PERIYAR UNIVERSITY

NAAC 'A++' Grade - State University
NIRF Rank 56 – State Public University Rank 25
SALEM - 636 011, Tamil Nadu, India.

CENTRE FOR DISTANCE AND ONLINE EDUCATION (CDOE)

MASTER OF SCIENCE IN MATHEMATICS

SEMESTER - II

CORE: ADVANCED ALGEBRA

(Candidates admitted from 2024 onwards)

PERIYAR UNIVERSITY

CENTRE FOR DISTANCE AND ONLINE EDUCATION (CDOE)

M.Sc., MATHEMATICS 2024 admission onwards

CORE
Advanced Algebra

Prepared by:

Centre for Distance and Online Education (CDOE)
Periyar University
Salem 636011

Contents

SYLLABUS: ADVANCED ALGEBRA

Objectives:

This course aims to The objective of this course is to study field extension, roots of polynomials, Galois Theory, finite fields, division rings, solvability by radicals and to develop computational skill in abstract algebra.

Unit I: Algebraic Extension Extension fields - Transcendence of e.

Unit II: Splitting Field and Simple Extension Roots of Polynomials - More about roots.

Unit III: Galois Theory Elements of Galois Theory.

Unit IV: Finite fields Finite fields - Wedderburn's theorem on finite division rings.

Unit V: Frobenius and Four - Square theorem Solvability by radicals - A theorem of Frobenius - Integral Quaternions and the Four - Square theorem.

References:

1. I.N. Herstein, Topics in Algebra (II Edition) Wiley Eastern Limited, New Delhi, 1975.

Suggested Reading:

1. M. Artin, Algebra, Prentice Hall of India, 1991.

2. P.B. Bhattacharya, S.K. Jain, and S.R. Nagpaul, Basic Abstract Algebra (II Edition) Cambridge University Press, 1997. (Indian Edition)

3. I.S. Luther and I.B.S. Passi, Algebra, Vol. I âĂŞGroups(1996); Vol. II Rings, Narosa Publishing House , New Delhi, 1999

4. D.S. Malik, J.N. Mordeson and M.K. Sen, Fundamental of Abstract Algebra, McGraw Hill (International Edition), New York. 1997.

5. N. Jacobson, Basic Algebra, Vol. I & II Hindustan Publishing Company, New Delhi.

UNIT - 1

Unit 1

Extension Fields

Objectives:

- Recall rings and commutative ring.
- Analyze the characteristics of fields.
- Study how to extend a field to a extension field.
- Understand the concept of algebraic extensions.
- To show that the number e is transcendental.

1.1 Field Extension

Definition 1.1.1. Let R be a commutative ring with identity. R is a field if every non-zero element in R has multiplicative inverse (or) $(R^*, .)$ is an abelian group (or) R is a commutative skew field.

Example 1.1.2. (i) $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}, \mathbb{Z}_p$ are fields.

(ii) $\mathbb{Q}(x), \mathbb{R}(x), \mathbb{C}(x), \mathbb{Z}_p(x)$ are fields.

Definition 1.1.3. Let F be a field. A field K is a field extension of F if F is subfield of K.

$[K : F]$ denote K is field extension of F.

Example 1.1.4. (i) $[\mathbb{C} : \mathbb{R}], [\mathbb{C} : \mathbb{Q}], [\mathbb{R} : \mathbb{Q}]$ are field extensions.
(ii) Every field F is a field extension of itself.

Remark 1.1.5. If $[K : F]$ is a field extension, then F is a subfield of K and so K is a non-zero vector space over F. Hence K has basis B and $dim_F K = |B|$. Hence the degree of $[K : F]$ is $[K : F] = dim_F K$.

Remark 1.1.6. If $\phi : F \to K$ is any ring homomorphism, where F, K are fields, then $\phi = 0$ or ϕ is $1 - 1$.

Theorem 1.1.7. *Let $p(x)$ be a non-zero constant irreducible polynomial of degree n over F. Then there exists a field extension K of F such that K has a root of $p(x)$ and $[K : F] = n$.*

Proof. Since $p(x)$ is irreducible over F, $< p(x) >$ is maximal ideal in $\mathbb{F}[x]$. Clearly, F is a subring of $F[x]$. Clearly $\frac{F[x]}{<p(x)>}$ is a field. Take $K = \frac{F[x]}{<p(x)>} = \{f(x)+ < p(x) >: f(x) \in F[x]\}$.

Define $\phi : F \to K$ by $\phi(a) = a+ < p(x) >$, for all $a \in F$. Let $a, b \in F$. Now $\phi(a+b) = (a+b)+ < p(x) >= a+ < p(x) > +b+ < p(x) >= \phi(a)+ \phi(b)$, $\phi(ab) = ab+ < p(x) >= (a+ < p(x) >)(b+ < p(x) >) = \phi(a)\phi(b)$. Therefore ϕ is a ring homomorphism. Since $\phi(1) = 1+ < p(x) \neq 0+ <$

$p(x) >$, ϕ is non-zero ring homomorphism. By Remark 1.1.6, ϕ is $1-1$ $\Rightarrow Ker\phi = \{0\}$. By first isomorphism Theorem, $F \cong \phi(F)$ is a subring of K and so $[K : F]$ is a field extension.

Define $\psi : F[x] \to K$ by $\psi(g(x)) = g(x)+ < p(x) >$, for all $g(x) \in F[x]$. Let $g(x), h(x) \in F[x]$. $\psi(g(x)+h(x)) = (g(x)+h(x))+ < p(x) >= (g(x)+ < p(x) >) + (h(x))+ < p(x) >= \psi(g(x)) + \psi(h(x))$

$\psi(g(x)h(x)) = g(x)h(x)+ < p(x) >= (g(x)+ < p(x) >)(h(x)_{<}p(x) >) = \psi(g(x))\psi(h(x))$. Thus ψ is a ring homomorphism. Clearly, $\psi(a) = a+ < p(x) >= \phi(a)$, for all $a \in F \subset F[x]$. Since $F \cong \phi(F)$, $a = \phi(a) = a+ < p(x) >, \forall a \in F$. Let $p(x) = a_0 + a_1x + \cdots + a_nx^n \in F[x]$. Then $\psi(p(x)) = 0+ < p(x) >$ in K. Let $\alpha = x+ < p(x) >\in K$. Then $\psi(p(x)) = 0+ < p(x) >$ in K. $\Rightarrow \psi(a_0+a_1x+\cdots+a_nx^n) = 0+ < p(x) >$ in K.

$\Rightarrow \psi(a_0) + \psi(a_1)\psi(x) + \cdots + \psi(a_n)\psi(x^n) = 0+ < p(x) >$ in K. $a_0+ < p(x) > +a_1+ < p(x) > (x+ < p(x) >) + \cdots + (a_n+ < p(x) >)(x^n+ < p(x) >) = 0+ < p(x) >$ in K.

$\Rightarrow a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n = 0+ < p(x) >$ in K. Thus α is a root of $p(x)$ in K. Since $\alpha = x+ < p(x) >$, we have $1+ < p(x) >= 1, \alpha, \alpha^2, \ldots, \alpha^{n+1} \in K$. Let $B = \{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\} \subset K$. Suppose $a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} = 0+ < p(x) >$, where $a_i \in F$. Then, $a_0 + a_1(x+ < p(x) >) + a_2(x^2+ < p(x) >) + \cdots + a_{n-1}(x^{n-1}+ < p(x) >) = 0+ < p(x) >$.

$\Rightarrow a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1}+ < p(x) >= 0+ < p(x) >$.

$\Rightarrow a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \in< p(x) >= \{\lambda(x)f(x) : \lambda(x) \in F[x]\}$.

$\longrightarrow (1)$.

For any $g(x) \in< p(x) >$ and $g(x) \neq 0$, $deg(g(x)) \leq n$. (1) is possible, when $a_0 + a_1x + \cdots + a_{n-1}x^{n-1} = 0$. Since, $\{1, x, \ldots, x^{n-1}\} \subseteq \{1, x, x^2, \ldots, x^n, \ldots\}$ is lineraly independent in $F[x]$.

$\Rightarrow \{1, x, \ldots, x^{n-1}\}$ is linearly independent. Since $a_0+a_ax+\cdots+a_{n-1}x^{n-1} = 0$, $a_i = 0$. Thus B is linearly independent subset of K. For any $g(x)+ < p(x) >\in K$, $g(x)+ < p(x) >\neq 0+ < p(x) >$. Thus $g(x) \notin< p(x) >$ and $g(x) \neq 0$, $g(x) \in F[x]$. By division algorithm, there exists $q(x), r(x) \in F[x]$ such that $g(x) = p(x)q(x) + r(x)$, where $r(x) = 0$ or $deg(r(x)) < deg(p(x)) = n$.

Let $r(x) = a_0+a_1x+a_{n-1}x^{n-1} \in F[x]$. Then $g(x)+ < p(x) >= p(x)q(x)+ r(x)+ < p(x) >= r(x)+ < p(x) >= a_0+a_1x+\cdots+a_{n-1}x^{n-1}+ < p(x) >= (a_0+ < p(x) >) + (a_1+ < p(x) >)(x+ < p(x) >) + \cdots + (a_{n-1}+ < p(x) >)(x^{n-1}+ < p(x) >) = a_0+a_1\alpha+\cdots+a_{n-1}\alpha^{n-1}$. Thus B spans K and B is a basis for K over F and $K = \frac{F[x]}{<p(x)>} = \{a_0+a_1\alpha+\cdots+a_{n-1}\alpha^{n-1} : a_i \in F\}$. Hence $[K : F] = n$. □

Definition 1.1.8. Let $[K : F]$ be a field extension and $S \subseteq K$. Then

$$F(S) = \bigcap_{F,S \subseteq K_\alpha} K_\alpha,$$

K_α is a subfield of K. $F(S)$ is the smallest field containing both F and S. For any $\alpha \in K$, $F(\alpha)$ is the smallest field containing both F and α.

Corollary 1.1.9. *Let $p(x)$ be an irreducible polynomial of degree n over F. Then $K \cong F(\alpha)$.*

Proof. Clearly $K = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} : a_i \in F\}$ and $F(\alpha) \subseteq K \longrightarrow (1)$.

Define $\phi : K \to F(\alpha)$ by $\phi(g(x)+ < p(x) >) = g(\alpha), \forall g(x)+ < p(x) >\in K$. Then ϕ is a ring homomorphism and $\phi(1+ < p(x) >) = \phi(x+ < p(x) >) = x = 1 \neq 0$. By result 1, ϕ is 1-1. By first isomorphism theorem, $K \cong \phi(K) \subseteq F(\alpha) \longrightarrow (2)$. From (1) and (2), we get $K = F(\alpha)$. □

Problem 1.1.10. Let $p(x) = x^2 + 1 \in \mathbb{R}[x]$. Then $\pm i$ are roots of $p(x)$ and $\pm i \notin \mathbb{R}$. Thus $p(x)$ is irreducible over $\mathbb{R}$. Take $\alpha = i$ and $K = \mathbb{R}[i]$, $\{1, \alpha\}$ is a basis for K over $\mathbb{R}$ and $K = \mathbb{R}[i] = \{a_0 = a_1 i : a_i \in \mathbb{R}\} = \mathbb{C}$.

Problem 1.1.11. Let $p(x) = x^2 - 2 \in Q[x]$. Then $\pm\sqrt{2}$ are roots of $p(x)$ and $\pm\sqrt{2} \notin Q[x]$. Taking $\alpha = \sqrt{2}$, $\{1, \sqrt{2}\}$ is basis for K over Q. Thus $K = Q[\sqrt{2}] = \{a_0 + a_1\sqrt{2} : a_i \in Q\}$.

Theorem 1.1.12. *Let $f(x)$ be any non-constant polynomial of degree n over F. Then there exists an extension K of F such that K has a root of $f(x)$ and $[K : F] \leq deg(f(x))$.*

Proof. If $f(x)$ is irreducible, then by Theorem 3.2.24, there exists a field extension K of F such that K has a root, say α, of $p(x)$ and $[K : F] = n$. Suppose $f(x)$ is reducible over F. Since $F[x]$ is UFD, $f(x) = p_1(x) \cdots p_t(x)$, where $p_i's$ are irreducible over F. clearly, $deg(p_i(x)) \geq 1$. consider $p_1(x) \in F[x]$. Then by Theorem 3.2.24, there is a field extension K of F such that K has a root α of $p_1(x)$ and $[K : F] =$

$deg(p_1(x))$. Clearly $f(\alpha) = 0$ and α is a root of $f(x)$ over F and $[K : F] = deg(p_1(x)) \leq deg(f(x))$. □

1.1.1 Finite Extension

Definition 1.1.13. Let $[K : F]$ be a field extension. $[K : F]$ is a finite extension if $[K : F] < \infty$.

Example 1.1.14. $[Q(\sqrt{2}) : Q] = 2$ and $[Q(i) : Q] = 2$

Theorem 1.1.15. *Let $[L : K]$ and $[K : F]$ be finite extensions. Then $[L : F]$ is a finite extension and $[L : F] = [L : K][K : F]$.*

Proof. Let $[L : K] = n$ and $[K : F] = m$. Let $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$ be a basis for L over K, where $\alpha_i \in L$ and $\{\beta_1, \beta_2, \dots, \beta_m\}$ be a basis for K over F, where $\beta_j \in K$. Let $B = \{\alpha_i\beta_j : i = 1, 2, \dots, n \ , j = 1, 2, \dots, m\} \subseteq L$. Then $|B| = mn$. Clearly, $[L : F]$ is a field etension. Since $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$ is a basis for L over K, there exists $a_1, a_2, \dots, a_n \in K$ such that $u = a_1\alpha_1 + a_2\alpha_2 + \dots + a_n\alpha_n$, for any $u \in L$. Since $\{\beta_1, \beta_2, \dots, \beta_m\}$ be a basis for K over F, there exist $b_{i1}, b_{i2}, \dots, b_{im} \in F$ such that $a_i = b_{i1}\beta_1 + \cdots b_{im}\beta_m$. $\Rightarrow u = a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n = (b_{11}\beta_1 + \cdots b_{1m}\beta_m)\alpha_1 + \cdots + (b_{n1}\beta_1 + \cdots b_{nm}\beta_m)\alpha_n$. Thus B spans L over F. Since $|B| < \infty$, $dim_F(L) < \infty$.

Suppose $\sum\limits_{i=1}^{n}\sum\limits_{j=1}^{m} d_{ij}\beta_j\alpha_i = 0$, where $d_{ij} \in F \subseteq K$. Then, $(\sum\limits_{j=1}^{m} d_{1j}\beta_j)\alpha_1 + (\sum\limits_{j=1}^{m} d_{2j}\beta_j)\alpha_2 + \cdots + (\sum\limits_{j=1}^{m} d_{nj}\beta_j)\alpha_n = 0$, where $\beta_j, d_{ij} \in K$. Since $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$ is linearly independent in L over K, $\sum\limits_{j=1}^{m} d_{ij}\beta_j = 0$, for $i = 1, 2, \dots, n$. Since $\{\beta_1, \beta_2, \dots, \beta_m\}$ is linearly independent in K

over F, $d_{1j} = d_{2j} = \cdots = d_{nj} = 0$, for all $j = 1$ to m. Thus B is linearly independent and so B is a basis for L over F. Hence $[L : F] = [L : K][K : F] = nm$. □

Corollary 1.1.16. *Let $[L : K], [K : F]$ be field extensions. If either $[K : F] = \infty$ or $[L : K] = \infty$, then $[L : F] = \infty$.*

Proof. Suppose $[K : F] = \infty$, then $dim_F(K) = \infty$ and there exists $\alpha_1, \alpha_2, \ldots \in K$ such that $\{\alpha_1, \alpha_2, \ldots, \alpha_n, \ldots\}$ is linearly independent in K over F. Since L is a vector space over K, $\{1\}$ is linearly independent in L over K. Thus $\{1.\alpha_i : i \in \mathbb{N}\} \subset L$ is linearly independent in L over F.

Suppose $[L : K] = \infty$, then $dim_K(L) = \infty$ and there exists $\alpha_1, \alpha_2, \ldots \in L$ such that $\{\alpha_1, \alpha_2, \ldots, \alpha_n, \ldots\}$ is linearly independent in L over K. Since K is a vector space over F, $\{1\}$ is linearly independent in K over F. Thus $\{1.\alpha_i : i \in \mathbb{N}\} \subset L$ is linearly independent in L over F. Hence $[L : F] = \infty$. □

Corollary 1.1.17. *Let $[K : F]$ be a field extension. If $[K : F] = p$ is prime. Find all subfields of K containing F.*

Proof. Clearly, F, K are subfields of K containing F. Suppose E be any subfield of K containing F. If $[E : F] = \infty$, then $[K : F] = \infty$, which contradicts $[K : F] < \infty$. If $[K : E] = \infty$, then $[K : F] = \infty$, which contradicts $[K : F] < \infty$. Hence $[E : F], [K : E] < \infty$ and $p = [K : F] = [K : E][E : F]$. Thus $[K : E]$ or $[E : F]$ is one and so

$K = E$ or $E = F$. Hence, F and K are only subfieldd of K containing F. □

Corollary 1.1.18. *If $[L : F]$ is a finite extension and K is a subfield of L containing F, then $[K : F]$ divides $[L : F]$.*

Proof. Since $[L : F] < \infty$, $[K : F], [L : K] < \infty$. Thus $[L : F] = [L : K][K : F]$. clearly F, K are subfields of K. Suppose E is any subfield of K containing F. If $[E : F] = \infty$, then $[K : F] = \infty$, which contradicts $[K : F] < \infty$. If $[K : E] = \infty$, then $[K : F] = \infty$, which contradicts $[K : F] < \infty$. Hence $[E : F], [K : E] < \infty$ and $p = [K : F] = [K : E][E : F]$. Thus $[K : E]$ or $[E : F]$ is one and so $K = E$ or $E = F$. Hence $[K : F]$ divides $[L : F]$. □

1.1.2 Algebraic Extension

Definition 1.1.19. Let $[K : F]$ be a field extension and $\alpha \in K$. α is algebraic over F if $f(\alpha) = 0$, for some $f(x) \in F[x]$. α is transcendental element over F if α is not algebraic over F.

Example 1.1.20. Let $\alpha = \sqrt{2} + i \in \mathbb{C}$. Is α algebraic over $\mathbb{Q}$?

Proof. Let $\alpha = \sqrt{2} + i \in \mathbb{C}$. Then $\alpha^2 = 2 - 1 + 2\sqrt{2}i = 1 + 2\sqrt{2}i$.
$\Rightarrow (\alpha^2 - 1)^2 = -8$ and so $\alpha^4 - 2\alpha^2 + 9 = 0$. α is a root of $x^4 - 2x^2 + 9 \in Q[x]$. Thus α is algebraic over Q. □

Remark 1.1.21. If $[K : F]$ is field extension, then α is a root of $x - \alpha \in F[x]$, for all $\alpha \in F$. Thus α is algebraic over F, for all $\alpha \in F$.

Definition 1.1.22. Let $[K : F]$ be field extension, $[K : F]$ is algebraic extension if α is algebraic over $F, \forall \alpha \in K$.

Example 1.1.23. (i) $\mathbb{C}|\mathbb{R}$ is algebraic extension.
(ii) $\mathbb{C}|Q$ is not algebraic extension.

Theorem 1.1.24. *Any finite extension is algebraic.*

Proof. Let $[K : F]$ be a finite extension and $[K : F] = n$. Let $\alpha \in K$. Then $1, \alpha, \alpha^2, \ldots, \alpha^n \in K$. Since $[K : F] = n, \{1, \alpha, \ldots, \alpha^n\}$ is linearly dependent in K over F. There exists $a_0, a_1, \ldots, a_n$(not all zero) such that $a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$ ans so α is a root of $a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in F[x]$. This implies that α is algebraic over F and hence $[K : F]$ is algebraic.
Converse need not true. □

Problem 1.1.25. Find $[Q(\sqrt{2}, \sqrt{3}) : Q]$

Proof. We know that $[Q(\sqrt{2}) : Q] = 2$ and $\{1, \sqrt{2}\}$ is a basis for $Q(\sqrt{2})$ over Q.
$[Q(\sqrt{2}, \sqrt{3}) : Q(\sqrt{2})] = [Q(\sqrt{2})(\sqrt{3}) : Q(\sqrt{2})] = deg(x^2 - 3) = 2.\{1, \sqrt{3}\}$ is a basis for $Q(\sqrt{2})(\sqrt{3})$ over $Q(\sqrt{2})$.
$[Q(\sqrt{2}, \sqrt{3}) : Q] = [Q(\sqrt{2}, \sqrt{3}) : Q(\sqrt{2})][Q(\sqrt{2}) : Q] = 2.2 = 4$ and $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ is a basis for $Q(\sqrt{2}, \sqrt{3})$ over Q. □

Problem 1.1.26. Find $[Q(\sqrt{2},\sqrt{3},\sqrt{5}):Q]$

Proof. $[Q(\sqrt{2},\sqrt{3})(\sqrt{5}):Q(\sqrt{2},\sqrt{3})] = deg(x^2-5) = 2$ and $\{1,\sqrt{5}\}$ is a basis for $Q(\sqrt{2},\sqrt{3},\sqrt{5})$ over $Q(\sqrt{2},\sqrt{3})$.
$[Q(\sqrt{2},\sqrt{3},\sqrt{5}):Q] = [Q(\sqrt{2},\sqrt{3})(\sqrt{5}):Q(\sqrt{2},\sqrt{3})][Q(\sqrt{2},\sqrt{3}):Q] = 2.4 = 8$ and $\{1,\sqrt{2},\sqrt{3},\sqrt{6},\sqrt{5},\sqrt{10},\sqrt{15},\sqrt{30}\}$ is a basis for $Q(\sqrt{2},\sqrt{3},\sqrt{5})$ over Q.
In general, $[Q(\sqrt{p_1},\sqrt{p_2},\dots,\sqrt{p_n}):Q] = 2^n$, where $p_i's$ are prime. □

Example 1.1.27. Give an example of inifinite algebraic extension.

Proof. Let $K = \{Q(\sqrt{p}) : p \text{ is prime}\}$. Then $K|Q$ is a field extension.
Claim: If $p \notin \{p_1, p_2, \dots, p_n\}$, then $\sqrt{p} \notin Q(\sqrt{p_1},\sqrt{p_2},\dots,\sqrt{p_n})$.
If $n = 0$, then $\sqrt{p} \notin Q, \forall$ prime p. Suppose $n = 1$. Assume that $p \notin \{p_1\}$
Claim: $\sqrt{p} \notin Q(\sqrt{p_1}) = \{a + b\sqrt{p_1} : a, b \in Q\}$.
Suppose $\sqrt{p} \in Q(\sqrt{p_1})$. Then $\sqrt{p} = a + b\sqrt{p_1} \neq 0$ and $p = a^2 + b^2p_1 + 2ab\sqrt{p_1}$. If $a = 0$ and $b \neq 0$, then $p = b^2p_1$. $\Rightarrow p_1|p$, which contradicts $(p, p_1) = 1$. If $a \neq 0$ and $b = 0$, then $p = a^2$. $\Rightarrow \sqrt{p} = a \in Q$, which is a contradiction. If $a \neq 0, b \neq 0$, then $\sqrt{p_1} = \frac{p-a^2-b^2p_1}{2ab} \in Q$, which is a contradiction. Hence $\sqrt{p} \notin Q(p_1)$. Assume that the result is true for $n-1$. If $p \notin \{p_1, p_2, \dots, p_{n-1}\}$, then $\sqrt{p} \notin Q(\sqrt{p_1},\dots,\sqrt{p_{n-1}})$. Consider the field $Q(\sqrt{p_1},\dots,\sqrt{p_n}) = Q(\sqrt{p_1},\dots,\sqrt{p_{n-1}})(\sqrt{p_n})$. Suppose $\sqrt{p} \in Q(\sqrt{p_1},\dots,\sqrt{p_{n-1}})(\sqrt{p_n})$. Then $\sqrt{p} = a + b\sqrt{p_n}$, where $a, b \in Q(\sqrt{p_1},\dots,\sqrt{p_{n-1}})$. If $a = 0, b \neq$, then $p = b^2p_1$. $\Rightarrow p_1|p$, which contradicts $(p, p_1) = 1$. If $a \neq 0$ and $b = 0$, then $p = a^2$. $\Rightarrow \sqrt{p} = a \in Q$,

which is a contradiction. If $a \neq 0, b \neq 0$, then $\sqrt{p_1} = \frac{p-a^2-b^2p_1}{2ab} \in Q$, which is a contradiction. Hence $\sqrt{p} \notin Q(\sqrt{p_1}, \ldots, \sqrt{p_n})$. Note that $[Q(\sqrt{p_1}, \ldots, \sqrt{p_n}) : Q] = 2^n$, for all n and so $[K : Q] = \infty$. For any $\alpha \in K$, $Q\{\sqrt{p} : p\, is\, prime\} \subset \mathbb{R}$, there exists $q_1, q_2, \ldots, q_m$ distinct primes such that $\alpha \in Q(\sqrt{q_1}, \ldots, \sqrt{q_m})$. Since $[Q(\sqrt{q_1}, \ldots, \sqrt{q_m}) : Q = 2^m < \infty$, $Q(\sqrt{q_1}, \ldots, \sqrt{q_m})$ is algebraic. Thus α is algebraic over Q and $[K : Q]$ is algebraic extension. □

Theorem 1.1.28. *Let $[K : F]$ be a field extension, $\alpha \in K$. Then α is algebraic over F if and only if there exists a unique monic polynomial $\mathfrak{m}_{\alpha,F}(\alpha) \in F[x]$ such that $\mathfrak{m}(\alpha) = 0$.*

Proof. Suppose $\alpha \in K$ is algebraic over F. Then $f(\alpha) = 0$, for some $f(x) \in F[x]$. Let $S = \{deg(h(x)) \in \mathbb{Z}^+ : h(x) \in F[x], h(\alpha) = 0\}$. Then $S \neq \phi$ and $S \subset \mathbb{Z}^+$. By well ordering principle, S has least element,say m. Clearly, $m \leq deg(g(x))$, for some $g(x) \in F[x]$. Let $g(x)$ be the least degree polynomial in $F[x]$ such that $g(a) = 0$. Then $h(\alpha) \neq 0$, for all $h(x) \in F[x]$ and $deg(h(x)) < deg(g(x))$. Let $g(x) = a_0 + a_1x + \cdots + a_mx^m, a_m \neq 0$. If $a_m = 1$, then $g(x)$ is a monic polynomial. Suppose $a_m \neq 1$. Then $t(x) = a_m^{-1}g(x)$ and $deg(t(x)) = deg(g(x)) = n$ and so $t(x)$ is a monic polynomial in $F[x]$. Suppose $t(x)$ is irreducible, then by defn, $t(x) = s(x)h(x)$, for some $s(x), h(x) \in F[x]$. Since $t(\alpha) = 0$, $s(\alpha)h(\alpha) = 0, s(\alpha), h(\alpha) \in K$. Since K is integral domain, $s(\alpha) = 0$ or $h(\alpha) = 0$, which is a contradiction. Suppose $l(x)$ is a monic irreducible polynomial in $F[x]$ such that $l(\alpha) = 0$. By division algorithm, there exists $q(x), r(x) \in F[x]$ such that $l(x) =$

$q(x)t(x) + r(x)$, where $r(x) = 0$ or $deg(r(x)) < deg(t(x))$. If $deg(r(x)) < deg(t(x))$, then $r(\alpha) = l(\alpha) - q(\alpha)t(\alpha) = 0$, a contradiction. Hence $r(x) = 0$ and $l(x) = g(x)t(x)$. Since $l(x)$ is irreducible, $deg(l(x)) \geq 1$, $t(x)$ is not a unit, $g(x) = u$ is unit in F and $l(x) = ut(x)$. Since $l(x)$ is monic, leading coefficient of $l(x) = 1$. Thus $l(x) = t(x)$.

Conversely, suppose there exists a unique monic polynomial $\mathfrak{m}_{\alpha,F}(\alpha) \in F[x]$ such that $\mathfrak{m}(\alpha) = 0$. Then α is algebraic over F. □

Definition 1.1.29. Let $[K : F]$ be a field extension and $\alpha \in K$, α is algebraic of degree n over F if α is a root of non-zero polynomial $f(x) \in F[x]$ of degree n and $p(\alpha) \neq 0$, $\forall\ p(x) \in F[x]$ and $deg(p(x)) < deg(f(x))$.

Theorem 1.1.30. *Let $f(x) \in F[x]$. Then there is an extension K over F such that all roots of $f(x)$ lies in K and $[K : F] \leq deg(f(x))!$*

Proof. If $n = 1$, then $f(x) = ax + b$, $a, b \in F, a \neq 0$. Clearly $\frac{-b}{a} \in F$ and $f(\frac{-b}{a}) = 0$. In this case, $K = F$ and $[K : F] = 1!$. Suppose $n = 2$. If $f(x)$ is reducible over F. Then $f(x) = (a_1x + b_1) + (a_2x + b_2)$. $\frac{-b_i}{a_i} \in F$ be a root of $f(x)$. Here $K = F, [K : F] \leq 2! = 1$. Suppose $f(x)$ is irreducible over F, then there is an extension K of F such that K has a root of $f(x)$ and $[K : F] = 2$. Clearly, $K = F(\alpha)$ and $f(x)$ is reducible over F and $f(x) = (x - \alpha)(x - \beta)$ and $[K : F] = 2 = 2!$. Assume that the theorem is true for all non-constant polynomials of degree$< n$. Let $n \geq 3$ and α be a root of $f(x)$ in some extension of F. Then $f(\alpha) = 0$ and so $f(x)$ is reducible over $F[x]$. Clearly, $[F(\alpha) : \beta] \leq n$ and $f(x) = (x-\alpha)g(x)$, where

$g(x) \in F(\alpha)[x]$, $deg(g(x)) = n-1$. By induction there is an extension F' of $F(\alpha)$ such that all roots of $g(x)$ in F', $[F' : F(\alpha)] \leq (n-1)!$. Thus $[F' : F] = [F' : F(\alpha)][F(\alpha) : F] \leq (n-1)!n = n!$ and $\alpha \in F'$. Hence all roots of $f(x)$ in F'. □

Definition 1.1.31. Let $f(x) \in F[x]$ and $[K : F]$ be a field extension, $f(x)$ splits over K if $f(x) = \prod_{i=1}^{k}(ax_i + b_i)$, where $a_i, b_i \in K$. A field K is a splitting field for $f(x)$ over F if (i) All roots of $f(x)$ lies in K. (ii) If E is any proper subfield of K, then $f(x)$ is not split over F or K is the smallest field containing all roots of $f(x)$ over F.

Theorem 1.1.32. *If $\alpha \in K$ is algebraic over F and $f(\alpha) = 0$, for some $f(x) \in F[x]$, then $\mathfrak{m}_{\alpha,F}$ divides $f(x)$*

Proof. Let $f(x) \in F[x]$ and $\mathfrak{m}_{\alpha,F} \in F[x]$. By division algorithm, there exists $q(x), r(x) \in F[x]$ such that $f(x) = q(x)\mathfrak{m}_{\alpha,F} + r(x)$, where $r(x) = 0$ or $deg(r(x)) < deg(\mathfrak{m}_{\alpha,F})$. Also, $r(\alpha) = f(\alpha) - q(\alpha)\mathfrak{m}_{\alpha,F} = 0$. By choice of $\mathfrak{m}_{\alpha,F}, r(x) = 0$. Thus $f(x)q(x)\mathfrak{m}_{\alpha,F}$ and $\mathfrak{m}_{\alpha,F}$ divides $f(x)$. □

Theorem 1.1.33. *Let $\sigma : K_1 \to K_2$ be an isomorphism, if $f(x) \in K_1[x]$ and $\sigma f(x) \in K_2[x]$. If E_1 is a splitting field of $f(x)$ over K_1 and E_2 is splitting field of $\sigma f(x)$ over K_2. Then there is an isomorphism from E_1 onto E_2*

Proof. Clearly $E_1|K_1, E_2|K_2$ are field extensions. If $[E_1 : K_1] = 1$, then $dim_{K_1}(E_1) = 1$ and so $E_1 = K_1$. $f(x) = (x - \alpha_1)\cdots(x - \alpha_t)$, where

$\alpha_i \in E_1$. Now, $\sigma(f(x)) = \sigma(x-\alpha_1)\cdots\sigma(x-\alpha_t) = (x-\sigma(\alpha_1))\cdots(x-\sigma(\alpha_t))$. Since F_2 is a splitting field of $\sigma(f(x))$, $F_2 \subseteq K_2 \subseteq E_2$. Hence $\sigma : E_1 \to E_2$ is an isomorphism. Assume that theorem is true for $[E_1 : K_1] \leq n$. Let $[E_1 : K_1] = n > 1$. Since $f(x) \in K_1[x]$ and $K_1[x]$ is UFD, $f(x) = p_1(x)p_2(x)\cdots p_t(x)$. If $deg(p_1(x)) = 1$, for all i, then $p_i(x) = a_i(x) + b_i, \frac{-b_i}{a_i} \in K_1$ is a root of $p_i(x)$ and $f(x)$. Since E_1 is the splitting field of $f(x)$ over K, $E_1 \subseteq K_1 \subseteq F_1$, Thus $[E_1 : K_1] = 1$, a contradiction. Hence, $deg(p_i(x)) > 1$, for some i. Let α_1 be a root of $p_1(x)$ and α_2 be a root of $\sigma(f(x))$. Then there is an isomorphism $\theta : K_1(\alpha_1) \to K_2(\alpha_2)$. Then the splitting field of $f(x)$ over $K_1(\alpha_1)$ is E_1 and the splitting field of $\sigma(f(x))$ over $K_2(\alpha_2)$.$[E_1 : K_1] = [E_1 : K_1(\alpha_1)][K_1(\alpha_1) : K_1]$.
$\Rightarrow [E_1 : K_1(\alpha_1)] = \frac{[E_1:K_1]}{[K_1(\alpha_1):K_1]} < n$. By induction, there is an isomorphism from E_1 onto E_2. □

Let us sum up:

- Extension fields and finite extension.
- Algebraic of degree n over the field F.
- Algebraic extension.
- Algebraic number and Transcendental number.
- Fundamental theorem of Algebra.

Check your progress

1. If $\mathbb{Q}[\sqrt{3}] = \{a + b\sqrt{3} : \ a, b \in \mathbb{Q}\}$ is a field extension of $\mathbb{Q}$. Hence $[\mathbb{Q}[\sqrt{3}] : \mathbb{Q}] =$
2. A complex number is said to be an algebraic number if it is algebraic over the field of —

1.2 Transcendental

Definition 1.2.1. An element $\alpha \in \mathbb{C}$ is called transcendental over $\mathbb{Q}$ if α is not algebraic over $\mathbb{Q}$.

Example 1.2.2. Let $\alpha = \pi$. Then α is not algebraic over $\mathbb{Q}$ and so α is transcendental over $\mathbb{Q}$.

Clearly α is algebraic over $\mathbb{R}$ and so is transcendental over $\mathbb{R}$.

Theorem 1.2.3. *The number e is transcendental.*

Proof. Let $f(x) \in \mathbb{R}[x]$ and $deg(f(x)) = r$. Let $F(x) = f(x) + f^{(1)}(x) + f^{(2)}(x) + \cdots + f(r)(x)$. Clearly, $f^{(r+1)}(x = 0.)$ Now $\frac{d}{dx}(e^x F(x)) = e^{-x}F^{'}(x) - e^{-x}F(x) = -e^{-x}f(x)$.

(Mean Value Theorem: If $g(x)$ is a continuous differentiable, single valued function on $[a, b]$, then $\frac{g(a)-g(b)}{a-b} = g^{'}(a + \theta(b - a))$ where, $0 < \theta < 1$.)

Apply Mean value theorem of $e^{-x}F[x]$ on $[0, 1]$ we get, $e^{-1}F(1) - F(0) = -e^{\theta_1}f(\theta_1) \implies F(1) - eF(0) = -e^{1-\theta_1}f(\theta_1) = \epsilon_1, 0 < \theta_1 < 1$.

On $[0, 2]$, $\frac{e^{-2}F(2)-F(0)}{2} = e^{-2\theta_2}f(2\theta_2)$

$F(2) - e^2F(0) = -2e^{-2(1-\theta_2)}f(2\theta_2) = \epsilon_2.$

On $[0, n]$, $F(n) - e^nF(0) = -ne^{-n(1-\theta_n)}f(n\theta_n) = \epsilon_n, 0 < \theta_n < 1.$

In general, On $[0, n]$, $F(n)-e^nF(0) = -ne^{-n(1-\theta_n)}f(n\theta_n) = \epsilon_n \cdots\cdots\cdots (1)$

Suppose that, e is an algebraic number. Then, there exists

$$f(x) = c_0 + c_1x + \cdots + c_nx^n \in \mathbb{Z}[x],$$

$c_0 > 0$ such that $f(e) = 0$.

Clearly, $c_0 + c_1e + c_2e^2 + \cdots + c_ne^n = 0 \cdots\cdots\cdot (2)$.

Now, $c_1\epsilon_1 + c_2\epsilon_2 + \cdots + c_n\epsilon_n = c_1(F(1) - eF(0)) + c_2(F(2) - e^2F(0)) + \cdots + c_n(F(n) - e^nF(0)) = c_1F(1) + \cdots + c_nF(n)(c_1e + c_2e^2 + \cdots + c_ne^n)F(0)c_1F(1) + \cdots + c_nFn + c_0F_0 = c_0F(0) + c_1F(1) + \cdots + c_nF(n).$

Hence $c_1\epsilon_1 + \cdots + c_n\epsilon_n = c_0F(0) + c_1F(1) + \cdots + c_nF(n) \cdots\cdots\cdots (3)$

Choose any prime $p > n$ and $p > c_0$. Consider

$$f(x) = \frac{1}{(p-1)!}x^{p-1}(1-x)^p(2-x)^p \cdots (n-x)^p.$$

Let

$$F(x) = f(x) + f^{'}(x) + \cdots + f^r(x).$$

Clearly, $f(x)$ has a root of multiplicity p at $x = 1, 2, \cdots, n$.

From this, $f(j) = 0, f^{'}(j) = 0, f^{''}(j) = 0 \cdots, f^{r-1}(j) = 0$ for all $j = 1, 2, \cdots, n$.

Also $f(x)$ has a root of multiplicity $p - 1$ at $x = 0$.

Clearly, $f(x) = \frac{(n!)^p}{(p-1!)}x^{p-1} + \frac{a_0}{(p-1)!}x^p + \cdots + a_i \in \mathbb{Z}$

For i, p, $f^i(x) \in \mathbb{Z}[x]$and the coefficients of $f^i(x)$ are multiples of p. and so for integer j, $f^i(j)$ is multiple of p. Since $F(x) = f(x) + f^{'}(x) + f^2(x) + \cdots + f^{p-1}(x) + f^p(x) + f^r(j)$.

For $j = 1$ to n, $F(j)$ is an integer and multiple of p. Clearly, $f(0) = f^{'}(0) = \cdots = f^{p-1}(0) = 0$.

For $i \geq p$, $f^i(0) \in \mathbb{Z}$ and is multiple of p. but $f^{p-1}(0) = (n!^p$

Since $p \geq n$, $p \nmid n! \implies p \nmid (n!)^p$

$F(0) = f(0) + f^1(0) + \cdots + f^{(p-2)}(0) + f^{(p-1)}(0) + f^{(p)}(0) + \cdots + f^r(0)$.

Hence $p \nmid F(0)$. $p/F(1), \cdots, p/F(n)$.

From this, $c_0F(0) + c_1F(1) + \cdots + c_nF(n)$is an integer and is not divisible by p.

By (3), $c_0F(0) + c_1F(1) + \cdots + c_nF(n) = c_1\epsilon 1 + \cdots + c_n\epsilon_n$.

$\epsilon_i = -ie^{i(1-\theta_i)f(i\theta_i)}, 0 < \theta_1 < 1$.

$$\epsilon_i = \frac{-ie^{i(1-\theta_1)}(i\theta_1)^{p-1}(1-i\theta_1)^p \cdots (n-i\theta_1)^p}{(p-1)!}$$

$$|\epsilon_1| \leq \frac{n}{(p-1)!}e^n n^{p-1}1^p 2^p \cdots n^p = \frac{nn^{p-1}e^n(n!)^p}{(p-1)!}$$

$|\epsilon_i| \leq \frac{e^n(n!)^p n^p}{(p-1)!}$

as $p \to \infty, |\epsilon_i| \leq \frac{e^n(n!)^p n^p}{(p-1)!} \to 0$.

Thus we can find a large prime p such that, $p > c_0$, and $p > n$,

$|c_0\epsilon_1 + \cdots + c_n\epsilon_n| < n \implies c_1\epsilon_1 + \cdots + c_n\epsilon_n = 0$.

$c_0F(0) + \cdots + c_nF(n) = c_1\epsilon_1 + \cdots + c_n\epsilon_n = 0$.

$p|0 \implies p|c_0F(0) + \cdots + c_nF(n)$, which is a contradiction. Hence p is not algebraic over $\mathbb{Q}$.

□

Let us sum up:

- The number e is transcendental.
- $e^{m/n}$ is transcendental $(m > 0,\ n\ are\ integers)$.

Check your progress 5.2

1. The number e is called —
2. If $a, b \in K$ are algebraic over F of degrees m and n, then $F(a, b) =$

Unit Summary:

In this unit, we recalled the basic of rings and commutative ring with unit element. Next, we introduced fields and analyzed the characteristics of fields. Further studied how to extend a field to extension field and the concept of algebraic extensions. Finally we showed that the number e is transcendental.

Glossary:

- $[K : F]$ is the dimension of K over F.
- $[L : F] = [L : K][K : F]$.
- $[F(a) : F] = n$ If $a \in K$ is algebraic of degree n over F.
- The number e is transcendental.

Self Assessment Questions

1. Show that the number e is transcendental.

2. If $a \in K$ is algebraic over F, then prove $F(a)$ is a finite extension of F.

3. If $F(a)$ is a finite extension of F, then prove $a \in K$ is algebraic over F.

4. Prove that the mapping $\psi : F[x] \to F(a)$ defined by $h(x)\psi = h(a)$ is a homomorphism.

Exercises

1. In R, $\sqrt{2}$ and $\sqrt{3}$ are both algebraic over Q. Exhibit a polynomial of degree 4 over Q satisfied by $\sqrt{2}+\sqrt{3}$. Find the degree of $\sqrt{2}+\sqrt{3}$ over Q and degree $\sqrt{2}\sqrt{3}$ over Q.

2. If $m > 0$ and n are integers, prove that $e^{\frac{m}{n}}$ is transcendental.

3. What is the degree of $\sqrt{2}+\sqrt{3}$ over Q ? Prove your answer.

4. If a is an algebraic integer and m is an ordinary integer, prove
   (a) $a + m$ is an algebraic integer.
   (b) ma is an algebraic integer.

Answers for check your progress

Section 1.1

1. 2

2. Rational numbers

Section 1.2

1. Transcendental
2. $F(b, a)$

References:

1. I.N. Herstein, Topics in Algebra (II Edition) Wiley Eastern Limited, New Delhi, 1975.

Suggested Reading:

1. M. Artin, Algebra, Prentice Hall of India, 1991.
2. P.B. Bhattacharya, S.K. Jain, and S.R. Nagpaul, Basic Abstract Algebra (II Edition) Cambridge University Press, 1997. (Indian Edition)
3. I.S. Luther and I.B.S. Passi, Algebra, Vol. I âĂŞGroups(1996); Vol. II Rings, Narosa Publishing House , New Delhi, 1999
4. D.S. Malik, J.N. Mordeson and M.K. Sen, Fundamental of Abstract Algebra, McGraw Hill (International Edition), New York. 1997.
5. N. Jacobson, Basic Algebra, Vol. I & II Hindustan Publishing Company, New Delhi.

UNIT - 2

Unit 2

More About Roots

Objectives:

- Know to field and extension field over ring polynomials.
- To introduced splitting field with properties.
- To study more about roots of polynomials.
- Know to the concept of simple extension.

2.1 Roots of Polynomials

Definition 2.1.1. *If $p(x) \in F(x)$, then an element a lying in some extension field of $F(k)$ is called a root of $p(x)$ if $p(a) = 0$.*

Lemma 2.1.2. *If $p(x) \in F[x]$ and K is an extension of F, then for any element $b \in K$, $p(x) = (x - b)q(x) + p(b)$ where $q(x) \in K[x]$. and $degq(x) = degp(x) - 1$.*

Proof. Since $F \subset K, F[x]$ is contained in $K[x]$. we can consider $p(x)$ to be lying in $k[x]$.

By the division algorithm for polynomial in $k[x]$.

$$p(x) = (x - b)q(x) + r(x)$$

where $q(x) \in k[x]$ and $r = 0$ (or) $degr < deg(x - b)$.
This gives either $r = 0$ (or) deg $r = 0$, either r must be an element of K.
Since $p(x) = (x - b)q(x) + r$

$$P(b) = 0 + r \Rightarrow r = P(b)$$

Thus, $p(x) = (x - b)q(x) + p(b)$.

Then,

$$\begin{aligned} degp(x) &= deg[(x - b)q(x) + p(b)] \\ degp(x) &= deg(x - b) + degq(x) + degp(b) \\ degp(x) &= 1 + degq(x) + 0 \\ degp(x) - 1 &= degq(x) \end{aligned}$$

Hence proved. □

Corollary 2.1.3. *If $a \in K$ is a root of $p(x) \in F[x]$, where$F \in K$, then in $K[x], (x - a) \mid p(x)$.*

Proof. Since $p(x) \in F[x]$ and $F \in K$, then $p(x) \in F[x]$. but $a \in k$, then by lemma 2.1.1, in $k[x]$,

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

where $q(x) \in K[x]$ and $degp(x) - 1 = degq(x)$.

Since $a \in K$ is a root of $p(x)$ then $p(a) = 0$.

$$\Rightarrow p(x) = (x-a)q(x)$$

$$\Rightarrow (x-a) \mid p(x) \text{ in } k[x].$$

□

Definition 2.1.4. The element $a \in K$ is a root of $p(x) \in F[x]$ of multiplicity m if $(x-a)^m \mid p(x)$, whereas $(x-a)^{m+1}$ f $p(x)$.

Lemma 2.1.5. *A polynomial of degree n over a field can have atmost n roots in any extension fields.*

Proof. Proof: Let us prove this result by using induction on n, the degree of the polynomial $P(x)$.

If $p(x)$ is of degree 1, then it must be of the form $\alpha x+\beta$, where $\alpha, \beta \in F$ and $\alpha \neq 0$.

Any 'a' such that $p(a) = 0$ implies that $\alpha a + \beta = 0$.

$$\Rightarrow a = -\frac{\beta}{\alpha}$$

That is, $p(x)$ has the unique root $-\beta/\alpha$.

Therefore, the result is true in this case.

Assume that the result is true in any field for all polynomials of degree less than n.

Suppose that $p(x)$ is of degree n over F. Let k be any extension of F. If $P(x)$ has no roots in K, then for the number of roots in k, namely zero, is definitely at most n.

So, suppose that $P(x)$ has at least one root $a \in k$ and ‘ a ’ is a root of multiplicity m.

Since $(x-a)^m \mid p(x), m \leq n$, then

$$P(x) = (x-a)^m q(x), \quad q(x) \in K[x]$$

and deg $q(x) = n - m$.

From $(x-a)^{m+1} \nmid p(x)$,

we get

$$(x-a) \nmid q(x).$$

By corollary to lemma 2.1.1, ‘ a ’ is not a root of $q(x)$.

If $a \neq b \in K$ is a root of $P(x)$, then $p(b) = 0$

$$\Rightarrow (b-a)^m q(b) = 0$$

$$\Rightarrow q(b) = 0,$$

since $(b-a) \neq 0$.

That is, any root of $p(x)$, in K, other than ‘ a ’, must be a root of $q(x)$. since, degree of $q(x) = n - m$, which is less than n, then by our induction hypothesis, $q(x)$ has at most $n - m$ roots in K, which together with the other root ‘ a ’, counted m times, gives that $p(x)$ has at most $m + (n-m) = n$ roots in k.

Hence proved. □

Theorem 2.1.6. *If $p(x)$ is a polynomial in $F[x]$ of degree $n \geq 1$ and is irreducible over F, then there is an extension E of F, such that $[E : F] = n$, in which $p(x)$ has a root.*

Proof. Let $F[x]$ be the ring of polynomials in x over F. and let $V = (p(x))$ be the ideal of $F[x]$ generated by $p(x)$.

By lemma "The ideal $A = (P(x))$ in $F[x]$ is a maximal ideal if and only if $p(x)$ is irreducible over F", we have

V is a maximal ideal of $F[x]$.

Then by theorem "If R is a commutative ring with unit element and M is an ideal of R, then M is a maximal ideal of R if and only if R/M is a field", we have

$$E = F[x]/v$$

is a field.

First to show that E is an extension of F.
Let $\bar{F}$ be the image of F in E. i.e., $\bar{F} = \{\alpha + V \mid \alpha \in F\}$ We assert that $\bar{F}$ is a field isomorphic to F.

If $\psi : F[x] \to E$, defined by

$$f(x)\psi = f(x) + V \quad \forall f(x) \in F[x]$$

then the restriction of ψ to F induces an isomorphism of F onto F.

By using this isomorphism, consider E to be an extension of F.

We claim that, E is a finite extension of F of degree $n =$deg $p(x)$, for the elements

$$1+V, x+V, (x+V)^2 = x^2+V, \ldots, (x+V)^i = x^i+V, \ldots,$$
$$(x+V)^{n-1} = x^{n-1}+V.$$

form a basis of E over F.

Let ' a ' be any element in the field E, such that

$$a = x\psi = x+V$$

Given $f(x) \in F[x]$

To claim that $f(x)\psi = f(a)$. since ψ is a homomorphism and if

$$f(x) = \beta_0 + \beta_1 x + \beta_2 x^2 + \cdots + \beta_k x^k,$$

then

$$f(x)\psi = \beta_0\psi + (\beta_1 x)\,\psi + \left(\beta_2 x^2\right)\psi + \cdots + \left(\beta_k x^k\right)\psi$$

$$= \beta_0\psi + (\beta_1\psi)\,(x\psi) + (\beta_2\psi)\,(x^2\psi) + \cdots + (\beta_k\psi)\left(x^k\psi\right)$$

By using the identification indicated $\beta\psi$ with β,

$$\begin{aligned} f(x)\psi &= \beta_0 + \beta_1(x\psi) + \beta_2\left(x^2\psi\right) + \cdots + \beta_k\left(x^k\psi\right) \\ &= \beta_0 + \beta_1(x+V) + \beta_2\left(x^2+V\right) + \cdots + \beta_k\left(x^k+V\right) \\ &= \beta_0 + \beta_1(x+V) + \beta_2(x+V)^2 + \cdots + \beta_k\,(x+V)^k \\ &= \beta_0 + \beta_1 a + \beta_2 a^2 + \cdots + \beta_k a^k \\ &= f(\alpha) \end{aligned}$$

$$\Rightarrow f(x)\psi = f(a).$$

since $p(x) \in V and V$ is a maximal ideal of $F[x]$, then

$$p(x)\psi = 0$$

But, $p(x)\psi = p(a)$

$$\Rightarrow p(a) = 0$$

Thus, the element $a = x\psi$ in E is a root of $p(x)$. □

Let us sum up:

- Remainder Theorem.
- Roots of the polynomial and Roots of multiplicity.
- Reducible and irreducible of the polynomial.
- Splitting field.

Check your progress

1. If a is root of $p(x) \in F[x]$ of multiplicity m then —
2. The splitting field of $f(x) = x^2 - 3$ over Q is —

2.2 More About Roots

Definition 2.2.1. Let $f(x) \in F[x]$ and $\alpha \in K$ be a root of $f(x)$ in some extension K of F. α is a multiple root of $f(x)$ with multiplicity m if $(x-\alpha)^m | f(x)$ and $(x-\alpha)^{m+1} \not| f(x)$.

If $m = 1$, then α is a simple root of $f(x)$. If $f(x)$ is separable, it has no multiple roots. Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in F[x]$. Then, $f^x = a_1 + 2a_2 x + \cdots + n a_n x^{n-1} \in F[x]$.

$(f(x)+g(x))^{'} = f^{'}(x) + g^{'}(x), (\alpha f(x))^{'} = \alpha f^{'}(x)$ and $(f(x)g(x))^{'} = f^{'}(x)g(x) + g^{'}(x)f(x)$.

Theorem 2.2.2. Let $f(x) \in F[x]$. Let α be a root of $f(x)$. Then α is a multiple root of $f(x)$ iff $f^{'}(\alpha) = 0$.

Proof. Suppose α is a multiple roots of $f(x)$ with mutliply $m > 1$. By definition, $(x-\alpha)^m | f(x)$ and $(x-\alpha)^{m+1}$ does not divide $f(x)$. That implies, $f(x) = (x-\alpha)^m g(x)$, for some $g(x) \in K[x]$. $f^{'}(x) = (x-\alpha)^m g^{'}(x) + m(x-\alpha)^{m-1} g(x)$. Therefore, $f^{'}(x) = 0$. Conversely, $f^{'}(\alpha) = 0$, Suppose α is not a multiple root of $f(x)$. Then α is a simple root of $f(x)$. By remainder theorem, $f(x) = (x-\alpha)q(x)$ for some $g(x) \in F[x], g(\alpha) \neq 0$. That implies, $f^{'}(x) = (x-\alpha)q^{'}(x) + q(x), f^{'}(\alpha) \neq 0$, which is a contradiction to $f^{'}(\alpha) = 0$. Therefore, α is a multiple root of $f(x)$. □

Corollary 2.2.3. *Let $f(x) \in F[x]$. Then $f(x)$ has no multiple root if and only if $(f(x), f^{'}(x)) = 1$.*

Proof. Suppose, $f(x)$ has no multiple root, Clearly $(f(x), f^{'}(x)) \in F[x]$. Let $(f(x), f^{'}(x)) = deg(d(x)) \geq 1$. Then $f(x) = \lambda_1(x)d(x)$ and $f^{'}(x) = \lambda_1(x)d(x)$ for some $\lambda(x), \lambda_1(x) \in F[x]$. Let α be a root of $d(x)$. Then $d(\alpha) = 0$. Then, $f(\alpha) = 0$. α is a multiple root of $f(x)$, which is a contradiction.

Conversely, $(f(x), f^{'}(x)) = 1$, Suppose $f(x)$ has multiple roots say α. Then α is a root of $f^{'}(x), (x-\alpha)|f(x)$ and $(x-\alpha)|f^{'}(x)$. That implies, $(f(x), f^{'}(x)) = (x-\alpha)\lambda(x)$ for some $\lambda(x) \neq 1$, which is a contradiction. Hence $f(x)$ has no multiple roots. □

Proposition 2.2.4. *Let $x^{p^n - x} \in F[x]$ where char$(F) = p$, $f(x)$ has no mulitple root.*

Proof. Let $f(x) = x^{p^n - x} \in F[x]$. Then $f^{'}(x) = p^n x^{p^n - 1} - 1 = 0 - 1 = 1$. Also $f^{'}(x) = -1$. Therefore $(f(x), f^{'}(x)) = 1$ if and only if $f(x)$ has no multiple roots. □

Proposition 2.2.5. *Let char$(F) = 0$. If $f(x)$ is irreducible over F, then $f(x)$ has no multiple root.*

Proof. Clearly, $f'(x) \in F[x]$ and $\deg(f'(x)) < \deg(f(x))$. Since $f(x)$ is irreducible, $f(x)$ and 1 are the only factors of $f(x)$. Therefore, $f'(x)$ is not divisible by $f(x)$, and hence 1 is the only common factor of $f(x)$ and $f'(x)$. Thus, $(f(x), f'(x)) = 1$. By Corollary 2.2.3, $f(x)$ has no multiple roots. □

Corollary 2.2.6. *If $f(x)$ is irreducible over a field F where F is a subfield of K, then $f(x)$ has no multiple roots.If $f(x)$ is irreducible over a field F where F is a subfield of K, then $f(x)$ has no multiple roots.*

Proof. Clearly $\text{char}(F) = 0$ and the proof follows from the above proof.

□

2.2.1 Simple Extension

Definition 2.2.7. A simple extension of F is an extension K of F such that $K = F(a)$ for some $a \in K$.

Example 2.2.8. $\mathbb{Q}(\sqrt{2})|\mathbb{Q}$, $\mathbb{Q}(\sqrt{3})|\mathbb{Q}$ $\mathbb{Q}(\sqrt{5})/\mathbb{Q}$ are simple extensions.

Problem 2.2.9. Is $\mathbb{Q}(\sqrt{2}, \sqrt{3})|\mathbb{Q}$ simple?

Proof. Note that $\sqrt{2}, \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$ and $\sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Therefore, $\mathbb{Q}(\sqrt{2} + \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Let $\sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$, $\alpha = \frac{1}{(\sqrt{2}+\sqrt{3})}$. Then $\alpha = \frac{\sqrt{2}-\sqrt{3}}{(\sqrt{2}+\sqrt{3})(\sqrt{2}-\sqrt{3})} = -(\sqrt{2} - \sqrt{3}) \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Hence, $2\sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$
$\sqrt{2}, \sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$ and so $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

Therefore, $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ is a simple extension. □

Proposition 2.2.10. *Let F be a finite field of order p^n. Then $(F^{\times}, \cdot)$ is cyclic.*

Proof. Let $|F| = p^n$. Then $(F^\times, +, \cdot)$ is an abelian group and $|F^\times| = p^n - 1$.

Let α be a maximum order element in $F^\times$ and let $m = \mathrm{ord}(\alpha)$. Then $|\beta|/|\alpha|$ for all $\beta \in F^\times$. For $\beta \in F^\times, \beta^m = \beta^{t|\beta|} = (\beta^{|\beta|})^t = 1$. β is a root of $x^m - 1$, where $forall \beta \in F^\times$. Since $\alpha^m = 1$, $1, \alpha, \alpha^2, \ldots, \alpha^m$ are distinct elements in$F^\times$. $|F^\times| \geq m \mid |F^\times| = m > \alpha$. Therefore, $F^\times$ is a cyclic group generated by α, and α is a primitive element in F. □

Proposition 2.2.11. *Let G be a simple finite abelian group. Let a be the maximum order element in G. Then $|b|$ divides $|a|$ for all $b \neq a$ in G.*

Proof. Suppose there is an element $b \neq e \in G$ such that $|b| \nmid |a|$. Then, $ab \in G$, $|ab| = \gcd(|a|, |b|), lcm\{(|a|, |b|)\} > |a|$ which is a contradiction to choice of a. Hence, $|b|/|a|$ for all $b \neq e$ in G. □

Theorem 2.2.12. *Let $f(x) \in F[x]$, where $char(F) = p$ (prime). Then $f'(x) = g(x^p)$ for some $g(x) \in F[x]$.*

Proof. Let $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$. Then, $f'(x) = a_1 + 2a_2x + 3a_3x^2 + \cdots + na_nx^{n-1}$.

Suppose $f^{'}(x) = 0$. Then, $1 \cdot a_1 + 2 \cdot_2 x + 3 \cdot a_3x^2 + \cdots + na_nx^{n-1} = 0$. Since $F[x]$ is a vector space over F, $\{1, x, x^2, \cdots,\}$ is a basis for $F[x]$ over F.and $\{1, x, x^2, \ldots, x^{n-2}, x^{n-1}\}$ is a linearly independent in $F[x]$ over F. we have $a_1 = 2a_2 = \cdots = (n-1)a_{n-1} = na_n = 0$. $a_m = 0$if $p \nmid m$. Therefore, $f(x) = a_0 + a_px^p + a_{2p}x^{2p} + \cdots + a_{tp}x^{tp} = g(x^p)$, where $g(x) = a_0 + a_px + a_{2p}x^2 + \cdots + a_{tp}x^t \in F[x]$.

Conversely, suppose $f(x) = g(x^p)$, where $g(x) = b_0 + b_1 x + \cdots + b_m x^m \in F[x]$. Then, $f(x) = b_0 + b_1 x^p + b_2 x^{2p} + \cdots + b_m x^{mp}$, and $f'(x) = pb_1 x^{p-1} + 2pb_2 x^{2p-1} + \cdots + mpb_m x^{mp-1}$.

Since char$(F) = p$, we have $f'(x) = 0$. □

Proposition 2.2.13. *Let char$(F) = 0$ and $f(x) \in F[x]$. If $f'(x) = 0$, then $f(x)$ is a constant polynomial.*

Proof. $f'(x) = 0 \Rightarrow a_1 + 2a_2 x + 3a_3 x^2 + \cdots + na_n x^{n-1} = 0$.

Since char$(F) = 0$, F is a field of characteristic zero,Q is a subfield of F, Since $\{1, x, x^2, \ldots, x^{n-1}\}$ is a linearly independent in $F[x]$ over F. $ma_m = 0$, for all $m = 1$ to n. $\rightarrow a_m = 0$. Hence, $f(x) = a_0$ is a constant polynomial. □

Theorem 2.2.14. *Let $f(x) \in F[x]$ be an irreducible polynomial over F. Then all the roots of $f(x)$ have the same multiplicity.*

Proof. Let $f(x) \in F[x]$ be an irreducible polynomial. If char$(F) = 0$, then $f(x)$ has no multiple roots. Hence, all its roots have multiplicity 1.Assumechar$(F) = p$ (prime). Let α be a root of $f(x)$ with multiplicity m. Let $f(x) = (x - \alpha)^m g(x)$ for some $g(x) \in F(\alpha)[x]$. $\rightarrow g(\alpha) \neq 0$, Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ Let β be the root of $f(x)$ and $\beta \neq \alpha$. Consider $I : F \rightarrow F$ is an identity isomorphim. Then $I(f(x)) = f(x)$. By theorem, there exists an isomorphism $\sigma : F(\alpha) \rightarrow F(\beta)$ such that $\sigma(\alpha) = I(\alpha)$ for all $\alpha \in F$ and $\sigma(\alpha) = \beta$.Then, $\sigma(f(x)) = \sigma(a_0) + \sigma(a_1)x + \cdots + \sigma(a_n)x^n =$

$a_0 + a_1x + \cdots + a_n$

$\sigma(f(x)) = f(x) = \sigma((x-\beta)^m(g(x))$.we have $f(x) - \sigma(f(x)) = (x - \beta)^m\sigma(g(x))$. Claim: $\sigma(g(\beta)) \neq 0$ Let $g(x) = b_0 + b_1x + \cdots + b_mx^m \in F(\alpha)[x]$.

Then$\sigma(g(x)) = \sigma(b_0) + \sigma(b_1)x + \cdots + \sigma(b_m)x^m$

$= \sigma(b_0) + \sigma(b_1)\beta + \cdots + \sigma(b_m)\beta^m$

$= \sigma(b_0) + \sigma(b_1)\sigma(\alpha) + \cdots + \sigma(b_m)\sigma(\alpha)^m$

$= \sigma(b_0 + b_1\alpha + \cdots + b_m\alpha^m)$

$= \sigma(g(\alpha)) \neq 0$. Therefore, β is not root of $\sigma(g(x))$.

By definition, β is a root of $f(x)$ with multiplicity m. □

2.2.2 Separable Extension

Definition 2.2.15. *Let $[K : F]$ be a field extension. An element $\alpha \in K$ is separable over F if $f(\alpha) = 0$ for some separable polynomial $f(x) \in F[x]$. $[K : F]$ is separable extension if $\alpha \in K$ is separable over F, for all $\alpha \in K$.*

Proposition 2.2.16. *Let char$(F) = 0$. Then any algebraic extension of F is separable.*

Proof. Let $[K : F]$ be any algebraic extension. For any $\alpha \in K$, α is a root of some minimal polynomial $m_\alpha(x) \in F[x]$. Since $m_\alpha(x)$ is irreducible and char$(F) = 0$, $m_\alpha(x)$ is separable over F. Hence, $[K : F]$ is a separable extension. □

Example: $K = \mathbb{Q}(\sqrt{p}$: p is prime)is an infinite algebraic extension.

Theorem 2.2.17. *Let $f(x) = x^p - a \in F[x]$, where char$(F) = p$. Then either $f(x)$ is irreducible over F (or) $f(x)$ is the pth power of a linear polynomial.*

Proof. Let $f(x) = x^p - a \in F[x]$. Let b be a root of $f(x)$ in some extension K of F. Then $F(b) = 0$, $b^p - a = 0 \implies a = b^p \in F$.

Therefore, $f(x) = x^p - b^p = (x - b)^p$. If $b \in F$, then $f(x) = (x - b)^p$. Suppose, $b \notin F$. Since b is a root of $f(x)$ over F, b is algebraic over F. Let $m_b(x)$ be the minimal polynomial of b over F. Then $m_b(x) \mid f(x)$.

Since $f(x) = (x - b)^p$, if $b \in F$, then $f(x) = (x - b)^p$. Suppose b is a root of $f(x)$ over F, b is algebraic over F. $m_{b,F}(x)/f(x)$ or $m_{b,F}(x) \in F[x]$ we have $f(x) = (x - b)^t$ for some $t \leq p$. Then b is a root of $q(x)$ and $q(x) = m_{b,F}(x) = (x - b)^t$.

Sinc$m_{b,F}(x) \mid f(x)$, we have $f(x) = m_{b,F}(x) \cdot \eta_{b,F}(x) \cdots \eta_{b,F}(x) = (x - b)^{tm}$. Since $\deg(f(x)) = p$, $p = tm$ and p is prime, $t = 1$ or $m = 1$. $t = 1$, then $m_{b,F}(x) = x - b \implies \in F$, which is a contradiction. Hence, $m = 1, t = p$, $f(x) = (x - b)^t = (x - b)^p = m_{b,F}(x)$.Hence, $f(x)$ is irreducible over F. □

Theorem 2.2.18. *Let char$(F) = p$. Then every algebraic extension of F is separable if and only if $F = F^p$.*

Proof. Let $F_p^n = \{\alpha^p : \alpha \in F_{p^n}\}$ and $\sigma : F_{p^n} \to F_{p^n}$ by $\sigma(\alpha) = \alpha^p \implies \sigma \in Aut(F_{p^n})$. $(\sigma) = F_{p^n} = \{\alpha^p : \alpha \in F_{p^n}\}$. suppose, any algebraic extension of F is separable, For any $\alpha \in F$, Le$f(x) = x^p - a \in F[x]$ then

b is a root of $f(x)$ in some extension of F and $K = F(\alpha)$ $[F(b) : F] = \deg(g(x)) < \infty$, $\implies$ $F(b)/F$ is algebraic. By hypothesis, $F(b)/F$ is separable and b is separable over F. Suppose $b \notin F$. Then by previous theorem, $f(x)$ is irreducible over F and $f'(x) = px^{p-1}$. $f^{'}(b) = pb^{p-1} = 0$ $\rightarrow b$ is a root of both $f(x)$ and $f'(x)$, By theorem, b is a multiple root of $f(x)$ and so $\implies$ b is not separable over F. which is a contradicition.f Hence,$b \in F, b^p - a = 0 \implies a = b^p \in F^p \implies F \subseteq F^p$ For any, $y \in F$, $y = d^p$ for some $d \in F \implies y \in F \implies F^p \subseteq F$. Hence, $F = F^p$. Let $[K : F]$ be any algebraic extension. Suppose $[K : F]$ is not separable.Then, there exists $\alpha \in K, \alpha \notin F_1$, such that α is not separable over F. $\implies$ $m_{\alpha,F'}(x) = 0$. $\implies$ $m_{\alpha,F}(x) = g(x^p)$ for some $g(x) \in F[x]$.Put $g(x) = a_0 + a_1x + \cdots + a_mx^m \in F[x]$. Since $a_i \in F$, and $F = F^p$, $a_i = b_i^p$ $g(x) = b_0^p + b_1^px + \cdots + b_m^px^m = (b_0 + b_1x + \cdots + b_mx^m)^p \implies m_{\alpha,F}(x)$ is irreducible over F. which is a contradiction to $m_{\alpha,F}(x)$ is irreducible over F. □

Definition 2.2.19. *A field F is perfect if all finite extensions of F are separable.*

(1) Let $[K : F]$ be any finite extension. Then $[K : F]$ is algebraic. For any $a \in K$, let $m_a(x)$ be the minimal polynomial of a over F. Since $\mathrm{char}(F) = 0$, $m_a(x)$ is separable over F. Hence $[K : F]$ is a separable extension. Therefore, F is perfect.

(2) If char$(F) = 0$ and $[K : F]$ is any finite extension, then $[K : F]$ is a separable extension. Hence, F is perfect.

Theorem 2.2.20. *Let F be a field and char$(F) = p$. Then F is perfect if and only if $F = F^p$.*

Proof. Suppose F is perfect. Then by definition, every finite extension K of F is separable. $[K : F]$ is algebraic, $[K : F]$ is separable $\Rightarrow F = F^p$.Conversely, $F = F^p$. Let $[K : F]$ be any finite extension.

Then$[K : F]$ is algebraic and $[K : F]$ is separable. Therefore, F is perfect. □

Theorem 2.2.21. *Let $[K : F]$ be a finite separable extension. Then $K = F(a)$ for some $a \in K$.*

Proof. Since, $[K : F]$, is finite, $K = F(\alpha_1, \alpha_2, \cdots \alpha_n)$. where $\{\alpha_1, \alpha_2, \cdots \alpha_n\}$ is a basis for K over F. Suppose, F is a finite field. Clearly, $K = \{a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n : a_i \in F\}$ Consider, $F = \mathbb{F}_p^m$ and $|K| = (p^m)^n = p^{mn} \implies K = F_{p^{mn}}$. $F_{p^{mn}} =< \alpha >= F_{p^{mn}}(\alpha) \implies [K : F]$ is simple extension.

Suppose, F is an infinite field.Then $|K| < \infty$ we prove by induction on n, when $n = 2$, For any $\alpha, \beta \in K, \alpha \neq \beta, \alpha, \beta$ are separabl over F. $m_{\alpha,F}(x), m_{\beta,F}(x)$ are separable over F. $\alpha = \{a_1, a_2, \ldots, a_m\}$ be a root of $m_{\alpha,F}(x)$. $\beta = \{b_1, b_2, \ldots, b_n\}$ be a root of $m_{\beta,F}(x)$.

Consider the equation, $(\alpha - a_i) + (\beta - b_j)x = 0$ for $i = 1$ to m, $j = 1$ to t. Since F is infinite, there exists $\gamma \in F$, such that

$(a-a_i)+\gamma(\beta-b_j)x \neq 0$, $\alpha+\gamma\beta \neq a_i+\gamma b_j$ for all i, j. Let $\lambda = \alpha+\gamma\beta \in K$. Therefore, $h(x) = m_{\alpha,F}(\lambda-\gamma x)$. Then, $h(\beta) = m_{\alpha,F}(\lambda-\gamma x) = m_{\alpha,\beta}(\alpha) = 0$. Therefore, β is a root of both $h(x)$ and $m_{\beta,F}(x)$. Suppose b_j is a root of $h(x)$ for some $j \geq 2$. Then $h(b_j) = m_{\alpha,F}(\lambda - \gamma b_j) = 0.\lambda - \gamma b_j$ is a root of $m_{\alpha,F}(x)$. Since $\{a_1, a_2, \cdots, a_n\}$ are roots of $m_{\alpha,F}(x)$. $\lambda, \gamma b_j = a_i$ for some i. $\lambda = a_i + \gamma b_j$ which is contradiction $\lambda \neq a_i + \gamma b_j$ for all i, j. Therefore, b_1 is the only common root to both $h(x)$ and $m_{\beta,F}(x)$. Since, $F \in F(\lambda), m_{\beta,F}(x) \in F(\lambda)[x]$. Since, $b_1(x) \in F(\lambda)[x]$, $m_{\beta,F}(x), h(x)) = (x - \beta) \in F(\lambda)[x]$. $\implies$ $\beta \in F(\lambda)$ and $\gamma\beta \in F(\lambda)$. Since, $\lambda = \alpha + \beta\gamma \in F[\lambda], \lambda - \beta\gamma = \alpha \in F(\lambda)$. $\implies$ $K = F(\alpha, \beta) \subseteq F(\lambda)$ $\implies$ $F(\lambda) = F(\alpha, \beta) = K$. Therefore, $[K : F]$ is simple extension. Assume that the theorem is true for $n - 1$, Then $K = F(\alpha_1, \alpha_2, \cdots \alpha_n) = F(\delta)$ for some $\delta \leq k$. Since $K = F(\alpha_1, \alpha_2, \cdots \alpha_n) = F(\alpha_1, \alpha_2, \cdots \alpha_n - 1)(\alpha_n) = F(\delta)(\alpha_n) = F(\delta, \alpha_n) = F(\lambda^{'})$ $\implies$ $\lambda^{'} \in K$. Therefore, $[K : F]$ is simple extension. □

Theorem 2.2.22. *Let $f(x) = x^{p^n} - x \in F[x]$. Then $f(x)$ is the product of distinct irreducible polynomials $p(x)$ and* $\deg(p(x))$ *divides n.*

Proof. Since $F[x]$ is a unique factorization domain, $f(x) = P_1(x) \cdots P_k(x)$ where each $P_i(x)$ is irreducible over F of degree d_i. $P_i(x) \neq p_j(x)$.

Consider $P_i(x)$, Then by the above theorem, $P_i(x) | x^{p^{d_i}} - x$ over F.

All roots of $P_i(x)$ lie in $F_{p^{d_i}}$ and $F_{p^{d_i}} = F(\alpha_i)$, where α_i is a root of

$P_i(x) for i = 1 to t.$.and $f(\alpha_i) = 0$, so $\alpha_i \in F_{p^n}$ and $F(\alpha_i) \subseteq F_{p^n}$, $|F[\alpha_i]| = p^{d_i}$ and $F(\alpha_i)$ is a subfield of $\mathbb{F}_{p^n}$.

Therefore$d_i|n$. □

Let us sum up:

- Derivative of the polynomial.
- Nontrivial common factor.
- Simple extension.
- Seperable and perfect.

Check your progress

1. If $f(x) \in F[x]$ is irreducible with characteristic of F is 0, then $f(x)$ has —
2. If F is of characteristic 0 and $f(x) \in F[x]$ then —

Unit Summary:

In this unit, we studied the field and extension field over ring polynomials. In addition, we introduced splitting field with properties. Also, analysed more about roots of polynomials. Finally, we introduced the concept of simple extension.

Glossary:

- Remainder theorem.

- Extension field.

- Splitting fields.

- If $x^{p^n} - x \in F[x]$ for $n \geq 1$, has distinct roots.

- Simple extension.

Self Assessment questions

1. Show that the any two splitting fields of the same polynomial over a given field F are isomorphic by an isomorphism leaving every element of F fixed.

2. The polynomial $f(x) \in F[x]$ has a multiple root if and only if $f(x)$ and $f'(x)$ have a nontrivial common factor.

3. A polynomial of degree n over a field can have at most n roots in any extension field.

4. There is an isomorphism τ^{**} of $F[x]/(f(x))$ onto $F'[t]/(f'(t))$ with the property that for every $\alpha \in F$, $\alpha\tau^{**} = \alpha^{'}, (x + (f(x)))\tau^{**} = t + (f'(t))$.

Exercises

1. If $p(x)$ is irreducible in $F[x]$ and if v is a root of $p(x)$, then prove $F(v)$ is isomorphic to $F'(w)$ where w is a root of $p'(t)$; moreover, this

isomorphism σ can so be chosen that

1. $v\sigma = w$.
2. $\alpha\sigma = \alpha^{'}$ for every $\alpha \in F$.

2. If F is of characteristic 0 and if a, b, are algebraic over F, then prove there exists an element $c \in F(a, b)$ such that $F(a, b) = F(c)$.

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

4. Let F be the field of rational numbers. Determine the degrees of the splitting fields of the polynomials over F.

   (a) $x^4 + 1$

   (b)$x^6 + x^3 + 1$

Answers for check your progress

Section 2.1

1. $(x - a)^m / p(x)$

2. $Q(\sqrt{3})$

Section 2.2

1. No multiple roots

2. $f^{'}(x) = 0$

References:

1. I.N. Herstein, Topics in Algebra (II Edition) Wiley Eastern Limited, New Delhi, 1975.

Suggested Reading:

1. M. Artin, Algebra, Prentice Hall of India, 1991.
2. P.B. Bhattacharya, S.K. Jain, and S.R. Nagpaul, Basic Abstract Algebra (II Edition) Cambridge University Press, 1997. (Indian Edition)
3. I.S. Luther and I.B.S. Passi, Algebra, Vol. I âĂŞGroups(1996); Vol. II Rings, Narosa Publishing House , New Delhi, 1999
4. D.S. Malik, J.N. Mordeson and M.K. Sen, Fundamental of Abstract Algebra, McGraw Hill (International Edition), New York. 1997.
5. N. Jacobson, Basic Algebra, Vol. I & II Hindustan Publishing Company, New Delhi.

UNIT - 3

Unit 3

The Elements of Galois Theory

Objectives:

- Recall the fixed field and subfield.
- To introduced finite extension and simple extension.
- Explain the Galois group and the fundamental theorem of Galios theory.

3.1 Basics of Automorphism

Let R be any commutative ring with identity. A function $\sigma : R \to R$ is an automorphism if σ is bijective and σ is ring homomorphism.

(1) For any commutative ring R with identity, define $I : R \to R$ by $I(x) = x$, clearly, I is bijective, and $I(xy) = I(x)I(y) = xy$, $I(x + y) = I(x) + I(y)$ for all $x, y \in G$. Therefore, I is automorphism of R.

(2) $Aut(R) = \{\sigma : \sigma \text{ is an automorphism of } R\}$. Clearly, $I \in Aut(R) \neq \emptyset$.

(3) $Aut(R)$ is a group under composition.

Example 3.1.1. Consider the integral domain $R = (\mathbb{Z}, +, \cdot)$.

For any, $\sigma \in Aut(R)$ $\sigma(0) = 0$.

For any $m \in \mathbb{Z}^+, \sigma(m) = \sigma(1 + 1 + \cdots + 1) = \sigma(1) + \sigma(1) + \cdots + \sigma(1)$. So $\sigma(m) = m\sigma(1)$.

For any $m \in \mathbb{Z}^-$, m $= -1 - 1 \cdots - 1$ and so $\sigma(m) = \sigma(-1) + \sigma(-1) + \cdots + \sigma(-1). = -m\sigma(-1) = m\sigma(1)$. Therefore, $\sigma(m) = m\sigma(1) = m\sigma(1)$.

Hence, $\sigma(m) = m\sigma(1)$ for all $m \neq 0$ in $\mathbb{Z}$.

Since R is integral domain, $\sigma(1) = 1$ and hence $\sigma(m) = m\sigma(1) = m$ for all $m \in \mathbb{Z}$ and so $Aut(\mathbb{Z}) = \{I\}$.

3.2 Galios Group

Theorem 3.2.1. *Let $[K : F]$ be a field extension and $g(x) \in F[x]$. If σ is an automorphism of K leaving every element of F fixed, then σ is must take a root of $g(x)$ lying in E into a root of $g(x)$ in E.*

Proof. Let $g(x) = a_0 + a_1x + \cdots + a_nx^n \in F[x]$.
Given, $\alpha \in K$, is a root of $g(x), \sigma(a_i) = a_i$ for all i.

Now, $g(\alpha) = a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$.

$g(\sigma(\alpha)) = \sigma_0 + \sigma_1 a_1 + \cdots + \sigma(\alpha^n)a_n = \sigma(a_0) + \sigma(a_1)\sigma(\alpha) + \cdots + \sigma(a_n)\sigma(\alpha^n)$
$= \sigma(a_0) + \sigma(a_1\alpha) + \sigma(a_2\alpha^2) + \cdots + \sigma(a_n\alpha^n)$
$= \sigma(a_0 + a_1\alpha + \cdots + a_n\alpha^n) = \sigma(0) = 0$. Hence $\sigma(\alpha)$ is a root of $g(x)$. □

Example 3.2.2. Find $Aut(\mathbb{C})$.

For any $\sigma \in Aut(\mathbb{C})$, $\sigma(a) = a$ for all $a \in \mathbb{R}$ and $\sigma(a+ib) = \sigma(a) + \sigma(i)\sigma(b)$. From this we get $\sigma(a+ib) = a + \sigma(i)$. Since i is a root of $x^2+1 \in \mathbb{Q}[x]$(or) $\mathbb{R}[x]$ and so $\sigma(i) = \pm i$. Hence $Aut(\mathbb{C}) = \{I, sigma : \sigma(a+ib) = a - ib\} \equiv \mathbb{Z}_2$.

Remark 3.2.3. (i) A prime field is a field containing no proper subfields.
(ii) For any field K, $\mathbb{Q}$ or $\mathbb{Z}_p$ is a prime subfield of K.

Proposition 3.2.4. *Let K be a field and F be a prime subfield of K and $\sigma \in Aut(K)$. Then $\sigma(a) = a$ for all $a \in F$.*

Proof. If char$(K) = 0$, then $\mathbb{Q}$ is prime subfield of K. Therefore $[K : Q]$ is a field extension. For any $p/q \in \mathbb{Q}, \sigma(p/q) = p/q$.
If $char(K) = p$, then $\mathbb{Z}_p$ is subfield of K and so $K|\mathbb{Z}_p$ is field extension. For $m \in \mathbb{Z}_p, \sigma(m) = \sigma(1)m = m$. □

In view of Proposition, we have the following.

Example 3.2.5. If $R = (\mathbb{Q}, +, \cdot)$ or $(\mathbb{R}, +, \cdot)$, then $Aut(R) = \{I\}$.

Definition 3.2.6. Let K be a field and $H \leq Aut(K)$. The fixed field of H is $F_H = \{\alpha \in K : \sigma(\alpha) = \alpha \; \forall \; \sigma \in H\}$.

Clearly F_H is a subset of K.

Proposition 3.2.7. *Let K be a field and $H < Aut(K)$. Then F_H is a subfield of K.*

Proof. Clearly, $F_H \subseteq K$. For any$\sigma \in H, \sigma(0) = 0$, and $\sigma(1) = 1$ and so $0, 1 \in F_H$. Let $a, b \in F_H$ and $b \neq 0$, Then $\sigma(a) = a, \sigma(b) = b, \forall \sigma \in H$. By definition of F_H, $\sigma(a \pm b) = \sigma(a) \pm \sigma(b) = a \pm b$ and so $a \pm b \in F_H$ for all $\sigma \in H$. Also $\sigma(ab) = \sigma(a)\sigma(b) = ab$ for all $\sigma \in H$ and so $ab \in F_H$.

Clearly, $b^{-1} \in K, \sigma(b^{-1}) = \sigma(b)^{-1} = b^{-1}$. From this we get $b^{-1} \in F_H$ and so F_H is a subfield of K. □

Theorem 3.2.8. *Let F be a subfield of K and $G(K : F) = \{\sigma \in Aut(K) : \sigma(a) = a$ for all $a \in F\}$. Then $G(K : F)$ is a subgroup of $Aut(K)$.*

Proof. Let $I \in Aut(K)$ with $I(a) = a \ \forall \ a \in K$. Then $I(a) = a \ \forall \ a \in F, \implies I \in G(K : F)$. Hence $G(K : F)$ is non-empty. Let $\sigma, \tau \in G(K : F)$. Then $\sigma(a) = a, \tau(a) = a \ \forall \ a \in F$. Clearly, $\sigma \circ \tau \in Aut(K)$. Also $(\sigma \circ \tau)(a) = \sigma(\tau(a)) = \sigma(a) = a$ for all $a \in F$ and so $\sigma \cdot \tau \in G(K : F)$ and $\sigma^{-1} \in Aut(K)$. Since, $\sigma(a) = a \forall a \in F, \sigma^{-1}(\sigma(a)) = \sigma^{-1}(a), \ \forall \ a \in F$. This implies $(\sigma^{-1} \cdot \sigma)(a) = \sigma^{-1}(a) \ \forall \ a \in F$. Hence $a = I(a) = \sigma^{-1}(a) \ \forall \ a \in F$ and so $\sigma^{-1} \in G(K : F)$. Hence $G(K : F)$ is a subgroup of $Aut(K)$. □

Theorem 3.2.9. *Let K be a field. If $H_1, H_2 \subseteq Aut(K)$ and $H_1 \subseteq H_2$, then $F_{H_2} \subseteq F_{H_1}$.*

Proof. For any $a \in F_{H_1}$, we have $\sigma(a) = a$ for all $\sigma \in H_2$. Since $H_1 \subseteq H_2$, we also have $\sigma(a) = a$ for all $\sigma \in H_1$. By definition, F_{H_1}, this means $a \in F_{H_1}$.Therefore, $F_{H_2} \subseteq F_{H_1}$. □

Theorem 3.2.10. *If F_1 and F_2 are subfields of k and $F_1 \subseteq F_2$, then $Aut(k/F_2) \subseteq Aut(k/F_1)$.*

Proof. Clearly, $Aut(k/F_2) \subseteq Aut(k)$. Let $\sigma \in Aut(k/F_2)$. Then, for any $a \in F_2$, we have $\sigma(a) = a$. Since $F_1 \subseteq F_2$, we also have $a \in F_1$, and therefore $\sigma(a) = a$ for all $a \in F_1$. This means $\sigma \in Aut(k/F_1)$. Hence $Aut(k/F_2) \subseteq Aut(k/F_1)$. □

In view of Proposition 3.2.4 and Theorem 3.2.8, we have the following.

Corollary 3.2.11. *Let K be a field and let F be a prime subfield of K. Then $Aut(K) = G(K : F)$.*

Theorem 3.2.12. *Let $[K : F]$ be a finite extension. Then $|G(K : F)| \leq [K : F]$*

Proof. Clearly $G(K : F)$ is a subgroup of $Aut(K)$. Let $n = |G(K : F)|$
Suppose, $|G(K : F)| > [K : F]$
Let $\{\alpha_1, \alpha_2, \cdots, \alpha_m\}$ be a basis for K over F and $dim_F = m < n$,
Let $G(K : F) = \{I, \sigma_1, \cdots, \sigma m\}$. Consider the system of equations,

$\sigma_1(\alpha_1)x_1 + \sigma_2(\alpha_1)x_2 + \cdots + \sigma_n(\alpha_1)x_n = 0,$

$\sigma_1(\alpha_2)x_1 + \sigma_2(\alpha_2)x_2 + \cdots + \sigma_n(\alpha_2)x_n = 0,$

$\vdots$

$\sigma_1(\alpha_m)x_1 + \sigma_2(\alpha_m)x_2 + \cdots + \sigma_n(\alpha_m)x_n = 0. - - - - - - - - -(1)$

Clearly, the number of equation is less than the number of unknowns, (1) has non-trivial solutions, say $\beta_1, \beta_2, \ldots, \beta_m$ (not all zero).

Let $a_1, a_2, \ldots, a_m$ be any arbitrary elements in F. Then $\sigma(a_i) = a_i \; \forall \; \sigma \in G(K:F)$.

Since, $\beta_1, \beta_2, \ldots, \beta_n$ are solutions of (1), (1) $\implies \sigma_1((\alpha_1)\beta_1 + \sigma_2(\alpha_1)\beta_2 + \cdots + \sigma_n(\alpha_1)\beta_n = 0, \vdots \sigma_1(\alpha_m)\beta_1 + \sigma_2(\alpha_m)\alpha_2 + \cdots + \sigma_n(\alpha_m)\beta_n = 0.$

From this we get , $a_1\sigma_1((\alpha_1)\beta_1 + a_1\sigma_2(\alpha_1)\beta_2 + \cdots + a_1\sigma_n(\alpha_1)\beta_n = 0, \ldots$

$a_m\sigma_1(\alpha_n)\beta_1 + a_m\sigma_2(\alpha_m)\alpha_2 + \cdots + a_m\sigma_n(\alpha_m)\beta_n = 0.$

‘ Since $G(K:F) = \{\sigma_1, \sigma_2, \cdots, \sigma_n\}, \; \sigma_i(a_j) = a_j \; \forall \; i, j$, from this, we get

$\sigma_1(a_1)\sigma_1(\alpha_1)\beta_1 + \cdots + \sigma_n(a_1)\sigma_n(\alpha_1)\beta_n = 0.$

$\vdots$

$\sigma_1(a_m)\sigma_1(\alpha_m)\beta_1 + \cdots + \sigma_m(a_n)\sigma_n(\alpha_m)\beta_n = 0.$

$\implies \sigma_1(\alpha_1 a_1 + \cdots + a_m\alpha_m)\beta_1 + \sigma_2(\alpha_1 a_1 + \cdots + a_m\alpha_m)\beta_2 + \cdots + \sigma_n(a_1\alpha_1 + \cdots + a_m\alpha_m)\beta_m = 0.$

$\implies \sum_{i=1}^{n} \sigma(a_1\alpha_1 + \cdots + \sigma(a_m)\alpha_m\beta_i) = 0.$

$\implies \sum_{i=1}^{n} \sigma_i(y)\beta_i = 0 \; \forall \; y \in K = \{b_1\beta_1 + \cdots + b_m\beta_m : b_i \in F.\}$

$\implies \beta_1\sigma_1(y) + \cdots + \beta_n\sigma_n(y) = 0 \; \forall \; y \in K.$

Since $\{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ is linearly independent over K, $\beta_i = 0 \; \forall \; i$, which is a contradiction. Hence $|G(K:F)| \leq [K:F]$. □

Definition 3.2.13. (Galois extension)

Let $[K:F]$ be a finite extension. Then $[K:F]$ is a Galois extension if $|G(K:F)| = [K:F]$.

If $[K:F]$ is Galoios extension, then the **Galois group** of $[K:F]$ is $G(K:F)$.

In general, $Gal(K:F) = G(K:F) = Aut(K:F)$.

Example 3.2.14. (1) $G(\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}) = Aut(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{I\}$. Therefore $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ and so $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not a Galois extension.

(2) $G(\mathbb{Q}(\sqrt[4]{5}) : \mathbb{Q}) = Aut(\mathbb{Q}(\sqrt[4]{5})/\mathbb{Q}) \cong \mathbb{Z}_2$. Therefore, $[\mathbb{Q}(\sqrt[4]{5}) : \mathbb{Q}] = 4$ and $\mathbb{Q}(\sqrt[4]{5})/\mathbb{Q}$ is not a Galois extension.

Definition 3.2.15. (Galois group)

Let $f(x) \in F[x]$ and K be the splitting field of $f(x)$ over F. Then the Galois group of $f(x)$ is the group $G(K : F)$.

Example 3.2.16. Let $K = \mathbb{Q}(\sqrt{2})$. Then $\{1, \sqrt{2}\}$ is a basis for a vector space K over $\mathbb{Q}$ and so $K = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$. For any $\sigma \in Aut(K) = Aut(K|\mathbb{Q})$, $\sigma(a) = a$ for all $a \in \mathbb{Q}$. For any $y = a + b\sqrt{2} \in K$, $\sigma(y) = a + b\sigma(\sqrt{2})$. Since $\sqrt{2}$ is root of $x^2 - 2$ over $\mathbb{Q}$, $\sigma(\sqrt{2})$ is a root of $x^2 - 2$ and so $\sigma(\sqrt{2}) = \pm\sqrt{2}$ and hence $Gal(K|\mathbb{Q}) \cong \mathbb{Z}_2$.

Example 3.2.17. Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Then $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ is a basis for a vector space K over $\mathbb{Q}$ and so $K = \{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} : a, b, c, d \in \mathbb{Q}\}$. For any $\sigma \in Aut(K) = Aut(K|\mathbb{Q})$, $\sigma(a) = a$ for all $a \in \mathbb{Q}$. For any $y = a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} \in K$, $\sigma(y) = a+b\sigma(\sqrt{2})+c\sigma(\sqrt{3})+d\sigma(\sqrt{2})\sigma(\sqrt{3})$. Since $\sqrt{2}$ is root of $x^2 - 2$ over $\mathbb{Q}$, $\sigma(\sqrt{2})$ is a root of $x^2 - 2$ and so $\sigma(\sqrt{2}) = \pm\sqrt{2}$. Similar way, we get $\sigma(\sqrt{3}) = \pm\sqrt{3}$. Hence $Gal(K|\mathbb{Q}) = \{I, \sigma_1, \sigma_2, \sigma_3\}$, where $\sigma_1(\sqrt{2}) = \sqrt{2}$, $\sigma_1(\sqrt{3}) = -\sqrt{3}$, $\sigma_2(\sqrt{2}) = -\sqrt{2}$, $\sigma_2(\sqrt{3}) = \sqrt{3}$, $\sigma_3(\sqrt{2}) = -\sqrt{2}$, $\sigma_3(\sqrt{3}) = -\sqrt{3}$.

Hence $Gal(K|\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Example 3.2.18. (1) Let $f(x) = x^3+x+1 \in \mathbb{Z}_2[x]$. Then $f(0) = f(1) = 1$ and so $f(x)$ has no roots in $\mathbb{Z}_2$. Hence $f(x)$ is irreducible over $\mathbb{Z}_2$

Let α be a root of $f(x)$ in some extension in $\mathbb{Z}_2$. Then $K = \mathbb{Z}_2(\alpha)$ and $\{1, \alpha, \alpha^2\}$ is a basis for K over $\mathbb{Z}_2$ and $\mathbb{Z}_2(\alpha) = \{a_0+a_1\alpha+a_2\alpha^2 : a_i \in \mathbb{Z}_2\} = \{0, 1, \alpha, \alpha^2, 1+\alpha^2, \alpha+\alpha^2, \alpha^2+\alpha+1\}$ and $[\mathbb{Z}_2(\alpha) : \mathbb{Z}_2] = 3$.

$f(\alpha) = 0 \Rightarrow \alpha^3 + \alpha + 1 = 0 \Rightarrow \alpha^3 = -\alpha - 1 = \alpha + 1$

α is a root of $f(x)$ and $\alpha \in \mathbb{Z}_2(\alpha)$

$f(\alpha^2) = (\alpha^2)^3 + \alpha^2 + 1 = (\alpha^3)^2 + \alpha^2 + 1 = 0$

$f(\alpha + \alpha^2) = (\alpha + \alpha^2)^3 + \alpha + \alpha^2 + 1 = 0$

$f(x) = (x - \alpha)(x - \alpha^2)g(x), g(x) \in \mathbb{Z}_2(\alpha)[x]$

Therefore, $\mathbb{Z}_2(\alpha)$ is a splitting field of $f(x)$ over $\mathbb{Z}_2$

$\sigma(x) = a + b\sigma(\alpha) + c\sigma(\alpha)^2$

Since α is a root of $f(x)$, $\sigma(\alpha)$ is a root of $f(x)$ and $\sigma(\alpha) = \alpha, \alpha^2$ or $\alpha + \alpha^2 \Rightarrow Gal(\mathbb{Z}_2(\alpha)/\mathbb{Z}_2) \cong \mathbb{Z}_3$

(2) Let $f(x) = x^4 + x^2 + 1 \in \mathbb{Q}[x]$. Then $\pm\omega, \pm\omega^2$ are the roots of $f(x)$. where ω is root of $x^2 + x + 1$ and so $\mathbb{Q}(\omega)$ is a splitting field of $f(x)$ over $\mathbb{Q}$. Hence $\mathbb{Q}(\omega)/\mathbb{Q}$ is a Galois extension and $[\mathbb{Q}(\omega) : \mathbb{Q}] == 2 = |Gal(\mathbb{Q}(\omega)/\mathbb{Q})|$.

Clearly $\{1, \omega\}$ is a basis for $\mathbb{Q}(\omega)$ over $\mathbb{Q}$ and $\mathbb{Q}(\omega) = \{a_0 + a_1\omega : a_i \in \mathbb{Q}\}$ and $\sigma(x) = a_0 + a_1\sigma(\omega)$ for all σ. Clearly ω is a root of $x^2 + x + 1 \in \mathbb{Q}[x]$, $\sigma(\omega)$ is a root of $x^2 + x + 1 \in \mathbb{Q}[x]$. This implies $\sigma(\omega) = \omega$ or ω^2 and hence $Gal(\mathbb{Q}(\omega)/\mathbb{Q}) = \{I, \sigma : \sigma(\omega) = \omega^2\} \cong \mathbb{Z}_2$.

Example 3.2.19. Let $K = \mathbb{Q}(\sqrt[3]{2})$ and $F = \mathbb{Q}$, where $\omega^3 = 1$. Let $\alpha = \sqrt[3]{2}, \omega\alpha, \omega^2\alpha \notin \mathbb{Q}$ are root of $p(x) = x^3 - 2$, $p(x)$ is irreducible over $\mathbb{Q}$ and so $\{1, \alpha, \alpha^2\}$ is basis for $\mathbb{Q}(\sqrt{3})$ over $\mathbb{Q}$. Thus $\mathbb{Q}(\sqrt[3]{2}) = \{a + b\alpha + c\alpha^2 : a, b, c \in \mathbb{Q}\}$. For any $\sigma \in Aut(\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q})$, $\sigma(a) = a$ for all $a \in \mathbb{Q}$. Also $\sigma(a + b\alpha + c\alpha^2) = a + \sigma(\alpha)b + \sigma(\alpha)^2c$ and so $\sigma(\alpha)$ is root of $p(x)$ and so $\sigma(\alpha) = \alpha$. Hence $\sigma(a + b\alpha + c\alpha^2) = a + \alpha b + \alpha^2 c$ and so $\sigma = I$. From this we get $Aut(\mathbb{Q}(\sqrt[3]{2})) = Aut(\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q}) = \{I\}$ and so $\mathbb{Q}(\sqrt[3]{2}, \omega)|\mathbb{Q}$ is not Galois extension.

Example 3.2.20. Let $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$ and $F = \mathbb{Q}$, where $\omega^3 = 1$. Then $\mathbb{Q}(\sqrt[3]{2}, \omega)$ is a splitting of $x^3 - 2 \in \mathbb{Q}[x]$ and $[K : \mathbb{Q}] = |Aut(K|\mathbb{Q})| = 6$. Thus $\{1, \alpha = \sqrt[3]{2}, \alpha^2, \omega, \omega\alpha, \omega\alpha^2\}$ is a basis for K over F and so $K = \{x = a + b\alpha + c\alpha^2 + d\omega + e\omega\alpha + f\omega\alpha^2 : a, b, c, d, e, f \in \mathbb{Q}\}$. For any $\sigma \in Aut(K)$, $\sigma(x) = a + b\sigma(\alpha) + c\sigma(\alpha)^2 + d\sigma(\omega) + e\sigma(\omega)\sigma(\alpha) + f\sigma(\omega)\sigma(\alpha)^2$. This implies ω is root of $x^2 + x + 1$ and $\sqrt[3]{2}$ is root of $x^3 - 2$ and so $\sigma(\omega) = \omega$ or ω^2 and $\sigma(\alpha) = \alpha$, $\omega\alpha$ or $\omega^2\alpha$. Hence $Gal(K|Q) \cong S_3$.

Example 3.2.21. Let $K = \mathbb{Q}(\sqrt{3}, i)$ and $F = \mathbb{Q}$. Then $\mathbb{Q}(\sqrt{3}, i)$ is a splitting of $(x^2 - 3)(x^2 + 1) \in \mathbb{Q}[x]$ and $[K : \mathbb{Q}] = |Aut(K|\mathbb{Q})| = 4$. From this, $\{1, \sqrt{3}, i, i\sqrt{3}\}$ is a basis for K over F and $K = \{a + b\sqrt{3} + ci + di\sqrt{3} : a, b, c, d \in \mathbb{Q}\}$. For any $\sigma \in Aut(K)$, $\sigma(a + b\sqrt{3} + ci + di\sqrt{3}) == a + \sigma(\sqrt{3})b + c\sigma(i) + d\sigma(i)\sigma(\sqrt{3})$. This implies $\sigma(\sqrt{3})$ is root of $x^2 - 3$ and so $\sigma(\sqrt{3}) = \pm\sqrt{3}$. Note that $\sigma(i)$ is root of $x^2 + 1$ and so $\sigma(i) = \pm i$. Hence $Aut(\mathbb{Q}(\sqrt{5})|\mathbb{Q}) = \{I, \sigma_1, \sigma_2, \sigma_3\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, where $\sigma_1 : \sqrt{3} \to \sqrt{3}$ and $i \to -i$, $\sigma_2 : \sqrt{3} \to -\sqrt{3}$ and $i \to i$ $\sigma_3 : \sqrt{3} \to -\sqrt{3}$ and $i \to -i$

Theorem 3.2.22. *Let $[K : F]$ be a finite extension. Then $[K : F]$ is a Galois extension if and only if K is the splitting field of seperable polynomial over F.*

Proof. Suppose K is the splitting field of some seperable polynomial over F. Then $|Aut[K : F]| = [K : F]$ and hence, $[K : F]$ is Galois extension.

$\Rightarrow K/F$ is normal

Conversely, $[K : F]$ is Galois extension. then $[K : F] = |Gal[K : F]| = n < \infty$

Let $Gal[K : F] = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$

Claim 1: If $p(x)$ is monic irreducible over F and $\alpha \in K$ is a root of $f(x)$ then all the roots of $f(x)$ be in K and $p(x)$ is seperable over F

Let $S = \{\sigma(\alpha) : \sigma \in Gal[K : F]\}$. Then $S = \{\alpha_1 = \alpha, \ldots, \alpha_k\}$ where $\alpha_i \neq \alpha_j$.

For any $j = 1, \ldots, n$, $\sigma_j(\alpha_i) = \sigma_j(\sigma_t(\alpha)) = \sigma_j \circ \sigma_t(\alpha) = \sigma(\alpha) = \alpha_m \in S$. This implies $\sigma(S) = S\ \forall\ \sigma \in Gal[K : F]$

Define $g(x) = \Pi_{i=1}^{k}(x - \alpha_i) \in K[x]$

Let $g(x) = a_0 + a_1 x + \ldots + a_{k-1}x^{k-1} + x^k \in K[x]$

Thus, $\sigma(g(x)) = \Pi_{i=1}^{k}(x - \sigma(\alpha_i)) = \Pi_{j=1}^{k}(x - \alpha_j) = g(x)$

$\sigma(a_0) + \sigma(a_1)x + \ldots + \sigma(a_{k-1})x^{k-1} + x^k = a_0 + a_1 x + \ldots + a_{k-1}x^{k-1} + x^k$

$\Rightarrow (\sigma(a_0) - a_0) + \ldots + (\sigma(a_{k-1}) - a_{k-1})x^{k-1} = 0$ and $\sigma_i(a_i) - a_i \in K$. Since $\{1, x, \ldots, x^{k-1}\}$ is linearly independent in $K[x]$ over K, $\sigma_i(a_i) - a_i = 0\ \forall\ i$

□

Theorem 3.2.23 (Fundamental theorem of Galois theory)**.** *Let $[K : F]$ be a Galois extension and $G = Gal[K : F]$.*
Let $A = \{E :\ E\ is\ a\ subfield\ of\ K\ containing\ F\}$, $B = \{H : H \leq G\}$. Then there is a bijection $A \leftrightarrow B$ given by the correspondence $E \rightarrow$\{the elements of G fixing E\} and \{the fixed field of H\}$\leftarrow H$ which are inverse to each other.

Proof. Let $H_1, H_2 \in B$ and $H_1 \neq H_2$. Then $F_{H_1} \neq F_{H_2}$, where F_{H_i} is the fixed field of H_i. Clearly, F_{H_i} is a subfield of K containing F. $F_{H_1}, F_{H_2} \in A$ and $F_{H_1} \neq F_{H_2}$. From this, $B \rightarrow A$ is 1-1. Let $E \in A$. Then E is the subfield of K containing F. Since, $[K : F]$ is Galois extension, K is the splitting field of some seperable polynomial $f(x)$ over F. Since $F \subseteq E, F[x] \subseteq E[x]$ and $f(x) \in E[x]$, we have K is the splitting field of $f(x)$ over E. Thus $[K : E]$ is Galois extension and $|Aut[K : E]| = [K : E]$. Also E is the fixed field of $Aut[K : E] \leq G$. Thus $A \rightarrow B$ is onto. Hence $A \leftrightarrow B$ is a bijection and $|A| = |B|$ □

Under this correspondence

(i) If E_1, E_2 corresponds to H_1, H_2 respectively, then $E_1 \subseteq E_2$ if and only if $H_2 \subseteq H_1$.

Proof: Clearly F_i is the fixed field of H_i and so $H_i = Aut[K : E_i]$. Suppose $E_1 \subseteq E_2$. For any $\sigma \in H_2 = Aut[K : E]; \sigma(a) = a, \forall a \in E_2$.

$\Rightarrow \sigma(a) = a, \forall a \in E_1 \subseteq E_2$ and $\sigma \in Aut[K : E_1]$. Thus $H_2 \subset H_1$.

Conversely, $H_2 \subseteq H_1$. For any σH_1, by definition of $E_1, \sigma(a) = a, \forall a \in H_1$. Since $H_2 \subseteq H_1$, we have $\sigma \in H_2$.

(ii) $[K : E] = |H|$ and $[E : F] = [G : H]$.

Proof: Clearly, E is the fixed field of H and $H = Aut[K : E]$ and $|H| = |Aut(K|E)| = [K : E](\because [K : E]$ is a Galois extension). Since $[K : F]$ is a Galois extension, $[K : F] < \infty$. Thus $[K : E]$ and $[K : E]$ are finite extensions. Clearly, $[K : F] = [K : E][E : F]$.

$\Rightarrow [K : F] = |H|\,[E : F]$

$\Rightarrow [E : F] = \frac{[K:F]}{[K:E]} = \frac{|G|}{|H|} = [G : H]$.

(iii) Let $E \subseteq A$. Then $[K : F]$ is Galois extension and $Gal[K : E] = Aut[K : E] \leq G$.

Proof: Since $[K : F]$ is Galois extension and K is the splitting field of seperable polynomial $f(x)$ over F, $Gal[K : E] = Aut[K : E] \leq G$.

Theorem 3.2.24. *Let F_i be the fixed field of $H_i \leq G$ and $\sigma \in G$. F_1 and F_2 are conjugates under σ if and only if $\sigma H_1 \sigma^{-1} = H_2$.*

Proof. $(\sigma^{-1} \circ \tau \circ \sigma)(x) = x, \forall \tau \in H_2 \Rightarrow \sigma^{-1} \circ \tau \circ \sigma \in H_1, \forall \tau \in H_2 \Rightarrow \sigma^{-1} H_2 \sigma \in H_1 \Rightarrow H_2 \subseteq \sigma H_1 \sigma^{-1}$, $H_2 = \sigma H_1 \sigma^{-1}$.

Conversely, suppose $\sigma H_1 \sigma^{-1} = H_2$. For any $y \in F_2$, $\sigma \circ \tau \circ \sigma^{-1} \in H_2, \forall \tau \in H_1$. $(\sigma \circ \tau \circ \sigma^{-1})(y) = y, \forall \tau \in H_1$. $(\tau \circ \sigma^{-1})(y) = \sigma^{-1}(y), \forall \tau \in H_1$ which implies $\sigma^{-1}(y) = x$, for some $x \in F_1, y = \sigma(x) \in \sigma(F_1)$ and so $F_2 \subseteq \sigma(F_1)$. For any $x \in F_1$, $\sigma^{-1} \circ \tau \circ \sigma \in H_1, \forall \tau \in H_2$. $(\sigma^{-1} \circ \tau \circ \sigma)(x) = x, \forall \tau \in H_2$. $(\tau \circ \sigma)(x) = \sigma(x), \forall \tau \in H_2$ which implies $\sigma(x) \in F_2$ for all $x \in F_1$ and so $\sigma(F_1) \subseteq F_2$. □

(iv) $[E : F]$ is Galois extension if and only if $H \trianglelefteq G$.

Proof: Suppose $[E : F]$ is Galois extension. Then by definition of Galois extension, $[E : F] = |Aut(E|F)| < \infty$ and $[E : F]$ is finite extension. Also E is the splitting field of some seperable polynomial $f(x)$ over F and hence $E = F(\alpha_1, \alpha_2, \cdots, \alpha_m)$, where α_i is root of $f(x)$ over F. For any $\sigma \in Gal[K : F], \sigma(\alpha_i)$ is a root of $f(x)$ over $F, \forall i$.

$\{\sigma(\alpha_1), \sigma(\alpha_2), \cdots, \sigma(\alpha_m)\} = \{\alpha_1, \alpha_2, \cdots, \alpha_m\}$.

$\sigma(E) = F(\sigma(\alpha_1), \sigma(\alpha_2), \cdots, \sigma(\alpha_m)) = F(\alpha_1, \alpha_2, \cdots, \alpha_m) = E$.

$\Rightarrow E$ is conjugate to itself under $\sigma, \sigma \in Gal[K : F]$. By Theorem 3.2.24, $\sigma H \sigma^{-1} = H, \forall \sigma \in Gal[K : F]$. Thus $H \trianglelefteq G = Gal[K : F]$.

Conversely, $H \trianglelefteq G = Gal[K : F]$. Then $\sigma H \sigma^{-1} = H, \forall \sigma \in G$ and by Theorem 3.2.24, $\sigma(E) = E, \forall \sigma \in G$. $[E : F] < \infty$ and so $[E : F]$ is algebraic. Clearly, $E = F(\beta_1, \beta_2, \cdots, \beta_n)$, where $\beta_i^{\prime}s$ are algebraic over F. By (i) and (ii), E is splitting field of some seperable polynomial over F and $[E : F]$ is Galois extension. Clearly, $[E : F] = \frac{|G|}{|H|} = |Aut[E : F]|$ and $\frac{G}{H}$ is a group.

Define $\Phi : G \to Aut[E : F]$ by $\Phi(\sigma) = \sigma_{1E}$, where $\sigma_1 \in Gal[E : F], \sigma_{1E}(a) = \sigma(a), \forall a \in E$. Let $\sigma, \tau \in G$. Then $\sigma.\tau \in G$ and $(\sigma.\tau)_{1E}(a) = (\tau.\sigma)a = \sigma(\tau(a)) = \sigma_{1E}(\tau(a)) = \sigma_{1E}(\tau_{1E}(a)) = (\sigma_{1E}.\tau_{1E})(a), \forall a \in E$. $(\sigma.\tau)_{1E} = \sigma_{1E}.\tau_{1E}$. Thus $\Phi(\sigma.\tau) = (\sigma.\tau)_{1E} = \sigma_{1E}.\tau_{1E} = \Phi(\sigma).\Phi(\tau)$. Suppose $\sigma \in Ker\Phi$. Then $\Phi(\sigma) = I_E$. $\sigma_{1E} = I_E \Leftrightarrow \sigma_{1E}(a) = I_E(a) = a, \forall a \in E \Leftrightarrow \sigma(a) = a, \forall a \in E \Leftrightarrow \sigma \in H \Rightarrow Ker\Phi = H$. By first isomorphism theorem, $(\frac{G}{H}) \cong \Phi(G) \leq Gal[K : F]$ and so $\frac{|G|}{|H|} = [E : F] = |\Phi(G)| \leq |Gal[E : F]| = [E : F]$.

$\Rightarrow |Gal[E : F]| = [E : F] = \left|\frac{G}{H}\right|$.

$\Rightarrow Gal[E:F] = \frac{G}{H}$.

(v) Let E_i be the fixed field of $H_i, i = 1, 2$. Then $E_1 \cap E_2$ is the fixed field of $H =< H_1, H_2 >$.

Proof: Let F_H be the fixed field of H. For any $\alpha \in F_H, \sigma(\alpha) = \alpha, \forall \sigma \in H$. Since $H =< H_1, H_2 >, H_1, H_2 \subseteq H$, we have $\sigma(\alpha) = \alpha, \forall \sigma \in H_1$ and $\tau(\alpha) = \alpha, \forall \tau \in H_2$.
$\Rightarrow \alpha \in E_1, \alpha \in E_2 \Rightarrow \alpha \in E_1 \cap E_2$. Thus $F_H \subseteq E_1 \cap E_2$. Let $\beta \in E_1 \cap E_2$. Then $\beta \in E_1, \beta \in E_2$. Since E_i is the fixed field of H_i, $\sigma(\beta) = \beta, \forall \sigma \in H_1, \tau(\beta) = \beta, \forall \tau \in H_2$. Since $H =< H_1, H_2 >$, for any $\delta = \sigma \circ \tau$, where $\sigma \in H_1, \tau \in H_2$. $\delta(\beta) = (\sigma \circ \tau)(\beta) = \sigma(\tau(\beta)) = \sigma(\beta)$. Thus $\beta \in F_H$ and $E_1 \cap E_2 \subseteq F_H$. Hence $E_1 \cap E_2 = F_H$ is a fixed field of H.

3.2.1 Symmetric function

Definition 3.2.25. Let $x_1, x_2, \ldots, x_n$ be indeterminates. A polynomial $f(x_1, x_2, \ldots, x_n) \in F[x_1, x_2, \ldots, x_n]$ is a symmetric function if for any $\sigma \in S_n$, $f(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}) = f(x_1, x_2, \ldots, x_n)$.

For any $\sigma \in S_n$, $\sigma(i) = i$,

$$f(x_1, x_2, \ldots, x_n) = x_1 + x_2 + \cdots + x_n.$$

Then, $f(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}) = x_1 + x_2 + \cdots + x_n$.
when $n = 3$, $\sigma = \{1, 2, 3\}$,

$f(x_1, x_2, x_3) = x_1 + x_2 + x_3$. $\sigma = \{1, 3, 2\} \Rightarrow f(x_1, x_3, x_2) = x_1 + x_3 + x_2 = f(x_1, x_2, x_3)$, $\sigma = \{2, 1, 3\} \Rightarrow f(x_2, x_1, x_3) = x_2 + x_1 + x_3 = f(x_1, x_2, x_3)$,

$\sigma = \{3,2,1\} \Rightarrow f(x_3,x_2,x_1) = x_3 + x_2 + x_1 = f(x_1,x_2,x_3)$. Therefore, $f(x_1,x_2,x_3) = x_1 + x_2 + x_3$ is a symmetric function.

Definition 3.2.26. Let F be a field and let $x_1, x_2, ..., x_n$ be distinct n indterminants $x_i \neq x_j$. Let $F[x_1, x_2, \ldots, x_n]$ be an integral domain. Then, $F(x_1, x_2, \ldots, x_n)$ is the field of fractions of $F[x_1, x_2, \ldots, x_n]$.
$F(x_1, x_2, \ldots, x_n) = \{\frac{f(x_1,x_2,\ldots,x_n)}{g(x_1,x_2,\ldots,x_n)} : f, g \in F(x_1, x_2, \ldots, x_n)\}$.

$f(x_1, x_2, \ldots, x_n) \in F(x_1, x_2, \ldots, x_n)$ is a symmetric rational function if for any permutation $\sigma \in S_n$, $f(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}) = f(x_1, x_2, \ldots, x_n)$.

When $n = 2$, $f(x_1, x_2) = x_1 + x_2$, x_1x_2, $x_1^2 + x_2^2$, $x_1^m + x_2^m$ are symmetric functions.

Definition 3.2.27. Elementary Symmetric function $s_1 = \sum\limits_{i=1}^{n} x_i = x_1 + x_2 + \cdots + x_n$,

$s_2 = \sum\limits_{i \neq j} x_ix_j$

$s_3 = \sum\limits_{i \neq j \neq k} x_ix_jx_k$

$\vdots$

$s_n = x_1x_2 \cdots x_n$

Let $S = \{f(x_1, x_2, \ldots, x_n) \in F(s_1, s_2, \ldots, s_n) : f \text{ is a } \text{ symmetric}\}$ be the subfield of $F(x_1, x_2, \ldots, x_n)$, and $F(s_1, s_2, \ldots, s_n)$ is the subfield of S containing F. Then, $F(x_1, x_2, \ldots, x_n)|S, F(x_1, x_2, \ldots, x_n)|F(s_1, s_2, \ldots, s_n)$ $\implies S|F(s_1, s_2, \ldots, s_n)$ are a field extension.

Problem 3.2.28. *Find $G(F(x_1, x_2, \ldots, x_n) : S)$ (or) $AutF(x_1, x_2, \ldots, x_n)|S$.*

Proof. For any $\sigma \in S_n$, define:$\tau_\sigma(F(x_1, x_2, \dots, x_n)) \to (F(x_1, x_2, \dots, x_n))$ by $\tau_\sigma(f(x_1, x_2, \dots, x_n)) = (x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)})$.

Claim: $\tau_\sigma \in Aut(F(x_1, x_2, \dots, x_n))|S$.

Let $f(x_1, x_2, \dots, x_n)$, $g(x_1, x_2, \dots, x_n) \in F(x_1, x_2, \dots, x_n)$ Then,

$\tau_\sigma(f(x_1, x_2, \dots, x_n) + g(x_1, x_2, \dots, x_n)) = \tau_\sigma(h(x_1, x_2, \dots, x_n))$
$= h(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)}) = f(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)}) + g(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)})$
$= \tau_\sigma(f) + \tau_\sigma(g)$.

Now $\tau_\sigma(f(x_1, x_2, \dots, x_n)g(x_1, x_2, \dots, x_n)) = \tau_\sigma(k(x_1, x_2, \dots, x_n))$
$= k(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)}) = f(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)})g(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)})$
$= \tau_\sigma(f)\tau_\sigma(g)$ τ_σ is a ring homomorphism. Clearly, $\tau_\sigma(1) = 1 \neq 0, \tau_\sigma \neq 0$. τ_σ is one-one. For any $h(x_{\sigma^{-1}(1)}, \dots, x_{\sigma^{-1}(n)}) \in F(x_1, x_2, \dots, x_n)$,
$\tau_\sigma(h(x_{\sigma^{-1}(1)}, \dots, x_{\sigma^{-1}(n)})) = h(x_{\sigma(\sigma^{-1}(1))}, \dots, x_{\sigma(\sigma^{-1}(n))}) = h(x_1, x_2, \dots, x_n)$
Hence, $\tau_\sigma \in Aut(F(x_1, x_2, \dots, x_n))$ and so $|Aut(F(x_1, x_2, \dots, x_n))| \geq n!$.

Define $\hat{\Phi} : S_n \to Aut(F(x_1, x_2, \dots, x_n))$ by $\Phi(\sigma) = T_\sigma$. Let $\sigma, \tau \in S_n$. Then $\sigma\tau \in S_n$.

$T_{\sigma\tau}(f(x_1, x_2, \dots, x_n)) = f(x_{\sigma\tau(1)}, x_{\sigma\tau(2)}, \dots, x_{\sigma\tau(n)})$
$= f(x_{\tau(\sigma(1))}, x_{\tau(\sigma(2))}, \dots, x_{\tau(\sigma(n))}) = T_\tau(f(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)}))$
$= T_\tau(T_\sigma(f(x_1, x_2, \dots, x_n)))$
$= (T_\sigma T_\tau)(f(x_1, x_2, \dots, x_n))$.

Therefore, $\Phi(\sigma\tau) = T_{\sigma\tau} = T_\sigma T_\tau = \Phi(\sigma)\Phi(\tau)$. Hence, Φ is a group homomorphism.

Suppose $\sigma \in \ker\Phi$. Then by definition, $T_\sigma = \Phi(\sigma) = I$.Let I be the identity automorphism of $F(x_1, x_2, \dots, x_n)$. Then, $\sigma(i) \neq i$ implies $\sigma(i^*) = j^*$ for some $j \in \{1, 2, \dots, n\}$. Hence, $\sigma \neq I$ and so $\ker\Phi = \{1\}$.

By First Isomorphism Theorem, $S_n \cong \Phi(S_n) \subseteq Aut(F(x_1, x_2, \ldots, x_n))$. Clearly, $|\Phi(S_n)| = |S_n| = n!$. Let F_H be the fixed field of $H \subseteq Aut(F(x_1, x_2, \ldots, x_n))$. Then, $F_H \subseteq F(x_1, x_2, \ldots, x_n)$.

Let $f(x_1, x_2, \ldots, x_n) \in F_H$. Then, $T_\sigma(f(x_1, x_2, \ldots, x_n)) = f(x_1, x_2, \ldots, x_n)$ for all $\sigma \in S_n$. This implies $f(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}) = f(x_1, x_2, \ldots, x_n)$ for all $\sigma \in S_n$. Hence, $f(x_1, x_2, \ldots, x_n)$ is a symmetric rational function.

Let $S = \{\tau_\sigma : \sigma \in S_n\} \subseteq Aut(F(x_1, x_2, \ldots, x_n))$. Then, $|S| = |S_n| = n!$.

Let $f(x) = x^n + s_1 x^{n-1} + s_2 x^{n-2} + \cdots + (-1)^n s_n \in F[s_1, s_2, \ldots, s_n][x]$. Then, $f(x) \in F(x_1, x_2, \ldots, x_n)$. Hence, $|Aut(F(x_1, x_2, \ldots, x_n))| \geq n!$.

Therefore, $|Aut(F(x_1, x_2, \ldots, x_n))| = n!$. □

Let us sum up:

- Automorphisms and Fixed field.
- Elementary symmetric functions.
- Normal extension.
- Galois group.
- Fundamental theorem of Galois theory.

Check your progress

1. What is $[F(x_1, x_2, ..., x_n : S)] = ?$

2. Let K is the field of complex numbers and F is field of real numbers, then the order of $G(K, F)$ is —

3. What is $G(F(x_1, x_2, ..., x_n), S) =$?

Unit Summary:

In this unit, we discussed the concept of fixed field, subfield, finite extension and simple extension. Further, we introduced the Galois group and the fundamental theorem of Galios theory.

Glossary:

- $G(K, F)-$ is the set all group of automorphisms.
- $o(G(K, F)) \leq [K : F]$
- Symmetric rational functions
- Norma extension
- Galois group
- $K_H = \{x \in G(K, F) | \sigma(x) = x \text{ for every} \sigma \in H\}$

Self Assessment questions

1. If K is a finite extension of F, then $G(K, F)$ is a finite group and its order, $o(G(K, F))$ satisfies $o(G(K, F)) \leq [K : F]$.

2. Show that the fixed field of G is a subfield of K.

3. K is the normal extention of F iff K is the splitting field of some polynomial over F.

4. G(K,F) is a subgroup of the group of all automorphisms of K.

Exercises

1. Prove that a symmetric polynomial in $x_1, , , x_n$ is a polynomial in the elementary symmetric functions in $x_1, , , x_n$.

2. If $p(x) = x^n - 1$ prove that the Galois group of $p(x)$ over the field of rational numbers is abelian.

3. Using the Eisenstein criterian, prove that $x^4 + x^3 + x^3 + x + 1$ is irreducible over the field of rational numbers.

4. Express the following polynomials in the elementary symmetric functions in x_1, x_2, x_3 :

   (a) $x_1^2 + x_2^2 + x_3^2$

   (b) $x_1^3 + x_2^3 + x_3^3$

Answers for check your progress

1. $n!$

2. 2

3. S_n

References:

1. I.N. Herstein, Topics in Algebra (II Edition) Wiley Eastern Limited, New Delhi, 1975.

Suggested Reading:

1. M. Artin, Algebra, Prentice Hall of India, 1991.
2. P.B. Bhattacharya, S.K. Jain, and S.R. Nagpaul, Basic Abstract Algebra (II Edition) Cambridge University Press, 1997. (Indian Edition)
3. I.S. Luther and I.B.S. Passi, Algebra, Vol. I âĂŞGroups(1996); Vol. II Rings, Narosa Publishing House , New Delhi, 1999
4. D.S. Malik, J.N. Mordeson and M.K. Sen, Fundamental of Abstract Algebra, McGraw Hill (International Edition), New York. 1997.
5. N. Jacobson, Basic Algebra, Vol. I & II Hindustan Publishing Company, New Delhi.

UNIT - 4

Unit 4

Finite Fields

Objectives:

- Recall the finite field and splitting field.
- To prove the Wedderburns theorem on finite division rings.

4.1 Finite Field

Definition 4.1.1. The nature of fields having only a finite number of elements such fields are called fields.

Lemma 4.1.2. *Let F be a finite field with q elements and suppose that $F \in K$, where K is also a finite field. Then K has q^n elements where $n = [K : F]$.*

Proof. Since K is a vector space over F and since k is finite, then K is a finite-dimensional vector space over F.

Suppose that $[K : F] = n$.

Then K has a basis of n elements over F.

Let $v_1, v_2, \ldots, v_n$ be the basis elements, then every element of K has unique representation in the form $\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n$, where $\alpha_1, \alpha_2, \ldots, \alpha_n$ are in F.

The number of elements in K is the number of $\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n$ as the $\alpha' s$ range over F. Since each coefficients can have q values, K must have q^n elements. □

Corollary 4.1.3. *Let F be a finite field, then F has p^m elements (where p is a prime number), then P is the characteristic of F.*

Corollary 4.1.4. *If the finite field F has p^m elements, then every $a \in F$ satisfies $a^{p^m} = a$.*

Proof. If $a = 0$, the result is trivially true.
If the non-zero elements of F form a group under multiplication of order $p^m - 1$.

By corollary 2. "If G is a finite group and $a \in G$, then $a^{o(G)} = e$", we have

$$a^{p^m - 1} = 1$$
$$\Rightarrow \frac{a^{p^m}}{a} = 1$$
$$\Rightarrow a^{p^m} = a$$

□

Lemma 4.1.5. *If the finite field F has P^m elements, then the polynomial $x^{P^m} - x$ in $F[x]$ factors in $F[x]$ as $x^{P^m} - x = \Pi_{\lambda \in F}(x - \lambda)$.*

Proof. By lemma, ”A polynomial of degree n over a field can have at most n roots in any extension field.”

The polynomial $x^{p^m} - x$ has at most p^m roots in F.

However, by corollary, we know that p^m roots are all the elements of F.

Then by corollary, ”If $a \in K$ is a root of $p(x) \in F[x]$, where FCK, then in $K[x]$, $(x - a) \mid p(x)$”, we have

$$x^{P^m} - x = \prod_{\lambda \in \mathrm{F}} (x - \lambda).$$

□

Corollary 4.1.6. *If the field F has p^m elements, then F is the splitting field of the polynomial $x^{P^m - x}$.*

Proof. By lemma, $x^{p^m} - x$ splits in F.

However, it cannot split in any smaller field to have all the roots of this polynomial and to have at least p^m elements.

Thus, F is the splitting field of $x^{p^m} - x$. □

Lemma 4.1.7. *Any two finite fields having the same number of elements are isomorphic.*

Proof. If these fields have p^m elements, by the above corollary, they are (K_1, K_2) both splitting fields of the polynomial $x^{p^m} - x$ over J_p (the ring of integers modulo any prime p)

If p is a prime, then J_p is field.

Therefore, they are isomorphic. □

Lemma 4.1.8. *For every prime number P and every positive integer m there exists a field having p^m elements.*

Proof. Consider the polynomial $x^{p^m} - x$ in $J_p[x]$, the ring of polynomials in x over J_p, the field of integers mod P.

Let K be the splitting field of this polynomial.

In K, let $F = \{a \in k : a^{p^m} = a\}$. The elements of F are the roots of $x^{p^m} - x$.

By corollary -2 are distinct.

whence F has p^m elements.

Now claim that F is a field. If $a, b \in F$, then, $a^{p^m} = a$, $b^{p^m} = b$, and so $(ab)^{p^m} = a^{p^m} b^{p^m} = ab$.

$$\Rightarrow (ab)^{p^m} = ab, \quad a, b \in F.$$

Also, since the characteristic is p.

$$(a \pm b)^{p^m} = a^{p^m} \pm b^{p^m}$$
$$\Rightarrow (a \pm b)^{p^m} = a \pm b, \quad a \pm b \in F.$$

consequently F is a subfield of K and is a field having p^m elements. □

Theorem 4.1.9. *For every prime number p and every positive integer m there is a unique field having p^m elements.*

Theorem 4.1.10. *Let G be a finite abelian group with the property that the relation $x^n = e$ is satisfied by atmost n elements of G, for every integer n.*

Proof. If the order of G is a power of some prime number q, then the result is very easy.

Suppose that $a \in G$ is an element whose order is as large as possible.

Let the order of ' a ' be q^r for some integer r.

The element $e, a, a^2, \ldots .a^{q^r-1}$ gives us q^r distinct solutions of the equation $x^{q^r} = e$.

By our hypothesis, there are all the solution of this equation. If $b \in G$ its order is q^s where $s \leq r$.

Then

$$b^{q^r} = \left(b^{q^s}\right)^{q^{r-s}} = e^{q^{r-s}} = e$$

. By the observation made, we have $b = a^i$ for some i.

Therefore, G is cyclic. □

Definition 4.1.11. Let F be a commutative ring with 1. F is a field if $(F^*, \ .)$ is an abelian group. (or) Every non-zero element in F has multiplicative inverse.

F is finite field if $|F| < \infty$.

Proposition 4.1.12. *Let F be a finite field of order p^n. Then $(F^\times, \cdot)$ is cyclic.*

Proof. Let $|F| = p^n$. Then $(F^\times, +, \cdot)$ is an abelian group and $|F^\times| = p^n - 1$.

Let α be a maximum order element in $F^{\times}$ and let $m = \text{ord}(\alpha)$. Then $|\beta|/|\alpha|$ for all $\beta \in F^{\times}$. For $\beta \in F^{\times}, \beta^m = \beta^{t|\beta|} = (\beta^{|\beta|})^t = 1$. β is a root of $x^m - 1$, where $forall\beta \in F^{\times}$. Since $\alpha^m = 1$, $1, \alpha, \alpha^2, \ldots, \alpha^m$ are distinct elements in$F^{\times}$. $|F^{\times}| \geq m \mid |F^{\times}| = m > \alpha$. Therefore, $F^{\times}$ is a cyclic group generated by α, and α is a primitive element in F. □

Remark 4.1.13. Let F be a finite field.

(1) $(F^*, .)$ is a finite abelian group.

(2) $|a| < \infty$, for all $a \in F^*$.

(3) Clearly, $|1|_{(F,+)} < \infty$ and char(F)$= |1|_{(F,+)} < \infty$, Since char$(F) = 0$ or p.

(4) $\{0\}$ and $\{F\}$ are only ideals in F.

(5) $\mathbb{Z}_P$ is a prime subfield of F.

(6) $F/\mathbb{Z}_P$ is field extension and F is a vector space over $\mathbb{Z}_p$.

(7) From this, F has basis and so $dim_{Z_p}(F) = n = [F : \mathbb{Z}_p]$ since $|F| < \infty$.

(8) $Aut(F_{P^n}/\mathbb{Z}_p) = Z_n, \sigma : F_{p^n} \implies F_{p^n}\ by\ \sigma(a) = a^p$.

(9) $[F_{p^n} : \mathbb{Z}_p] = n = |Aut(F_{p^n}/\mathbb{Z}_p)|$ and so $F_{P^n}/\mathbb{Z}_p$ is Galois extension.

(10) $F_{p^n}/\mathbb{Z}_p$ is simple extension.

(11) $(F^*, .) =< \alpha >$ for some $\alpha \in F$.

(12) F is perfect and F_{p^n} is a spliting field of separable polynomial $x^{P^n} - x$ over $\mathbb{Z}_p$.

Theorem 4.1.14. *Let F be a finite field with q elements $F \subset K$, where K is finite field. Then $|K| = q^m$ for some m.*

Proof. Since, $F \subset K, [K : F]$ is field extension, and so K is a vector space over F. Since, $|K| < \infty$, $\dim_F(K) = m < \infty$, Let $\{\alpha_1, \alpha_2, \cdots \alpha_n\}$ be a basis for K over F. Then $K = \{a_1\alpha_1 + a_2\alpha_2 + \cdots a_m\alpha_m : \alpha_i \in F\}$ and so $|K| = q \cdots q = q^m$. □

Theorem 4.1.15. *For every prime p, and every positive integer m, there exists a unique finite field with p^m elements.*

Proof. Let $f(x) = x^{p^n} - x \in \mathbb{Z}_p[x]$. Then, there exists a spliting field K of $f(x)$ over $\mathbb{Z}_P$. Let $K = \mathbb{Z}_p$ (all roots of $f(x)$) and char$(K) = p$. Clearly, $f'(x) = p^m x^{p^m - 1} - 1$. If $\alpha \in K$, is a root of $f(x)$, then $f'(\alpha) = p^m \alpha^{p^m - 1} - 1$. Therefore $f(x)$ is separable over $\mathbb{Z}_p$. Let $S = \{$ *all roots of* $f(x)\}$. Then $|S| = p^m$, and $S \subseteq K$. Let $a, b \neq 0 \in S$, then $a^{p^m} - a = 0$ implies that $a^{p^m} = a, b^{p^m} = b$. $(a \pm b)^{P^m} = a^{p^m} \pm b^{p^m} = a \pm b$. $\implies a \pm b$ are roots of $f(x), a \pm b \in S$. Now, $(ab)^{p^m} = a^{p^m} b^{p^m} = ab \implies (ab)^{p^m} = -ab = 0$. ab is a root of $f(x)$ over Z_p and $ab \in S$. Clearly, $(b^{-1})^{p^m} = (b^{p^m})^{-1} \implies b^{-1}$ is a root of $x^{p^m} - x$. $\implies b^{-1} \in S$. Since $(S, +, .)$ is a field, and $\sigma : F_{p^m} \to F_{p^m}$ by $\sigma(a) = a^p$. S is a subfield of K. Since, K is the splitting field of $f(x), K \subseteq S$. and so $F_{p^n}|\mathbb{Z}_p$ is Galois extension. $\implies K = S$ and $|K| = p^m$. $\implies K = F_{p^m}$. □

Corollary 4.1.16. *F_{p^m} is a spliting field of $x^{P^n} - x$ over $\mathbb{Z}_p$.*

Corollary 4.1.17. *If F_1, F_2 are finite fields with $|F_1| = |F_2| = P^n$, then $F_1 \equiv F_2$.*

Proof. F_1 is a spliting field of $x^{p^m} - x$ over $\mathbb{Z}_p$. F_2 is a spliting field of $x^{P^m} - x$ over Z_p. Therefore, $\{F_1 \equiv F_2\}$. □

Proposition 4.1.18. *Let $m, n \in Z^+$, then $m|n \implies x^m - 1|x^n - 1$.*

Proof. By definition, $n = mk + r$, where $0 \leq r < m$. Now, $x^r(1 + x^m + x^{2m} + \cdots + x^{(k-1)m})(x^m - 1) + (x^r - 1)$.
$= x^r(x^m + x^{2m} + \cdots + x^{km} - 1 - x^m - x^{2m} \cdots x^{(k-1)m} + x^r - 1$.
$= -x^r + x^{km+r} + (x^r - 1) = x^n - 1$.
$x^r(\sum_{i=0}^{k-1} x^{im})(x^m - 1)(x^r - 1) = (x^n - 1)$.
Suppose, $x^m - 1|x^n - 1$ if and only if $x^r - 1 = 0$ if and only if $n = mk + 0$ if and only if $m|n$. □

Proposition 4.1.19. *If $m|n$, then $x^{p^m} - x|x^{p^n} - x$.*

Proof. Since, $m/n, n = \lambda m$, for some λ and $m \leq n$, $\implies p^m - 1|p^n - 1$
$\implies x^{p^m - 1} - 1|x^{p^n - 1} - 1$
$\implies x^{p^m} - x|x^{p^n} - x$.
Therefore, $[F_p : \mathbb{Z}_p] = n$. □

Theorem 4.1.20. *F_{p^m} is a subfield of F_{p^n} iff $m|n$.*

Proof. Suppose, F_{p^m} is a subfield of F_{p^n}. Then F_{p^n}/F_{p^m} is a field extension, and F_{p^n} is a vector space over F_{p^m}. Since, $|F_{p^n}| < \infty, [F_{p^n} : F_{p^m}] < \infty$, Since char $(F_{p^m}) = p$, $\mathbb{Z}_p$ is a prime subfield of F_{p^m}, and $[F_{p^n} : Z_p] = m < \infty$.

Clearly, $[F_{p^n} : \mathbb{Z}_p] = [F_{p^n} : F_{p^m}][F_{p^m} : \mathbb{Z}_p]$

$n = [F_{p^n} : F_{p^m}].m$ Clearly, $[F_{p^n} : F_{p^m}] = n/m$.

Conversely, $m|n$, Consider, $f(x) = x^{p^m - x}, g(x) = x^{p^n - x} \in \mathbb{Z}_p[x]$. Then, F_{p^m} is spliting field of $f(x)$ over $\mathbb{Z}_p$. and F_{p^n} is spliting field of $g(x)$ over Z_p. Clearly, $F_{p^n} = \mathbb{Z}_p$ (all roots of $g(x)$) and $F_{p^m} = z_p$ (all roots of $f(x)$.) Since $m|n$, $x^{p^m} - x/x^{p^n} - x$ over Z_p.

$x^{p^n} - x = x^{p^m} - x\lambda(x), \lambda(x) \in \mathbb{Z}_p[x]$. For any $\alpha \in F_{p^m}$, α is a root of $x^{p^m - x}$ over $\mathbb{Z}_p$ and so $\alpha \in F_{p^n}$. So $F_{p^m} \subseteq F_{p_n}$. Since F_{p^m} is field, F_{p^m} is a subfield of F_{p^n}. □

Remark 4.1.21. *Consider F_{p^m}. The number of subfields of F_{p^n} is $\tau(n)$.*

Theorem 4.1.22. *Let $p(x)$ be any irreducible polynomial of degree d over $\mathbb{Z}_p$. Then $p(x)|x^{p^n} - x$ over $\mathbb{Z}_p$ for some n. and hence $p(x)$ is separable.*

Proof. Let $p(x)$ be any irreducible polynomial over $\mathbb{Z}_p$. and $deg(p(x)) = d$. Then there exists an extension k of $\mathbb{Z}_p$ such that K has a root α of $p(x)$ and $[K : \mathbb{Z}_p] = deg(p(x))d$. Clearly, $\{1, \alpha, \alpha^2, \cdots \alpha^{d-1}\}$ is a basis for K over $\mathbb{Z}_p$. $K = \mathbb{Z}_p(\alpha) = \{a_0 + 1.a_1\alpha + \cdots + a_{d-1}\alpha^{d-1} : \alpha_i \in Z_P\}$. and $|K| = p^d$, and $K = \mathbb{F}_{p^d}$is a spliting field of $x^{P^d - x}$ over $\mathbb{Z}_p$. Therefore, $\alpha \in K$ is a root of $x^{P^d - x}$ over Z_p. Clearly, $\mathbb{Z}^{(\alpha)}_{\alpha,\mathbb{Z}_p} = P(x)$ and $P(x)/x^{p^d - x}$

over $\mathbb{Z}_p$. Since, $x^{p^d - x}$ is separable over $\mathbb{Z}_p$ and $p(x)$ is separable over $\mathbb{Z}_p$.

□

Proposition 4.1.23. *Given any positive integer n, there exists an irreducible polynomial of degree n over a finite field F.*

Proof. Consider, F_{p^m}, then F_{p^m} is a subfield of $F_{p^{mn}}$. That implies $F_{p^{mn}}/F_{p^m}$ is field extension.

$[F_{P^{mn}} : F_{p^m}] = mn/m = n$. Since $F_{p^{mn}} = F_{p^{m(\alpha)}}$.

$[F_{P^{mn}} : F_{p^m}] = [F_{p^{m(\alpha)}} : F_{P^m}] < \infty$. α is algebraic over F_{p^m}.

$[F_{p^{m(\alpha)}} : F_{P^m}] = deg(m_{\alpha, F_{p^m}}(\alpha)) = n$. □

Let us sum up:

- Finite field.
- Cyclic group.
- Division ring.

Check your progress

1. If the finite field F has p^m elements then every $a \in F$ satisfy —
2. Any two finite fields having the same number of elements are —

4.2 Wedderburn Theorem

Theorem 4.2.1 (Wedderburn theorem). *Every finite divisional ring is a field.*

Proof. Let D be any finite divisional ring. Let $F = Z(D) = \{x \in D : xy = yx, \text{ for all } y \in D\}$. Then F is a field and $F \subseteq D$. Clearly D is a vector space over F and $dim_F(D) = n < \infty$. Since $|D| < \infty$, $|F| = q < \infty$.

Clearly $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ is a basis for D over F and so

$$D = \{a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n : a_i \in F\}$$

and $|D| = q^n$. Let $G = (D^*, .)$ be a group. Then $Z(G) = \{x \in D^* : xy = yx, \text{ for all } y \in D^*\} = F^*$. Clearly $|G| = q^n - 1$ and $|F^*| = q - 1$. By Class equation,

$$|G| = |Z(G)| + \sum_{a \notin Z(G)} [G : N_G(a)] \longrightarrow (1)$$

.

For any $a \in Z(G), cl_G(a) = \{gag^{-1} : g \in G\} = \{a\}$. For any $a \notin Z(G), N_G(a) < G$.

$$|cl_G(a)| = [G : N_G(a)] = \frac{|G|}{|N_G(a)|}$$

. In $D, C_D(a) = \{x \in D : xa = ax\}, N_G(a) = \{x \in D : xa = ax\}$ and $C_D(a)^* = N_G(a)$. Clearly, $(C_D(a), +) \leq (D, +)$ and by Lagrange's theorem, $|C_D(a)|$ divides $|D| = q^n$. Thus $|C_D(a)| = q^{n(a)}$, for some $n(a) \in \mathbb{Z}^+$. Since $N_G(a) = C_D(a)^*, |N_G(a)| = q^{n(a)} - 1$. Since $N_G(a)$ is a subgroup of G, $|N_G(a)|$ divides $|G|, q^{n(a)} - 1 \mid q^n - 1$ if and only if $n(a) \mid n$ and $n(a) \neq n$.

Equation (1), $|G| = q - 1 + \sum\limits_{n(a)|n, n(a)\neq n} \frac{q^n - 1}{q^{n(a)-1}}$.

Let $x^n - 1 = \prod\limits_{d|n} \Phi_d(x) \in \mathbb{Z}[x]$. For $d|n, d \neq n$, $x^d - 1 = \prod\limits_{m|d, m\neq n} \Phi_m(x)$. $x^d - 1 | x^n - 1 \Rightarrow x^n - 1 = (x^d - 1)g(x)$, where $g(x) \in \mathbb{Z}[x] = (x^d - 1)\Phi_n(x)h(x)$, where $h(x) \in \mathbb{Z}[x]$. From this we get, $\frac{x^n-1}{x^d-1} = \Phi_n(x)h(x)$. Now $\Phi_n(x) \mid \frac{x^n-1}{x^d-1}$, for all $d|n\&\ d \neq n$.

$\Rightarrow \Phi_n(x) \mid \sum\limits_{d|n\&\ d\neq n} \frac{x^n-1}{x^d-1}$. Since $\Phi_n(x) \in \mathbb{Z}[x], \Phi_n(q) \in \mathbb{Z}$

$\Rightarrow \Phi_n(q) \mid \sum\limits_{n(a)|n, n(a\neq n)} \frac{q^n-1}{q^{n(a)}-1}$. Since, $x^n - 1 = \Phi_n(x) \prod\limits_{d|n, d\neq n} \Phi_d(x)$.

$q^n - 1 = \Phi_n(q) \prod\limits_{d|n, d\neq n} \Phi_d(q)$.

$\Rightarrow \Phi_n(q) | q^n - 1$.

$\Phi_n(q) | (|G| - \sum\limits_{n(a)|n, n(a)\neq n} \frac{q^n-1}{q^{n(a)}-1})$ and so $\Phi_n(q) | q - 1$.

Claim: $n = 1$.

If $n > 1$, then $\Phi_n(x) = \prod\limits_{\alpha\in\mu_n, |\alpha|=n} (x - \alpha)$. $\Phi_n(q) = \prod\limits_{\alpha\in\mu_n, |\alpha|=n} (q - \alpha) \in \mathbb{Z}$.

For $\alpha \in \mu_n$ and $|\alpha| = n, |q - \alpha| > q - 1$. $|\Phi_n(x)| > q - 1$ which implies $\Phi_n(q) \nmid q - 1$, which is a contradiction. Hence $n = 1$ and $F = D$. □

Let us sum up:

- Wedderburn theorem.
- Commutative field.
- Finite division ring.
- Jacobson theorem.

Check your progress

1. A finite division ring is necessarily —

2. Any finite subring of a division ring is —

Unit Summary:

In this unit, we discussed the concept of finite extension and splitting field. Further, we proved the WedderburnâĂŹs theorem on finite division rings.

Glossary:

- If F has p^m elements then every $a \in F$ satisfies $a^{p^m} = a$.
- $x^{p^m} - x = \Pi_{\lambda \in F}(x - \lambda)$
- The Wedderburn's theorem.
- Cyclotomic polynomials (Examples: $\Phi_1(x) = x - 1,\ \Phi_2(x) = x + 1$ and $\Phi_3(x) = x^1 + x + 1$.)

Self Assessment questions

1. The multipicative group of non-zero elements of a finite field is cyclic.
2. Prove that for every prime number p and every positive integer m there exists a field having p^m elements.
3. Show that a finite division ring is necessarily a commutative field.
4. If R is a finite ring in which $x^n = x$, for all $x \in R$ where $n > 1$ prove that R is commutative.

Exercises

1. Let G be a finite abelian group enjoying the property that the relation $x^n = e$ is satisfied by at most n elements of G, for every integer n. Then G is a cyclic group.

2. If the field F has p^n elements prove that the automorphisms of F form a cyclic group of order n.

3. If $\theta \neq 1$ is a root of unity and if q is a positive integer, prove that $|q - \theta| > q - 1$

4. Let D be a division ring and K a subdivision ring of D such that $xKx^{-1} \subset K$ for every $x \neq 0$ in D. Prove that either $K \subset Z$, the center of D or $K = D$.

Answer for check your progress

Section 4.1

1. $a^{p^m} = a$

2. Isomorphic

Section 4.2

1. Commutative field

2. Division ring

References:

1. I.N. Herstein, Topics in Algebra (II Edition) Wiley Eastern Limited, New Delhi, 1975.

Suggested Reading:

1. M. Artin, Algebra, Prentice Hall of India, 1991.
2. P.B. Bhattacharya, S.K. Jain, and S.R. Nagpaul, Basic Abstract Algebra (II Edition) Cambridge University Press, 1997. (Indian Edition)
3. I.S. Luther and I.B.S. Passi, Algebra, Vol. I âĂŞGroups(1996); Vol. II Rings, Narosa Publishing House , New Delhi, 1999
4. D.S. Malik, J.N. Mordeson and M.K. Sen, Fundamental of Abstract Algebra, McGraw Hill (International Edition), New York. 1997.
5. N. Jacobson, Basic Algebra, Vol. I & II Hindustan Publishing Company, New Delhi.

UNIT - 5

Unit 5

Solvability of Radicals

Objectives:

- Recall the splitting field of polynomial over F.
- To know the solvable by radicals over F.
- To prove the Frobenius theorem and Four-square theorem.

5.1 Frobenious Theorem

Definition 5.1.1. A division ring D is said to be algebraic over a field F if

1. $F \subseteq Z(D)$
2. For any $\alpha \in D$, $f(\alpha) = 0$ for some $f(x) \in F[x]$

Remark 5.1.2. *If D is algebraic over F, then F is subdivision ring of D and so D is a vector space over F and D has a non-zero basis.*

Theorem 5.1.3. *Let D be the division ring. If D is algebraic over $\mathbb{C}$, then $D = \mathbb{C}$.*

Proof. By definition, $\mathbb{C}$ is the subdivision ring of D and so $\mathbb{C} \subseteq D$. For any $\alpha \in D$, α is a root of some $f(x) \in F[x]$ and $deg(f(x)) = n$.
By Fundamental Theorem of Algebra,

$$f(x) = (x - \lambda_1)(x - \lambda_2) \cdots (x - \lambda_n)$$

where $\lambda_i \in \mathbb{C}$. Clearly $f(\alpha) = (\alpha - \lambda_1)(\alpha - \lambda_2) \cdots (\alpha - \lambda_n) = 0$. $(\alpha - \lambda_1)(\alpha - \lambda_2) \dots (\alpha - \lambda_n) = 0$ in D ....(1).

Since $\alpha, \lambda_i \in D$, $\alpha - \lambda_i \in D$ $\forall i$. Since D has no zero divisor, $\prod\limits_{i=1}^{n}(\alpha - \lambda_i) = 0 \Rightarrow \alpha - \lambda_i = 0$ for some i. From this, we get $\alpha = \lambda_i \in D$; $ab = 0 \Rightarrow a = 0$ or $b = 0$. Therefore $D \subseteq \mathbb{C}$ and hence $D = \mathbb{C}$. □

Theorem 5.1.4. *(Frobenious Theorem) Let D be the division ring. If D is algebraic over $\mathbb{R}$, then $D = \mathbb{R}, \mathbb{C}$ or real quaterinion ring.*

Proof. By definition $\mathbb{R}$ is a subdivision ring of D. If $D = \mathbb{R}$, then trivial fact. Suppose $D \neq \mathbb{R}$. Then there exists $a \in D$ such that $a \notin \mathbb{R}$. Since D is algebraic over $\mathbb{R}$, a is a root of some irreducible polynomial $g(x)$ over $\mathbb{R}$. Clearly $deg(g(x)) = 1$ or 2. If $deg(g(x)) = 1$, then $g(x) = cx + d$ where $c, d \in \mathbb{R}$ and $c \neq 0$. Now $g(a) = 0 \Rightarrow ca + d = 0$ and so $a = -\frac{d}{c} \in \mathbb{R}$, which is a contradiction to $a \notin \mathbb{R}$. Hence $deg(g(x)) = 2$. Let $g(x) = x^2 - 2\alpha x + \beta \in \mathbb{R}[x]$ where $\alpha, \beta \in \mathbb{R}$ and $\beta \neq 0$. Since $g(a) = 0 \Rightarrow a^2 - 2a\alpha + \beta = 0$, $a^2 - 2a\alpha + \alpha^2 = \alpha^2 - \beta$ and so $(a - \alpha)^2 = \alpha^2 - \beta$.

Claim: $\alpha^2 - \beta < 0$. Suppose $\alpha^2 - \beta > 0$. Then there exists $\delta \in \mathbb{R}$ such that $\alpha^2 - \beta = \delta^2 = (a - \alpha)^2$. This implies $a - \alpha = \pm\delta$ and so $a = \pm\delta + \alpha \in \mathbb{R}$, which is a contradiction to $a \notin \mathbb{R}$. Hence $\alpha^2 - \beta = 0$. Since $(a - \alpha)^2 = \alpha^2 - \beta$, $(a - \alpha)^2 = \alpha^2 - \beta - \gamma^2$ for some $\gamma \in \mathbb{R}$. From this, $(\frac{a-\alpha}{\gamma})^2 = -1$. Take $i = \frac{a-\alpha}{\gamma}$, $i^2 = -1$.

Suppose D is a commutative ring. Then $\mathbb{R} \subseteq \mathbb{R}(i) \subseteq D$, $\lambda_i = 0$ for some i. Since D is algebraic over F, D is algebraic over $\mathbb{R}(i) = \mathbb{C}$. By above theorem, $D = \mathbb{C}$.

Suppose D is not commutative.

Claim: $Z(D) = \mathbb{R}$**.**

Suppose $Z(D) \neq \mathbb{R}$. Since D is algebraic over $\mathbb{R}$, $\mathbb{R} \subsetneq Z(D)$ and $\exists$ $a \in Z(D)$ such that $a \notin \mathbb{R}$. $a \in D$, by above argument, $\exists$ $\alpha, \gamma \in F$ such that $(\frac{a-\alpha}{\gamma})^2 = -1$ and $i = \frac{a-\alpha}{\gamma} \notin \mathbb{R}$ and $i \in D$, $i^2 = -1$. Clearly $R \subsetneq \mathbb{R}(i) \subsetneqq D$. Since D is algebraic over $\mathbb{R}$, D is algebraic over $\mathbb{R}(i) = \mathbb{C}$. By above theorem $D = \mathbb{C}$ is a commutative ring which is a contradiction. Hence $Z(D) = \mathbb{R} \neq D$.

Let $a \in D$ with $a \notin \mathbb{R}$. Then there exists $\alpha, \gamma \in \mathbb{R}$ such that $i = \frac{a-\alpha}{\gamma} \notin \mathbb{R}$ and $i^2 = -1$ and $i \notin \mathbb{R}$. $i \notin Z(D)$, then $\exists$ $b \in Z(D)$ such that $ib \neq bi$. Let $c = bi - ib \neq 0$ in D. Then $ic + ci = i(bi - ib) + (bi - ib)i$ implies $ic + ci = ibi - i^2b + bi^2 - ibi$ and so $ic + ci = b - b = 0$ implies $ic = -ci$. Also $ic^2 = (ic)c = (-ci)c = -c(ic) = c^2i$ implies $ic^2 = c^2i$. Since $c \in D$, c is a root of $f(x)$ over $\mathbb{R}$. This implies c is a root of the irreducible polynomial $x^2 + \lambda x + \mu \in \mathbb{R}[x]$ and so $c^2 + \lambda c + \mu = 0$. Hence $\lambda c = -c^2 - \mu$. Since $\lambda \in \mathbb{R}$, $i\lambda = \lambda i$. Also $(\lambda c)i = (-c^2 - \mu)i = -c^2i - \mu i = -ic^2 - i\mu =$

$i(-c^2 - \mu) = i(\lambda c)$ and so $2\lambda ci = 0$.

Since $c \neq 0$ and $i \neq 0$ and D is a division ring, $\lambda = 0$ and $c^2 = -\lambda$.

If $\mu < 0$ then $c^2 > 0$ and $c^2 \in \mathbb{R}$ and $c^2 = (bi - ib)(bi - ib)$ and $c^2 = i(ib^2 - b^2 i) \notin \mathbb{R}$, which is contradiction to $c^2 \in \mathbb{R}$. Hence $\mu > 0$ and $c^2 = -\nu^2$ $(\mu = \nu^2)$ and $(\frac{c}{\nu}) = -1$. Take $j = \frac{c}{\nu}$ and $k = ij$.

Let $T = \{\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k : \alpha_i \in \mathbb{R}\}$. Then $T \subset D$, T is a subdivision ring of D.

If $\nu \in D$ satisfies $\nu^2 = -1$, then $C(\nu) = \{x \in D : x\nu = \nu x\}$ is a subring of D and $1, 0 \in C(\nu)$ and $C(\nu)$ is a subring of D. Now $Z(D) = \mathbb{R} \subset C(\nu) \Rightarrow C(\nu)$ is a vector space over $\mathbb{R}$ and $dim_{\mathbb{R}}(C(\nu)) = 2$. From this, $\{1, \nu\}$ is a basis for $C(\nu)$ over $\mathbb{R}$ and so $C(\nu) = \{\alpha_0 + \alpha\nu / \alpha_i \in \mathbb{R}\}$.

Suppose $D \neq T$. Then there exists $u \in D$ such that $u \notin D$ and so $u \notin \mathbb{R}$ and for $\alpha, \gamma \in \mathbb{R}$ such that $(\frac{u-\alpha}{\gamma})^2 = -1$. Let $w = \frac{u-\alpha}{\gamma}$ and $iw + wi \in D$, $i(iw + wi) = -w + iwi = w(-1) + iwi = wi^2 + iwi = (wi + iw)i$ and $w(iw + wi) = wiw + w^w i = wiw + (-1)i = wiw + i(-1) = wiw + iw^2 = (wi + iw)w$. This implies $iw + wi \in C(i)$ and $iw + wi = \alpha_0 + \alpha_1 i = \alpha'_0 + \alpha'_1 i$. Clearly $iw + wi \in C(w)$. □

Theorem 5.1.5. *Let F be a field and F contains all n^{th} roots of unity and $a \neq 0 \in F$. If $f(x) = x^n - a \in F[x]$, then*

1. *the splitting field of $f(x)$ over F is $F(u)$ for some root u of $f(x)$*

2. *$[K : F]$ is normal extension*

3. *$Gal[K : F]$ is abelian.*

Proof. Let ω be the n^{th} root of unity. Then $1, \omega, \omega^2, \ldots, \omega^{n-1}$ are distinct roots of $x^n - 1$ over F and so $\nu_n = \{1, \omega, \omega^2, \ldots, \omega^{n-1}\}\} =< \omega >$.

Let $f(x) = x^n - a \in F[x]$. Then $\sqrt[n]{a}$, $\sqrt[n]{a}\omega, \ldots, \sqrt[n]{a}\omega^{n-1}$ are roots of $f(x)$ over F. If $\omega^j \sqrt[n]{a} = \omega^j \sqrt[n]{a}$ for $1 \leq i \leq j \leq n$. Then by cancellation law, $\omega^i = \omega^j$

$\omega^{i-j} = 1$. Since $|w| = n$ and $i - j < n$, $\omega^{i-j} = 1$. This is not possible. Hence $\sqrt[n]{a}$, $\sqrt[n]{a}\omega, \ldots, \sqrt[n]{a}\omega^{n-1}$ are distinct roots of $f(x)$ over F and so $f(x)$ is separable over F. By hypothesis, $1, \omega, \omega^2, \ldots, \omega^{n-1} \in F$ and so $K = F(\sqrt[n]{a})$ is the splitting field of $f(x)$ over F and so $[K : F]$ is Galois extension. Let $\sigma, \tau \in Gal[K : F]$. Then $\sigma(\sqrt[n]{a})$ and $\tau(\sqrt[n]{a})$ are roots of $f(x)$ over F. Let $\sigma(\sqrt[n]{a}) = \omega^i \sqrt[n]{a}$ and $\tau(\sqrt[n]{a}) = \omega^j \sqrt[n]{a}$, $i \neq j$. Clearly $(\sigma \circ \tau)(\sqrt[n]{a}) = \sigma(\tau(\sqrt[n]{a})) = \sigma(\omega^j(\sqrt[n]{a})) = \omega^i \omega^j \sqrt[n]{a}$ and so $(\sigma \circ \tau)(\sqrt[n]{a}) = \omega^{i+j} \sqrt[n]{a}$. Clearly $(\tau \circ \sigma)(\sqrt[n]{a}) = \tau(\sigma(\sqrt[n]{a})) = \tau(\omega^i(\sqrt[n]{a})) = \omega^j \omega^i \sqrt[n]{a}$ and so $\omega^{i+j} \sqrt[n]{a}$. Therefore $(\tau \circ \sigma)(\sqrt[n]{a} = (\sigma \circ \tau)(\sqrt[n]{a})$ and $(\tau \circ \sigma) = (\sigma \circ \tau)$ and hence $Gal[K : F]$ is abelian. Since $\mathbb{R}$ is the splitting of $f(x)$ over F, $[K : F]$ is normal extension □

Let us sum up:

- Algebraic over a field F.
- Frobenius theorem.

Check your progress

1. If C be the field of complex numbers and suppose that the division ring D is algebraic over C, then —

2. If D be a division ring over F. If $a \in D,\ a \notin F$ such that $[(a-\alpha)/\gamma]^2 =$

5.2 Radical Extension

Definition 5.2.1. A group G is said to be solvable(or soluble) if there exists a chain of subgroups

$$\{e\} = H_0 \subseteq \cdots \subseteq H_n = G$$

such that each H_i is a normal subgroup of H_{i+1} and the factor groups H_{i+1}/H_i is abelian for every $i = 0, \ldots n-1$.

The above series is referred to as solvable series of G.

Example 5.2.2. Any abelian group is solvable.

Example 5.2.3. Any non-abelian simple group is not solvable.

Definition 5.2.4. Let G be a group and $a, b \in G$. Then $aba^{-1}b^{-1}$ is called the *commutator* of a and b and is denoted by $[a, b]$. Let $A = \{aba^{-1}b^{-1} : a, b \in G\} = \{[a, b] : a, b \in G\}$ be the set of all commutators of elements in G.

Definition 5.2.5. Let G be a group. The subgroup of G generated by the commutators of elements of G is called the *commutator subgroup* of G. The commutator subgroup of a group G is denoted by G' or $G^{(1)}$ or $[G, G]$. Note that commutator subgroup is also called derived subgroup of G.

Theorem 5.2.6. *Let G be a group. Then $G' = \{e\}$ if and only if G is abelian.*

Proof. Let G' be the commutator subgroup of G. Assume that $G' = \{e\}$. Then by Definition 5.2.5, $aba^{-1}b^{-1} = e$ for all $a, b \in G$ and hence $ab = ba$ for all $a, b \in G$. Hence G is abelian.

Conversely, assume that G is abelian. Then $ab = ba$ for all $a, b \in G$ which implies $ab\,(ba)^{-1} = aba^{-1}b^{-1} = e$ for all $a, b \in G$ and hence $G' = \{e\}$. □

Theorem 5.2.7. *Let G be a group. Then*

(i) G' is a normal subgroup of G.

(ii) G/G' is abelian.

(iii) If H is a subgroup of G, then G/H is abelian and H is a normal subgroup of G if and only if $G' \subseteq H$.

Proof. (i) Let $g \in G$ and $x \in G'$. Then $x = c_1 \ldots c_n$ where $c_i^{'}$ s are commutators of elements in G and hence $c_i = a_i b_i a_i^{-1} b_i^{-1}$ for some $a_i, b_i \in G$ for all $i = 1, \ldots, n$. Now

$$\begin{aligned} gxg^{-1} &= g\,(c_1 \ldots c_n)\,g^{-1} \\ &= g\left(a_1 b_1 a_1^{-1} b_1^{-1} \cdots a_n b_n a_n^{-1} b_n^{-1}\right) g^{-1} \\ &= \left(g a_1 g^{-1}\right)\left(g b_1 g^{-1}\right)\left(g a_1^{-1} g^{-1}\right)\left(g b_1^{-1} g^{-1}\right) \cdots \left(g a_n g^{-1}\right) \\ &\quad \left(g b_n g^{-1}\right)\left(g a_n^{-1} g^{-1}\right)\left(g b_n^{-1} g^{-1}\right) \end{aligned}$$

Hence $gxg^{-1} \in G'$ and so G' is normal subgroup of G.

(ii) By (i), G/G' is a group and also $aba^{-1}b^{-1} \in G'$ for all $a, b \in G$. From this, we get $abG' = baG'$ for all $a, b \in G$ and so $aG'bG' = bG'aG'$ for all $a, b \in G$. Hence G/G' is abelian.

(iii) Assume that G/H is abelian and H is a normal subgroup of G. Then $xH\ yH = yH\ xH$ for all $x, y \in G$ and so $(xy)\,(yx)^{-1} \in H$ for all $x, y \in G$. Thus $xyx^{-1}y^{-1} \in H$ for all $x, y \in G$ and so $G' \subseteq H$.

Conversely, assume that $G' \subseteq H$. For any $g \in G$ and $x \in H$, $gxg^{-1} = gxg^{-1}x^{-1}x \in H$, which shows that H is a normal subgroup of G. Since $G' \subseteq H$, $aba^{-1}b^{-1} \in H$ for all $a, b \in G$ and so $aH\ bH = bH\ aH$ for all $a, b \in G$. Hence G/H is abelian. □

Definition 5.2.8. Let $[K : F]$ be a field extension. $[K : F]$ is simple radical extension if $K = F(\alpha)$ such that $\alpha^n \in F$ for some $n \in \mathbb{Z}^+$.

Example 5.2.9. $\mathbb{Q}(\sqrt{2})|\mathbb{Q}$, $\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q}$ and $\mathbb{Q}(\omega)|\mathbb{Q}$ are all simple radical extensions.

Example 5.2.10. Is $\mathbb{Q}(\sqrt{2}, \sqrt{3})|\mathbb{Q}$ a simple radical extension?

Solution:

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

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

$(\sqrt{2}+\sqrt{3})^3 = (\sqrt{2}+\sqrt{3})(5+2\sqrt{6})$ and so $(\sqrt{2}+\sqrt{3})^n \notin \mathbb{Q}$ for any $n \in \mathbb{Z}^+$. Clearly $\mathbb{Q}(\sqrt{2}, \sqrt{3})|\mathbb{Q}$ is not a simple radical extension

Definition 5.2.11. $[K : F]$ is radical extension if there is a tower of fields $F = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_i \subset F_{i+1} \subset \cdots \subset F_k = K$ such that each $F_{i+1}|F_i$ is simple radical.

Example 5.2.12. Is $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ a radical extension?

Clearly $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})|\mathbb{Q}$ is radical extension, since $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$, $\mathbb{Q} \subset \mathbb{Q}(\sqrt{3}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$ and $\mathbb{Q} \subset \mathbb{Q}(\sqrt{6}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Example 5.2.13. Clearly $\mathbb{Q}(\sqrt[4]{5}, i)|\mathbb{Q}$ is radical extension, since $\mathbb{Q} \subset \mathbb{Q}(i) \subset \mathbb{Q}(\sqrt[4]{5}, i) \subset \mathbb{Q}(\sqrt[4]{5}, i)$.

Definition 5.2.14.

1. Let $[K : F]$ be algebraic extension and $\alpha \in K$. Then α is solvable by radical or α is solvable over F if there exists a radical extension $[L : F]$ such that $\alpha \in L$.
2. $[K : F]$ is solvable if α is solvable over F for all $\alpha \in K$.
3. Let $f(x) \in F[x]$ be solvable. Then all of roots the splitting field are solvable over F.

Example 5.2.15. Let $f(x) = x^3 - 2 \in \mathbb{Q}[x]$. Then $\sqrt[3]{2}$, $\omega\sqrt[3]{2}$, $\omega^2\sqrt[3]{2}$ are the roots of $f(x)$ over $\mathbb{Q}$ and so $K = \mathbb{Q}(\sqrt[3]{2}, \omega)|\mathbb{Q}$ is radical extension, since $\mathbb{Q} \subset \mathbb{Q}(\omega) \subset \mathbb{Q}(\sqrt[3]{2}, \omega)$, $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{Q}(\sqrt[3]{2}, \omega)$, and $\mathbb{Q} \subset \mathbb{Q}(\omega\sqrt[3]{2}) \subset \mathbb{Q}(\sqrt[3]{2}, \omega)$, and $\mathbb{Q} \subset \mathbb{Q}(\omega^2) \subset \mathbb{Q}(\sqrt[3]{2}, \omega)$. Therefore $f(x)$ is solvable over $\mathbb{Q}$.

Theorem 5.2.16. *If $p(x) \in F[x]$ is solvable by radicals over F, then the Galois group over F of $p(x)$ is a solvable group.*

Proof. Let K be the splitting field of $p(x)$ over F.

Then the galois group of $p(x)$ over F is $G(K, f)$.

Since $p(x)$ is solvable by radicals over F, then there exists a sequence of fields.

$$F \subset F_1 = F\left(\omega_1\right) \subset F_2 = F_1\left(\omega_2\right) \subset \ldots \subset F_K = F_{K-1}\left(\omega_K\right)$$

, where $\omega_1^{r_1} \in F, \omega_2^{r_2} \in F_1, \ldots, \omega_k^{r_k} \in F_{K-1}$ and KCF_k. W.L.O.G, assume that F_K is a normal extension of F.

Since F_K is a normal extension of F, then F_K is also a normal extension of any intermediate field.

Hence F_k is a normal extension of each F_i. By lemma, each F_i is a normal extension of F_{i-1} and since F_K is a normal over F_{i-1}, by theorem, $G\left(F_K, F_{i-1}\right)$ is a normal subgroup in $G\left(F_K, F_{i-1}\right)$.

consider the chain,

$$G\left(F_k, F\right) \supset G\left(F_k, F_1\right) \supset \ldots \supset G\left(F_k, F_{k-1}\right) \supset \{e\} \qquad (1)$$

Each subgroup in this chain is a normal subgroup.

Since F_i is a normal extension of F_{i-1}, by the fundamental theorem of

Galois theory, the group of F_i over F_{i-1},

$$G\left(F_i, F_{i-1}\right) \text{ is isomorphic to } \frac{G\left(F_k, F_{i-1}\right)}{G\left(F_k, F_i\right)}$$

By lemma, $G\left(F_i, F_{i-1}\right)$ is an abelian group.

Thus, each quotient group $\frac{G(F_h, F_{i-1})}{G(F_F, F_i)}$ of the chain (1) is abelian.

Thus the group $G\left(F_K, F\right)$ is solvable.

Since $K \subset F_K$ and K is a normal extension of F by Theorem , $G\left(F_K, F\right)$ is a normal subgroup of $G\left(F_K, F\right)$ and $G(K, F)$ is isomorphic to $\frac{G(F_K, F)}{G(F_K, K)}$.

Thus, $G(K, F)$ is a homomorphic image of $G\left(F_K, F\right)$.

Since $G\left(F_K, F\right)$ is a solvable group, by the corollary to lemma-5.7.1, $G(K, F)$ must be a solvable group.

Since $G(K, F)$ is a galois group of $p(x)$ over F, and $G(K, F)$ is solvable, then the galois group of $p(x)$ over F is solvable group. □

Remark 5.2.17. *The converse of this theorem is also true. i.e. If the Galois group of $P(x)$ over F is solvable, then $p(x)$ is solvable by radicals over F.*

Theorem -5.7.2 and its converse part are true even if F does not contain roots of unity.

Theorem 5.2.18. *(Classic Theorem of Abel): The general polynomial of degree $n \geq 5$ is not solvable by radicals.*

Proof. If $F\left(a_1, a_2, \ldots, a_n\right)$ is the field of rational functions in the n variables $a_1, a_2, \ldots, a_n$.

Then the Galois group of the polynomial

$$p(t) = t^n + a_1 t^{n-1} + \cdots + a_n$$

over $F\left(a_1, a_2, \ldots, a_n\right)$ was s_n the symmetric group of degree n. Then, S_n is not a solvable group when $n \geq 5$.

Thus, $p(t)$ is not solvable by radicals over $F\left(a_1, a_2, \ldots, a_n\right)$ when $n \geq 5$.

□

Let us sum up:

- Solvable by radicals.
- Solvable.
- Homomorphic image.
- Galois group is solvable group.

Check your progress

1. S_n is not solvable for —
2. If α, β, γ are the roots of the equation $x^3 + 3x^2 + 2x + 1 = 0$, then the value of $\sum \alpha\beta =$

5.3 Integral Quaternions

Let Q be the division ring of real quaternions.

Definition 5.3.1. For $x = a_0 + a_1 i + a_j + a_3 k \in Q$, the adjoint of x, denoted by x^*, is defined by $x^* = a_0 - a_1 i - a_2 j - a_3 k$.

Lemma 5.3.2. *The adjoint in Q satisfies*

(i) $x^{**} = x$

(ii) $(\alpha x + \beta y)^* = \alpha x^* + \beta y^*$, *where* $\alpha, \beta \in \mathbb{R}$

(iii) $(xy)^* = y^* x^*$.

Proof. (i) Let $x = a_0 + a_1 i + a_j + a_3 k \in Q$. Then $x^* = a_0 - a_1 i - a_2 j - a_3 k$ and $(x^*)^* = a_0 + a_1 i + a_2 j + a_3 k = x$.

(ii) Let $x = a_0 + a_1 i + a_j + a_3 k$ and $y = b_0 + b_1 i + b_j + b_3 k \in Q$. Then $\alpha x + \beta y = (\alpha a_0 + \beta b_0) + (\alpha a_1 + \beta b_1)i + (\alpha a_2 + \beta b_2)j + (\alpha a_3 + \beta b_3)k$. Therefore by the definition of $*$, $(\alpha x + \beta y)^* = (\alpha a_0 + \beta b_0) - (\alpha a_1 + \beta b_1)i - (\alpha a_2 + \beta b_2)j - (\alpha a_3 + \beta b_3)k = \alpha x^* + \beta y^*$.

(iii) It is enough to do so for a basis of Q over the reals. We prove it for the particular basis $1, i, j, k$. Now $ij = k$ and $(ij)^* = k$ and $(ij)^* = -k$. Similarly $(ik)^* = k^* i^*$, $(jk)^* = k^* j^*$. Also $(i^2)^* = -1 = (i^*)^2$, and similarly for j and k. Since part (iii) is true for the basis elements and part (ii) holds, (iii) is true for all linear combinations of the basis elements with real coefficients, hence (ii) holds for all arbitrary $x, y \in Q$ □

Definition 5.3.3. If $x \in Q$, then the norm of x, denoted by $N(x)$, is defined by $N(x) = xx^*$.

Note that if $x = a_0 + a_1 i + a_2 j + a_3 k \in Q$, then $x^* = a_0 - a_1 i - a_2 j - a_3 k$ and $N(x) = a_0^2 + a_1^2 + a_2^2 + a_3^2$. Also $N(0) = 1$ and $N(x)$ is a positive real number for $x \neq 0$ in Q. In particular, for any real number a, $N(a) = a^2$. If $x \neq 0$, then $x^{-1} = \frac{1}{N(x)} x^*$.

Lemma 5.3.4. *For all $x, y \in Q$, $N(xy) = N(x)N(y)$.*

Proof. By the very definition of norm, $N(xy) = (xy)(xy)^*$. By Lemma 5.3.2, $(xy)^* = y^* x^*$ and so $N(xy) = xyy^* x^* = xN(y)x^*$. Since $N(y)$ is real and $N(y)$ is in center of Q, $N(xy) = xx^* N(y) = N(x)N(y)$. □

Theorem 5.3.5. *Every positive integer can be expressed as the sum of squares of four integers.*

Proof. Given a positive integer n.
To claim: $n = x_0^2 + x_1^2 + x_2^2 + x_3^2$ for four integers x_0, x_1, x_2, x_3.
Since every integer factors into a product of prime numbers, if every prime number were written as a sum of four squares. By Lagrange identity, every integer can be expressed as a sum of four squares.

Thus, we have to prove this theorem for prime numbers n.

For $n = 2$, the prime number 2 can be written as $1^2 + 1^2 + 0^2 + 0^2$ as a sum of four squares.

Thus, WLOG , assume that n is an odd Prime number p. consider the quaternions W_p over J_p, the integer mod p.

$$W_p = \{\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k \mid \alpha_0, \alpha_1, \alpha_2, \alpha_3 \in J_p\}$$

$\Rightarrow W_p$ is a finite ring. since $p \neq 2$, it is not commutative for $ij = -ji \neq ji$. Thus, by Wedderburn's theorem, Wp cannot be a division ring. (By problem 1 of sec.3.5) It must have a left-ideal, which is neither (0) nor Wp.

But then the two-sided ideal V in H, defined by

$$V = \{x_0\xi + x_1 i + x_2 j + x_3 k \mid P \text{ divides all of } x_0, x_1, x_2, x_3\}.$$

It cannot be a maximal left -ideal of H, since H/V is isomorphic to Wp. (If V were a maximal left-ideal in $H, H/V$ and so W_p, would have no left -ideals other than (0) and H/V).

Thus, there is a left-ideal L of H satisfying $L \neq H, L \neq V$ and $L \supset V$.

By lemma, there exists $u \in L$ such that every element in L is a left -multiple of u.

since $p \in V$ and $p \in L$, then $p = cu$ for some $c \in H$.

Since $u \notin V, c$ cannot have an inverse in H, otherwise $u = c^{-1}p$ would be in V.

Thus, $N(C) > 1$ by lemma.

since $L \neq H, U$ cannot have an inverse in H, hence, $N(u) > 1$. Since

$p = cu$ & $p^2 = N(p)$ gives

$$\begin{aligned} p^2 &= N(p) \\ &= N(cu) \\ &= N(c)N(u) \end{aligned}$$

But $N(c)$ & $N(u)$ are integers, since both c and U are in H, both are larger than 1& both divide p^2.

The only way this is possible is that $N(C) = N(U) = P$.

since $u \in H$, $u = m_0\xi + m_1 i + m_2 j + m_3 k$

where m_o, m_1, m_2, m_3 are integers.

Thus, $\quad 2u = 2m_0 b + 2m_1 i + 2m_2 j + 2m_3 k$

$$= (m_0 + m_0 i + m_0 j + m_0 k) + 2m_1 i + 2m_2 j + 2m_3 k$$

$$= m_0 + (2m_1 + m_0)\, i + (2m_2 + m_0)\, j + (2m_3 + m_0)\, k.$$

Therefore, $N(2u) = m_0^2 + (2m_1 + m_0)^2 + (2m_2 + m_0)^2 + (2m_3 + m_0)^2$.

But $N(2u) = N(2)N(u) = 4P$.

since $N(8) = 4$ and $N(4) = P$. we have shown that

$$4p = m_0^2 + (2m_1 + m_0)^2 + (2m_2 + m_0)^2 + (2m_3 + m_0)^2$$

We are almost done. To finish the proof we introduce an old trick of Euler's:

If $2a = x_0^2 + x_1^2 + x_2^2 + x_3^2$ where a, x_0, x_1, x_2 and x_3 are integers.

Then $a = y_0^2 + y_1^2 + y_2^2 + y_3^2$ for some integers y_0, y_1, y_2, y_3

Since $2a$ is even, the x 's are all even, all odd or two are even and two are odd.

At any rate in all three cases we can renumber the $x's$ and pair them in such a way that

$$y_0 = \frac{x_0 + x_1}{2}, y_1 = \frac{x_0 - x_1}{2}, y_2 = \frac{x_2 + x_3}{2}$$

and $y_3 = \frac{x_2 - x_3}{2}$ are all integers.

But, $y_0^2 + y_1^2 + y_2^2 + y_3^2 = \left(\frac{x_0+x_1}{2}\right)^2 + \left(\frac{x_0-x_1}{2}\right)^2 + \left(\frac{x_2+x_3}{2}\right)^2$

$$\begin{aligned} &= \frac{1}{2}\left(x_0^2 + x_1^2 + x_2^2 + x_3^2\right) \\ &= \frac{1}{2}(2a) \\ &= a \end{aligned}$$

since $4p$ is a sum of four squares, by the remark just made $2p$ also is:

Since $2p$ is a sum of four squares, p also must be such a sum.

Thus $p = a_0^2 + a_1^2 + a_2^2 + a_3^2$ for some integers a_0, a_1, a_2, a_3 and Lagrange's theorem is established. □

Let us sum up:

- Adjoint.and Norm.
- Lagrange Identity.
- Left Division Algorithm.
- Left and right Ideal.

Check your progress

1. If $a \in H$ the $a^{-1} \in H$ if and only if —
2. Which form of the primes numbers can be expressed the sum of two squares ?

Unit Summary:

In this unit, we discussed the splitting field of polynomial over F and the solvable by radicals over F. Further, we proved the Frobenius theorem and Four-square theorem.

Glossary:

- Solvable and commutator
- S_n is not solvable for $n \geq 5$.
- Only irreducible polynomials over the field of real numbers are of degree 1 or 2.
- The Frobenius theorem.
- $N(x) = xx^*$
- $Q = \{x \in Q/x = \alpha_0+\alpha_1 i+\alpha_2 j+\alpha_3 k,\ and\ x^* = \alpha_0-\alpha_1 i-\alpha_2 j-\alpha_3 k.\}$
- Four square theorem.

Self Assessment questions

1. Let D be a division ring algebraic over F, the field of real numbers. Then prove D is isomorphic to one of: the field of real numbers, the field of complex numbers, or the division ring of real quaternions.

2. Prove that if $a \in H$ then $a^{-1} \in H$ if and only if $N((a) = 1$.

3. Let $G = S_n$, where $n \geq 5$; then $G^{(k)}$ for $k = 1, 2, 3, ...$ contains every 3-cycle of S_n.

4. The general polynomial of degree $n \geq 5$ is not solvable by radicals.

Exercises

1. Every positive integer can be expressed as the sum of squares of four integers.

2. Prove that subgroup of a solvable group is solvable.

3. If A is a ring algebraic over a field F and A has no zero divisors prove that A is a division ring.

4. Exhibit an infinite number f positive integers which cannot be written as the sum of three squares.

Answers for check your progress

Section 5.1

1. $D = C$

2. -1

Section 5.2

1. $n \geq 5$

2. 2

Section 5.3

1. $N(a) = 1$

2. $4n + 1$

References:

1. I.N. Herstein, Topics in Algebra (II Edition) Wiley Eastern Limited, New Delhi, 1975.

Suggested Reading:

1. M. Artin, Algebra, Prentice Hall of India, 1991.

2. P.B. Bhattacharya, S.K. Jain, and S.R. Nagpaul, Basic Abstract Algebra (II Edition) Cambridge University Press, 1997. (Indian Edition)

3. I.S. Luther and I.B.S. Passi, Algebra, Vol. I âĂŞGroups(1996); Vol. II Rings, Narosa Publishing House , New Delhi, 1999

4. D.S. Malik, J.N. Mordeson and M.K. Sen, Fundamental of Abstract Algebra, McGraw Hill (International Edition), New York. 1997.

5. N. Jacobson, Basic Algebra, Vol. I & II Hindustan Publishing Company, New Delhi.