Master of Science (Mathematics) (DDE)

Semester – II

Paper Code – 20MAT22C1

THEORY OF FIELD EXTENSIONS

DIRECTORATE OF DISTANCE EDUCATION

MAHARSHI DAYANAND UNIVERSITY, ROHTAK

(A State University established under Haryana Act No. XXV of 1975)

NAAC 'A^{+}' Grade Accredited University

Material Production

Content Writer: *Dr Jagbir Singh*

Maharshi Dayanand University
ROHTAK – 124 001

ISBN :

Price : Rs. 325/-

Publisher: Maharshi Dayanand University Press

Publication Year : 2021

M.Sc. (Mathematics) (DDE)
Paper Code : 20MAT22C1
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 $K \neq F$. $\quad [F \subseteq K]$

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, $\pi^2, \ldots, \pi^n$} 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, $\alpha^2, \ldots, \alpha^n$ 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, $\alpha^2, \ldots, \alpha^n$ 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

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

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 $K\,|\,F$ 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 $f(x)=\lambda_0+\lambda_1x+\lambda_2x^2+...+\lambda_nx^n\in F[x]$. Clearly,

$$f(a)=\lambda_0+\lambda_1a+\lambda_2a^2+...+\lambda_na^n\in F(a)$$

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 $\left[F(a):F\right]$ is finite, that is F(a) is a finite extension over F. Moreover, $\left[F(a):F\right]=n$, where n is the degree of minimal polynomial of '*a*' over F.

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

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

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

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

Thus, *a* satisfies the polynomial $f(x)=\lambda_0+\lambda_1 x+\lambda_2 x^2+\ldots+\lambda_n x^n$. 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 $p(x)=\lambda_0+\lambda_1 x+\lambda_2 x^2+\ldots+\lambda_n x^n$, $\lambda_n \neq 0$ 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

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

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 $F \subseteq E \quad \Rightarrow \quad F[x] \subseteq E[x] \quad \Rightarrow \quad f[x] \in E[x]$ 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 $\deg p_1(x) \le \deg p(x)$.

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

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 $p \mid \alpha_0, p \mid \alpha_1, ..., p \mid \alpha_{n-1}, p \nmid \alpha_n$ 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 $(x-a) \mid f(x)$ in K[x], that is, iff there exists some g(x) in K[x] such that f(x) = (x-a)g(x).

Proof. Let $(x-a) \mid f(x)$ 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,

$$F[x]/\langle p(x) \rangle \cong F[a] = F(a).$$

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 $Ker\eta = \langle p(x) \rangle$.

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

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

$\Rightarrow \quad f(x) = p(x)q(x)$, 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 $[E:F]=n=\deg p(x)$.

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

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

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

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

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

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

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,

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

Thus, $\bar{1}, \overline{x}, \overline{x}^2, ..., \overline{x}^{n-1}$ 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 $f(x)=\lambda_0+\lambda_1x+\lambda_2x^2+...+\lambda_nx^n$. 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 $\sigma^*:R[x]/A\to R'[t]/\bar{\sigma}\left(A\right)$ 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 $K = F(\alpha_1, \alpha_2, ..., \alpha_n)$. 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 $F(\alpha_1, \alpha_2, ..., \alpha_n)$.

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

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, $m = [F(a):F] \mid [F(a,b):F]$ and $n = [F(b):F] \mid [F(a,b):F]$.

Since $(m,n) = 1 \Rightarrow mn \mid [F(a,b):F] \Rightarrow [F(a,b):F] \ge mn$ …(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, $p(a) = 0 \Rightarrow t(x) \mid p(x) \Rightarrow \deg p(x) \ge \deg t(x) \Rightarrow \deg t(x) \le m$.

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

Then, by (*),

$$[F(a,b):F] = [F(a,b):F(b)][F(b):F] \le mn \qquad \ldots(1)$$

By (1) and (2), we have

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

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,

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

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

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

$$\Rightarrow \quad aX = -Y \qquad \text{…(2)}$$

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

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

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, $f(x) \mid f'(x)$.

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, $a \in F(a) \quad \Rightarrow \quad a^p \in F(a) \quad \Rightarrow \quad F(a^p) \subseteq F(a)$ ---(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 $g(x^p) = \lambda_0^p + \lambda_1^p x^p + \ldots + \lambda_{n-1}^p x^{(n-1)p} + x^{np} = \left(\lambda_0 + \lambda_1 x + \ldots + \lambda_{n-1} x^{n-1} + x^n\right)^p = \left(f(x)\right)^p$

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

Taking derivatives both sides

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

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

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

If k = 0, then $h(x^p) = (f(x))^0 = 1 \quad \Rightarrow \quad h(x^p) = 1$, 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.

2

Galois Theory

Structure

2.1. Introduction. In this chapter, we shall discuss about normal extensions, fixed fields, Galois extensions, norms, traces and the dependence of all these on normal extensions.

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

(i) Normal Extensions.

(ii) Fixed Fields, Galios Groups

(iii) Norms and Traces.

2.1.2. Keywords. Normal Extensions, Galois Group, Fixed Fields.

2.3. Normal Extension. An algebraic extension K of F is said to be normal extension of F if each irreducible polynomial f(x) over F having a root in K splits into linear factors over K, that is, if one root is in K, then all the roots are in K.

If E is the splitting field of f(x) over F such that a root 'a' of f(x) is in K, then $E \subseteq K$.

2.3.1. Lemma. Let [K : F] = 2, then K is normal extension of F always.

Proof. Let $g(x) \in F[x]$ be any irreducible polynomial over F. Let α be a root of f(x) and $\alpha \in K$. Now, we have

$$[F(\alpha):F] \leq [K:F] = 2 \quad \Rightarrow \quad [F(\alpha):F] \leq 2 \quad \Rightarrow \quad \deg f(x) \leq 2.$$

If degf(x) = 1, then let

$$f(x) = ax+b \quad \text{with } a,b \in F, a \neq 0.$$

Then, $0 = f(\alpha) = a\alpha + b \quad \Rightarrow \quad \alpha = -\frac{b}{a}, a \neq 0$.

But $-\frac{b}{a} \in F \subseteq K \quad \Rightarrow \quad \alpha \in K$.

If degf(x) = 2, then let f(x) = ax^2+bx+c with $a \neq 0$. If α be a root of f(x), then,

$$f(x) = (x-\alpha)(x+\alpha+\frac{b}{a}), \quad a \in K$$

$\Rightarrow \quad -(\alpha+\frac{b}{a})$ is other root of f(x).

Since $\frac{b}{a} \in F \subseteq K$ and $\alpha \in K \quad \Rightarrow \quad -(\alpha+\frac{b}{a}) \in K$.

Hence K is a normal extension of F.

2.3.2. Theorem. Let K be a finite algebraic extension of a field F then K is a normal extension of F iff K is the splitting field of some non-zero polynomial over F.

Proof. Let K = $F(a_1,a_2,\ldots,a_n)$ be a finite algebraic extension of F. Suppose K is normal extension of F. For each $a_i \in K$, let $f_i(x)$ be the minimal polynomial of a_i over F. Since K is normal extension of F, so $f_i(x)$ splits completely into linear factors over K.

Let $f(x) = f_1(x)f_2(x)\ldots f_n(x)$.

Let 'a' be any root of f(x), then 'a' is also a root of some $f_i(x)$ and hence $a \in K$. Let E be the splitting field of f(x). Then, $E \subseteq K$.

Now, $F(a_i) = \prod_{j=1}^{n} f_j(a_i) = 0$. Therefore, a_i is a root of f(x), that is, $a_i \in E$.

Therefore, $F(a_1, a_2, ..., a_n) \subseteq E \quad \Rightarrow \quad K \subseteq E$.

Thus, K = E.

Hence K is the splitting field of f(x) over F.

Conversely, let K be the splitting field of some non-zero polynomial f(x) over F. Let $a_1,a_2,\ldots,a_n$ be the roots of f(x). Then, K = $F(a_1,a_2,\ldots,a_n)$.

By definition, $[K:F]\le n!$.

So, K is finite algebraic extension of F. Let p(x) be any irreducible polynomial over F with a root β in K. p(x) is also a polynomial over K with $(x-\beta)$ as a factor in K[x]. So p(x) is not irreducible over K.

Let L be the splitting field of p(x) over K. We claim that L=K.

Let, if possible, $L\neq K$. Then, there exists a root $\beta'$of p(x) in L such that $\beta'\notin K$. As β and $\beta'$are conjugates over F, there exists an isomorphism $\sigma:F(\beta)\to F(\beta')$ such that $\sigma(\beta)=\beta'$ and $\sigma(\lambda)=\lambda$ for every λ in F. Now, $F\subseteq F(\beta)\subseteq K$ gives K is a splitting field of f(x) over $F(\beta)$.

Further, $K(\beta')=F(a_1,a_2,...,a_n)(\beta')=F(\beta')(a_1,a_2,...,a_n)$ gives $K(\beta')$ is a splitting field of f(x) over $F(\beta')$. Then, there exists an isomorphism $\tau:K\to K(\beta')$ such that

$$\tau(x)=\sigma(x) \text{ for every x in } F(\beta).$$

But then $\tau(\beta)=\sigma(\beta)=\beta'$ and $\tau(\lambda)=\sigma(\lambda)=\lambda$ for every λ in F.

Hence $\tau:K\to K(\beta')$ is an onto isomorphism, such that $\tau(\beta)=\beta'$ and $\tau(\lambda)=\lambda$ for every λ in F. If

$$f(x)=\alpha_0+\alpha_1x+...+\alpha_{n-1}x^{n-1}+\alpha_nx^n$$

in F[x] with $\alpha_n\neq 0$. Then,

$$f(x)=\alpha_n(x-a_1)(x-a_2)...(x-a_n)$$

Let $\tau':K[x]\to K(\beta')[x]$ be an extension of τ such that

$$\begin{aligned}\tau'(f(x))&=\tau'(\alpha_0+\alpha_1x+...+\alpha_{n-1}x^{n-1}+\alpha_nx^n)=\tau'(\alpha_0)+\tau'(\alpha_1)x+...+\tau'(\alpha_{n-1})x^{n-1}+\tau'(\alpha_n)x^n\\&=\tau(\alpha_0)+\tau(\alpha_1)x+...+\tau(\alpha_{n-1})x^{n-1}+\tau(\alpha_n)x^n=\alpha_0+\alpha_1x+...+\alpha_{n-1}x^{n-1}+\alpha_nx^n\\&=f(x)\end{aligned}$$

Also,

$$\begin{aligned}\tau'(f(x))&=\tau'(\alpha_n(x-a_1)(x-a_2)...(x-a_n))=\tau'(\alpha_n)\tau'(x-a_1)\tau'(x-a_2)...\tau'(x-a_n)\\&=\alpha_n(x-\tau(a_1))(x-\tau(a_2))...(x-\tau(a_n))\end{aligned}$$

We get that $\tau(a_1),\tau(a_2),...,\tau(a_n)$ are also roots of f(x). Since τ is one-one, so

$$\{\tau(a_1),\tau(a_2),...,\tau(a_n)\}=\{a_1,a_2,...,a_n\}$$

It implies τ permutes the roots of f(x). Therefore,

$$K=F(a_1,a_2,...,a_n)=F(\tau(a_1),\tau(a_2),...,\tau(a_n))$$

However,

$$K(\beta')=\tau(K)=\tau\left(F(a_1,a_2,...,a_n)\right)=F(\tau(a_1),\tau(a_2),...,\tau(a_n))=F(a_1,a_2,...,a_n)=K$$

It implies $\beta'\in K$, which is a contradiction.

Thus, L = K, so p(x) splits completely over K. Hence K is a normal extension of F.

2.3.3. Corollary. Let K be a finite normal extension of F. If E be any subfield of K such that $F\subseteq E\subseteq K$, then K is normal extension of E.

Proof. Since *K* is a finite normal extension of *F*, so there exist a polynomial *f*(*x*) over *F* such that *K* is splitting field of *f*(*x*) over *F*. Then *K* is also a splitting field of *f*(*x*) over *E*. Hence by above theorem *K* is normal extension of *E*.

2.3.4. Corollary. Let K be finite normal extension of F. If α_1 and α_2 be any two elements in K conjugate over F, then there exists an F automorphism σ of K such that $\sigma(\alpha_1)=\alpha_2$.

Proof. Let *K* be the splitting field of the non-zero polynomial *f*(*x*) over *F*. Since α_1, α_2 are conjugates over *F* there exist an isomorphism σ such that $\sigma : F(\alpha_1) \to F(\alpha_2)$ defined by

$$\sigma(\alpha_1) = (\alpha_2) \text{ and } \sigma(\lambda) = \lambda \text{ for all } \lambda \in F.$$

Now $[F(\alpha_1) : F] = [F(\alpha_2) : F]$ = degree of minimal polynomial of α_1 (or α_2).

Now , $f(x) \in F[x] \subseteq F(\alpha_1)[x]$ and $f(x) \in F[x] \subseteq F(\alpha_2)[x]$

Therefore, *K* is splitting field of $f(x)$ over $F(\alpha_1)$ as well as $F(\alpha_2)$.

Then there exists $\Psi : K \to K$ s.t. $\Psi(\alpha) = \sigma(\alpha)$ for all $\alpha \in F(\alpha_1)$ and $\Psi(\lambda) = \sigma(\lambda) = \lambda$ for all $\lambda \in F$. Then $\Psi(\alpha_1) = \sigma(\alpha_1) = \alpha_2$. Hence Ψ is an *F*-automorphism of *K* such that $\Psi(\alpha_1) = \alpha_2$.

Remark. Converse of Corollary 1 need not be true, for if $F=Q, E=Q(\sqrt{2})$ and $K=Q(\sqrt[4]{2})$. Then K is normal extension of E, E is normal extension of F but K is not a normal extension of F.

2.3.5. M(S, K). Let K be any field and S be any non-empty set.The set of all mappings from S to K is denoted by M(S, K).

2.3.6. Theorem. If $\sigma_1,\sigma_2,...,\sigma_n$ be any n monomorphisms in M(E, K), then these are always L.I., where E and K are fields.

Proof. If n = 1, then consider σ_1 and let, for $a_1\in K$

$$a_1\sigma_1=\bar{0} \quad \Rightarrow \quad a_1\sigma_1(\alpha)=0 \text{ for all } \alpha\in \mathrm{E}$$

Since $a_1\sigma_1$ is a homomorphism from E to K and

$$a_1\sigma_1(\alpha)=0 \text{ for all } \alpha\in \mathrm{E}$$

In particular, $\left(a_1\sigma_1\right)(1)=0$ where $1\in \mathrm{E} \quad \Rightarrow \quad \left(a_1\right)\sigma_1(1)=0$.

Since σ_1 is a monomorphism so $\sigma_1(1) \neq 0$, then $a_1 = 0$.

Hence σ_1 is linearly independent.

Now, let us assume, as our induction hypothesis, that $\sigma_1, \sigma_2, ..., \sigma_{n-1}$ are L.I.

We have to prove that $\sigma_1, \sigma_2, ..., \sigma_n$ are L.I.

Let $\lambda_1, \lambda_2, ..., \lambda_n$ are scalars such that

$$\lambda_1\sigma_1 + \lambda_2\sigma_2 + ... + \lambda_n\sigma_n = \bar{0} \qquad ...(1)$$

If any of λ_i is zero, then the above relation reduces to a combination of (n - 1) σ_i's and by induction hypothesis, all λ_i's are zero. Hence we assume that $\lambda_1, \lambda_2, ..., \lambda_n$ are all non-zero.

So, let W.L.O.G., $\lambda_n \neq 0$. Then dividing (1) by λ_n, we have

$$b_1\sigma_1 + b_2\sigma_2 + ... + b_{n-1}\sigma_{n-1} + \sigma_n = \bar{0} \qquad ...(2)$$

where $b_i = \dfrac{\lambda_i}{\lambda_n} = \lambda_i\lambda_n^{-1}$.

Since σ_1 and σ_n are distinct, so there exists an element $x_1 \in E$ such that

$$\sigma_1(x_1) \neq \sigma_n(x_1)$$

Then, clearly $x_1 \neq 0$, since image of 0 is 0 for any homomorphism.

Now, let $x \in E$ be any element then $xx_1 \in E$ also. Compute

$$\left(b_1\sigma_1 + b_2\sigma_2 + ... + b_{n-1}\sigma_{n-1} + \sigma_n\right)\left(xx_1\right) = \bar{0}\left(xx_1\right) = 0$$

$$\Rightarrow \quad b_1\sigma_1\left(xx_1\right) + b_2\sigma_2\left(xx_1\right) + ... + b_{n-1}\sigma_{n-1}\left(xx_1\right) + \sigma_n\left(xx_1\right) = 0$$

$$\Rightarrow \quad b_1\sigma_1\left(x\right)\sigma_1\left(x_1\right) + b_2\sigma_2\left(x\right)\sigma_2\left(x_1\right) + ... + b_{n-1}\sigma_{n-1}\left(x\right)\sigma_{n-1}\left(x_1\right) + \sigma_n\left(x\right)\sigma_n\left(x_1\right) = 0$$

Since $\sigma_n(x_1) \neq 0$, so dividing above equation by $\sigma_n(x_1)$.

$$b_1\frac{\sigma_1\left(x_1\right)}{\sigma_n\left(x_1\right)}\sigma_1\left(x\right) + b_2\frac{\sigma_2\left(x_1\right)}{\sigma_n\left(x_1\right)}\sigma_2\left(x\right) + ... + b_{n-1}\frac{\sigma_{n-1}\left(x_1\right)}{\sigma_n\left(x_1\right)}\sigma_{n-1}\left(x\right) + \sigma_n\left(x\right) = 0 \qquad ...(*)$$

From (2), we also have

$$b_1\sigma_1(x) + b_2\sigma_2(x) + ... + b_{n-1}\sigma_{n-1}(x) + \sigma_n(x) = 0 \qquad ...(**)$$

Subtracting (**) from (*), we get

$$b_1\left(\frac{\sigma_1(x_1)}{\sigma_n(x_1)}-1\right)\sigma_1(x)+b_2\left(\frac{\sigma_2(x_1)}{\sigma_n(x_1)}-1\right)\sigma_2(x)+\ldots+b_{n-1}\left(\frac{\sigma_{n-1}(x_1)}{\sigma_n(x_1)}-1\right)\sigma_{n-1}(x)=0 \quad \ldots(3)$$

Since $\sigma_1(x_1)\neq\sigma_n(x_1) \Rightarrow \frac{\sigma_1(x_1)}{\sigma_n(x_1)}\neq 1 \Rightarrow \frac{\sigma_1(x_1)}{\sigma_n(x_1)}-1\neq 0$

Now as above equation (3) holds for every $x\in E$, so

$$b_1\left(\frac{\sigma_1(x_1)}{\sigma_n(x_1)}-1\right)\sigma_1+b_2\left(\frac{\sigma_2(x_1)}{\sigma_n(x_1)}-1\right)\sigma_2+\ldots+b_{n-1}\left(\frac{\sigma_{n-1}(x_1)}{\sigma_n(x_1)}-1\right)\sigma_{n-1}=0$$

which is a combination of (n-1) σ_i 's. So, we get

$$b_1\left(\frac{\sigma_1(x_1)}{\sigma_n(x_1)}-1\right)=b_2\left(\frac{\sigma_2(x_1)}{\sigma_n(x_1)}-1\right)=\ldots=b_{n-1}\left(\frac{\sigma_{n-1}(x_1)}{\sigma_n(x_1)}-1\right)=0$$

Now, as $\frac{\sigma_1(x_1)}{\sigma_n(x_1)}-1\neq 0$, so $b_1 = 0$ and so $\frac{\lambda_1}{\lambda_n}=0$, which implies $\lambda_1=0$, a contradiction.

Hence any set of n monomorphism is linearly independent.

2.3.7. Definition. Let K be any field, then the set of all automorphisms on K is denoted by AutK.

2.3.8. Corollary. AutKconsists of linearly independent elements.

Take E = K in above theorem, the result follows.

2.3.9. Exercise. The set of all automorphisms of K form a group under composition of mappings.

2.4. F-Automorphisms. Let F be any field and K be any extension of F. An automorphism $\sigma: K\to K$ is called F-automorphism of K if

$$\sigma(x)=x \text{ for all } x\in F.$$

Notation. G(K, F) will denote the group of all F-automorphisms of K. G(K, F) is called Galio's group of K over F and known as group of automorphisms from K to K which fixes F.

2.4.1. Exercise. Prove that G(K, F) is a subfield of AutK.

2.4.2. Theorem. If P is a prime subfield of K, then prove that AutK = G(K, P), that is every automorphism on K fixes P.

Proof. Let $\sigma \in \text{Aut}(K)$ then $\sigma(0) = 0$ and $\sigma(1) = 1$

Case 1. Char$K = P$ for some prime p.

Then $P \cong Z_p = \{0, 1, \ldots\ldots, p-1\}$. If $\alpha \in Z_p$ then $\alpha = 1+1+\ldots\ldots+1$ (α times)

$$\sigma(\alpha) = \sigma(1+1+\ldots\ldots+1) = \sigma(1)+\sigma(1)+\ldots\ldots+\sigma(1) = 1+1+\ldots\ldots+1 = \alpha$$

$\Rightarrow \quad \sigma(\alpha) = \alpha$ for all $\alpha \in Z_p$. $\Rightarrow$ σ fixes P.

$\Rightarrow \quad \sigma \in G(K, P) \Rightarrow \text{Aut } K \subseteq G(K, P)$.

Case 2. Char$K$ = 0.

Then $P \cong Q = \{mn^{-1} : m\ n \in Z\}$ and

$$\sigma(mn^{-1}) = \sigma(m)\,\sigma(n^{-1}) = \sigma(m)\left(\sigma(n)\right)^{-1} = mn^{-1} \text{ for all } mn^{-1} \in Q$$

$\Rightarrow$ σ fixes P. $\Rightarrow$ $\sigma \in G(K, P)$ $\Rightarrow$ Aut $K \subseteq G(K, P)$.

So, in both cases, we get Aut $(K) \subseteq G(K, P)$. But $G(K, P) \subseteq$ Aut (K) always.

So Aut $(K) = G(K, P)$.

2.4.3. Theorem. Let K be any extension of F and $\sigma \in G(K,F)$. If 'a' is an element which is algebraic over F then 'a' and '$\sigma(a)$' are conjugates over F.

Proof. We know that $G(K, F) = \{ \sigma \in \text{Aut } K : \sigma(\lambda) = \lambda \text{ for all } \lambda \in F \}$.

Let $a \in K$ be an algebraic element over F. So let $f(x) = \lambda_0 + \lambda_1 x + ... + x^n$ be the minimal polynomial of 'a' over F and then $0 = f(a) = \lambda_0 + \lambda_1 a + ... + a^n \in K$ also, since $a, \lambda_0, \lambda_1, ... \in K$.

Now, $0 = \sigma(0) = \sigma\left(f(a)\right) = \sigma(\lambda_0 + \lambda_1 a + ... + a^n)$

$= \sigma(\lambda_0) + \sigma(\lambda_1)\,\sigma(a) + ... + \sigma(a^n)$

$= \lambda_0 + \lambda_1 \sigma(a) + ... + \left(\sigma(a)\right)^n = f\left(\sigma(a)\right)$

$\Rightarrow$ $f\left(\sigma(a)\right) = 0$, so $\sigma(a)$ is also a root of $f(x)$

$\Rightarrow$ $\sigma(a)$ is conjugate of 'a' over F.

2.4.4. Exercise. Let G be a group of automorphisms of a field K. Then, the set $F_0 = \{x \in K : \sigma(x) = x \text{ for all } \sigma \in G\}$ is a subfield of K.

Also, this subfield is known as **fixed field under G**.

2.4.5. Example. Let $K = Q\left(\sqrt[3]{2}\right)$. The minimal polynomial of $\sqrt[3]{2}$ over Q is $x^3 - 2$. It has only one root, namely, $\sqrt[3]{2}$ in K. Since K is a field of real numbers. Let σ be any Q – automorphisms of K. Then $\sigma\left(\sqrt[3]{2}\right) \in K$ is a root of $x^3 - 2$. So, $\sigma\left(\sqrt[3]{2}\right) = \sqrt[3]{2}$. Let x be any element of K, then x can be expressed as:

$$a + \sqrt[3]{2}b + \left(\sqrt[3]{2}\right)^2 c, \text{ where } a, b, c \in Q.$$

So, $\sigma(x) = \sigma(a) + \sigma(\sqrt[3]{2})\sigma(b) + \sigma\left(\left(\sqrt[3]{2}\right)^2\right)\sigma(c) = a + \sqrt[3]{2}b + \left(\sqrt[3]{2}\right)^2 c = x$

$\Rightarrow$ $\sigma = I$. Thus, AutK = { I }.

Hence in this case K itself is the fixed field under AutK.

2.4.6. Theorem. Let G be a finite subgroup of AutK. If F_0 is fixed subfield under G, that is, $F_0 = \{x \in K : \sigma(x) = x \text{ for all } \sigma \in G\}$. Then, $[K : F_0] = o(G)$.

Proof. Let $[K : F_0] = m$ and $o(G) = n$.

Let, if possible, $m < n$.

Let $\sigma_1, \sigma_2, ..., \sigma_n$ are elements of G and let $\{x_1, x_2, . . . , x_m\}$ be a basis of K over F_0.

Consider a system of m linear homogeneous equations, $1 \le j \le m$

$$\sigma_1(x_j)u_1 + \sigma_2(x_j)u_2 + ... + \sigma_n(x_j)u_n = 0 \qquad \text{…(1)}$$

Note that $\sigma_1(x_j), \sigma_2(x_j), ..., \sigma_n(x_j)$ are elements of K and $u_1, u_2, . . . , u_n$ are variables.

Since the number of equations is less that the number of variables, so the system (1) has a non-trivial solution, say, $y_1, y_2, . . . , y_n$, here not all y_i's are zero.

$$\sigma_1(x_j)y_1 + \sigma_2(x_j)y_2 + ... + \sigma_n(x_j)y_n = 0 \qquad \text{…(2)}$$

for j = 1, 2, … , m.

Now, if $x \in K$, then

$$x = \alpha_1 x_1 + \alpha_2 x_2 + ... + \alpha_n x_n, \text{ where } \alpha_i \in F_0.$$

Multiplying j^{th} equation of (2) by α_j, we get

$$\sigma_1(x_j)y_1\alpha_j + \sigma_2(x_j)y_2\alpha_j + ... + \sigma_n(x_j)y_n\alpha_j = 0$$

$$\Rightarrow \quad \sigma_1(x_j)\ \sigma_1(\alpha_j)y_1 + \sigma_2(x_j)\sigma_2(\alpha_j)y_2 + ... + \sigma_n(x_j)\sigma_n(\alpha_j)y_n = 0$$

because $\alpha_j \in F_0$ and $\sigma_j \in G$ and F_0 is fixed under G.

$$\Rightarrow \quad \sigma_1(\alpha_j x_j)\ y_1 + \sigma_2(\alpha_j x_j)y_2 + ... + \sigma_n(\alpha_j x_j)y_n = 0 \text{ for } j = 1, 2, …, m.$$

Thus, we have the system of equations,

$$\sigma_1(\alpha_1 x_1)\ y_1 + \sigma_2(\alpha_1 x_1)y_2 + ... + \sigma_n(\alpha_1 x_1)y_n = 0$$
$$\sigma_1(\alpha_2 x_2)\ y_1 + \sigma_2(\alpha_2 x_2)y_2 + ... + \sigma_n(\alpha_2 x_2)y_n = 0$$
$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$$
$$\sigma_1(\alpha_m x_m)\ y_1 + \sigma_2(\alpha_m x_m)y_2 + ... + \sigma_n(\alpha_m x_m)y_n = 0$$

Adding all these equations, we get

$$\sigma_1(\alpha_1 x_1 + \alpha_2 x_2 + ... + \alpha_m x_m)\ y_1 + \sigma_2(\alpha_1 x_1 + \alpha_2 x_2 + ... + \alpha_m x_m)y_2 + ... + \sigma_n(\alpha_1 x_1 + \alpha_2 x_2 + ... + \alpha_m x_m)y_n = 0$$

$$\Rightarrow \quad \sigma_1(x)\ y_1 + \sigma_2(x)y_2 + ... + \sigma_n(x)y_n = 0 \qquad \text{for all } x \in E$$

$\Rightarrow \quad (y_1\sigma_1 + y_2\sigma_2 + ... + y_n\sigma_n)(x) = 0 \quad$ for all $x \in E$

$\Rightarrow \quad y_1\sigma_1 + y_2\sigma_2 + ... + y_n\sigma_n = \bar{0}$

where atleast one of $y_j \neq 0$.

Hence $\sigma_1, \sigma_2, ..., \sigma_n$ are L.D. over K, a contradiction.

Thus, $m \nless n$.

Now, if possible, suppose that m > n.

Then, there exist (n + 1) L.I. elements, say $x_1, x_2, \ldots, x_{n+1}$ in K over F_0. Consider the system of n linear homogeneous equations in (n+1) variables

$$\sigma_j(x_1)u_1 + \sigma_j(x_2)u_2 + ... + \sigma_j(x_{n+1})u_{n+1} = 0 \qquad \ldots(3)$$

for j = 1,2,…n.

Since the number of variables is again greater than the number of equations, so these homogeneous equations have a non-trivial solution. Let $z_1, z_2, \ldots, z_{n+1}$ be a non-trivial solution of the system (3). Let r be the smallest non-zero integer such that $z_j = 0$ for all $j \geq r+1$.

Then, the system (3) reduces to

$$\sigma_j(x_1)z_1 + \sigma_j(x_2)z_2 + ... + \sigma_j(x_r)z_r = 0 \qquad \ldots(4)$$

Since $z_r \neq 0$ and $z_r \in K$. Consider, $z_i^l = \dfrac{z_i}{z_r}$. Then, from (4), we get

$$\sigma_j(x_1)z_1^l + \sigma_j(x_2)z_2^l + ... + \sigma_j(x_{r-1})z_{r-1}^l + \sigma_j(x_r) = 0 \qquad \ldots(5)$$

for j = 1,2,…n.

Let for j = 1, $\sigma_1 = I$, we get from (5), that

$$x_1z_1^l + x_2z_2^l + ... + x_{r-1}z_{r-1}^l + x_r = 0 \qquad \ldots(6)$$

If all $z_1^l, z_2^l, ..., z_{r-1}^l$ are in F_0, then from (6), we get that $x_1, x_2, \ldots, x_r$ are L.D. over F_0, which is not possible.

Hence atleast one of z_i^l is not in F_0, say $z_1^l \notin F_0$.

Further, we get that $r \neq 1$, because if r = 1, then we get that $z_1^l = 1$ and so $z_1^l \in F_0$.

Since $z_1^l \notin F_0$, so there exists some $\sigma_i \in G$ such that $\sigma_i(z_1^l) \neq z_1^l$.

Applying $\sigma_i \in G$ to (5), to get

$$\sigma_i(\sigma_j(x_1)z_1^l) + \sigma_i(\sigma_j(x_2)z_2^l) + ... + \sigma_i(\sigma_j(x_{r-1})z_{r-1}^l) + \sigma_i(\sigma_j(x_r)) = 0$$

$$\Rightarrow \quad \sigma_i\sigma_j(x_1)\sigma_i(z_1^l) + \sigma_i\sigma_j(x_2)\sigma_i(z_2^l) + ... + \sigma_i\sigma_j(x_{r-1})\sigma_i(z_{r-1}^l) + \sigma_i\sigma_j(x_r) = 0$$

Since G is a group, the set $\{\sigma_i\sigma_1, \sigma_i\sigma_2, ..., \sigma_i\sigma_n\}$ coincide with the set $\{\sigma_1, \sigma_2, ..., \sigma_n\}$, though the order of elements will be different. So, we get

$$\sigma_j(x_1)\sigma_i(z_1^l) + \sigma_j(x_2)\sigma_i(z_2^l) + ... + \sigma_j(x_{r-1})\sigma_i(z_{r-1}^l) + \sigma_j(x_r) = 0 \quad ...(7)$$

Subtracting (7) from (5), we have

$$\sigma_j(x_1)\left[z_1^l - \sigma_i(z_1^l)\right] + \sigma_j(x_2)\left[z_2^l - \sigma_i(z_2^l)\right] + ... + \sigma_j(x_{r-1})\left[z_{r-1}^l - \sigma_i(z_{r-1}^l)\right] = 0$$

Put $t_k = z_k^l - \sigma_i(z_k^l)$. Then, the above system becomes

$$\sigma_j(x_1)t_1 + \sigma_j(x_2)t_2 + ... + \sigma_j(x_{r-1})t_{r-1} = 0$$

where $t_1 \neq 0$. Thus, (t_1, t_2, …, t_{r-1}, 0, 0, …, 0) is a non-trivial solution of given system, which is a contradiction to the choice of r. Therefore, $n \not< m$

So, m = n. Hence the proof.

2.5. Galois Extension. A finite extension K of a field F is said to be Galoi's extension of F if F is the fixed subfield of K under the group G(K, F) of all F-automorphisms of K i.e. K/F is Galoi's extension if $K_{G(K,F)} = F$.

2.5.1. Simple Extension. An extension K/F is said to be simple extension if K is generated by a single element over F.

2.5.2. Corollary. Let $K = F(\alpha)$ be a simple finite separable extension of F. Then, K is the splitting field of the minimal polynomial of α over F iff F is the fixed field under the group of all F-automorphisms of K, that is K is Galoi's extension of F.

Proof : Let $f(x)$ be the minimal polynomial of α over F and let degree $f(x) = m$.

Then $[K : F] = m$. Let $\alpha_1 = \alpha, \alpha_2, \alpha_3, \ldots, \alpha_r$ be the distinct conjugates of α in K.

Then $K = F(\alpha_i)$ for all $i = 1, 2, \ldots, r$. Since α and α_i are conjugates over F, so $\exists$ an isomorphism, say $\sigma_i : F(\alpha_1) \to F(\alpha_i)$ given by $\sigma_i(\alpha_1) = \alpha_i$ and $\sigma_i(\lambda) = \lambda$ for all $\lambda \in F$. But $K = F(\alpha_i)$ for all i, so we have that

$$\sigma_i : K \to K \text{ s.t. } \sigma_i(\alpha_1) = \alpha_i \text{ and } \sigma_i(\lambda) = \lambda \text{ for all } \lambda \in F.$$

Since α_1 generates K over F, each σ_i is uniquely determined. Further, we know for any F-automorphism σ of K, $\sigma_i(\alpha_1)$ is a conjugate of α_1 and hence $\sigma_i(\alpha_1) = \alpha_i$ for some α_i.

From this, it follows that $\sigma = \sigma_i$ for some i.

Hence the group $G(K, F)$ consists of $\sigma_1, \sigma_2, \ldots, \sigma_r$. Let F_0 be the fixed field under $G(K, F)$. Then by theorem 2.4.6.,

$$[K : F_0] = o[G(K, F)] = r.$$

So , $F = F_0$ if and only if $r = m$. Hence F is the fixed field under G if and only iff $f(x)$ has all m roots in K, that is, if and only if K is the splitting field of $f(x)$ over F.

2.5.3. Theorem. Let K be a finite extension of F and ch.F = 0. Then, K is normal extension of F iff the fixed field under G(K, F) is F itself, that is, K is Galoi's extension of F.

Proof. We know that any finite field extension of a field of characteristic zero is simple extension so K/F is a simple extension. So , let $K = F(\alpha)$ for some $\alpha \in K$.

Now, suppose that K is a normal extension of F. Then, by definition, every irreducible polynomial over F having one root in K splits into linear factors over K. Since $[K : F]$ is finite , so α is algebraic over F. Let $f(x)$ be minimal polynomial of α over F and K' be its splitting field over F. Then $K' \subseteq K$. Also, $\alpha \in K'$, $F \subseteq K'$

$$\Rightarrow \quad K \subseteq K'.$$

So $K = K'$ i.e. K is splitting field of $f(x)$ over F. Hence, by corollary 2.5.2., F is itself fixed subfield under $G(K , F)$, that is, K/F is Galois extension.

Conversely, suppose that F is itself the fixed subfield under $G(K, F)$. Again, by corollary 2.5.2., K is the splitting field of the minimal polynomial of α over F. Further we know that if K is a finite algebraic extension of a field F iff K is the splitting field of some non-zero polynomial over F. Hence K is a normal extension of F.

2.5.4. Fundamental Theorem of Galoi's Theory.

Given any subfield E of K containing F and subgroup H of G(K, F)

(i) $E = K_{G(K,E)}$

(ii) $H = G(K, K_H)$

(iii) [K : E] = o(G(K, E)) and [E : F] = index of G(K, E) in G(K, F)

(iv) E is a normal extension of F iff G(K, E) is a normal subgroup of G(K, F)

(v) when E is a normal extension of F, then

$$G(E,F) \cong {G(K,F)}\big/{G(K,E)}.$$

Proof. (i) Since K is a finite normal extension of F and $F \subseteq E \subseteq K$, we must have that K is a finite normal extension of E. so, by above theorem fixed field under G(K, E) is E itself, that is E = G(K, E).

(ii) By definition, $K_H = \{x \in K : \sigma(x) = x \ \forall \ \sigma \in H\}$, that is each element of K_H remains invariant under every automorphisms of H. So, clearly, we have

$$H \subseteq G(K, K_H)$$

Now, we know that if F_0 is fixed subfield under subgroup G, then $[K : F_0] = o(G)$.

Here K_H is fixed subfield under H, so we must have $[K: K_H] = o(H)$ …(1)

Now, K is normal extension of K_H, so K_H is fixed subfield under $G(K, K_H)$, by above theorem. So again we have

$$[K : K_H] = o(G(K, K_H)) \qquad \ldots(2)$$

By (1) and (2), we obtain

$$O(H) = o(G(K, K_H))$$

So, $\quad H = G(K, K_H)$

(iii) Since K|F and K|E both are finite normal extensions, so by above theorem fixed field under G(K, F) and G(K, E) are F and E respectively.
Hence [K : E] = o(G(K, E)) and [K : F] = o(G(K, F))

Now, [K : F] = [K : E][E : F]

So $\quad [E:F]=\dfrac{[K:F]}{[K:E]}=\dfrac{o(G(K:F))}{o(G(K:E))}=$ index of G(K, E) in G(K, F)

(iv) Let E be a normal extension of F. Then, E is algebraic extension of F. Let $a \in E$, then 'a' is algebraic over F. Let p(x) be the minimal polynomial of 'a' over F. Then, E|F being normal and E contains a root of p(x), then all roots of p(x) are in F.
Hence E contains all the conjugates of 'a' over F. Let $\sigma \in G(K,F)$, then $\sigma(a)$ is a conjugate of 'a' and hence $\sigma(a) \in E$.
Let $\eta \in G(K,E)$ then $\eta : K \to K$ such that $\eta(\lambda)=\lambda$ for all $\lambda \in E$. In particular,

$$\eta(\sigma(a))=\sigma(a) \qquad [\sigma(a)\in E]$$

$$\Rightarrow \quad \sigma^{-1}(\eta(\sigma(a)))=\sigma^{-1}\sigma(a)=a \quad \Rightarrow \quad (\sigma^{-1}\eta\sigma)(a)=a \quad \Rightarrow \quad \sigma^{-1}\eta\sigma \in G(K,E)$$

Hence $G(K,E)\,\Delta\, G(K,F)$.
Conversely, let $G(K,E)\,\Delta\, G(K,F)$.
We shall prove that E is a normal extension of F.
Let $a \in E \subseteq K \quad \Rightarrow \quad a \in K$ and K is normal extension of F.
Therefore, K contains all the roots of minimal polynomial p(x) of 'a' over F. Equivalently, if L is the splitting field of p(x) over F, then $L \subseteq K$.
Let b be any other root of p(x), then $b \in L \subseteq K$ and b is a conjugate of 'a' over F. Hence there exists an isomorphism $\sigma : K \to K$ such that

$$\sigma(a)=b \text{ and } \sigma(\lambda)=\lambda \text{ for all } \lambda \in F$$

Let $\eta \in G(K,E)$, then $\sigma^{-1}\eta\sigma \in G(K,E)$. Therefore,

$$\sigma^{-1}\eta\sigma(a)=a \quad \Rightarrow \quad \eta(\sigma(a))=\sigma(a) \quad \Rightarrow \quad \eta(b)=b \text{ for all } \eta \in G(K,E)$$

But E is fixed under G(K, E), therefore, we get

$$b=\sigma(a)\in E \quad \Rightarrow \quad b \in E \quad \Rightarrow \quad L \subseteq E$$

Thus, E is normal extension of F.
(v) Let E be a normal extension of F. Then, E = F(a) for some $a \in E$. For any $\sigma \in G(K,F)$, let σ_E denotes the restriction of σ to E. Since $\sigma(a) \in E$, we get $\sigma(E) \subseteq E$.

But $[\sigma(E):F]=[E:F]$. Therefore, we get $\sigma(E)=E$. Hence σ_E is an F-automorphism of E and so $\sigma_E \in G(E,F)$.

Define a mapping $\lambda : G(K,F) \to G(E,F)$ by setting

$$\lambda(\sigma)=\sigma_E \text{ for all } \sigma \in G(K,F)$$

Clearly, for any $\sigma, \eta \in G(K,F)$, we have

$$\lambda(\sigma\eta)=(\sigma\eta)_E=\sigma_E\eta_E=\lambda(\sigma)\lambda(\eta)$$

Hence λ is a group homomorphism.

Consider any $\gamma \in G(E,F)$. Now, $\gamma(a)$ is a conjugate of 'a' over F. Thus, there exists an F-automorphism σ on K such that $\sigma(a)=\gamma(a)$.

Further, as σ and η are both identity of F and E is generated by 'a' over F. We get

$$\sigma(x)=\gamma(x) \text{ for all } x \in F(a)=E \quad \Rightarrow \quad \gamma=\sigma_E=\lambda(\sigma)$$

This proves λ is onto mapping. Hence

$$G(E,F) \cong G(K,F)/Ker\lambda$$

Now, if $\lambda \in Ker\lambda$ iff σ_E is identity on E iff $\sigma(x)=x$ for all $x \in E$ iff $\sigma \in G(K,E)$.

Hence $Ker\lambda = G(K,E)$ and we obtain

$$G(E,F) \cong G(K,F)/G(K,E).$$

2.5.5. Example. Determining Galois group of splitting field of x^4+1 over Q.

Solution. Roots of x^4+1 over Q are

$$x = e^{\frac{(2m+1)\pi i}{4}}, \quad m = 0, 1, 2, 3$$

$$= e^{\frac{\pi i}{4}}, e^{\frac{3\pi i}{4}}, e^{\frac{5\pi i}{4}}, e^{\frac{7\pi i}{4}}$$

Let $\quad a = e^{\frac{\pi i}{4}}$,

Then roots are $\quad x = a, a^3, a^5, a^7$

Therefore, splitting field K of x^4+1 over Q is given by

$$K = Q(a, a^3, a^5, a^7) = Q(a).$$

Clearly, x^4+1 is irreducible over Q, so it is minimal polynomial of x^4+1 over Q.

Now, $\quad [K : Q] = [Q(a) : Q]$

$\quad = $ degree of minimal polynomial of 'a' over Q

$\quad = $ degree $(x^4+1) = 4$

Since K is splitting field of some non-zero polynomial over Q, so K must be normal extension of Q. Also, char$Q$ = 0, so we must have that the fixed field under the Galois group $G(K, Q)$ is Q itself.

So, we must have $\quad o(G(K,Q)) = [K : Q] = 4$

Now , $K = Q(a)$ and $[K : Q] = 4$

so $\{1, a, a^2, a^3\}$ must be a basis of K over Q. If $y \in K$ be any arbitrary element, then

$$y = \alpha_0.1 + \alpha_1 . a + \alpha_2 . a^2 + \alpha_3 . a^3 \quad , \quad \alpha_i \in Q \, , \quad 0 \le i \le 3.$$

and
$$\sigma(y) = \sigma(\alpha_0.1) + \sigma(\alpha_1 . a) + \sigma(\alpha_2 . a^2) + \sigma(\alpha_3 . a^3)$$
$$= \alpha_0 + \alpha_1 \sigma(a) + \alpha_2 (\sigma(a))^2 + \alpha_3 (\sigma(a))^3$$

Hence any $\sigma \in G(K , Q)$ is determined by its effect on 'a'.

Now, $\sigma(a)$ must be a conjugate of 'a' and $G(K, Q)$ contains four elements, so we must have

$G(K , Q) = \{\sigma_1 , \sigma_2 , \sigma_3 , \sigma_4\}$, where $\sigma_1(a) = a$, $\sigma_2(a) = a^3$, $\sigma_3(a) = a^5$, $\sigma_4(a) = a^7$.

Now, $G(K, Q)$ is a group of order four means that either it is a cyclic group of order 4 or it is isomorphic to Klein's group.

We observe that $\sigma_1(a) = a \quad \Rightarrow \quad \sigma_1 = I$ and $\sigma_2^2(a) = \sigma_2(\sigma_2(a)) = a^9 = a$

$$\sigma_3^2(a) = \sigma_3(\sigma_3(a)) = a^{25} = a \quad \text{and} \quad \sigma_4^2(a) = \sigma_4(\sigma_4(a)) = a^{49} = a$$

Hence, $\sigma_2^2 = \sigma_3^2 = \sigma_4^2 = I$.

So, the Galois group $G(K, Q)$ contains no element of order 4 which in turn implies that

$G(K, Q)$ is isomorphic to Klein's four group.

2.6. Norms and Traces.

Let E be a finite separable extension of degree n over the subfield F and K be a normal closure of E over F. Then, there are exactly n distinct F-monomorphisms, say, $\tau_i, 1 \le i \le n$, of E into K. Consider the mappings $N_{E/F}$ and $S_{E/F}$ of E into K as:

$$N_{E/F}(x) = \prod_{i=1}^{n} \tau_i(x), \qquad S_{E/F}(x) = \sum_{i=1}^{n} \tau_i(x),$$

for every $x \in E$ and $1 \le i \le n$.

Then, $N_{E/F}(x)$ and $S_{E/F}(x)$ are known as norm and trace respectively of x from E to F.

The next theorem, indicates why to use "of x from E to F" in the definition of norm and trace.

2.6.1. Theorem. Norm, $N_{E/F}(x)$ is a homomorphism of the group $E^* = E-\{0\}$ of the field E into the group $F^* = F-\{0\}$ of the field F. Also, the trace $S_{E/F}$ is a non-zero homomorphism of the additive group E of the field E into the additive group F of F.

Proof. For justifying that these mappings are homomorphisms on the said structures, consider $x, y \in E$, then

$$N_{E/F}(xy) = \prod_{i=1}^{n} \tau_i(xy) = \prod_{i=1}^{n} \tau_i(x)\tau_i(y) = \prod_{i=1}^{n} \tau_i(x) \prod_{i=1}^{n} \tau_i(y) = N_{E/F}(x) N_{E/F}(y)$$

and,

$$S_{E/F}(x+y)=\sum_{i=1}^{n}\tau_i(x+y)=\sum_{i=1}^{n}\left(\tau_i(x)+\tau_i(y)\right)=\sum_{i=1}^{n}\tau_i(x)+\sum_{i=1}^{n}\tau_i(y)=S_{E/F}(x)+S_{E/F}(y)$$

Further, if τ is any F-automorphism of K, then, for $x\in E$, the mappings ρ_i, $1 \leq i \leq n$, of E into K defined by $\rho_i(x)=\tau(\tau_i(x))$ are clearly n distinct F- monomorphisms of E into K and so $\{\rho_1,\rho_2,...,\rho_n\} = \{\tau_1,\tau_2,...,\tau_n\}$, might be with different order. Let x be any arbitrary element of E, then

$$\tau\left(N_{E/F}(x)\right)=\tau\left(\prod_{i=1}^{n}\tau_i(x)\right)=\prod_{i=1}^{n}\tau\tau_i(x)=\prod_{i=1}^{n}\rho_i(x)=N_{E/F}(x)$$

and $$\tau\left(S_{E/F}(x)\right)=\tau\left(\sum_{i=1}^{n}\tau_i(x)\right)=\sum_{i=1}^{n}\tau\tau_i(x)=\sum_{i=1}^{n}\rho_i(x)=S_{E/F}(x).$$

Therefore, norm and trace of x belong to the fixed field under G(K,F). Since K is a normal closure of a seperable extension, so it is finite separable normal extension of F. Hence it follows that the fixed field under G(K,F) is F itself. Hence $N_{E/F}(x), S_{E/F}(x)\in F$.

Now, we only need to prove that $S_{E/F}$ is not the zero homomorphism. On the contrary assume that

$$S_{E/F}(x)=\sum_{i=1}^{n}\tau_i(x)=0, \qquad \text{for all } x\in E$$

However, it concludes that the set $\{\tau_1,\tau_2,...,\tau_n\}$ of distinct monomorphisms of E into K is linearly dependent over K, which in turn contradicts as we already have proved the result “If E and K be any two fields, then every set of distinct monomorphisms of E into K is linearly independent”. Hence the proof.

Now consider two possibilities:

1. Let D be a finite separable extension of subfield F and E be a subfield of D, containing F. Then D is a separable extension of E and E is a separable extension of F. Thus if x is any element of D, define the norm $N_{D/E}(x)$ of x from D to E, which is an element of E as obtained in Theorem 1, and then define the norm of $N_{D/E}(x)$ from E to F, which is an element of F.
2. Also, define the norm of x from D to F.

The next theorem shows that these two procedures lead to the same element of F.

2.6.2. Theorem. Let D be a finite separable extension of a subfield F and E be a subfield of D containing F. Then, for every x $\in$ D,

i) $N_{E/F}(N_{D/E}(x)) = N_{D/F}(x)$

ii) $S_{E/F}(S_{D/E}(x)) = S_{D/F}(x)$.

Proof. Let K be a normal closure of D over F and [E : F] = n, [D : E] = m, then due to tower law, [D : F] = mn. Thus, there are exactly n distinct F-monomorphisms $\sigma_1,\ldots,\sigma_n$ (say) of E into K and m distinct E-monomorphisms $\tau_1, \ldots, \tau_m$ (say) of D into K. Extending $\sigma_1,\ldots,\sigma_n$ from E to K, we can obtain n distinct F-automorphisms $\sigma_1^{'},\sigma_2^{'},...,\sigma_n^{'}$ of K which act like $\sigma_1,\ldots,\sigma_n$ on E.

Let φ_{ij}(i = 1,…, n; j = 1,…., m) be the mappings of D into K defined by

$$\varphi_{ij}(x) = \sigma_i^{'}(\tau_j(x)) \text{ for all } x \in D.$$

These mn mappings are distinct F-monomorphisms of D into K and hence they form a complete set of F-monomorphisms of D into K. If $x \in D$, then we have

$$N_{D/F}(x) = \prod_{\substack{1\le i\le n\\ 1\le j\le m}} \phi_{ij}(x) = \prod_{\substack{1\le i\le n\\ 1\le j\le m}} \sigma_i^{'}\left(\tau_j(x)\right) = \prod_{1\le i\le n} \sigma_i^{'}\left(\prod_{1\le j\le m} \tau_j(x)\right)$$
$$= \prod_{1\le i\le n} \sigma_i^{'}\left(N_{D/E}(x)\right) = \prod_{1\le i\le n} \sigma_i\left(N_{D/E}(x)\right) = N_{E/F}\left(N_{D/E}(x)\right)$$

Similarly, we can derive the result for traces also.

2.7. Check Your Progress.

1. Consider F = **Q** and E = **Q(i),** define norm and trace for this structure.
2. Find the Galois group of $x^3 - 2$ over Q.

2.8. Summary.

In this chapter, we have derived results related to normal extensions and observed that finite algebraic extension is normal if it becomes splitting field of a non-zero polynomial

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 editioin, 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.

3

Galois Fields

Structure

3.1. Introduction. In this chapter, we shall discuss about finite fields, cyclic and cyclotomic extensions. Also it will be derived that a field of composite order does not exist. Further, the relation between finite division rings and finite fields is obtained.

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

(i) Normal bases.

(ii) Cyclic and Cyclotomic Extensions.

(iii) Cyclotomic Polynomials.

3.1.2. Keywords. Galois Field, Normal Extensions, Splitting Fields.

3.2. Galois Field. A field is said to be Galois field if it is finite.

3.2.1. Theorem. Let F be a field having q elements and ch.F = p, where p is a prime number. Then, q = p^n for some integer $n \geq 1$.

Proof. Let P be the prime subfield of F. Now, we know that upto isomorphism there are only two prime fields, one is Q and other is Z_p. Since P is finite prime field. So, P must be isomorphic to Z_p. Hence P must have p elements. Now, F is a finite field and $P \subseteq F$ so F is a finite dimensional vector space over P.

Let [F : P] = n(say) and let $\{a_1, a_2, \ldots, a_n\}$ be a basis of F over P. Then, each element of F can be written uniquely as

$$\lambda_1 a_1 + \lambda_2 a_2 + ... + \lambda_n a_n \text{ where } \lambda_i \in P .$$

As each λ_i can be choosen in p ways, the total number of elements of F is p^n.

So, we have q = p^n for some integer $n \geq 1$.

Remark. In the other direction of above theorem, we shall show that for every prime p and integer $n \geq 1$, there exists a field having p^n elements. First we prove a lemma:

3.2.2. Lemma. If a field F has q elements, then F is the splitting field of $f(x) = x^q - x \in P[x]$, where P is the prime subfield of F.

Proof. We know that the set of all non-zero elements of a field form an abelian group w.r.t. multiplication. So, F* = F – {0} is a multiplicative abelian group. Now, we are given that o(F) = q. Therefore, o(F*) = q-1.

Now, let λ be an arbitrary element of F*. Then,

$$\lambda^{q-1} = 1$$

where 1 is the multiplicative identity of F. Thus,

$$\lambda\lambda^{q-1} = \lambda \quad \Rightarrow \quad \lambda^q = \lambda \quad \Rightarrow \quad \lambda^q - \lambda = 0$$

That is, λ satisfies the polynomial $f(x) = x^q - x$. Therefore, all the elements of F* are root of $f(x) = x^q - x$. Also, f(0) = 0 and so

$$f(\lambda) = 0 \quad \text{for all } \lambda \in \mathrm{F}$$

Since f(x) is of degree q, so it cannot have more than q roots in any extension of P. Thus, F is the smallest extension of P containing all the roots of f(x).

Hence F is the splitting field of f(x) over P.

Remark. In above lemma, we have proved that every finite field is splitting field of some non-zero polynomial.

3.2.3. Theorem. For every prime p and integer $n \geq 1$, there exists a field having p^n elements.

Proof. Since p is a prime number. Therefore, $Z_p = \{0, 1, \ldots, p-1\}$ is a field w.r.t. $+_p$ and x_p and is also a prime field. Consider the polynomial

$$f(x) = x^{p^n} - x \in Z_p[x]$$

Let K be the splitting field of f(x). Then, K contain all the roots of f(x).

Since degree of f(x) is p^n, so f(x) has p^n roots in K. Let these roots be $a_1, a_2, \ldots, a_{p^n}$. Then, we can write

$$x^{p^n} - x = \prod_{i=1}^{p^n} (x - a_i) \qquad \text{where } a_i \in K.$$

Let $T = \{a \in K : a^{p^n} = a\}$. Then, $T \neq 0$, because $0 \in T$ as $0^{p^n} = 0$ and $0 \in K$.

Now, $1 \in K$ and $1^{p^n} = 1 \quad \Rightarrow \quad 1 \in T$.

Let $k \in Z_p$ be any arbitrary element. Then, k = 1+1+…+1 (k-times). Therefore,

$$k^{p^n} = (1+1+\ldots+1)^{p^n} = 1^{p^n} + 1^{p^n} + \ldots + 1^{p^n} = 1+1+\ldots+1 = k \qquad [ch.F = p]$$

$$\Rightarrow \quad k \in T$$

So, every element of Z_p is in T, that is, T contains prime field Z_p of K. Further, consider a_i any root of f(x). Then,

$$f(a_i) = 0 \;\Rightarrow\; a_i^{p^n} - a_i = 0 \;\Rightarrow\; a_i^{p^n} = a_i \;\Rightarrow\; a_i \in T$$

Thus, T also contains all the roots of f(x).

We claim that T is a subfield of f(x).

Let $\alpha, \beta \in T$. Then, $\alpha^{p^n} = \alpha$ and $\beta^{p^n} = \beta$. Now,

$$(\alpha - \beta)^{p^n} = \alpha^{p^n} - \beta^{p^n} - 0 = \alpha - \beta \quad \Rightarrow \quad \alpha - \beta \in T$$

and $\quad (\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n} = \alpha\beta \quad \Rightarrow \quad \alpha\beta \in T$.

Thus, T is a subfield of K. So, $T \subseteq K$.

So, we have T is a field which contains all the roots of f(x). But K is splitting field of f(x). So, $K \subseteq T$. Thus, we have K = T.

Now, if $\lambda \in T$, then $\lambda^{p^n} = \lambda \;\Rightarrow\; \lambda^{p^n} - \lambda = 0 \;\Rightarrow\; f(\lambda) = 0$

Thus, every element of T is a root of f(x).

Therefore, $T = \{a_1, a_2, \ldots, a_{p^n}\}$.

Now, we claim that all these elements are distinct.

We have $f(x) = x^{p^n} - x$. Any root a_i of f(x) is a multiple root of $f(x)$ iff a_i is a root of $f'(x)$. But

$$f'(x) = p^n x^{p^n - 1} - 1 = -1 \qquad \because ch.Z_p = p$$

So, a_i is not a root of $f'(x)$. Therefore, no root of f(x) is a multiple root. So, all elements of T are distinct. Hence

$$o(T) = p^n = o(K).$$

Thus, we have obtained a field of order p^n.

3.2.4. Theorem. Finite fields having same number of elements are isomorphic.

Proof. Let K_1 and K_2 be finite fields such that $o(K_1) = o(K_2)$.

Let $ch.K_1 = p_1$ and $ch.K_2 = p_2$, where p_1 and p_2 are primes. Then, we have

Then, we have $o(K_1) = p_1^{n_1}$ and $o(K_2) = p_2^{n_2}$ for some integers n_1 and n_2. So, we have

$$p_1^{n_1} = p_2^{n_2} \quad \Rightarrow \quad p_1 = p_2 = p(\text{say}) \text{ and } n_1 = n_2 = n(\text{say})$$

Let P_1 and P_2 are prime subfields of K_1 and K_2 respectively. Then,

$$P_1 \cong Z/\langle p \rangle \cong P_2. \text{ So, } P_1 \cong P_2$$

By previous lemma, K_1 is the splitting field of the polynomial $f(x) = x^{p^n} - x \in P_1[x]$.

Now, $P_1 \cong P_2$ so $P_1[x] \cong P_2[x]$.

Let $f'(t)$ be the corresponding polynomial of f(x) and $f'(t) = t^{p^n} - t \in P_2[t]$.

Again, by previous lemma, K_2 is the splitting field of the polynomial $f'(t) \in P_2[t]$.

But $P_1 \cong P_2$. Therefore, splitting field will also be isomorphic, that is, $K_1 \cong K_2$.

3.2.5. Theorem. A field is finite iff $F^* = F - \{0\}$ is a multiplicative cyclic group.

Proof. Let F be a finite field with q elements. Then, $F^* = F - \{0\}$ is a multiplicative group with (q – 1) elements.

We claim that F^* contains elements having order (q - 1).

Since F^* is a finite group, so if $\lambda \in F^*$, then by Lagrange's theorem

$$\lambda^{o(F^*)} = 1 \quad \text{for all } \lambda \in F^*$$

That is, multiplicative order of each element is finite, so let 'n' be the least positive integer such that

$$\lambda^n = 1 \quad \text{for all } \lambda \in F^*$$

Then, $n \le q - 1$.

Now, consider the polynomial $f(x) = x^n - 1$.

Then, $f(\lambda)=\lambda^n-1=0 \Rightarrow \quad \lambda$ satisfies f(x) for all $\lambda \in F^*$.

But f(x) is of degree n, it can have atmost n roots. Also, all elements of F* are roots of f(x). Therefore, $o(F^*)\le n \quad \Rightarrow \quad q-1\le n$.

Hence there exists atleast one element $\lambda \in F^*$ such that $o(\lambda)=o(F^*)=q-1$.

Therefore, F* is cyclic.

Conversely, suppose that F* is cyclic. Let F* = < a >.

If a = 1, then o(F*) = o(a) = o(1) = 1. So, F = {0, 1} is finite.

So, let us assume that $a\ne 1$.

Case I. $ch.F=0$

Since $1\in F^* \quad \Rightarrow \quad -1\in F^*$. Therefore, $-1=a^n$ for some integer n.

W.L.O.G., let $n\ge 1$, then

$a^{2n}=1 \ \Rightarrow \ o(a)\le 2n \ \Rightarrow \ o(a)$ is finite $\ \Rightarrow \ o(F^*)$ is finite $\ \Rightarrow \ o(F)$ is finite.

Since Ch.F = 0, then prime subfield P of F is such that $P\subseteq F$ and $P\cong Q$, a contradiction, as $o(Q)=\infty$ and $o(P)<\infty$.

Hence this case is not possible.

Case II. $ch.F\ne 0$

Then, we must have ch.F = p for some prime p.

Let P be the subfield of F, then $P\cong Z_p$ and o(P) = p. Since $a\ne 1,\ a-1\in F$

$\Rightarrow \quad a-1\in F^*=<a> \quad \Rightarrow \quad a-1=a^n$ for some integer n $\quad \Rightarrow \quad a^n-a+1=0$.

Thus, ‘a’ satisfies the polynomial f(x) = $x^n - x - 1$ over P[x] and hence ‘a’ is algebraic over P.

Then, [P(a) : P] = degree of minimal polynomial of ‘a’ over P = r (say)

Therefore, P(a) is a vector space over P of dimension r. Thus, $P(a)\cong P^{(r)}=\{(\alpha_1,\alpha_2,...,\alpha_r):\alpha_i\in P\}$.

But $o(P)=p \quad \Rightarrow \quad o(P^{(r)})=p^r \quad \Rightarrow \quad o(P(a))=p^r$. Now, F* = < a > and $a\in P(a)$.

$\Rightarrow \quad F^*\subseteq P(a) \quad \Rightarrow \quad \mathrm{o}(F^*)\le o(P(a)) \quad \Rightarrow \quad \mathrm{o}(F^*)<\infty$.

Therefore, o(F*) is finite.

Remark. The above theorem may not be true when a field F is infinite. We give an example of field of rational numbers. Let $Q^*=\{\alpha\in Q:\alpha\ne 0\}$.

We shall prove that the multiplicative group Q* is not cyclic.

Let, if possible, Q* is cyclic. So, let g be its generator, that is, Q* = < g >, where

$$g = \frac{p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}}{q_1^{\beta_1} q_2^{\beta_2} ... q_t^{\beta_t}}$$

where p_i's and q_i's are distinct primes.

Now since $1 \in Q^*$, so there must exist a positive integer n such that

$$1 = g^n = \left(\frac{p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}}{q_1^{\beta_1} q_2^{\beta_2} ... q_t^{\beta_t}} \right)^n \quad \Rightarrow \quad p_1^{n\alpha_1} p_2^{n\alpha_2} ... p_r^{n\alpha_r} = q_1^{n\beta_1} q_2^{n\beta_2} ... q_t^{n\beta_t}$$

which is a contradiction, since p_i's and q_i's are distinct primes. Hence Q* is not cyclic.

Remark. In view of the above remark, we can say that R* and C* are not cyclic because every subgroup of a cyclic group is cyclic and Q* is not cyclic.

3.3. Normal Bases. Let K be a finite separable normal extension of a subfield F and

$$G(K, F) = \{\tau_1, \tau_2, ..., \tau_n\}$$

be the Galois group of K over F. If $x \in K$, then a basis of the form $\{\tau_1(x), \tau_2(x), ..., \tau_n(x)\}$ for K over F is called a normal basis of K over F.

3.3.1. Theorem. Let K be a finite separable normal extension of degree n over a subfield F with Galois group $G(K, F) = \{\tau_1, \tau_2, ..., \tau_n\}$. The subset $\{x_1, x_2, ..., x_n\}$ of K is a basis for K over F if and only if the matrix

$$\left(\tau_i(x_j)\right) = \begin{pmatrix} \tau_1(x_1) & \tau_1(x_2) & \cdots & \tau_1(x_n) \\ \tau_2(x_1) & \tau_2(x_2) & ... & \tau_2(x_n) \\ \vdots & & \ddots & \vdots \\ \tau_n(x_1) & \tau_n(x_2) & \cdots & \tau_n(x_n) \end{pmatrix}$$

is non-singular.

Proof. Suppose first that the matrix $\left(\tau_i(x_j)\right)$ is non-singular.

Since [K : F] = n, so it is enough to show that the set $\{x_1, x_2, ..., x_n\}$ is linearly independent over F. For this, consider

$$a_1x_1 + a_2x_2 + ... + a_nx_n = 0$$

where $a_i, 1 \le i \le n,$ are elements of F.

Applying the F-automorphisms $\tau_1, \tau_2, ..., \tau_n$, to obtain

$$\begin{array}{lll} a_1\tau_1(x_1) + a_2\tau_1(x_2) + ... + a_n\tau_1(x_n) = 0 \\ a_1\tau_2(x_1) + a_2\tau_2(x_2) + ... + a_n\tau_2(x_n) = 0 \\ . \qquad\qquad . \qquad\qquad . \\ . \qquad\qquad . \qquad\qquad . \\ . \qquad\qquad . \qquad\qquad . \\ a_1\tau_n(x_1) + a_2\tau_n(x_2) + ... + a_n\tau_n(x_n) = 0, \end{array}$$

which is a homogeneous system of equations in unknowns $a_i, 1 \le i \le n,$ with non-singular matrix of coefficients $\left(\tau_i(x_j)\right)$. It follows from the theory of homogeneous linear equations that $a_1 = a_2 = ... = a_n = 0$. Thus $\{x_1, x_2, ..., x_n\}$ is linearly independent and so forms a basis, as required.

Next, suppose that the matrix $\left(\tau_i(x_j)\right)$ is singular.

Again, due to the theory of homogeneous linear equations, it follows that there exist a non-trivial solution for the system

$$\begin{array}{l} a_1\tau_1(x_1) + a_2\tau_1(x_2) + ... + a_n\tau_1(x_n) = 0 \\ a_1\tau_2(x_1) + a_2\tau_2(x_2) + ... + a_n\tau_2(x_n) = 0 \\ . \qquad\qquad\qquad . \qquad\qquad\qquad . \\ . \qquad\qquad\qquad . \qquad\qquad\qquad . \\ . \qquad\qquad\qquad . \qquad\qquad\qquad . \\ a_1\tau_n(x_1) + a_2\tau_n(x_2) + ... + a_n\tau_n(x_n) = 0, \end{array}$$

in K, say, $\alpha_1, \alpha_2, ..., \alpha_n$. Since trace is a non-zero homomorphism, so there exists an element α of K such that $S_{K/F}(\alpha)$ is non-zero. If α_k is non-zero, we multiply the above system of equations by $\alpha\alpha_k^{-1}$ to obtain:

$$\begin{array}{l} \beta_1\tau_1(x_1) + \beta_2\tau_1(x_2) + ... + \beta_n\tau_1(x_n) = 0 \\ \beta_1\tau_2(x_1) + \beta_2\tau_2(x_2) + ... + \beta_n\tau_2(x_n) = 0 \\ . \qquad\qquad\qquad . \qquad\qquad\qquad . \\ . \qquad\qquad\qquad . \qquad\qquad\qquad . \\ . \qquad\qquad\qquad . \qquad\qquad\qquad . \\ \beta_1\tau_n(x_1) + \beta_2\tau_n(x_2) + ... + \beta_n\tau_n(x_n) = 0, \end{array}$$

where $\beta_j = \alpha\alpha_k^{-1}\alpha_j$ (j = 1, …, n). Applying the F-automorphisms $\tau_1^{-1}, \tau_2^{-1}, ..., \tau_n^{-1}$ to the above equations respectively, to obtain

$$\begin{array}{l} \tau_1^{-1}(\beta_1)x_1 + \tau_1^{-1}(\beta_2)x_2 + ... + \tau_1^{-1}(\beta_n)x_n = 0 \\ \tau_2^{-1}(\beta_1)x_1 + \tau_2^{-1}(\beta_2)x_2 + ... + \tau_2^{-1}(\beta_n)x_n = 0 \\ . \qquad\qquad\qquad . \qquad\qquad\qquad . \\ . \qquad\qquad\qquad . \qquad\qquad\qquad . \\ . \qquad\qquad\qquad . \qquad\qquad\qquad . \\ \tau_n^{-1}(\beta_1)x_1 + \tau_n^{-1}(\beta_2)x_2 + ... + \tau_n^{-1}(\beta_n)x_n = 0, \end{array}$$

Adding all these equations, as τ_i runs through the group G, so does τ_i^{-1}. we deduce that

$$S_{K/F}(\beta_1)x_1 + \ldots + S_{K/F}(\beta_n)x_n = 0.$$

As $S_{K/F}(\beta_k)$ is a member of F and $\beta_k = \alpha\alpha_k^{-1}\alpha_k = \alpha$, so $S_{K/F}(\beta_k) = S_{K/F}(\alpha)$ is non zero, hence the set $\{x_1, x_2, ..., x_n\}$ is linearly dependent over F and so it does not form a basis, a contradiction to the assumption. Hence the result follows.

3.3.2. Corollary. The collection $\{\tau_1(x), \tau_2(x), ..., \tau_n(x)\}$, images of an element x under the automorphisms in the Galois group $G(K,F) = \{\tau_1, \tau_2, ..., \tau_n\}$, form a normal basis if and only if the matrix $(\tau_i\tau_j(x))$ is non-singular.

Next result proves that every separable normal extension of finite degree has a normal basis. However, we will prove the result for an infinite field first.

Before starting the main result we are defining some terms:

1. If K is any field, then $P_n(K)$ represents the collection of all polynomials in n indeterminates with scalars from the field K.
2. If K is any field and f(x) is a polynomial over F, for $\alpha \in K$, we define $\sigma_\alpha(f) = f(\alpha)$. Further, if $f \in P_n(F)$, means it is a polynomial in n inderminates, say $x_1, x_2, ..., x_n$, then for any n-tuple $\alpha = (\alpha_1, \alpha_2, ..., \alpha_n)$ we can obtain $\sigma_\alpha(f)$ by replacing x_i with α_i for $1 \le i \le n$.

3.3.3. Theorem. Let K be some extension of an infinite subfield F and f be a non-zero polynomial in $P_n(K)$. Then there are infinitely many ordered n-tuples $\alpha = (\alpha_1, \alpha_2, ..., \alpha_n)$ of elements of F such that $\sigma_\alpha(f) \neq 0$.

Proof. Mathematical induction on n is applied to obtain the required result.

For n = 1, let f(x) be a polynomial of degree d in P(K) = K[x]. Then f can have at most d roots in F (as obtained earlier in Section - I), and so there are infinitely many elements in F which does not satisfy f(x), that is, $f(\alpha) \neq 0$ or $\sigma_\alpha(f) \neq 0$ for infinitely many α in F.

Now assume that result holds for n = k, that is, if g is any polynomial in $P_k(K)$ then there are infinitely many ordered k-tuples $\beta = (\beta_1, \beta_2, ..., \beta_k)$ of elements of F such that $\sigma_\beta(g) \neq 0$.

Consider n = k+1, and let f be any non-zero polynomial in $P_{k+1}(K) = P(P_k(K))$, so we may express f in the form

$$f = g_0 + g_1x_{k+1} + g_2x_{k+1}^2 + ... + g_tx_{k+1}^t,$$

where $g_0, g_1, g_2, ..., g_t$ are polynomials in $P_k(K)$. Since f is a non-zero polynomial, at least one of the polynomials $g_0, g_1, g_2, ..., g_t$ must be non-zero, say, g_i. According to the induction hypothesis, there are infinitely many ordered k-tuples $\beta = (\beta_1, \beta_2, ..., \beta_k)$ of elements of F such that $\sigma_\beta(g_i) \neq 0$. For each of these k-tuples $\beta = (\beta_1, \beta_2, ..., \beta_k)$, the polynomial

$$f_\beta = \sigma_\beta(g_0) + \sigma_\beta(g_1)x_{k+1} + \sigma_\beta(g_2)x_{k+1}^2 + ... + \sigma_\beta(g_t)x_{k+1}^t$$

is a non-zero polynomial in P(K). Now following the similar lines as for n = 1, we conclude that there are infinitely many elements δ of F such that $\sigma_\delta(f_\beta) \neq 0$. But if we set $\alpha = (\beta_1, \beta_2, ..., \beta_k, \delta)$ it is clear that $\sigma_\alpha(f) = \sigma_\delta(f_\beta)$.

Hence we see that the result is true for n = k+1. This completes the induction.

3.3.4. Theorem. Let K be a finite separable normal extension of degree n over an infinite subfield F. Let $G(K,F) = \{\tau_1, \tau_2, ..., \tau_n\}$ be the Galois group of K over F. If f is a polynomial in $P_n(K)$ with indeterminates $X_1, X_2, ..., X_n$ such that, for every $\alpha \in K$, $\sigma_{\tau(\alpha)}(f) = 0,$ where, $\tau(\alpha) = (\tau_1(\alpha), \tau_2(\alpha), ..., \tau_n(\alpha))$ then f is the zero polynomial.

Proof. Let $\{x_1, x_2, ..., x_n\}$ be a basis for K over F. Then, due to Theorem 1, the matrix $(\tau_i(x_j))$ is non-singular, and so is invertible with inverse, say, (p_{ij}). Thus, $(\tau_i(x_j))(p_{ij}) = I_n$ and so the (i , r)th entry of this matrix are

$$\sum_{j=1}^{n} \tau_i(x_j) p_{jr} = \begin{cases} 1, & \text{if i = r} \\ 0, & \text{if i} \neq \text{r} \end{cases}$$

Let $\beta_i = \sum_{j=1}^{n} \tau_i(x_j) X_j = \tau_i(x_1)X_1 + \tau_i(x_2)X_2 + ... + \tau_i(x_n)X_n$ and $\beta = (\beta_1, \beta_2, ..., \beta_n)$. Then, define the polynomial g in $P_n(K)$ as

$$g(X_1, X_2, ..., X_n) = \sigma_\beta(f).$$

If $a = (a_1, a_2, ..., a_n)$ is any ordered n-tuple of elements of F and $\alpha = a_1x_1 + a_2x_2 + ... + a_nx_n$, then

$$\begin{aligned} \sigma_a(g) = g(a_1, a_2, ..., a_n) &= f\left(\sum_{j=1}^{n} \tau_1(x_j)a_j, \sum_{j=1}^{n} \tau_2(x_j)a_j, ..., \sum_{j=1}^{n} \tau_n(x_j)a_j\right) \\ &= f\left(\sum_{j=1}^{n} \tau_1(a_jx_j), \sum_{j=1}^{n} \tau_2(a_jx_j), ..., \sum_{j=1}^{n} \tau_n(a_jx_j)\right) \\ &= f\left(\tau_1(\alpha), \tau_2(\alpha), ..., \tau_n(\alpha)\right) \\ &= 0 \end{aligned}$$

by given hypothesis.

Now, if $b = (b_1, b_2, ..., b_n)$ be any ordered n-tuple of elements of F and $c_j = \sum_{r=1}^{n} p_{jr}b_r$, for $1 \leq j \leq n$. Then,

$$\sum_{j=1}^{n} \tau_i(x_j)c_j = \sum_{j=1}^{n}\sum_{r=1}^{n} \tau_i(x_j)p_{jr}b_r = \sum_{r=1}^{n}\sum_{j=1}^{n}\left(\tau_i(x_j)p_{jr}\right)b_r = b_i,$$

since $\sum_{j=1}^{n} \tau_i(x_j)p_{jr} = \begin{cases} 1, & \text{if i = r} \\ 0, & \text{if i} \neq \text{r} \end{cases}$.

Hence if $c=(c_1,c_2,...,c_n)$, then

$$\begin{aligned}\sigma_c(g)=g(c_1,c_2,...,c_n)&=f\left(\sum_{j=1}^{n}\tau_1(x_j)c_j,\sum_{j=1}^{n}\tau_2(x_j)c_j,...,\sum_{j=1}^{n}\tau_n(x_j)c_j\right)\\&=f\left(b_1,b_2,...,b_n\right)\\&=\sigma_b(f)\end{aligned}$$

However, $\sigma_c(g)=0$ as obtained above, so $\sigma_b(f)=0$ for any ordered n-tuple $b=(b_1,b_2,...,b_n)$ of elements of F. Thus f is the zero polynomial, otherwise it will contradict Theorem 2.

Remark. Let $G(K,F)=\{\tau_1,\tau_2,...,\tau_n\}$ be a Galois group of K over F. If $\tau_i,\tau_j\in G(K,F)$, then $\tau_i\tau_j\in G(K,F)$ and so it must be an element of $\{\tau_1,\tau_2,...,\tau_n\}$. We consider $\tau_i\tau_j=\tau_{p(i,j)}$. Since $G(K,F)=\{\tau_1,\tau_2,...,\tau_n\}$ is a group so due to left and right cancellation laws, $\tau_i\tau_j=\tau_i\tau_k$ if and only if j = k, that is, $\tau_{p(i,j)}=\tau_{p(i,k)}$ if and only if j = k, it follows that p(i, j) = p(i, k) if and only if j = k. Similarly, p(h, j) = p(i, j) if and only if h = i.

We can now prove the Normal Basis Theorem for the case of infinite fields.

3.3.5. Theorem. Let K be a finite separable normal extension of on infinite subfield F. Then there exists a normal basis for K over F.

Proof. Consider now the polynomial f in $P_n(K)$ obtained by

$$f=\det\begin{pmatrix}X_{p(1,1)} & X_{p(1,2)} & \cdots & X_{p(1,n)}\\ X_{p(2,1)} & X_{p(2,2)} & \cdots & X_{p(2,n)}\\ \vdots & & \ddots & \vdots\\ X_{p(n,1)} & X_{p(n,2)} & \cdots & X_{p(n,n)}\end{pmatrix}.$$

Then as discussed in the remark above X_i occurs exactly once in each row and exactly once in each column of this matrix. If we replace ordered n-tuple $(X_1,X_2,...,X_n)$ by (1, 0, …, 0) in f, we obtain the determinant of a matrix in which the identity element 1 of F occurs exactly once in each row and exactly once in each column; the determinant of such matrix is either 1 or –1. Hence f is a non-zero polynomial.

Due to Theorem 3, there is at least one element x of K such that

$$f\left(\tau_1(x),\tau_2(x),...,\tau_n(x)\right)\neq 0.$$

By the definition of the polynomial f, this in term becomes

$$\det\left(\tau_i\tau_j(x)\right)\neq 0.$$

Hence, by corollary to Theorem 1, $\{\tau_1(x),\tau_2(x),...,\tau_n(x)\}$ is a normal basis for K over F.

3.4. Cyclotomic Extensions. Let F be a field, for every positive integer m define

$$\mathrm{k_m} = X^m - 1$$

in $F[X]$. If an extension K of F, is a splitting field of one of the polynomials k_m, then it is called a **cyclotomic extension**.

3.4.1. Theorem. Let F be a field with non-zero characteristic, then the cyclotomic extension is both separable and normal.

Proof. Suppose that F has non-zero characteristic p, then every positive integer m can be expressed in the form $m = p^r m_1$, where $r \geq 0$ and p does not divide m_1. Then we have $\mathrm{k_m} = X^m - 1 = \left(X^{m_1} - 1\right)^{p^r} = (k_{m_1})^{p^r}$, and so roots of k_m are similar to those k_{m_1}. Thus splitting field of k_{m_1} over F is also a splitting field for k_m over F. Thus in this case we consider only those polynomials k_m for which m is not divisible by the characteristic. Then,

$$\frac{\mathrm{dk_m}}{\mathrm{dX}} = mX^{m-1}$$

The only non-zero factor of this polynomial are powers of X, none of which is a factor of k_m. Thus, no roots of k_m are repeated and so k_m is a separable polynomial. Also being a splitting field of some non-zero polynomial this extension is normal too. Hence all cyclotomic extensions of F are separable and normal.

Remark. Let K_m be a splitting field for k_m over F, where m is not divisible by the characteristic of F. Also assume that F is contained in K_m. As the m roots of k_m in K_m are all distinct, we call them the m^{th} roots of unity in K_m and denote them by $\xi_1, \ldots, \xi_m$. Now if ξ_i and ξ_j are m^{th} roots of unity in K_m, we have $(\xi_i \xi_j)^m = \xi_i{}^m \xi_j{}^m = 1$ so $\xi_i \xi_j$ is also m^{th} roots of unity, therefore the collection of m^{th} roots of unity form a subgroup of the multiplicative group on non-zero elements of K_m. Further, being a finite multiplicative subgroup of non-zero elements of a group this subgroup must be a cyclic group. Any generator of this group is called a primitive m^{th} root of unity in K_m. If ξ is a primitive m^{th} root of unity, then ξ^r is also a primitive m^{th} root of unity for each r, relatively prime to m.

If m is a prime number, then every m^{th} root of unity, except the identity element, is a primitive m^{th} root of unity. It is clear that any primitive m^{th} root of unity ξ may be taken as a primitive element for K_m over F, that is to say, $K_m = F(\xi)$.

First we are to define the group $\boldsymbol{R_m}$.

The elements of $\boldsymbol{R}_m$ are the residue classes modulo m consisting of integers which are relatively prime to m, with the product of two relatively prime residue classes C_1, C_2 is defined to be the residue class containing $n_1 n_2$, where n_1, n_2 are members from C_1, C_2 respectively. The order of $\boldsymbol{R}_m$ by $\emptyset(m)$.

In the next theorem we will obtain the Galois group of a cyclotomic extension.

3.4.2. Theorem. Let F be a field, m a positive integer which is not divisible by the characteristic of F, if ch.F is non-zero. Let K_m be a splitting field for k_m over F including F. Then the Galois group $G(K_m, F)$ is isomorphic to a subgroup of $\mathbf{R}_m$.

Proof. Let ξ be a primitive m^{th} root of unity in K_m. If τ is any element of $G(K_m, F)$, then $\tau(\xi)$ is also a primitive m^{th} root of unity. Hence $\tau(\xi) = \xi^{n_\tau}$, where g.c.d.(n_τ, m) = 1. Define a mapping $: G \to \boldsymbol{R}_m$ as follows:

$$\theta(\tau) = \text{the residue class of } n_\tau \text{ modulo } m.$$

If τ and ρ are elements of G, then

$$\xi^{n_{\tau\rho}} = (\tau\rho)(\xi) = \tau\big(\rho(\xi)\big) = \tau(\xi^{n_\rho}) = (\tau(\xi))^{n_\rho} = \xi^{n_\tau n_\rho},$$

so $n_{\tau\rho} \equiv n_\tau n_\rho (\text{mod } m)$, and therefore $\theta(\tau\rho) = \theta(\tau)\theta(\rho)$. Hence θ is a homomorphism.

Further, θ is one-to-one, as if $\tau \neq \rho$ then $\tau(\xi) \neq \tau(\xi)$, that is, $\xi^{n_\tau} \neq \xi^{n_\rho}$ and hence n_τ and n_ρ are members of different residue classes modulo m.

Hence, G is isomorphic to the subgroup $\theta(G)$ of $\boldsymbol{R}_m$.

3.5. Cyclotomic Polynomial. Let F be an arbitrary field and K_m a splitting field for k_m over F containing F, we assume that m is not divisible by the characteristic of F if ch.F is non-zero. If d/m, the polynomial $k_d = X^d - 1$ divides $k_m = X^m - 1$ and hence roots of k_d are included among the m^{th} roots of unity in K_m, that is, there are d distinct d^{th} roots of unity among the m^{th} roots of unity and, in particular, $\phi(d)$ primitive d^{th} roots of unity. Thus, for each divisor d of m we may define the polynomial ϕ_d in $P(K_m)$ as

$$\phi_d = \prod (X - \xi_d),$$

where the product is taken over all the primitive d^{th} roots of unity ξ_d in K_m, then $deg\phi_d = \emptyset(d)$. Since every m^{th} root of unity ξ is a primitive d^{th} root of unity for some d/m, it follows that

$$k_m = X^m - 1 = \prod_{d/m} \phi_d.$$

The polynomial ϕ_m is called the m^{th} **cyclotomic polynomial**.

3.5.1. Theorem. For every positive integer m, the coefficients of the m^{th} cyclotomic polynomial belong to the prime subfield of F. In case if ch.F = 0, and the prime field is **Q**, then these coefficients are integers.

Proof. Mathematical induction on m is sued to obtain the result.

For m = 1, result is obvious as $\phi_1 = X - 1$ has coefficients in the prime field.

Suppose now that the result holds for all factors d of m such that $d < m$.

Then we have

$$X^m - 1 = \phi_m \prod_{\substack{1 \le d < m \\ d/m}} \phi_d.$$

By hypothesis, all the factors in the product have coefficients in the prime field; $X^m - 1$ has coefficients in the prime field. Hence so does ϕ_m. In the case, when the prime field is $\boldsymbol{Q}$, every factor in the product has integer coefficients with leading coefficient 1, when we divide a polynomial with integer coefficients by a polynomial with integer coefficients and leading coefficient 1 the quotient has integer coefficients. Thus ϕ_m have integer coefficients.

3.5.2. Example. Compute ϕ_{20}.

Since the divisors of 20 are 1, 2, 4, 5, 10 and 20, so we have

$$X^{20} - 1 = \phi_1\phi_2\phi_4\phi_5\phi_{10}\phi_{20.}$$

Similarly, the divisors of 10 are 1, 2, 5 and 10, so we have

$$X^{10} - 1 = \phi_1\phi_2\phi_5\phi_{10}.$$

Hence $\qquad X^{10} + 1 = \phi_4\phi_{20.}$

Now we need to calculate ϕ_4. For this, the divisors of 4 are 1, 2 and 4, so we have

$$X^4 - 1 = \phi_1\phi_2\phi_4.$$

Also, $\qquad X^2 - 1 = \phi_1\phi_2.$

So, we have $\qquad \phi_4 = X^2 + 1.$

Hence $\qquad \phi_{20} = \frac{X^{10}+1}{X^2+1}.$

3.6. Cyclotomic Extensions of the Rational Number Field.

In this section, we will consider that the field F = Q, field of rational numbers, and prove that the Galois group $G(K_m, Q)$ is isomorphic to the multiplicative group R_m of residue classes modulo m relatively prime to m.

3.6.1. Content of a Polynomial. Let $f(x) = \lambda_0 + \lambda_1 x + \lambda_2 x^2 + ... + \lambda_n x^n \in Z[x]$ be a polynomial over Z, then the content 't' of f is defined as $t = g.c.d.(\lambda_0, \lambda_1, \lambda_2, ..., \lambda_n)$.

3.6.2. Primitive Polynomial. A polynomial $f(x) \in Z[x]$ is said to be primitive polynomial if its content is 1.

It should be noted that if $f(x) \in Z[x]$, we may write $f(x) = cf_1(x)$, where c is the content of $f(x)$ and $f_1(x)$ is a primitive polynomial in $Z[x]$.

3.6.3. Theorem. If a polynomial $f(x) \in Z[x]$ can be expressed as a product of two polynomials over Q, the rational field, then it can be expressed as a product of two polynomials over Z.

Proof. Let $f(x) \in Z[x]$ and $g_1(x), g_2(x) \in Q[x]$ such that $f(x) = g_1(x).g_2(x)$. Let d_1, d_2 be the least common multiples of the denominators of the coefficients of $g_1(x), g_2(x)$ respectively. Then

$p_1(x) = d_1 g_1(x)$ and $p_2(x) = d_2 g_2(x)$ are polynomials in $Z[x]$. Let t_1 and t_2 be the content of $p_1(x)$ and $p_2(x)$ and write $p_1(x) = t_1 k_1(x)$ and $p_2(x) = t_2 k_2(x)$, where $k_1(x)$ and $k_2(x)$ are primitive polynomials in $Z[x]$. Then we have

$$d_1 d_2 f(x) = t_1 t_2 k_1(x) k_2(x).$$

We claim that $k_1(x)k_2(x)$ is a primitive polynomial.

Let p be any prime number. Since $k_1(x) = a_0 + a_1 x + a_2 x^2 + \ldots$ and $k_2(x) = b_0 + b_1 x + b_2 x^2 + \ldots$ are primitive polynomials so each polynomial has at least one coefficient which is not divisible by p. Let a_i and b_j be the first coefficients of $k_1(x)$ and $k_2(x)$ respectively, which are not divisible by p. Then the coefficients of X^{i+j} in $k_1(x).k_2(x)$ is

$$\sum_{u+v=i+j} a_u . b_v \ .$$

If $v \neq i$, $u \neq j$ and $u + v = i + j$, then either $u < i$ or $v < j$ and hence either a_u is divisible by p or b_v is divisible by p. Thus, all the terms, except for $a_i b_j$, in the summation are divisible by p and so the sum is not divisible by p. It follows that for every prime number p, $k_1(x).k_2(x)$ has at least one coefficient which is not divisible p, which implies that the g.c.d. of the coefficients of $k_1(x).k_2(x)$ is 1. Hence $k_1(x).k_2(x)$ is a primitive polynomial.

Thus, $t_1 t_2$ is the content of $(d_1 d_2) f(x)$. However, $d_1 d_2$ is a divisor of the content of $(d_1 d_2) f(x)$. Hence $\frac{t_1 t_2}{d_1 d_2}$ is an integer, say, l. Then $f(x) = (l k_1(x)) k_2(x)$ is a factorisation of $f(x)$ in $Z[x]$.

3.6.4. Corollary. If $f(x) \in Q[x]$ is a monic polynomial dividing $x^m - 1$, then $f(x) \in Z[x]$.

3.6.5. Definition. If $f(x) = \lambda_0 + \lambda_1 x + \lambda_2 x^2 + \ldots + \lambda_n x^n \in F[x]$ and k is any positive integer, then we denote by $f_k(x)$ the polynomial obtained as

$$f_k(x) = \lambda_0 + \lambda_1 x^k + \lambda_2 x^{2k} + \ldots + \lambda_n x^{nk} \in F[x]$$

3.6.6. Theorem. Let $f(x) \in Z[x]$ divides $x^m - 1$ and k is any positive integer such that g.c.d.(k,m)=1, then $f(x)$ divides $f_k(x)$ in $Z[x]$.

Now we will prove that the Galois group $G(K_m, Q)$ is isomorphic to the multiplicative group R_m of residue classes modulo m relatively prime to m.

3.6.7. Theorem. Let K_m be a splitting field of k_m over **Q.** Then $G(K_m, Q) \cong R_m$.

Proof. Let ζ be a primitive m^{th} root of unity in K_m. Define a monomorphism : $G(K_m, Q) \to R_m$ as follows:

$$\theta(\tau) = \text{the residue class of } n_\tau \text{ modulo } m,$$

for each automorphism τ in $G(K_m, Q)$, we defined $\tau(\zeta) = \zeta^{n_\tau}$ where n_τ is relatively prime to m.

This mapping is onto as well. Hence the required result holds.

3.6.8. Corollary. The cyclotomic polynomials ϕ_m are all irreducible in $Q[x]$.

3.7. Cyclic Extension. Let F be a field. A finite separable normal extension K of F is said to be cyclic extension of F if $G(K,F)$ is cyclic. We are considering that $F \subseteq K$.

3.7.1. Theorem. Let K be a cyclic extension of a subfield F and $G(K,F) = <\tau>$. If $x \in K$, then $N_{K/F}(x) = 1$ if and only if there is an element $y \in K$ such that $x = \dfrac{y}{\tau(y)}$, and $S_{K/F}(x) = 0$ if and only if there is an element z in K such that $x = z - \tau(z)$.

Proof. Since K is a finite extension of F so let $[K:F] = n$; then $|G(K,F)|$=n and so $\tau^n = I$, the identity automorphism.

First, suppose that $x = \dfrac{y}{\tau(y)}$. Then

$$N_{K/F}(x) = I(x)\tau(x)\tau^2(x)\ldots\tau^{n-1}(x) = \frac{y}{\tau(x)}\frac{\tau(y)}{\tau^2(y)}\frac{\tau^2(y)}{\tau^3(y)}\ldots\frac{\tau^{n-1}(y)}{\tau^n(y)} = 1.$$

Similarly, if $x = z - \tau(z)$, we have

$$\begin{aligned} S_{K/F}(x) &= I(x) + \tau(x) + \tau^2(x) + \ldots + \tau^{n-1}(x) \\ &= z - \tau(z) + \tau(z) - \tau^2(z) + \tau^2(z) - \tau^3(z) + \ldots + \tau^{n-1}(z) - \tau^n(z) = 0. \end{aligned}$$

Conversely, suppose that

$$N_{K/F}(x) = I(x)\tau(x)\tau^2(x)\ldots\tau^{n-1}(x) = x\tau(x)\tau^2(x)\ldots\tau^{n-1}(x) = 1.$$

Then x is clearly non-zero and so is invertible with $x^{-1} = \tau(x)\tau^2(x)\ldots\tau^{n-1}(x)$.

Next, since the set of automorphisms $\{I, \tau, \tau^2, \ldots, \tau^{n-1}\}$ is linearly independent over K, the mapping

$$\varepsilon + x\tau + x\tau(x)\tau^2 + \ldots + x\tau(x)\ldots\tau^{n-2}(x)\tau^{n-1}$$

is non-zero mapping of K into itself. That is to say, there is an element t of K such that

$$y = t + x\tau(t) + x\tau(x)\tau^2(t) + \ldots + x\tau(x)\ldots\tau^{n-2}(x)\tau^{n-1}(t)$$

is non-zero. Applying the automorphism τ, we obtain

$$\tau(y) = \tau(t) + \tau(x)\tau^2(t) + \tau(x)\tau^2(x)\tau^3(t) + \ldots \tau(x)\tau^2(x)\ldots\tau^{n-1}(x)t = x^{-1}y.$$

Thus $x = y/\tau(y)$. Similarly suppose

$$S_{K/F}(x) = x + \tau(x) + \tau^2(x) + \ldots + \tau^{n-1}(x) = 0.$$

Then of course $\tau(x) + \tau^2(x) + \ldots + \tau^{n-1}(x) = -x$.

Since $S_{K/F}$ is not the zero mapping; so let t be an element of K such that $S_{K/F}(t)$ is non-zero, and consider the element

$$z_1 = x\tau(t) + (x+\tau(x))\tau^2(t) + \ldots + (x+\tau(x)+\ldots+\tau^{n-2}(x))\tau^{n-1}(t).$$

Applying the automorphism τ we obtain

$$\tau(z_1) = \tau(x)\tau^2(t) + (\tau(x)+\tau^2(x))\tau^3(t) + \ldots + (\tau(x)+\tau^2(x)+\ldots+\tau^{n-1}(x))t$$

$$= \tau(x)\tau^2(t) + (\tau(x)+\tau^2(x))\tau^3(t) + \ldots - xt.$$

Hence we have

$$z_1 - \tau(z_1) = x(t+\tau(t)+\tau^2(t)+\ldots+\tau^{n-1}(t)) = xS_{K/F}(t).$$

Since $S_{K/F}(t)$ lies in F and hence is left fixed by τ, it follows that if we write $z = z_1 / S_{K/F}(t)$, then $x = z - \tau(z)$.

3.7.2. Definition. Let a be any element of a division ring D. Then the **normaliser** of a in D is the set N(a) consisting of elements of D which commute with a:

so n belongs to N(a) if and only if an = na.

3.7.3. Exercise. Let D be a division ring. Then the centre Z of D is a subfield of D and the normalizer of each element of D is a division subring of D including Z.

3.7.4. Wedderburn theorem. Every finite division ring is a field.

Proof. Let D be a finite division ring, with centre Z. Suppose Z has q elements and D has q^n elements. We claim that D = Z and n = 1.

The multiplicative group D* can be expressed as a union of finitely many conjugate classes, say $C_1,\ldots,C_k$, w.r.t. the subgroup Z*. Then, $|C_i| = \dfrac{q^n-1}{q^{t_i}-1}$ where $t_i < n$. Thus,

$$q^n - 1 = q - 1 + \sum_{i=1}^{k} \frac{q^n-1}{q^{t_i}-1}.$$

Now the nth cyclotomic polynomial Φ_n in P(**Q**) is a factor of both the polynomials $X^n - 1$ and $\dfrac{X^n-1}{X^{t_i}-1}$.

Let a = $\Phi_n(q)$. Then a divides $q^n - 1$ and $\dfrac{q^n-1}{q^{t_i}-1}$. Hence a divides q – 1.

If n > 1, then for every primitive nth root of unity ζ in the field of complex numbers **C** we have |q - ζ| > q – 1. Hence |a| = ∏| q - ζ |> q – 1, and hence a cannot be a factor of q – 1.

It follows that there is no conjugate class C_i containing more than one element. Hence n = 1 and D = Z, as required.

3.7.5. Corollary. If F is a finite set, then it is a division ring if and only if it is a field.

3.8. Check Your Progress.

1. Design fields of order 27, 16, 25, 49.

2. Compute ϕ_{30}.

3.9. Summary.

In this chapter, we have derived results related to cyclotomic extensions and cyclic extensions. Also It was proved that a finite division ring is a field, therefore we can say that a division ring which is not a field is always infinite.

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.

4

Ruler and Compass Construction

Structure

4.1. Introduction. In this chapter, possibility to construct some geometrical figures using ruler and compass are discussed by the help of some algebraic structures. Also the solvability by radicals of generic polynomial is discussed

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

(i) Normal Extensions.

(ii) Fixed Fields, Galios Groups

(iii) Norms and Traces.

4.1.2. Keywords. Normal Extensions, Galois Group, Fixed Fields.

4.2. Ruler-and-compasses constructions.

Three main problem of Geometry are:

Using the traditional geometrical instruments ruler and compasses can we

1. Trisect an arbitrary given angle.
2. Construct a cube having volume double to that of a given cube.
3. Construct a square with area equal to that of a given circle.

We shall show that these three problems are insolvable.

Consider the Euclidean plane and two straight lines intersecting at right angles in this plane meeting at a point O. Assume I is an arbitrary point on one of those lines. Then, by taking O as origin and I to be the point $(1,0)$, we can set up a Cartesian coordinate system in the plane. Let B be a collection of points in this plane, including O and I. With the points in B we can start our construction and so these points will be called basic points.

By ruler-and-compasses construction based on B we mean a finite sequence of operations of the following types:

(1) Drawing a straight line through two points which are either basic points or points previously constructed in the sequence of operations.

(2) Drawing a circle with center at a basic point or a point previously constructed with radius equal to the distance between two points, each of which is either a basic point or a point previously constructed.

(3) Obtaining points of intersection of any two obtained in (1) and (2), which are (a) points of straight lines, (b) pairs of circles, (c) straight lines and circles.

Any point P which is obtained by (3) based on B is said to be **constructible from** B. If B consists of the points O and I and no others, we simply say that B is **constructible.**

Let P be any point of the plane with coordinates (α,β) determined by O and I. The subfield of $\mathbf{R}$ obtained by adjoining α and β to $\mathbf{B}$ will be denoted by $\mathbf{B}(P)$.

4.2.1. Theorem. If the point P is constructible from B, then the $[\mathbf{B}(P) : \mathbf{B}] = 2^n$ for some non-negative integer n.

Proof. To obtain P from B in ruler-and-compasses construction let the sequence is $P_1, P_2, \dots, P_n = P$ of operations of type (3). Suppose that P_1 is one of the basic points and the co-ordinates of $P_i (i = 1, \dots, n)$ be (α_i, β_i).

Let $K = \mathbf{B}(P_1, \dots, P_n)$. We claim that $[\mathbf{K} : \mathbf{B}] = 2^n$. Then the result follows directly as $\mathbf{B}(P)$ is a subfield of K and hence $[\mathbf{B}(P) : \mathbf{B}]$ is a factor of $[K : \mathbf{B}]$.

We prove by induction on n.

If $n = 1$, then $K = \mathbf{B}(P_1) = \mathbf{B}$, thus $[K : \mathbf{B}] = 1 = 2^0$.

Now assume result holds for $n = k-1$, that is, if L is the subfield of $\mathbf{R}$ obtained by adjoining to $\mathbf{B}$ the coordinates of $P_1, \dots, P_{k-1}$ then $[L : \mathbf{B}] = 2^s$ for some s.

If P_i and P_j are distinct points $(1 \le i, j \le k-1)$ then the equation of straight line λ_{ij} joining them is

$$(\alpha_j - \alpha_i)(y - \beta_i) = (\beta_j - \beta_i)(x - \alpha_i).$$

Similarly, if P_r and P_s are distinct points and P_t is any point $(1 \le r, s, t \le k-1)$, then the equation of circle $\sum_{rs}^{t}$, with center P_t and radius equal to the distance between P_r and P_s is

$$(x-\alpha_t)^2 + (y-\beta_t)^2 = (\alpha_r - \alpha_s)^2 + (\beta_r - \beta_s)^2. \qquad (1)$$

Let T = $\mathbf{B}(P_1, \ldots, P_k)$ =L(P_k). If P_k is obtained from $P_1, \ldots, P_{k-1}$ by intersection of two lines like λ_{ij}, then its coordinates are obtained by solving two linear equations with coefficients in L and so its coordinates lie in L Thus, T = L and so $[L : \mathbf{B}] = [T : \mathbf{B}] = 2^s$.

Similarly, in other cases $[T : \mathbf{B}] = 2^t$ for some t (Left as an exercise to the reader).

This completes the Proof.

4.2.2. Theorem. Let P be a point in the plane and $\mathbf{B}(P)$ has a sequence of subfields, $\mathbf{B}(P) = K_n, K_{n-1}, \ldots, K_1, K_0 = \mathbf{B}$ such that K_i includes K_{i-1} and $[K_i : K_{i-1}] = 2 (i = 1, \ldots, n)$, then P is constructible from B.

Proof. We proceed by induction on n.

If $n = 0$ then $\mathbf{B}(P) = \mathbf{B}$. Hence, P is constructible from B. Now, let result holds for $n = k\text{-}1$.

Assume that K has a sequence of subfields $K = K_k, K_{k-1}, \ldots, K_1, K_0 = \mathbf{B}$. Since $[K_k : K_{k-1}] = 2$, it follows that K_k is a normal extension of K_{k-1}. If $\beta \in K_k$ such that $\beta \notin K_{k-1}$, then $K_k = K_{k-1}(\beta)$. If minimum polynomial of β over K_{k-1} is $X^2 + aX + b = (X + \frac{1}{2}a)^2 + (b - \frac{1}{4}a^2)$. Considering $\alpha = \beta + \frac{1}{2}a$, we have $\alpha^2 = \frac{1}{4}a^2 - b \ge 0$; thus α^2 is a positive element of K_{k-1} and clearly $K_k = K_{k-1}(\beta) = K_{k-1}(\alpha)$.

Now, since $(\alpha^2, 0)$ has coordinates in K_{k-1}, it is constructible from **B,** by the induction hypothesis. Hence every point with coordinates in K_k is constructible from B. This completes the induction.

4.2.3. Corollary. Let P be a point in the plane. If the field $\mathbf{B}(P)$ is a normal extension of $\mathbf{B}$ such that $[\mathbf{B}(P) : \mathbf{B}]$ is a power of 2, then the point P is constructible from B.

Proof. Let G be the Galois group of $\mathbf{B}(P)$ over $\mathbf{B}$, Then $|G|$ = [$\mathbf{B}(P)$: $\mathbf{B}$] = 2^s. Then, G has a sequence of subgroups, $G = A_0, A_1, A_2, \ldots, A_n = \{e\}$ each of index 2 in the preceding. Thus, $\mathbf{B}(P)$ has a sequence of subfields $\mathbf{B}(P) = K_0, K_1, K_2, \ldots, K_n = \mathbf{B}$ each of degree 2 over the next. Hence P is constructible from B.

4.3. Solution by radicals.

Let F be a field of characteristic zero and E is an extension of F, then E is said to be an **extension** of F by **radicals** if there exists a sequence of subfields $F = E_0, E_1, \dots, E_{r-1}, E_r = E$ such that

$$E_{i+1} = E_i(\alpha_i),$$

for $i = 0, \dots, r-1$, where α_i is a root of an irreducible polynomial in $P(E_i)$ of the form $X^{ni} - a_i$. A polynomial f(x) in F[x] is said to be **solvable by radicals** if the splitting field of f(x) over F is contained in an extension of F by radicals.

4.3.1. Theorem. Let F be a field of characteristic zero, K a normal extension of F with G(K,F) is abelian. If $[K : F] = n$ and the polynomial $k_n = X^n - 1$ splits completely in F[X], then K is an extension of F by radicals.

Proof. Let G = G(K,F). Then, G may be expressed as a direct product of cyclic groups, say

$$G = C_1 \times \dots \times C_r.$$

Define, $G_i = C_1 \times C_2 \times \dots \times C_{r-i}$, for $i = 0, \dots, r-1$, and $G_r = \langle I \rangle$, where I is the identity element of G. Then G_{i+1} is a normal subgroup of G_i and

$$G_i / G_{i+1} \cong C_i \quad \text{for } i = 0, \dots, r-1.$$

Let E_i be the subfield of K left fixed by G_i for $i = 0, \dots, r$. Then, E_{i+1} is a normal extension of E_i with cyclic Galois group, isomorphic to C_{r-1} for $i = 0, \dots, r-1$. Since the degree n_i of E_{i+1} over E_i is a factor of n and k_n splits completely in F[X] and hence in $E_i[X]$, it follows that k_n splits completely in $E_i[X]$. So $E_{i+1} = E_i(\alpha_i)$ where α_i is a root of an irreducible polynomial in $E_i[X]$ of the form $X^{ni} - a_i$ for $i = 0, \dots, r-1$.

Thus K is an extension of F by radicals, as asserted.

4.3.2. Theorem. Let F be a field of characteristic zero. For every positive integer n, the polynomial $k_n = X^n - 1$ in F[X] is solvable by radicals.

Proof. We prove the result by induction on n.

If $n = 1$, then the splitting field for k_n over F is F itself, which is an extension of itself by radicals.

Now, suppose that every polynomial k_l with $l < m$ is solvable by radicals.

Let K_m be a splitting field of k_m over F containing F. If $[K_m : F] = r$, then $r \leq \varphi(m) < m$. According to induction hypothesis, k_r is solvable by radicals and so there is a splitting field K_r of k_r over F which is contained in an extension E of F by radicals. Without loss of generality assume that E and K_m are contained in the same algebraic closure C of F, then consider $L = E(K_m) \subseteq C$.

Then, L is a separable normal extension of E and the Galois group G(L, E) of L over E is isomorphic to a subgroup of the Galois group $G(K_m, F)$ of K_m over F. Hence G(L, E) is Abelian. It follows that $s = [L : E]$ is a factor of $r = [K_m : F]$. Since k_r splits completely in E[X], so too does k_s. Thus L is an extension of E by radicals. Since E is also an extension of F by radicals it follows that L is also an extension of F by radicals and hence k_m is solvable by radicals.

This completes the induction.

Before proceeding further, we discuss some results of solvable groups.

4.4. Solvable Group. A group G is said to be solvable if there exists a sequence of subgroups

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \ldots \supseteq G_n = \langle e \rangle$$

such that (i) $G_{i+1} \trianglelefteq G_i$ for $0 \leq i \leq n-1$

(ii) G_i / G_{i+1} is abelian for $0 \leq i \leq n-1$.

Results.

1. Every subgroup of a solvable group is solvable.
2. Every quotient group of a solvable group is solvable.
3. Let G be a group and H be a normal subgroup of G. Then if H and G/H both are solvable, then prove that G is also a solvable group.
4. A finite p-group is solvable.
5. Direct product of two solvable groups is solvable .
6. Let H and K are solvable subgroups of G and $H \trianglelefteq G$ then HK is also solvable.
7. Show that every group of order pq is solvable where p , q are prime numbers not necessarily distinct.
8. Prove that every group of order p^2q , p and q are primes , is solvable .
9. S_n is solvable for $n \leq 4$.
10. S_n is not solvable for $n > 4$.
11. If a subgroup G of S_n $(n > 4)$ contains every 3 – cycle and H be any normal subgroup of G such that G/H is abelian then H contains all the 3 – cycles.
12. Homomorphic image of a solvable group is solvable.
13. A <u>finite</u> group G is solvable iff there exist a sequence of subgroups

$$G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_n = \langle e \rangle$$

such that $G_{i+1} \trianglelefteq G_i$ and G_i/G_{i+1} is cyclic group of prime order for $0 \leq i \leq n$.

14. A group G in is solvable iff $G^{(n)} = \langle e \rangle$ for some $n \geq 0$.
15. A_n is not solvable for $n \geq 5$ and hence S_n is also not solvable for $n \geq 5$.

We now state a criterion for a polynomial to be solvable by radicals.

4.4.1. Exercise. Let F be a field of characteristic zero. A polynomial f(x) in F[x] has splitting field over F with a solvable Galois group iff f(x) is solvable by radicals.

4.5. Solution of Polynomial Equations by Radicals.

An extension field K of F is called a radical extension of F if there exist elements $\alpha_1, \alpha_2, \ldots, \alpha_m \in K$ such that

1. $K = F(\alpha_1, \alpha_2, \ldots, \alpha_m)$
2. $\alpha_1^{n_1} \in F$ and $\alpha_i^{n_i} \in F(\alpha_1, \alpha_2, \ldots, \alpha_{i-1})$ for $i = 1, 2, \ldots, m$ and integers $n_1, n_2, \ldots, n_m$

For $f(x) \in F[x]$ the polynomial equation f(x) = 0 is said to be solvable by radicals if there exists a radical extension K of F that contains all roots of f(x).

If now $\{x_1, \ldots, x_n\}$ is asubset of a field E algebraically independent over the subfield F of E, the polynomial

$$g_n = X^n - x_1 X^{n-1} + x_2 X^{n-2} - \ldots + (-1)^n x_n$$

in $P(F(x))$ is called a **generic polynomial** of degree n over F. So a generic polynomial over F is one which has no polynomial relations with coefficients in F connecting its coefficients

4.5.1. Theorem. Let $g_n = X^n - x_1 X^{n-1} + \ldots + (-1)^n x_n$ be a generic polynomial of degree n over a field F of characteristic zero. Then the Galois group of any splitting field of g_n over $F(x_1, \ldots, x_n) = F(x)$ is isomorphic to the symmetric group on n digits. **(Left as an exercise for students)**

4.5.2. Theorem. The generic polynomial of degree $n \geq 5$ is not solvable by radicals.

Proof. Since the Galois group of any splitting field of g_n over $F(x_1, \ldots, x_n) = F(x)$ is isomorphic to the symmetric group S_n,. But S_n is not solvable group when $n \geq 5$. Hence f(x) is not solvable by radicals over $F(x_1, \ldots, x_n) = F(x)$ when $n \geq 5$.

4.6. Check Your Progress.

1. Design fields of order 27, 16, 25, 49.
2. Compute ϕ_{30}.

4.7. Summary.

Constructing a cube having volume double to that of a given cube is equivalent to the construction from the basic points O and I of the point $(\alpha, 0)$, where α is the real number such that $\alpha^3 = 2$. Since the polynomial $X^3 - 2$ is irreducible in $P(\mathbf{Q})$, the field $\mathbf{Q}(\alpha)$ has degree 3 over $\mathbf{Q}$ and hence, since 3 is not a power of 2, the point $(\alpha, 0)$ is not constructible from O and I. Constructing a square with area equal to that of a given circle is equivalent to the construction of the point $(\sqrt{\pi}, 0)$. However, π is not algebraic over the field of rational numbers. Hence $(\mathbf{Q}(\pi) : \mathbf{Q})$ is infinite and hence cannot a power of 2.

Books Suggested:

1. Stewart, I., Galios Theory, Chapman and Hall/CRC, 2004.
2. Adamson, I. T., Introduction to Field Theory, Cambridge University Press, 1982.