H.S. contains $n-1$ elements and result being true for $n-1$, we find $m-1 = n-1 \Rightarrow m = n$.

Also, just as we showed that q_1 is an associate of p_1, we can show that q_2 is an associate of p_2, by considering

$p_1 p_2 \cdots p_m = q_2 (q_1 q_3 \cdots q_n)$

Thus q_i will be an associate of p_i.

Hence R is a UFD.

Second defn of UFD:

An integral domain R with unity is called a UFD, 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.

→ An integral domain R with unity is a UFD iff every non-zero, non unit element is finite product of primes.

Soln: If R is a UFD then every non-zero, non unit element is a finite product of irreducibles (by defn) and also every irreducible element is prime,

Hence the result follows.

Conversely,

Let $a \in R$ be a non-zero non-unit element.

Then $a = p_1 p_2 \dots p_n$, where p_i are prime elements ~~$\forall i$~~.

Since R is an integral domain, prime elements are irreducible. and so each p_i is irreducible.

We now show that every irreducible element of R is a prime element.

Let $x \in R$ be any irreducible element.

Then $x \neq 0$, non unit.

Thus $x = q_1 q_2 \dots q_m$ where q_j are prime.

Suppose $m > 1$. Since x is irreducible, either q_1 or $(q_2 q_3 \dots q_m)$ is a unit.

But q_1 is prime and thus cannot be a unit.

So $(q_2 q_3 \cdots q_m)$ is a unit which implies q_2 is a unit but that is not true as q_2 is a prime.

Hence $m=1$ or that x is prime.

By the second defn. of above, R is a UFD.

→ If R is an integral domain with unity then the following are equivalent.

(i) R is a UFD

(ii) every non-zero, non-unit element of R is a finite product of irreducible elements and every irreducible element is prime.

(iii) Every non-zero, non-unit element of R is a finite product of prime elements.

→ Show that every Euclidean domain is a unique factorization domain (UFD)

Sol We know that, in a ED, an elt is prime ⟺ it is irreducible. ($\because$ ED ⟹ PID)

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.

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

$$p_1 \mid q_1 q_2 \ldots q_n \implies p_1 \mid q_j, \quad \text{for some } j, 1 \le j \le n.$$

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 $$p_2 p_3 \ldots p_m = u_1 q_2 \ldots q_n. \qquad (\because p_1 \neq 0 \in R) \quad \ldots(2)$$

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 $p_2 \nmid u_1$, for otherwise, $p_2 \mid u_1$ and $u_1 \mid 1 \implies p_2 \mid 1 \implies p_2$ 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 $q_1 \mid q_1 q_2 \ldots q_n \implies q_1 \mid p_1 p_2 \ldots p_m \implies q_1 \mid p_1$ 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.

→ An element in a U.f.D. is prime iff it is irreducible.

proof: Let R be a UFD.

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 $p = p1$, $p \mid p$

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,

$$a = p_1 p_2 \cdots p_n, \; b = q_1 q_2 \cdots q_m, \qquad \ldots(1)$$

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

$$c = r_1 r_2 \ldots r_k, \qquad \ldots(2)$$

where each r_i is an irreducible element in R.

Putting (1) and (2) in $ab = cp$, we get

$$p_1 p_2 \cdots p_n q_1 q_2 \cdots q_m = p\, r_1 r_2 \ldots r_k.$$

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 $p \mid q_j \; (1 \le j \le m) \Rightarrow p \mid p_1 p_2 \cdots p_n$ or $p \mid q_1 q_2 \cdots q_m \Rightarrow p \mid a$ 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 $c^2 + 3d^2 = 1$;

(*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 $\quad 1 + \sqrt{-3} = (a + b\sqrt{-3})(c + d\sqrt{-3})$; $a, b, c, d \in J$

$\Rightarrow \quad 1 - \sqrt{-3} = (a - b\sqrt{-3})(c - d\sqrt{-3})$.

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 $\mathbf{Z}$; $48 = 2^4 \cdot 3^1 \cdot 5^0$ and $75 = 2^0 \cdot 3^1 \cdot 5^2$]

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

$$d = p_1^{\gamma_1} p_2^{\gamma_2} \dots p_n^{\gamma_n} \qquad (\gamma_i \text{ being non-negative integers})$$

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 $x = p_1^{\mu_1} p_2^{\mu_2} \dots p_n^{\mu_n} \in R$ 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 $$c_k = a_0 b_k + a_1 b_{k-1} + a_2 b_{k-2} + \ldots + a_k b_0. \quad \ldots(1)$$

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

$$r = p_1 p_2 \ldots p_l, \text{ where each } p_i \text{ is irreducible}$$

$$\Rightarrow \quad p_i \mid r \text{ and } r \mid c_k \;\forall\; k \Rightarrow p_i \mid c_k \;\forall\; k$$

Thus there exists some irreducible element $p \in R$ such that

$$p \mid c_k \;\forall\; k. \quad \ldots(2)$$

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

$$p \mid a_0, p \mid a_1, \ p \mid a_2 \ldots, p \mid a_{i-1} \text{ but } p \nmid a_i. \qquad \ldots(3)$$

Similarly, let b_j be the **first** coefficient of $g(x)$, which is not divisible by p. It means

$$p \mid b_0, p \mid b_1, p \mid b_2, \ldots, p \mid b_{j-1} \text{ but } p \nmid b_j. \qquad \ldots(4)$$

From (1), we obtain

$$c_{i+j} = (a_0 b_{i+j} + a_1 b_{i+j-1} + \ldots + a_{i-1} b_{j+1}) + a_i b_j + (a_{i+1} b_{j-1} + a_{i+2} b_{j-2} + \ldots + a_{i+j} b_0) \qquad \ldots(5)$$

From (3) and (4), we see that

$$p \mid (a_0 b_{i+j} + a_1 b_{i+j-1} + \ldots + a_{i-1} b_{j+1}), \qquad \ldots(6)$$

and
$$p \mid (a_{i+1} b_{j-1} + a_{i+2} b_{j-2} + \ldots + a_{i+j} b_0). \qquad \ldots(7)$$

From (2), $p \mid c_{i+j}$. $\qquad \ldots(8)$

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.

$$\therefore \quad f(x)\, g(x) = ab\, f_1(x)\, g_1(x). \qquad \ldots(1)$$

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

$$f(x) = g_1(x)\, h_1(x), \quad \text{where} \quad g_1(x) \in D[x],\ h_1(x) \in D[x].$$

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 $\quad deg\ g(x) > 0 \quad$ 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

$\Rightarrow f_1(x)$ is not a unit of $R[x]$ ...(1)

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* **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 **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, $k \le r < n$. 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

$$p \mid [a_k - (b_0 c_k + b_1 c_{k-1} + \ldots + b_{k-1} c_1) \text{ i.e., } p \mid b_k c_0, \text{ by (2)}$$

$\Rightarrow$ $p \mid b_k$ 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 $f(x) = 1 + x + x^2 + \ldots + x^{p-1} = \dfrac{x^p - 1}{x - 1}$.

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 $\deg g(x) > 0$ and $\deg h(x) > 0$.

$\therefore \quad f(x+1) = g(x+1)\,h(x+1)$,

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 $f(x) = x^4 + x^3 + x^2 + x + 1 = \dfrac{x^5 - 1}{x - 1}$

$$\therefore \quad f(x+1) = \frac{(1+x)^5 - 1}{x}$$

$$= \frac{1}{x}\left(1 + 5_{c_1}x + 5_{c_2}x^2 + 5_{c_3}x^3 + 5_{c_4}x^4 + x^5 - 1\right)$$

$$= 5 + 10x + 10x^2 + 5x^3 + 1 \,.\, x^4.$$

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., 1998]

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 $F = Z_7 = \{0, 1, 2, 3, 4, 5, 6\}$.

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

$$0 = a + b, \qquad ...(1)$$
$$1 = ab. \qquad ...(2)$$

(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.

2013
2009

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

$$2 = a + b, \quad \ldots(1)$$
$$3 = ab. \quad \ldots(2)$$

(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

$$f(x) = (x^2 + 2x + 3)\, t(x) + r(x), \quad \ldots(1)$$

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 $f(x) + A = r(x) + A = \alpha x + \beta + A, \quad \ldots(2)$

since $(x^2 + 2x + 3)\, t(x) \in A = \langle x^2 + 2x + 3 \rangle$.

In (2), we see that $\alpha, \beta \in F = \mathbf{Z}_5$ and $o(\mathbf{Z}_5) = 5$. 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

$$F = \mathbf{Z}_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}.$$

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 e., $f(\alpha) \neq 0$ for each $\alpha \in F$). Consequently, $x^2 + x + 4$ is not expressible a product of two linear factors in $F[x]$. Hence $x^2 + x + 4$ is irreducible F. By Theorem 3.4.6., $\dfrac{F[x]}{\langle x^2 + x + 4 \rangle}$ is a field. Any element of this field 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 $\frac{F[x]}{\langle x^4 + x + 4 \rangle}$ 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 $\frac{F[x]}{\langle f(x) \rangle}$ is a field with p^n elements.*

Solution. Since $f(x)$ is irreducible over $F = \mathbf{Z}_p$, $\frac{F[x]}{\langle f(x) \rangle}$ 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 $\frac{F[x]}{\langle f(x) \rangle}$ 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

$$f(x)+\langle x^3+3x+1\rangle, \quad \text{where} \quad f(x)\in \mathbf{Q}[x].$$

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

$$f(x)=t(x)(x^3+3x+1)+r(x), \qquad \ldots(1)$$

where $\quad deg\, r(x) < deg\,(x^3+3x+1)=3.$

We may choose $\quad r(x)=a_0+a_1x+a_2x^2\in \mathbf{Q}[x].$

By (1), $\quad f(x)+A=r(x)+t(x)(x^3+3x+1)+A,$

where $\quad A=\langle x^3+3x+1\rangle=\{(x^3+3x+1)\,g(x): g(x)\in \mathbf{Q}[x]\}.$

$\therefore \quad f(x)+A=r(x)+A,$ since $t(x)(x^3+3x+1)\in A.$

Hence $f(x)+\langle x^3+3x+1\rangle=a_0+a_1x+a_2x^2+\langle x^3+3x+1\rangle, \quad \ldots(2)$

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 $\quad a_0+a_1x+A=a_0+a_1t,$ 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 $\theta : C \to F[x]/A$ 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

$$\alpha_i = \frac{b_i}{a_i}\ ;\ b_i \in R,\ a_i \neq 0 \in R,\ 1 \leq i \leq n.$$

$$\therefore \qquad f(x) = \frac{b_0}{a_0} + \frac{b_1}{a_1}x + \ldots + \frac{b_n}{a_n}x^n$$

$$= \frac{1}{a}(b_0 a_1 \ldots a_n + b_1 a_0 a_2 \ldots a_n x + b_n a_0 a_1 \ldots a_{n-1} x^n),$$

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 $a_1a_2 \ldots a_n = b_1\,b_2 \ldots b_n$.

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 $u \in R$

$$\Rightarrow \quad \frac{a_i}{b_i} = u^{-1} \quad \Rightarrow \quad u_i = u^{-1},\ u^{-1} \text{ is a unit in } R.$$

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 lement 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]