To prove the reverse inclusion, we proceed as follows :

Let $a = \sqrt{2} + \sqrt[3]{5}$. Then $a \in Q(a) \Rightarrow a^2 \in Q(a)$

$\Rightarrow 2 + 2\sqrt{2}\sqrt[3]{5} + \sqrt[3]{25} \in Q(a)$

$\Rightarrow 2\sqrt{2}\sqrt[3]{5} + \sqrt[3]{25} \in Q(a)$, since $2 \in Q(a)$

$\Rightarrow \sqrt[3]{5}(\sqrt{2} + \sqrt{2} + \sqrt[3]{5}) \in Q(a)$

$\Rightarrow 5[\sqrt{2} + (\sqrt{2} + \sqrt[3]{5})]^3 \in Q(a)$

$\Rightarrow (\sqrt{2} + a)^3 \in Q(a)$, since $5 \in Q(a)$

$\Rightarrow 2\sqrt{2} + 6a + 3\sqrt{2}a^2 + a^3 \in Q(a)$, where $6a + a^3 \in Q(a)$

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

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

$\Rightarrow a - \sqrt[3]{5} \in Q(a)$, since $a = \sqrt{2} + \sqrt[3]{5}$

$\Rightarrow \sqrt[3]{5} \in Q(a)$, since $a \in Q(a)$.

Thus $\sqrt{2}, \sqrt[3]{5} \in Q(\sqrt{2} + \sqrt[3]{5})$ and so

$$Q(\sqrt{2}, \sqrt[3]{5}) \subseteq Q(\sqrt{2} + \sqrt[3]{5}). \qquad ...(2)$$

From (1) and (2), $Q(\sqrt{2}, \sqrt[3]{5}) = Q(\sqrt{2} + \sqrt[3]{5})$.

Example 4.3.4. *Find an element* $u \in \mathbf{R}$ *(Real nos) such that* $Q(\sqrt{2}, \sqrt[3]{5}) = Q(u)$.

Hint. $u = \sqrt{2} + \sqrt[3]{5} \in \mathbf{R}$.

Example 4.3.5. *Show that* $\sqrt{2} + \sqrt[3]{5}$ *is algebraic of degree 6 over rationals.* [D.U., 1999]

Solution. We have seen that $Q(\sqrt{2}\sqrt[3]{5}) = Q(\sqrt{2} + \sqrt[3]{5})$. [Example 4.3.3]

Since $x^2 - 2$ is an irreducible monic polynomial of least degree 2 over Q satisfied by 2, so

$$[Q(\sqrt{2}) : Q] = 2.$$

By Eisenstein criterion, $x^3 - 5$ is irreducible over Q. Indeed $x^3 - 5$ is an irreducible monic polynomial of least degree 3 over $Q \subset Q(\sqrt{2})$ satisfied by $\sqrt[3]{5}$. So

$[(Q(\sqrt{2}))(\sqrt[3]{5}) : Q(\sqrt{2})] = 3$ or $[Q(\sqrt{2}, \sqrt[3]{5}) : Q(\sqrt{2})] = 3$.

We have $Q \subset Q(\sqrt{2}) \subset Q(\sqrt{2}, \sqrt[3]{5})$ and

$[Q(\sqrt{2}, \sqrt[3]{5}) : Q] = [Q(\sqrt{2}, \sqrt[3]{5}) : Q(\sqrt{2})]\,[Q(\sqrt{2}) : Q] = 3 \times 2 = 6.$

$\therefore \quad [Q(\sqrt{2} + \sqrt[3]{5}) : Q] = 6.$

Hence $\sqrt{2} + \sqrt[3]{5}$ is algebraic of degree 6 over Q.

Example 4.3.6. *Determine the minimal polynomial over* Q *of the number* $\sqrt{2} + \sqrt[3]{5}$.

Solution. Let $a = \sqrt{2} + 5^{1/3}$. Then $(a - \sqrt{2})^3 = 5$

$\Rightarrow a^3 - 3\sqrt{2}a^2 + 6a - 2\sqrt{2} = 5 \Rightarrow a^3 + 6a - 5 = \sqrt{2}(3a^2 + 2)$

$\Rightarrow (a^3 + 6a - 5)^2 = 2(3a^2 + 2)^2$

$\Rightarrow a^6 + 36a^2 + 25 + 12a^4 - 10a^3 - 60a = 2(9a^4 + 12a^2 + 4)$

$\Rightarrow a^6 - 6a^4 - 10a^3 + 12a^2 - 60a + 17 = 0.$

Thus $\sqrt{2} + \sqrt[3]{5}$ satisfies the polynomial $f(x) = x^6 - 6x^4 - 10x^3 + 12x^2 - 60x + 17$ over $\mathbf{Q}$ and $deg\, f(x) = 6$.

Example 4.3.7. *Show that $\sqrt{3} + \sqrt[3]{2}$ is algebraic of degree 6 over Q.*

Please try yourself

Example 4.3.8. *Give an example of an algebraic extension which is not a finite extension.* [D.U., 1994]

Solution. Let $K = \mathbf{C}$ (field of complex numbers) and $F = \mathbf{Q}$ (field of rational numbers). Let T be the set of all elements of K which are algebraic over F. Then T is a subfield of K [See Theorem 4.3.5.] and $F \subseteq T$. It is clear that T is an algebraic extension of F. We shall show that T is not a finite extension of F. Let, if possible, $[T : F] = n$ (finite).

Let $f(x) = x^{n+1} - 3 \in F[x]$.

By Eisenstein criterion, $f(x)$ is irreducible over F of degree $n + 1$. Let α be a root of $f(x)$ *i.e.*, $f(\alpha) = 0$. It means that α is algebraic over F and so $\alpha \in T$. By Remark of Theorem 4.3.4, we see that

$$[F(\alpha) : F] = deg\, f(x) = n + 1.$$

We have $[T : F] = [T : F(\alpha)]\,[F(\alpha) : F]$

or $n = [T : F(\alpha)]\,(n + 1)$ *i.e.*, $n > n + 1$, which is impossible.

Hence $[T : F]$ is not finite *i.e.*, T is not a finite extension of F, although T is an algebraic extension and F.

Example 4.3.9. *Let F be a finite field and K a subfield of F. Prove that F/K is algebraic.* [D.U., 1998]

Solution. By the given hypothesis, F is a finite dimensional vector space over K and so $[F : K] = dim_K F$, which is finite $\Rightarrow F$ is a finite extension of K.

Hence F is an algebraic extension of K. [Theorem 4.3.1]

Example 4.3.10. *Let $a, b \in K$ be algebraic over F of degrees m and n, respectively. If m and n are relatively prime, then prove that $F(a, b)$ is of degree mn over F.*

Solution. We have $[F(a) : F] = m$ and $[F(b) : F] = n$.

Let $f(x) = x^n + \alpha_1 x^{n-1} + \ldots + \alpha_n$ be the minimal polynomial of b over F. Then $f(x)$ is also a polynomial over $F(a)$. [$\because F \subset F(a)$]

Thus b is algebraic of degree at most n over $F(a)$. Consequently,

$$[(F(a))(b) : F(a)] \leq n \text{ i.e., } [F(a, b) : F(a)] \leq n$$

$$\therefore \quad [F(a, b) : F] = [F(a, b) : F(a)]\,[F(a) : F] \leq nm$$

Solution. Let $a = \sqrt{2} + 5^{1/3}$. Then $(a - \sqrt{2})^3 = 5$

$\Rightarrow a^3 - 3\sqrt{2}a^2 + 6a - 2\sqrt{2} = 5 \Rightarrow a^3 + 6a - 5 = \sqrt{2}(3a^2 + 2)$

$\Rightarrow (a^3 + 6a - 5)^2 = 2(3a^2 + 2)^2$

$\Rightarrow a^6 + 36a^2 + 25 + 12a^4 - 10a^3 - 60a = 2(9a^4 + 12a^2 + 4)$

$\Rightarrow a^6 - 6a^4 - 10a^3 + 12a^2 - 60a + 17 = 0.$

Thus $\sqrt{2} + \sqrt[3]{5}$ satisfies the polynomial $f(x) = x^6 - 6x^4 - 10x^3 + 12x^2 - 60x + 17$ over $\mathbf{Q}$ and $deg\, f(x) = 6$.

Example 4.3.7. *Show that* $\sqrt{3} + \sqrt[3]{2}$ *is algebraic of degree* 6 *over* Q.

Please try yourself

Example 4.3.8. *Give an example of an algebraic extension which is not a finite extension.* [D.U., 1994]

Solution. Let $K = \mathbf{C}$ (field of complex numbers) and $F = \mathbf{Q}$ (field of rational numbers). Let T be the set of all elements of K which are algebraic over F. Then T is a subfield of K [See Theorem 4.3.5.] and $F \subseteq T$. It is clear that T is an algebraic extension of F. We shall show that T is not a finite extension of F. Let, if possible, $[T : F] = n$ (finite).

Let $f(x) = x^{n+1} - 3 \in F[x]$.

By Eisenstein criterion, $f(x)$ is irreducible over F of degree $n + 1$. Let α be a root of $f(x)$ *i.e.*, $f(\alpha) = 0$. It means that α is algebraic over F and so $\alpha \in T$. By Remark of Theorem 4.3.4, we see that

$$[F(\alpha) : F] = deg\, f(x) = n + 1.$$

We have $[T : F] = [T : F(\alpha)]\,[F(\alpha) : F]$

or $n = [T : F(\alpha)]\,(n + 1)$ *i.e.*, $n > n + 1$, which is impossible.

Hence $[T : F]$ is not finite *i.e.*, T is not a finite extension of F, although T is an algebraic extension and F.

Example 4.3.9. *Let* F *be a finite field and* K *a subfield of* F. *Prove that* F/K *is algebraic.* [D.U., 1998]

Solution. By the given hypothesis, F is a finite dimensional vector space over K and so $[F : K] = dim_K F$, which is finite $\Rightarrow$ F is a finite extension of K.

Hence F is an algebraic extension of K. [Theorem 4.3.1]

Example 4.3.10. *Let* $a, b \in K$ *be algebraic over* F *of degrees* m *and* n, *respectively. If* m *and* n *are relatively prime, then prove that* $F(a, b)$ *is of degree* mn *over* F.

Solution. We have $[F(a) : F] = m$ and $[F(b) : F] = n$.

Let $f(x) = x^n + \alpha_1 x^{n-1} + \ldots + \alpha_n$ be the minimal polynomial of b over F. Then $f(x)$ is also a polynomial over $F(a)$. [$\because F \subset F(a)$]

Thus b is algebraic of degree at most n over $F(a)$. Consequently,

$$[(F(a))(b) : F(a)] \leq n \text{ i.e., } [F(a, b) : F(a)] \leq n$$

$$\therefore \quad [F(a, b) : F] = [F(a, b) : F(a)]\,[F(a) : F] \leq nm$$

i.e., $[F(a, b) : F] \leq mn.$ ...(1)

Again $[F(a, b) : F] = [F(a, b) : F(a)]\,[F(a) : F]$

$\Rightarrow$ $[F(a) : F]$ divides $[F(a, b) : F]$ ...(2)

$\Rightarrow m$ divides $[F(a, b) : F]$.

Also $[F(a, b) : F] = [F(a, b) : F(b)]\,[F(b) : F]$

$\Rightarrow$ $[F(b) : F]$ divides $[F(a, b) : F]$

$\Rightarrow n$ divides $[F(a, b) : F]$. ...(3)

Since $(m, n) = 1$, so by (2) and (3), mn divides $[F(a, b) : F]$

$\Rightarrow$ $mn \leq [F(a, b) : F]$. ...(4)

From (1) and (4), $[F(a, b) : F] = mn$.

Example 4.3.11. *If $a \in K$ is algebraic over F of odd degree, prove that $F(a) = F(a^2)$.*

Solution. Since $F(a)$ is the smallest field containing F and a, $a^2 \in F(a)$ and so $F(a^2) \subseteq F(a)$. ...(1)

Since $a \in K$ is algebraic over F of odd degree, we may take

$$p(x) = x^{2n+1} + \alpha_0 x^{2n} + \alpha_1 x^{2n-1} + \ldots + \alpha_{2n}$$

as the minimal polynomial of a over F. Then

$$0 = p(a) = a^{2n+1} + \alpha_0 a^{2n} + \alpha_1 a^{2n-1} + \alpha_2 a^{2n-2} + \ldots + \alpha_{2n-1} a + \alpha_{2n}$$

or $$a(a^{2n} + \alpha_1 a^{2n-2} + \ldots + \alpha_{2n-1}) + (\alpha_0 a^{2n} + \alpha_2 a^{2n-2} + \ldots + \alpha_{2n}) = 0$$ ...(2)

We have $[F(a) : F] = deg\, p(x) = 2n + 1$.

It follows that $a^{2n} + \alpha_1 a^{2n-2} + \ldots + \alpha_{2n-1} \neq 0$, for otherwise, a satisfies the polynomial $x^{2n} + \alpha_1 x^{2n-2} + \ldots + \alpha_{2n-1} \in F[x]$ of degree less than $2n + 1$, which is a contradiction.

We write $b = a^{2n} + \alpha_1 a^{2n-2} + \ldots + \alpha_{2n-1}$.

Then $b \neq 0 \in K$ and so b^{-1} exists.

From (2), we obtain

$$a = -(\alpha_0 a^{2n} + \alpha_2 a^{2n-2} + \ldots + \alpha_{2n})(a^{2n} + \alpha_1 a^{2n-2} + \ldots + \alpha_{2n-1})^{-1}$$ ...(3)

The R.H.S. of (3) being a polynomial in a^2 over F implies that

$$a \in F(a^2) \Rightarrow F(a) \subseteq F(a^2).$$ ...(4)

From (1) and (4), $F(a) = F(a^2)$.

Definition of an algebraic number

A complex number is said to be an **algebraic number**, *if it is algebraic over* **Q** *(rationals).*

For example, $1 + i$ is an algebraic number, since $a = 1 + i$ satisfies the polynomial $x^2 - 2x + 2 \in Q[x]$.

[Notice that $a = 1 + i \Rightarrow (a - 1)^2 = -1 \Rightarrow a^2 - 2a + 2 = 0$]

Definition of an algebraic integer

An algebraic number is said to be an **algebraic integer**, *if it satisfies an integer monic polynomial of the form*

$$x^n + \alpha_1 x^{n-1} + \ldots + \alpha_n \in \mathbf{Z}[x].$$

For example, $1 + i$ is an algebraic integer.

Example 4.3.12. *If a is any algebraic number, prove that there exists a positive integer n such that na is an algebraic integer.* [D.U., 1994]

Solution. Since a is an algebraic number, there exists a non-zero polynomial $f(x) \in \mathbf{Q}[x]$ such that $f(a) = 0$.

Let $\quad f(x) = x^r + \alpha_1 x^{r-1} + \alpha_2 x^{r-2} + \ldots + \alpha_r, \quad \alpha_i \in \mathbf{Q}.$

We can write $\alpha_i = \dfrac{m_i}{n_i}$, m_i, n_i are integers and $n_i > 0$.

Since $f(a) = 0$, $a^r + \dfrac{m_1}{n_1} a^{r-1} + \dfrac{m_2}{n_2} a^{r-2} + \ldots + \dfrac{m_r}{n_r} = 0.$ ...(1)

Let $n = n_1 n_2 \ldots n_r$, which is a positive integer.

From (1), we get

$$na^r + m_1 n_2 \ldots n_r a^{r-1} + m_2 n_1 n_3 \ldots n_r a^{r-2} + m_r n_1 n_2 \ldots n_{r-1} = 0.$$

Multiplying throughout by n^{r-1}, we get

$$n^r a^r + m_1 n_2 \ldots n_r . n^{r-1} a^{r-1} + m_2 n_1 n_3 \ldots n_r n . n^{r-2} a^{r-2} + \ldots + m_r n_1 n_2 \ldots n_{r-1} n^{r-1} = 0$$

We see that na satisfies the integer monic polynomial

$$x^r + m_1 n_2 \ldots n_r x^{r-1} + \ldots + m_r n_1 n_2 \ldots n_{r-1} n^{r-1}.$$

Hence na is an algebraic integer, where $n = n_1 n_2 \ldots n_r$ is a +ve integer.

Example 4.3.13. *If a is an algebraic integer and m is an ordinary integer, prove that ma is an algebraic integer.*

Solution. Since a is an algebraic integer, a satisfies some integer monic polynomial, say

$$\therefore \quad x^n + \alpha_1 x^{n-1} + \ldots + \alpha_n \in \mathbf{Z}[x].$$

$$a^n + \alpha_1 a^{n-1} + \ldots + \alpha_n = 0. \quad \ldots(1)$$

Multiplying throughout by m^n, we get

$$m^n a^n + \alpha_1 m^n a^{n-1} + \alpha_2 m^n a^{n-2} + \ldots + \alpha_{n-1} m^n a + \alpha_n m^n = 0$$

or $\quad (ma)^n + \alpha_1 m (ma)^{n-1} + \alpha_2 m^2 (ma)^{n-2} + \ldots + \alpha_{n-1} m^{n-1} (ma) + \alpha_n m^n = 0.$

This shows that ma satisfies the integer monic polynomial

$$x^n + (\alpha_1 m) x^{n-1} + (\alpha_2 m^2) x^{n-2} + \ldots + (\alpha_{n-1} m^{n-1}) x + (\alpha_n m^n).$$

Hence ma

Example 4.3.14. *If the rational number r is also an algebraic inte prove that r must be an ordinary integer.*

Solution. Let $r = p/q$, where p, q are relatively prime integers $q > 0$. Since r is an algebraic integer, r satisfies an integer monic polynomial, say

$$x^n + \alpha_1 x^{n-1} + \ldots + \alpha_{n-1} x + \alpha_n \in \mathbf{Z}[x].$$

$$\therefore \quad r^n + \alpha_1 r^{n-1} + \ldots + \alpha_{n-1} r + \alpha_n = 0$$

or $$\frac{p^n}{q^n} + \alpha_1 \frac{p^{n-1}}{q^{n-1}} + \ldots + \alpha_{n-1} \frac{p}{q} + \alpha_n = 0$$

or $$p^n + \alpha_1 p^{n-1} q + \ldots + \alpha_{n-1} p q^{n-1} + \alpha_n q^n = 0$$

or $$p^n + q(\alpha_1 p^{n-1} + \ldots + \alpha_{n-1} p q^{n-2} + \alpha_n q^{n-1}) = 0$$

or $$p^n + qt = 0, \quad \text{where} \quad t = \alpha_1 p^{n-1} + \ldots + \alpha_n q^{n-1} \text{ is an integer}$$

or $$p^n = q(-t) \Rightarrow q \mid p^n, \text{ where } (p, q) = 1$$

$$\Rightarrow \quad q = 1 \Rightarrow r = p, \; p \text{ is an integer.}$$

Hence r is an ordinary integer.

Example 4.3.15. *Prove that sin 1° is an algebraic number.*

Solution. We know

$$e^{\pi i/180} = \cos\frac{\pi}{180} + i \sin\frac{\pi}{180}.$$

$$\therefore \quad (e^{\pi i/180})^{180} = \left(\cos\frac{\pi}{180} + i \sin\frac{\pi}{180}\right)^{180} = \cos\pi + i \sin\pi = -1.$$

It follows that $e^{\pi i/180}$ is a root of $x^{180} + 1 = 0$

and so $$e^{\pi i/180} = \cos\frac{\pi}{180} + i \sin\frac{\pi}{180} \text{ is an algebraic number.}$$

Similarly, $$\cos\frac{\pi}{180} - i \sin\frac{\pi}{180} \text{ is an algebraic number.}$$

Consequently, $2\cos\frac{\pi}{180}$ is an algebraic number and so

$$\cos\frac{\pi}{180} \text{ is an algebraic number.}$$

This shows that cos 1° is an algebraic number.

Since $\cos\frac{\pi}{180} + i \sin\frac{\pi}{180}$, $\cos\frac{\pi}{180}$ are algebraic numbers ; so

$$i \sin\frac{\pi}{180} \text{ is an algebraic number.}$$

Since i is an algebraic number ($\because$ i satisfies $x^2 + 1 \in Q[x]$, $\sin\frac{\pi}{180}$ is an algebraic number. Hence sin 1° is an algebraic number

Example 4.3.16. *Prove that for every integer m, both cos m° and sin m° are algebraic numbers.*

Hint. We know

$$(e^{\pi mi/180}) = \cos m\pi + i \sin m\pi = \pm 1$$

i.e., $e^{\pi mi/180}$ is a root of $x^{180} \pm 1 = 0$.

Now proceed like Example 4.3.15.

4.4 Roots of Polynomials

Let F be any field and $p(x) \in F[x]$. Our aim is to find an extension K of F in which $p(x)$ has a root. *An element $a \in K$ is called a* **root** *of $p(x)$, if $p(a) = 0$.*

Theorem 4.4.1. (Remainder Theorem)

Let K be an extension of a field F and let $p(x) \in F[x]$ and $a \in K$. Then there exists $q(x) \in K[x]$ such that $p(x) = (x-a)\,q(x) + p(a)$, where $\deg q(x) = \deg p(x) - 1$. [D.U., 1994]

Proof. Since $F \subseteq K$, $F[x] \subseteq K[x]$ and so $p(x) \in K[x]$. Also $a \in K$ $\Rightarrow x - a \in K[x]$. By Division algorithm in $K[x]$, for $p(x)$, $(x-a) \in K[x]$; there exist $q(x)$ and $r(x) \in K[x]$ such that

$$p(x) = (x-a)\,q(x) + r(x), \qquad \ldots(1)$$

where either $r(x) = 0$ or $\deg r(x) < \deg (x-a) = 1$.

In the latter case, $r(x)$ is a constant polynomial and so $r(x) = \alpha$, for some $\alpha \neq 0 \in K$. Now (1) can be written as

$$p(x) = (x-a)\,q(x) + \alpha \qquad \ldots(2)$$

$\Rightarrow$ $p(a) = \alpha$ and so (2) becomes

$$p(x) = (x-a)\,q(x) + p(a). \qquad \ldots(3)$$

Since $\deg (x-a) = 1$ and $p(a) = \alpha$ is a constant, (3) implies that

$$\deg q(x) = \deg p(x) - 1.$$

Hence the theorem.

Corollary. *If $a \in K$ is a root of $p(x) \in F[x]$, then $(x-a)$ divides $p(x)$ in $K[x]$.*

Proof. We have proved above that

$$p(x) = (x-a)\,q(x) + p(a).$$

Since $a \in K$ is a root of $p(x)$; $p(a) = 0$ and so

$$p(x) = (x-a)\,q(x).$$

Since the above equation holds in $K[x]$, it follows that $(x-a)$ divides $p(x)$ in $K[x]$.

Definition. *If K be an extension of a field F, then $a \in K$ is called a root of $p(x) \in F[x]$ of* **multiplicity** *m, if*

$$(x-a)^m \mid p(x), \text{ but } (x-a)^{m+1} \nmid p(x).$$

Theorem 4.4.2. *A polynomial of degree $n \geq 1$ over a field F can have at most n roots in any extension field of F.*

Proof. Let $p(x) \in F[x]$ be a polynomial of degree $n \geq 1$. We shall prove that result by induction on n. In $n = 1$, then $p(x)$ is of the form $p(x) = \alpha x + \beta$; where $\alpha \neq 0 \in F$ and $\beta \in F$. Let $a = -\alpha^{-1}\beta \in F$.

Then $p(a) = 0$ and so $p(x)$ has exactly one root $a = -\alpha^{-1}\beta \in F$ and F is an extension field of F itself. Thus the result is true for $n = 1$. Suppose that the result is true for all polynomials of positive degree $< n$ over any *field*. Let K be an extension of F. If K has no roots of $f(x)$, the result is obviously true. Suppose some $b \in K$ is a root of $p(x)$, of multiplicity $m \geq 1$. Then $(x-b)^m$ divides $p(x)$ in $K[x]$. Therefore,

$$p(x) = (x-b)^m f(x), \text{ for some } f(x) \in K[x]. \quad \ldots(1)$$

We see that $deg\, f(x) = n - m < n$.

By induction hypothesis, $f(x)$ has at most $n - m$ roots in K. Hence, by (1), $p(x)$ has at most $m + (n - m) = n$ roots in K. This completes the induction and the theorem is proved.

Theorem 4.4.3. (Kronecker Theorem)

If $p(x)$ is an irreducible polynomial of degree $n \geq 1$ over a field F, then there exists an extension K of F such that $[K : F] = n$ and $p(x)$ has a root in K. [D.U., 1998, 9

Proof. Since $p(x)$ is irreducible over the field F, $M = \langle p(x) \rangle$ is maximal ideal of $F[x]$ and so $\frac{F[x]}{M}$ is a field. Let $K = \frac{F[x]}{M}$.

Define a mapping $\theta : F \to K$ as

$$\theta(\alpha) = \alpha + M \in K, \forall\, \alpha \in F$$

Then θ is well-defined and one-to-one, since

$$\theta(\alpha) = \theta(\beta) \Leftrightarrow \alpha + M = \beta + M \Leftrightarrow \alpha - \beta \in M$$
$$\Leftrightarrow \alpha - \beta = 0 \Leftrightarrow \alpha = \beta.$$

For any $\alpha, \beta \in F$; we have

$$\theta(\alpha + \beta) = \alpha + \beta + M = (\alpha + M) + (\beta + M) = \theta(\alpha) + \theta(\beta),$$
$$\theta(\alpha\beta) = \alpha\beta + M = (\alpha + M)(\beta + M) = \theta(\alpha)\,\theta(\beta).$$

Thus θ is an isomorphism of F into K and so $F \approx \theta(F)$, where $\theta(F)$ is a subfield of K. *K can be regarded as an extension of F, where we identify F with its image $\theta(F)$ in K and each α in F with $\bar{\alpha} = \alpha + M$ in K.*

Let $\quad p(x) = \alpha_0 + \alpha_1 x + \ldots + \alpha_n x^n \in F[x],\ \alpha_n \neq 0 \in F.$

Then $deg\, p(x) = n$ and $p(x) \in M \Rightarrow p(x) + M = M \Rightarrow \overline{p(x)} = \bar{0}$.

By the identification $\alpha \leftrightarrow \bar{\alpha}$, $\overline{p(x)} = \bar{0}$ reduces to

or $\quad \alpha_0 + \alpha_1 \bar{x} + \alpha_2 (\bar{x})^2 + \ldots + \alpha_n (\bar{x})^n = \bar{0},$

where $\quad \bar{x} = x + M \in K.$

Hence it follows that $\bar{x} \in K$ is a root of $p(x)$ and further

$$[K : F] \geq deg\, p(x) = n \text{ i.e., } [K : F] \geq n.$$

By Division algorithm in $F[x]$, for *any* $f(x) \in F[x]$ and $p(x) \in F[x]$, there exist $t(x), r(x) \in F[x]$ such that $f(x) = p(x)\, t(x) + r(x)$, where either $r(x) = 0$ or $deg\, r(x) < deg\, p(x) = n$.

Now $$f(x) + M = p(x)\, t(x) + r(x) + M = r(x) + M,$$
since $p(x)\, t(x) \in M = \langle p(x) \rangle$.

Since $r(x) = 0$ or $deg\, r(x) < n$, we can take

$$r(x) = \beta_0 + \beta_1 x + \ldots + \beta_{n-1} x^{n-1} \in F[x].$$

We have $f(x) + M = r(x) + M \Rightarrow \overline{f(x)} = \overline{r(x)}$.

$$\overline{f(x)} = \beta_0 + \beta_1 \bar{x} + \ldots + \beta_{n-1} (\bar{x})^{n-1}, \forall \overline{f(x)} \in K$$

$\therefore$ This shows that every element of K is spanned over F by the set

$$\{\bar{1}, \bar{x}, (\bar{x})^2, \ldots (\bar{x})^{n-1}\}.$$

Consequently, $$[K : F] \leq n. \qquad \ldots(2)$$

From (1) and (2), $[K : F] = n$.

We have earlier proved that K is an extension of F in which $p(x)$ has a root.

Corollary. *If $f(x) \in F[x]$, then there is a finite extension K of F in which $f(x)$ has a root. Further $[K : F] \leq deg\, f(x)$.*

Proof. Let $p(x)$ be an irreducible factor of $f(x)$ in $F[x]$. Then $f(x) = p(x)\, g(x)$, for some $g(x) \in F[x]$.

Since $p(x)$ is irreducible over F, there exists an extension K of F in which $p(x)$ has a root. Let $\alpha \in K$ be a root of $p(x)$, so that $p(\alpha) = 0$. We have

$$f(\alpha) = p(\alpha)\, g(\alpha) = 0, \alpha \in K.$$

It follows that $\alpha \in K$ is a root of $f(x)$.

Further $[K : F] = deg\, p(x) \leq deg\, f(x)$.

Theorem 4.4.4. *If $f(x)$ is any polynomial of degree $n \geq 1$ over a field F, then there exists an extension K of F such that $f(x)$ has n roots in K and $[K : F] \leq n!$.*

Proof. We have $deg\, f(x) = n$. We shall prove the result by induction on n. If $n = 1$, than $f(x)$ is of the form : $f(x) = \alpha x + \beta$, where $\alpha, \beta \in F$ and $\alpha \neq 0$. It is clear that $-\alpha^{-1} \beta \in F$ is the root of $f(x)$ and $[F : F] = 1$.

Thus the result is true for $n = 1$.

Suppose the result is true for *any* polynomial of degree $< n$ over *any* field. We shall prove that the result is true for $f(x)$ with $deg\, f(x) = n$. By the above corollary, there exists an extension L of F in which $f(x)$ has a root say $a \in L$, and $[L : F] \leq deg\, f(x) = n$. We can write $f(x) = (x - a)\, g(x)$, where $(x - a) \in L[x], g(x) \in L[x]$ and $deg\, g(x) = n - 1 < n$. By induction hypothesis, there exists an extension K of L containing $(n - 1)$ roots of $g(x)$ and $[K : L] \leq (n - 1)!$.

Thus $[K : F] = [K : L]\, [L : F] \leq n(n - 1)! = n!$.

Obviously, $a \in L \Rightarrow a \in K$ and K also contains $(n - 1)$ roots of $g(x)$.

Hence K is an extension of F such that $f(x)$ has n roots in K and $[K : F] \leq n!$. This completes the induction and the theorem is proved.

Remark. In the above theorem, if $a_1, a_2, \ldots, a_n$ are the n roots of $f(x)$ in K, then $F(a_1, a_2, \ldots, a_n)$ is the smallest subfield of K containing F and all the roots of $f(x)$. Further we can express $f(x)$ as a product of linear factors in $K[x]$ as follows :

$$f(x) = \alpha (x - a_1)(x - a_2) \ldots (x - a_n), \alpha \neq 0 \in F.$$

The field $F(a_1, a_2, \ldots, a_n)$ is called a *splitting field* of $f(x)$ over F.

Definition (Splitting Field)

Let $f(x)$ be any polynomial of degree $n \geq 1$ over a field F. A field extension K of F is called a **splitting field** *of $f(x)$, if*

(i) $f(x)$ can be factored into n linear factors over K, and

(ii) $f(x)$ cannot be factored into n linear factors over any subfield of K containing F.

In other words, K is a splitting field of $f(x) \in F[x]$ with $\deg f(x) = n \geq 1$, if K contains the n roots $a_1, a_2, \ldots, a_n$ of $f(x)$ and $K = F(a_1, a_2, \ldots, a_n)$, the smallest field containing F and n roots $a_1, a_2, \ldots, a_n$ of $f(x)$ in K.

In the light of the above definition, Theorem 4.4.4 can be restated as

Theorem 4.4.5. *There exists a splitting field for every polynomial $f(x) \in F[x]$ with $\deg f(x) \geq 1$.*

Theorem 4.4.6. *Any two splitting fields of a polynomial $f(x) \in F[x]$ with $\deg f(x) \geq 1$ are isomorphic. More specifically, if K and K' are any two splitting fields of a polynomial $f(x)$ of degree $n \geq 1$ over a field F, then there exists are isomorphism ψ of K onto K' such that $\psi(\alpha) = \alpha$, for all $\alpha \in F$.*

The proof of the theorem is omitted.

In the following problems of splitting fields, we shall use the following :

Formula. *If $a \in K$ is algebraic over F, then*

$[F(a) : F]$ = *degree of the unique monic irreducible polynomial over F satisfied by a.* [See Theorem 4.3.4.]

EXAMPLES

Example 4.4.1. *Find the degree of the splitting field of $x^2 - 3$ over* **Q**.

Solution. We have $x^2 - 3 = (x - \sqrt{3})(x + \sqrt{3})$.

Hence the splitting field of $x^2 - 3$ over **Q** is $\mathbf{Q}(\sqrt{3})$.

Further $x^2 - 3$ is the irreducible polynomial of lowest degree over **Q** satisfied by $\sqrt{3}$. Hence

$$[\mathbf{Q}(\sqrt{3}) : \mathbf{Q}] = \deg(x^2 - 3) = 2.$$

Example 4.4.2. *Find the degree of the splitting field of $x^4 - 1$ o* **Q**.

[D U., 19

Solution. We have

$$x^4 - 1 = (x^2 - 1)(x^2 + 1) = (x - 1)(x + 1)(x - i)(x + i).$$

Thus the roots of $x^4 - 1 = 0$ are ± 1 and $\pm i$, $i = \sqrt{-1}$. Hence the splitting field of $x^4 - 1$ over $\mathbf{Q}$ is $\mathbf{Q}(i)$ and $[\mathbf{Q}(i) : Q] = 2$, since $x^2 + 1$ is the irreducible polynomial of degree 2 over $\mathbf{Q}$, which is satisfied by i.

Example 4.4.3. *Obtain the splitting field and its degree over* $\mathbf{Q}$ *for* $f(x) = x^4 - 5x^2 + 6 \in \mathbf{Q}[x]$. [D.U., 2000]

Solution. We have

$$f(x) = (x^2 - 3)(x^2 - 2) = (x - \sqrt{3})(x + \sqrt{3})(x - \sqrt{2})(x + \sqrt{2}).$$

Thus the roots of $f(x)$ are $\pm\sqrt{2}$ and $\pm\sqrt{3}$. Hence $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ is the splitting field of $f(x)$ over $\mathbf{Q}$. We have

$$[\mathbf{Q}(\sqrt{2}) : \mathbf{Q}] = deg\,(x^2 - 2) = 2,$$

since $x^2 - 2$ is the irreducible polynomial over $\mathbf{Q}$ of degree 2, satisfied by $\sqrt{2}$. Again $x^2 - 3$ is an irreducible polynomial of degree 2 over $\mathbf{Q} \subset \mathbf{Q}(\sqrt{2})$, which is satisfied by $\sqrt{3}$. Consequently,

$$[(\mathbf{Q}(\sqrt{2}))(\sqrt{3}) : \mathbf{Q}(\sqrt{2})] = deg\,(x^2 - 3) = 2$$

$$[\mathbf{Q}(\sqrt{2}, \sqrt{3}) : \mathbf{Q}(\sqrt{2})] = 2.$$

i.e., Hence

$$[\mathbf{Q}(\sqrt{2}, \sqrt{3}) : \mathbf{Q}] = [\mathbf{Q}(\sqrt{2}, \sqrt{3}) : \mathbf{Q}(\sqrt{2})]\,[\mathbf{Q}(\sqrt{2}) : \mathbf{Q}]$$
$$= 2 \times 2 = 4.$$

Example 4.4.4. *Obtain the splitting field and its degree over* $\mathbf{Q}$ *for* $f(x) = x^4 - 8x^2 + 15 \in \mathbf{Q}[x]$

Hint. $K = \mathbf{Q}(\sqrt{3}, \sqrt{5})$ is the splitting field of $f(x)$ over $\mathbf{Q}$ and $[K : \mathbf{Q}] = 4$.

Example 4.4.5. *Find the degree of the splitting field of* $x^4 + 1$ *over* $\mathbf{Q}$. [D.U., 1995, 94]

Solution. We have $x^4 + 1 = 0 \Rightarrow x = (-1)^{1/4}$.

$\therefore$ $x = (\text{as } \pi + i \sin \pi)^{1/4}$.

By De Moivre's Theorem, we get

$$x = \cos\frac{2k\pi + \pi}{4} + i \sin\frac{2k\pi + \pi}{4},\ k = 0, 1, 2, 3$$

or

$$x = \frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}},\ -\frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}},\ -\frac{1}{\sqrt{2}} - \frac{i}{\sqrt{2}},\ \frac{1}{\sqrt{2}} - \frac{i}{\sqrt{2}};\ i = \sqrt{-1}.$$

The smallest field containing $\mathbf{Q}$ and the above roots is $\mathbf{Q}(\sqrt{2}, i)$. Hence $\mathbf{Q}(\sqrt{2}, i)$ is the splitting field of $x^4 + 1$ over $\mathbf{Q}$. We see that

$$\mathbf{Q} \subset \mathbf{Q}(\sqrt{2}) \subset \mathbf{Q}(\sqrt{2}, i).$$

Since $x^2 - 2$ is the irreducible polynomial over $\mathbf{Q}$ of degree 2, satisfied by $\sqrt{2}$;

$$[\mathbf{Q}(\sqrt{2}) : \mathbf{Q}] = deg\,(x^2 - 2) = 2.$$

Again x^2+1 is the irreducible polynomial of degree 2 over $Q \subset Q(\sqrt{2})$, which is satisfied by i. Consequently,

$$[(Q(\sqrt{2}))(i) : Q(\sqrt{2})] = deg\,(x^2+1) = 2$$

or $$[Q(\sqrt{2}, i) : Q(\sqrt{2}) = 2.$$

Hence $$[Q(\sqrt{2}, i) : Q] = [Q(\sqrt{2}, i) : Q(\sqrt{2})]\,[Q(\sqrt{2}) : Q]$$
$$= 2 \times 2 = 4.$$

Example 4.4.6. *Find the smallest splitting field of* x^4+2 *over* Q. *Also find its degree over* Q. [D.U., 1998]

Solution. $x^4+2=0 \Rightarrow x=(-2)^{1/4}=2^{1/4}(-1)^{1/4}$.

As done in Example 4.4.5, all the roots of x^4+2 are

$$2^{1/4}\cdot\frac{1}{\sqrt{2}}(1\pm i), -2^{1/4}\cdot\frac{1}{\sqrt{2}}(1\pm i),\ i=\sqrt{-1}$$

or $$\frac{1}{2^{1/4}}(1\pm i), -\frac{1}{2^{1/4}}(1\pm i).$$

The smallest field containing Q, $2^{1/4}$ and i is $Q(2^{1/4}, i)$ and the above 4 roots obviously belong to $Q(2^{1/4}, i)$. Hence $Q(2^{1/4}, i)$ is the splitting field of x^4+2 over Q.

By Eisenstein criterion, $x^4-2 \in Q[x]$ is the irreducible polynomial of lowest degree 4 over Q, which is satisfied $2^{1/4}$.

$\therefore$ $$[Q(2^{1/4}) : Q] = deg\,(x^4-2) = 4.$$

Again $x^2+1 \in Q[x]$ is the irreducible polynomial of lowest degree 2 over $Q \subset Q(2^{1/4})$, which is satisfied by i. Consequently,

$$[(Q(2^{1/4}))(i) : Q(2^{1/4})] = deg\,(x^2+1) = 2$$

i.e., $$[Q(2^{1/4}, i) : Q(2^{1/4})] = 2.$$

Hence $$[Q(2^{1/4}, i) : Q] = [Q(2^{1/4}, i) : Q(2^{1/4})]\,[Q(2^{1/4}) : Q]$$
$$= 2 \times 4 = 8.$$

Example 4.4.7. *Determine the splitting field of* x^4-2 *over rationals.* [D.U., 1996]

Solution. $x^4-2 \Rightarrow x=2^{1/4}\cdot 1^{1/4}=2^{1/4}(\cos 0 + i \sin 0)^{1/4}$

or $$x=2^{1/4}\left[\cos\frac{2k\pi}{4}+i\sin\frac{2k\pi}{4}\right], k=0, 1, 2, 3$$

Thus the four roots of x^4-2 are $2^{1/4}, 2^{1/4}\cdot i, -2^{1/4}\cdot i, -2^{1/4}$.

The smallest field containing Q and the above roots is $Q(2^{1/4}, i)$. Hence $Q(2^{1/4}, i)$ is the required splitting field of x^4-2 over Q. Further $[Q(2^{1/4}, i) : Q] = 8$.

Example 4.4.8. *Find the degree of the splitting field of* x^6+1 *over* Q [See Example 4.4.6]

Solution. $x^6+1=0 \Rightarrow x=(-1)^{1/6}=(\cos\pi + i\sin\pi)^{1/6}$.

By De Moivre's Theorem, we get

$$x = \cos\frac{2k\pi+\pi}{6} + i\sin\frac{2k\pi+\pi}{6}, k = 0, 1, 2, 3, 4, 5.$$

The six roots of $x^6 + 1 = 0$ are

$$\frac{\sqrt{3}}{2}+\frac{i}{2}, i, -\frac{\sqrt{3}}{2}+\frac{i}{2}, -\frac{\sqrt{3}}{2}-\frac{i}{2}, -i, \frac{\sqrt{3}}{2}-\frac{i}{2}.$$

The smallest field containing $\mathbf{Q}$ and these six roots is $\mathbf{Q}(\sqrt{3}, i)$, which is the required splitting field of $x^6 + 1$ over $\mathbf{Q}$.

As discussed in Example 4.4.5, we see that

$$[\mathbf{Q}(\sqrt{3}, i) : \mathbf{Q}] = [\mathbf{Q}(\sqrt{3}, i) : \mathbf{Q}(\sqrt{3})]\,[\mathbf{Q}(\sqrt{3}) : \mathbf{Q}]$$
$$= 2 \times 2 = 4,$$

since $x^2 - 3$ is irreducible over $\mathbf{Q}$ of degree 2, which is satisfied by $\sqrt{3}$ and $x^2 + 1$ is irreducible over $\mathbf{Q}(\sqrt{3})$ of degree 2, which is satisfied by i.

Example 4.4.9. *Find the degree of the splitting field of $x^3 - 2$ over $\mathbf{Q}$.*

Solution. $x^3 - 2 = 0 \Rightarrow x = 2^{1/3} \cdot 1^{1/3} = 2^{1/3}(\cos 0 + i \sin 0)^{1/3}$.

By De Moivre's theorem, we get

$$x = 2^{1/3}\left[\cos\frac{2k\pi}{3} + i\sin\frac{2k\pi}{3}\right], k = 0, 1, 2.$$

The 3 roots of $x^3 - 2$ are

$$2^{1/3}, 2^{1/3}\left(-\frac{1}{2}+\frac{\sqrt{3}}{2}i\right), 2^{1/3}\left(-\frac{1}{2}-\frac{\sqrt{3}}{2}i\right).$$

The smallest field containing $\mathbf{Q}$ and the above roots is $\mathbf{Q}(2^{1/3}, \sqrt{3}\,i)$. Hence the splitting field of $x^3 - 2$ over $\mathbf{Q}$ is $\mathbf{Q}(2^{1/3}, \sqrt{3}\,i)$.

By Eisenstein criterion, $x^3 - 2 \in \mathbf{Q}[x]$ is the irreducible polynomial over $\mathbf{Q}$ of lowest degree 3, which is satisfied by $2^{1/3}$.

$$\therefore \quad [\mathbf{Q}(2^{1/3}) : \mathbf{Q}] = deg\,(x^3 - 2) = 3.$$

Again $x^2 + 3 \in \mathbf{Q}[x]$ is the irreducible polynomial over $\mathbf{Q} \subset \mathbf{Q}(2^{1/3})$ of lowest degree 3, which is satisfied by $\sqrt{3}\,i$.

$$\therefore \quad [(\mathbf{Q}(2^{1/3}))(\sqrt{3}\,i) : \mathbf{Q}(2^{1/3})] = deg\,(x^2 + 3) = 2$$

or
$$[\mathbf{Q}(2^{1/3}, \sqrt{3}\,i) : \mathbf{Q}(2^{1/3})] = 2.$$

Hence
$$[\mathbf{Q}(2^{1/3}, \sqrt{3}\,i) : \mathbf{Q}] = [\mathbf{Q}(2^{1/3}, \sqrt{3}\,i) : \mathbf{Q}(2^{1/3})]\,[\mathbf{Q}(2^{1/3}) : \mathbf{Q}]$$
$$= 2 \times 3 = 6.$$

Example 4.4.10. *Find the splitting field and its degree over $\mathbf{Q}$ of the polynomial $x^3 + 2$.*

Hint. The 3 roots of $x^3 + 2$ are $-2^{1/3}, 2^{1/3}\left(\frac{1 \pm \sqrt{3}\,i}{2}\right)$.

Hence the splitting field of $x^3 + 2$ over $\mathbf{Q}$ is $\mathbf{Q}(2^{1/3}, \sqrt{3}\,i)$ and its degree over $\mathbf{Q}$ is 6. (See Example 4.4.9)

Example 4.4.11. *Find the degree of the splitting field of* $f(x) = x^5 - 3x^3 + x^2 - 3$ *over* **Q**.

Solution. We see that $f(x) = (x^3 + 1)(x^2 - 3)$.

The roots of $x^2 - 3 = 0$ are $\pm\sqrt{3}$ and those of $x^3 + 1 = 0$ are $1, \frac{-1 \pm \sqrt{3}\, i}{2}$. Hence the splitting field of $f(x)$ over **Q** is $\mathbf{Q}(\sqrt{3}, i)$ and $[\mathbf{Q}(\sqrt{3}, i) : \mathbf{Q}] = 4$. [See Example 4.4.3]

Example 4.4.12. *Find the degree of the splitting field of* $f(x) = x^6 - 2x^4 + x^2 - 2$ *over* **Q**.

Hint. $f(x) = (x^4 + 1)(x^2 - 2)$. Its roots are

$$\frac{1}{\sqrt{2}}(1 \pm i), -\frac{1}{\sqrt{2}}(1 \pm i), \pm\sqrt{2}.$$ [See Example 4.4.5]

Hence the splitting field of $f(x)$ over **Q** is $\mathbf{Q}(\sqrt{2}, i)$ and $[\mathbf{Q}(\sqrt{2}, i) : \mathbf{Q}] = 4$.

Example 4.4.13. *Show that* $x^2 + 3$ *and* $x^2 + x + 1$ *over* **Q** *have same splitting field.* [D.U., 1999]

Solution. We have $x^2 + 3 = (x + \sqrt{3}\, i)(x - \sqrt{3}\, i)$.

Hence the splitting field of $x^2 + 3$ over **Q** is $\mathbf{Q}(\sqrt{3}\, i)$.

Solving $x^2 + x + 1 = 0$, we get

$$x = \frac{-1 \pm \sqrt{1 - 4}}{2} = \frac{-1 \pm \sqrt{3}\, i}{2}.$$

The smallest field containing **Q** and the above 2 roots is $\mathbf{Q}(\sqrt{3}\, i)$, which is the required splitting field of $x^2 + x + 1$ over **Q**. Hence $x^2 + 3$ and $x^2 + x + 1$ have same splitting field over **Q** *viz.* $\mathbf{Q}(\sqrt{3}\, i)$ and $[\mathbf{Q}(\sqrt{3}\, i) : \mathbf{Q}] = 2$, since $x^2 + 3$ is the irreducible polynomial over **Q** of lowest degree 2, which is satisfied by $\sqrt{3}\, i$.

Example 4.4.14. *Find the splitting field of* $x^p - 1$ *over* **Q**, *p being a prime number.*

Solution. $x^p - 1 = 0 \Rightarrow x = (1)^{1/p}$.

By De Moivre's Theorem, we obtain

$$x = \cos\left(\frac{2k\pi}{p}\right) + i \sin\left(\frac{2k\pi}{p}\right), \quad k = 0, 1, 2, \ldots, p - 1.$$

Hence the p roots of $x^p - 1$ are $e^{2k\pi i/p}$, $k = 0, 1, \ldots, p - 1$

Equivalently, the roots of $x^p - 1$ are

$$1, \alpha, \alpha^2, \ldots, \alpha^{p-1}; \quad \text{where} \quad \alpha = e^{2\pi i/p}.$$

The smallest field containing **Q** and the above roots is $\mathbf{Q}(\alpha)$.

Notice that $\alpha \in \mathbf{Q}(\alpha) \Rightarrow \alpha, \alpha^2, \alpha^3, \ldots, \alpha^{p-1} \in \mathbf{Q}(\alpha)$, since $\mathbf{Q}(\alpha)$ is a field. Hence $\mathbf{Q}(\alpha)$ is the splitting field of $x^p - 1$ over **Q**, where $\alpha = e^{2\pi i/p}$.

Clearly, α is a root of $\dfrac{x^p-1}{x-1} = x^{p-1}+x^{p-2}+\ldots+x^2+x+1$.

By Eisenstein Criterion, $1+x+x^2+\ldots+x^{p-1}$ (p a prime) is an irreducible polynomial over $\mathbf{Q}$ of degree $p-1$, which is satisfied by α. [See Example 3.4.5., Chapter 3]

Hence $[\mathbf{Q}(\alpha):\mathbf{Q}] = p-1$.

Example 4.4.15. *Determine the degree of the splitting field of the polynomial x^5-1 over the field of rational numbers.* [D.U., 1997]

Hint. Take $p=5$ in Example 4.4.14.

$\mathbf{Q}(e^{2\pi i/5})$ is the splitting field of x^5-1 over $\mathbf{Q}$.

and $[\mathbf{Q}(e^{2\pi i/5}):\mathbf{Q}] = 5-1 = 4$.

Example 4.4.16. *Determine the splitting field of x^4+x^2+1 over $\mathbf{Q}$. Also find its degree over $\mathbf{Q}$.*

Solution. If $w^3=1$, then $w^2+w+1=0$ or $w^4+w^3+w^2=0$ or $w^4+w^2+1=0 \Rightarrow w$ is a root of $x^4+x^2+1=0 \Rightarrow -w$ is also a root of x^4+x^2+1 (since w is a complex root).

We have $x^4+x^2+1 = (x^2-w^2)(x^2-w)$, since $w^3=1$, $w+w^2=-1$

$= (x^2-w^2)(x^2-w^4)$, since $w^4=w$

$= (x-w)(x+w)(x-w^2)(x+w^2)$.

Thus the four roots of x^4+x^2+1 are $\pm w, \pm w^2$. The smallest field containing $\mathbf{Q}$ and these four roots is $\mathbf{Q}(w)$.

Hence $\mathbf{Q}(w)$ or $\mathbf{Q}(\sqrt{3}\,i)$ is the splitting field of x^4+x^2+1 over $\mathbf{Q}$ and

$$[\mathbf{Q}(w):\mathbf{Q}] = [\mathbf{Q}(\sqrt{3}\,i):\mathbf{Q}] = 2,$$

since $x^2+3 \in \mathbf{Q}[x]$ is the irreducible polynomial of lowest degree 2 over $\mathbf{Q}$, which is satisfied by $\sqrt{3}\,i$.

Example 4.4.17. *If E is an extension of F and $f(x) \in F[x]$ and if ϕ is an automorphism of E leaving every element of F fixed, prove that ϕ must take a root of $f(x)$ in E into a root of $f(x)$ in E.*

Solution. We are given that $\phi : E \to E$ is a homomorphism and

$\phi(\alpha) = \alpha \;\forall\; \alpha \in F$. ...(1)

Let $f(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \ldots + \alpha_n x^n \in F[x]$, $\alpha_i \in F$.

Let $a \in E$ be a root of $F[x]$. Then

$$\alpha_0 + \alpha_1 a + \alpha_2 a^2 + \ldots + \alpha_n a^n = 0.$$

$$\therefore \quad \phi(\alpha_0 + \alpha_1 a + \alpha_2 a^2 + \ldots + \alpha_n a^n) = \phi(0)$$

or $$\phi(\alpha_0) + \phi(\alpha_1)\phi(a) + \phi(\alpha_2)\phi(a^2) + \ldots + \phi(\alpha_n)\phi(a^n) = 0,$$

ϕ is a homomorphism

Clearly, α is a root of $\dfrac{x^p-1}{x-1} = x^{p-1} + x^{p-2} + \ldots + x^2 + x + 1$.

By Eisenstein Criterion, $1 + x + x^2 + \ldots + x^{p-1}$ (p a prime) is an irreducible polynomial over $\mathbf{Q}$ of degree $p-1$, which is satisfied by α.

[See Example 3.4.5., Chapter 3]

Hence $[\mathbf{Q}(\alpha) : \mathbf{Q}] = p - 1$.

Example 4.4.15. *Determine the degree of the splitting field of the polynomial $x^5 - 1$ over the field of rational numbers.* [D.U., 1997]

Hint. Take $p = 5$ in Example 4.4.14.

$\mathbf{Q}(e^{2\pi i/5})$ is the splitting field of $x^5 - 1$ over $\mathbf{Q}$.

and $[\mathbf{Q}(e^{2\pi i/5}) : \mathbf{Q}] = 5 - 1 = 4$.

Example 4.4.16. *Determine the splitting field of $x^4 + x^2 + 1$ over $\mathbf{Q}$. Also find its degree over $\mathbf{Q}$.*

Solution. If $w^3 = 1$, then $w^2 + w + 1 = 0$ or $w^4 + w^3 + w^2 = 0$ or $w^4 + w^2 + 1 = 0 \Rightarrow w$ is a root of $x^4 + x^2 + 1 = 0 \Rightarrow -w$ is also a root of $x^4 + x^2 + 1$ (since w is a complex root).

We have $x^4 + x^2 + 1 = (x^2 - w^2)(x^2 - w)$, since $w^3 = 1$, $w + w^2 = -1$

$= (x^2 - w^2)(x^2 - w^4)$, since $w^4 = w$

$= (x - w)(x + w)(x - w^2)(x + w^2)$.

Thus the four roots of $x^4 + x^2 + 1$ are $\pm w, \pm w^2$. The smallest field containing $\mathbf{Q}$ and these four roots is $\mathbf{Q}(w)$.

Hence $\mathbf{Q}(w)$ or $\mathbf{Q}(\sqrt{3}\, i)$ is the splitting field of $x^4 + x^2 + 1$ over $\mathbf{Q}$ and

$$[\mathbf{Q}(w) : \mathbf{Q}] = [\mathbf{Q}(\sqrt{3}\, i) : \mathbf{Q}] = 2,$$

since $x^2 + 3 \in \mathbf{Q}[x]$ is the irreducible polynomial of lowest degree 2 over $\mathbf{Q}$, which is satisfied by $\sqrt{3}\, i$.

Example 4.4.17. *If E is an extension of F and $f(x) \in F[x]$ and if ϕ is an automorphism of E leaving every element of F fixed, prove that ϕ must take a root of $f(x)$ in E into a root of $f(x)$ in E.*

Solution. We are given that $\phi : E \to E$ is a homomorphism and

$\phi(\alpha) = \alpha \;\forall\; \alpha \in F$. ...(1)

Let $f(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \ldots + \alpha_n x^n \in F[x]$, $\alpha_i \in F$.

Let $a \in E$ be a root of $F[x]$. Then

$$\alpha_0 + \alpha_1 a + \alpha_2 a^2 + \ldots + \alpha_n a^n = 0.$$

$\therefore$ $\phi(\alpha_0 + \alpha_1 a + \alpha_2 a^2 + \ldots + \alpha_n a^n) = \phi(0)$

or $\phi(\alpha_0) + \phi(\alpha_1)\phi(a) + \phi(\alpha_2)\phi(a^2) + \ldots + \phi(\alpha_n)\phi(a^n) = 0$, since ϕ is a homomorphism

or $\alpha_0 + \alpha_1 \phi(a) + \alpha_2 \{\phi(a)\}^2 + \ldots + \alpha_n \{\phi(a)\}^n = 0$, using (1) and ϕ is a homomorphism.

This shows that $\phi(a) \in E$ is a root of $f(x)$. Hence ϕ takes a root of $f(x)$ in E into a root of $f(x)$ in E.

Example 4.4.18. *If a complex number α is a root of the polynomial $P(x)$ with real coefficients, then its complex conjugate $\bar{\alpha}$, is also a root of $P(x)$.*

Solution. Let **C** and **R** denote the fields of complex and real numbers, respectively. Then **C** is an extension of **R**. The mapping

$$\phi : \mathbf{C} \to \mathbf{C} \text{ defined as } \phi(\alpha) = \bar{\alpha} \ \forall \ \alpha \in \mathbf{C}$$

is an automorphism of **C**, which leaves every element of **R** fixed ($\because \phi(a) = \bar{a} = a$ for all $a \in \mathbf{R}$). By Example 4.4.17, if $\alpha \in \mathbf{C}$ is a root of $p(x) \in \mathbf{R}[x]$, then $\phi(\alpha) \in \mathbf{C}$ is also a root of $p(x)$. Hence $\bar{\alpha}$ is also a root of $p(x)$.

EXERCISES

1. Find the splitting fields and their degrees of the following polynomials over **Q** :

(*i*) $x^2 - 4$ [Ans. Q, 1]

(*ii*) $x^2 + 4$ [Ans. Q (*i*), 2]

(*iii*) $x^4 - x^2 - 2$ [Ans. Q ($\sqrt{2}$, *i*), 4]

(*iv*) $x^6 - 1$ [Ans. Q ($\sqrt{3}$ *i*), 2]

(*v*) $x^3 - 1$ [Ans. Q ($\sqrt{3}$ *i*), 2]

(*vi*) $x^7 - 1$ [Ans. Q ($e^{2\pi i/7}$), 6]

[**Hint.** Take $p = 7$ in Example 4.4.14]

2. Find a suitable number a such that :

(*i*) $\mathbf{Q}(\sqrt{2}, \sqrt{5}) = \mathbf{Q}(a)$, (*ii*) $\mathbf{Q}(\sqrt{3}, i) = \mathbf{Q}(a)$

[**Ans.** (i) $a = \sqrt{2} + \sqrt{5}$, (ii) $a = \sqrt{3} + i$]

3. Let **Q** denote the field of rational numbers, $K = \mathbf{Q}(\sqrt{5})$, $L = K(\sqrt{7})$. Prove that $[L : K] = 2$ and $[K : \mathbf{Q}] = 2$. What do you conclude about $[L : \mathbf{Q}]$? [**Ans.** $[L : \mathbf{Q}] = 4$]

4. Show that the splitting field of $x^6 - 1$ over **Q** is same as that of $x^4 + x^2 + 1$ over **Q** and that its degree over **Q** is 2.

[**Hint.** See Example 4.4.16 and Ex. 1 (*iv*) above.]

5. Let m be a positive integer, which is not a perfect square. If $(\alpha + \beta\sqrt{m})$, where α and β are rationals be a root of polynomial $f(x)$ having rational coefficients, then $\alpha - \beta\sqrt{m}$ is also a root of $f(x)$.

[**Hint.** Refer to Example 4.4.17. Let $K = \{a + b\sqrt{m} : a, b \in \mathbf{Q}\}$. Then K is a field under usual addition and multiplication and further K is an extension of **Q**. The mapping $\phi : K \to K$ defined by $\phi(a + b\sqrt{m}) = a - b\sqrt{m}$ is an automorphism of K and further $\phi(a) = a$ $\forall$ $a \in \mathbf{Q}$. By Example 4.4.17, if $a + b\sqrt{m} \in K$ is a root of $f(x) \in \mathbf{Q}[x]$, then $\phi(a + b\sqrt{m}) = a - b\sqrt{m}$ is also a root of $f(x)$ in K.]

4.5 Constructions by Ruler and Compass

The theory of field extensions helps us to solve many of the ancient geometric problems such as :

1. Can we construct by ruler and compass a cube having twice the volume of a given cube ?
2. Can we trisect a given angle by ruler and compass ?
3. Can we construct by ruler and compass a regular polygon having n sides ?

Using the techniques of field extensions discussed earlier in the chapter, we shall prove that (*i*) *it is impossible to trisect an angle of* $60°$ *by ruler and compass*, (*ii*) *it is impossible to construct a regular septagon by ruler and compass*, (*iii*) *it is impossible to duplicate a given cube by ruler and compass etc. etc.*.

Definition. (Constructible Number)

A real number α *is said to be a* **constructible number**, *if we can construct a line segment of length* $|\alpha|$ *by using ruler and compass alone, when we are given some fundamental unit length.*

Remark. *All rational numbers are constructible.*

If the unit length is OA, then a positive rational number m/n is m times the nth part of OA (obtained by ruler and compass) and so m/n is constructible etc.

We can do the following constructions by using ruler and compass alone :

(*i*) Draw a line joining two points.

(*ii*) Draw a line perpendicular to a given line.

(*iii*) Draw a line parallel to a given line.

Theorem 4.5.1. *If* α *and* β *are constructible numbers, then so are* $\alpha+\beta$, $\alpha-\beta$, $\alpha\beta$ *and* α/β (*when* $\beta \neq 0$).

Proof. Since α and β are constructible, we can construct line segments of lengths $|\alpha|$ and $|\beta|$.

Firstly, we show $\alpha+\beta$ *and* $\alpha-\beta$ *are constructible.*

Let $\alpha > 0$ and $\beta > 0$, so that $|\alpha| = \alpha$ and $|\beta| = \beta$. Let AB be the line segment of length α. With the help of compass, mark a point C (along the extended line AB) such that $BC = \beta$. Then AC is the line segment of length $\alpha+\beta$ and so $\alpha+\beta$ is constructible. In order to construct $\alpha-\beta$, we construct a line segment AB (with the ruler) of length equal to the maximum of α and β. With A as centre, measure off length AC (with compass and along AB) equal to the minimum of α and β. Then CB is the line segment of length $|\alpha-\beta|$ and so $\alpha-\beta$ is constructible.

Let $\alpha > 0$ and $\beta < 0$. We take $\beta = -\gamma$, $\gamma > 0$. Since α and β are constructible, so are α and γ. As proved above, $\alpha+\gamma$ and $\alpha-\gamma$ are constructible i.e., $\alpha-\beta$ and $\alpha+\beta$ are constructible.

Let $\alpha < 0$ and $\beta > 0$. The result follows on the similar lines.

Let $\alpha < 0$ and $\beta < 0$. We take $\alpha = -\gamma$ and $\beta = -\delta$; $\gamma > 0$ and $\delta > 0$.

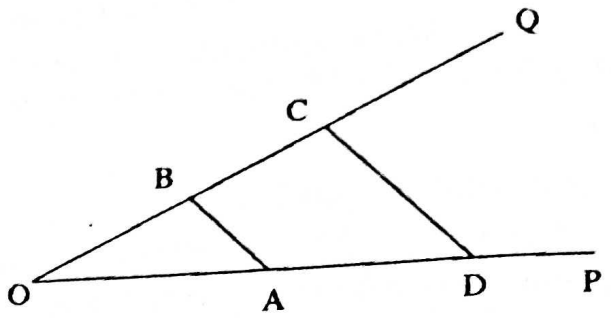
Then $\delta + \gamma$ and $\delta - \gamma$ are constructible. We have

$$|\delta + \gamma| = 1 - (\alpha + \beta)| = |\alpha + \beta|, |\delta - \gamma| = |\alpha - \beta|.$$

Thus $\alpha + \beta$ and $\alpha - \beta$ are constructible.

Now we proceed to show that $\alpha\beta$ is constructible.

With the help of ruler, draw a line OP and construct the line segment OA of length $|\alpha|$. We draw another line OQ through O but not containing OP.



With the help of compass, mark two points B and C on the line OQ such that $OB = 1$ and $OC = |\beta|$. With the help of ruler and compass, join BA and draw the line segment CD parallel to BA.

From similar triangles OAB and ODC, we obtain

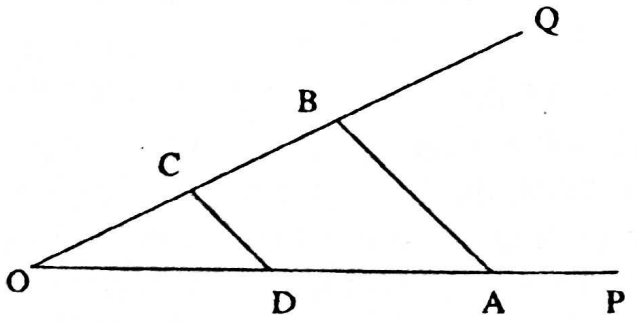
$$\frac{OB}{OA} = \frac{OC}{OD} \quad \text{or} \quad \frac{1}{|\alpha|} = \frac{|\beta|}{OD} \quad \text{or} \quad OD = |\alpha||\beta| = |\alpha\beta|.$$

Hence $\alpha\beta$ is constructible, if α and β are so.

Finally, we show that α/β ($\beta \neq 0$) is constructible.

As explained above, with the help of ruler and compass we can make another diagram in which

$$OA = |\alpha|, OB = |\beta| \text{ and } OC = 1.$$



From similar triangles OAB and ODC, we obtain

$$\frac{OD}{OC} = \frac{OA}{OB} \text{ or } \frac{OD}{1} = \frac{|\alpha|}{|\beta|} = \left|\frac{\alpha}{\beta}\right|$$

$$\therefore \quad OD = \left|\frac{\alpha}{\beta}\right|.$$

Hence α/β is constructible, if α and β are so and $\beta \neq 0$.

Corollary. *The set W of all constructible numbers form a subfield of the field* **R** *of real numbers.*

Remark. Since the field **Q** of rational numbers is the smallest field of **R**, $\mathbf{Q} \subseteq W$.

In the following theorem, we shall prove that any constructible number can be obtained from the rational field **Q** by a *finite* number of constructions.

Theorem 4.5.2. *A real number* α *is constructible if and only if there exist finite number of real numbers* $\lambda_1, \lambda_2, \ldots, \lambda_n$ *such that*

$$\lambda_1^2 \in \mathbf{Q},\ \lambda_2^2 \in \mathbf{Q}(\lambda_1),\ \lambda_3^2 \in \mathbf{Q}(\lambda_1, \lambda_2),\ \ldots,\ \lambda_n^2 \in \mathbf{Q}(\lambda_1, \lambda_2, \ldots, \lambda_{n-1})$$

and

$$\alpha \in \mathbf{Q}(\lambda_1, \lambda_2, \ldots, \lambda_n).$$

Proof. The set $\mathbf{Q} \times \mathbf{Q} = \{(x, y) : x, y \in \mathbf{Q}\}$ is called the *plane of* **Q**. Any straight line joining two points in the plane of **Q** has an equation of the form : $ax + by + c = 0$, where $a, b, c \in \mathbf{Q}$. Any circle having as centre a point in the plane of **Q** and having radius an element of **Q** has an equation of the form : $x^2 + y^2 + gx + fy + h = 0$; where $g, f, h \in \mathbf{Q}$.

We call these lines and circles as *lines and circles in* **Q**.

A point in a plane can be located by using ruler and compass in one of the following three ways :

(*i*) as an intersection of two straight lines

(*ii*) as an intersection of a line and a circle

(*iii*) as an intersection of two circles.

Case I. Consider two non-parallel straight lines in the plane of **Q** :

$$a_1x + b_1y + c_1 = 0,\ a_2x + b_2y + c_2 = 0\ ;\ a_i, b_i, c_i \in \mathbf{Q}.$$

These lines intersect in the point

$$\left(\frac{b_1 c_2 - b_2 c_1}{a_1 b_2 - a_2 b_1}, \frac{a_2 c_1 - a_1 c_2}{a_1 b_2 - a_2 c_1}\right),$$ which lies in the plane of **Q**.

Case II. Consider a line and a circle in **Q** having equations :

$$ax + by + c = 0,\ a, b, c \in \mathbf{Q}\ (a \neq 0)$$

$$x^2 + y^2 + gx + fy + h = 0,\ g, f, h \in \mathbf{Q}.$$

Eliminating x between these equations, we get

$$\left(\frac{by + c}{a}\right)^2 + y^2 - \frac{g}{a}(by + c) + fy + h = 0$$

or $$y^2\left(\frac{b^2}{a^2} + 1\right) + y\left(\frac{2bc}{a^2} - \frac{bg}{a} + f\right) + \left(\frac{c^2}{a^2} - \frac{gc}{a} + h\right) = 0.$$

Writing this equation as $\alpha y^2 + \beta y + \gamma = 0$ and solving for y, we get

$$y = \frac{-\beta \pm \sqrt{\beta^2 - 4\alpha\gamma}}{2\alpha},\ \alpha = \frac{b^2}{a^2} + 1 \text{ etc. and } \beta^2 - 4\alpha\gamma \geq 0.$$

Putting these values of y in $x = -\frac{1}{a}(by + c)$, we get

$$x = -\frac{b}{a}\left[\frac{-\beta \pm \sqrt{\beta^2 - 4\alpha\gamma}}{2\alpha}\right] - \frac{c}{a}.$$

If we take $\lambda_1 = \sqrt{\beta^2 - 4\alpha\gamma}$, then $\lambda_1^2 \in \mathbf{Q}$.

From the above values of x and y, we conclude that a line and a circle in $\mathbf{Q}$ intersect in a point in the plane of $\mathbf{Q}$ or in the plane of $\mathbf{Q}(\lambda_1)$, where $\lambda_1^2 \in \mathbf{Q}$.

Case III. Consider two circles in $\mathbf{Q}$ having equations :

$$x^2 + y^2 + g_1 x + f_1 y + h_1 = 0$$

$$x^2 + y^2 + g_2 x + f_2 y + h_2 = 0, \quad \text{where} \quad g_i, f_i, h_i \in \mathbf{Q}.$$

The line passing through their points of intersection is

$$(g_1 - g_2)\, x + (f_1 - f_2)\, y + h_1 - h_2 = 0. \qquad \ldots(1)$$

Thus the points of intersection of the two circles are the same as the points of intersection of either of the circles and the line (1). Consequently, this case reduces to case II.

Hence the lines and circles in $\mathbf{Q}$ give us points either in $\mathbf{Q}$ or in some quadratic extension of $\mathbf{Q}$ *viz.*, $\mathbf{Q}(\lambda_1)$, for $\lambda_1^2 \in \mathbf{Q}$.

Similarly, lines and circles in $\mathbf{Q}(\lambda_1)$ intersect in points in the plane $\mathbf{Q}(\lambda_1, \lambda_2)$, where $\lambda_2^2 \in \mathbf{Q}(\lambda_1)$ and so on. Hence it follows that a real number α is constructible, if there exist real numbers $\lambda_1, \lambda_2, \ldots, \lambda_n$ such that $\lambda_1^2 \in \mathbf{Q}$, $\lambda_2^2 \in \mathbf{Q}(\lambda_1)$, $\lambda_3^2 \in \mathbf{Q}(\lambda_1, \lambda_2), \ldots,$ $\lambda_n^2 \in \mathbf{Q}(\lambda_1, \lambda_2, \ldots, \lambda_{n-1})$ and $\alpha \in \mathbf{Q}(\lambda_1, \lambda_2, \ldots, \lambda_n)$.

Now we shall prove the *only* if part.

Suppose that α is a real number such that

$$\lambda_1^2 \in \mathbf{Q},\ \lambda_i^2 \in \mathbf{Q}(\lambda_1, \lambda_2, \ldots, \lambda_{i-1}) \quad \text{for} \quad i = 1, 2, \ldots, n$$

and $\alpha \in \mathbf{Q}(\lambda_1, \lambda_2, \ldots, \lambda_n)$; $\lambda_1, \lambda_2, \ldots, \lambda_n$ being real numbers.

Let W be the field of all constructible numbers. We prove by induction on i that $F_i \subseteq W$, $0 \le i \le n$; where

$$F_i = \mathbf{Q}(\lambda_1, \lambda_2, \ldots, \lambda_i) \text{ and } F_0 = \mathbf{Q}.$$

It is clear that $F_0 = \mathbf{Q} \subseteq W$. [See Remark of Theorem 4.5.1].

Suppose $F_i \subseteq W$, for some i.

Now $F_{i+1} = F_i(\lambda_{i+1})$, for some $\lambda_{i+1} \in F_{i+1}$. If $F_i = F_{i+1}$, obviously $F_{i+1} \subseteq W$. If $F_i \neq F_{i+1}$, then $\lambda_{i+1}^2 \in F_i$ (by the given hypothesis) *i.e.*, λ_{i+1}^2 is quadratic over F_i and $F_i \subseteq W$ (by induction hypothesis). Since every root of a quadratic over W is in W, $\lambda_{i+1}^2 \in W$.

$$\therefore \quad F_i(\lambda_{i+1}) \subseteq W \Rightarrow F_{i+1} \subseteq W.$$

Hence, by induction, $F_i \subseteq W$ for all i.

In particular, $F_n \subseteq W$ and so $\alpha \in F_n \Rightarrow \alpha \in W$.

Hence α is constructible.

Theorem 4.5.3. *If a real number α is constructible, then α lies in some extension field K of $\mathbf{Q}$ such that $[K : \mathbf{Q}] = 2^r$, for some non-negative integer r.*

Proof. If α is a rational number, then $\alpha \in \mathbf{Q}$ and $[\mathbf{Q} : \mathbf{Q}] = 1 = 2^0$.

Let α be a real number such that $\alpha \notin \mathbf{Q}$. By Theorem 4.5.2, there exist a finite number of real numbers $\lambda_1, \lambda_2, \ldots, \lambda_n$ such that $\lambda_1^2 \in \mathbf{Q}$, $\lambda_2^2 \in \mathbf{Q}(\lambda_1), \ldots, \lambda_n^2 \in \mathbf{Q}(\lambda_1, \lambda_2, \ldots, \lambda_{n-1})$ and $\alpha \in \mathbf{Q}(\lambda_1, \lambda_2, \ldots, \lambda_n)$.

We have $[\mathbf{Q}(\lambda_1) : \mathbf{Q}] = 1$ or 2, according as $\lambda_1 \in \mathbf{Q}$ or $\lambda_1 \notin \mathbf{Q}$

and $[\mathbf{Q}(\lambda_1, \lambda_2, \ldots, \lambda_i) : \mathbf{Q}(\lambda_1, \lambda_2, \ldots, \lambda_{i-1})] = 1$ or 2 ; for $i = 1, 2, \ldots, n$. ...(1)

Hence α lies in the extension field $K = \mathbf{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ such that

$$[K : \mathbf{Q}] = [\mathbf{Q}(\lambda_1, \lambda_2, \ldots, \lambda_n) : \mathbf{Q}]$$

or
$$[K : \mathbf{Q}] = [\mathbf{Q}(\lambda_1, \lambda_2, \ldots, \lambda_n) : \mathbf{Q}(\lambda_1, \lambda_2, \ldots, \lambda_{n-1})] \times [\mathbf{Q}(\lambda_1, \lambda_2, \ldots, \lambda_{n-1}) : \mathbf{Q}(\lambda_1, \lambda_2, \ldots, \lambda_{n-2})] \ldots [\mathbf{Q}(\lambda_1, \lambda_2) : \mathbf{Q}(\lambda_1)] [\mathbf{Q}(\lambda_1) : \mathbf{Q}] \quad \ldots(2)$$

From (1) and (2), we obtain

$[K : \mathbf{Q}] = 2^r$, where r is some non-negative integer.

Now we prove an important theorem which gives us a sufficient condition for a real number to be non-constructible.

Theorem 4.5.4. *If a real number α satisfies an irreducible polynomial of degree n over the rationals, and if n is not a power of 2, then α is not constructible.*

Proof. Since α satisfies an irreducible polynomial of degree n over $\mathbf{Q}$, $[\mathbf{Q}(\alpha) : \mathbf{Q}] = n$. Let, if possible, α be constructible. By Theorem 4.5.3, there exists an extension field K of $\mathbf{Q}$ such that $\alpha \in K$ and $[K : \mathbf{Q}] = 2^r$, for some non-negative integer r. We know $\mathbf{Q}(\alpha)$ is the smallest field containing $\mathbf{Q}$ and α. Thus $\mathbf{Q}(\alpha)$ is a subfield of K which contains $\mathbf{Q}$. By Cor. 1 of Theorem 4.1.1, $[\mathbf{Q}(\alpha) : \mathbf{Q}]$ divides $[K : \mathbf{Q}] = 2^r$. Consequently, $[\mathbf{Q}(\alpha) : \mathbf{Q}]$ is a power of 2 *i.e.*, n is a power of 2, which is contrary to the given hypothesis. Hence α is not constructible.

Definitions.

1. *A* **line segment** *is said to be* **constructible**, *if its end-points are constructible.*
2. *A* **polygon** *is said to be* **constructible**, *if each of its sides is constructible.*
3. *An* **angle** *of α radians is said to be* **constructible**, *if the point $(\cos \alpha, \sin \alpha)$ is constructible.*

Remark. *An angle of α radians is constructible if and only if the real number $\cos\alpha$ ($\sin\alpha$) is constructible.*

For the proof, see Example 4.5.3.

EXAMPLES

Example 4.5.1. *Show that the real number $\sqrt[3]{2}$ is not constructible.*

Solution. $\alpha = \sqrt[3]{2}$ satisfies an irreducible polynomial $x^3 - 2$ over $\mathbf{Q}$ of degree 3 and since 3 is not a power of 2, $\alpha = \sqrt[3]{2}$ is not constructible (Theorem 4.5.4).

Example 4.5.2. *For any constructible positive number α, show that $\pm\sqrt{\alpha}$ are constructible.*

Solution. The circle with diameter joining the points $(-\alpha, 0)$ and $(1, 0)$ is constructible. The equation of this circle is

$$(x+\alpha)(x-1)+(y-0)(y-0)=0$$

or

$$x^2+y^2+(\alpha-1)x-\alpha=0.$$

This circle and the line $x=0$ intersect in the points $(0, \pm\sqrt{\alpha})$. Hence $\pm\sqrt{\alpha}$ are constructible.

Remark. Since all integers are constructible, it follows that $\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}$ etc. are all constructible numbers.

Example 4.5.3. *Prove that an angle of α radians is constructible if and only if the real number $\cos\alpha$ ($\sin\alpha$) is constructible.*

Solution. Since α is constructible, by definition, $(\cos\alpha, \sin\alpha)$ is a constructible point. The constructible circle $(x-\cos\alpha)^2+(y-\sin\alpha)^2=1$ and the constructible line $y=0$ intersect in the constructible points $(2\cos\alpha, 0)$ and $(0, 0)$. Thus $2\cos\alpha$ is a constructible number and since 2 is a constructible number, $2\cos\alpha/2$ *i.e.*, $\cos\alpha$ is a constructible number.

Conversely, let $\cos\alpha$ be a constructible number. Then $\sin\alpha = \sqrt{1-\cos^2\alpha}$ is a constructible number. Consequently, the lines $x=\cos\alpha$ and $y=\sin\alpha$ are constructible lines, which intersect in the point $(\cos\alpha, \sin\alpha)$. Hence an angle of α radians is constructible.

Example 4.5.4. *Show that it is impossible to duplicate the cube by use of straightedge and compass.* [D.U., 2000]

Solution. Duplicating a cube means constructing a cube whose volume is twice that of the given cube. We may assume that the side of the given cube is of unit length and so the volume of the given cube is 1 cu. unit. We have to show that it is impossible to construct the side of a cube (by straightedge and compass) whose volume is 2 cu. units. Suppose there exists a cube of side α such that $\alpha^3 = 2$. Then $\alpha = 2^{1/3}$ satisfies an irreducible polynomial $x^3 - 2$ over $\mathbf{Q}$ of degree 3. Since 3 is not a power of 2, $\alpha = 2^{1/3}$ is not constructible. Hence it is impossible to construct a cube of side $\alpha = 2^{1/3}$.

DELHI UNIVERSITY EXAMINATION PAPERS
B.A./B.Sc. (Hons.)/III–2001
MATHEMATICS – Unit XII
(Algebra—III)

Time : 2 hours *Maximum Marks : 50*

Attempt any one question from each Section.

Section I

1. (*a*) If R is a division ring, show that $\{0\}$ and R are only ideals of R. Is the converse true ? Justify your answer.

   (*b*) Let R be a ring with unity. Show that no proper ideal of R can contain an invertible element of R. Hence prove that a field F has no proper ideals.

   (*c*) Show that $2x = 0$ for all $x \in R$, where R is a Boolean ring.

2. (*a*) Find all nilpotent elements of $\frac{Z}{<70>}$, where Z denotes the ring of integers.

   (*b*) Define characteristic of ring R. Assume R is an integral domain and $na = 0$ for some non-zero $a \in R$ and a non-zero integer n. Show that R has a finite characteritic. What is the relation between the characteristic of D and number n ?

   (*c*) Let R be a ring with unit 1. Show that : $(-1)(-1) = 1$.

Section II

3. (*a*) Consider the ring R of all the real-valued continuous functions on a closed unit interval.

   Let $M = \{ f : f \in R \text{ and } f(\frac{1}{5}) = 0 \}$. Show that M is a maximal ideal of R.

   (*b*) Show that $\frac{Z}{<2>}$ is isomorphic to $\frac{5Z}{10Z}$, where Z denotes the ring of integers.

   (*c*) Show that $\ker f = \{0\}$ if and only if f is an isomorphism, where $f : R \to S$ is a homomorphism of a ring R onto a ring S.

4. (*a*) Let D be an integral domain and $a, b \in D$. Suppose $a^n = b^n$ and $a^m = b^m$ for any two relatively prime positive integers m and n. Prove that $a = b$.

   (*b*) Consider the ideal generated by x in $Z[x]$, where Z denotes the ring of integers. Is it maximal ? Is it prime ? Justify your answer.

   (*c*) Prove that in a Principal Integral Domain an element is prime if and only if it is irreducible.

Section III

5. (*a*) Prove that product of two primitive polynomials is a primitive polynomial in $D[x]$, where D is a Unique Factorization Domain.

   (*b*) Show that $4x^2 + 6x + 2$ is not a primitive polynomial in $Z[x]$, where Z is the ring of integers. Will $4x^2 + 6x + 2$ be a primitive polynomial over $Q[x]$? Justify your answer.

   (*c*) Prove that in a Principal Integral Domain factorization of a non-zero non-unit element into irreducibles is unique upto associates.

6. (*a*) State and prove Eisenstein Criterion to decide the irreducibility of a polynomial with integer coefficients over rationals. Apply it to discuss the irreducibility of a polynomial over rationals of your choice.

   (*b*) Prove that every Euclidean ring possesses a unit element. Also show that a necessary and sufficient condition that the element a in the Euclidean ring be a unit is that $d(a) = d(1)$, where d is the valuation function of the Euclidean ring.

Section IV

7. (*a*) Let L be an algebraic extension of K and K be an algebraic extension of F. Show that L is an algebraic extension of F.

   (*b*) Obtain the splitting field and its degree over Q for

   $$f(x) = x^4 - 5x^2 + 6 \in Q[x].$$

   (*c*) Is it possible to square the circle by ruler and compass ? Justify.

8. (*a*) Prove that a polynomial of degree n over a field can have at most n roots in any extension field.

   (*b*) Show that $\sqrt{5} + \sqrt{7} \in R$ is algebraic of degree 4 over Q.

   (*b*) Prove that the regular septagon is not constructible by ruler and compass.

DELHI UNIVERSITY EXAMINATION PAPERS
B.A./B.Sc. (Hons.)/III – 2002
MATHEMATICS – Unit XII
(Algebra – III)

Time : 2 hours *Maximum Marks : 50*

Attempt any one question from each Section.

Section I

1. (*a*) R is a system satisfying all the conditions for a ring with unit element, with the possible exception of $a + b = b + a$. Prove that the system R is a ring.

   (*b*) Show that a ring is commutative if each of its elements is an idempotent. What is such a ring called ?

   (*c*) Show that a finite integral domain is a field. Give an example of an infinite integral domain which is not a field.

2. (*a*) Define characteristic of a ring. If an integral domain is of finite characteristic, then its characteristic is a prime number. Prove.

   (*b*) Define a division ring. Show that the ring of all 2×2 matrices

$$\begin{bmatrix} z_1 & z_2 \\ -\bar{z}_2 & \bar{z}_1 \end{bmatrix}$$

   where z_1 and z_2 are complex numbers is a division ring which is not a field. (The operations are usual matrix addition and multiplication).

   (*c*) Show that an ideal is always a subring. Is the converse true ? Justify your answer.

Section II

3. (*a*) Z is the ring of integers. U is the ideal consisting of ll multiples of 13. Then U is a maximal ideal of Z. Prove. If U consists of all multiples of 12, then is it a maximal ideal ? Give reasons.

   (*b*) Find the field of quotients of the integral domain $J[i] = \{a + ib : a, b \in Z\}$.

4. (*a*) R is a ring with unity ; $\phi : R \to R'$ is a homomorphism, where R' is an integral domain, such that $k_\phi \neq R$. Show that $\phi(1)$ is the unity of R'. Show by an example that we can have a homomorphism $\phi : R \to R'$ (where R is a ring with unity) such that $\phi(1)$ is not unity of R'.

   (*b*) Define a Principal Ideal Domain (PID). Show that in a PID, a non-zero ideal is prime if and only if it is maximal.

Section III

5. (*a*) Show that every Euclidean domain is a Principal Ideal Domain.

   (*b*) Find the g.c.d. in $J[i]$, the ring of Gaussian integers, of $(3+4i)$ and $(4-3i)$ and hence show that these two elements are co-prime in $J[i]$.

6. (*a*) State Einstein's criterion for irreducibility of polynomials over rationals. Hence show 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.

   (*b*) 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 factorisation domain. Prove.

Section IV

7. (*a*) Let $p(x)$ be a non-constant irreducible polynomial in $F[x]$, then there exists an extension K of F such that $[K : F] = \deg. p(x)$ and K has a root of $p(x)$. Prove.

   (*b*) Find the degree of the splitting field of $x^4 + 2$ over Q.

8. (*a*) Define $F[a]$ and $F(a)$. Prove that if $a \in K$ be algebraic over F, then :

   (*i*) $F[a] = F(a)$; and

   (*ii*) $[F(a) : F] = \deg.$ irr. (F, a).

   (*b*) Show that :

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

   (*c*) Prove that 60° cannot be trisected by ruler and compass.

B.A./B.Sc.(Hons.)/III – 2003
MATHEMATICS–Unit 12
(Algebra–III)

Time : 2 hours *Maximum Marks : 50*

All the sections/questions are compulsory.

Section I

1. (*a*) In any ring R, show that : $(-a)(-b) = ab \quad \forall \quad a, b \in R$. Also, give an example of a finite non-commutative ring.

Or

(*a*) For any prime integer p, show that the ring z_p of integers modulo p, is a field. $3\frac{1}{2}$

(*b*) If x is a non-zero element of an integral domain R such that $mx = 0$ for some positive integer m, prove that characteristic of R is finite. Also, show that characteristic of R divides m.

Or

(*b*) Show that there does not exist any integral domain having 15 elements. 5

(*c*) Let L be a left ideal of a ring R. Let :

$$I = \{x \in R \mid xa = 0 \quad \forall \quad a \in L\}.$$

Show that I is an ideal of R.

Or

(*c*) Show that the set of all nilpotent elements in a commutative ring R is an ideal of R. Also, find all the nilpotent elements of z_5, the ring of integers modulo 5. 4

Section II

2. (*a*) Let Φ be a homomorphism from a ring R to a ring R'. Show that $\Phi(R)$ is isomorphic to a quotient ring of R.

Or

(*a*) Let R be a ring with unity 1 and let Φ be a homomorphism from R into an integral domain R' such that kernel $(\Phi) \neq R$. Show that $\Phi(1)$ is unity of R'.

(*b*) Let R be an integral domain with unity. Let x be a prime element of R. Show that x is irreducible. Is the converse true if every ideal of R is a principal ideal ? Justify.

Or

(*b*) Let R be an integral domain and let F its quotient field. Let $0 \neq a \in R$. Show that the mapping $\Phi : R \to F$ defined by $\Phi(x) = [xa, a] \quad \forall \quad x \in R$ is an isomorphism of R into F. $4\frac{1}{2}$

(*c*) Let P be a prime ideal of a Boolean ring R such that $P \neq R$. Show that P is a maximal ideal of R.

Or

(*c*) Let R be a non-zero commutative ring with unity. Show that R is a field if and only if every ideal of R is a prime ideal. 4

Section III

3. (*a*) Let R be a Euclidean domain. Let a and b be non-zero elements of R. Prove that $d(ab) = d(a)$, if and only if b is invertible. 4

Or

(*a*) Let F be any field. Show that the ring $F[x, y]$, of polynomials in x and y over F, is not a principal ideal domain. 4

(*b*) Let R be an integral domain with unity. Prove that units of R and $R[x]$ are same. Hence, find units of $z_7[x]$. 4

Or

(*b*) Prove that the product of any two primitive polynomials in $R[x]$ is again a primitive polynomial in $R[x]$, where R is a unique factorization domain. 4

(*c*) State 'Eisenstein Criterion' for the irreducibility of a polynomial with integral coefficients over the field Q of rational numbers. Use it to show that the polynomial $1 + x + x^2 + x^3 + x^4$ is irreducible over Q. 4

Or

(*c*) Show that the polynomial $x^2 + x + 2$ is irreducible over the field of integers modulo 3. Use it to construct a field having 9 elements. $4\frac{1}{2}$

Section IV

4. (*a*) Is every algebraic extension finite ? Justify.

Or

(*a*) Is it possible to duplicate a cube by using straight edge and compass only ? Justify. $3\frac{1}{2}$

(*b*) Let L, K and F be fields such that L is an algebraic extension of K and K is an algebraic extension of F. Show that L is an algebraic extension of F.

Or

(*b*) Let K be an extension of a field F. Let $a \in K$ be algebraic over F. Let the degree of the minimal polynomial for a over F be m. Show that : 5

$$[F(a) : F] = m.$$

(*c*) Find the degrees of $Q(\sqrt{2}i)$ and $Q(\sqrt{2}, i)$ over Q. Also find a basis of $Q(\sqrt{2}i)$ over Q.

Or

(*c*) Find the splitting field and its degree over Q for the polynomial $x^4 + x^2 + 1$ 4

B.A./B.Sc. (Hons.)/III – 2004
MATHEMATICS – Unit 12
(Algebra – III)

Maximum Marks : 50

Time : 2 hours

Attempt one question from each Section.

SECTION I

1. (*a*) Prove that Z_p, the ring of integers modulo an integer p, is a field if and only if p is a prime integer. $4\frac{1}{2}$

(*b*) Let R be a commutative ring of characteristic p - p is a prime number. Prove that

$$(a+b)^p = a^p + b^p \text{ for all } a, b \in R. \quad 4$$

(*c*) Show that a ring is commutative if each of its elements is an idempotent. What is such a ring called ? 4

2. (*a*) Define the product of two ideals in a ring. Show that the product AB of two ideals A and B of a ring R is an ideal of R. $4\frac{1}{2}$

(*b*) Let R be a ring with unity. If R has no right ideals except (O) and R, then prove that R must be a division ring. 4

(*c*) If R is a ring without unity, show that every idempote[illegible] is a zero-divisor. If R has no nonzero nilpotent elements, prove that every idempotent of R is in the centre of R. 4

SECTION II

3. (*a*) Let R be a commutative ring. An ideal P of R is prime if and only if for two ideals A, B of R, $AB \subseteq P$ implies that $A \subseteq P$ or $B \subseteq P$. $6\frac{1}{2}$

(*b*) In a principal ideal domain, prove that an element is irreducible if and only if it is prime. 6

4. (*a*) Prove that isomorphic integral domains have isomorphic fields of quotients. Give an example to show that converse is not true. $6\frac{1}{2}$

(*b*) Let D be a principal ideal domain which is not a field. Prove that any ideal $A \neq D$ is a maximal ideal of D if and only if it is generated by an irreducible element of D. 6

SECTION III

5. (*a*) Let a and b be non-zero elements of a Euclidean domain R and d be a Euclidean function on R. If a divides b, but a is not an associate of b, then prove that $d(a) < d(b)$. 4

(*b*) Prove that $x^2 + x + 4$ is an irreducible polynomial over $\mathbf{Z}_{11}$ the field of integers modulo 11. Hence prove that $\mathbf{Z}_{11}[n]/< x^2 + x + 4 >$ is a field containing 121 elements. 4½

(*c*) Find the g.c.d. of $10 + 11i$ and $8 + i$ in $\mathbf{Z}[i]$. 4

6. (*a*) Let R be an ID with 1. Show that $R[x]/< x > \cong R$, where $< x >$ is the ideal generated by x. Deduce that R is a field if $R[x]$ is a principal ideal domain. 6½

(*b*) State Eisenstein's criterion to decide irreducibility of a polynomial with integral coefficients, over rationals. Use it to show that the polynomial $8x^3 - 8x - 1$ is irreducible over field of rationals. 4

(*c*) If R is an integral domain with 1, then prove that units of R are the only unit of $R[x]$. 2

SECTION IV

7. (*a*) Let L be an algebraic extension of a field K and K be an algebraic extension of a field F ; prove that L is also an algebraic extension of F. 6½

(*b*) Obtain the splitting field and its degree over Q, of the polynomial $x^4 + 2 \in Q[n]$. 4

(*c*) Let F be a field having q elements and if $b \in |K|_F$ is algebraic over F, prove that $b^{q^m} = b$ for some $m > 0$. 2

8. (*a*) Let K be an extension of a field F and $a \in K$ be algebraic over F. Let $p(x) \in F[x]$ be a polynomial over F of least degree such that $p(a) = 0$. Show that following :

(*i*) $p(x)$ is irreducible over F.

(*ii*) If $g(x) \in F[x]$ is such that $g(a) = 0$ then show that $p(x)$ must divide $g(x)$. 4½

(*b*) Prove that a regular 9-gen cannot be constructed by ruler and compass alone. 4

(*c*) If a is any algebraic number, prove that there exists a positive integer n such that na, is an algebraic integer. 4

B.A./B.Sc. (Hons.)/III – 2005
MATHEMATICS – Unit 12
(Algebra – III)

Maximum Marks : 50

Time : 2 Hours

Attempt one question from each Section.

Section I

1. (*a*) Define the centre of a ring. Prove that the centre of a division ring is a field. 4

(*b*) Let u be an ideal of a ring R and let $[R : u] = \{x \in R \mid rn \in u$ for every $r \in R\}$. Prove that $[R : u]$ is an ideal of R and that it contains u. $4\frac{1}{2}$

(*c*) If in a ring R with unity, $(xy)^2 = x^2 y^2$ for all $x, y \in R$, then prove that R is commutative. 4

2. (*a*) Let R be a ring having more than one element such that $aR = R$ $\forall$ $a\,(x = 0) \in R$. Prove that R is a division ring. $4\frac{1}{2}$

(*b*) If a finite field of characteristic p has q elements, then prove that $q = p^n$ for some n. 4

(*c*) Prove that the field Q of rational numbers has no proper subfield. 4

Section II

3. (*a*) If D_1 and D_2 are two isomorphic integral domains, prove that their field of quotients F_1 and F_2 are also isomorphic. Is the converse true ? 5

(*b*) If R is a ring with unity 1 and $f : R \to R'$ is a homomorphism where R' is an integral domain such that Ker $f \neq R$, then prove that $f(1)$ is unity of R'. $3\frac{1}{2}$

(*c*) In a P.I.D., prove that an element is prime iff it is irreducible. 4

4. (*a*) Find the field of quotients of $Z[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in Z\}$, where Z is the ring of integers. 4

(*b*) In the ring of integers, prove that an ideal is maximal iff it is generated by a prime number. 4

(*c*) Let R^C be the set of all real-valued continuous functions with domain [0, 1].

Let $M = \left\{ f \in R^C \mid f\left(\frac{1}{3}\right) = 0 \right\}$. $4\frac{1}{2}$

Show that M is a maximal ideal of Rc.

Section III

5. (*a*) Prove that the ideal (x) of $Z[x]$ is a prime ideal but not maximal. 4

(*b*) For every non-zero non-unit element '*a*' in a P.I.D., R, prove that $\exists$ an irreducible element p such that $p \mid a$. 4

(*c*) Find out if $x^3 + 3x + 1$ is irreducible over Q. Write an element of $\frac{Q[x]}{\langle x^3 + 3x + 1 \rangle}$. $4\frac{1}{2}$

6. (*a*) Prove that the ring of Gaussian integers $Z[i]$ is a Euclidean domain. 4

(*b*) Prove that in a PID, every non-zero proper ideal is a unique product of prime ideals. 4

(*c*) Show that $Z_5[x]$ is a UFD. Is $x^2 + 2x + 3$ reducible in $Z_5[x]$? Using this polynomial, construct a field consisting of 25 elements. $4\frac{1}{2}$

Section IV

7. (*a*) Define an algebraic extension of a field. Prove that a finite extension is an algebraic extension. Is the converse true ? Justify. $6\frac{1}{2}$

(*b*) Show that it is impossible to trisect $60°$ by ruler and compass. 6

8. (*a*) Prove that a polynomial of degree $n \geq 1$ over a field F cannot have more than n roots in any extension of F. 6

(*b*) If a and b are constructible numbers, then prove that $a \pm b$, ab, ab^{-1} $(b \neq 0)$ are constructible by ruler and compass. $6\frac{1}{2}$

B.A./B.Sc. (Hons.)/III – 2006

MATHEMATICS – Unit 12 (Algebra – II)

Maximum Marks : 38

Time : 2 Hours

Attempt one question from each Section.

Section I

1. (*a*) Prove that $\bar{z}_p$, the ring of integers modulo p is a field if and only if p is a prime number. 3

(*b*) If A and B are two left ideals of a ring R, then prove that $A \cap B$ is also a left ideal of R. What can you say about $A \cap B$, if A is a right ideal and B is a left ideal of R ? Justify. $3\frac{1}{2}$

(*c*) Prove that if A and B are two ideals of a ring R than $A + B = \langle A \cup B \rangle$ where for any subset $S \subseteq R$, $\langle S \rangle$ denotes the ideal of R generated by S. 3

2. (*a*) Let R be a ring that has no right ideals except $\{0\}$ and R. Show that either R is a division ring or R has a prime number of elements such that $ab = 0$ $\forall\ a, b \in R$. 5

(*b*) If I, J are respectively left and right ideals of a ring R, Prove that IJ is a two sided ideal of R. Is JI also an ideal of R ? $4\frac{1}{2}$

Section II

3. (*a*) State and prove the Fundamental Theorem of ring homomorphisms. Prove further that $z_n \cong z/(n)$. $5\frac{1}{2}$

(*b*) Prove that any ring R can be embedded into a ring with unity ? 4

4. (*a*) (*i*) Let R be a commutative ring, prove that an ideal P of R is prime if and only if R/P is an integral domain.

(*ii*) Prove or disprove that the sum of two prime ideals of a ring R may not be a prime ideal of R. 3, 2

(*b*) (*i*) In the ring of even integers $\langle E, +, . \rangle$, show that the ideal $H_4 = \{4n \mid n$ is an integer$\}$ is a maximal ideal of E.

(*ii*) Let $A \neq R$ be an ideal of ring R. For an element of $x \in R$, $x \notin A$ if $A + (x) = R$, prove that A is a maximal ideal of R and conversely. 2, $2\frac{1}{2}$

Section III

5. (*a*) Prove that any Euclidean Domain is a principal ideal domain. 4

(*b*) State and prove the Einstein criterion for irreducibility of polynomials over Q, the rationals. Find out if $x^3 + 3x + 1$ is irreducible over Q. $5\frac{1}{2}$

6. (*a*) Prove that if $f(x) \in z[x]$ is primitive and $f(x)$ is irreducible over z then f is irreducible over Q. $5\frac{1}{2}$

(*b*) (*i*) Find the g.c.d. of $x^4 + x^3 + 2x^2 + x + 1$ and $x^3 - 1$ in $Q[x]$. 2

(*ii*) Prove that $z[Fs]$ is an integral domain which is not a UFD. 2

Section IV

7. (*a*) Prove that if L is an algebraic extension of a field K and K is an algebraic extension of a field F then L is an algebraic extension of F. 4

(*b*) Find the degree of a minimal splitting field of $x^4 + 2$ over the field of rational numbers Q. $5\frac{1}{2}$

8. (*a*) Prove that the regular hexagon is constructible with straight edge and compass. Discuss in detail the case for a regular septagon. 6

(*b*) Prove that the real number c is constructible if $\exists$ real numbers $v_1, v_2, \ldots\ldots, v_n$ such that : $Q = F_0 \subseteq F_1 = Q(v_1) \subseteq F_2 = F_1(v_2) \subseteq \ldots\ldots, \subseteq F_n$ $= F_{n-1}(v_n) = Q(v_1, v_2, \ldots\ldots, v_n)$, $v_1^2 \in Q$, $v_i^2 \in Q(v_1, v_2, \ldots\ldots, v_{i-1})$ for all i and $c \in F_n$. $3\frac{1}{2}$

B.A./B.Sc. (Hons)/III 2007
Mathematics – Unit 12
(Algebra–III)

Time : 2 Hours *Maximum Marks : 36*

Attempt one questions from each Section

Section I

1. (*a*) If in a ring R, the equation $ax = b$, $a \neq 0$ has a solution for all $a, b \in R$, prove that R is a division ring.

   (*b*) Give an example of : 3

   (*i*) A non-commutative ring without unity.

   (*ii*) A ring R with unity having a subring with unity, which is different from the unity of R.

   (*c*) Let R be the ring of 2×2 matrices over integers. If 3

$$a = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \in R,$$

   then prove that aR is not a left ideal of R.

2. (*a*) In a ring without unity, prove that every non-zero idempotent is a zero divisor but is not nilpotent. 3½

   (*b*) Let R be a finite (non-zero) integral domain. Prove that R has finite characteristic which is prime and $O(R) = p^n$, p a prime. 3

   (*c*) Let R be a non-commutative ring with unity. Prove that $Z(R)$, the centre of R, is a subring of R. Is it an ideal ? Justify. 3½

Section II

3. (*a*) Prove that any ring can be embedded in a ring with unity. 6

   (*b*) In a PID, prove that every non-zero prime ideal is maximal. 3½

4. (*a*) Let R be the ring of matrices of the form :

$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$$

   where a and b are rational numbers. Let

$$I = \left\{ \begin{pmatrix} 0 & x \\ 0 & 0 \end{pmatrix} / x \text{ rational} \right\}.$$

   Prove that I is maximal ideal of R. 4½

   (*b*) Prove that a homomorphism of a field is either a monomorphism or a zero homomorphism. 2½

   (*c*) Show by an example that there can be a homomorphism $f : R \to R'$ such that 1 is the unity of R but $f(1)$ is not a unity of R'. 2½

Section III

5. (*a*) Find the units of $z[i]$, the ring of Gaussian Integers. 3
   (*b*) Is the polynomial $x^2 + 2x + 3$ irreducible over $z_5[x]$? Using this or otherwise construct a field containing 25 elements. 3½
   (*c*) If R is an integral domain prove that so is $R[x]$. 3
6. (*a*) Prove that a Euclidean Domain has unity. 3
   (*b*) In a PID prove that every irreducible element is prime. 3½
   (*c*) If R is an integral domain with unity, then R and $R[x]$ have the same units. 3

Section IV

7. (*a*) If L is an algebraic extension of K and K is an algebraic extension of F, then prove that L is an algebraic extension of F. Moreover, prove that $[L : F] = [L : K]\,[K : F]$, if L is a finite extension of F. 5½
   (*b*) Determine the degree of the splitting field of $x^4 - 2$. 4
8. (*a*) Is a regular septagon constructible by ruler and compass ? Justify. 3
   (*b*) Determine the degree of the splitting field of $x^6 + 1$. 4
   (*c*) Is an algebraic extension finite ? Justify. 2½

B.A./B.Sc. (Hons.)/III – 2008
MATHEMATICS – Unit XII (Algebra – III)

Time : 2 Hours *Maximum Marks : 38*

Attempt any two Parts from each Section.

Section I

1. (*a*) Let R be the ring of all 2×2 matrices over $\mathbf{Q}$, the field of rational numbers. Let $S = \left\{ \begin{pmatrix} x & x \\ x & x \end{pmatrix} : x \in Q \right\}$

   Prove that : (*i*) S is a subring of R ; (*ii*) S is a field

   Let $f : \mathbf{Q} \to S$ be defined as : $f(x) = \begin{pmatrix} x & x \\ x & x \end{pmatrix}$ 4½

   Is f an isomorphism ? Justify your answer.

   (*b*) (*i*) Define a principal ideal of a ring. Let R be a commutative ring without unity, $a \in R$. Prove that the principal ideal generated by a is :

   $\{na + ar \mid r \in R, n \text{ is an integer}\}$.

   (*ii*) Give an example of the following :

   (α) A finite non-commutative ring without unity *Or*

   (β) A ring in which an element fails to have an inverse but possesses an inverse as an element of a subring. 4½

   (*c*) (*i*) Let L be a left ideal of a ring R show that :

   $\lambda(L) = \{x \in R : xa = 0 \ \forall\ a \in L\}$ is an ideal of R.

(*ii*) Define characteristic of a ring. Let R be a ring such that $x^2 = x$ holds for all $x \in R$. Prove that the characteristic of R is non-zero and finite. 6½

Section II

2. (*a*) (*i*) Let R be a commutative ring with 1. Prove that : M is a maximal ideal, if and only if $M + \langle a \rangle = R$ for all $a \in R$, $a \notin M$, if and only if $M + N = R$ for every ideal N of R such that $N \not\subseteq M$

(*ii*) Let R be a ring with unity 1 and R' be an integral domain. If $f : R \to R'$ is a non-zero homomorphism, prove that $f(1)$ is the unity of R'. 5

(*b*) Prove that $\mathbf{Z}$ the ring of integers is a PID (Principal Ideal Domain). If $A = \langle 15 \rangle$, $B = \langle 70 \rangle$, find an integer n such that $A + B = \langle n \rangle$. Also find an expression for n in terms of 15 and 70. 5

(*c*) (*i*) Let D be an integral domain and K be a field such that : $D \subseteq K$. If $F = \{ ab^{-1} \in K \mid a, b \in D, b \neq 0 \}$. Prove that F is the field of quotients of D.

(*ii*) Prove that the fields of quotients of integral domains $2\mathbf{Z}$, $3\mathbf{Z}$ are isomorphic but $2\mathbf{Z}$ and $3\mathbf{Z}$ are not isomorphic. 5

Section III

3. (*a*) Let R be a commutative ring with 1. Prove that : $\dfrac{R[n]}{\langle n \rangle} \cong R$.

Deduce that $\langle n \rangle$ is a prime ideal but not a maximal ideal of $Z[n]$. 5

(*b*) (*i*) State Eienstein criterion of irreducibility of polynomials with integral coefficients over the field of rational numbers.

Use it to show that : $x^{p-1} + x^{p-2} + ... + 1$, where p is a prime, is irreducible over the field of rationals.

(*ii*) In $\mathbf{Z}[i]$ find the g.c.d. of $11 + 7i$, $3 + 7i$. 5

(*c*) (*i*) Let R be an integral domain with unity. If $f \in R[n]$ is a unit, then prove that f must be a unit in R.

(*ii*) Let R be a UFD (Unique Factorization Domain) and $f(x) \in R[x]$ be an irreducible element of $R[x]$. Prove that either f is an irreducible element of R or f is an irreducible primitive polynomial of $R[x]$. 5

Section IV

4. (*a*) Let $F = \{x \in \mathbf{C} : x \text{ is a algebraic over } \mathbf{Q}\}$ where $\mathbf{C}$ is the field of complex numbers, $\mathbf{Q}$ is the field of rationals. Prove that : (*i*) F is a subfield of $\mathbf{C}$ (*ii*) $[F : \mathbf{Q}]$ is not finite. 4½

(*b*) Obtain the splitting field K and its degree over $\mathbf{Q}$ of the polynomial $x^6 - 2x^4 + x^2 - 2$. Also find a basis of K over $\mathbf{Q}$. 4½

(*c*) (*i*) If α is a constructible number, prove that $\sqrt{\alpha}$ is also constructible

(*ii*) Is it possible to trisect an angle of 72° by ruler and compass ? Justify. 4½

B.A./B.Sc. (Hons.)/III – 2009
Mathematics – Unit 12 (Algebra III)

Maximum Marks : 38

Time : 2 Hours

Attempt one question from each Section.

Section I

1. (*a*) In a ring R, $x^2 = x$, $\forall x \in R$. Prove R is commutative. Give an example of such a ring. 3

(*b*) For any prime integer P, show that the ring Z_P of integers modulo P is a field. 2½

(*c*) Prove that the characteristic of a finite integral domain must be a prime number. Give example of an infinite integral domain with finite characteristic. 4

2. (*a*) U is an ideal of a ring R. If $[R : U] = \{x \in R \mid rx \in U, \text{ for every } r \in R\}$, then prove that $[R : U]$ is an ideal of R and that it contains U. 4

(*b*) Give an example of the smallest non-commutative ring. 1½

(*c*) If R is a commutative ring with unity having no ideals except $\{0\}$ and R, then prove that R is a field. 4

Section II

3. (*a*) Prove that every ring with unity can be imbedded in a ring of endomorphisms of some additive abelian group. 5

(*b*) Show that in a P.I.D. (principal ideal domain) R, a non-zero ideal $P \neq R$ is prime iff it is maximal. 4½

4. (*a*) Find the field of quotients of the integral domain $Z[i] = \{a + bi \mid a, b \in Z, i = \sqrt{-1}\}$. What is the field of quotients of a finite integral domain ? 5

(*b*) If A and B are two ideals of a ring R, then prove that : $\frac{A+B}{A} \cong \frac{B}{A \cap B}$. Hence, prove that : $\frac{Z}{2Z} \cong \frac{5Z}{10Z}$ 4½

Section III

5. (*a*) State Eienstein's criterion for irreducibility of polynomials over Q, the field of rationals. Hence, show that the polynomial $1 + x + x^2 + x^3 + x^4$ is irreducible over Q. 4½

(*b*) Prove that every Euclidean domain is a P.I.D. (Principal Ideal Domain). 5

6. (*a*) Prove that the polynomial $x^2 + x + 4$ is irreducible over F, the field of integers modulo 11. Prove directly that $f[x]/(x^2 + x + 4)$ is a field having 121 elements. 4½

(*b*) R is a U.F.D. (Unique factorization domain). Prove that every pair of non-zero elements in R have a g.c.d. (greatest common divisor). How are two g.c.d.s of a pair of non-zero elements in a UFD related ?

Section IV

7. (*a*) Find the degree of the splitting field of the polynomial $x^4 + 2$ over Q. Find a basis of this splitting field over Q.

(*b*) Prove that a regular 9-gon cannot be constructed by ruler and compass alone.

8. (*a*) If K is a finite extension of a field F and L is a finite extension of K, then prove that L is a finite extension of F and $[L : F] = [L : K]\,[K : F]$.

(*b*) Prove that it is impossible to duplicate the cube by using ruler and compass alone.

(*c*) Find the splitting field of $x^4 + 1$ over Q.

B.A./B.Sc. (Hons.)/III – 2010
MATHEMATICS – Unit 12
(Algebra – III)

Time : 2 Hours *Maximum Marks : 38*

Attempt one question from each Section.

Section I

1. (*a*) Show that an element in Z_n is a unit iff a and n are relatively prime. 4

   (*b*) Define characteristic of a ring R. If R is a non-zero finite integral domain, show that $O(R) = p^n$, where p is a prime number. 5

2. (*a*) If R is a commutative ring and $a \in R$, then show that $(a) = \{ar + na : r \in R, n \in Z\}$. 5

   (*b*) If A, B and C are ideals of a ring $R : B \subseteq A$, then show that $A \cap (B + C) = B + (A \cap C)$. 4

Section II

3. (*a*) Prove that if K is any field which contains an integral domain D, then K contains a subfield isomorphic to F, where F is the field of quotients of D. 5

   (*b*) If R^C be the set of all real-valued continuous functions with domain $[0, 1]$ and if $M = \left\{ f \in R^C : f\left(\frac{1}{2}\right) = 0 \right\}$. Show that M is a maximal ideal of R^C. 5

4. (*a*) If R is a commutative ring with unity and if every ideal of R is prime, show that R is a field. 4

   (*b*) If R is a commutative ring having an ideal I and if P is a prime ideal of I, then show that P is an ideal of R. 3

   (*c*) Show that $M = \{0, 6\}$ is a maximal ideal of the ring $R = \{0, 2, 4, 6, 8, 10\}$ mod 12. Also find the unity of R/M. 3

Section III

5. (*a*) If R is a Principal Ideal Domain which is not a field, show that an ideal $A = (a)$ is a maximal ideal in R iff a is an irreducible element. 4

   (*b*) Show that $\frac{Q[x]}{I}$, where $I = \langle x^2 - 6x + 6 \rangle$ is a field. 3

   (*c*) Show that the polynomial : $f(x) = 1 + x + x^2 + \ldots\ldots + x^{p-1}$, where p is prime is irreducible over Q. 3

6. (*a*) State and prove Einstein's irreducibility criterion. 5

   (*b*) Show that the ideal $A = \{xf(x) + 2g(x) : f(x), g(x) \in z[x]\}$ of $z[x]$ is not a principal ideal. 3

   (*c*) Show that the ideal $\langle x^2 + 1 \rangle$ is a maximal ideal in $\mathbf{R}[x]$. 2

Section IV

7. (*a*) If F is a field and K is an extension of F, prove that $a \in K$ is algebraic over F iff $F(a)$ is an algebraic extension of F.

   (*b*) Find a basis of $Q(\sqrt{2}, \sqrt{3})$ over Q.

   (*c*) Prove that a regular hexagon is constructible using ruler and compass.

8. (*a*) Prove that a polynomial of degree n over a field can have at most n roots in any extension field.

   (*b*) Find the splitting field of $x^4 + 1$ over Q.

   (*c*) Show that it is impossible to duplicate the cube by using ruler and compass.