Master of Science (Mathematics)
Semester – II
Paper Code –

THEORY OF FIELD EXTENSIONS

M.Sc. (Mathematics) (DDE)
Paper Code : Theory of Field Extensions

M. Marks = 100
Term End Examination = 80
Time = 3 Hours ***Assignment = 20***

Course Outcomes

Students would be able to:

CO1 Use diverse properties of field extensions in various areas.
CO2 Establish the connection between the concept of field extensions and Galois Theory.
CO3 Describe the concept of automorphism, monomorphism and their linear independence in field theory.
CO4 Compute the Galois group for several classical situations.
CO5 Solve polynomial equations by radicals along with the understanding of ruler and compass constructions.

Section - I

Extension of fields: Elementary properties, Simple Extensions, Algebraic and transcendental Extensions. Factorization of polynomials, Splitting fields, Algebraically closed fields, Separable extensions, Perfect fields.

Section - II

Galios theory: Automorphism of fields, Monomorphisms and their linear independence, Fixed fields, Normal extensions, Normal closure of an extension, The fundamental theorem of Galois theory, Norms and traces.

Section - III

Normal basis, Galios fields, Cyclotomic extensions, Cyclotomic polynomials, Cyclotomic extensions of rational number field, Cyclic extension, Wedderburn theorem.

Section - IV

Ruler and compasses construction, Solutions by radicals, Extension by radicals, Generic polynomial, Algebraically independent sets, Insolvability of the general polynomial of degree $n \geq 5$ by radicals.

Note : The question paper of each course will consist of **five** Sections. Each of the sections **I to IV** will contain **two** questions and the students shall be asked to attempt **one** question from each. **Section-V** shall be **compulsory** and will contain **eight** short answer type questions without any internal choice covering the entire syllabus.

Books Recommended:

1. Luther, I.S., Passi, I.B.S., Algebra, Vol. IV-Field Theory, Narosa Publishing House, 2012.
2. Stewart, I., Galios Theory, Chapman and Hall/CRC, 2004.
3. Sahai, V., Bist, V., Algebra, Narosa Publishing House, 1999.
4. Bhattacharya, P.B., Jain, S.K., Nagpaul, S.R., Basic Abstract Algebra (2nd Edition), Cambridge University Press, Indian Edition, 1997.
5. Lang, S., Algebra, 3rd edition, Addison-Wesley, 1993.
6. Adamson, I. T., Introduction to Field Theory, Cambridge University Press, 1982.
7. Herstein, I.N., Topics in Algebra, Wiley Eastern Ltd., New Delhi, 1975.

Contents

1

Extension of a Field

Structure

1.1. Introduction. In this chapter field theory is discussed in detail. The concept of minimal polynomial, degree of an extension and their relation is given. Further the results related to the order of a finite field and its multiplicative group are discussed.

1.1.1. Objective. The objective of these contents is to provide some important results to the reader like:

(i) Algebraic extension and transcendental extension.

(ii) Minimal polynomials and degree of an extension.

(iii) Splitting fields, separable and inseparable extensions.

1.1.2. Keywords. Extension of a Field, Minimal Polynomial, Splitting Fields.

1.2. Field. A non-empty set with two binary operations denoted as "+" and "*" is called a field if it is

(i) abelian group w.r.t. "+"
(ii) abelian group w.r.t. "*"
(iii) "*" is distributive over "+".

1.3. Extension of a Field. Let K and F be any two fields and $\sigma : F \to K$ be a monomorphism. Then, $F \cong \sigma(F) \subseteq K$. Then, (K, σ) is called an extension of field F. Since $F \cong \sigma(F)$ and $\sigma(F)$ is a subfield of K, so we may regard F as a subfield of K. So, if K and F are two fields such that F is a subfield of K then K is called an extension of F and we denote it by ${}^{K}\backslash_{F}$ or $K \mid F$ or I_F^K.

Note. (i) Every field is an extension of itself.

(ii) Every field is an extension of its every subfield, for example, R is a field extension of Q and C is a field extension of R.

Remark. Let $K \mid F$ be any extension. Then, F is a subfield of K. we define a mapping $\phi : F\text{x}K \to K$ by setting

$$\phi(\lambda, k) = \lambda k \text{ for all } \lambda \in F, k \in K.$$

We observe that K becomes a vector space over F under this scalar multiplication. Thus, K must have a basis and dimension over F.

1.3.1. Degree of an extension. The dimension of K as a vector space over F is called degree of $K \mid F$, that is, degree of $K \mid F$ = [K : F].

If [K : F] = n $< \infty$, then we say that K is a finite extension of F of degree n

and, if [K : F] = ∞, then we say that K is an infinite extension of F.

Note. Every field is a vector space over itself. Therefore, deg $F \mid F$ = deg $K \mid K$ = 1.

Also, we have [K : F] = 1 iff K = F and [K : F] > 1 iff $K \neq F$. [$F \subseteq K$]

1.3.2. Example. [C : R] = 2, because basis of vector space C over the field R is {1, i}, that is, every complex number can be generated by this set. Hence [C : R] = 2.

1.3.3. Transcendental Number. A number (real or complex) is said to be transcendental if it does not satisfy any polynomial over rationals, for example, π, e.Note that every transcendental number is an irrational number but converse is not true. For example, $\sqrt{2}$ is an irrational number but it is not transcendental because it satisfies the polynomial x^2-2.

1.3.4. Algebraic Number. Let $K \mid F$ be any extension. If $\alpha \in K$ and α satisfies a polynomial over F, that is, $f(\alpha) = 0$, where $f(x) = \lambda_0 + \lambda_1 x + \lambda_2 x^2 + ... + \lambda_n x^n;\ \lambda_i \in F$ .Then, α is called algebraic over F.

If α does not satisfy any polynomial over F, then α is called transcendental over F. For example, π is transcendental over set of rationals but π is not transcendental over set of reals.

Note. Every element of F is always algebraic over F.

1.3.5. Example. $R|Q$ is an infinite extension of Q, OR, [R : Q] = ∞.

Solution. We prove it by contradiction. Let, if possible, [R : Q] = n(finite).

Then, any subset of R having atleast (n+1) elements is always linearly dependent. In particular, π is a real number and we can take the set {1, π, π^2,…, π^n} of n+1 elements. Then, there exists scalars $\lambda_0, \lambda_1, \lambda_2, ..., \lambda_n \in Q$ (not all zero) such that

$$\lambda_0 + \lambda_1\pi + \lambda_2\pi^2 + ... + \lambda_n\pi^n = 0$$

Thus, π satisfies the polynomial $\lambda_0 + \lambda_1 x + \lambda_2 x^2 + ... + \lambda_n x^n$. So, π is not a transcendental number, which is a contradiction.

Hence our supposition is wrong. Therefore, [R : Q] = ∞.

1.3.6. Algebraic Extension. The extension $K|F$ is called algebraic extension if every element of K is algebraic over F. otherwise, $K|F$ is said to be transcendental extension if atleast one element is not algebraic over F.

1.3.7. Theorem. Every finite extension is an algebraic extension.

Proof. Let $K|F$ be any extension and let [K : F] = n(finite), that is, dim $K|F$ = n.

Every element of F is obviously algebraic. Now, $\alpha \in K$ be any arbitrary element. Consider the elements 1, α, α^2,…, α^n in K.

Either all these elements are distinct, if not, then $\alpha^i = \alpha^j$ for some $i \neq j$. Thus, $\alpha^i - \alpha^j = 0$.

Consider the polynomial $f(x) = x^i - x^j \in F[x]$ and $f(\alpha) = \alpha^i - \alpha^j = 0$.

Thus, α satisfies $f(x) \in F[x]$ and hence α is algebraic over F.

If 1, α, α^2,…, α^n are all distinct, then these must be linearly dependent over F. so there exists $\lambda_0, \lambda_1, \lambda_2, ..., \lambda_n \in F$ (not all zero) such that

$$\lambda_0 + \lambda_1\alpha + \lambda_2\alpha^2 + ... + \lambda_n\alpha^n = 0$$

Thus, α satisfies the polynomial $f(x) = \lambda_0 + \lambda_1 x + \lambda_2 x^2 + ... + \lambda_n x^n$. So, α is algebraic over F.

Hence every finite extension is an algebraic extension.

Remark. Converse of above theorem is not true, that is, every algebraic extension is not a finite extension. We shall give an example for this later on.

1.3.8. Exercise. If an element α satisfies one polynomial over F, then it satisfies infinitely many polynomials over F.

Proof. Let α satisfies $f(x) \in F[x]$ .Then $f(\alpha) = 0$. We define $h(x) = f(x)g(x)$ for any $g(x) \in F[x]$. Then α also satisfies $h(x)$.

1.4. Minimal Polynomial. If $p(x)$ be a polynomial over F of smallest degree satisfied by α, then $p(x)$ is called minimal polynomial of α. W.L.O.G., we can assume that leading co-efficient in $p(x)$ is 1, that is, $p(x)$ is a monic polynomial.

1.4.1. Lemma. If $p(x)\in F[x]$ be a minimal polynomial of α and $f(x)\in F[x]$ be any other polynomial such that $f(\alpha)=0$, then $p(x)/f(x)$.

Proof. Since F is a field so F[x] must be a unique factorization domain and so division algorithm hold in F[x]. therefore, there exists polynomial $q(x)$ and $r(x)$ such that $f(x)=p(x)q(x)+r(x)$ where either $r(x)=0$ or $\deg r(x)<\deg p(x)$.

Now, $f(\alpha)=0 \quad\Rightarrow\quad p(\alpha)q(\alpha)+r(\alpha)=0 \quad\Rightarrow\quad r(\alpha)=0 \qquad [\because p(\alpha)=0]$

If $r(x)\in F[x]$ is a non-zero polynomial, then it is a contradiction to minimality of $p(x)$, since $\deg r(x) < \deg p(x)$. So, we must have r(x) = 0. Thus, $f(x)=p(x)q(x)$.

Hence $p(x)/f(x)$.

1.4.2. Unique Factorization Domain. An integral domain R with unity is called unique factorization domain if

(i) Every non-zero element in R is either a unit in R or can be written as a product of finite number of irreducible elements of R.

(ii) The decomposition in (i) above is unique upto the order and the associates of irreducible elements.

Remark. Let F be any field and F[x] be a ring of polynomials over F, then division algorithm hold in F[x].

1.4.3. Corollary. Minimal polynomial of an element is unique.

Proof. Let p(x) and q(x) be two minimal polynomials of α. Since p(x) is a minimal polynomial of α, so $p(x)/q(x)$. Thus,

$$\deg p(x)<\deg q(x) \qquad \text{---(1)}$$

Also, q(x) is a minimal polynomial of α, so $q(x)/p(x)$. Thus,

$$\deg q(x)<\deg p(x) \qquad \text{---(2)}$$

By (1) and (2), degp(x) = degq(x). Hence

$$p(x)=\lambda q(x) \qquad \text{for some } \lambda\in \text{F}$$

Now, p(x) and q(x) are both monic polynomials, so comparing the co-efficients of leading terms on both sides, we get $\lambda=1$. Therefore, p(x) = q(x).

Remark. $\alpha \in$ F iff $\deg p(x) = 1$, where p(x) is minimal polynomial of α. In this case, $p(x) = x - \alpha$.

1.4.4. Irreducible Polynomial. A polynomial $f(x) \in F[x]$ is said to be irreducible over F if f(x) = g(x)h(x) for some polynomial $g(x), h(x) \in F[x]$ imply that either $\deg g(x) = 0$ or $\deg h(x) = 0$.

1.4.5. Proposition. Minimal polynomial of any element is irreducible over F.

Proof. Let, if possible, minimal polynomial p(x) of $\alpha \in$ F is reducible over F. Then, we have p(x) = q(x)t(x) for some $q(x), t(x) \in F[x]$.

Then, $0 = p(\alpha) = q(\alpha)t(\alpha) \quad \Rightarrow \quad$ either $q(\alpha)$=0 or $t(\alpha) = 0$

which is not possible because $\deg q(x) < \deg p(x)$ and $\deg t(x) < \deg p(x)$ and p(x) is an irreducible polynomial.

1.4.6. Definition. Let S be a subset of a field K, then the subfield K' of K is said to be generated by S if

(i) $S \subseteq K'$

(ii) For any subfield L of K, $S \subseteq L$ implies $K' \subseteq L$ and we denote the subfield generated by S by <S>. Essentially the subfield generated by S is the intersection of all subfields of K which contains S.

1.4.7. Definition. Let K be a field extension of F and S be any subset of K, then the subfield of K generated by $F \cup S$ is said to be the subfield of K generated by S over F and this subfield is denoted by F(S). However, if S is a finite set and its members are $a_1, a_2, ..., a_n$, then we write $F(S) = F(a_1, a_2, ..., a_n)$. Sometimes, $F(a_1, a_2, ..., a_n)$ is also called adjunction of $a_1, a_2, ..., a_n$ over F.

1.4.8. Definition. A field K is said to be finitely generated over F if there exists a finite number of elements $a_1, a_2, ..., a_n$ in K such that $K = F(a_1, a_2, ..., a_n)$.

In particular, if K is generated by a single element 'a' over F, that is, K = F(a), then K is called a **simple extension** of F.

1.4.9. Definition. Let $K \mid F$ be any field extension and let F[x] be the ring of polynomials over F. We define,

$$F[a] = \{ f(a) : f(x) \in F[x] \}$$

Let $f(a) \in F[a]$ where $f(x) = \lambda_0 + \lambda_1 x + \lambda_2 x^2 + ... + \lambda_n x^n \in F[x]$. Clearly,

$$f(a) = \lambda_0 + \lambda_1 a + \lambda_2 a^2 + ... + \lambda_n a^n \in F(a)$$

Thus, $F[a] \subseteq F(a)$.

Remark. $a_1 \in F$ iff $F(a_1) = F$.

1.4.10. Theorem. Let $K|F$ be any field extension. Then, $a \in K$ is algebraic over F iff $[F(a):F]$ is finite, that is F(a) is a finite extension over F. Moreover, $[F(a):F]=n$, where n is the degree of minimal polynomial of '*a*' over F.

Proof. Let $[F(a):F]$ is finite and let $[F(a):F]=n$. Thus, $\dim_F F(a)=n$

Now, Consider the elements 1, a, $a^2, \dots, a^n$ in F(a).

These are (n+1) distinct elements of F(a), then these must be linearly dependent over F. so there exists $\lambda_0, \lambda_1, \lambda_2, \dots, \lambda_n \in F$ (not all zero) such that

$$\lambda_0 + \lambda_1 a + \lambda_2 a^2 + \dots + \lambda_n a^n = 0$$

Thus, a satisfies the polynomial $f(x) = \lambda_0 + \lambda_1 x + \lambda_2 x^2 + \dots + \lambda_n x^n$. So, a is algebraic over F.

Hence a is algebraic over F.

Conversely, let $a \in K$ be algebraic over F.

Let $p(x) \in F[x]$ be the minimal polynomial of '*a*' over F. Further, let $\deg p(x) = n \geq 1$.

We claim that [F(a) : F] = n.

Let $p(x) = \lambda_0 + \lambda_1 x + \lambda_2 x^2 + \dots + \lambda_n x^n$, $\lambda_n \neq 0$ is the minimal polynomial of '*a*' over F, so $p(a) = 0$ and, if $g(x) \in F[x]$ is any polynomial such that $g(a) = 0$, then $p(x)|g(x)$.

Consider $t \in F[a]$. Then, t = f(a) for some $f(x) \in F[x]$.

If $t \neq 0$, then $f(a) \neq 0$, that is, f(x) is not satisfied by '*a*'. Thus, $p(x) \nmid g(x)$.

Since p(x) is irreducible in F[x] and $f(x) \in F[x]$ such that $p(x) \nmid f(x)$.

As F[x] is an Euclidean ring, so we get g.c.d.(p(x), f(x)) = 1. Therefore, there exists polynomials $h(x), g(x) \in F[x]$ such that

$$1 = f(x)g(x) + p(x)h(x)$$

Put $x = a$, $1 = f(a)g(a) + p(a)h(a) \quad \Rightarrow \quad 1 = f(a)g(a)$

Now, $g(x) \in F[x] \quad \Rightarrow \quad g(a) \in F[a] \quad \Rightarrow \quad f(a)$ is invertible .

We know that an integral domain in which every non-zero element is invertible is a field. Hence, F[a] is a field.

But we know that $F[a] \subseteq F(a)$, where F(a) is the field of quotients of F[a]. Therefore,

F[a] = F(a).

Let $t \in F[a] = F(a) \quad \Rightarrow \quad t = f(a)$ for some $f(x) \in F[x]$.

Now, $f(x) \in F[x]$ and $p(x) \in F[x]$, so by division algorithm, we can write

f(x) = p(x)q(x) + r(x) where either r(x) = 0 or deg*r*(x) < deg*p*(x).

So let $r(x) = \lambda_0^{'} + \lambda_1^{'}x + \lambda_2^{'}x^2 + ... + \lambda_{n-1}^{'}x^{n-1} \in F[x]$

Note that we are saying nothing about $\lambda_0^{'}, \lambda_1^{'}, \lambda_2^{'}, ..., \lambda_{n-1}^{'}$ which enables us to take degree of r(x) is equal to (n-1).

Then, $t = f(a) = p(a)q(a) + r(a) = r(a) = \lambda_0^{'} + \lambda_1^{'}a + \lambda_2^{'}a^2 + ... + \lambda_{n-1}^{'}a^{n-1}$

Thus, t is a linear combination of $1, a, a^2, ..., a^{n-1}$ over F. Thus, the set $\{1, a, a^2, ..., a^{n-1}\}$ generates F(a).

Let, if possible, the set $\{1, a, a^2, ..., a^{n-1}\}$ is linearly dependent.

Thus, there exists scalars $\nu_0, \nu_1, ..., \nu_{n-1} \in F$ (not all zero) such that

$$\nu_0 + \nu_1 a + \nu_2 a^2 + ... + \nu_{n-1}a^{n-1} = 0$$

That is, '*a*' satisfies a polynomial of (*n*-1) degree, which is a contradiction to minimal polynomial.

Hence $\{1, a, a^2, ..., a^{n-1}\}$ is linearly dependent and so it is a basis for F(a) over F.

Therefore, $[F(a) : F] = n < \infty$.

1.4.11. Theorem. Let K/F be a finite extension of degree n and L/K be a finite extension of degree m, then L/F is a finite extension of degree mn, that is

[L : F] = [L : K][K : F].

-OR- Prove that finite extension of a finite extension is also a finite extension.

Proof. Given that L/K be a finite extension such that [L : K] = m, that is $\dim_K L = m$.

Let $\{x_1, x_2, ..., x_m\}$ be a basis of L over K. Now, given that K/F is finite extension such that [K : F] = n, that is $\dim_F K = n$.

Let $\{y_1, y_2, ..., y_n\}$ be a basis of K over F.

Let $\alpha \in L$. Then,

$$\alpha = \alpha_1 x_1 + \alpha_2 x_2 + ... + \alpha_m x_m = \sum_{i=1}^{m} \alpha_i x_i, \qquad \alpha_i \in K$$

Now, $\alpha_i \in K$ and $\{y_1, y_2, ..., y_n\}$ be a basis of K over F, so

$$\alpha_i = \alpha_{i1}y_1 + \alpha_{i2}y_2 + ... + \alpha_{in}y_n = \sum_{j=1}^{n} \alpha_{ij}y_j, \qquad \alpha_{ij} \in F$$

Thus, $\alpha = \sum_{i=1}^{m} \alpha_i x_i = \sum_{i=1}^{m}\left(\sum_{j=1}^{n} \alpha_{ij}y_j\right)x_i = \sum_{i,j} \alpha_{ij}x_i y_j, \qquad \alpha_{ij} \in F$ and $x_i, y_j \in L$.

Therefore, $\{x_1y_1, x_1y_2, ..., x_1y_n, x_2y_1, x_2y_2, ..., x_2y_n, ..., x_my_1, x_my_2, ..., x_my_n\}$ spans L over F and have *mn* elements in number.

We claim that these *mn* elements are linearly independent over F.

If $\alpha = 0$, then

$$0 = \sum_{i,j} \alpha_{ij} x_i y_j = \sum_{i=1}^{m} \left(\sum_{j=1}^{n} \alpha_{ij} y_j \right) x_i = \sum_{i=1}^{m} \alpha_i x_i$$

Since $\alpha_i \in K$ and $\{x_1, x_2, ..., x_m\}$ are L.I. over K. Thus, $\alpha_i = 0$ for $i = 1, 2, ..., m$.

Again, since $\{y_1, y_2, ..., y_n\}$ are L.I. over F. Thus, $\alpha_{ij} = 0$ for $j = 1, 2, ..., n$.

Thus, $\alpha_{ij} = 0$ for $i = 1, 2, ..., m, j = 1, 2, ..., n$.

So $\{x_1y_1, x_1y_2, ..., x_1y_n, x_2y_1, x_2y_2, ..., x_2y_n, ..., x_my_1, x_my_2, ..., x_my_n\}$ is L.I. and hence it is basis for L over F.

Therefore, [L : F] = [L : K][K : F] = mn.

1.4.12. Proposition. If $F \subseteq E \subseteq K$ and $a \in K$ is algebraic over F, then

$$\left[E(a) : E\right] \leq \left[F(a) : F\right].$$

Proof. Let $F \subseteq E \subseteq K$ and $a \in K$ is algebraic over F. Thus, there exists a polynomial

$$f(x) = \lambda_0 + \lambda_1 x + \lambda_2 x^2 + ... + \lambda_n x^n \in F[x]$$

such that $f(a) = 0$.

Since $f(x) \in F[x]$ and $F \subseteq E \Rightarrow F[x] \subseteq E[x] \Rightarrow f[x] \in E[x]$ and $f(a) = 0$.

If p(x) is the minimal polynomial of '*a*' over F and $p_1(x)$ be minimal polynomial of '*a*' over E, then $p_1(x) \mid p(x)$, since p(x) may be reducible in E[x], that is $\deg p_1(x) \leq \deg p(x)$.

Hence $\left[E(a) : E\right] \leq \left[F(a) : F\right]$.

Remark. Let K / F be any field extension, then

$$\begin{aligned} F(a_1, a_2, ..., a_n) &= F(a_1, a_2, ..., a_{n-1})(a_n) = F(a_1, a_2, ..., a_{n-2})(a_{n-1}, a_n) \\ &= ... \\ &= F(a_1)(a_2, ..., a_{n-1}, a_n) \end{aligned}$$

1.4.13. Theorem. Let K / F be an algebraic extension and L / K is also algebraic extension, then L / F is an algebraic extension.

-OR- Prove that algebraic extension of an algebraic extension is also a algebraic extension.

Proof. To prove that L/F is algebraic extension, it is sufficient to show that every element of L is algebraic over F. Equivalently, we have to prove that if $a \in L$, then $\left[F(a):F\right] < \infty$.

Now, 'a' satisfies some polynomial f(x) over K[x], say $f(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + ... + \alpha_n x^n \in K[x]$, where $\alpha_i \in K$ for $0 \le i \le n$.

Now, $\alpha_0, \alpha_1, \alpha_2, ..., \alpha_n$ are elements of K and K/F is an algebraic extension. Thus, each α_i is algebraic over F.

Consider the element α_0. Then, α_0 is algebraic over F. Thus,

$$\left[F(\alpha_0):F\right] < \infty \quad \Rightarrow \quad \left[F_0 : F\right] < \infty, \quad \text{where } F_0 = F(\alpha_0)$$

and we have $F \subseteq F_0 \subseteq K$.

Now, $\alpha_1 \in K$ is algebraic over F. So by above remark, we have

$$\left[F_0(\alpha_1):F_0\right] \le \left[F(\alpha_1):F\right] < \infty$$

Put $F_0(\alpha_1) = F_1$, then $\left[F_1 : F_0\right] < \infty$.

So, we have $F \subseteq F_0 \subseteq F_1 \subseteq K$.

Now, consider $F_1(\alpha_2) = F_1$. Then, as discussed above, we have

$$\left[F_2 : F_1\right] \le \left[F_1(\alpha_2):F_1\right] < \infty.$$

In general similarly, we choose $F_{i-1}(\alpha_i) = F_i$, then $\left[F_i : F_{i-1}\right] < \infty$.

Then, by definition, $F_{n-1}(\alpha_n) = F_n$, then $\left[F_n : F_{n-1}\right] < \infty$.

By construction, we get that

$$F_n = F_{n-1}(\alpha_n) = F_{n-2}(\alpha_{n-1}, \alpha_n) = ... = F_0(\alpha_1, \alpha_2, ..., \alpha_n) = F(\alpha_0, \alpha_1, \alpha_2, ..., \alpha_n).$$

Now, by last theorem, we have

$$\left[F_n : F\right] = \left[F_n : F_{n-1}\right]\left[F_{n-1} : F_{n-2}\right]...\left[F_1 : F_0\right]\left[F_0 : F\right].$$

Thus, $\left[F_n : F\right]$ is finite since all the numbers on R.H.S. are finite.

Now, as $\alpha_0, \alpha_1, \alpha_2, ..., \alpha_n \in F_n$, so $f(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + ... + \alpha_n x^n \in F_n[x]$ and since $f(a) = 0$. Thus, 'a' is algebraic over F_n. So

$$\left[F_n(a):F_n\right] = \text{ degree of minimal polynomial '}a\text{' over } F_n < \infty.$$

Therefore, $\left[F_n(a):F\right] = \left[F_n(a):F_n\right]\left[F_n : F\right] < \infty$.

Thus, $F_n(a)/F$ is a finite extension. So $F_n(a)$ is algebraic extension over F. In turn, 'a' is algebraic over F.

Hence L is algebraic extension of F.

1.4.14. Theorem. Let K/F be any extension and let $S=\{x\in K: x \text{ is algebraic over } F\}$. Then, S is a subfield of K containing F and S is the largest algebraic extension of F contained in K.

Proof. Let $\alpha\in F\subseteq K$. Since α satisfies a polynomial $f(x)=x-\alpha$ in F[x], so α is algebraic over F. Thus, $\alpha\in S$ and so $F\subseteq S$. So, S is non-empty.

Let $a,b\in S$. We claim that $a-b\in S$ and if $b\neq 0$, then $ab^{-1}\in S$. Since K is a field, therefore, trivially $a-b\in K$ and if $b\neq 0$, then $ab^{-1}\in K$.

Now, to prove that $a-b\in S$ and if $b\neq 0$, then $ab^{-1}\in S$ it is sufficient to show that $a-b$ and ab^{-1} are algebraic over F. We have $a\in S$, that is, 'a' is algebraic over F. Thus, $[F(a):F]<\infty$.

Put F(a) = F_1, so $[F_1:F]<\infty$.

Also, $b\in S$, that is, 'b' is algebraic over F. Thus, $[F(b):F]<\infty$.

Now, b is algebraic over F and $F\subseteq F_1\subseteq K$. So, b is algebraic over F_1 and

$$[F_1(b):F_1]<[F(b):F]<\infty$$

Now, $[F_1(b):F]=[F_1(b):F_1][F_1:F]<\infty$. Thus, F_1(b) is finite extension of F and, thus, F(a,b) is an algebraic extension of F, as F_1(b) = F(a,b). Hence every element F(a,b) is algebraic over F.

Since $a,b\in F(a,b) \quad\Rightarrow\quad a-b\in F(a,b)$ and $ab^{-1}\in F(a,b)$.

Thus, a-b and ab^{-1} are algebraic over F.

So, $a-b, ab^{-1}\in S$ and, therefore, S is a subfield of K containing F. Hence S is an algebraic extension of F.

Let E be any other algebraic extension such that $F\subseteq E\subseteq K$. Let $\alpha\in E\subseteq K \;\Rightarrow\; \alpha\in K$. Therefore, α is algebraic over F. Thus, $\alpha\in S \;\Rightarrow\; E\subseteq S$.

So, S is the largest algebraic extension of F contained in K.

1.4.15. Corollary. If K/F is algebraic extension. Then, K = S.

Proof. In above theorem, S is a subfield of K. Therefore, $S\subseteq K$.

Also, S is the largest algebraic extension of F and K is an algebraic extension of F. Therefore, $K\subseteq S$.

Hence S = K.

Note. In above theorem, the field S is called **algebraic closure of F in K**.

1.4.16. Corollary. If K/F be any extension and $a,b\in K$ be algebraic over F. Then, $a+b, a-b, ab$ and $ab^{-1}(b\neq 0)$ are also algebraic over F.

Proof. If a and b are algebraic over F, then F(a,b) is algebraic extension of F. So, every element of F(a,b) is algebraic over F. This implies $a+b, a-b, ab$ and $ab^{-1}(b\neq 0)$ are also algebraic over F.

1.4.17 Eisenstein Criterion of Irreducibility. Let $f(x)=\alpha_0+\alpha_1 x+\alpha_2 x^2+...+\alpha_n x^n$ where $\alpha_i\in Z, \alpha_n\neq 0$. Let p be a prime number such that $p|\alpha_0, p|\alpha_1, ..., p|\alpha_{n-1}, p\nmid\alpha_n$ and $p^2\nmid\alpha_0$, then f(x) is irreducible over the rationals.

1.4.18. Counter Example. Example to show that every algebraic extension need not be finite.

Let C be the field of complex numbers and Q be the field of rationals. Then $z\in C$ is called an algebraic integer if it is algebraic over Q.

Let $E=\{z\in C : z \text{ is algebraic integer}\}$.

Then, trivially $Q\subseteq E$ and so E is a subfield of C containing Q such that E/Q is algebraic extension.

We claim that E/Q is an infinite extension.

Let, if possible, $[E:Q]=n<\infty$.

Consider the polynomial f(x) = x^{n+1}-p, where p is some prime.

Then, by Eisenstein criterion of irreducibility, f(x) is irreducible over Q. Let α be any zero of the polynomial f(x). Then, α will be a complex number such that $f(\alpha)=0$. Thus, $\alpha\in E$.

Since f(x) = x^{n+1}-p is irreducible monic polynomial satisfied by $\alpha\in E$, therefore, f(x) is minimal polynomial of α over Q. So,

$$[Q(\alpha):Q]=n+1$$

Now, $\alpha\in E$ and $Q\subseteq E$. So, $Q(\alpha)\subseteq E$, since $Q(\alpha)$ is the smallest field containing Q and α. Therefore,

$$[Q(\alpha):Q]\leq[E:Q] \quad\Rightarrow\quad n+1\leq n$$

which is a contradiction. Thus, E/Q is an infinite extension.

1.5. Factor Theorem. Let K/F be any extension and $f(x)\in F[x]$, then the element $a\in K$ is a root of polynomial f(x) iff $(x-a)|f(x)$ in K[x], that is, iff there exists some g(x) in K[x] such that f(x) = (x-a)g(x).

Proof. Let $(x-a)|f(x)$ in K[x]. Then, we have f(x) = (x-a)g(x) for some some g(x) in K[x]. Therefore,

f(a) = (a-a)g(a) = 0

Thus, ‘*a*’ is a root of f(x).

Conversely, let ‘a’ be a root of f(x) where $a \in K$.

Consider thepolynomial x-a in K[x].

Now, $f(x) \in F[x] \subseteq K[x]$. Therefore, by division algorithm in K[x], there exists unique polynomials q(x) and r(x) in K[x] such that

$$f(x) = (x-a)q(x) + r(x)$$

where either r(x) = 0 or degr(x) < deg(x-a) = 1, that is, r(x) = constant.

But f(a) = 0, implies that r(a) = 0. Thus, r(x) = 0.

Hence f(x) = (x-a)g(x). Therefore, $(x-a) \mid f(x)$ in K[x].

Note. We have earlier proved that if ‘a’ is algebraic over F, then F[a] = F(a).

1.5.1. Theorem. Let K/F be any extension and $a \in K$ is algebraic over F. Let $p(x) \in F[x]$ be the minimal polynomial of ‘a’. Then,

$$F[x]/< p(x) > \cong F[a] = F(a).$$

Proof. Consider the rings F[x] and F[a]. We define the mapping $\eta : F[x] \to F[a]$ by setting

$$\eta(f(x)) = f(a)$$

We claim that η is an onto ring homomorphism.

Let $f(x), g(x) \in F[x]$. Then,

$$\eta(f(x) + g(x)) = f(a) + g(a) = \eta(f(x)) + \eta(g(x))$$

and $$\eta(f(x)g(x)) = f(a)g(a) = \eta(f(x))\eta(g(x))$$

Thus, η is a ring homomorphism.

Again, let $\alpha \in F[a]$, then $\alpha = h(a)$ for some $h(x) \in F[x]$.

Then, $\eta(h(x)) = h(a) = \alpha$.

Thus, η is onto.

By Fundamental theorem of ring homomorphism

$$F[x]/Ker\eta \cong F[a]$$

Now, we claim that $Ker\eta =< p(x) >$.

Let $f(x) \in Ker\eta \Rightarrow \eta(f(x)) = 0 \Rightarrow f(a) = 0 \Rightarrow a$ satisfies $f(x)$.

$\Rightarrow p(x) \mid f(x)$, since p(x) is minimal polynomial.

$\Rightarrow f(x) = p(x)q(x)$, for some $q(x) \in F[x]$.

$\Rightarrow \quad f(x) = < p(x) >$.

$\Rightarrow \quad Ker\eta \subseteq < p(x) >$.

Again, let $f(x) \in < p(x) >$.

$\Rightarrow \quad f(x) = p(x)q(x)$, for some $q(x) \in F[x]$.

$\Rightarrow \quad f(a) = p(a)q(a)$.

$\Rightarrow \quad f(a) = 0$.

$\Rightarrow \quad \eta\left(f(x)\right) = 0 \quad \Rightarrow \quad f(x) \in Ker\eta$

$\Rightarrow \quad < p(x) > \subseteq Ker\eta$.

Thus, $Ker\eta = < p(x) >$ and so

$$F[x]/< p(x) > \cong F[a]$$

Since ‘a’ is algebraic over F, therefore, F[a] = F(a) and hence

$$F[x]/< p(x) > \cong F[a] = F(a).$$

Note. In the above theorem, preimage of ‘a’ is x+f(x), where $f(x) \in < p(x) >$.

Proof. $\eta\left(x + f(x)\right) = \eta\left(x + p(x)q(x)\right) = \eta(x) + \eta\left(p(x)q(x)\right) = a + p(a)q(a) = a$.

1.5.2. Conjugates. Let K/F be any extension. Two algebraic elements $a, b \in K$ are said to be conjugates over the field F if they have the same minimal polynomial, that is, we can say that all the roots of a minimal polynomial are conjugates of each other.

1.5.3. Corollary. If ‘a’ and ‘b’ are two conjugate elements of K over F, where K/F is an extension. Then, $F(a) \cong F(b)$.

Proof. Let p(x) be the minimal polynomial of ‘a’ and ‘b’ both. Then by above theorem

$$F[x]/< p(x) > \cong F[a] \text{ and } F[x]/< p(x) > \cong F[b] \quad \Rightarrow \quad F[a] \cong F[b]$$

1.5.4. Corollary . If ‘a’ and ‘b’ are any two conjugates over F, then there always exists an isomorphism $\psi : F[a] \to F[b]$ such that $\psi(a) = b$ and $\psi(\lambda) = \lambda$ for all $\lambda \in F$.

Proof. Given that ‘a’ and ‘b’ are conjugates over F, therefore, they satisfy same minimal polynomial, say p(x), over F. Then, there exists an isomorphism $\sigma_1 : F(a) \to F[x]/< p(x) >$ given by

$$\sigma_1(\lambda) = \lambda + < p(x) > \text{ and } \sigma_1(a) = x + < p(x) >. \qquad \ldots(1)$$

Further, p(x) is also minimal polynomial for ‘b’, so there exists an isomorphism $\sigma_2 : F(b) \to F[x]/< p(x) >$ given by

$$\sigma_2(\lambda) = \lambda + < p(x) > \text{ and } \sigma_2(b) = x + < p(x) >. \qquad \ldots(2)$$

Consider $F(a)\xrightarrow{\sigma_1}F[x]/<p(x)>\xrightarrow{\sigma_2^{-1}}F(b)$. Take, $\psi=\sigma_2^{-1}\sigma_1$. Then,

$$\psi(a)=\sigma_2^{-1}\sigma_1(a)=\sigma_2^{-1}(x+<p(x)>)=b$$

and $$\psi(\lambda)=\sigma_2^{-1}\sigma_1(\lambda)=\sigma_2^{-1}(\lambda+<p(x)>)=\lambda.$$

1.5.5. Definition. Let K/F be any extension and $f(x)\in F[x]$ be a non-zero polynomial. Then, 'a' is said to be a root of f(x) of multiplicity $m\geq 1$ if $(x-a)^m \mid f(x)$ but $(x-a)^{m+1}\nmid f(x)$.

1.5.6. Proposition. Let $p(x)\in F[x]$ be an irreducible polynomial over F. Then, there always exists an extension E of F which contains atleast one root of p(x) and $\left[E:F\right]=n=\deg p\left(x\right)$.

Proof. Let I = <p(x)> be an ideal of F[x]. Now, we know that a ring of polynomials over a field is a Euclidean domain and any ideal of Euclidean domain is maximal iff it is generated by some irreducible element. So, F[x] is a Euclidean domain and I = <p(x)> is a maximal ideal as p(x) is irreducible.

Now, since every Euclidean domain possess unity, therefore, F[x] is a commutative ring with unity. We further know that if R is a commutative ring with unity and M is a maximal ideal of R, then R/M is a field. So, $F[x]/<p(x)>$ is a field.

We claim that E is an extension of F.

We define a mapping $\sigma:F\to E$ by setting

$$\sigma(\lambda)=\bar{\lambda}=\lambda+I \text{ for all } \lambda\in F.$$

Then, for $\lambda_1,\lambda_2\in F$, we have

$$\sigma(\lambda_1+\lambda_2)=\lambda_1+\lambda_2+I=\left(\lambda_1+I\right)+\left(\lambda_2+I\right)=\sigma(\lambda_1)+\sigma(\lambda_2)$$

and $$\sigma(\lambda_1\lambda_2)=\lambda_1\lambda_2+I=\left(\lambda_1+I\right)\left(\lambda_2+I\right)=\sigma(\lambda_1)\sigma(\lambda_2)$$

Therefore, σ is a homomorphism.

Also, if $\sigma(\lambda_1)=\sigma(\lambda_2) \;\Rightarrow\; \lambda_1+I=\lambda_2+I \;\Rightarrow\; \lambda_1-\lambda_2+I=I=<p(x)>$

$$\Rightarrow\; \lambda_1-\lambda_2\in<p(x)> \;\Rightarrow\; p(x)\mid\lambda_1-\lambda_2 \;\Rightarrow\; \lambda_1-\lambda_2=0 \;\Rightarrow\; \lambda_1=\lambda_2$$

Therefore, σ is monomorphism.

Thus, (E, σ) is an extension of F.

Let $p\left(x\right)=\lambda_0+\lambda_1x+\lambda_2x^2+\ldots+\lambda_nx^n\in I=<p(x)>$

Consider the element $\bar{x}=x+I\in E$. Then,

$$p\left(\bar{x}\right)=\lambda_0+\lambda_1\bar{x}+\lambda_2\bar{x}^2+\ldots+\lambda_n\bar{x}^n=\lambda_0+\lambda_1x+\lambda_2x^2+\ldots+\lambda_nx^n+I=p(x)+I=I$$

Thus, p(x) has a root $\bar{x}$ in E.

We claim that $\overline{1}, \overline{x}, \overline{x}^2, ..., \overline{x}^{n-1}$ form a basis of E over F. Let us consider a representation

$$\begin{aligned}
&\lambda_0 \overline{1} + \lambda_1 \overline{x} + \lambda_2 \overline{x}^2 + ... + \lambda_{n-1} \overline{x}^{n-1} = \overline{0}, \text{ identity of E} \\
\Rightarrow\quad &\lambda_0 + \lambda_1 x + \lambda_2 x^2 + ... + \lambda_{n-1} x^{n-1} + I = I \\
\Rightarrow\quad &\lambda_0 + \lambda_1 x + \lambda_2 x^2 + ... + \lambda_{n-1} x^{n-1} \in I = < p(x) > \\
\Rightarrow\quad &p(x) \mid \lambda_0 + \lambda_1 x + \lambda_2 x^2 + ... + \lambda_{n-1} x^{n-1} \\
\Rightarrow\quad &\lambda_0 = \lambda_1 = \lambda_2 = ... = \lambda_{n-1} = 0 \qquad (\because \deg p(x) = n)
\end{aligned}$$

Thus, $\overline{1}, \overline{x}, \overline{x}^2, ..., \overline{x}^{n-1}$ are linearly independent.

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

We can write f(x) = p(x)q(x) + r(x), where either r(x) = 0 or degr(x) < degp(x).

Then,

$$\begin{aligned}
\alpha &= f(x) + I = \left[p(x)q(x) + r(x)\right] + I \\
&= \left[p(x)q(x) + I\right] + \left[r(x) + I\right] = I + r(x) + I = r(x) + I
\end{aligned}.$$

But degr(x) < n, therefore,

$$\begin{aligned}
\alpha &= r(x) + I = \gamma_0 + \gamma_1 x + \gamma_2 x^2 + ... + \gamma_{n-1} x^{n-1} + I \\
&= \gamma_0 (1 + I) + \gamma_1 (x + I) + \gamma_2 (x^2 + I) + ... + \gamma_{n-1} (x^{n-1} + I) \\
&= \gamma_0 \overline{1} + \gamma_1 \overline{x} + \gamma_2 \overline{x}^2 + ... + \gamma_{n-1} \overline{x}^{n-1}
\end{aligned}$$

Thus, $\overline{1}, \overline{x}, \overline{x}^2, ..., \overline{x}^{n-1}$ generates E and so it is a basis for E.

Hence we get [E : F] = n = degp(x).

1.5.7. Theorem. Let $f(x) \in F[x]$ be any polynomial of degree $n \geq 1$, then no extension of F contains more than n roots of f(x).

Proof. Given that $f(x) \in F[x]$ and degf(x) = n.

If n = 1, then $f(x) = \alpha x + \beta, \quad \alpha, \beta \in \mathrm{F}, \alpha \neq 0$.

Consider the element $-\beta\alpha^{-1} \in F$. Then, $f\left(-\beta\alpha^{-1}\right) = 0$. Thus, $-\beta\alpha^{-1}$ is a root of f(x).

Let K be any extension of F and let θ be any root of f(x) in K, then

$$f\left(\theta\right) = 0 \;\Rightarrow\; \alpha\theta + \beta = 0 \;\Rightarrow\; \theta = -\beta\alpha^{-1}$$

So, any extension K of F contains the only root $-\beta\alpha^{-1}$ of f(x). Therefore, K cannot contain more than one root of the polynomial f(x).

Since K was an arbitrary extension, so Theorem is true for n = 1.

Let us assume that the result is true for all polynomials of degree less than degree of f(x) over any field.

Now, let E be any extension of F. If E does not contain any root of f(x), then result is trivially true.

So, let E contain atleast one root of the polynomial f(x) say 'a'. Then, we have to prove that E does not contain more than n roots. Since $a \in E$ and 'a' is a root of f(x). suppose the multiplicity of 'a' is m. Then, by definition, we can write

$$f(x) = (x-a)^m g(x), \qquad g(x) \in E[x]$$

and $(x-a)^m \mid f(x)$ but $(x-a)^{m+1} \nmid f(x)$.

Now, $(x-a)^m \mid f(x)$, therefore, $m \le n$.

Further, $g(x) \in E[x]$ and degg(x) = n-m < n.

Therefore, by induction hypothesis, any extension of E does not contain more than n-m roots of g(x). So, E/E being an extension of E cannot contain more than n-m roots of g(x). Now, any root of g(x) is also a root of f(x) and a root of f(x) other than 'a' is also a root of g(x). Hence f(x) cannot have more than (n-m)+m, that is, n roots in any extension of F.

1.5.8. Theorem. Let $f(x) \in F[x]$ be any polynomial of degree n. Then, there exists an extension E of F containing all the roots of f(x) and $[E:F] \le n!$.

Proof. We prove the result by induction on n.

Given that $f(x) \in F[x]$ be a polynomial of degree n.

If n = 1, then $f(x) = \alpha x + \beta,\ \alpha \ne 0$, with a root $-\beta\alpha^{-1}$. Since

$$\alpha, \beta \in F \quad \Rightarrow \quad -\beta\alpha^{-1} \in F .$$

Hence F contains all the roots of the given polynomial with $[F:F] = 1 \le 1!$.

Thus, result is true for n = 1.

Let n > 1 and suppose that result is true for any polynomial of degree less that n over any field.

Then, $f(x) \in F[x]$ is either irreducible or f(x) has an irreducible factor over F. Now, let $p(x) \in F[x]$ be any irreducible factor of f(x). Then, $\deg p(x) \le \deg f(x) = n$.

Suppose that degp(x) = m. Then, $p(x) \in F[x]$ is irreducible polynomial over F with degp(x) = m. Therefore, there exists an extension E' of F containing atleast one root of p(x) and $[E':F] = m \le n$.

Let α be a root of p(x) in E', then α is also a root of f(x). So, we get that $f(x) \in F[x]$ is a polynomial with root $\alpha \in E'$ such that $[E':F] = m \le n$. Since $\alpha \in E'$ is a root of f(x) so $(x-\alpha) \mid f(x)$ in $E'[x]$.

Hence we can write $f(x) = (x-\alpha)g(x)$ where $g(x) \in E'[x]$ and degg(x) = n-1. Now, $g(x) \in E'[x]$ and degg(x) = n-1 < n.

Therefore, by induction hypothesis, there exists an extension E of E' such that E contains all the roots of g(x) and $[E:E'] \le n-1!$.

Since $\alpha \in E' \subseteq E \Rightarrow \alpha \in E$ also.

Therefore, E is an extension of F which contains all the roots of f(x). Then, we have

$[E:F]=[E:E'][E':F]\leq n-1!.m\leq n(n-1)!\leq n!.$

1.5.9. Remark. Let R and R' be any rings and $\sigma : R \to R'$ is an isomorphism onto. Consider the rings R[x] and $R'[t]$. Then, σ can be extended to an isomorphism from R[x] to $R'[t]$.

Proof. Let $f(x) \in R[x]$ and $f(x)=\lambda_0+\lambda_1 x+\lambda_2 x^2+...+\lambda_n x^n$.

We define $\bar{\sigma} : R[x] \to R'[t]$ by setting

$$\bar{\sigma}(f(x))=\sigma(\lambda_0)+\sigma(\lambda_1)t+\sigma(\lambda_2)t^2+...+\sigma(\lambda_n)t^n$$

We claim that $\bar{\sigma}$ is an extension of σ and is an isomorphism also.

Let $g(x)=\gamma_0+\gamma_1 x+\gamma_2 x^2+...+\gamma_m x^m \in R[x]$. Then, if k = max{m,n}

$$\begin{aligned}\bar{\sigma}(f(x)+g(x)) &= \sigma(\lambda_0+\gamma_0)+\sigma(\lambda_1+\gamma_1)t+\sigma(\lambda_2+\gamma_2)t^2+...+\sigma(\lambda_k+\gamma_k)t^k \\ &= \sigma(\lambda_0)+\sigma(\gamma_0)+[\sigma(\lambda_1)+\sigma(\gamma_1)]t+...+[\sigma(\lambda_k)+\sigma(\gamma_k)]t^k \\ &= \bar{\sigma}(f(x))+\bar{\sigma}(g(x))\end{aligned}$$

Similarly, we can show that

$$\bar{\sigma}(f(x)g(x))=\bar{\sigma}(f(x))\bar{\sigma}(g(x))$$

Therefore, $\bar{\sigma}$ is a ring homomorphism.

We claim that $\bar{\sigma}$ is one-one.

Let $f(x)\in \ker\bar{\sigma} \Rightarrow \bar{\sigma}(f(x))=0,$ identity of R[x]

$\Rightarrow \sigma(\lambda_0)+\sigma(\lambda_1)t+\sigma(\lambda_2)t^2+...+\sigma(\lambda_n)t^n=0 \Rightarrow \sigma(\lambda_i)=0$ for all $0\leq i\leq n$

Since σ is a monomorphism, so $\lambda_i=0$ for all $0\leq i\leq n$.

Thus, $f(x)=0 \Rightarrow \ker\bar{\sigma}=\{0\}$

Therefore, $\bar{\sigma}$ is a monomorphism.

We claim that $\bar{\sigma}$ is onto.

Let $f'(t)\in R'[t]$ and $f'(t)=\gamma_0'+\gamma_1't+...+\gamma_n't^n$ where $\gamma_i'\in R'$.

Now, since $\sigma : R\to R'$ is onto, therefore, there exists $\gamma_i \in R$ such that $\sigma(\gamma_i)=\gamma_i'$.

Consider $f(x)=\gamma_0+\gamma_1 x+\gamma_2 x^2+...+\gamma_n x^n \in R[x]$ and we have

$$\bar{\sigma}(f(x))=f'(t)$$

Therefore, $\bar{\sigma}$ is onto.

Remark. If $f(x)=\lambda_0+\lambda_1 x+\lambda_2 x^2+...+\lambda_n x^n$. Then, $f'(t)=\lambda_0^{'}+\lambda_1^{'}t+...+\lambda_n^{'}t^n$ where $\sigma(\lambda_i)=\lambda_i^{'}$ is called the **corresponding polynomial** of f(x) in $R'[t]$.

Remark. $f(x)\in R[x]$ is irreducible iff $f'(t)\in R'[t]$ is irreducible, where $f'(t)$ is corresponding polynomial of f(x). Also, if A is any ideal in R[x] then $\bar{\sigma}(A)$ is also an ideal of $R'[t]$. Further, A is maximal iff $\bar{\sigma}(A)$ is maximal. Also, we can find an isomorphism σ^* such that $\sigma^*: R[x]/A\to R'[t]/\bar{\sigma}(A)$ given by

$$\sigma^*(f(x)+A)=f'(t)+\bar{\sigma}(A).$$

1.5.10. Proposition. Let $\eta: F\to F'$ be an isomorphism onto. Let p(x) be any irreducible polynomial of degree n in F[x] and $p'(t)$ be corresponding polynomial in $F'(t)$. Let u be any root of p(x) and v be any root of $p'(t)$ in some extension of F and F' respectively. Then, there exists an isomorphism, say $\mu: F(u)\to F'(v)$ which is onto and is such that $\mu(\lambda)=\eta(\lambda)$ for all $\lambda\in F$ and $\mu(u)=v$.

Proof. Given that $p(x)\in F[x]$ is irreducible polynomial over F with root u which is in some extension of F. Then, we know that there exists an isomorphism onto, say $\sigma_1: F[x]/<p(x)>\to F(u)$ given by

$$\sigma_1(f(x)+<p(x)>)=f(u)$$

and [F(u) : F] = degree of minimal polynomial of u over F.

Since $p'(t)$ is irreducible polynomial over F' andvis a root of $p'(t)$ in some extension of F', so there exists an isomorphism onto, say $\sigma_2: F'[t]/<p'(t)>\to F'(v)$ given by

$$\sigma_2(g'(t)+<p'(t)>)=g'(v)$$

Now, $\eta: F\to F'$ is given to be an isomorphism onto. By last remarks, we have η is also an extension of η from $F(x)\to F'(t)$ with $\eta(p(x))=p'(t)$ and correspondingly, we denote the isomorphism for $F[x]/<p(x)>\to F'[t]/<p'(t)>$ by η again. Now, we have

$$\sigma_1^{-1}: F(u)\to F[x]/<p(x)>$$
$$\eta: F[x]/<p(x)>\to F'[t]/<p'(t)>$$
$$\sigma_2: F'[t]/<p'(t)>\to F'(v)$$

Consider $\mu=\sigma_2\eta\sigma_1^{-1}: F(u)\to F'(v)$.

Now, σ_2,η and σ_1^{-1} are all isomorphism onto, therefore, μ is also isomorphism onto.

For $\lambda\in F$, we have

$$\mu(\lambda)=\sigma_2\eta\sigma_1^{-1}(\lambda)=\sigma_2\eta\left(\sigma_1^{-1}(\lambda)\right)=\sigma_2\eta(\lambda+<p(x)>)=\sigma_2(\eta(\lambda)+<p'(t)>)=\eta(\lambda)$$

Now, compute

$$\mu(u)=\sigma_2\eta\sigma_1^{-1}(u)=\sigma_2\eta(x+<p(x)>)=\sigma_2(t+<p'(t)>)=v.$$

1.6. Splitting Field. Let F be any field and $f(x)\in F[x]$ be any polynomial over F. An extension E of F is called a splitting field of f(x) over F if

(i) f(x)is written as a product of linear factors over E.

(ii) If E' is any other extension of F such that f(x) is written as product of linear factors over E', then $E\subseteq E'$.

Remark. We have proved a theorem that for any polynomial $f(x)\in F[x]$, where degf(x) = n, there always exist an extension E of F such that E contains all the roots of f(x) and $[E:F]\le n!$. So, we can say that splitting field of a polynomial is always a finite extension.

1.6.1. Another Form. Let $f(x)\in F[x]$ and let $\alpha_1,\alpha_2,...,\alpha_n$ be roots of f(x). Consider the extension $K=F\left(\alpha_1,\alpha_2,...,\alpha_n\right)$. By definition, K is the smallest extension of F containing $\alpha_1,\alpha_2,...,\alpha_n$. Also, let E be the splitting field of F.

Now, $F\subseteq E$ and also $\alpha_1,\alpha_2,...,\alpha_n\in E$, therefore, $K\subseteq E$.

Also, $E\subseteq K$, since E is the splitting field. Therefore,

E = K.

Thus, splitting field is always obtained by adjunction of all the roots of f(x) with F. Hence if $f(x)\in F[x]$ is a polynomial of degree n and $\alpha_1,\alpha_2,...,\alpha_n$ are its roots, then splitting field is $F\left(\alpha_1,\alpha_2,...,\alpha_n\right)$.

1.6.2. Example. Let F be any field and K be its extension. Let $a\in K$ be algebraic over F of degree m and $b\in K$ be algebraic over F of degree n such that (m, n) = 1. Then, $[F\left(a,b\right):F]=mn$.

Solution. Let p(x) be minimal polynomial of ‘a’ over F. Then,

degp(x) = m = [F(a) : F].

Let q(x) be the minimal polynomial of ‘b’ over F. Then,

degq(x) = n = [F(b) : F].

Now, [F(a,b) : F] = [F(a,b) : F(a)][F(a) : F] = [F(a,b) : F(b)][F(b) : F] …(*)

Therefore, $m=[F(a):F]|[F(a,b):F]$ and $n=[F(b):F]|[F(a,b):F]$.

Since $(m,n)=1 \;\Rightarrow\; mn|[F(a,b):F] \;\Rightarrow\; [F(a,b):F]\ge mn$ …(1)

Now, $a\in F(a,b)$ is algebraic over F with minimal polynomial p(x) of degree m.

Since $F\subseteq F(b) \;\Rightarrow\; p(x)\in F(b)[x]$. Therefore, ‘a’ is algebraic over F(b).

So, let t(x) be the minimal polynomial of ‘a’ over F(b).

Now, $p(a)=0 \;\Rightarrow\; t(x)|\,p(x) \;\Rightarrow\; \deg p(x)\ge \deg t(x) \;\Rightarrow\; \deg t(x)\le m$.

$\Rightarrow \ [F(a,b):F(b)]=[F(b)(a):F(b)]=\deg t(x)\leq m$

Then, by (*),

$[F(a,b):F]=[F(a,b):F(b)][F(b):F]\leq mn$ …(1)

By (1) and (2), we have

$$[F\left(a,b\right):F]=mn.$$

1.6.3. Definition. A field F is said to be **algebraically closed field** if it has no algebraic extension.

Thus, a field is called algebraically closed if f(x) has splitting field E, then E = F. For example, field of complex numbers is algebraically closed.

1.6.4. Remark. Algebraically closed fields are always infinite.

Proof. Let F be any algebraically closed field and, if possible, suppose that F is finite. Then, $F = \{a_1,a_2,\ldots,a_n\}$. Consider the polynomial

$$f(x) = (x-a_1)(x-a_2)\ldots(x-a_n)+1$$

in F, where 1 is unity of F.

This polynomial has no roots in F. So, F cannot be algebraically closed.

Hence our supposition is wrong and so F must be infinite.

1.6.5. Example. Find the splitting field and its degree for the polynomial $f(x) = x^3 – 2$ over Q.

Solution. Let $x^3-2\in Q[x]$. Then, $\alpha=\sqrt[3]{2},\alpha w,\alpha w^2$ are its roots.

Let E be the splitting field of $x^3 – 2$ over Q. Therefore, $\alpha,\alpha w,\alpha w^2\in E \quad \Rightarrow \quad w\in E$.

Thus, $E=Q(\alpha,w)$

Consider [E : Q]. Here, $\alpha\in E$ and $\alpha\notin Q$. So,

$$[E:Q]=[E:Q(\alpha)][Q(\alpha):Q]$$

Now, $\alpha\notin Q$, therefore,

$$[Q(\alpha):Q]=\text{degree of minimal polynomial of } \alpha \text{ over } Q=3$$

since $x^3 – 2$ is monic and irreducible.

Also, $w\in E$ and $w\notin Q$. Therefore,

$$[Q(w) : Q] = 2$$

since basis of Q(w) over Q is {1,w}. Also,

$$[E : Q] = [E : Q(w)][Q(w) : Q]$$

Since (2, 3) = 1, so we have [E : Q] = 6 = 3!.

1.6.6. Algebraic Number. A complex number is said to be an algebraic number if it is algebraic over the field of rational numbers.

1.6.7. Algebraic Integer. An algebraic number is said to be an algebraic integer if it satisfies a monic polynomial over integers.

Exercise. Find the splitting field and its degree over Q for the polynomials

(a) $f(x) = x^p-1$
(b) $f(x) = x^4-1$
(c) $f(x) = x^2+3$

Exercise. Show that the polynomials x^2+3 and x^2+x+1 have same splitting field over Q.

Exercise. Show that $\sin m^0$ is an algebraic integer for every integer m.

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

1.6.8. Example. If $a \in K$ is algebraic over F of odd degree show that $F(a) = F(a^2)$.

Solution. Let K be an extension of F and $a \in K$ be algebraic of odd degree. Let p(x) be minimal polynomial of 'a'. We can write

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

Now, $a \in F(a) \quad \Rightarrow \quad a^2 \in F(a) \quad \Rightarrow \quad F(a^2) \subseteq F(a)$ ...(1)

To prove $F(a) \subseteq F(a^2)$, it is sufficient to prove that $a \in F(a^2)$.

We are given that p(a) = 0, that is,

$$\alpha_0 + \alpha_1 a + ... + \alpha_{2n} a^{2n} + \alpha_{2n+1} a^{2n+1} = 0$$

$$\Rightarrow \quad a(\alpha_{2n+1} a^{2n} + \alpha_{2n-1} a^{2n-1} + ... + \alpha_1) + \alpha_{2n} a^{2n} + \alpha_{2n-2} a^{2n-2} + ... + \alpha_0 = 0$$

$$\Rightarrow \quad a(\alpha_{2n+1} a^{2n} + \alpha_{2n-1} a^{2n-2} + ... + \alpha_1) = -(\alpha_{2n} a^{2n} + \alpha_{2n-2} a^{2n-2} + ... + \alpha_0)$$

$$\Rightarrow \quad aX = -Y \qquad ...(2)$$

where $X = \alpha_{2n+1} a^{2n} + \alpha_{2n-1} a^{2n-2} + ... + \alpha_1$, $Y = \alpha_{2n} a^{2n} + \alpha_{2n-2} a^{2n-2} + ... + \alpha_0$ in $F(a^2)$.

Now, we prove that $X \neq 0$.

If X = 0, then 'a' satisfies the polynomial

$$\alpha_{2n+1} x^{2n} + \alpha_{2n-1} x^{2n-2} + ... + \alpha_1$$

which is of degree 2n < degp(x).

But p(x) is minimal polynomial of 'a' which is a contradiction. Hence $X \neq 0$ and so X^{-1} exists. By (2),

$$a = -YX^{-1}$$

But $X \in F(a^2), Y \in F(a^2) \quad \Rightarrow \quad \text{-YX}^{-1} \in F(a^2) \quad \Rightarrow \quad a \in F(a^2)$.

Therefore, $F(a) \subseteq F(a^2)$ ---(3)

By (1) and (3), we have

$$F(a) = F(a^2)$$

Remark. Let F be a field of characteristic p and let f(x) = x^p-1.

Then, $f'(x) = px^{p-1} = 0$ $[\because \text{p.1} = 0]$.

So, degree of $f'(x)$ depends upon the characteristic of field considered.

Again, let F = {0, 1} be the given field and f(x) be a polynomial over F given by

$$f(x) = x^{10} + x^9 + ... + x + 1$$

Then, $f'(x) = 10x^9 + 9x^8 + ... + 2x + 1 = 0x^9 + x^8 + ... + 1 = x^8 + x^6 + ... + 1$

So, $\deg f'(x) = 8$.

1.6.9. Lemma. Let $f(x) \in F[x]$ be a non-constant polynomial. Then, an element α of field extension K of F is a multiple root of f(x) iff α is a common root of f(x) and $f'(x)$.

Proof. Let α be a root of f(x) of multiplicity m > 1. Then, we can write

$$f(x) = (x-\alpha)^m g(x), \quad g(x) \in K[x] \text{ and } g(\alpha) \neq 0$$

$$f'(x) = m(x-\alpha)^{m-1} g(x) + (x-\alpha)^m g'(x)$$

$$f'(\alpha) = m(\alpha-\alpha)^{m-1} g(\alpha) + (\alpha-\alpha)^m g'(\alpha) = 0$$

Thus, α is a root $f'(x)$ also.

Conversely, let α is a common root of f(x) and $f'(x)$. Then, we have to prove that α is a multiple root of f(x).

Let, if possible, α is not a multiple root of f(x).

Then, $f(x) = (x-\alpha) g(x), \quad g(x) \in K[x]$ and $g(\alpha) \neq 0$.

Therefore, $f'(x) = g(x) + (x-\alpha) g'(x)$ and so $f'(\alpha) = g(\alpha) = 0$, a contradiction.

Hence α is a multiple root of f(x).

1.6.10. Lemma. Let $f(x) \in F[x]$ be irreducible polynomial over F, then f(x) has a multiple root in some extension of F iff $f'(x) = 0$ identically.

Proof. Let $f(x) \in F[x]$ has a multiple root of multiplicity m > 1, in some extension K of F where f(x) is an irreducible polynomial over F.

Let $f(x) = \lambda_0 + \lambda_1 x + ... + \lambda_n x^n \in F[x]$ be an irreducible polynomial of degree n. Let α be its multiple root of multiplicity m > 1. Then, by above lemma, α is also a root of $f'(x)$, that is, $f'(\alpha) = 0$. But $f'(x) = \lambda_1 + 2\lambda_2 x + ... + n\lambda_n x^{n-1} \in F[x]$ and $\deg f'(x) \le n-1$.

W.L.O.G., we can assume that $\lambda_n = 1$ so that f(x) is monic and irreducible polynomial and hence is minimal polynomial of α. But α satisfies $f'(x)$. Therefore, $f(x) | f'(x)$.

Thus, $f'(x) = 0$ identically, since $\deg f'(x) \le \deg f(x)$.

Conversely, let $f'(x) = 0$ and K the splitting field of f(x) over F. Let $\deg f(x) = n$.

Let $\lambda_1, \lambda_2, ..., \lambda_n$ be the roots of f(x) in K. We can write

$$f(x) = \lambda(x-\lambda_1)(x-\lambda_2)...(x-\lambda_n) \text{ for some } \lambda \in \mathrm{F}.$$

Then, we have

$$f'(x) = \lambda(x-\lambda_2)...(x-\lambda_n) + \lambda(x-\lambda_1)(x-\lambda_3)...(x-\lambda_n) + ... + \lambda(x-\lambda_1)(x-\lambda_2)...(x-\lambda_{n-1})$$

$$\Rightarrow \quad f'(\lambda_i) = \lambda(\lambda_i - \lambda_1)...(\lambda_i - \lambda_{i-1})(\lambda_i - \lambda_{i+1})...(\lambda_i - \lambda_n)$$

Now, since $f'(x) = 0$ identically, so $f'(\lambda_i) = 0$. But $\lambda \ne 0 \Rightarrow \lambda_i = \lambda_j$ for some $i \ne j$.

Therefore, f(x) has multiple roots.

1.6.11. Corollary. Let charF = 0 and f(x) be any irreducible polynomial over F, then f(x) cannot have multiple roots.

Proof. Let degf(x) = n >1.

Let $f(x) = \lambda_0 + \lambda_1 x + ... + \lambda_n x^n \in F[x]$. Here n > 1 and $\lambda_n \ne 0$.

$$f'(x) = \lambda_1 + 2\lambda_2 x + ... + n\lambda_n x^{n-1}$$

Now, $n\lambda_n \ne 0 \quad \Rightarrow \quad f'(\alpha) \ne 0 \quad \Rightarrow \quad f'(x) \ne 0$

Hence by above lemma, f(x) cannot have multiple roots.

Remark. Any irreducible polynomial over field of rationals, field of reals or field of complex numbers cannot have multiple roots because all these fields are of characteristic zero.

1.7. Separable polynomial. Let $f(x) \in F[x]$ be any polynomial of degree n > 1, then it is said to be separable over F if all its irreducible factors are separable. Otherwise f(x) is said to be inseparable.

1.7.1. Separable irreducible polynomial. An irreducible polynomial $f(x) \in F[x]$ of degree n is said to be separable over F if it has n distinct roots in its splitting field, that is, it has no multiple roots.

1.7.2. Inseparable irreducible polynomial. An irreducible polynomial which is not separable over F is called inseparable over F. Equivalently, if $f(x) \in F[x]$ is irreducible polynomial having multiple roots of multiplicity n > 1 is called inseparable over F.

Remark. By the corollary of above lemma, we conclude that inseparable implies $ch.F \neq 0$ and ch.F = 0 implies separable. But converse is not true, that is, if $ch.F \neq 0$, then the polynomial may be separable or inseparable.

1.7.3. Lemma. Let $ch.F = p(\neq 0)$ and $f(x) \in F[x]$ be an irreducible polynomial over F. Then, f(x) is inseparable iff $f(x) \in F[x^p]$.

Proof. Let f(x) be any irreducible polynomial over F of degree n and is separable. Let

$$f(x) = \lambda_0 + \lambda_1 x + ... + \lambda_n x^n, \quad \lambda_n \neq 0$$

Therefore, $f'(x) = \lambda_1 + 2\lambda_2 x + ... + n\lambda_n x^{n-1}$

Since $f(x) \in F[x]$ is irreducible polynomial and is inseparable, so f(x) must have repeated roots. Therefore,

$$f'(x) = 0 \quad \Rightarrow \quad \lambda_1 + 2\lambda_2 x + ... + n\lambda_n x^{n-1} = 0 \quad \Rightarrow \quad \lambda_1 = 2\lambda_2 = ... = n\lambda_n = 0 \quad \text{---(*)}$$

Since $\lambda_i \in F$ andch.F p > 0. Therefore, if $k\lambda_i = 0 \quad \Rightarrow \quad p \mid k$ or if $p \nmid k$, then $\lambda_i = 0$.

Therefore, by (*), we get

$$\lambda_1 = \lambda_2 = ... = \lambda_{p-1} = 0$$

and $p\lambda_p = 0 \quad \Rightarrow \quad \lambda_p$ may or may not be zero.

Further, $(p+1)\lambda_{p+1} = 0 \quad \Rightarrow \quad \lambda_{p+1} = 0$. So

$$\lambda_{p+1} = \lambda_{p+2} = ... = \lambda_{2p-1} = 0$$

Again, $2p\lambda_{2p} = 0 \quad \Rightarrow \quad \lambda_{2p}$ may or may not be zero and so on. Therefore,

$$f(x) = \lambda_0 + \lambda_p x^p + \lambda_{2p} x^{2p} + ... + \lambda_m x^{mp}$$

where n = mp if $\lambda_m \neq 0$. Thus,

$$f(x) = \lambda_0 + \lambda_p x^p + \lambda_{2p} \left(x^p\right)^2 + ... + \lambda_m \left(x^p\right)^m \in F[x^p]$$

Conversely, if $f(x) \in F[x^p]$. Then,

$$f(x) = \lambda_0 + \lambda_p x^p + \lambda_{2p} x^{2p} + ... + \lambda_k x^{kp}$$

where $\lambda_0, \lambda_p, \lambda_{2p}, ..., \lambda_k \in F$.

Then, $f'(x) = 0 + p\lambda_p x^{p-1} + 2p\lambda_{2p} x^{2p-1} + ... + kp\lambda_k x^{kp-1} = 0 \qquad [ch.F \ = \ p].$

Thus, f(x) has multiple roots and hence f(x) is inseparable.

1.7.4. Separable Element. Let K be any extension of F. An algebraic element $\alpha \in K$ is said to be separable over F if the minimal polynomial of α is separable over F.

1.7.5. Separable Extension. An algebraic extension K of F is called separable extension if every element of K is separable.

1.7.6. Proposition. Prove that if ch.F = 0, then any algebraic extension of F is always separable extension.

Proof. Given that ch.F = 0 and let K be any algebraic extension of F. Let $\alpha \in K$. Then, α is algebraic over F.

So, let p(x) be the minimal polynomial of α over F. Then, p(x) is irreducible polynomial over F and so p(x) is separable.

Therefore, α is separable. But α was an arbitrary element of K. So, K is separable extension.

1.7.7. Perfect Field. A field F is called perfect if all its finite extensions are separable.

1.7.8. Theorem. Let K be an algebraic extension of F, where F is a perfect field then K is separable extension of F.

Proof. Let $a \in K$. Since K is algebraic, so 'a' is algebraic over F. Therefore,

[F(a) : F] = degree of minimal polynomial of 'a' over F = r (say)

Thus, F(a) is finite extension. But F is perfect, therefore, F(a) is separable extension. So, 'a' is separable over F.

Hence K is separable.

1.7.9. Theorem. Let ch.F = p > 0. Prove that the element 'a' in some extension of F is separable iff $F(a^p) = F(a)$.

Proof. Let K be some extension of F such that $a \in K$ and 'a' is separable over F. So, 'a' is algebraic element with its minimal polynomial, say

$$f(x) = \lambda_0 + \lambda_1 x + ... + \lambda_{n-1} x^{n-1} + x^n$$

and f(x) has no multiple roots.

Let g(x) be the polynomial

$$g(x) = \lambda_0^p + \lambda_1^p x + ... + \lambda_{n-1}^p x^{n-1} + x^n$$

Then,

$$g(a^p) = \lambda_0^p + \lambda_1^p a^p + ... + \lambda_{n-1}^p a^{(n-1)p} + a^{np} = \left(\lambda_0 + \lambda_1 a + ... + \lambda_{n-1} a^{n-1} + a^n\right)^p = \left(f(a)\right)^p = 0$$

Therefore, a^p satisfies a polynomial $g(x) \in F[x]$.

Now, $a \in F(a) \Rightarrow a^p \in F(a) \Rightarrow F(a^p) \subseteq F(a)$ ---(1)

Further, $F(a^p)$ and F(a) both are vector spaces over F and $F(a^p) \subseteq F(a)$, therefore,

$$[F(a^p):F] \leq [F(a):F] = n$$

We claim that $[F(a^p):F] = n$.

We know that $[F(a^p):F]$ = degree of minimal polynomial of a^p over F.

We shall prove that g(x) is minimal polynomial of a^p over F. For this, it is sufficient to prove that g(x) is an irreducible polynomial.

Let $h(x) \in F[x]$ be a factor of g(x). Then,

$$g(x) = h(x)t(x)$$

for some $t(x) \in F[x]$. Thus,

$$g(x^p) = h(x^p)t(x^p)$$

and so $h(x^p)$ is a factor of $g(x^p)$ in F[x].

But $g(x^p) = \lambda_0^p + \lambda_1^p x^p + \ldots + \lambda_{n-1}^p x^{(n-1)p} + x^{np} = \left(\lambda_0 + \lambda_1 x + \ldots + \lambda_{n-1} x^{n-1} + x^n\right)^p = \left(f(x)\right)^p$

$\Rightarrow h(x^p) \mid \left(f(x)\right)^p \Rightarrow h(x^p) = \left(f(x)\right)^k$ for some integer k, $0 \leq k \leq p$.

Taking derivatives both sides

$$h'(x^p)px^{p-1} = k\left(f(x)\right)^{k-1} f'(x) \Rightarrow 0 = k\left(f(x)\right)^{k-1} f'(x) \quad [\text{ch.}F = p]$$

Since f(x) is separable polynomial so $f'(x) \neq 0$. Therefore, either k = 0 or k = p.

If k = p, then $h(x^p) = (f(x))^p = g(x^p) \Rightarrow h(x) = g(x)$.

If k = 0, then $h(x^p) = (f(x))^0 = 1 \Rightarrow h(x^p) = 1$, a constant function, so h(x) = 1.

Thus, g(x) is irreducible polynomial of degree n, therefore,

$$[F(a^p) : F] = n.$$

Hence $[F(a^p) : F] = [F(a) : F] \Rightarrow F(a^p) = F(a)$.

Conversely, suppose $F(a^p) = F(a)$.

We claim that ‘a’ is separable over F.

Let, if possible, ‘a’ is not separable.

Let $f(x) \in F[x]$ be the minimal polynomial of 'a'. Then, by our assumption f(x) is not separable over F. Since ch.F = p > 0 and f(x) is inseparable over F.

So, $f(x) \in F[x^p]$.

Let $f(x) = g(x^p)$ for some $g(x) \in F[x] \quad \Rightarrow \quad g(a^p) = f(a) = 0$.

a^p is a root of the polynomial $g(x) \in F[x]$. But

$$\deg f(x) = \frac{\deg f(x)}{p} = \frac{n}{p}\text{, where n = deg f(x).}$$

Therefore, degree of minimal polynomial of $a^p \leq \frac{n}{p}$.

So, we get $n = [F(a):F] = [F(a^p):F] \leq \frac{n}{p}$

which is a contradiction. Hence 'a' is separable over F.

1.8. Check Your Progress.

1. Find the splitting field of x^5-1 over Q.
2. Find the splitting field of x^2-9 over Q.
3. Show that [K : F] = 1 if and only if K = F.

1.9. Summary.

In this chapter, we have defined Extension of a field and derived various results. The result worth mentioning is that if p(x) is a polynomial of degree n over some field F, then the number of zeros, to be considered, of this polynomial depends on the extension that we are considering.

Books Suggested:

1. Luther, I.S., Passi, I.B.S., Algebra, Vol. IV-Field Theory, Narosa Publishing House, 2012.
2. Stewart, I., Galios Theory, Chapman and Hall/CRC, 2004.
3. Sahai, V., Bist, V., Algebra, Narosa Publishing House, 1999.
4. Bhattacharya, P.B., Jain, S.K., Nagpaul, S.R., Basic Abstract Algebra (2nd Edition), Cambridge University Press, Indian Edition, 1997.
5. Lang, S., Algebra, 3rd edition, Addison-Wesley, 1993.
6. Adamson, I. T., Introduction to Field Theory, Cambridge University Press, 1982.
7. Herstein, I.N., Topics in Algebra, Wiley Eastern Ltd., New Delhi, 1975.