DIRECTORATE OF DISTANCE EDUCATION

UNIVERSITY OF NORTH BENGAL

MASTER OF SCIENCES- MATHEMATICS

SEMESTER -IV

FIELD EXTENSION AND GALOIS THEORY

DEMATH4ELEC5

BLOCK-1

UNIVERSITY OF NORTH BENGAL

Postal Address:
The Registrar,
University of North Bengal,
Raja Rammohunpur,
P.O.-N.B.U.,Dist-Darjeeling,
West Bengal, Pin-734013,
India.
Phone: (O) +91 0353-2776331/2699008
Fax:(0353) 2776313, 2699001
Email: regnbu@sancharnet.in ; regnbu@nbu.ac.in
Wesbsite: www.nbu.ac.in

First Published in 2019

FOREWORD

The Self Learning Material (SLM) is written with the aim of providing simple and organized study content to all the learners. The SLMs are prepared on the framework of being mutually cohesive, internally consistent and structured as per the university's syllabi. It is a humble attempt to give glimpses of the various approaches and dimensions to the topic of study and to kindle the learner's interest to the subject

We have tried to put together information from various sources into this book that has been written in an engaging style with interesting and relevant examples. It introduces you to the insights of subject concepts and theories and presents them in a way that is easy to understand and comprehend.

We always believe in continuous improvement and would periodically update the content in the very interest of the learners. It may be added that despite enormous efforts and coordination, there is every possibility for some omission or inadequacy in few areas or topics, which would definitely be rectified in future.

We hope you enjoy learning from this book and the experience truly enrich your learning and help you to advance in your career and future endeavours.

FIELD EXTENSION AND GALOIS THEORY

BLOCK-1

BLOCK -2

BLOCK-1 FIELD EXTENSION AND GALOIS THEORY

In mathematics, **Galois theory** provides a connection between field theory and group theory. Using Galois theory, certain problems in field theory can be reduced to group theory, which is in some sense simpler and better understood. It has been used to solve classic problems including showing that two problems of antiquity cannot be solved as they were stated (doubling the cube and trisecting the angle; a third problem of antiquity, squaring the circle, is also unsolvable, but this is shown by other methods); showing that there is no quintic formula; and showing which polygons are constructible.

The subject is named after Évariste Galois, who introduced it for studying the roots of a polynomial and characterizing the polynomial equations that are **solvable by radicals** in terms of properties of the permutation group of their roots—an equation is *solvable by radicals* if its roots may be expressed by a formula involving only integers, *n*th roots, and the four basic arithmetic operations.

The theory has been popularized among mathematicians and developed by Richard Dedekind, Leopold Kronecker, Emil Artin, and others who interpreted the permutation group of the roots as the automorphism group of a field extension.

Galois theory has been generalized to Galois connections and Grothendieck's Galois theory.

UNIT-1 INTRODUCTION TO THE FIELD THEORY I

STRUCTURE

1.0 OBJECTIVES

Understand the concept of Rings

Understand the concept of Fields

Enumerate the polynomial rings

Understand the concept of Factoring polynomials

Enumerate the Extension fields

Understand the Construction of some extension fields

1.1 INTRODUCTION

Galois Theory uncovers a relationship between the structure of groups and the structure of fields. It then uses this relationship to describe how the roots of a polynomial relate to one another.

1.2 RINGS

A ***ring*** is a set R with two binary operations + and – such that
(a) (R, +) / is a commutative group;
(b) · is associative, and there exists an element 1R such that a $a \cdot 1_R = a = 1_{R \cdot a}$ for all a ∈ R;
(c) the distributive law holds: for all a,b,c ∈ R,

$$(a + b) \cdot c = a \cdot c + b \cdot c$$

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

We usually omit "." and write 1 for 1_R when this causes no confusion. If $1_R = 0$, then R = {0}.

A ***subring*** of a ring R is a subset S that contains 1_R and is closed under addition, passage to the negative, and multiplication. It inherits the structure of a ring from that on R.
A **homomorphism of rings** α: R→ R' is a map such that

$$\alpha(a+b) = \alpha(a) + \alpha(b), \quad \alpha(ab) = \alpha(a)\alpha(b), \quad \alpha(1_R) = 1_{R'}$$

for all a;b ∈ R. A ring R is said to be ***commutative*** if multiplication is commutative:

$$ab = ba \text{ for all } a, b \in R.$$

A commutative ring is said to be an ***integral domain*** if $1_R \neq 0$ and the cancellation law holds for multiplication:

$$ab = ac, a \neq 0, \text{ implies } b = c.$$

An ***ideal*** I in a commutative ring R is a subgroup of (R,C) that is closed under multiplication by elements of R:

$$r \in R, a \in I, \text{ implies } ra \in I.$$

The ideal generated by elements $a_1, \ldots, a_n$ is denoted by $(a_1, \ldots, a_n)$. For example, (a) is the principal ideal aR.

For example, in Z (more generally, any Euclidean domain) an ideal I is generated by any “smallest” nonzero element of I , and unique factorization into powers of prime elements holds.

1.3 FIELDS

A ***field*** is a set F with two composition laws C and such that

(a) (F, +) is a commutative group;

(b) $(F^{\times}, \cdot)$ where $F^{\times}$ = F \{0}, is a commutative group;

(c) the distributive law holds.

Thus, a field is a nonzero commutative ring such that every nonzero element has an inverse. In particular, it is an integral domain. A field contains at least two distinct elements, 0 and 1. The smallest, and one of the most important, fields is $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z} = \{0;1\}$.

A ***subfield*** S of a field F is a subring that is closed under passage to the inverse. It inherits the structure of a field from that on F .

LEMMA: *A nonzero commutative ring* R *is a field if and only if it has no ideals other than* (0) *and* R.

PROOF. Suppose that R is a field, and let I be a nonzero ideal in R. If a is a nonzero element of I , then 1 = a^{-1} a ∈ I , and so I = R. Conversely, suppose that R is a commutative ring with no proper nonzero ideals. If a ≠ 0, then (a) = R, and so there exists a b in R such that ab = 1.

EXAMPLE: The following are fields: $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p =$ ℤ/pℤ, (p prime).

A homomorphism of fields is simply a homomorphism of rings. Such a homomorphism is always injective, because its kernel is a proper ideal (it doesn’t contain 1), which must therefore be zero.

Let F be a field. An F -algebra (or algebra over F) is a ring R containing F as a subring (so the inclusion map is a homomorphism). A homomorphism of F -algebras α: R→R' is a homomorphism of rings such that α(c) = c for every c ∈ F .

1.3.1The characteristic of a field:

One checks easily that the map:

$$\mathbb{Z} \to F, \quad n \mapsto n \cdot 1_F \overset{\text{def}}{=} 1_F + 1_F + \cdots + 1_F \quad (n \text{ copies of } 1_F),$$

is a homomorphism of rings. For example,

$$\underbrace{(1_F + \cdots + 1_F)}_{m} + \underbrace{(1_F + \cdots + 1_F)}_{n} = \underbrace{1_F + \cdots + 1_F}_{m+n}$$

because of the associativity of addition. Therefore its kernel is an ideal in ℤ.

CASE 1: The kernel of the map is (0), so that

$$n \cdot 1_F = 0 \quad (\text{in } R) \implies n = 0 \quad (\text{in } \mathbb{Z}).$$

Nonzero integers map to invertible elements of F under $n \mapsto n \cdot 1_F \colon \mathbb{Z} \to F$, and so this map extends to a homomorphism

$$\frac{m}{n} \mapsto (m \cdot 1_F)(n \cdot 1_F)^{-1}: \mathbb{Q} \hookrightarrow F.$$

Thus, in this case, F contains a copy of ℚ, and we say that it has ***characteristic zero***.

CASE 2: The kernel of the map is ≠ (0), so that n ·1_F = 0 for some n ≠ 0. The smallest positive such n will be a prime p (otherwise there will be two nonzero elements in F whose product is zero), and p generates the kernel. Thus, the map $n \longmapsto n \cdot 1_F: \mathbb{Z} \to F$ defines an isomorphism from ℤ/pℤ onto the subring

$$\{m \cdot 1_F \mid m \in \mathbb{Z}\}$$

of F . In this case, F contains a copy of 𝔽p, and we say that it has ***characteristic*** p.

The fields $\mathbb{F}_2$, $\mathbb{F}_3$, $\mathbb{F}_5$,…,ℚ are called the ***prime fields.*** Every field contains a copy of exactly one of them.

REMARK: The usual proof by induction shows that the binomial theorem

$$(a+b)^m = a^m + \binom{m}{1}a^{m-1}b + \binom{m}{2}a^{m-2}b^2 + \cdots + b^m$$

holds in any commutative ring. If p is prime, then p divides p rn for all r with$1 \leq r \leq p^n - 1$. Therefore, when F has characteristic p

$$(a+b)^{p^n} = a^{p^n} + b^{p^n} \text{ all } n \geq 1,$$

and so the map $a \mapsto a^p: F \longrightarrow F$is a homomorphism. It is called the ***Frobenius endomorphism*** of F. When F is finite, the Frobenius endomorphism is an automorphism.

Check your Progress-1

1. Define ring

2. Explain Field

1.4 REVIEW OF POLYNOMIAL RINGS

Let F be a field.

The ring F [X] of polynomials in the symbol (or “indeterminate” or “variable”) X with coefficients in F is an F -vector space with basis 1, X, . . . , X^n, . . . , and with the multiplication

$$\left(\sum_i a_i X^i\right)\left(\sum_j b_j X^j\right) = \sum_k \left(\sum_{i+j=k} a_i b_j\right) X^k.$$

The F -algebra F [X] has the following universal property: for any F - algebra R and element *r* of R, there is a unique homomorphism of F - algebras $\alpha: F[X] \to R$ such that α(X) = r

Division algorithm: given f (X), g(X) ∈ F [X] with g ≠ 0, there exist q(X), r(X) ∈ F [X] • with r = 0 or deg(r)< deg(g) such that

$$f = gq + r$$

moreover, q(X) and r(X) are uniquely determined. Thus F [X] is a Euclidean domain with deg as norm, and so it is a unique factorization domain.

Let f ∈ F [X]be no constant, and let a ∈ F . The division algorithm shows that

$$f = (X - a)q + c$$

with q ∈ F [X] and c ∈ F . Therefore, if a is a root of f (that is, f (a) = 0), then X – a divides f . From unique factorization, it now follows that f has at most deg(f) roots

Euclid's algorithm: Let f (X), g(X) ∈ F [X]. Euclid's algorithm constructs polynomials a(X), b(X), and d(X)such that

$$a(X)\cdot f(X)+b(X)\cdot g(X)=d(X), \quad \deg(a)<\deg(g), \quad \deg(b)<\deg(f)$$

and d(X) = gcd(f,g)

Recall how it goes. We may assume that deg (f)≥ deg(g) since the argument is the same in the opposite case. Using the division algorithm, we construct a sequence of quotients and remainder

$$\begin{aligned} f &= q_0 g + r_0 \\ g &= q_1 r_0 + r_1 \\ r_0 &= q_2 r_1 + r_2 \\ &\cdots \\ r_{n-2} &= q_n r_{n-1} + r_n \\ r_{n-1} &= q_{n+1} r_n \end{aligned}$$

with r_n the last nonzero remainder. Then, r_n divides r_{n-1} hence g, and hence *f* . Moreover,

$$r_n = r_{n-2} - q_n r_{n-1} = r_{n-2} - q_n(r_{n-3} - q_{n-1} r_{n-2}) = \cdots = af + bg$$

and so every common divisor of *f* and g divides r_n: we have shown r_n = gcd(f,g). Let af + bg = d. If deg(a) ≥ deg(g), write a = gq + r with deg(r) < deg (g); then

$$rf + (b + qf)g = d,$$

and b + qf automatically has degree < deg(f).

PARI knows how to do Euclidean division: typing divrem (13,5) in PARI returns [2;3], meaning that 13 = 2 × 5+ 3, and gcd(m,n) returns the greatest common divisor of m and n.

Let I be a nonzero ideal in F [X], and let f be a nonzero polynomial of least degree in I ; then I = (f) (because F [X] is a Euclidean domain).

When we choose *f* to be ***monic***, i.e., to have leading coefficient one, it is uniquely determined by I. Thus, there is a one-to-one correspondence between the nonzero ideals of F [X] and the monic polynomials in F [X]. The prime ideals correspond to the irreducible monic polynomials.

As F [X] is an integral domain, we can form its field of fractions F(X). Its elements are quotients *f* /*g*, *f* and *g* polynomials, $g \neq 0$

1.5 FACTORING POLYNOMIALS

The following results help in deciding whether a polynomial is reducible, and in finding its factors.

PROPOSITION: *Let* r ∈ ℚ *be a root of a polynomial*

$$a_m X^m + a_{m-1} X^{m-1} + \cdots + a_0, \quad a_i \in \mathbb{Z},$$

and write r = c/d, c,d ∈ Z, gcd(c; d) = 1. *Then* $c|a_0$ *and* $d|a_m$:

PROOF. It is clear from the equation

$$a_m c^m + a_{m-1} c^{m-1} d + \cdots + a_0 d^m = 0$$

that $d|a_m c^m$, and therefore, $d|a_m$: Similarly, $c|a_0$.

EXAMPLE: The polynomial f (X) = $X^3 - 3X - 1$ is irreducible in Q[X] because its only possible roots are ±1, and f (1) ≠ 0 ≠ f (– 1).

PROPOSITION (GAUSS'S LEMMA): Let f (X) ∈ Z[X]. If f (X) factors nontrivially in Q[X], then it factors nontrivially in Z[X].

PROOF. Let f = gh in ℚ[X] with g; h nonconstant. For suitable integers m and n, $g_1 \overset{def}{===}$ mg and $h_1 \overset{def}{===}$ nh have coefficients in ℤ, and so we have a factorization

$$mnf = g_1 \cdot h_1 \text{ in } \mathbb{Z}[X].$$

If a prime p divides mn, then, looking modulo p, we obtain an equation

$$0 = \overline{g_1} \cdot \overline{h_1} \text{ in } \mathbb{F}_p[X].$$

Since $\mathbb{F}_p$ [X] is an integral domain, this implies that p divides all the coefficients of at least one of the polynomials g_1; h_1, say g_1, so that g_1 = pg_2 for some $g_2 \in$ Z[X]. Thus, we have a factorization.

$$(mn/p)f = g_2 \cdot h_1 \text{ in } \mathbb{Z}[X].$$

Continuing in this fashion, we eventually remove all the prime factors of m, n, and so obtain a nontrivial factorization of f in Z[X]

PROPOSITION If f ∈ Z[X] is monic, then every monic factor of f in ℚ[X] lies in Z[X].

PROOF. Let g be a monic factor of f in Q[X], so that f = gh with h ∈ ℚ[X] also monic. Let m; n be the positive integers with the fewest prime factors such that mg, nh ∈ ℤ[X]. As in the proof of Gauss's Lemma, if a prime p divides m,n, then it divides all the coefficients of at least one of the polynomials mg, nh, say mg, in which case it divides m because g is monic. Now m/ p g ∈ ℤ[X], which contradicts the definition of m.

PROPOSITION (EISENSTEIN'S CRITERION): *Let*

$$f = a_m X^m + a_{m-1} X^{m-1} + \cdots + a_0, \quad a_i \in \mathbb{Z};$$

suppose that there is a prime p such that:

p does not divide a_m,

p *divides* a_{m-1},..., a_0

p^2 *does not divide* a_0.

Then f *is irreducible in* ℚ[X].

PROOF. If f(X) factors nontrivially in Q[X], then it factors nontrivially in ℤ[X], say,

$$a_m X^m + a_{m-1} X^{m-1} + \cdots + a_0 = (b_r X^r + \cdots + b_0)(c_s X^s + \cdots + c_0)$$

with bi,ci ∈ ℤ and r,s < m. Since p, but not p^2, divides $a_0 = b_0 c_0$, p must divide exactly one of b_0, c_0, say, b_0. Now from the equation

$$a_1 = b_0 c_1 + b_1 c_0,$$

we see that $p|b_1$; and from the equation

$$a_2 = b_0 c_2 + b_1 c_1 + b_2 c_0,$$

that $p|b_2$. By continuing in this way, we find that p divides $b_0;b_1\ldots$,br, which contradicts the condition that p does not divide a_m.
The last three propositions hold *mutatis mutandis* with Z replaced by a unique factorization domain R (replace Q with the field of fractions of R and p with a prime element of R).

REMARK : There is an algorithm for factoring a polynomial in ℚ[X]. To see this, consider f ∈ ℚ[X]. Multiply f (X)by a rational number so that it is monic, and then replace it by $D^{\deg(f)}$ f (X/D) with D equal to a common denominator for the coefficients of *f* , to obtain a monic polynomial with integer coefficients. Thus we need consider only polynomials.

$$f(X) = X^m + a_1 X^{m-1} + \cdots + a_m, \quad a_i \in \mathbb{Z}.$$

From the fundamental theorem of algebra, we know that *f* splits completely in ℂ[X] •

$$f(X) = \prod_{i=1}^{m} (X - \alpha_i), \quad \alpha_i \in \mathbb{C}.$$

From the equation

$$0 = f(\alpha_i) = \alpha_i^m + a_1\alpha_i^{m-1} + \cdots + a_m,$$

it follows that $|\alpha_i|$ is less than some bound depending only on the degree and coefficients of f ; in fact,

$$|\alpha_i| \leq \max\{1, mB\},\ B = \max|a_i|.$$

Now if g(X) is a monic factor of f (X), then its roots in ℂ are certain of the α_i, and its coefficients are symmetric polynomials in its roots. Therefore, the absolute values of the coefficients of g(X) are bounded in terms of the degree and coefficients of f. Since they are also integers we see that there are only finitely many possibilities for g(X). Thus, to find the factors of f (X) we (better PARI) have to do only a finite amount of checking

1.6 EXTENSION FIELDS

A field E containing a field F is called an ***extension field*** of F (or simply an ***extension*** of F , and we speak of an extension E/F). Such an E can be regarded as an F -vector space.

The dimension of E as an F -vector space is called the ***degree*** of E over F , and is denote by [E:F]. We say that E is ***finite*** over F when it has finite degree over F.

When E and E' are extension fields of F , an F -***homomorphism*** E → E' is a homomorphism φ:E→E' such that φ (c) = c for all c ∈ F .

EXAMPLE: (a) The field of complex numbers ℂ has degree 2 over R (basis {1;i})

(b) The field of real numbers R has infinite degree over ℚ: the field ℚ is countable, and so every finite-dimensional ℚ -vector space is also countable, but a famous argument of Cantor shows that R is not countable.

(c) The field of ***Gaussian numbers***

$$\mathbb{Q}(i) \overset{\text{def}}{=} \{a + bi \in \mathbb{C} \mid a, b \in \mathbb{Q}\}$$

has degree 2 over $\mathbb{Q}$ (basis {1;i}).

(d) The field F.X/ has infinite degree over F ; in fact, even its subspace F[X] has infinite dimension over F (basis 1,X,X^2;…).

PROPOSITION (MULTIPLICATIVITY OF DEGREES) *Consider fields* L ⊃ E ⊃ F. *Then* L=F *is of finite degree if and only if* L=E *and* E=F *are both of finite degree, in which case*

$$[L: F] = [L: E][E: F].$$

PROOF. If L is finite over F , then it is certainly finite over E; moreover, E, being a subspace of a finite-dimensional F -vector space, is also finite-dimensional. Thus, assume that L/E and E/F are of finite degree, and let $(e_i)_{1\leq i\leq m}$ be a basis for E as an F -vector space and let $(l_j)_{1\leq j\leq n}$ be a basis for L as an E-vector space. To complete the proof of the proposition, it suffices to show that $(e_i l_j)_{1\leq i\leq m, 1\leq j\leq n}$ is a basis for L over F , because then L will be finite over F of the predicted degree.

First, $(e_i\, l_j)_{i, j}$ spans L. Let γ ∈ L. Then, because $(l_j)_j$ spans L as an E-vector space,

$$\gamma = \textstyle\sum_j \alpha_j l_j, \qquad \text{some } \alpha_j \in E,$$

and because $(e_i)_i$ spans E as an F -vector space,

$$\alpha_j = \textstyle\sum_i a_{ij} e_i, \qquad \text{some } a_{ij} \in F.$$

On putting these together, we find that

$$\gamma = \textstyle\sum_{i,j} a_{ij} e_i l_j.$$

Second, $(e_i\, l_j)_{i,\, j}$ is linearly independent. A linear relation $\sum a_{ij} e_i l_j = 0$, $a_{ij} \in F$, can be rewritten $\sum_j (\sum_i a_{ij} e_i)\, l_j = 0$. The linear independence of the l_j 's now shows that $\sum_i a_{ij} e_i = 0$ for each j , and the linear independence of the e_i's shows that each $a_{ij} = 0$

1.6.1 The subring generated by a subset:

An intersection of subrings of a ring is again a ring (this is easy to prove). Let F be a subfield of a field E, and let S be a subset of E. The intersection of all the subrings of E containing F and S is obviously the smallest subring of E containing both F and S. We call it the subring of E ***generated by*** F ***and*** S (or ***generated over*** F ***by*** S), and we denote it by F[S].

When S = $\{\alpha_1, \ldots \alpha_n\}$we write $F[\alpha_1, \ldots \alpha_n]$ for F[S]. For example, $\mathbb{C} = \mathbb{R}[\sqrt{-1}]$.

LEMMA The ring F[S] consists of the elements of E that can be expressed as finite sums of the form

$$\sum a_{i_1 \cdots i_n} \alpha_1^{i_1} \cdots \alpha_n^{i_n}, \quad a_{i_1 \cdots i_n} \in F, \quad \alpha_i \in S, \quad i_j \in \mathbb{N}. \tag{1}$$

PROOF. Let R be the set of all such elements. Obviously, R is a subring of E containing F and S and contained in every other such subring. Therefore it equals F[S]. •

EXAMPLE The ring $\mathbb{Q}[\pi]$, π = 3:14159…, consists of the real numbers that can be expressed as a finite sum

$$a_0 + a_1\pi + a_2\pi^2 + \cdots + a_n\pi^n, \quad a_i \in \mathbb{Q}.$$

The ring $\mathbb{Q}[i]$, consists of the complex numbers of the form a + bi, a, b ∈ Q.

Note that the expression of an element in the form (1) will *not* be unique in general. This is so already in R[i].

LEMMA: Let R be an integral domain containing a subfield F (as a subring). If R is finite-dimensional when regarded as an F -vector space, then it is a field.

PROOF. Let α be a nonzero element of R — we have to show that ¿ has an inverse in R.
The map x ↦ α x : R→R is an injective linear map of finite-dimensional F -vector spaces, and is therefore surjective. In particular, there is an element β ∈ R such that ¿ αβ = 1.
Note that the lemma applies to the subrings containing F of an extension field E of F of finite degree.

1.6.2 The subfield generated by a subset

An intersection of subfields of a field is again a field. Let F be a subfield of a field E, and let S be a subset of E. The intersection of all the subfields of E containing F and S is obviously the smallest subfield of E containing both F and S. We call it the subfield of E ***generated by*** F ***and*** S (or ***generated over*** F ***by*** S), and we denote it F.S/. It is the field of fractions of F [S] in E because this is a subfield of E containing F and S and contained in every other such field. When S = {α_1,…α_n}, we write F(α_1,…α_n) for F(S). Thus, F[α_1,…α_n] consists of all elements of E that can be expressed as polynomials in the α_i with coefficients in F , and F(α_1,…α_n) consists of all elements of E that can be expressed as a quotient of two such polynomials.

Lemma shows that F [S] is already a field if it is finite-dimensional over F , in which case F(S) = F [S].

EXAMPLE: (a) The field $\mathbb{Q}[\pi]$, π = 3:14…, consists of the complex numbers that can be expressed as a quotient

$$g(\pi)/h(\pi), \quad g(X), h(X) \in \mathbb{Q}[X], \quad h(X) \neq 0.$$

(b) The ring $\mathbb{Q}[i]$ • is already a field.

An extension E of F is said to be ***simple*** if E = F(α)some α ∈ E. For example, $\mathbb{Q}[\pi]$, and $\mathbb{Q}[i]$are simple extensions of $\mathbb{Q}$.

Let F and F' be subfields of a field E. The intersection of the subfields of E containing both F and F' is obviously the smallest subfield of E containing both F and F'. We call it the ***composite*** of F and F' in E, and we denote it by F· F'. It can also be described as the subfield of E generated over F by F 0, or the subfield generated over F'by F :

$$F(F') = F \cdot F' = F'(F).$$

Check your Progress-2

3. Explain *Euclid's algorithm*.

____

____

____

4. Explain - The subfield generated by a subset

____

____

____

1.7 CONSTRUCTION OF SOME EXTENSION FIELDS

Let f (X) ∈ F [X] be a monic polynomial of degree m, and let (f) be the ideal generated by f . Consider the quotient ring F [X] /(f (X)), and write x for the image of X in

F [X] /(f (X)), i.e., x is the coset X + (f (X))/.

(a) The map

$$P(X) \mapsto P(x) \colon F[X] \to F[x]$$

is a homomorphism sending f (X) to 0. Therefore, f (x) = 0.

(b) The division algorithm shows that each element g of F [X] =(f) is represented by a unique polynomial r of degree < m. Hence each element of F [x] can be expressed uniquely as a sum

$$a_0 + a_1 x + \cdots + a_{m-1} x^{m-1}, \qquad a_i \in F. \qquad (2)$$

(c) To add two elements, expressed in the form (2), simply add the corresponding coefficients.

(d) To multiply two elements expressed in the form (2), multiply in the usual way, and use the relation f (x) = 0 to express the monomials of degree ≥ m in x in terms of lower degree monomials.

(e) Now assume that f (X) is irreducible. Then every nonzero α ∈ F [x] has an inverse, which can be found as follows. Use (b) to write α = g(x) with g(X) a polynomial of degree ≤ m – 1, and use Euclid's algorithm in F [X] to obtain polynomials a(X) and b(X) such that

$$a(X)f(X) + b(X)g(X) = d(X)$$

with d(X)the gcd of f and g. In our case, d(X)is 1 because f (X) is irreducible and deg g(X) < deg f (X). When we replace X with x, the equality becomes

b(x) g(x) = 1

Hence b(x) is the inverse of g(x).

From these observations, we conclude:

For a monic irreducible polynomial f (X) of degree m in F [X] • ,is a field of degree m over F . Moreover, computations in F [x] • reduce to computations in F .

Note that, because F [x] is a field, F(x) = F [x] •

1.8 LET US SUM UP

We have studied the basic concepts that are involved in Field Extension and Galois Theory.

1.9 KEYWORDS

Subset : A set A is a **subset** of another set B if all elements of the set A are elements of the set B.

Inherits - to take or receive

Commutative ring is a **ring** in which the multiplication operation is **commutative**

1.10 QUESTIONS FOR REVIEW

1. Let E = ℚ[α], where α^3- α^2+ α+ 2 = 0. Express (α^2+ α +1)(α^2 – 1) and (α – 1) $^{-1}$ in the form a α^2+b α +c with a,b,c ∈ Q.

2. Let F be a field, and let f (X) ∈ F [X].

(a) For every a ∈ F , show that there is a polynomial q(X) ∈ F [X] such that

f (X) = q(X)(X – a)+ f (a)

(b) Deduce that f (a) = 0 if and only if (X – a)|f (X).

(c) Deduce that f (X) can have at most deg *f* roots.

1.11 SUGGESTED READINGS AND REFERENCES

1. M. Artin, Algebra, Perentice -Hall of India, 1991.
2. P.M. Cohn, Algebra, vols, I,II, & III, John Wiley & Sons, 1982, 1989, 1991.
3. N. Jacobson, Basic Algebra, vols. I & II, W. H. Freeman, 1980 (also published by Hindustan Publishing Company)
4. S. Lang. Algebra, 3rd edn. Addison-Weslley, 1993.
5. I.S. Luther and I.B.S. Passi, Algebra, Vol.III-Modules, Narosa Publishing House.

6. D. S. Malik, J. N. Modrdeson, and M. K. Sen, Fundamentals of Abstract Algebra, McGraw-Hill, International Edition, 1997.
7. VivekSahai and VikasBist, Algebra, Narosa Publishing House, 1999
8. I. Stweart, Galois Theory, 2nd edition, Chapman and Hall, 1989.
9. J.P. Escofier, Galois theory, GTM Vol.204, Springer, 2001.

1.12 ANSWERS TO CHECK YOUR PROGRESS

1. Provide the definition – 1.2

2. Provide explanation – 1.3

3. Provide explanation – 1.4

4. Provide explanation – 1.6.2

UNIT-2 INTRODUCTION TO THE FIELD THEORY II

STRUCTURE

2.0 OBJECTIVES

Understand the concept of Stem fields.

Understand the concept of Algebraic and transcendental elements

Enumerate Constructions with straight-edge and compass

Understand the concept of Algebraically closed fields

2.1 INTRODUCTION

There are two problems which provide some motivation for studying Galois theory - the existence of polynomials which aren't soluble by radicals, and some results about classical Euclidean geometry, for example that you cannot trisect an angle using a ruler and compass, and that certain regular polygons cannot be constructed using a ruler and compass.

2.2 STEM FIELDS

Let *f* be a monic irreducible polynomial in F [X]. A pair (E, α) consisting of an extension E of F and an α ∈ E is called a ***stem field for*** *f* if E = F[α] and f (α) = 0. For example, the pair (E, α) with E = F [X] /(f) = F [x] • and α = x is a stem field for f . Let (E, α) be a stem field, and consider the surjective homomorphism of F –algebras

$$g(X) \mapsto g(\alpha): F[X] \to E.$$

Its kernel is generated by a nonzero monic polynomial, which divides f , and so must equal it. Therefore the homomorphism defines an F –isomorphism

$$x \mapsto \alpha: F[x] \to E, \quad F[x] \overset{\text{def}}{=} F[X]/(f).$$

In other words, the stem field (E, α) of f is F -isomorphic to the standard stem field (F [X])/(f),x). It follows that every element of a stem field (E, α) for f can be written uniquely in the form

$$a_0 + a_1\alpha + \cdots + a_{m-1}\alpha^{m-1}, \quad a_i \in F, \quad m = \deg(f),$$

and that arithmetic in F [α] can be performed using the same rules as in F [x]. If (E', α') is a second stem field for f, then there is a unique F -isomorphism E → E' sending α to α'. We sometimes abbreviate “stem field (F [α], α)” to “stem field F [α] ”.

2.3 ALGEBRAIC AND TRANSCENDENTAL ELEMENTS

For a field F and an element α of an extension field E, we have a homomorphism

$$f(X) \mapsto f(\alpha): F[X] \to E.$$

There are two possibilities.

CASE 1: The kernel of the map is (0), so that, for f ∈ F [X],

$$f(\alpha) = 0 \implies f = 0 \text{ (in } F[X]).$$

In this case, we say that α ***transcendental over*** F. The homomorphism X ↦α : F[X] → F[α] is an isomorphism, and it extends to an isomorphism F(X) → F(α) on the fields of fractions.

CASE 2: The kernel is ≠ (0), so that g(α) = 0 for some nonzero g ∈ F [X]. In this case, we say that α is ***algebraic over*** F. The polynomials *g* such that g(α) =0 form a nonzero ideal in F [X], which is generated by the monic polynomial *f* of least degree such f (α) = 0. We call *f* the ***minimum (or minimal) polynomial*** of α over F. It is irreducible, because otherwise there would be two nonzero elements of E whose product is zero. The minimum polynomial is characterized as an element of F[X] by each of the following conditions:

- f is monic, f(α) = 0, and *f* divides every other g in F [X]such that g(α) = 0;
- f is the monic polynomial of least degree such that f (α) = 0;
- f is monic, irreducible, and f (α) = 0.

Note that g(X) ↦ g(α) defines an isomorphism F [X] /(f) → F[α]. Since the first is a field, so also is the second:

$$F(\alpha) = F[\alpha]$$

Thus, F[α] is a stem field for f .

EXAMPLE: Let α ∈ ℂ be such that $\alpha^3 - 3\alpha - 1 = 0$. Then $X^3 - 3X - 1$ is monic, irreducible, and has α as a root, and so it is the minimum polynomial of α over ℚ. The set $\{1, \alpha, \alpha^2\}$ is a basis for ℚ[α] over ℚ.

REMARK : PARI knows how to compute in Q[α]. For example, factor(X^4+4) returns the factorization

$$X^4 + 4 = (X^2 - 2X + 2)(X^2 + 2X + 2)$$

in ℚ[X] . Now type nf = nfinit(a^2+2*a+2) to define a number field “nf” generated over ℚ by a root a of X^2+2X+2. Then nf factor(nf, x^4+4) returns the factorization

$$X^4 + 4 = (X - a - 2)(X - a)(X + a))(X + a + 2),$$

in ℚ[a] .

A extension E/F of fields is said to be ***algebraic*** (and E is said to be ***algebraic over*** F), if all elements of E are algebraic over F ; otherwise it is said to be ***transcendental*** (and E is said to be ***transcendental over*** F). Thus, E/F is transcendental if at least one element of E is transcendental over F.

PROPOSITION : *Let* E ⊃ F *be fields. If* E/F *is finite, then* E *is algebraic and finitely generated (as a field) over* F *; conversely, if* E *is generated over* F *by a finite set of algebraic elements, then it is finite over* F .

PROOF. ⟹To say that α is transcendental over F amounts to saying that its powers $1, \alpha, \alpha^2, \ldots$ are linearly independent over F . Therefore, if E is finite over F, then it is algebraic over F. It remains to show that E is finitely generated over F. If E = F, then it is generated by the empty set. Otherwise, there exists an α_1 ∈ E XF . If E ≠ F Œ¸ 1 • , there exists an ¸2 2 E \ F [α_1] , and so on. Since

$$[F[\alpha_1]: F] < [F[\alpha_1, \alpha_2]: F] < \cdots < [E: F]$$

this process terminates with E = F [α_1,α_2,…].

⇐: Let E = F(α_1,…, α_n).with α_1,α_2,… α_n algebraic over F . The extension F(α_1) / F is finite because α_1 is algebraic over F, and the extension F(α_1, α_2) / F(α_1) is finite because $\alpha_2$is algebraic over F and hence over F(α_1) Thus, F(α_1, α_2)is finite over F.

Now repeat the argument.

COROLLARY: *(a) If* E *is algebraic over* F *, then every subring* R *of* E *containing* F *is a field.*

(b) Consider fields L ⊃ E ⊃ F. *If* L *is algebraic over* E *and* E *is algebraic over* F *, then* L *is algebraic over* F.

PROOF. (a) If α ∈ R, then F [α] ⊂ R. But F [α] is a field because α is algebraic and so R contains α_1.

(b) By assumption, every α ∈ L is a root of a monic polynomial

$$X^m + a_{m-1}X^{m-1} + \cdots + a_0 \in E[X].$$

Each of the extensions

$$F[a_0,\ldots,a_{m-1},\alpha] \supset F[a_0,\ldots,a_{m-1}] \supset F[a_0,\ldots,a_{m-2}] \supset \cdots \supset F$$

is generated by a single algebraic element, and so is finite. Therefore F [a_0,…,a_{m-1},α];, is finite over F which implies that α is algebraic over F .

2.3.1 Transcendental numbers :

A complex number is said to be algebraic or transcendental according as it is algebraic or transcendental over Q. First some history:

1844: Liouville showed that certain numbers, now called Liouville numbers, are transcendental.

1873: Hermite showed that e is transcendental.

1874: Cantor showed that the set of algebraic numbers is countable, but that R is not countable. Thus most numbers are transcendental (but it is usually very difficult to prove that any particular number is transcendental).

1882: Lindemann showed that is transcendental.

1934: Gel’fond and Schneider independently showed that α^{β} is transcendental if α and β are algebraic, $\alpha \neq 0{,}1$, and β ∉ Q. (This was the seventh of Hilbert’s famous problems.)

2018: Euler’s constant

$$\gamma \overset{\text{def}}{=} \lim_{n\to\infty}\left(\sum_{k=1}^{n} 1/k - \log n\right)$$

has not yet been proven to be transcendental or even irrational.

2018: The numbers e + π and e – π are surely transcendental, but again they have not even been proved to be irrational!

PROPOSITION: The set of algebraic numbers is countable.

PROOF. Define the height h(r) of a rational number to be max(|m|;|n|), where r = m/n is the expression of r in its lowest terms. There are only finitely many rational numbers with height less than a fixed number N . Let A(N) denote the set of algebraic numbers whose minimum equation over ℚ has degree ≤ N and has coefficients of height < N . Then A(N) is finite for each N . Choose a bijection from some segment [0,n(1)] of N onto A(10), extend it to a bijection from a segment [0,n(2)] onto A(100), and so on.

A typical Liouville number is

$$\sum_{n=0}^{\infty} \frac{1}{10^{n!}} \cdot$$

in its decimal expansion there are increasingly long strings of zeros. Since its decimal expansion is not periodic, the number is not rational. We prove that the analogue of this number in base 2 is transcendental.

THEOREM: *The number* $\alpha = \sum \frac{1}{2^{n!}}$ *is transcendental.*

PROOF: Suppose not, and let

$$f(X) = X^d + a_1 X^{d-1} + \cdots + a_d, \quad a_i \in \mathbb{Q},$$

be the minimum polynomial of α over ℚ. Thus [ℚ [α]:ℚ] = d. Choose a nonzero integer D such that D f (X) ∈ ℤ [X] • .

Let $\sum_N = \sum_{n=0}^{N} \frac{1}{2^{n!}}$, so that $\sum_N \to \alpha$ as N → ∞, and let $x_N = f(\sum_N)$. As α is not $(2^{N!})^d D x_N \in \mathbb{Z}$, rational, f (X), being irreducible of degree > 1, has no rational root. Since $\sum_N \neq \alpha$, it can't be a root of f (X), and so $x_N \neq 0$. Obviously, $x_N \in \mathbb{Q}$; in fact , and so

$$|(2^{N!})^d D x_N| \geq 1. \tag{3}$$

From the fundamental theorem of algebra (see 5.6 below), we know that f splits in ℂ[X] say,

$$f(X) = \prod_{i=1}^{d} (X - \alpha_i), \quad \alpha_i \in \mathbb{C}, \quad \alpha_1 = \alpha,$$

And so

$$|x_N| = \prod_{i=1}^{d} |\Sigma_N - \alpha_i| \leq |\Sigma_N - \alpha_1| (\Sigma_N + M)^{d-1}, \quad \text{where } M = \max_{i \neq 1}\{1, |\alpha_i|\}.$$

But

$$|\Sigma_N - \alpha_1| = \sum_{n=N+1}^{\infty} \frac{1}{2^{n!}} \leq \frac{1}{2^{(N+1)!}} \left(\sum_{n=0}^{\infty} \frac{1}{2^n} \right) = \frac{2}{2^{(N+1)!}}.$$

Hence

$$|x_N| \leq \frac{2}{2^{(N+1)!}} \cdot (\Sigma_N + M)^{d-1}$$

and

$$|(2^{N!})^d D x_N| \leq 2 \cdot \frac{2^{d \cdot N!} D}{2^{(N+1)!}} \cdot (\Sigma_N + M)^{d-1}$$

which tends to 0 as $N \to \infty$ because $\frac{2^{d \cdot N!}}{2^{(N+1)!}} = \left(\frac{2^d}{2^{N+1}}\right)^{N!} \to 0$. This contradicts (3).

Check your Progress-1

1. State the characters of the minimum polynomial.

____

____

____

2. Prove : *The number* $\alpha = \sum \frac{1}{2^{n!}}$ *is transcendental.*

____

____

____

2.4 CONSTRUCTIONS WITH STRAIGHT-EDGE AND COMPASS.

The Greeks understood integers and the rational numbers. They were surprised to find that the length of the diagonal of a square of side 1, namely, $\sqrt{2}$, is not rational. They thus realized that they needed to extend their number system. They then hoped that the “constructible” numbers would suffice. Suppose we are given a length, which we call 1, a straight-edge, and a compass (device for drawing circles). A real number (better a length) is ***constructible*** if it can be constructed by forming successive intersections of

- lines drawn through two points already constructed, and
- circles with centre a point already constructed and radius a constructed length.

This led them to three famous questions that they were unable to answer: is it possible to duplicate the cube, trisect an angle, or square the circle by straight-edge and compass constructions? We’ll see that the answer to all three is negative.

Let F be a subfield of R. For a positive a ∈ F , $\sqrt{a}$ denotes the positive square root of a in R. The F ***-plane*** is $F \times F \rightarrow \mathbb{R} \times \mathbb{R}$. We make the following definitions:

An F ***-line*** is a line in RR through two points in the F -plane. These are the lines given by equations

$$ax + by + c = 0, \quad a, b, c \in F.$$

An F ***-circle*** is a circle in RR with centre an F -point and radius an element of F . These are the circles given by equations

$$(x-a)^2 + (y-b)^2 = c^2, \quad a, b, c \in F.$$

2.4.1 LEMMA: *Let* L ≠ L' *be* F *-lines, and let* C ≠ C' *be* F *-circles.*

(a) L∩ L' = ∅ *or consists of a single* F *-point.*

(b) L∩ C = ∅ *or consists of one or two points in the* F [$\sqrt{e}$]*-plane, some* e ∈ F , e > 0.

(c) C ∩ C' = ∅ *or consists of one or two points in the* F [$\sqrt{e}$]- *plane, some* e ∈ F , e > 0.

PROOF. The points in the intersection are found by solving the simultaneous equations, and hence by solving (at worst) a quadratic equation with coefficients in F.

2.4.2 LEMMA : *(a) If* c *and* d *are constructible, then so also are* c + d, – c , cd, *and* c/d (d ≠ 0).

(b) If c > 0 *is constructible, then so also is* $\sqrt{c}$.

SKETCH OF PROOF. First show that it is possible to construct a line perpendicular to a given line through a given point, and then a line parallel to a given line through a given point.

Hence it is possible to construct a triangle similar to a given one on a side with given length.

By an astute choice of the triangles, one constructs cd and c^{-1}. For (b), draw a circle of radius c+1/ 2 and centre . (c+ ½, 0), and draw a vertical line through the point A = (1,0) to meet the circle at P . The length AP is $\sqrt{c}$.

2.4.3 THEOREM (a) The set of constructible numbers is a field.

(b) A number α is constructible if and only if it is contained in a subfield of R of the form

$$\mathbb{Q}[\sqrt{a_1},\ldots,\sqrt{a_r}], \quad a_i \in \mathbb{Q}[\sqrt{a_1},\ldots,\sqrt{a_{i-1}}], \quad a_i > 0.$$

PROOF. (a) This restates (a) of Lemma 2.4.2.

(b) It follows from Lemma 2.4.1 that every constructible number is contained in such a field $\mathbb{Q}$ $[\sqrt{a_1},\ldots,\sqrt{a_r}]$. Conversely, if all the elements of $\mathbb{Q}$ $[\sqrt{a_1},\ldots,\sqrt{a_{i-1}}]$. are constructible, then $\sqrt{a_i}$ is constructible (by 1.35b), and so all the elements of $[\sqrt{a_1},\ldots,\sqrt{a_i}]$ are constructible (by (a)). Applying this for i = 0;1,…, we find that all the elements of $\mathbb{Q}$ $[\sqrt{a_1},\ldots,\sqrt{a_r}]$ are constructible.

2.4.4 COROLLARY: *If* α *is constructible, then* α *is algebraic over* $\mathbb{Q}$*, and* $[\mathbb{Q}[\alpha]\colon \mathbb{Q}]$*is a powerof* 2.

PROOF. According to Proposition ŒQŒ‚ • WQ • divides

$$[\mathbb{Q}[\sqrt{a_1}]\cdots[\sqrt{a_r}]\colon\mathbb{Q}]$$

2.4.5 COROLLARY: *In general, it is impossible to trisect an angle by straight-edge and compass constructions.*

PROOF. Knowing an angle is equivalent to knowing the cosine of the angle. Therefore, to trisect 3α, we have to construct a solution to

$$\cos 3\alpha = 4\cos^3\alpha - 3\cos\alpha.$$

For example, take 3α = 60 degrees. As $\cos 60^0 = 1/2$, to construct ‚ α we have to solve $8x^3 – 6x –1 = 0$, which is irreducible and so $[\mathbb{Q}[\alpha]\colon \mathbb{Q}] = 3/$

2.4.6 COROLLARY: *It is impossible to square the circle by straight-edge and compass constructions.*

PROOF: A square with the same area as a circle of radius r has side $\sqrt{\pi r}$. Since is transcendental, so also is $\sqrt{\pi}$.

We next consider another problem that goes back to the ancient Greeks: list the integers n such that the regular n-sided polygon can be constructed using only straight-edge and compass. Here we consider the question for a prime p.

Note that $X^p -1$ is not irreducible; in fact

$$X^p - 1 = (X-1)(X^{p-1} + X^{p-2} + \cdots + 1).$$

2.4.7 LEMMA: *If* p *is prime, then* $X^{p-1} + \ldots + 1$ is irreducible; hence Q$[e^{2\pi i/p}]$ has degree p –1 over $\mathbb{Q}$.

PROOF.

Let

$$f(X) = (X^p - 1)/(X-1) = X^{p-1} + \cdots + 1; \text{ then}$$

$$f(X+1) = \frac{(X+1)^p - 1}{X} = X^{p-1} + \cdots + a_i X^i + \cdots + p,$$

with $a_i = \binom{p}{i+1}$. Now $p|a_i$ for i = 1,…,p – 2, and so f (X +1) is irreducible by Eisenstein's criterion. This implies that f (X) is irreducible. In order to construct a regular p-gon, p an odd prime, we need to construct

$$\cos\frac{2\pi}{p} = \frac{e^{\frac{2\pi i}{p}} + e^{-\frac{2\pi i}{p}}}{2}.$$

Note that

$$\mathbb{Q}[e^{\frac{2\pi i}{p}}] \supset \mathbb{Q}[\cos\tfrac{2\pi}{p}] \supset \mathbb{Q}.$$

The degree of $\mathbb{Q}[e^{\frac{2\pi i}{p}}]$ over $\mathbb{Q}[\cos\frac{2\pi}{p}]$ is 2 because the equation

$$\alpha^2 - 2\cos\tfrac{2\pi}{p}\cdot\alpha + 1 = 0, \quad \alpha = e^{\frac{2\pi i}{p}},$$

shows that it is at most 2, and it is not 1 because $e^{2\pi i/p}]\ \notin \mathbb{R}$. Hence

$$[\mathbb{Q}[\cos\tfrac{2\pi}{p}]:\mathbb{Q}] = \frac{p-1}{2}.$$

We deduce that, if the regular p-gon is constructible, then (p – 1)/ 2 is a power of 2; later we'll prove the converse statement. Thus, the regular p-gon is constructible if and only if p = 2^r + 1 for some positive integer r.

A number 2^r + 1 can be prime only if r is a power of 2: if t is odd, then

$$Y^t + 1 = (Y+1)(Y^{t-1} - Y^{t-2} + \cdots + 1)$$

And so

$$2^{st} + 1 = (2^s + 1)((2^s)^{t-1} - (2^s)^{t-2} + \cdots + 1).$$

We conclude that the primes p for which the regular p-gon is constructible are exactly those of the form 2^{2^r} + 1 for some r. Such p are called ***Fermat primes*** (because Fermat conjectured that all numbers of the form 2^{2^r} + 1 are prime). For r = 0,1,2,3,4, we have 2^{2^r} + 1 = 3,5,17,257,65537, which are indeed prime, but Euler showed that 2^{32} + 1 =(641)(6700417), and we don't know whether there are any more Fermat primes. Thus, we do not know the list of primes p for which the regular p-gon is constructible.

Gauss showed that

$$\cos\frac{2\pi}{17} = -\frac{1}{16} + \frac{1}{16}\sqrt{17} + \frac{1}{16}\sqrt{34 - 2\sqrt{17}} + \frac{1}{8}\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}}$$

when he was 18 years old. This success encouraged him to become a mathematician.

2.5 ALGEBRAICALLY CLOSED FIELDS

We say that a polynomial ***splits*** in F [X] (or, more loosely, in F) if it is a product of polynomials of degree 1 in F [X].

2.5.1 PROPOSITION *For a field Ω, the following statements are equivalent:*

(a) *Every nonconstant polynomial in Ω* [X] *splits in Ω* [X] .

(b) *Every nonconstant polynomial in Ω* [X] *has at least one root in* Ω*.*

(c) *The irreducible polynomials in Ω* [X] *are those of degree* 1.

(d) *Every field of finite degree over* Ω *equals* Ω*.*

PROOF. The implications (a)⇒(b)⇒(c) are obvious.

(c)⇒(a). This follows from the fact that *Ω* [X] is a unique factorization domain.

(c)⇒(d). Let E be a finite extension of Ω, and let α ∈ E. The minimum polynomial of α being irreducible, has degree 1, and so α ∈ Ω .

(d)⇒(c). Let *f* be an irreducible polynomial in Ω[X]. Then Ω[X]/ (f) is an extension field of Ω of degree deg(*f*) and so deg(*f*) = 1.

DEFINITION: (a) A field Ω is ***algebraically closed*** if it satisfies the equivalent statements of Proposition.

(b) A field Ω is an ***algebraic closure*** of a subfield F if it is algebraically closed and algebraic over F .

For example, the fundamental theorem of algebra says that $\mathbb{C}$ is algebraically closed. It is an algebraic closure of $\mathbb{R}$.

2.5.2 PROPOSITION : *If* Ω *is algebraic over* F *and every polynomial* f

∈ F [X] • *splits in* Ω[X], *then* Ω *is algebraically closed (hence an algebraic closure of* F *).*

PROOF. Let f be a non constant polynomial in Ω[X]. We have to show that f has a root in Ω. We know that *f* has a root α in some finite extension Ω' of Ω. Set

$$f = a_n X^n + \cdots + a_0, \quad a_i \in \Omega,$$

and consider the fields

$$F \subset F[a_0, \ldots, a_n] \subset F[a_0, \ldots, a_n, \alpha].$$

Each extension generated by a finite set of algebraic elements, and hence is finite. Therefore α lies in a finite extension of F and so is algebraic over F — it is a root of a polynomial *g* with coefficients in F. By assumption, g splits in Ω[X] and so the roots of g in Ω' all lie in Ω. In particular, α ∈ Ω.

2.5.3 PROPOSITION: *Let* Ω ⊃ F*; then*

{α ∈ Ω| α *algebraic over* F} *is a field.*

PROOF. If α and β are algebraic over F , then F [α, β] is a field of finite degree over F. Thus, every element of F [α, β] is algebraic over F . In particular, $\alpha \pm \beta$, α/β and αβ are algebraic over F .

The field constructed in the proposition is called the ***algebraic closure of*** F ***in*** Ω.

2.5.4 COROLLARY : *Let* Ω *be an algebraically closed field. For any subfield* F *of* Ω*, the algebraic closure of* F *in* Ω *is an algebraic closure of* F:

PROOF. From its definition, we see that it is algebraic over F and every polynomial in F [X] splits in it. Now Proposition 2.5.3 shows that it is an algebraic closure of F .

Thus, when we admit the fundamental theorem of algebra , every subfield of C has an algebraic closure (in fact, a canonical algebraic closure).

Check your Progress-2

3. Explain concept of ***constructible***

____

____

____

4. Discuss Algebraically closed fields

____

____

____

2.6 LET US SUM UP

We understood the concept of Stem fields, Algebraic and transcendental elements. We discussed Constructions with straight-edge and compass. We have discussed the concept of Algebraically closed fields

2.7 KEYWORDS

Irreducible polynomial: or prime polynomial is, roughly speaking, a non-constant polynomial that cannot be factored into the product of two non-constant polynomials.

Degree of Field: The **degree** may be **finite** or **infinite**, the field being called a **finite** extension or **infinite** extension accordingly.

Unique Factorization Domain. A **unique factorization** domain, called UFD for short, is any integral domain in which every nonzero noninvertible element has a **unique factorization**, i.e., an essentially **unique** decomposition as the product of **prime** elements or irreducible elements.

2.8 QUESTIONS FOR REVIEW

1. Determine $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}]$ •

2. Let f [X] be an irreducible polynomial over F of degree n, and let E be a field extension of F with [E:F] = m. If gcd(m,n) = 1, show that f is irreducible over E.

3. Show that there does not exist a polynomial f (X) ∈ $\mathbb{Z}$[X] of degree > 1 that is irreducible modulo p for all primes p.

2.9 SUGGESTED READINGS AND REFERENCES

1. M. Artin, Algebra, Perentice -Hall of India, 1991.
2. P.M. Cohn, Algebra, vols, I,II, & III, John Wiley & Sons, 1982, 1989, 1991.
3. N. Jacobson, Basic Algebra, vols. I & II, W. H. Freeman, 1980 (also published by Hindustan Publishing Company)
4. S. Lang. Algebra, 3rd edn. Addison-Weslley, 1993.
5. I.S. Luther and I.B.S. Passi, Algebra, Vol.III-Modules, Narosa Publishing House.
6. D. S. Malik, J. N. Modrdeson, and M. K. Sen, Fundamentals of Abstract Algebra, McGraw-Hill, International Edition, 1997.
7. VivekSahai and VikasBist, Algebra, Narosa Publishing House, 1999
8. I. Stweart, Galois Theory, 2nd edition, Chapman and Hall, 1989.
9. J.P. Escofier, Galois theory, GTM Vol.204, Springer, 2001.

2.10 ANSWERS TO CHECK YOUR PROGRESS

1. Provide the characteristics – 2.3

2. Provide proof – 2.3.1

3. Provide explanation – 2.4

4. Provide explanation – 2.5

UNIT-3 SPLITTING FIELDS

STRUCTURE

3.0 OBJECTIVES

Understand the concept of Homomorphisms from simple extensions.

Enumerate the concept of Splitting fields and Multiple roots

Understand the Groups of automorphisms of fields

3.1 INTRODUCTION

In abstract algebra, a **splitting field** of a polynomial with coefficients in a field is the smallest field extension of that field over which the polynomial *splits* or decomposes into linear factors.

3.2 HOMOMORPHISMS FROM SIMPLE EXTENSIONS.

Let E and E' be fields containing F . Recall that an F -homomorphism is a homomorphism

$$\varphi\colon E \to E'$$

such that φ(a) = a for all a ∈ F . Thus an F -homomorphism φ maps a polynomial

$$\sum a_{i_1\cdots i_m}\alpha_1^{i_1}\cdots\alpha_m^{i_m},\quad a_{i_1\cdots i_m}\in F,\quad \alpha_i\in E,$$

$$\sum a_{i_1\cdots i_m}\varphi(\alpha_1)^{i_1}\cdots\varphi(\alpha_m)^{i_m}.$$

An F -***isomorphism*** is a bijective F -homomorphism.

An F -homomorphism E → E' of fields is, in particular, an injective F -linear map of F -vector spaces, and so it will be an F -isomorphism if E and E' have the same finite degree over F .

3.2.1 PROPOSITION : *Let* F(α)*be a simple field extension of a field* F , *and let be a second field containing* F.

(a) *Let* α *be transcendental over* F . *For every* F *–homomorphism* $\varphi\colon F[\alpha]\to\Omega$, φ(α) *transcendental over* F , *and the map* $\varphi\colon\to\varphi(\alpha)$ *defines a one-to-one correspondence*

$$\{F\text{-homomorphisms } F(\alpha)\to\Omega\}\leftrightarrow\{\text{elements of } \Omega \text{ transcendental over } F\}.$$

(b) *Let* α *be algebraic over* F *with minimum polynomial* f (X). *For every* F *-homomorphism* $\varphi\colon F[\alpha]\to\Omega$, φ(α) *is a root of* f (X) *in* Ω, *and the map* $\varphi\colon\to\varphi(\alpha)$ *defines a one-toone correspondence*

$$\{F\text{-homomorphisms } \varphi\colon F[\alpha]\to\Omega\}\leftrightarrow\{\text{roots of } f \text{ in } \Omega\}.$$

In particular, the number of such maps is the number of distinct roots of f in Ω.

PROOF. (a) To say that α is transcendental over F means that F [α] is isomorphic to the polynomial ring in the symbol α. Therefore, for every γ ∈ Ω there is a unique F - homomorphism $\varphi: F[\alpha] \to \Omega$ such that $\varphi(\alpha) = \gamma$. This φ extends to the field of fractions F(α) of F[α] if and only if the nonzero elements of F[α] are sent to nonzero elements of Ω, which is the case if and only if γ is transcendental over F .

Thus we see that here are one-to-one correspondences between
(a) the F -homomorphisms $F(\alpha) \to \Omega$ (b) the F -homomorphisms $\varphi: F[\alpha] \to \Omega$ such that $\varphi(\alpha)$ is transcendental, (c) the transcendental elements of Ω.

(b) Let f (X) = $\sum a_i X^i$, and consider an F -homomorphism $\varphi: F[\alpha] \to \Omega$ On applying φ to the equality $\sum a_i \alpha^i = 0$, we obtain the equality $\sum a_i \varphi(\alpha)^i =$ 0, which shows that $\varphi(\alpha)$ is a root of f (X) in Ω. Conversely, if γ ∈ Ω is a root of f(X), then the map F [X]→Ω g(X)→ g(γ), factors through F [X]/ (f (X)). When composed with the inverse of the isomorphism X + f (X) ↦ α: F [X] / (f (X))→F [α] this becomes a homomorphism F [α]→Ω sending α to γ.

We'll need a slight generalization of this result.

3.2.2 PROPOSITION : *Let* F [α] *be a simple field extension of a field* F *, and let* $\varphi_0: F \to \Omega$ *be a homomorphism from* F *into a second field* Ω.
(a) *If* α *is transcendental over* F , *then the map* $\varphi: \varphi(\alpha) \to \Omega$ *defines a one-to-one correspondence*

$$\{\text{extensions } \varphi: F(\alpha) \to \Omega \text{ of } \varphi_0\} \leftrightarrow \{\text{elements of } \Omega \text{ transcendental over } \varphi_0(F)\}.$$

(b) *If* α *is algebraic over* F , *with minimum polynomial* f (X), *then the* $\varphi \to \varphi(\alpha)$ *map defines a one-to-one correspondence*

$$\{\text{extensions } \varphi\colon F[\alpha] \to \Omega \text{ of } \varphi_0\} \leftrightarrow \{\text{roots of } \varphi_0 f \text{ in } \Omega\}.$$

In particular, the number of such maps is the number of distinct roots of $\varphi_0 f$ in Ω.

By $\varphi_0 f$ we mean the polynomial obtained by applying φ_0 to the coefficients of f. By an extension of φ_0 to F(α) we mean a homomorphism $\varphi : F \to \Omega$ whose restriction to F is φ_0 .

The proof of the proposition is essentially the same as that of the preceding proposition.

3.3 SPLITTING FIELDS

Let f be a polynomial with coefficients in F. A field E containing F is said to ***split*** f if f splits in E[X]:

$$f(X) = a\prod_{i=1}^{m}(X - \alpha_i) \text{ with all } \alpha_i \in E.$$

If E splits f and is generated by the roots of f

$$E = F[\alpha_1, \ldots, \alpha_m],$$

then it is called a ***splitting*** or ***root field*** for f .

Note that $\prod f_i(X)^{m_i}$ and $\prod f_i(X)$ have the same splitting fields.

Note also that f splits in E if it has deg(f) - 1 roots in E because the sum of the roots of f lies in F

$$(\text{if } f = aX^m + a_1X^{m-1} + \cdots, \text{ then } \textstyle\sum \alpha_i = -a_1/a).$$

EXAMPLE :

(a) Let f (X) = $aX^2 + bX + c \in \mathbb{Q}[X]$, and let $\alpha = \sqrt{b^2 - 4ac}$. The subfield $\mathbb{Q}$ [α] of $\mathbb{C}$ is a splitting field for f.

(b) Let f (X) = $X^3+aX^2 + bX + c \in \mathbb{Q}[X]$, be irreducible, and let $\alpha_1, \alpha_2, \alpha_3$ be its roots in $\mathbb{C}$. Then $\mathbb{Q}$ [$\alpha_1, \alpha_2, \alpha_3$] = $\mathbb{Q}$ [α_1, α_2] is a splitting field for f (X). Note that [$\mathbb{Q}$ [α_1]: $\mathbb{Q}$] = 3 and that [$\mathbb{Q}$ [α_1, α_2]: $\mathbb{Q}$ [α_1]] • = 1 or 2, and so [$\mathbb{Q}$ [α_1, α_2]: $\mathbb{Q}$] = 3 or 6.

3.3.1 PROPOSITION : *Every polynomial* f ∈ F [X] *has a splitting field* E_f *, and*

$$[E_f : F] \leq (\deg f)! \quad (\textit{factorial} \deg f).$$

PROOF. Let F_1 = F [α_1] be a stem field for some monic irreducible factor of *f* in F [X] • .

Then *f* (α_1) = 0, and we let $F_2 = F_1$ [α_2] be a stem field for some monic irreducible factor of f (X) /(X – α_1) in F_1[X]. Continuing in this fashion, we arrive at a splitting field E_f.

Let n = degf . Then [F_1:F] = deg $g_1 \leq$ n, [F_2:F_1] ≤ n – 1,…, and so [E*f* :F] • ≤ n!.

EXAMPLE :(a) Let f (X) = (X^p – 1) /(X – 1) ∈ $\mathbb{Q}$ [X], p prime. If ζ is one root of *f* , then the remaining roots are ζ^2; ζ^3,…, ζ^{p-1}, and so the splitting field of *f* is $\mathbb{Q}$ [ζ] • .

(b) Let F have characteristic p ≠ 0, and let f = X^p – X– a ∈ F [X]. If α is one root of *f* in some extension of F, then the remaining roots are α+1 ,… α+p–1, and so the splitting field of f is F [α].

(c) If α is one root of X^n – a, then the remaining roots are all of the form ζα , where ζ^n = 1. Therefore, if F contains all the nth roots of 1 (by which we mean that X^n –1 splits in F [X]), then F[α] is a splitting field for X^n – a. Note that if p is the characteristic of F , then X^p– 1 = (X– 1)^p, and so F automatically contains all the pth roots of 1.

3.3.2 PROPOSITION: Let f ∈ F[X] be monic. Let E be a field containing F and generated over F by roots of *f*, and let Ω be a field containing F in which f splits.

(a) There exists an F -homomorphism φ: E → Ω the number of such homomorphisms is at most [E: F] , and equals [E: F] if has distinct roots in Ω.

(b) If E and Ω are both splitting fields for f , then every F -homomorphism E → Ω is an isomorphism. In particular, any two splitting fields for f are F -isomorphic.

To say that *f* splits in Ω means that f (X) = $\prod_{i=1}^{\deg f}(X - \alpha_i)$ with α_1, α_2,. .. ∈ Ω , to say that f has distinct roots in Ω means that $\alpha_i \neq \alpha_j$ if i ≠ j .

PROOF. We begin with an observation: let F , f , and Ω be as in the statement of the proposition, let L be a subfield of Ω containing F , and let g be a monic factor of *f* in L[X], then g divides f in Ω[X], and so (by unique factorization in Ω[X]), g is product of certain number of the factors X - α_i of f in Ω[X], in particular, we see that g splits in Ω, and that its roots are distinct if the roots of *f* are distinct.

(a) By hypothesis, E = F [α_1, …,α_m]with each α_i a root of f (X). The minimum polynomial of α_1 is an irreducible polynomial f_1 dividing *f* . From the initial observation with L = F , we see that f_1 splits in Ω, and that its roots are distinct if the roots of f are distinct. According to Proposition 3.2.1, there exists an F -homomorphism φ_1: F[α_1] → Ω , and the number of such homomorphisms is at most [F[α_1] :F], with equality holding when f has distinct roots in Ω.

The minimum polynomial of α_2 over F[α_1] is an irreducible factor f_2 of *f* in F[α_1] [X]. On applying the initial observation with L = φ_1 F[α_1] and g = φ_1 f_2 we see that φ_1 f_2 splits in Ω, and that its roots are distinct if the roots of *f* are distinct. According to Proposition 3.2.2

each φ_1 extends to a homomorphism φ_2: $F[\alpha_1,\alpha_2]\to\Omega$, and the number of extensions is at most $F[\alpha_1,\alpha_2]$: $F[\alpha_1]]$, with equality holding when *f* has distinct roots in Ω.

On combining these statements we conclude that there exists an F -homomorphism

$$\varphi: F[\alpha_1,\alpha_2] \to \Omega,$$

and that the number of such homomorphisms is at most $F[\alpha_1,\alpha_2]$: F], with equality holding if *f* has distinct roots in Ω:

After repeating the argument ***m*** times, we obtain (a).

(b) Every F -homomorphism E → Ω is injective, and so, if there exists such a homomorphism, then [E:F] ≤ [Ω:F]. If E and Ω are both splitting fields for f , then (a) shows that there exist homomorphisms E ⇄ Ω, and so [E: F] = [Ω:F]. It follows that every F -homomorphism E → Ω is an F -isomorphism.

3.3.3COROLLARY : *Let* E *and* L *be extension fields of* F , *with* E *finite over* F .

(a) *The number of* F *-homomorphisms* E → L *is at most* [E: F] • .

(b) *There exists a finite extension* Ω/L *and an* F *-homomorphism* E→Ω.

PROOF. Write E = F $[\alpha_1,\ldots,\alpha_m]$ • , and let f ∈ F [X] be the product of the minimum polynomials of the α_i; thus E is generated over F by roots of *f* . Let Ω be a splitting field for *f* regarded as an element of L[X]. The proposition shows that there exists an F -homomorphism E →Ω and the number of such homomorphisms is ≤ [E :F]. This proves (b), and since an F -homomorphism E → L can be regarded as an F -homomorphism E →Ω, it also proves (a).

REMARK : (a) Let $E_1,E_2,\ldots, E_m$ be finite extensions of F , and let L be an extension of F . From the corollary we see that there exists a finite extension L_1/L such that L_1 contains an isomorphic image of E_1; then that there exists a finite extension L_2/L_1 such that L_2 contains an isomorphic image of E_2. On continuing in this fashion, we find that there exists a finite extension Ω/L such that Ω contains an isomorphic copy of every Ei.

(b) Let f ∈ F [X]. If E and E' are both splitting fields of *f*, then we know there exists an F -isomorphism E → E', but there will in general be no *preferred* such isomorphism.

Error and confusion can result if the fields are simply identified. Also, it makes no sense to speak of "the field F [α] generated by a root of *f* " unless f is irreducible (the fields generated by the roots of two different factors are unrelated). Even when *f* is irreducible, it makes no sense to speak of "the field F [α, β] generated by two roots α, β of *f* " (the extensions of F [α] generated by the roots of two different factors of *f* in F [α][β] may be very different).

Check your Progress-1

1. Explain Homomorphisms from simple extensions.

____

____

____

2.   Discuss Splitting Field

____

____

____

3.4 MULTIPLE ROOTS

Even when polynomials in F [X] • have no common factor in F [X], one might expect that they could acquire a common factor in Ω[X] for someΩ ⊃ F . In fact, this doesn't happen — greatest common divisors don't change when the field is extended.

3.4.1 PROPOSITION : *Let* f *and* g *be polynomials in* F [X] • *, and let˝ be an extension of* F*. If* r(X) *is the gcd of* f *and* g *computed in* F [X]*, then* *it is also the gcd of* f *and* g *in* Ω[X]. *In particular, distinct monic irreducible polynomials in* F [X] *do not acquire a common root in any extension field of* F:

PROOF. Let $r_F(X)$ and r_Ω (X) be the greatest common divisors of *f* and *g* in F [X]and Ω[X] respectively. Certainly r_F (X) | r_Ω (X) in Ω[X], but Euclid's algorithm shows that there are polynomials a and b in F[X] • such that

$$a(X)f(X)+b(X)g(X)=r_F(X),$$

and so $r_\Omega(X)$ divides $r_F(X)$ in Ω[X].
For the second statement, note that the hypotheses imply that gcd(f, g) = 1 (in F [X]), and so *f* and g can't acquire a common factor in any extension field.

$$f(X)=a\prod_{i=1}^{r}(X-\alpha_i)^{m_i},\ \alpha_i \text{ distinct}, m_i \geq 1,\ \sum_{i=1}^{r} m_i = \deg(f), \qquad (4)$$

The proposition allows us to speak of the greatest common divisor of f and g without reference to a field.
Let f ∈ F [X]. Then *f* splits into linear factors in Ω [X] for some extension field Ω of F. We say that α_i is a root of *f* of ***multiplicity*** m_i in Ω. If $m_i > 1$, then α_i is said to be a ***multiple root*** of f , and otherwise it is a ***simple root***.

The unordered sequence of integers $m_1, \ldots , m_r$ in (4) is independent of the extension field Ω chosen to split *f* . Certainly, it is unchanged when Ω is replaced with its subfield F [$\alpha_1, \ldots , \alpha_m$], but F [$\alpha_1, \ldots , \alpha_m$], is a splitting field for *f* , and any two splitting fields are F –isomorphic. We say that f ***has a multiple root*** when at least one of the $m_i > 1$,and we say that f has ***only simple roots*** when all $m_i = 1$.

We wish to determine when a polynomial has a multiple root. If f has a multiple factor in F [X], say f = $\prod f_i(X)_{m_i}$ with some $m_i > 1$, then obviously it will have a multiple root.

If f = $\prod f_i$ with the f$_i$ distinct monic irreducible polynomials, then Proposition 3.4.1 shows that *f* has a multiple root if and only if at least one of the f$_i$ has a multiple root. Thus, it suffices to determine when an *irreducible* polynomial has a multiple root.

EXAMPLE : Let F be of characteristic p≠0, and assume that F contains an element a that is not a pth-power, for example, a = T in the field $\mathbb{F}_p$(T) . Then X^p – a is irreducible in F [X], but by we have X^p – a = (X– α)^p in its splitting field. Thus an irreducible polynomial can have multiple roots.

The derivative of a polynomial f (X) = $\sum_{a_i} X^i$ is defined to be f '(X) = $\sum_{ia_i} X^{i-1}$. When *f* has coefficients in R, this agrees with the definition in calculus. The usual rules for differentiating sums and products still hold, but note that in characteristic p the derivative of X^p is zero.

3.4.2 PROPOSITION: For a non constant irreducible polynomial *f* in F [X], the following statements are equivalent:

(a) f has a multiple root;

(b) gcd(f, f ') ≠ 1;

(c) F has nonzero characteristic p and *f* is a polynomial in X^p,

(d) all the roots of *f* are multiple.

PROOF. (a)) (b). Let ˛ be a multiple root of f , and write f = (X – α)^m g(X), m > 1, in some field splitting *f* . Then

$$f'(X) = m(X-\alpha)^{m-1}g(X) + (X-\alpha)^m g'(X). \qquad (5)$$

Hence *f* and *f* ' have X – α as a common factor.

(b) ⇒ (c). As f is irreducible and deg(*f* ') < deg.f /,

$$\gcd(f, f') \neq 1 \implies f' = 0.$$

But, because f is non constant, *f* 'can be zero only if F has characteristic p $\neq$ 0 and f is a polynomial in X^p.

(c) ⇒ (d). Suppose f (X) = g(X^p), and let g(X) = $\prod_i (X-\alpha)^{m_i}$ in some field splitting *f* . Then

$$f(X) = g(X^p) = \prod_i (X^p - a_i)^{m_i} = \prod_i (X - \alpha_i)^{pm_i}$$

where α_i^p = a_i. Hence every root of f (X) has multiplicity at least p.

(d) ⇒ (a). Obvious.

3.4.3 PROPOSITION : *For a non constant polynomial f in* F [X], *the following statements are equivalent:*
(a) gcd(f , f ') = 1*;*
(b) f *has only simple roots (in any field splitting* f *).*

PROOF. Let Ω be an extension of F splitting f . We see that a root α of f in Ω is multiple if and only if it is also a root of *f* '
If gcd(f , f ') =1, then f and f 0 have no common factor in Ω [X]. In *f* particular, they have no common root, and so *f* has only simple roots.
If *f* has only simple roots, then gcd(f , f ') must be the constant polynomial, because otherwise it would have a root in Ω which would then be a common root of f and f '.

3.4.4 **DEFINITION:** A polynomial is ***separable*** if it has only simple roots (in any field splitting the polynomial).

Thus a non constant irreducible polynomial *f* is not separable if and only if F has characteristic p $\neq$ 0 and f is a polynomial in X^p . A nonconstant polynomial *f* is separable if and only if gcd(f , f ') =1. Let f = $\prod f_i$ with f and the f_i monic and the f_i irreducible; then *f* is separable if and only if the f_i are distinct and separable. If *f* is separable as a polynomial in F [X], then it is separable as a polynomial in Ω[X] for every field Ω containing F.

3.4.5 DEFINITION: A field F is ***perfect*** if every irreducible polynomial in F [X] is separable.

3.4.6 PROPOSITION : *A field* F *is perfect if and only if*

(a) F *has characteristic zero, or*

(b) F *has nonzero characteristic* p *and every element of* F *is a* p^{th} *power.*

PROOF. A field of characteristic zero is obviously perfect, and so we may suppose F has characteristic p ≠ 0. If F contains an element a that is not a p^{th} power, then $X^p – a$ is irreducible in F [X] but not separable. Conversely, if every element of F is a p^{th} power, then every polynomial in Xp with coefficients in F is a p^{th} power in F [X] and so it is not irreducible.

$$\sum a_i X^{ip} = \left(\sum b_i X^i\right)^p \quad \text{if} \quad a_i = b_i^p,$$

EXAMPLE : (a) A finite field F is perfect, because the Frobenius endomorphism a ↦ a^p : F → F is injective and therefore surjective (by counting).

(b) A field that can be written as a union of perfect fields is perfect. Therefore, every field algebraic over $\mathbb{F}p$ is perfect.

(c) Every algebraically closed field is perfect.

(d) If F_0 has characteristic p ≠ 0, then F = $F_0(X)$ is not perfect, because X is not a p^{th} power.

3.5 GROUPS OF AUTOMORPHISMS OF FIELDS

Consider fields E ⊃ F. An F -isomorphism E → E is called an F -***automorphism*** of E. The F -automorphisms of E form a group, which we denote Aut (E/F).

EXAMPLE : (a) There are two obvious automorphisms of ℂ, namely, the identity map and complex conjugation.

(b) Let E =ℂ(X). A ℂ -automorphism of E sends X to another generator of E over ℂ. Below are exactly the elements

$$\frac{aX+b}{cX+d}, ad-bc \neq 0.$$

Therefore Aut(E/ ℂ) consists of the maps

$$f(X) \mapsto f\left(\frac{aX+b}{cX+d}\right), ad-bc \neq 0,$$

And so

$$\mathrm{Aut}(E/\mathbb{C}) \simeq \mathrm{PGL}_2(\mathbb{C}),$$

the group of invertible 2×2 matrices with complex coefficients modulo its centre. Analysts will note that this is the same as the automorphism group of the Riemann sphere. Here is the explanation. The field E of meromorphic functions on the Riemann sphere $P^1_{\mathbb{C}}$ consists of the rational functions in z, i.e., E = ℂ(z)≃ ℂ (X), and the natural map Aut($P^1_{\mathbb{C}}$) → Aut(E/ ℂ) is an isomorphism.

(c) The group Aut(ℂ.(X_1, X_2) /ℂ) is quite complicated — there is a map

$$\mathrm{PGL}_3(\mathbb{C}) = \mathrm{Aut}(\mathbb{P}^2_{\mathbb{C}}) \hookrightarrow \mathrm{Aut}(\mathbb{C}(X_1, X_2)/\mathbb{C}),$$

but this is very far from being surjective. When there are even more variables X, the group is not known. The group Aut(ℂ.(X_1, …, X_n) /ℂ) is the group of birational automorphisms of projective n-space $\mathbb{P}^n_{\mathbb{C}}$, and is called the ***Cremona group.*** Its study is part of algebraic geometry.

In this section, we'll be concerned with the groups Aut (E/F) when E is a finite extension of F

3.5.1 PROPOSITION : *Let* E *be a splitting field of a separable polynomial* f *in* F [X]*; then* Aut.E=F / *has order* [E: F].

PROOF. As f is separable, it has deg f distinct roots in E. Therefore Proposition 2.7 shows that the number of F -homomorphisms E →E is [E: F] . Because E is finite over F, all such homomorphisms are isomorphisms.

EXAMPLE: Consider a simple extension E = F [α] and let *f* be a polynomial in F [X] having ˛ as a root. If α is the only root of *f* in E, then Aut(E/F) = 1.

For example, let $\sqrt[3]{2}$ denote the real cube root of 2; then Aut($\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}$) = 1.

As another example, let F be a field of characteristic p ≠ 0, and let a be an element of F that is not a p^th^ power. Let E be a splitting field of f = X^p – a. Then *f* has only one root in E and so Aut(E/F) = 1.

These examples show that, in the statement of the proposition, is necessary that E be a *splitting* field of a *separable* polynomial.

When **G** is a group of auto orphisms of a field E, we set

$$E^G = \text{Inv}(G) = \{\alpha \in E \mid \sigma\alpha = \alpha, \text{ all } \sigma \in G\}.$$

It is a subfield of E, called the subfield of G-***invariants*** of E or the ***fixed field*** of G.

In this section, we'll show that, when E is the splitting field of a separable polynomial in F [X] and G = Aut(E/F), then the maps

$$M \mapsto \text{Aut}(E/M), \quad H \mapsto \text{Inv}(H)$$

give a one-to-one correspondence between the set of intermediate fields M , F ⊂ M ⊂ E, and the set of subgroups H of G.

3.5.2 THEOREM : Let **G** be a finite group of auto orphisms of a field E, and let

$$E^G = \mathrm{Inv}(G) = \{\alpha \in E \mid \sigma\alpha = \alpha, \text{all } \sigma \in G\}.$$

PROOF. Let G = $\{\sigma_1, \dots, \sigma_m\}$ with σ_1 the identity map. It suffices to show that every set $\{\alpha_1, \dots, \alpha_n\}$ of elements of E with n > m is linearly dependent over F . For such a set, bconsider the system of linear equations

$$\begin{aligned} \sigma_1(\alpha_1)X_1 + \cdots + \sigma_1(\alpha_n)X_n &= 0 \\ &\vdots \\ \sigma_m(\alpha_1)X_1 + \cdots + \sigma_m(\alpha_n)X_n &= 0 \end{aligned} \tag{6}$$

with coefficients in E. There are m equations and n > m unknowns, and hence there are nontrivial solutions in E. We choose one $(c_1, \dots, c_n)$ having the fewest possible non- zero elements. After renumbering the α_i, we may suppose that $c_1 \neq 0$, and then, after multiplying by a scalar, that $c_1 \in F$. With these normalizations, we'll show that all $c_i \in F$. Then the first equation

$$\alpha_1 c_1 + \cdots + \alpha_n c_n = 0$$

(recall that σ_i= id) will be a linear relation on the α_i.

If not all c_i are in F , then $\sigma_k(c_i) \neq c_i$ for some k ≠ 1 and i ≠ 1. On applying $\sigma_k$to the equations

$$\begin{aligned} \sigma_1(\alpha_1)c_1 + \cdots + \sigma_1(\alpha_n)c_n &= 0 \\ &\vdots \\ \sigma_m(\alpha_1)c_1 + \cdots + \sigma_m(\alpha_n)c_n &= 0 \end{aligned}$$

and using that $\{\sigma_k\,\sigma_1, \dots, \sigma_k\,\sigma_m\}$ is a permutation of $\{\sigma_1, \dots, \sigma_m\}$, we find that

$$(c_1, \sigma_k(c_2), \dots, \sigma_k(c_i), \dots)$$

is also a solution to the system of equations (6). On subtracting it from the first, we obtain a solution (0;:::;c$_i$ – σ_k(c$_i$),…), which is nonzero (look at the ith entry), but has more zeros than the first solution (look at the first entry) — contradiction.

3.5.3 COROLLARY *Let* G *be a finite group of automorphisms of a field* E*; then* G = Aut(E/E^G).

PROOF. As G ⊂ Aut Aut(E/E^G).we have inequalities

$$[E:E^G] \overset{3.4}{\leq} (G:1) \leq (\mathrm{Aut}(E/E^G):1) \overset{2.8a}{\leq} [E:E^G].$$

All the inequalities must be equalities, and so G = Aut(E/E^G).

3.6 LET US SUM UP

We have discussed different concepts like Homomorphisms from simple extensions, Splitting fields and Multiple roots. We have explored and understood Groups of automorphisms of fields.

3.7 KEYWORDS

Distinct roots - all the **roots**(solutions) of the equations are not equal to one another.

Bijective function - one-to-one correspondence, or invertible function, is a function between the elements of two sets, where each element of one set is paired with exactly one element of the other set, and each element of the other set is paired with exactly one element of the first set.

Transcendental number - is a complex number that is not an algebraic number—that is, not a root (i.e., solution) of a nonzero polynomial equation with integer coefficients.

3.8 QUESTIONS FOR REVIEW

1. Let F be a field of characteristic ¤ 2.

(a) Let E be quadratic extension of F (i.e., ŒEWF • D 2); show that

$$S(E) = \{a \in F^{\times} \mid a \text{ is a square in } E\}$$

is a subgroup of F containing F 2.

(b) Let E and E0 be quadratic extensions of F ; show that there is an F -isomorphism

'WE ! E0 if and only if S.E/ D S.E0/.

2-2 (a) Let F be a field of characteristic p. Show that if Xp X a is reducible in F ŒX • ,

then it splits into distinct factors in F ŒX • .

(b) For every prime p, show that Xp X 1 is irreducible in QŒX • .

3.10 SUGGESTED READINGS AND REFERENCES

1. M. Artin, Algebra, Perentice -Hall of India, 1991.
2. P.M. Cohn, Algebra, vols, I,II, & III, John Wiley & Sons, 1982, 1989, 1991.
3. N. Jacobson, Basic Algebra, vols. I & II, W. H. Freeman, 1980 (also published by Hindustan Publishing Company)
4. S. Lang. Algebra, 3rd edn. Addison-Weslley, 1993.
5. I.S. Luther and I.B.S. Passi, Algebra, Vol.III-Modules, Narosa Publishing House.
6. D. S. Malik, J. N. Modrdeson, and M. K. Sen, Fundamentals of Abstract Algebra, McGraw-Hill, International Edition, 1997.
7. VivekSahai and VikasBist, Algebra, Narosa Publishing House, 1999
8. I. Stweart, Galois Theory, 2nd edition, Chapman and Hall, 1989.

J.P. Escofier, Galois theory, GTM Vol.204, Springer, 2001

3.11 ANSWERS TO CHECK YOUR PROGRESS

1. Provide Explanation – 3.2

2. Refer Explanation – 3.3

3. Provide definition– 3.4.1

4. Provide definition – 3.4.4 and 3.4.5

UNIT-4 COMPUTING GALOSIS GROUP I

STRUCTURE

4.0 OBJECTIVES

Understand the Separable, normal, and Galois extensions

Comprehend the fundamental theorem of Galois theory

Understand the Galois group of a polynomial

Comprehend Solvability of equations

4.1 INTRODUCTION

In this chapter, we prove the fundamental theorem of Galois theory, which classifies the subfields of the splitting field of a separable polynomial f in terms of the Galois group of *f*.

4.2 SEPARABLE, NORMAL, AND GALOIS EXTENSIONS

4.2.1 DEFINITION: An algebraic extension E = F is ***separable*** if the minimum polynomial of every element of E is separable; otherwise, it is ***inseparable***.

Thus, an algebraic extension E/F is separable if every irreducible polynomial in F [X] having a root in E is separable, and it is inseparable if

- F is nonperfect, and in particular has characteristic p ≠ 0, *and*
- there is an element α of E whose minimum polynomial is of the form $g(X^p)$/, g ∈ F [X] .

For example, E = $\mathbb{F}_p(T)$ is an inseparable extension of $\mathbb{F}_p(T^p)$ because T has minimum polynomial $X^p - T^p$.

4.2.2 DEFINITION An algebraic extension E/F is ***normal*** if the minimum polynomial of every element of E splits in E[X]. In other words, an algebraic extension E/F is normal if and only if every irreducible polynomial f ∈ F[X] having a root in E splits in E[X].
Let f be an irreducible polynomial of degree m in F [X], and let E be an algebraic extension of F. If *f* has a root in E, then

$$\left.\begin{array}{lll} E/F \text{ separable} & \implies & \text{roots of } f \text{ distinct} \\ E/F \text{ normal} & \implies & f \text{ splits in } E \end{array}\right\} \implies f \text{ has } m \text{ distinct roots in } E.$$

It follows that E/F is separable and normal if and only if the minimum polynomial of every element α of E has [F:[α]:F] distinct roots in E.

EXAMPLE (a) The polynomial $X^3 - 2$ has one real root $\sqrt[3]{2}$ and two non real roots in C. Therefore the extension $\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}$ (which is separable) is not normal.

(b) The extension $\mathbb{F}_p$(T) / $\mathbb{F}_p$(T^{p}) (which is normal) is not separable because the minimum polynomial of T is not separable.

4.2.3 DEFINITION: An extension E/F of fields is ***Galois*** if it is of finite degree and F is the fixed field of the group of F -automorphisms of E

4.2.4 THEOREM : *For an extension* E/F *, the following statements are equivalent:*

(a) E *is the splitting field of a separable polynomial* f ∈ F [X] • *;*
(b) E *is Galois over* F *;*
(c) F = E^{G} *for some finite group* G *of automorphisms of* E*;*
(d) E *is normal, separable, and finite over* F .

PROOF. (a)) (b). Let G D Aut.E=F /, and let F' = E^{G} ⊃ F. We have to show that F' = F. Note that E is also the splitting field of *f* regarded as a polynomial with coefficients in F', and that *f* is still separable when it is regarded in this way. Hence

$$\left|\mathrm{Aut}(E/F')\right| = [E\colon F'] \leq [E\colon F] = |\mathrm{Aut}(E/F)|\,.$$

According to Corollary 3.5.3, Aut(E/ F') = G. As G = Aut (E/F), we deduce that [E: F'] = [E: F] and so F = F'.

(b) ⇒ (c). By definition, F = E $^{\text{Aut (E/F).}}$ As E is finite over F, with reference to earlier Corollary shows Aut (E/F) to be finite.
(c) ⇒(d). By Theorem 3.5.2, we know that [E:F] ≤ (G : 1); in particular, it is finite. Let α ∈ E, and let *f* be the minimum polynomial of α; we have to show that *f* splits into distinct factors in E[X]. Let {α1=α, α_2…, α_m} be the orbit of α under the action of G on E, and let

$$g(X) = \prod\nolimits_{i=1}^{m}(X - \alpha_i) = X^m + a_1 X^{m-1} + \cdots + a_m.$$

The coefficients a_j are symmetric polynomials in the ˛i, and each $\sigma \in G$ permutes the α_i, and so $\sigma a_j = a_j$ for all j . Thus $g(X) \in F[X]$. As it is monic and $g(\alpha) = 0$, it is divisible by the minimum polynomial f . Let $\alpha_i = \sigma\alpha$ on applying σ to the equation $f(\alpha) = 0$ we find that $f(\alpha_i) = 0$. Therefore every α_i is a root of *f* , and we conclude that g divides *f* . Hence f = g, and so f (X) splits into distinct factors in E.

(d) ⇒(a). Because E has finite degree over F, it is generated over F by a finite number of elements, say, $E = F[\alpha_1, \ldots, \alpha_m]$ $\alpha_i \in E$, α_i algebraic over F . Let *f*i be the minimum polynomial of α_i over F, and let *f* be the product of the distinct f_i. Because E is normal over F, each f_i splits in E, and so E is the splitting field of *f*: Because E is separable over F , each f_i is separable, and so f is separable.

Any one of the four conditions in the theorem can be used as the definition of a Galois extension. When E/F is Galois, the group Aut(E/F) is called the ***Galois group*** of E over F, and it is denoted by Gal(E/F).

4.2.5 REMARK :(a) Let E be Galois over F with Galois group G, and let $\alpha \in E$. The elements $\alpha_1, \alpha_2, \ldots, \alpha_m$ of the orbit of α under G are called the ***conjugates*** of α. In the course of proving the theorem we showed that the minimum polynomial of α is $\prod(X - \alpha_i)$

(b) Let G be a finite group of auto orphisms of a field E, and let F D EG. Then E/F satisfies the equivalent conditions of Theorem 4.2.4. Hence E is Galois over F.

Moreover, Gal (E/F) = G and [E:F] = |Gal (E/F)| •

4.2.6 COROLLARY : *Every finite separable extension* E *of* F *is contained in a Galois extension.*

PROOF. Let $E = F[\alpha_1, \ldots, \alpha_m]$ and let f_i be the minimum polynomial of α_i over F . The product of the distinct f_i is a separable polynomial iin F [X] • whose splitting field is a Galois extension of F containing E.

4.2.7 COROLLARY : *Let* E ⊃ M ⊃ F *; if* E *is Galois over* F *, then it is Galois over* M:

PROOF. We know E is the splitting field of some separable f ∈ F [X], it is also the splitting field of f regarded as an element of M [X].

4.2.8 REMARK : When we relax the separability conditions, we can still say something. An element α of an algebraic extension of F is said to be ***separable*** over F if its minimum polynomial over F is separable.

The proof of Corollary 4.2.6 shows that a finite extension generated by separable elements is separable. Therefore, the elements of an algebraic extension E of F that are separable over F form a subfield E_{sep} of E that is separable over F . When E is finite over F, we let $[E:F]_{sep} = [E_{sep}: F]$ • and call it the ***separable degree*** of E over F . If Ω is an algebraically closed field containing F , then every F –homomorphism $E_{sep} \to \Omega$ extends uniquely to E, and so the number of F -homomorphisms E →Ω is $[E: F]_{sep}$. When E ⊃ M ⊃ F (finite extensions),

$$[E:F]_{\text{sep}} = [E:M]_{\text{sep}}[M:F]_{\text{sep}}.$$

In particular, E is separable over F ⇔ E is separable over M and M is separable over F.

4.2.9 DEFINITION : A finite extension E ⊃ F is a ***cyclic***, ***abelian, ...,*** ***solvable*** extension if it is Galois and its Galois group is cyclic, abelian, ..., solvable Galois group.

4.3 THE FUNDAMENTAL THEOREM OF GALOIS THEORY

4.3.1 THEOREM : (FUNDAMENTAL THEOREM OF GALOIS THEORY)

Let E *be a Galois extension of* F *, and let* G = Gal(E/F) *The maps* H ↦ E^H *and* M ↦ Gal(E/M) *are inverse bijections between the set of subgroups of* G *and the set of intermediate fields between* E *and* F *:*

$$\{\text{subgroups of } G\} \leftrightarrow \{\text{intermediate fields } F \subset M \subset E\}.$$

Moreover,

(a) *the correspondence is inclusion-reversing:* $H_1 \supset H_2 \iff E^{H_1} \subset E^{H_2}$;

(b) *indexes equal degrees:* $(H_1 : H_2) = [E^{H_2} : E^{H_1}]$;

(c) $\sigma H \sigma^{-1} \leftrightarrow \sigma M$, *i.e.*, $E^{\sigma H \sigma^{-1}} = \sigma(E^H)$; $\mathrm{Gal}(E/\sigma M) = \sigma\,\mathrm{Gal}(E/M)\sigma^{-1}$.

(d) H *is normal in* $G \iff E^H$ *is normal (hence Galois) over* F*, in which case*

$$\mathrm{Gal}(E^H/F) \simeq G/H.$$

PROOF. For the first statement, we have to show that H ↦ E^H and M ↦ Gal(E/M) are inverse maps. Let H be a subgroup of G. Then, Corollary 3.5.3 shows that Gal(E/E^H) = H. Let M be an intermediate field. Then E is Galois over M by (4.2.7), which means that E $^{\mathrm{Gal(E/M)}}$ = M .

(a) We have the obvious implications,

$$H_1 \supset H_2 \implies E^{H_1} \subset E^{H_2} \implies \mathrm{Gal}(E/E^{H_1}) \supset \mathrm{Gal}(E/E^{H_2}).$$

As Gal(E/E^{Hi}) = H_i, this proves (a).

(b) Let H be a subgroup of G. According to 4.2.5 (b),

$$(\mathrm{Gal}(E/E^H) : 1) = [E : E^H].$$

This proves (b) in the case H_2 = 1, and the general case follows, using that

$$\begin{aligned} (H_1 : 1) &= (H_1 : H_2)(H_2 : 1) \\ [E : E^{H_1}] &\overset{1.20}{=} [E : E^{H_2}][E^{H_2} : E^{H_1}]. \end{aligned}$$

(c) For τ ∈ G and α ∈ E,

$$\tau\alpha = \alpha \iff \sigma\tau\sigma^{-1}(\sigma\alpha) = \sigma\alpha.$$

Therefore, τ fixes M if and only if $\sigma\tau\sigma^{-1}$ fixes σM , and so σ Gal(E/M) σ^{-1} = Gal(E/σM). This shows that σGal (E/M) σ^{-1} corresponds to σM.

(d) Let H be a normal subgroup of G. Because σH σ^{-1} = H for all σ ∈ G, we must have $\sigma E^H = E^H$ for all σ ∈ G, i.e., the action of G on E stabilizes E^H . We therefore have a homomorphism

$$\sigma \mapsto \sigma|E^H : G \to \text{Aut}(E^H/F)$$

whose kernel is H . As $(E^H)^{G/H}$ = F , we see that E^H is Galois over F (by Theorem 4.2.4) and that G/H ≃ Gal(E^H/F).

Conversely, suppose that M is normal over F , and let $\alpha_1,\ldots\alpha_m$ generate M over F . For σ ∈ G, $\sigma\alpha_i$ is a root of the minimum polynomial of α_i over F, and so lies in M . Hence σM = M , and this implies that σH σ^{-1} = H (by (c)).

4.3.2 REMARK : The theorem shows that there is an order reversing bijection between the intermediate fields of E/F and the subgroups of G. Using this we can read off more results. (a) Let M_1, M_2,…,M_r be intermediate fields, and let H_i be the subgroup corresponding to M_i (i.e., H_i = Gal(E/M_i). Then (by definition) $M_1M_2\ldots M_r$ is the smallest field containing all Mi; hence it must correspond to the largest subgroup contained in all Hi, which is ∩H_i. Therefore

$$\text{Gal}(E/M_1\cdots M_r) = H_1 \cap \ldots \cap H_r.$$

(b) Let H be a subgroup of G and let M D EH . The largest normal subgroup contained in H is N = $\bigcap_{\sigma\in G} \sigma H\sigma^{-1}$ (see GT 4.10), and so E^N is the smallest normal extension of F containing M . Note that, by (a), E^N is the composite of the fields σM . It is called the normal, or Galois, closure of M in E.

4.3.3 PROPOSITION : Let E and L be field extensions of F contained in some common field. If E/F is Galois, then EL/L and E/E ⋂L are Galois, and the map

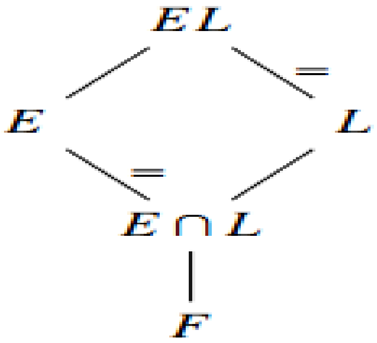
$$\sigma \mapsto \sigma|E\colon \mathrm{Gal}(EL/L) \to \mathrm{Gal}(E/E \cap L)$$

is an isomorphism.

PROOF. Because E is Galois over F , it is the splitting field of a separable polynomial f ∈ F [X]. Then EL is the splitting field of *f* over L, and E is the splitting field of *f* over E \ L. Hence EL=L and E=E \ L are Galois. Every automorphism σ of EL fixing the elements of L maps roots of *f* to roots of *f* , and so σE = E. There is therefore a homomorphism

$$\sigma \mapsto \sigma|E\colon \mathrm{Gal}(EL/L) \to \mathrm{Gal}(E/E \cap L).$$

If σ ∈ Gal(EL/L) fixes the elements of E, then it fixes the elements of EL, and hence is the identity map. Thus, σ ↦ σ | E is injective. If α ∈ E is fixed by all σ ∈ Gal(EL/L), then α ∈ E ⋂ L. By Corollary this implies that the image of σ ↦σ |E is Gal(E/E ⋂ L).



4.3.4 COROLLARY : *Suppose, in the proposition, that* L *is finite over* F *. Then*

$$[EL\colon F] = \frac{[E\colon F][L\colon F]}{[E \cap L\colon F]}.$$

PROOF. According to Proposition

$$[EL\colon F] = [EL\colon L][L\colon F],$$

$$[EL\colon L] \;=\; [E\colon E\cap L] \;=\; \frac{[E\colon F]}{[E\cap L\colon F]}.$$

4.3.5 PROPOSITION : *Let* E_1 *and* E_2 *be field extensions of* F *contained in some common field. If* E_1 *and* E_2 *are Galois over* F, *then* E_1E_2 *and* $E_1 \cap E_2$ *are Galois over* F, *and the map*

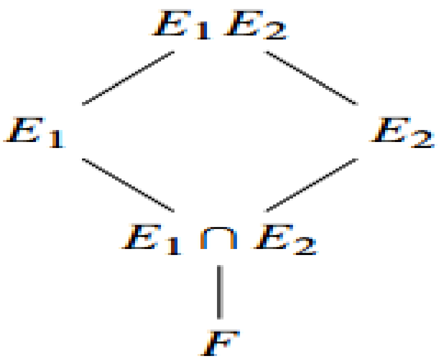
$$\sigma \mapsto (\sigma|E_1, \sigma|E_2)\colon \mathrm{Gal}(E_1E_2/F) \to \mathrm{Gal}(E_1/F) \times \mathrm{Gal}(E_2/F)$$

is an isomorphism of Gal.E1E2=F / *onto the subgroup*

$$H = \{(\sigma_1, \sigma_2) \mid \sigma_1|E_1 \cap E_2 = \sigma_2|E_1 \cap E_2\}$$

of $\mathrm{Gal}(E_1/F) \times \mathrm{Gal}(E_2/F)$.

PROOF: Let a ∈ $E_1 \cap E_2$, and let *f* be its minimum polynomial over F . Then *f* has deg *f* distinct roots in E_1 and deg *f* distinct roots in E_2. Since f can have at most deg *f* roots in E_1E_2, it follows that it has deg *f* distinct roots in $E_1 \cap E_2$. This shows that $E_1 \cap E_2$is normal and separable over F, and hence Galois (4.2.5). As E_1 and E_2 are Galois over F, they are splitting fields for separable polynomials $f_1, f_2 \in F[X]$. Now E_1E_2 is a splitting field for lcm(f_1, f_2), and hence it also is Galois over F . The map σ ↦(σ|E_1 σ|E_2) is clearly an injective homomorphism, and its image is contained in H. We'll prove that the image is the whole of H by counting



From the fundamental theorem,

$$\frac{\mathrm{Gal}(E_2/F)}{\mathrm{Gal}(E_2/E_1 \cap E_2)} \simeq \mathrm{Gal}(E_1 \cap E_2/F),$$

and so, for each

$$\sigma_1 \in \mathrm{Gal}(E_1/F), \sigma_1|E_1 \cap E_2$$

has exactly $[E_2 : E_1 \cap E_2]$ extensions to an element of $\mathrm{Gal}(E_2/F)$.

Therefore

$$(H:1) = [E_1:F][E_2:E_1 \cap E_2] = \frac{[E_1:F]\cdot[E_2:F]}{[E_1 \cap E_2:F]},$$

which equals $[E_1E_2:F]$ • by (3.19):

Example:

We analyse the extension $\mathbb{Q}[\zeta]/\mathbb{Q}$, where ζ is a primitive 7th root of 1, say $\zeta = e^{2\pi i/7}$.

Note that $\mathbb{Q}[\zeta]$ is the splitting field of the polynomial $X^7 - 1$, and that ζ has minimum polynomial

$$X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$$

Therefore, $\mathbb{Q}[\zeta]$ is Galois of degree 6 over $\mathbb{Q}$. For any $\sigma \in \mathrm{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q})$, $\sigma\zeta = \zeta^i$, some i, $1 \leq i \leq 6$, and the map $\sigma \mapsto i$ defines an isomorphism $\mathrm{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q}) \rightarrow (\mathbb{Z}/7\mathbb{Z})^\times$. Let σ be the element of $\mathrm{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q})$ such that $\sigma\zeta = \zeta^3$.

Then σ generates $\mathrm{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q})$ because the class of 3 in $(\mathbb{Z}/7\mathbb{Z})^\times$generates it (the powers of 3 mod 7 are 3,2,6,4,5,1). We investigate the subfields of $\mathbb{Q}[\zeta]$ corresponding to the subgroups $\langle\sigma^3\rangle$ and $\langle\sigma^2\rangle$.

$$\begin{tikzcd}
& \mathbb{Q}[\zeta] \arrow[dl, dash, "\langle\sigma^3\rangle"'] \arrow[dr, dash, "\langle\sigma^2\rangle"] & \\
\mathbb{Q}[\zeta+\bar{\zeta}] \arrow[dr, dash, "\langle\sigma\rangle/\langle\sigma^3\rangle"'] & & \mathbb{Q}[\sqrt{-7}] \arrow[dl, dash, "\langle\sigma\rangle/\langle\sigma^2\rangle"] \\
& \mathbb{Q} &
\end{tikzcd}$$

Note that $\sigma^3\zeta = \zeta^6 = \bar{\zeta}$ (complex conjugate of ζ), and so $\zeta + \bar{\zeta} = 2\cos 2\pi/7$ is fixed by σ^3. Now

$$\mathbb{Q}[\zeta] \supset \mathbb{Q}[\zeta]^{\langle\sigma^3\rangle} \supset \mathbb{Q}[\zeta+\bar{\zeta}] \neq \mathbb{Q}, \text{ and so } \mathbb{Q}[\zeta]^{\langle\sigma^3\rangle} = \mathbb{Q}[\zeta+\bar{\zeta}] \text{ (look at degrees).}$$

As $\langle\sigma^3\rangle$ is a normal subgroup of $\langle\sigma\rangle$, $\mathbb{Q}[\zeta+\bar{\zeta}]$ is Galois over $\mathbb{Q}$, with Galois group $\langle\sigma\rangle/\langle\sigma^3\rangle$,

The conjugates of

$$\alpha_1 \overset{\text{def}}{=} \zeta+\bar{\zeta} \text{ are } \alpha_3 = \zeta^3+\zeta^{-3},\ \alpha_2 = \zeta^2+\zeta^{-2}.$$

Direct calculation shows that

$$\begin{aligned}
\alpha_1+\alpha_2+\alpha_3 &= \sum\nolimits_{i=1}^{6} \zeta^i = -1, \\
\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3 &= -2, \\
\alpha_1\alpha_2\alpha_3 &= (\zeta+\zeta^6)(\zeta^2+\zeta^5)(\zeta^3+\zeta^4) \\
&= (\zeta+\zeta^3+\zeta^4+\zeta^6)(\zeta^3+\zeta^4) \\
&= (\zeta^4+\zeta^6+1+\zeta^2+\zeta^5+1+\zeta+\zeta^3) \\
&= 1.
\end{aligned}$$

Hence the minimum polynomial[1] of $\zeta+\bar{\zeta}$ is

$$g(X) = X^3+X^2-2X-1.$$

$$\cos\tfrac{2\pi}{7} = \tfrac{\alpha_1}{2}$$

The minimum polynomial of is therefore

$$\frac{g(2X)}{8} = X^3 + X^2/2 - X/2 - 1/8.$$

The subfield of $\mathbb{Q}[\zeta]$ corresponding to $\langle\sigma^2\rangle$ is generated by $\beta = \zeta + \zeta_2 + \zeta_4$.Let $\beta' = \sigma\beta$. Then $(\beta - \beta')^2 = -7$. Hence the field fixed by $\langle\sigma^2\rangle$ is $\mathbb{Q}[\sqrt{-7}]$

Check your Progress-1

1. Define Conjugate and Separable

____

____

____

2. What do you understand by - *If* E_1 *and* E_2 *are Galois over* F, *then* E_1E_2 *and* $E_1 \cap E_2$ *are Galois over* F ?

____

____

____

4.4 CONSTRUCTIBLE NUMBERS REVISITED

Earlier we showed that a real number α is constructible if and only if it is contained in a subfield of ℝ of the form $\mathbb{Q}[\sqrt{a_1},\ldots,\sqrt{a_r}]$ • with each a_i a positive element of $\mathbb{Q}[\sqrt{a_1},\ldots,\sqrt{a_{i-1}}]$. In particular

$$\alpha \text{ constructible} \implies [\mathbb{Q}[\alpha]:\mathbb{Q}] = 2^s \text{ some } s. \qquad (7)$$

Now we can prove a partial converse to this last statement.

4.4.1 THEOREM: *If* α *is contained in a subfield of* R *that is Galois of degree* 2^r *over* ℚ, *then it is constructible.*

PROOF. Suppose α ∈ E ⊂ R where E is Galois of degree 2^r over ℚ, and let G = Gal(E/ ℚ).

Because finite p-groups are solvable there exists a sequence of groups

$$\{1\} = G_0 \subset G_1 \subset G_2 \subset \cdots \subset G_r = G$$

with Gi/G_{i-1} of order 2. Correspondingly, there will be a sequence of fields,

$$E = E_0 \supset E_1 \supset E_2 \supset \cdots \supset E_r = \mathbb{Q}$$

with E_{i-1} of degree 2 over E_i. The next lemma shows that $E_i = E_{i-1}[\sqrt{a_i}]$ • for some $a_i \in E_{i-1}$, and $a_i > 0$ because otherwise E_i would not be real. This proves the theorem.

4.4.2 LEMMA : *Let* E/F *be a quadratic extension of fields of characteristic* ≠ 2. *Then* E =F [$\sqrt{d}$] • *for some* d ∈ F .

PROOF. Let α ∈ E, α ∉ F , and let $X^2 + bX + c$ be the minimum polynomial of ‸.

$$\alpha = \frac{-b\pm\sqrt{b^2-4c}}{2}, \text{ and so } E = F[\sqrt{b^2-4c}].$$

4.4.5 COROLLARY: *If* p *is a prime of the form* $2^k + 1$, *then* cos 2π/ p *is constructible.*

PROOF. The field ℚ[$e^{2\pi i/p}$] is Galois over ℚ with Galois group G ≃ (ℤ=pℤ), which has order p – 1 = 2^k. The field ℚ [cos2π/p] is contained in ℚ[$e^{2\pi i/p}$] , and therefore is Galois of degree dividing 2^k . As ℚ [cos2π/p] is a subfield of ℝ, we can apply the theorem.

Thus a regular p-gon, p prime, is constructible if and only if p is a Fermat prime, i.e., of the form $2^{2^r} + 1$. For example, we have proved that the regular 65537-polygon is constructible, without (happily) having to exhibit an explicit formula for cos 2 π/ 65537.

4.4.6 REMARK : The converse to (7) is false; in particular, there are non constructible algebraic numbers of degree 4 over ℚ. The polynomial

$$f(X) = X^4 - 4X + 2 \in \mathbb{Q}[X]$$

Is irreducible, and we'll show below that the Galois group of a splitting field E for f is S4. Each root of f (X) lies in an extension of degree 2^2 of ℚ . If the four roots of f (X) were constructible, then all the elements of E would be constructible , but if H denotes a Sylow 2-subgroup of S4, then E^H has odd degree over ℚ, and so no element of $E^H \setminus$ ℚ is constructible.

4.5 THE GALOIS GROUP OF A POLYNOMIAL

If a polynomial f ∈ F[X] is separable, then its splitting field F_f is Galois over F , and we call Gal(F_f / F) the ***Galois group*** G_f of f:

Let f (X) = $\prod_{i=1}^{n}(X - \alpha_i)$ in a splitting field F_f. We know that the elements of Gal(F_f / F) map roots of *f* to roots of *f* , i.e., they map the set $\{\alpha_1,\alpha_2,\ldots,\alpha_n\}$ into itself.

Being automorphisms, they act as permutations on $\{\alpha_1,\alpha_2,\ldots,\alpha_n\}$. As as the α_i generate F_f over F , an element of Gal(F_f / F) is uniquely determined by the permutation it defines.

Thus G_f can be identified with a subset of Sym.($\{\alpha_1,\alpha_2,\ldots,\alpha_n\}$) $\approx S_n$ (symmetric group on *n* symbols). In fact, G_f consists exactly of the permutations σ of $\{\alpha_1,\alpha_2,\ldots,\alpha_n\}$) such that, for P∈ F $[X_1,\ldots,X_n]$ • ,

$$P(\alpha_1,\ldots,\alpha_n) = 0 \implies P(\sigma\alpha_1,\ldots,\sigma\alpha_n) = 0. \qquad (8)$$

To see this, note that the kernel of the map

$$F[X_1,\ldots,X_n] \to F_f, \quad X_i \mapsto \alpha_i, \qquad (9)$$

consists of the polynomials $P(X_1,\ldots,X_n)$ such that $P(\alpha_1,\ldots,\alpha_n)= 0$. Let σ be a permutation of the α_i satisfying the condition (8). Then the map

$$F[X_1,\ldots,X_n] \to F_f, \quad X_i \mapsto \sigma\alpha_i,$$

factors through the map (9), and defines an F -isomorphism $F_f \to F_f$, i.e., an element of the Galois group. This shows that every permutation satisfying the condition (8) extends uniquely to an element of G_f, and it is obvious that every element of G_f arises in this way. This gives a description of G_f not mentioning fields or abstract groups, neither of which were available to Galois. Note that it shows again that(G_f : 1), hence [F_f :F], divides deg (f)!

4.6 SOLVABILITY OF EQUATIONS

For a polynomial f ∈ F [X], we say that f (X) = 0 is ***solvable in radicals*** if its solutions can be obtained by the algebraic operations of addition, subtraction, multiplication, division, and the extraction of mth roots, or, more precisely, if there exists a tower of fields

$$F = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_m$$

such that

(a) $F_i = F_{i-1}[\alpha_i], \alpha_i^{m_i} \in F_{i-1}$;

(b) F_m contains a splitting field for f.

4.6.1 THEOREM (GALOIS, 1832) *Let* F *be a field of characteristic zero, and let* f ∈ F [X]. *The equation* f (X) = 0 *is solvable in radicals if and only if the Galois group of* f *is solvable.*

We'll prove this later . Also we'll exhibit polynomials f (X) ∈ ℚ [X] • with Galois group S_n, which are therefore not solvable when n ≥ 5.

4.6.2 REMARK When F has characteristic p, the theorem fails for two reasons:

(a) *f* need not be separable, and so not have a Galois group;
(b) $X^p - X - a = 0$ need not be solvable in radicals even though it is separable with abelian Galois group.

If the definition of solvable is changed to allow extensions defined by polynomials of the type in (b) in the chain, then the theorem holds for fields F of characteristic $p \neq 0$ and separable $f \in F[X]$.

Check your Progress-2

3. *Prove : If* α *is contained in a subfield of* R *that is Galois of degree* 2^r *over* ℚ*, then it is constructible*

____

____

____

4. Explain Solvability of equations

____

____

____

4.7 LET US SUM UP

We have discussed the Separable, normal, and Galois extensions. We seen the fundamental theorem of Galois theory. We have discussed the Galois group of a polynomial. We discussed about the Solvability of equations.

4.8 KEYWORDS

Automorphism: In mathematics, an **automorphism** is an isomorphism from a **mathematical** object to itself. It is, in some sense, a symmetry of the object, and a way of mapping the object to itself while preserving all of its structure.

A **polygon** is any 2-dimensional shape formed with straight lines. Triangles, quadrilaterals, pentagons, and hexagons are all examples of **polygons**.

Lemma- informal logic and argument mapping,
a **lemma** (plural **lemmas** or lemmata) is a generally minor, proven proposition which is used as a stepping stone to a larger result

4.9 QUESTIONS FOR REVIEW

$M = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$ and $E = M[\sqrt{(\sqrt{2}+2)(\sqrt{3}+3)}]$ (subfields of $\mathbb{R}$).
1. Let

(a) Show that M is Galois over $\mathbb{Q}$ with Galois group the 4-group $C_2 \times C_2$.
(b) Show that E is Galois over $\mathbb{Q}$ with Galois group the quaternion group.

2. Let E be a Galois extension of F with Galois group G, and let L be the fixed field of a subgroup H of G. Show that the automomorphism group of L/F is N/H where N is the normalizer of H in G.

3 Let E be a finite extension of F . Show that the order of Aut(E / F) divides the degree [E:F].

4.10 SUGGESTED READINGS AND REFERENCES

1. M. Artin, Algebra, Perentice -Hall of India, 1991.
2. P.M. Cohn, Algebra, vols, I,II, & III, John Wiley & Sons, 1982, 1989, 1991.
3. N. Jacobson, Basic Algebra, vols. I & II, W. H. Freeman, 1980 (also published by Hindustan Publishing Company)
4. S. Lang. Algebra, 3rd edn. Addison-Weslley, 1993.

5. I.S. Luther and I.B.S. Passi, Algebra, Vol.III-Modules, Narosa Publishing House.
6. D. S. Malik, J. N. Modrdeson, and M. K. Sen, Fundamentals of Abstract Algebra, McGraw-Hill, International Edition, 1997.
7. VivekSahai and VikasBist, Algebra, Narosa Publishing House, 1999
8. I. Stweart, Galois Theory, 2nd edition, Chapman and Hall, 1989.
9. J.P. Escofier, Galois theory, GTM Vol.204, Springer, 2001.

4.11 ANSWERS TO CHECK YOUR PROGRESS

1. Refer Definition from Remark – 4.2.5 & 4.2.8

2. Provide proof – 4.3.5

3. Provide proof– 4.4.1

4. Provide explanation – 4.6

UNIT-5 COMPUTING GALOIS GROUPS II

STRUCTURE

5.0 OBJECTIVES

Understand the various ways to Compute Galois Groups

Understand Polynomials of degree at most three

Comprehend the examples of Quartic polynomials

Understand the concept of Finite fields

5.1 INTRODUCTION

In this chapter, we investigate general methods for computing Galois groups

5.2 WHEN IS GF ⊂ AN?

Let σ be a permutation of the set {1,2,…, n} The pairs (i , j)with i < j but σ (i) > σ (j) are called the ***inversions*** of σ, and σ is said to be ***even*** or ***odd*** according as the number of inversions is even or odd.

The ***signature*** of σ, sign (σ), is +1 or – 1 according as σ is even or odd. We can define the signature of a permutation σ of any set S of n elements by choosing a numbering of the set and identifying σ with a permutation of {1,…, n}. Then sign is the unique homomorphism Sym(S) → {±1} such that sign (σ) = – 1 for every transposition. In particular, it is independent of the choice of the numbering.

Now consider a monic polynomial

$$f(X) = X^n + a_1X^{n-1} + \cdots + a_n$$

and let

$$f(X) = \prod_{i=1}^{n}(X - \alpha_i)$$

in some splitting field. Set

$$\Delta(f) = \prod_{1\leq i<j\leq n}(\alpha_i - \alpha_j), \qquad D(f) = \Delta(f)^2 = \prod_{1\leq i<j\leq n}(\alpha_i - \alpha_j)^2.$$

The ***discriminant*** of *f* is defined to be D(*f*). Note that D(*f*) is nonzero if and only if *f* has only simple roots, i.e., is separable. Let G_f be the Galois group of *f*, and identify it with a subgroup of Sym({α_1,…, α_n}) .

5.2.1 PROPOSITION: *Let* f ∈ F [X] *be a separable polynomial, and let* σ ∈ G_f .

(a) $\sigma\Delta(f) = sign\ (\sigma)\Delta(f)$ *where* sign $\sigma\Delta(f)$ *is the signature of* σ:

(b) $\sigma D(f) = D(f)$

PROOF. Each inversion of σ introduces a negative sign into $\sigma\Delta(f)$ and so (a) follows from the definition of sign (σ). The equation in (b) is obtained by squaring that in (a).

While $\Delta(f)$ depends on the choice of the numbering of the roots of *f* , D(*f*) does not.

5.2.2 COROLLARY *Let* f (X) ∈ F [X] • *be separable of degree* n. *Let* F_f *be a splitting field for f and let* G_f = Gal(F_f /F).

(a) *The discriminant* D(*f*)∈ F .

(b) *The subfield of* F_f *corresponding to* $A_n \cap G_f$ *is* F [$\Delta(f)$].

Hence

$$G_f \subset A_n \iff \Delta(f) \in F \iff D(f) \text{ is a square in } F.$$

PROOF. (a) The discriminant of f is an element of F_f fixed by

$$G_f \overset{\text{def}}{=} \mathrm{Gal}(F_f/F),$$

and hence lies in F (by the fundamental theorem).

(b) Because f has simple roots, $\Delta(f)$ f ≠ 0, and so the formula $\sigma\Delta(f) = sign\ (\sigma)\Delta(f)$shows that an element of G_f fixes $\Delta(f)$ if and only if it lies in A_n. Thus, under the Galois correspondence,

$$G_f \cap A_n \leftrightarrow F[\Delta(f)].$$

$$G_f \cap A_n = G_f \iff F[\Delta(f)] = F.$$

By completing the cube, one can put any cubic polynomial in this form (in characteristic ≠ 3).

Although there is a not a universal formula for the roots of *f* in terms of its coefficients when the deg(f) > 4, there is for its discriminant. However, the formulas for the discriminant rapidly become very complicated, for example, that for $X^5 + aX^4 + bX^3 + cX^2 + dX + e$ has 59 terms. Fortunately, PARI knows them. For example, typing poldisc (X^3+a*X^2+b*X+c,X) returns the discriminant of $X^3 + aX^2+bX + c$, namely,

$$-4ca^3 + b^2a^2 + 18cba + (-4b^3 - 27c^2).$$

5.2.3REMARK : Suppose F R. Then D(f) will not be a square if it is negative. It is known that the sign of D(f) is $(- 1)^s$ where 2s is the number of non real roots of *f* in ℂ (see ANT 2.40). Thus if *s* is odd, then G_f is not contained in A_n. This can be proved more directly by noting that complex conjugation acts on the roots as the product of s disjoint transpositions. The converse is not true: when *s* is even, G_f is not necessarily contained in A_n.

When does G_f act transitively on the roots?

5.3 WHEN DOES GF ACT TRANSITIVELY ON THE ROOTS?

5.2.4 PROPOSITION: Let f (X) ∈ F [X] be separable. Then f (X) is irreducible if and only if G_f permutes the roots of *f* transitively.

PROOF. ⇒W If α and β are two roots of (X) in a splitting field F_f for *f* , then they both have (X) as their minimum polynomial, and so F [α] and F [β] are both stem fields for *f* . Hence, there is an F –isomorphism

$$F[\alpha] \simeq F[\beta], \qquad \alpha \leftrightarrow \beta.$$

Write F_f = F [$\alpha_1, \alpha_2,\ldots$] with $\alpha_{1=}$ α and $\alpha_2, \alpha_{3,}\ldots$ the other roots of f (X) Then the F -homomorphism α↦β: F [α] → F_f extends (step by step) to an F –homomorphism $F_f \to F_f$, which is an F -isomorphism sending α to β.

$\Leftarrow$: Let g(X) $\in$ F [X]be an irreducible factor of *f* , and let α be one of its roots. If β is a second root of *f* , then (by assumption) $\beta=\sigma\alpha$ for some $\sigma \in G_f$. Now, because g has coefficients in F ,

$$g(\sigma\alpha) = \sigma g(\alpha) = 0,$$

and so β is also a root of g. Therefore, every root of *f* is also a root of *g*, and so f(X) = g(X).

Note that when f(X) is irreducible of degree n, n|(G_f :1) because [F [α]: F] = n and [F [α]: F] divides [F_f: F] = (G_f: F) Thus G_f is a transitive subgroup of S_n whose order is divisible by n.

Check your Progress-1

1. Define ***signature*** of σ.

2.Explain –When does G_f act transitively on the roots?

5.4 POLYNOMIALS OF DEGREE AT MOST THREE

EXAMPLE : Let f (X) $\in$ F [X] be a polynomial of degree 2. Then f is inseparable $\Leftrightarrow$ F has characteristic 2 and f (X) = $X^2 - a$ for some a $\in$ F \ F^2. If f is separable, then G_f = 1(= A_2)or S_2 according as D(f) is a square in F or not.

EXAMPLE: Let f (X) $\in$ F [X] be a polynomial of degree 3. We can assume *f* to be irreducible, for otherwise we are essentially back in the previous case. Then *f* is inseparable if and only if F has characteristic 3 and f (X) = $X^3 - a$ for some a ∈ F \ F^3. If f is separable, then G_f is a transitive subgroup of S_3 whose order is divisible by 3. There are only two possibilities: $G_f = A_3$ or S_3 according as D(f) is a square in F or not. Note that A_3 is generated by the cycle.

For example, $X^3 - 3X + 1$ is irreducible in ℚ[X]. Its discriminant is $-4(-3)^3 - 27 = 81 = 9^2$, and so its Galois group is A^3.

On the other hand, $X^3 + 3X + 1$ ∈ ℚ[X] is also irreducible, but its discriminant is –135 which is not a square in ℚ, and so its Galois group is S_3.

5.5 QUARTIC POLYNOMIALS

Let f (X) be a separable quartic polynomial. In order to determine G_f we'll exploit the fact that S_4 has

$$V = \{1, (12)(34), (13)(24), (14)(23)\}$$

as a normal subgroup — it is normal because it contains all elements of type 2+2 .Let E be a splitting field of *f* , and let f(X) = $\prod(X - \alpha_i)$ in E. We identify the Galois group G_f of *f* with a subgroup of the symmetric group Sym({α_1, α_2, α_3, α_4 }) Consider the partially symmetric elements

$$\alpha = \alpha_1\alpha_2 + \alpha_3\alpha_4$$
$$\beta = \alpha_1\alpha_3 + \alpha_2\alpha_4$$
$$\gamma = \alpha_1\alpha_4 + \alpha_2\alpha_3.$$

They are distinct because the α_i are distinct; for example

$$\alpha - \beta = \alpha_1(\alpha_2 - \alpha_3) + \alpha_4(\alpha_3 - \alpha_2) = (\alpha_1 - \alpha_4)(\alpha_2 - \alpha_3).$$

The group Sym({α_1, α_2, α_3, α_4 }) permutes {α,β,γ}transitively. The stabilizer of each of α,β,γ must therefore be a subgroup of index 3 in S_4, and hence has order 8. For example, the stabilizer of β is ⟨(1234), (13) ⟩ Groups of order 8 in S_4 are Sylow 2-subgroups. There are three of them, all isomorphic to D_4. By the Sylow theorems, V is contained in a Sylow 2-subgroup; in fact, because the Sylow 2-subgroups are conjugate and V is normal, it is contained in all three. It follows that V is the intersection of the three Sylow 2-subgroups. Each Sylow 2-subgroup fixes exactly one of α, β or γ and therefore their intersection V is the subgroup of Sym ($\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$) fixing α, β and γ.

5.5.1 LEMMA *The fixed field of* $G_f \cap V$ *is* F [α, β, γ]. *Hence* F [α, β, γ] *is Galois over* F *with Galois group* $G_f / G_f \cap V$

$$\begin{tikzcd}
E \arrow[d, dash, "G_f \cap V"] \\
F[\alpha,\beta,\gamma] \arrow[d, dash, "G_f/G_f \cap V"] \\
F
\end{tikzcd}$$

PROOF. The above discussion shows that the subgroup of G_f of elements fixing F [α, β, γ] is $G_f \cap V$, and so $E^{G_f \cap V}$ = D F F [α, β, γ] • by the fundamental theorem of Galois theory. The remaining statements follow from the fundamental theorem using that V is normal.

Let M = F [α, β, γ] and let g(X) =(X – α) (X – β) (X – γ) ∈ M[X] • — it is called the ***resolvent cubic*** of f . Every permutation of the α_i (*a fortiori*, every element of G_f) merely permutes α, β, γ and so fixes g(X). Therefore (by the fundamental theorem) g(X) has coefficients in F . More explicitly, we have.

5.5.2 LEMMA : *The resolvent cubic of*

$$f = X^4 + bX^3 + cX^2 + dX + e$$

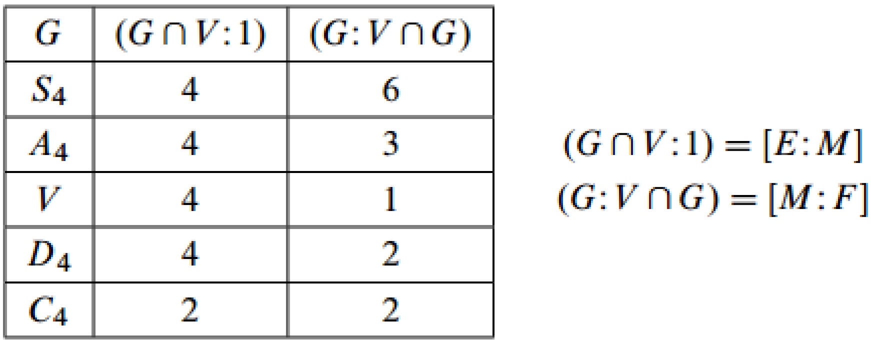
is

$$g = X^3 - cX^2 + (bd - 4e)X - b^2e + 4ce - d^2.$$

The discriminants of f *and* g *are equal.*

SKETCH OF PROOF. Expand f $= (X - \alpha_1)(X - \alpha_2)(X - \alpha_3)(X - \alpha_4)$ to express b,c,d,e in terms of $\alpha_1, \alpha_2, \alpha_3, \alpha_4$. Expand $g = (X - \alpha)(X - \beta)(X - \gamma)$ to express the coefficients of g in terms of $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ and substitute to express them in terms of b,c,d,e.

Now let *f* be an irreducible separable quartic. Then $G = G_f$ is a transitive subgroup of S_4 whose order is divisible by 4. There are the following possibilities for G:



G	$(G \cap V : 1)$	$(G : V \cap G)$
S_4	4	6
A_4	4	3
V	4	1
D_4	4	2
C_4	2	2

$$(G \cap V : 1) = [E : M]$$
$$(G : V \cap G) = [M : F]$$

The groups of type D_4 are the Sylow 2-subgroups discussed above, and the groups of type C_4 are those generated by cycles of length 4.

We can compute $(G{:}V \cap G)$from the resolvent cubic g, because $G{:}V \cap G = \mathrm{Gal}(M/F)$ and M is the splitting field of g. Once we know $(G{:}V \cap G)$ we can deduce G except in the case that it is 2. If [M:F]= 2, then $G \cap V = V$ or C_2. Only the first group acts transitively on the roots of *f* , and so we see that in this case $G = D_4$ or C_4 according as *f* is irreducible or not in M[X].

EXAMPLE : Consider f $(X) = X^4 - 4X + 2 \in Q[X]$. It is irreducible by Eisenstein's criterion and its resolvent cubic is $g(X) = X^3 - 8X - 16$, which is irreducible because it has no roots in F5. The discriminant of g(X) is – 4864, which is not a square, and so the Galois group of g(X) is S_3. From the table, we see that the Galois group of f (X) is S_4.

EXAMPLE : Consider f $(X) = X^4 + 4X^2 + 2 \in Q[X]$. It is irreducible by

Eisenstein's criterion and its resolvent cubic is $(X-4)(X^2-8)$, thus M = $\mathbb{Q}[\sqrt{2}]$. From the table we see that G_f is of type D4 or C4, but f factors over M (even as a polynomial in X2), and hence G_f is of type C4.

EXAMPLE Consider f (X) = D $X^4 - 10X^2 + 4 \in \mathbb{Q}[X]$. It is irreducible in Q[X] because (by inspection) it is irreducible in $\mathbb{Z}[X]$. Its resolvent cubic is (X +10) (X +4) (X– 4) and so G_f is of type V .

EXAMPLE Consider f (X) = $X^4 \in \mathbb{Q}[X]$. It is irreducible by Eisenstein's criterion and its resolvent cubic is $g(X) = X^3 + 8X$. Hence M = $Q[i\sqrt{2}]$ • . One can check that *f* is irreducible over M, and G_f is of type D_4.
As we explained , PARI knows how to factor polynomials with coefficients in $\mathbb{Q}$ [α]

EXAMPLE : Consider f (X) = $X^4 - 2cX^3 - dX^2 + 2cdX - dc^2 \in \mathbb{Z}[X]$ • with a > 0, b > 0, c > 0, a > b and $d = a^2 - b^2$. Let $r = d/c^2$ and let *w* be the unique positive real number such that $r = w^3/(w^2+4)$. Let m be the number of roots of f (X) in $\mathbb{Z}$ (counted with multiplicities). The
Galois group of f is as follows:

- If m = 0 and *w* not rational, then G is S_4.
- If m = 1 and *w* not rational then G is S_3.
- If w is rational and $w^2 + 4$ is not a square then G = D4.
- If w is rational and $w^2 + 4$ is a square then G D V D $C_2 \times C_2$:

This covers all possible cases. The hard part was to establish that m = 2 could never happen.

5.6 EXAMPLES OF POLYNOMIALS WITH SP AS GALOIS GROUP OVER $\mathbb{Q}$

The next lemma gives a criterion for a subgroup of S_p to be the whole of S_p.
5.6.1 LEMMA : *For* p *prime, the symmetric group* Sp *is generated by any transposition and any* p-*cycle.*

PROOF. After renumbering, we may assume that the transposition is τ = (12) and we may write the p-cycle σ so that 1 occurs in the first position, σ = $(1i_2 \ldots i_p)$. Now some power of σ will map 1 to 2 and will still be a p-cycle (here is where we use that p is prime). After replacing σ with the power, we have σ = $(2j_3 \ldots j_p)$. and after renumbering again, we have σ = (123 …p).

Now

$$(i\ i+1) = \sigma^i(12)\sigma^{-i}$$

and so lies in the subgroup generated by σ and τ. These transpositions generate S_p .

5.6.2 PROPOSITION : *Let f be an irreducible polynomial of prime degree* p *in* ℚ[X]*. If f splits in* C *and has exactly two non real roots, then* $G_f = S_p$.

PROOF. Let E be the splitting field of f in C, and let ¸ 2 E be a root of f . Because f is irreducible, [ℚ[X]*:* ℚ] = deg f = p, and so p|[E: ℚ] = (G_f :1). Therefore G_f contains an element of order p (Cauchy's theorem) but the only elements of order p in S_p are p-cycles (here we use that p is prime again).

Let σ be complex conjugation on C. Then σ transposes the two non real roots of f (X) and fixes the rest. Therefore G_f S_p and contains a transposition and a p-cycle, and so is the whole of S_p.

It remains to construct polynomials satisfying the conditions of the Proposition.

EXAMPLE : Let p ≥ 5 be a prime number. Choose a positive even integer m and even integers

$$n_1 < n_2 < \cdots < n_{p-2},$$

$$g(X) = (X^2 + m)(X - n_1) \ldots (X - n_{p-2}).$$

The graph of g crosses the x-axis exactly at the points $n_1,\ldots,n_{p-2}$, and it doesn't have a local maximum or minimum at any of those points (because the n_i are simple roots). Thus $e = \min_{g'(x)=0} |g(x)| > 0$, and we can choose an odd positive integer n such that $2/n < e$.

Consider

$$f(X) = g(X) - \frac{2}{n}.$$

As $2/n < e$, the graph of f also crosses the x-axis at exactly p – 2 points, and so f has exactly two non-real roots. On the other hand, when we write

$$nf(X) = nX^p + a_1X^{p-1} + \cdots + a_p,$$

the a_i are all even and a_p is not divisible by 2^2, and so Eisenstein's criterion implies that *f* is irreducible. Over ℝ, *f* has p – 2 linear factors and one irreducible quadratic factor, and so it certainly splits over ℂ (high school algebra). Therefore, the proposition applies to *f* .

5.7 FINITE FIELDS

Let Fp = ℤ/pℤ, the field of p elements. As we noted in 1, every field E of characteristic p contains a copy of $\mathbb{F}_p$, namely, fm1E j m 2 Zg. No harm results if we identify $\mathbb{F}_p$ with this subfield of E.
Let E be a field of degree n over $\mathbb{F}_p$. Then E has $q = p^n$ elements, and so E is a group of order q – 1. Therefore the nonzero elements of E are roots of $X^{q-1} - 1$, and all elements of E are roots of $X^q - X$. Hence E is a splitting field for $X^q - X$, and so any two fields with q elements are isomorphic.

5.7.1 PROPOSITION : *Every extension of finite fields is simple.*

PROOF. Consider E ⊃ F . Then $E^{\times}$ is a finite subgroup of the multiplicative group of a field, and hence is cyclic. If ζ generates $E^{\times}$ as a multiplicative group, then certainly E = F [ζ].

Now let E be a splitting field of f (X) = X^q – X, q = p^n. The derivative f ' (X) = 1, which is relatively prime to f (X) (in fact, to every polynomial), and so f (X) has q distinct roots in E. Let S be the set of its roots. Then S is obviously closed under multiplication and the formation of inverses, but it is also closed under subtraction: if a^q = a and b^q = b, then

$$(a-b)^q = a^q - b^q = a - b.$$

Hence S is a field, and so S = E. In particular, E has p^n elements.

5.7.2 PROPOSITION : *For each power* q = p^n *of* p *there exists a field* $\mathbb{F}_q$ *with* q *elements. Every such field is a splitting field for* X^q – X*, and so any two are isomorphic. Moreover,* $\mathbb{F}_q$ *is Galois over* $\mathbb{F}_q$ *with cyclic Galois group generated by the Frobenius automorphism σ(a) =* a^p*.*

PROOF. Only the final statement remains to be proved. The field $\mathbb{F}_q$ is Galois over $\mathbb{F}_p$ because it is the splitting field of a separable polynomial.

We noted that $x \overset{\sigma}{\mapsto} x^p$ is an automorphism of $\mathbb{F}_q$. An element a of $\mathbb{F}_q$ is fixed by σ if and only if ap D a, but $\mathbb{F}_p$ consists exactly of such elements, and so the fixed field of hi is $\mathbb{F}_p$. This proves that $\mathbb{F}_q$ is Galois over $\mathbb{F}_p$ and that

$$\langle\sigma\rangle = \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$$

5.7.3 COROLLARY : *Let* E *be a field with* p_n *elements. For each divisor* m *of* n, m ≥ 0, E *contains exactly one field with* p^m *elements.*

PROOF. We know that E is Galois over $\mathbb{F}_p$ and that Gal.E=Fp/ is the cyclic group of order n generated by σ. The group $\langle\sigma\rangle$ has one subgroup of order n/m for each m dividing n, namely, $\langle\sigma^m\rangle$, and so E has exactly one subfield of degree m over $\mathbb{F}_p$ for each m dividing n, namely, E$\langle\sigma^m\rangle$. Because it has degree m over $\mathbb{F}_p$, E$\langle\sigma^m\rangle$ has p^m elements.

5.7.4 COROLLARY : *Each monic irreducible polynomial f of degree* djn *in* $\mathbb{F}_p$ [X] *occurs exactly once as a factor of* X^{p^n} – X*; hence, the degree of the splitting field of* f *is* $\leq$ d.

PROOF. First, the factors of X^{p^n} – X are distinct because it has no common factor with its derivative. If f (X) is irreducible of degree d, then f (X) has a root in a field of degree d over $\mathbb{F}_p$. But the splitting field of X^{p^n} – X contains a copy of every field of degree d over $\mathbb{F}_p$ with d|n. Hence some root of X^{p^n} – X is also a root of f (X) and therefore f (X) |X^{p^n} – X. In particular, f divides X^{p^d} – X, and therefore it splits in its splitting field, which has degree d over $\mathbb{F}_p$.

5.7.5 PROPOSITION : *Let* $\mathbb{F}$ *be an algebraic closure of* $\mathbb{F}_p$*. Then* F *contains exactly one field* $\mathbb{F}_{p^n}$ *for each integer* n ≥ 1, *and* $\mathbb{F}_{p^n}$ *consists of the roots of* X^{p^n} – X. *Moreover,*

$$\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n} \iff m|n.$$

The partially ordered set of finite subfields of $\mathbb{F}$ *is isomorphic to the set of integers* n ≥ 1 *partially ordered by divisibility.*

PROOF. Obvious from what we have proved.

5.7.6 PROPOSITION : *The field* $\mathbb{F}_p$ *has an algebraic closure* $\mathbb{F}$.

PROOF. Choose a sequence of integers 1 = $n_1 < n_2 < n_3 < \ldots$ such that $n_i|n_{i+1}$ for all i, and every integer n divides some n_i. For example, let n_i = i!. Define the fields $\mathbb{F}_{p^{n_i}}$ inductively as follows: $\mathbb{F}_{p^{n_1}} = \mathbb{F}_p$; $\mathbb{F}_{p^{n_i}}$ is the splitting field of $X^{p^{n_i}} - X$ over $\mathbb{F}_{p^{n_{i-1}}}$.

Then, $\mathbb{F}_{p^{n_1}} \subset \mathbb{F}_{p^{n_2}} \subset \mathbb{F}_{p^{n_3}}$, and we define F = $\bigcup \mathbb{F}_{p^{n_i}}$. As a union of a chain of fields algebraic over $\mathbb{F}_p$, it is again a field algebraic over $\mathbb{F}_p$.

Moreover, every polynomial in $\mathbb{F}_p$ [X]splits in $\mathbb{F}$, and so it is an algebraic closure of $\mathbb{F}$.

5.7.7 REMARK :Since the $\mathbb{F}_{p^n}$ are not subsets of a fixed set, forming the union requires explanation. Define S to be the disjoint union of the $\mathbb{F}_{p^n}$. For a , b ∈ S, set a ∼ b if a = b in one of the$\mathbb{F}_{p^n}$. Then ∼ is an equivalence relation, and we let F = S/∼ .

Any two fields with q elements are isomorphic, but not necessarily canonically isomorphic. However, once we have chosen an algebraic closure $\mathbb{F}$ of $\mathbb{F}_p$, there is a unique subfield of $\mathbb{F}$ with q elements.

PARI factors polynomials modulo p very quickly. Recall that the syntax is factormod (f(X),p). For example, to obtain a list of all monic polynomials of degree 1,2,or 4 over $\mathbb{F}_5$, ask PARI to factor $X^{625} - X$ modulo 5 (note that $625 = 5^4$).

5.8 COMPUTING GALOIS GROUPS OVER $\mathbb{Q}$

Recall that for a separable polynomial f ∈ F[X], $F_f$denotes a splitting field for F , and G_f = Gal(F_f /F) denotes the Galois group of *f* . Moreover, G_f permutes the roots $\alpha_1,\ldots\alpha_m$ = deg *f* , of *f* in F_f :

$$G \subset \mathrm{Sym}\{\alpha_1, \ldots, \alpha_m\}.$$

5.8.1 PROPOSITION 4.27 *Let* f (X) *be a separable polynomial in* F[X] *, and suppose that the orbits of* G_f *acting on the roots of f have* $m_1,\ldots,m_r$ *elements respectively. Then* f *factors as* f = $f_1,\ldots, f_r$ *with* f_i *irreducible of degree* m_i.

PROOF. We may suppose that f is monic. Let $\alpha_1,\ldots\alpha_m$, be the roots of f (X) in F_f . The monic factors of f (X) in F_f [X] correspond to subsets S of { $\alpha_1,\ldots\alpha_m$ }

$$S \leftrightarrow f_S = \prod_{\alpha \in S} (X - \alpha),$$

and f_S is fixed under the action of G_f (and hence has coefficients in F) if and only if S is stable under G_f . Therefore the irreducible factors of f in F [X] are the polynomials f_S corresponding to minimal subsets S of { $\alpha_1,\ldots\alpha_m$ }stable under G_f , but these subsets S are precisely the orbits of G_f in { $\alpha_1,\ldots\alpha_m$ }.

5.8.2 REMARK : Note that the proof shows the following: let { $\alpha_1,\ldots\alpha_m$ } = $\bigcup O_i$ be the decomposition of {$\alpha_1,\ldots\alpha_m$ }.into a disjoint union of orbits for the group G_f ; then

$$f = \prod f_i, \quad f_i = \prod_{\alpha_j \in O_i} (X - \alpha_j)$$

is the decomposition of f into a product of irreducible polynomials in F[X] . Now suppose that F is finite, with p^n elements say. Then G_f is a cyclic group generated by the Frobenius automorphism σ: x→x^{p^n}When we regard σ as a permutation of the roots of f , then the orbits of σ correspond to the factors in its cycle decomposition . Hence, if the degrees of the distinct irreducible factors of f are m_1, $m_2,\ldots m_r$, then σ has a cycle decomposition of type.

$$m_1 + \cdots + m_r = \deg f.$$

5.8.3 PROPOSITION : *Let* R *be a unique factorization domain with field of fractions* F , *and let f be a monic polynomial in* R[X]. *Let* P *be a prime ideal in* R, *let* $\bar{F}$= R/P , *and let* $\bar{f}$ *be the image of f in* $\bar{F}$[X] . *Assume that* $\bar{f}$ *is separable. Then f is separable, and its roots* {$\alpha_1,\ldots\alpha_m$} *lie in some finite extension* R' *of* R. *Their reductions* $\bar{\alpha}_i$ *modulo* PR0 *are the roots of* $\bar{f}$, *and* $G_{\bar{f}} \subset$ G_f *when both are identified with subgroups of* Sym{$\alpha_1,\ldots\alpha_m$} = Sym {$\bar{\alpha}_1, \ldots, \bar{\alpha}_m$}.

PROOF: Let f (X) be a separable polynomial in F [X] and $\alpha_1,\ldots\alpha_m$ its roots. Let $T_1,\ldots, T_m$ be symbols. For a permutation σ of {1, …, m}, we let σ_α and σ_T respectively denote the corresponding permutations of $\{\alpha_1,\ldots\alpha_m\}$ and $\{ T_1,\ldots, T_m \}$

Let

$$\theta = T_1\alpha_1 + \cdots + T_m\alpha_m$$

$$f(X,T) = \prod_{\sigma\in S_m} (X - \sigma_T\theta).$$

Clearly f (X,T) is symmetric in the α_i, and so its coefficients lie in F .

$$f(X,T) = f_1(X,T)\cdots f_r(X,T) \tag{10}$$

Let be the factorization of f (X,T) into a product of irreducible monic polynomials. Here we use that F $[X, T_1,\ldots, T_m]$ is a unique factorization domain. The permutations σ such that σ_T carries any one of the factors, say $f_1(X,T)$ into itself form a subgroup G of S_m.

Check your Progress-2

3. State the lemma gives a criterion for a subgroup of Sp to be the whole of S

____

____

____

4. Describe a practical method for computing Galois groups over ℚ and similar fields

____

____

____

5.7 LET US SUM UP

We have studied various ways to Compute Galois Groups. We have discussed about the Polynomials of degree at most three and solved examples of Quartic polynomials. We understood the concept of Finite fields

5.8 KEYWORDS

Maps- the term **mapping**, sometimes shortened as **map**, is a general function between two **mathematical** objects or structures.

Inavariant - an **invariant** is a property of a **mathematical** object (or a class of **mathematical** objects) which remains unchanged, after operations or transformations of a certain type are applied to the objects.

Linear Factorization. A factored form of a polynomial in which each **factor** is a **linear** polynomial.

5.9 QUESTIONS FOR REVIEW

1. Find the splitting field of $X^{m-1} \in \mathbb{F}_p[X]$ • .

2. Find the Galois group of $X^4 - 2X^3 - 8X - 3$ over $\mathbb{Q}$.

3 Find the degree of the splitting field of $X^8 - 2$ over $\mathbb{Q}$.

5.10 SUGGESTED READINGS AND REFERENCES

1. M. Artin, Algebra, Perentice -Hall of India, 1991.
2. P.M. Cohn, Algebra, vols, I,II, & III, John Wiley & Sons, 1982, 1989, 1991.
3. N. Jacobson, Basic Algebra, vols. I & II, W. H. Freeman, 1980 (also published by Hindustan Publishing Company)
4. S. Lang. Algebra, 3rd edn. Addison-Weslley, 1993.

5. I.S. Luther and I.B.S. Passi, Algebra, Vol.III-Modules, Narosa Publishing House.
6. D. S. Malik, J. N. Modrdeson, and M. K. Sen, Fundamentals of Abstract Algebra, McGraw-Hill, International Edition, 1997.
7. VivekSahai and VikasBist, Algebra, Narosa Publishing House, 1999
8. I. Stweart, Galois Theory, 2nd edition, Chapman and Hall, 1989.
9. J.P. Escofier, Galois theory, GTM Vol.204, Springer, 2001.

5.11 ANSWERS TO CHECK YOUR PROGRESS

1. Provide the definition– 5.2

2. Provide explanation – 5.3

3. Provide statement and proof – 5.6.1

4. Provide proposition with proof– 5.8.1

UNIT-6 APPLICATIONS OF GALOIS THEORY I

STRUCTURE

6.0 OBJECTIVES

Enumerated the Primitive element theorem
Comprehend the Fundamental Theorem of Algebra
Understand the concept of Cyclotomic extensions
Comprehend Dedekind’s theorem on the independence of characters and The Normal basis theorem

6.1 INTRODUCTION

In this chapter, we apply the fundamental theorem of Galois theory to obtain other results about polynomials and extensions of fields.

6.2 PRIMITIVE ELEMENT THEOREM.

Recall that a finite extension of fields E/=F is simple if E = F [α] for some element α of E. Such an α is called a ***primitive element*** of E. We'll show that (at least) all separable extensions have primitive elements.

Consider for example $\mathbb{Q}[\sqrt{2},\sqrt{3}]/\mathbb{Q}$. We know that its Galois group over Q is a 4-group $\langle\sigma,\tau\rangle$ where

$$\begin{cases} \sigma\sqrt{2} &= -\sqrt{2} \\ \sigma\sqrt{3} &= \sqrt{3} \end{cases}, \quad \begin{cases} \tau\sqrt{2} &= \sqrt{2} \\ \tau\sqrt{3} &= -\sqrt{3} \end{cases}.$$

Note that

$$\begin{aligned} \sigma(\sqrt{2}+\sqrt{3}) &= -\sqrt{2}+\sqrt{3}, \\ \tau(\sqrt{2}+\sqrt{3}) &= \sqrt{2}-\sqrt{3}, \\ (\sigma\tau)(\sqrt{2}+\sqrt{3}) &= -\sqrt{2}-\sqrt{3}. \end{aligned}$$

These all differ from $\sqrt{2}+\sqrt{3}$, and so only the identity element of Gal.($\mathbb{Q}[\sqrt{2},\sqrt{3}]/\mathbb{Q}$) fixes the elements of $\mathbb{Q}[\sqrt{2},\sqrt{3}]$. According to the fundamental theorem, this implies that $\sqrt{2}+\sqrt{3}$ is a primitive element:

$$\mathbb{Q}[\sqrt{2},\sqrt{3}] = \mathbb{Q}[\sqrt{2}+\sqrt{3}].$$

It is clear that this argument should work much more generally.

Recall that an element α algebraic over a field F is separable over F if its minimum polynomial over F has no multiple roots.

6.2.1 THEOREM : *Let* E = F [$\alpha_1,\ldots,\alpha_r$] *be a finite extension of* F *, and assume that* $\alpha_2,\ldots,\alpha_r$ *are separable over* F *(but not necessarily* α_1*). Then there is an element* $\gamma \in$ E *such that*
E = F[γ].

PROOF. For finite fields,we may assume F to be infinite. It suffices to prove the statement for r = 2, for then

$$F[\alpha_1,\alpha_2,\ldots,\alpha_r] = F[\alpha_1',\alpha_3,\ldots,\alpha_r] = F[\alpha_1'',\alpha_4,\ldots,\alpha_r] = \cdots .$$

Thus let E = F [α, β] with β separable over F . Let *f* and *g* be the minimum polynomials of α and β over F , and let L be a splitting field for *fg* containing E. Let $\alpha_1 = \alpha,\ldots, \alpha_s$ be the roots of *f* in L, and let $\beta_1 = \beta$, $\beta_2,\ldots \beta_t$ be the roots of g. For j ≠ 1, $\beta_j \neq \beta$, and so the the equation

$$\alpha_i + X\beta_j = \alpha + X\beta,$$

has exactly one solution, namely, $X = \frac{\alpha_i - \alpha}{\beta - \beta_j}$

If we choose a c ∈F different from any of these solutions (using that F is infinite), then

$$\alpha_i + c\beta_j \neq \alpha + c\beta \text{ unless } i = 1 = j.$$

Let γ=α+cβ . I claim that

$$F[\alpha,\beta] = F[\gamma].$$

The polynomials g(X)and f (γ –cX) have coefficients in F [γ] , and have β as a root:

$$g(\beta) = 0, \quad f(\gamma - c\beta) = f(\alpha) = 0.$$

In fact, β is their only common root, because we chose c so that $\gamma - c\beta_j \neq \alpha_i$ unless i = 1 = j . Therefore

$$\gcd(g(X), f(\gamma - cX)) = X - \beta.$$

Here we computed the gcd in L[X], but this is equal to the gcd computed in F [γ] [X]. Hence β ∈ F [γ] , and this implies that α =γ – cβ also lies in F [γ] . This proves the claim.

6.2.2 REMARK : When F is infinite, the proof shows that can be chosen to be of the form

$$\gamma = \alpha_1 + c_2\alpha_2 + \cdots + c_r\alpha_r, \quad c_i \in F.$$

If F [α_1,…, α_r] • is Galois over F , then an element of this form will be a primitive element provided it is moved by every nontrivial element of the Galois group. This remark makes it very easy to write down primitive elements.

Our hypotheses are minimal: if *two* of the α are not separable, then the extension need not be simple. Before giving an example to illustrate this, we need another result.

6.2.3 PROPOSITION: *Let* E = F [γ] *be a simple algebraic extension of* F . *Then there are only finitely many intermediate fields* M,

$$F \subset M \subset E.$$

PROOF. Let M be such a field, and let g(X) be the minimum polynomial of over M . Let M' be the subfield of E generated over F by the coefficients of g(X). Clearly M' ⊂ M , but (equally clearly) g(X) is the minimum polynomial of over M'. Hence

$$[E\colon M'] = \deg(g) = [E\colon M],$$

and so M = M', we have shown that M is generated by the coefficients of g(X).

Let *f*(X) be the minimum polynomial of γ over F . Then g(X) divides *f*(X) in M[X], and hence also in E[X]. Therefore, there are only finitely many possible g, and consequently only finitely many possible M

6.2.4 REMARK 5.4 (a) Note that the proof in fact gives a description of all the intermediate fields: each is generated over F by the coefficients of a factor g(X) of *f*(X) in E[X]. The coefficients of such a g(X) are partially symmetric polynomials in the roots of *f*(X) (that is, fixed by some, but not necessarily all, of the permutations of the roots).

(b) The proposition has a converse: if E is a finite extension of F and there are only finitely many intermediate fields M , F ⊂ M⊂ E, then E is a simple extension of F . This gives another proof of Theorem 6.2.1 in the case that E is separable over F , because Galois theory shows that there are only finitely many intermediate fields in this case (even the Galois closure of E over F has only finitely many intermediate fields).

EXAMPLE : The simplest nonsimple algebraic extension is k(X,Y) ⊃ k(X^p,Y^p), where k is an algebraically closed field of characteristic p. Let F = k(X^p,Y^p), For all c ∈ k,

$$k(X,Y) = F[X,Y] \supset F[X+cY] \supset F$$

We have with the degree of each extension equal to p. If

$$F[X+cY] = F[X+c'Y], \quad c \neq c',$$

then F [X+ cY] would contain both X and Y , which is impossible because [k(X,Y) : F] = p^2. Hence there are infinitely many distinct intermediate fields. Alternatively, note that the degree of k(X,Y) over k(X^p,Y^p), is p^2, but if α ∈ k(X,Y) then α^p ∈ k(X^p,Y^p), and so α generates a field of degree at most p over k(X^p,Y^p).

6.3 FUNDAMENTAL THEOREM OF ALGEBRA

We finally prove the misnamed fundamental theorem of algebra.

6.3.1 THEOREM : The field ℂ of complex numbers is algebraically closed.

PROOF. We define ℂ to be the splitting field of X^2+1 over ℝ, and we let i denote a rootof X^2+1 in ℂ. Thus ℂ = ℝ[i] . We have to show that every *f* (X) ∈ ℝ[X] • has aroot in C. We may suppose that *f* is monic, irreducible, and ≠ X^2+1.

We'll need to use the following two facts about ℝ:

- positive real numbers have square roots;
- every polynomial of odd degree with real coefficients has a real root.

Both are immediate consequences of the Intermediate Value Theorem, which says that a continuous function on a closed interval takes every value between its maximum and minimum values (inclusive). (Intuitively, this says that, unlike the rationales, the real line has no "holes".)

We first show that every element of ℂ has a square root. Write α = a + bi, with a, b ∈ ℝ, and choose c, d to be real numbers such that

$$c^2 = \frac{(a+\sqrt{a^2+b^2})}{2}, \quad d^2 = \frac{(-a+\sqrt{a^2+b^2})}{2}.$$

Then $c^2 - d^2$ = a and $(2cd)^2 = b^2$. If we choose the signs of c and d so that cd has the same sign as b, then $(c + di)^2$ =α and so c + di is a square root of α.

Let f (X) ∈ ℝ [X], and let E be a splitting field for f (X) (X^2+ 1). Then E contains ℂ, and we have to show that it equals ℂ. Since ℝ has characteristic zero, the polynomial is separable, and so E is Galois over ℝ. Let G be its Galois group, and let H be aSylow 2-subgroup of G.

Let M = E^H and let α ∈ M. Then M has of degree (G: H) over ℝ, which is odd, andso the minimum polynomial of α over R has odd degree (by the multiplicativity of degrees). This implies that it has a real root, and so is of degree 1. Hence α ∈ ℝ, and so M = ℝ and G = H.

We deduce that Gal(E/ $\mathbb{C}$) is a 2-group. If it is ≠ 1, then it has a subgroup N of index 2. The field E^N has degree 2 over $\mathbb{C}$, and so it is generated by the square root of an element of $\mathbb{C}$ (see 3.24), but all square roots of elements of $\mathbb{C}$ lie in $\mathbb{C}$. Hence $E^N = \mathbb{C}$, which is a contradiction. Thus Gal(E/ $\mathbb{C}$) =1and E = $\mathbb{C}$.

COROLLARY 5.7 (a) The field $\mathbb{C}$ is the algebraic closure of $\mathbb{R}$.
(b) The set of all algebraic numbers is an algebraic closure of $\mathbb{Q}$:

PROOF. Part (a) is obvious from the definition of "algebraic closure" and (b) follows from Corollary in Unit 2

Check your Progress-1

1. Explain **Primitive element theorem**

____

____

____

2. State two facts about Fundamental theorem of Algebra

____

____

____

6.4 CYCLOTOMIC EXTENSIONS

A primitive n^{th} root of 1 in F is an element of order n in $F^{\times}$. Such an element can exist only if F has characteristic 0 or if its characteristic p does not divide n.

6.4.1 PROPOSITION : Let F be a field of characteristic 0 or characteristic p not dividing n, and let E be the splitting field of $X^n - 1$.

(a) There exists a primitive nth root of 1 in E.

(b) If ζ is a primitive nth root of 1 in E, then E = F[ζ].

• .

(c) The field E is Galois over F ; for each σ ∈ Gal(E/F), there is an i ∈ $(\mathbb{Z}/n\mathbb{Z})^{\times}$ such that $\sigma\zeta = \zeta^{i}$ for all ζ with $\zeta^{n} = 1$; the map σ ↦ [i] is an injective homomorphism

$$\mathrm{Gal}(E/F) \to (\mathbb{Z}/n\mathbb{Z})^{\times}.$$

PROOF. (a) The roots of $X^{n} - 1$ are distinct, because its derivative $n X^{n} - 1$ has only zero as a root (here we use the condition on the characteristic), and so E contains n distinct n^th^ roots of 1. The n^th^ roots of 1 form a finite subgroup of $E^{\times}$, and so they form a cyclic group. Every generator has order n, and hence is a primitive nth root of 1.

(b) The roots of $X^{n} - 1$ are the powers of ζ, and F [ζ] contains them all.

(c) The extension E = F is Galois because E is the splitting field of a separable polynomial.

If ζ_0 is one primitive nth root of 1, then the remaining primitive n^th^ roots of 1 are the elements $\zeta_0^{i}$with i relatively prime to n. Since, for any automorphism σ of E, σ ζ_0 is again a primitiventh root of 1, it equals ζ_0^{i} for some i relatively prime to n, and the map σ ↦ i mod n isinjective because ζ_0 generates E over F . It obviously is a homomorphism. Moreover, for any other n^th^ root of 1, say, $\zeta = \zeta_0^{m}$,we have

$$\sigma\zeta = (\sigma\zeta_0)^{m} = \zeta_0^{im} = \zeta^{i},$$

and so the homomorphism does not depend on the choice of ζ_0.

The map σ ↦[i] : Gal(F [ζ]/F)→ $(\mathbb{Z}/n\mathbb{Z})^{\times}$ need not be surjective. For example, if F = ℂ ,then its image is{1}, and if F = ℝ, it is either {[1]}, or {[-1]}, {[1]}. On the otherhand, when n = p is prime, we showed in that $[\mathbb{Q}[\zeta]\colon \mathbb{Q}] = p - 1$, and so the map is surjective. We now prove that the map is surjective for all n when F = ℚ.

The polynomial $X^n - 1$ has some obvious factors in Q[X], namely, the polynomials $X^d - 1$ for any d|n. When we remove all factors of $X^n - 1$ of this form with d < n, thepolynomial we are left with is called the n^{th} **cyclotomic polynomial** Φ_n. Thus

$$\Phi_n = \prod (X - \zeta) \qquad \text{(product over the primitive } n\text{th roots of 1).}$$

It has degree φ(n), the order of . $(\mathbb{Z}/n\mathbb{Z})^\times$ Since every n^{th} root of 1 is a primitive d^{th} rootof 1 for exactly one d dividing n, we see that

$$X^n - 1 = \prod_{d|n} \Phi_d(X).$$

For example, $\Phi_1(X) = X - 1$, $\Phi_2(X) = X + 1$, $\Phi_3(X) = X^2 + X + 1$, and

$$\Phi_6(X) = \frac{X^6 - 1}{(X-1)(X+1)(X^2+X+1)} = X^2 - X + 1.$$

This gives an easy inductive method of computing the cyclotomic polynomials. Alternatively type polcyclo (n,X) in PARI.

Because $X^n - 1$ has coefficients in $\mathbb{Z}$ and is monic, every monic factor of it in Q[X]has coefficients in $\mathbb{Z}$. In particular, the cyclotomic polynomials lie in $\mathbb{Z}$[X].

6.4.2 LEMMA: Let F be a field of characteristic 0 or p not dividing n, and let ζ be a primitive n^{th} root of 1 in some extension field. The following are equivalent:

(a) the nth cyclotomic polynomial Φ_n is irreducible;

(b) the degree [F [ζ]: F]= φ_n

(c) the homomorphism

$$\text{Gal}(F[\zeta]/F) \to (\mathbb{Z}/n\mathbb{Z})^\times$$

is an isomorphism.

PROOF. Because ζ is a root of Φ_n, the minimum polynomial of ζ divides Φ_n. It equals it if and only if [F [ζ]: F]= φ_n which is true if and only if the injection Gal. [F [ζ]: F] →$(\mathbb{Z}/n\mathbb{Z})^{\times}$ is onto.

6.4.3 THEOREM The nth cyclotomic polynomial Φ_n is irreducible in Q[X].

PROOF. Let f (X)be a monic irreducible factor of Φ_n in Q(X). Its roots will be primitive n^th roots of 1, and we have to show they include all primitive nth roots of 1. For this it suffices to show that

$$\zeta \text{ a root of } f(X) \implies \zeta^i \text{ a root of } f(X) \text{ for all } i \text{ such that } \gcd(i,n) = 1.$$

Such an i is a product of primes not dividing n, and so it suffices to show that

$$\zeta \text{ a root of } f(X) \implies \zeta^p \text{ a root of } f(X) \text{ for all primes } p \text{ not dividing } n.$$

Write

$$\Phi_n(X) = f(X)g(X).$$

6.4.4 Proposition : shows that f (X) and g(X) lie in $\mathbb{Z}[X]$. Suppose that ζ is a root of *f* but that, for some prime p not dividing n, ζ^{p} is not a root of f . Then ζ^{p} is a root of g(X) , g(ζ^{p}) = 0, and so ζ is a root of g(X^p). As f (X) and g(X^p) have a common root, they have a nontrivial common factor in $\mathbb{Q}[X]$. (2.10), which automatically lies in $\mathbb{Z}[X]$.

Write h(X) ↦ $\bar{h}$(X) for the quotient map $\mathbb{Z}[X]$→ $\mathbb{F}_p[X]$. • , and note that, because f (X) and g.Xp/ have a common factor of degree _ 1 in Z.X • , so also do $\bar{f}$ (X) and $\bar{g}$(X^p) in $\mathbb{F}_p[X]$. The mod p binomial theorem shows that

$$\bar{g}(X)^p = \bar{g}(X^p)$$

(recall that $a^p = a$ for all $a \in \mathbb{F}_p$), and so $\overline{f}$ (X) and $\overline{g}$ (X) have a common factor of degree ≥ 1 in $\mathbb{F}_p[X]$. Hence $X^n - 1$, when regarded as an element of $\mathbb{F}_p[X]$, has multiple roots, but we saw in the proof of Proposition 6.4.1 that it doesn't. Contradiction.

6.4.5 REMARK : This proof is very old — in essence it goes back to Dedekind in 1857 —but its general scheme has recently become popular: take a statement in characteristic zero, reduce modulo p (where the statement may no longer be true), and exploit the existence of the Frobeniusautomorphism $a \mapsto a^p$ to obtain a proof of the original statement. For example, commutative algebraists use this method to prove results about commutative rings, and there are theorems about complex manifolds that were first proved by reducing things to characteristic p:

There are some beautiful relations between what happens in characteristic 0 and incharacteristic p. For example, let $f(X1,...,X_n) \in \mathbb{Z}[X1,...,X_n]$. We can

(a) look at the solutions of f = 0 in ℂ, and so get a topological space;

(b) reduce mod p, and look at the solutions of $\overline{f} = 0$ in $\mathbb{F}_{p^n}$.

6.4.6 THEOREM : The regular n-gon is constructible if and only if $n = 2^k p_1 \dots p_s$ where the p_i are distinct Fermat primes.

PROOF. The regular n-gon is constructible if and only if cos 2π/ n (equivalently, $\zeta = e^{2\pi i/n}$)is constructible. We know that ℚ[ζ] is Galois over ℚ, and so ζ is constructible if and only if [ℚ[ζ] : ℚ] is a power of 2. When we write $n = \prod p^{n(p)}$

$$\varphi(n) = \prod_{p|n} (p-1)p^{n(p)-1},$$

and this is a power of 2 if and only if n has the required form.

6.4.7 REMARK : (a) As mentioned earlier, the Fermat primes are those of the form $2^{2^r}+1$.It is known that these numbers are prime when r = 0, 1,2,3,4, but it is not known whetheror not there are more Fermat primes. Thus the problem of listing the n for which the regular n-gon is constructible is not yet solved .

(b) The final section of Gauss's, DisquisitionesArithmeticae (1801) is titled "Equationsdefining sections of a Circle". In it Gauss proves that the nth roots of 1 form a cyclic group, that $X^n - 1$ is solvable (this was before the theory of abelian groups had been developed,and before Galois), and that the regular n-gon is constructible when n is as in the Theorem. He also claimed to have proved the converse statement. This leads some people to credithim with the above proof of the irreducibility of _n, but in the absence of further evidence, I'm sticking with Dedekind.

6.5 DEDEKIND'S THEOREM ON THE INDEPENDENCE OF CHARACTERS

6.5.1 THEOREM (DEDEKIND) Let F be a field and G a group. Then every finite set $\{\chi_1,\ldots,\chi_m\}$of group homomorphisms G → $F^\times$ is linearly independent over F , i.e.,

$$\sum a_i\chi_i = 0 \text{ (as a function } G \to F) \implies a_1 = 0,\ldots,a_m = 0.$$

PROOF. We use induction on m. For m = 1, the statement is obvious. Assume it for m – 1,and suppose that, for some set $\{\chi_1,\ldots,\chi_m\}$of homomorphisms G → $F^\times$ and $a_i \in F$,

$$a_1\chi_1(x)+a_2\chi_2(x)+\cdots+a_m\chi_m(x)=0 \quad \text{for all } x \in G.$$

We have to show that the a_i are zero. As χ_1 and χ_2 are distinct, they will take distinct values on some g ∈ G. On replacing *x* with *gx* in the equation, we find that

$$a_1\chi_1(g)\chi_1(x)+a_2\chi_2(g)\chi_2(x)+\cdots+a_m\chi_m(g)\chi_m(x)=0 \quad \text{for all } x\in G.$$

On multiplying the first equation by χ_1 (g) and subtracting it from the second, we obtain the equation

$$a_2'\chi_2+\cdots+a_m'\chi_m=0, \qquad a_i'=a_i(\chi_i(g)-\chi_1(g)).$$

The induction hypothesis shows that a_i' = 0 for i = 2, 3, .. As χ_2 (g) – χ_1 (g) ≠ 0, this implies that a_2 = 0, and so

$$a_1\chi_1+a_3\chi_3+\cdots+a_m\chi_m=0.$$

The induction hypothesis now shows that the remaining ai are also zero.

6.5.2 COROLLARY Let F and E be fields, and letσ_1,... ,σ_m be distinct homomorphisms F → E. Then σ_1,... ,σ_m are linearly independent over E:

PROOF. Apply the theorem to $\chi_2 = \sigma_1|F^\times$

6.5.3 COROLLARY: Let E be a finite separable extension of F of degree m. Let σ_1,... ,σ_m be a basis for E as an F -vector space, and let σ_1,... ,σ_m be distinct F –homomorphismsfrom E into a field . Then the matrix whose (i , j) th-entry is $\sigma_i\,\sigma_j$ is invertible.

PROOF. If not, there exist $c_i \in \Omega$ such that $\sum_{i=1}^{m} c_i\sigma_i(\alpha_j) = 0$ for all j . But the map$\sum_{i=1}^{m} c_i\sigma_i : E \longrightarrow \Omega$ is F -linear, and so this implies that $\sum_{i=1}^{m} c_i\sigma_i(\alpha\,) = 0$ or all α ∈ E which contradicts Corollary 6.5.2

6.6 THE NORMAL BASIS THEOREM

6.6.1 DEFINITION Let E be a finite Galois extension of F . A basis for E as an F –vectorspace is called a normal basis if it consists of the conjugates of a single element of E. In other words, a normal basis is one of the form

$$\{\sigma\alpha \mid \sigma \in \mathrm{Gal}(E/F)\}$$

for some α ∈ E.

6.6.2 THEOREM (NORMAL BASIS THEOREM) Every Galois extension has a normal basis.

The group algebra FG of a group G is the F -vector space with basis the elements of G endowed with the multiplication extending that of G. Thus an element of FG is a sum $\sum_{\sigma \in G} a_\sigma \sigma,\ a_\sigma$ ∈ G

$$\left(\sum_\sigma a_\sigma \sigma\right)\left(\sum_\sigma b_\sigma \sigma\right) = \sum_\sigma \left(\sum_{\sigma_1\sigma_2=\sigma} a_{\sigma_1} b_{\sigma_2}\right)\sigma.$$

Every F -linear action of G on an F -vector space V extends uniquely to an action of FG on V .

Let E/F be a Galois extension with Galois group G. Then E is an FG-module, and Theorem 6.6.2 says that there exists an element α ∈ E such that the map

$$\sum_\sigma a_\sigma \sigma \mapsto \sum_\sigma a_\sigma \sigma\alpha : FG \to E$$

is an isomorphism of FG-modules, i.e., that E is a free FG-module of rank 1:

We give three proofs of Theorem 5.18. The first assumes that F is infinite and the secondthat G is cyclic. Since every Galois extension of a finite field is cyclic (4.20), this covers allcases. The third proof applies to both finite and infinite fields, but uses the Krull-Schmidttheorem.

PROOF FOR INFINITE FIELDS

6.6.3 LEMMA Let f ∈ F [X_1,..., X_m], and let S be an infinite subset of F . If f(a_1,..., a_m) = 0 for all a_1,...,a_m ∈ S, then f is the zero polynomial (i.e., f = 0 in F [X_1,..., X_m]).

PROOF. We prove this by induction on m. For m =1, the lemma becomes the statement that a nonzero polynomial in one symbol has only finitely many roots . For m > 1,rite f as a polynomial in X_m with coefficients in F [X_1,..., X_{m-1}], say,

$$f = \sum c_i(X_1, \ldots, X_{m-1})X_m^i.$$

For any m – 1 /-tuple a_1,..., a_{m-1} of elements of S,

$$f(a_1, \ldots, a_{m-1}, X_m)$$

is a polynomial in X_m having every element of S as a root. Therefore, each of its coefficientsis zero, c_i (a_1,..., a_{m-1}) = 0 for all i . Since this holds for all (a_1,..., a_{m-1}) the induction hypothesis shows that c_i. (X_1,..., X_{m-1}) is the zero polynomial.

We now prove 6.6.2 in the case that F is infinite. Number the elements of G as σ_1,..., σ_m with σ_1 the identity map.

Let f ∈ F [X_1,..,X_m] • have the property that

$$f(\sigma_1\alpha, \ldots, \sigma_m\alpha) = 0$$

for all α ∈ E. For a basis α_1,..., α_m of E over F , let

$$g(Y_1, \ldots, Y_m) = f(\textstyle\sum_{i=1}^m Y_i\sigma_1\alpha_i, \sum_{i=1}^m Y_i\sigma_2\alpha_i, \ldots) \in E[Y_1, \ldots, Y_m].$$

The hypothesis on *f* implies that g(a_1,...,a_m) = 0 for all a_i ∈ F , and so g = 0 (becauseF is infinite). But the matrix ($\sigma_i\alpha_j$) is invertible Since g is obtained from *f* by an invertible linear change of variables, *f* can be obtained from g by the inverse linear changeof variables. Therefore it also is zero.

Write $X_i = X(\sigma_i)$, and let A = $(X(\sigma_i\sigma_j))$, i.e., A is the m×m matrix having X_k in the (i, j)th place if $\sigma_i\sigma = \sigma_k$. Then det(A) is a polynomial in $X_1,...,X_m$, say, det(A)= h $(X_1,...,X_m)$. Clearly, h(1,0,..., 0) is the determinant of a matrix having exactly one 1 in each row and each column and its remaining entries 0. Hence the rows of the matrix are a permutation of the rows of the identity matrix, and so its determinant is ±1. In particular, h is not identically zero, and so there exists an $\alpha \in E^{\times}$ such that h.$(\sigma_1\alpha,..., \sigma_m \alpha)$ = det$(\sigma_i\sigma_j\alpha)$ is nonzero. We'll show that $\{\sigma_i\alpha\}$is a normal basis. For this, it suffices to show that the $\sigma_i\alpha$ are linearly independent over F . Suppose that

$$\sum\nolimits_{j=1}^{m} a_j\sigma_j\alpha = 0$$

for some $a_j \in F$. On applying $\alpha_1,..., \alpha_m$ successively, we obtain a system of m-equations

$$\sum a_j\sigma_i\sigma_j\alpha = 0$$

in the m "unknowns" a_j . Because this system of equations is non singular, the a_j are zero.This completes the proof of the theorem in the case that F is infinite.

6.6.4 PROOF WHEN G IS CYCLIC.

Assume that G is generated by an element σ_0 of order n. Then .EWF • D n. The minimum polynomial of σ_0 regarded as an endomorphism of the F -vector space E is the monic polynomial in F[X] of least degree such that $P(\sigma_0)$= 0 (as an endomorphism of E). It has the property that it divides every polynomial Q(X) ∈ F [X] such that Q (σ_0)= 0. Since σ_0^n = 1, P(X) divides X_n– 1. On the other hand, Dedekind's theorem on the independenceof characters implies that 1, σ_0,..., σ_0^{n-1} are linearly independent over F , and so deg P(X) > n –1. We conclude that P(X) = X_n – 1. Therefore, as an F (X)-module with X acting as σ_0, E is isomorphic to F [X] =(X_n–1). For any generator α of E as an F [X] -module, α, $\sigma_0\alpha$,..., $\sigma_0\alpha^{n-1}$ is an F -basis for E.

Check your progress

3. Explain **cyclotomic polynomial**

____

____

____

4.State and prove Dedekind's theorem on the independence of characters

____

____

____

6.7 LETS SUM UP

We have discussed various important theorem's like the Primitive element theorem, the Fundamental Theorem of Algebra, Comprehend Dedekind's theorem on the independence of characters and The Normal basis theorem. We seen in details the concept of Cyclotomic extensions

6.8 KEYWORDS

I*dentity element* -or neutral ***element***, is a special type of ***element*** of a set with respect to a binary operation on that set, which leaves any ***element*** of the set unchanged when combined with it.

Non-singular matrix: is a square one whose determinant is not zero

Determinant - In linear **algebra**, the **determinant** is a scalar value that can be computed from the elements of a square **matrix** and encodes certain properties of the linear transformation described by the **matrix**

6.9 QUESTIONS FOR REVIEW

1. For $a \in \mathbb{Q}$, let G_a be the Galois group of $X^4 + X^3 + X^2 + X + a$. Find integers a_1,a_2,a_3,a_4 such that $i \neq j \Rightarrow G_{a_i}$is not isomorphic to G_{a_j}.

2. State and prove the Normal Basis Theorem.

6.10 SUGGESTED READINGS

1. M. Artin, Algebra, Perentice -Hall of India, 1991.
2. P.M. Cohn, Algebra, vols, I,II, & III, John Wiley & Sons, 1982, 1989, 1991.
3. N. Jacobson, Basic Algebra, vols. I & II, W. H. Freeman, 1980 (also published by Hindustan Publishing Company)
4. S. Lang. Algebra, 3rd edn. Addison-Weslley, 1993.
5. I.S. Luther and I.B.S. Passi, Algebra, Vol.III-Modules, Narosa Publishing House.
6. D. S. Malik, J. N. Modrdeson, and M. K. Sen, Fundamentals of Abstract Algebra, McGraw-Hill, International Edition, 1997.
7. VivekSahai and VikasBist, Algebra, Narosa Publishing House, 1999
8. I. Stweart, Galois Theory, 2nd edition, Chapman and Hall, 1989.
9. J.P. Escofier, Galois theory, GTM Vol.204, Springer, 2001.

6.11 ANSWERS TO CHECK YOUR PROGRESS

1. Provide the statement and proof of theorem – 6.2

2. Provide facts – 6.3

3. Provide explanation – 6.4

4. Provide statement and proof of theorem – 6.5

UNIT-7 APPLICATIONS OF GALOIS THEORY II

STRUCTURE

7.0 OBJECTIVES

Comprehend Hilbert’s Theorem 90

Understand the concept of Cyclic extensions

Enumerate Kummer theory and Proof of Galois’s solvability theorem

Understand the concept of Symmetric polynomials

7.1 INTRODUCTION

In this chapter, we continue to apply the fundamental theorem of Galois theory to obtain other results about polynomials and extensions of fields.

7.2 HILBERT’S THEOREM 90

Let G be a group. A G-module is an abelian group M together with an action of G, i.e., a map G × M→M such that

(a) $\sigma(m+m')=\sigma m+\sigma m'$ for all $\sigma\in G,\ m,m'\in M$;
(b) $(\sigma\tau)(m)=\sigma(\tau m)$ for all $\sigma,\tau\in G,\ m\in M$;
(c) $1m=m$ for all $m\in M$.

Thus, to give an action of G on M is the same as giving a homomorphism G → Aut (M) (automorphisms of M as an abelian group).

EXAMPLE Let E be a Galois extension of F with Galois group G. Then (E , +) and ($E^{\times}$) are G-modules.

Let M be a G-module. A crossed homomorphism is a map f : G →M such that

$$f(\sigma\tau)=f(\sigma)+\sigma f(\tau) \text{ for all } \sigma,\tau\in G.$$

Note that the condition implies that f (1) = f (1 . 1) = f (1) + f (1), and so f (1) = 0.

EXAMPLE (a) Let f WG! M be a crossed homomorphism. For any _ 2 G,

$$\begin{aligned}
f(\sigma^2)&=f(\sigma)+\sigma f(\sigma),\\
f(\sigma^3)&=f(\sigma\cdot\sigma^2)=f(\sigma)+\sigma f(\sigma)+\sigma^2 f(\sigma)\\
&\cdots\\
f(\sigma^n)&=f(\sigma)+\sigma f(\sigma)+\cdots+\sigma^{n-1}f(\sigma).
\end{aligned}$$

Thus, if G is a cyclic group of order n generated by σ, then a crossed homomorphism f : G →M is determined by its value, x say, on σ, and x satisfies the equation

$$x + \sigma x + \cdots + \sigma^{n-1} x = 0, \qquad (12)$$

Moreover, if x ∈ M satisfies (12), then the formulas

$$f(\sigma^i) = x + \sigma x + \cdots + \sigma^{i-1} x$$

define acrossed homomorphism f : G → M. Thus, for a finite group G = $\langle\sigma\rangle$, there is a one-to-one correspondence

$$\{\text{crossed homs } f : G \to M\} \overset{f \leftrightarrow f(\sigma)}{\longleftrightarrow} \{x \in M \text{ satisfying } (12)\}.$$

(b) For every x ∈ M, we obtain a crossed homomorphism by putting

$$f(\sigma) = \sigma x - x, \qquad \text{all } \sigma \in G.$$

A crossed homomorphism of this form is called a principal crossed homomorphism.

(c) If G acts trivially on M, i.e.,$\sigma_m =$ m for all σ ∈ G and m ∈ M, then a crossed homomorphism is simply a homomorphism, and there are no non zero principal crossed homomorphisms.

The sum and difference of two crossed homomorphisms is again a crossed homomorphism, and the sum and difference of two principal crossed homomorphisms is again principal. Thus we can define

$$H^1(G, M) = \frac{\{\text{crossed homomorphisms}\}}{\{\text{principal crossed homomorphisms}\}}$$

(quotient abelian group). The cohomology groups $H^n(G, M)$ have been defined for all n ∈ N, but since this was not done until the twentieth century, it will not be discussed in this course. An exact sequence of G-modules

$$0 \to M' \to M \to M'' \to 0$$

gives rise to an exact sequence

$$0 \longrightarrow M'^G \longrightarrow M^G \longrightarrow M''^G \xrightarrow{d} H^1(G, M') \longrightarrow H^1(G, M) \longrightarrow H^1(G, M'').$$

Let m" ∈ M"G, and let m ∈ M map to m". For all σ ∈ G, σ m – m lies in the submodule M' of M, and the crossed homomorphism σ ↦ σm – m : G →M' represents d(m").

EXAMPLE : Let _π: $\tilde{X} \longrightarrow X$ be the universal covering space of a topological space X,and let Γ be the group of covering transformations. Under some fairly general hypotheses, a Γ -module M will define a sheaf $\mathcal{M}$on X, and H^1(X, $\mathcal{M}$) ≃ H^1(Γ; $\mathcal{M}$). For example, when $\mathcal{M}$ = ℤ with the trivial action of Γ , this becomes the isomorphism H^1(X, ℤ) ≃ H^1(Γ , ℤ). Hom(Γ , ℤ)

7.2.1 THEOREM Let E be a Galois extension of F with group G; then H^1(G, E) = 0, i.e.,every crossed homomorphism G → $E^\times$is principal.

PROOF. Let f be a crossed homomorphism G → $E^\times$. In multiplicative notation, this means that

$$f(\sigma\tau) = f(\sigma)\cdot\sigma(f(\tau)), \quad \sigma, \tau \in G,$$

and we have to find a γ ∈ $E^\times$ such that f (σ) = $\frac{\sigma\gamma}{\gamma}$ for all σ ∈ G. Because the f (τ) are nonzero, Corollary 6.5.2 implies that

$$\sum_{\tau \in G} f(\tau)\tau : E \to E$$

is not the zero map, i.e., there exists an α ∈ E such that

$$\beta \overset{\text{def}}{=} \sum_{\tau \in G} f(\tau)\tau\alpha \neq 0.$$

But then, for σ ∈ G,

$$\begin{aligned}\sigma\beta &= \sum\nolimits_{\tau\in G} \sigma(f(\tau))\cdot\sigma\tau(\alpha)\\ &= \sum\nolimits_{\tau\in G} f(\sigma)^{-1}\ f(\sigma\tau)\cdot\sigma\tau(\alpha)\\ &= f(\sigma)^{-1}\sum\nolimits_{\tau\in G} f(\sigma\tau)\sigma\tau(\alpha),\end{aligned}$$

which equals f $(\sigma^{-1})\beta$ because, as τ runs over G, so also does στ.

Therefore, f (σ) = $\frac{\sigma\beta}{(\beta)}$ and we can take β = γ^{-1}.

Let E be a Galois extension of F with Galois group G. We define the norm of an element α ∈ E to be

$$\mathrm{Nm}\alpha = \prod\nolimits_{\sigma\in G}\sigma\alpha.$$

For τ ∈ G,

$$\tau(\mathrm{Nm}\alpha) = \prod\nolimits_{\sigma\in G}\tau\sigma\alpha = \mathrm{Nm}\alpha,$$

and so Nm α ∈ F . The map

$$\alpha \mapsto \mathrm{Nm}\alpha\colon E^{\times} \to F^{\times}$$

is a obviously a homomorphism.

EXAMPLE : The norm map $\mathbb{C}^{\times} \longrightarrow \mathbb{R}^{\times}$ is $\alpha \to |\alpha|^2$ and the norm map $\mathbb{Q}[\sqrt{d}]^{\times} \longrightarrow \mathbb{Q}^{\times}$ is $a+ b\sqrt{d} \mapsto a^2 - db^2$.

We are interested in determining the kernel of the norm map. Clearly an element of the form $\frac{\beta}{\tau\beta}$ has norm 1, and our next result shows that, for cyclic extensions, all elements withorm 1 are of this form.

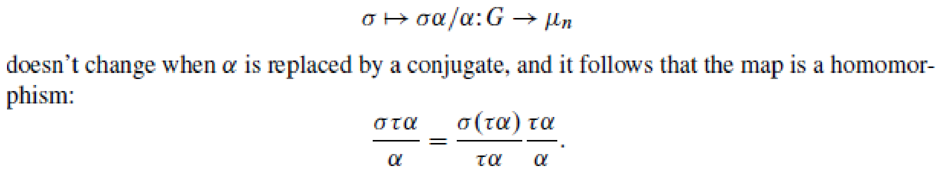
7.2.2 COROLLARY (HILBERT'S THEOREM 90) Let E be a finite cyclic extension of F and let σ generate Gal(E/F). Let α ∈ $E^{\times}$ if Nm $_{E/F}$ α = 1, then α = σβ for some α ∈ E.

PROOF. Let m = [E: F] . The condition on α is that α· σα ... σ^{m-1} α = 1, and so there is a crossed homomorphism f : $\langle\sigma\rangle \rightarrow E^{\times}$ with f (σ) = α Theorem 7.2.1 now shows that *f* is principal, which means that there is a β with f (σ) = $\frac{\beta}{\sigma\beta}$

7.3 CYCLIC EXTENSIONS

Let F be a field containing a primitive nth root of 1, some $n \geq 2$, and write μ_n for the groupof nth roots of 1 in F . Then μ_n is a cyclic subgroup of F^x of order n with generator ς say.In this section, we classify the cyclic extensions of degree *n* of F.

Consider a field E = F[α] generated by an element _ whose nth power (but no smallerpower) is in F. Then α is a root of X^n- *a*, and the remaining roots are the elements $\varsigma^i\alpha$, $1 \leq i \leq n-1$. Since these all lie in E, E is a Galois extension of F, with Galois group G say. For every σ∈G, σα is also a root of X^n -*a*, and so σα = $\varsigma^i\alpha$ for some i . Hence σα/α∈μ_n. The map



$$\sigma \mapsto \sigma\alpha/\alpha : G \rightarrow \mu_n$$

doesn't change when α is replaced by a conjugate, and it follows that the map is a homomorphism:

$$\frac{\sigma\tau\alpha}{\alpha} = \frac{\sigma(\tau\alpha)}{\tau\alpha}\frac{\tau\alpha}{\alpha}.$$

Because α generates E over F , the map is injective. If it is not surjective, then G maps intoa subgroup μ_d of μ_n, some d|*n*, d <*n*. In this case, $(\sigma\alpha/\alpha)^d$ = 1, i.e., $\sigma\alpha^d = \alpha^d$, for all σ∈G, and so α^d ∈ F, contradicting the hypothesis on α. Thus the map is surjective. We have proved the first part of the following statement.

7.3.1 PROPOSITION Let F be a field containing a primitive *n*th root of 1. Let E = F [α]where α^n∈ F and no smaller power of α is in F . Then E is a Galois extension of F withcyclic Galois group of order n. Conversely, if E is a cyclic extension of F of degree n, then E = F[α] for some α with α^{n}∈F .

PROOF. It remains to prove the last statement. Let σ generate G and let ς generate μ^{n}. It suffices to find an element α ∈ $E^{\times}$ such that σα= ς^{-1}α, for then α^{n} is the smallest powerof α lying in F . As 1, σ,....,σ^{n-1} are distinct homomorphisms $F^{\times} \rightarrow F^{\times}$, Dedekind'sTheorem shows that $\sum_{i=0}^{n-1}\varsigma^{i}\sigma^{i}$is not the zero function, and so there exists a γ such that $\alpha \overset{\text{def}}{=} \sum \varsigma^{i}\sigma^{i}\gamma \neq 0$. Now σα= ς^{-1}α.

ASIDE 5.27 (a) It is not difficult to show that the polynomial X^{n}-*a* is irreducible in F[X] if *a* isnot a *p*th power for any prime *p* dividing *n*. When we drop the condition that F contains a primitiventh root of 1, this is still true except that, if 4/*n*, we need to add the condition that *a*∈ - $4F^{4}$.

(b) If F has characteristic *p* (hence has no *p*th roots of 1 other than 1), then X^{p}-X - *a* is irreducible in F[X] unless *a*= b^{p}- b for some b ∈ F , and when it is irreducible, its Galois group iscyclic of order p (generated by α↦α + 1 where α is a root). Moreover, every cyclic extension of F of degree *p* is the splitting field of such a polynomial.

7.3.2 PROPOSITION : Let F be a field containing a primitive *n*th root of 1. Two cyclicextensions $F\left[\alpha\frac{1}{n}\right]\mathit{and}\ F\left[b\frac{1}{n}\right]$of F of degree *n* are equal if and only if $a = b^{r}c^{n}$ for some r ∈ℤ relatively prime to n and some c ∈ $F^{\times}$, i.e., if and only if *a* and *b* generate the samesubgroup of $F^{\times} = F^{\times n}$.

PROOF. Only the "only if" part requires proof. We are given that F[α] = F[α] = F[β] with α^{n}=αand β^{n}=*b*. Let σ be the generator of the Galois group with σα= ςα, and let $\sigma\beta=\varsigma^{i}\beta$,(*i*,n) = 1. We can write

$$\beta = \sum_{j=0}^{n-1} c_j \alpha^j, \quad c_j \in F,$$

and then

$$\sigma\beta = \sum_{j=0}^{n-1} c_j \zeta^j \alpha^j .$$

On comparing this with $\sigma\beta= \varsigma^{i}\beta$, we find that $\varsigma^{j}c_{j}=\varsigma^{j}c_{j}$ for all j . Hence $c_{j}= 0$ forj $\neq i$, and therefore $\beta = c_{i}\alpha^{i}$.

Check your Progress-1

1. Explain principal crossed homomorphism.

____

____

____

2. State and prove HILBERT'S THEOREM 90

____

____

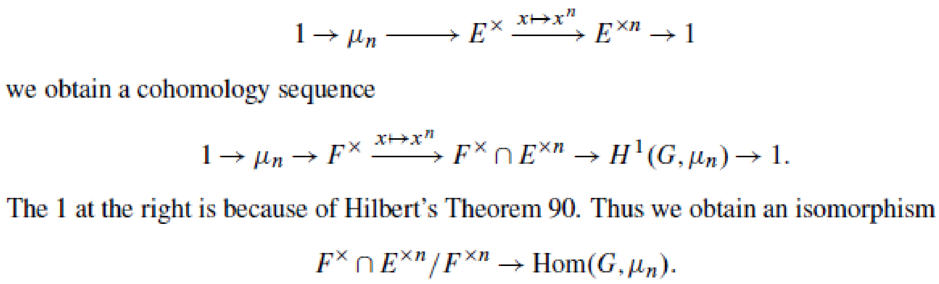
____

7.4 KUMMER THEORY

Throughout this section, *F* is a field and ς is a primitive nth root of 1 in *F* . In particular, F either has characteristic 0 or characteristic *p* not dividing *n*.

The last two proposition give us a complete classification of the cyclic extensions of F of degree *n*. We now extend this to a classification of all abelian extensions of *F* whose Galois group has exponent n. (Recall that a group G has exponent*n* if $\sigma^{n}= 1$ for all σ∈ G and n is the smallest positive integer for which this is true. A finite abelian group of exponent *n* is isomorphic to a subgroup of $(\mathbb{Z}/n\mathbb{Z})^{r}$ for some *r*.)

Let E/F be a finite Galois extension with Galois group G. From the exact sequence



$$1 \to \mu_n \longrightarrow E^{\times} \xrightarrow{x\mapsto x^n} E^{\times n} \to 1$$

we obtain a cohomology sequence

$$1 \to \mu_n \to F^{\times} \xrightarrow{x\mapsto x^n} F^{\times} \cap E^{\times n} \to H^1(G,\mu_n) \to 1.$$

The 1 at the right is because of Hilbert's Theorem 90. Thus we obtain an isomorphism

$$F^{\times} \cap E^{\times n}/F^{\times n} \to \mathrm{Hom}(G,\mu_n).$$

This map can be described as follows: let a be an element of F$^\times$ that becomes an nth powerin E, say a=α^n; then a maps to the homomorphism $\sigma \mapsto \frac{\sigma\alpha}{\alpha}$. If G is abelian of exponentn, then

$$|\mathrm{Hom}(G, \mu_n)| = (G:1).$$

7.4.1 THEOREM : The map

$$E \mapsto F^\times \cap E^{\times n}$$

defines a one-to-one correspondence between the sets

(a) of finite abelian extensions of F of exponent n contained in some fixed algebraic closure Ω of F; and

(b) of subgroups B of F$^\times$ containing F$^{\times n}$ as a subgroup of finite index.

The extension corresponding to B is F$\left[B^{\frac{1}{n}}\right]$, the smallest subfield of Ω containing F and an n$^{\text{th}}$ root of each element of B. If E ↔B, then .[E:F] = (B:F$^{\times n}$).

PROOF. For any finite Galois extension E of F, define B(E) = F$^\times$⋂E$^{\times n}$. Then E ⊃F$\left[B(E)^{\frac{1}{n}}\right]$, and for any group B containing F$^{\times n}$. as a subgroup of finite index, B(F$\left[B^{\frac{1}{n}}\right]$) ⊃ B. Therefore,

$$[E:F] \geq [F[B(E)^{\frac{1}{n}}]:F] = (B(F[B(E)^{\frac{1}{n}}]):F^{\times n}) \geq (B(E):F^{\times n}).$$

If E=F is abelian of exponent n, then [E:F]= (B(E):F$^{\times n}$), and so equalities hold throughout: E = F$\left[B(E)^{\frac{1}{n}}\right]$

Next consider a group B containing F$^{\times n}$ as a subgroup of finite index, and let E =F$\left[B^{\frac{1}{n}}\right]$. Then E is a composite of the extensions F$\left[a^{\frac{1}{n}}\right]$for a running through a set ofgenerators for B/F$^{\times n}$, and so it is a finite abelian extension of exponent n. Therefore

$$a \mapsto \left(\sigma \mapsto \frac{\sigma a^{\frac{1}{n}}}{a^{\frac{1}{n}}}\right): B(E)/F^{\times n} \to \mathrm{Hom}(G, \mu_n), \quad G = \mathrm{Gal}(E/F),$$

is an isomorphism. This map sends B/F$^{\times n}$ isomorphically onto the subgroup Hom(G/H, μ$_n$) of Hom (G,μ$_n$) where H consists of the σ∈ G such that $\in a^{\frac{1}{n}}/a^{\frac{1}{n}}$= 1 for all a∈ B. Butsuch aσ fixes all $a^{\frac{1}{n}}$ for a ∈ B, and therefore is the identity automorphism on E = F$\left[B^{\frac{1}{n}}\right]$. This shows that B(E)= B, and hence E ↦ B(E) and B ↦ F$\left[B^{\frac{1}{n}}\right]$are inverse bijections.

EXAMPLE : (a) The theorem says that the abelian extensions of ℝ of exponent 2 are indexed by the subgroups of ℝ$^{\times}$/=ℝ$^{\times 2}${±1}. This is certainly true.

(b) The theorem says that the finite abelian extensions of ℚ of exponent 2 are indexed by the finite subgroups of ℚ$^{\times}$/ ℚ$^{\times 2}$. Modulo squares, every nonzero rational number has a unique representative of the form $\pm p_1 \ldots p_r$ with the p_i prime numbers. Therefore ℚ$^{\times}$/ ℚ$^{\times 2}$is a direct sum of cyclic groups of order 2 indexed by the prime numbers plus ∞. The extension corresponding to the subgroup generated by the primes $p_1 \ldots p_r$ (and -1) is obtained by adjoining the square roots of $p_1 \ldots p_r$ (and -1) to ℚ.

7.4.3 REMARK :Let E be an abelian extension of F of exponent n, and let

$$B(E) = \{a \in F^{\times} \mid a \text{ becomes an } n\text{th power in } E\}.$$

There is a perfect pairing

$$(a, \sigma) \mapsto \frac{\sigma a^{\frac{1}{n}}}{a^{\frac{1}{n}}}: \frac{B(E)}{F^{\times n}} \times \mathrm{Gal}(E/F) \to \mu_n.$$

for the case n = 2.

7.5 PROOF OF GALOIS'S SOLVABILITY THEOREM

7.5.1 LEMMA :Let $f \in F[X]$ be separable, and let F' be a field containing F . Then the Galois group of f as an element of F'[X] is a subgroup of the Galois group of f as an element of F[X]

PROOF. Let E' be a splitting field for f over F', and let $\alpha_1,\ldots,\alpha_m$ be the roots of f [X] inE'. Then E = F[$\alpha_1,\ldots,\alpha_m$] is a splitting field of f over *F*. Every element of Gal.(E'/F')permutes the α_i and so maps E into itself. The map σ↦σ |E is an injection Gal.(E'/F')→Gal(E/F)

7.5.2 THEOREM : Let F be a field of characteristic 0. A polynomial in F[X] is solvable if and only if its Galois group is solvable.

PROOF.⇐ Let $f \in F[X]$ have solvable Galois group Gf . Let F' = F[ς] where ς is a primitive *n*th root of 1 for some large *n*—for example, *n* = (degf)!will do. The lemma shows that the Galois group G of f as an element of F'[X] is a subgroup of G_f, and hence is also solvable (GT 6.6a). This means that there is a sequence of subgroups

$$G = G_0 \supset G_1 \supset \cdots \supset G_{m-1} \supset G_m = \{1\}$$

such that each G_i is normal in $G_{i-1}$and G_{i-1}/G_i is cyclic. Let E be a splitting field of$f$ [X] over F', and let $F_i = E^{Gi}$. We have a sequence of fields

$$F \subset F[\zeta] = F' = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_m = E$$

with F_i cyclic over F_{i-1}. Theorem 7.3.1 shows that F_i=$F_{i-1}[\alpha_i]$ with $\alpha_i^{[F_i :F_{i-1}]} \in F_{i-1}$,each *i*, and this shows that f is solvable.

⇒It suffices to show that G_f is a quotient of a solvable group (GT 6.6a). Hence itsuffices to find a solvable extension Ẽ of F such that f [X] splits in Ẽ[X].

We are given that there exists a tower of fields

$$F = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_m$$

such that

(a) F$_i$ =F$_{i\text{-}1}$[α$_i$]. α_i^{ri}∈F$_{i\text{-}1}$;
(b) F$_m$ contains a splitting field for *f*:

Let *n*= $r_1 \cdots r_m$, and let *Ω*be a field Galois over F and containing (a copy of) F_m and aprimitive *n*th root ς of 1. For example, choose a primitive element for F_m over *F* and take to be a splitting field of g(X)(X$^{n\text{–}1}$) where g(X) is the minimum polynomial of *γ* over F . Alternatively, Let G be the Galois group of *Ω*F, and let Ẽ be the Galois closure of F_m[ς] in *Ω*. Ẽ is the composite of the fieldsσF_m[ς]σ∈ G, and so it is generated over F by the elements

$$\zeta, \alpha_1, \alpha_2, \ldots, \alpha_m, \sigma\alpha_1, \ldots, \sigma\alpha_m, \sigma'\alpha_1, \ldots .$$

We adjoin these elements to F one by one to get a sequence of fields

$$F \subset F[\zeta] \subset F[\zeta, \alpha_1] \subset \cdots \subset F' \subset F'' \subset \cdots \subset \tilde{E}$$

in which each field F'' is obtained from its predecessor F' by adjoining an *r*th root of an element of F' (*r* = $r_1, \ldots . r_m$, or *n*). According to (5.8) and (5.26), each of these extensions is abelian (and even cyclic after the first), and so Ẽ=F is a solvable extension.

7.6 SYMMETRIC POLYNOMIALS

Let R be a commutative ring .A polynomial P(X$_1$,….,X$_n$) ∈ R[X$_1$,….,X$_n$] is said to be symmetric if it is unchanged when its variables are permuted, i.e., if

$$P(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) = P(X_1, \ldots, X_n), \quad \text{all } \sigma \in S_n.$$

For example

$$\begin{aligned} p_1 &= \textstyle\sum_i X_i && = X_1 + X_2 + \cdots + X_n, \\ p_2 &= \textstyle\sum_{i<j} X_i X_j && = X_1X_2 + X_1X_3 + \cdots + X_1X_n + X_2X_3 + \cdots + X_{n-1}X_n, \\ p_3 &= \textstyle\sum_{i<j<k} X_i X_j X_k, && = X_1X_2X_3 + \cdots \\ &\cdots \\ p_r &= \textstyle\sum_{i_1<\cdots<i_r} X_{i_1} \ldots X_{i_r} \\ &\cdots \\ p_n &= X_1X_2\cdots X_n \end{aligned}$$

are each symmetric because p_r is the sum of all monomials of degree r made up out of distinct X$_i$. These particular polynomials are called the elementary symmetric polynomials.

7.6.1THEOREM (SYMMETRIC POLYNOMIALS THEOREM):
Every symmetric polynomial P(X$_1$,….,X$_n$) in R[X$_1$,….,X$_n$] is equal to a polynomial in the elementary symmetric polynomials with coefficients in R, i.e., P ∈ R[p_1,….,p_n].

PROOF. We define an ordering on the monomials in the X$_i$ by requiring that

$$X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n} > X_1^{j_1} X_2^{j_2} \cdots X_n^{j_n}$$

if either

$$i_1 + i_2 + \cdots + i_n > j_1 + j_2 + \cdots + j_n$$

or equality holds and, for some s,

$$i_1 = j_1, \ \ldots, \ i_s = j_s, \text{ but } i_{s+1} > j_{s+1}.$$

For example,

$$X_1X_2X_3^3 > X_1X_2^2X_3 > X_1X_2X_3^2.$$

Because P is symmetric, it contains all monomials obtained from $X_1^{i_1} \cdots X_1^{i_n}$by permutingthe X. Hence $i_1 \geq$ i$_2 \geq \cdots \geq i_n$.
The highest monomial in p_i is X$_1\cdots$X$_i$, and it follows that the highest monomial in $P_1^{d_i} \cdots P_n^{d_n}$ is

$$X_1^{d_1+d_2+\cdots+d_n} X_2^{d_2+\cdots+d_n} \cdots X_n^{d_n}.$$

Therefore the highest monomial of

$$P(X_1, \ldots, X_n) - c p_1^{i_1-i_2} p_2^{i_2-i_3} \cdots p_n^{i_n}$$

is strictly less than the highest monomial in P(X$_1$,….,X$_n$). We can repeat this argument with the polynomial (14), and after a finite number of steps, we will arrive at a representation of *P* as a polynomial in $p_1,\ldots,p_n$

7.6.2 REMARK : (a) The proof is algorithmic. Consider, for example,

$$\begin{aligned} P(X_1,X_2) &= (X_1+7X_1X_2+X_2)^2 \\ &= X_1^2+2X_1X_2+14X_1^2X_2+X_2^2+14X_1X_2^2+49X_1^2X_2^2. \end{aligned}$$

The highest monomial is $49X_1^2X_2^2$, and so we subtract $49p_2^2$, getting

$$P-49p_2^2 = X_1^2+2X_1X_2+14X_1^2X_2+X_2^2+14X_1X_2^2.$$

Continuing, we get

$$P-49p_2^2-14p_1p_2 = X_1^2+2X_1X_2+X_2^2$$

and finally,

$$P-49p_2^2-14p_1p_2-p_1^2=0.$$

(b) The expression of *P* as a polynomial in the p_i in (5.35) is unique. Otherwise, bysubtracting, we would get a nontrivial polynomial *Q*.($p_1,\ldots,p_n$) in the p_i which is zerowhen expressed as a polynomial in the X$_i$. But the highest monomials (13) in the polynomials$P_1^{d_i}\cdots P_n^{d_n}$ are distinct (the map $(d_1,\ldots,d_n)\to(d_1+\cdots+d_n,\ldots,d_n)$ is injective), and so they can't cancel.

Let

$$f(X)=X^n+a_1X^{n-1}+\cdots+a_n\in R[X],$$

and suppose that f splits over some ring S containing R:

$$f(X)=\textstyle\prod_{i=1}^n(X-\alpha_i),\quad \alpha_i\in S.$$

Then

$$a_1=-p_1(\alpha_1,\ldots,\alpha_n),\quad a_2=p_2(\alpha_1,\ldots,\alpha_n),\quad \ldots,\quad a_n=(-1)^np_n(\alpha_1,\ldots,\alpha_n).$$

Thus the elementary symmetric polynomials in the roots of *f* (*X*) lie in R, and so the theorem implies that every symmetric polynomial in the roots of *f* (*X*) lies in R. For example, the discriminant

$$D(f) = \prod_{i<j}(\alpha_i - \alpha_j)^2$$

of f lies in R.

7.6.3THEOREM 5.37 (SYMMETRIC FUNCTIONS THEOREM) Let F be a field. When S_n acts on F($X_1,\ldots.,X_n$) by permuting the X_i , the field of invariants is F($p_1,\ldots.,p_n$)

PROOF. Let f ∈ F($X_1,\ldots.,X_n$)be symmetric (i.e., fixed by Sn). Set f = g/h, g,h∈F[$X_1,\ldots.,X_n$]. The polynomials H =$\prod_{\sigma \epsilon S_n} \sigma h$ and *Hf* are symmetric, and therefore liein F [$p_1,\ldots.,p_n$] by 5.35. Hence their quotient *f*=*Hf* /H lies in F($p_1,\ldots.,p_n$).

7.6.4 COROLLARY : The field F($X_1,\ldots.,X_n$) is Galois over F($p_1,\ldots.,p_n$) with Galois groupS_n (acting by permuting the X_i).

PROOF. We have shown that F($p_1,\ldots.,p_n$) = F($X_1,\ldots.,X_n$)^{Sn}, and so this follows

The field F($X_1,\ldots.,X_n$) is the splitting field over F($p_1,\ldots.,p_n$) of

$$g(T) = (T - X_1)\cdots(T - X_n) = X^n - p_1X^{n-1} + \cdots + (-1)^n p_n.$$

Therefore, the Galois group of g(T)∈ F($p_1,\ldots.,p_n$)[T] is S_n.

Check your Progress-2

3. Provide Galois's solvability theorem

____

____

____

4. State and prove SYMMETRIC FUNCTIONS THEOREM

____

____

____

7.7 LETS SUM UP

We have discussed the application of Galois theory like Comprehend Hilbert’s Theorem 90, Enumerate Kummer theory and Proof of Galois’s solvability theorem. We have discussed various concepts like Cyclic extensions and Symmetric polynomials

7.8 KEYWORDS

Solvable extension: a field **extension** whose Galois group is a **solvable** group

Subgroup - A **subgroup** of a group G is a **subset** of G that forms a group with the same law of composition

7.9 QUESTIONS FOR REVIEW

1. Prove that the rational solutions a ,b ∈ ℚ of Pythagoras’s equation a^2 + b^2 = 1 are of
the form

$$a = \frac{s^2 - t^2}{s^2 + t^2}, \quad b = \frac{2st}{s^2 + t^2}, \qquad s, t \in \mathbb{Q},$$

and deduce that every right triangle with integer sides has sides of length

$$d(m^2 - n^2, 2mn, m^2 + n^2)$$

for some integers d, m, and n (Hint: Apply Hilbert’s Theorem 90 to the extension ℚ [i]/ℚ.)

2. Explain Kummer theory

7.10 SUGGESTED READINGS

1. M. Artin, Algebra, Perentice -Hall of India, 1991.
2. P.M. Cohn, Algebra, vols, I,II, & III, John Wiley & Sons, 1982, 1989, 1991.
3. N. Jacobson, Basic Algebra, vols. I & II, W. H. Freeman, 1980 (also published by Hindustan Publishing Company)
4. S. Lang. Algebra, 3rd edn. Addison-Weslley, 1993.
5. I.S. Luther and I.B.S. Passi, Algebra, Vol.III-Modules, Narosa Publishing House.
6. D. S. Malik, J. N. Modrdeson, and M. K. Sen, Fundamentals of Abstract Algebra, McGraw-Hill, International Edition, 1997.
7. VivekSahai and VikasBist, Algebra, Narosa Publishing House, 1999
8. I. Stweart, Galois Theory, 2nd edition, Chapman and Hall, 1989.
9. J.P. Escofier, Galois theory, GTM Vol.204, Springer, 2001.

7.11 ANSWERS TO CHECK YOUR PROGRESS

1. Provide the explanation and example – 7.2

2. Provide statement and proof of theorem – 7.2.1 & 7.2.2

3. Provide statement of Lemma and theorem – 7.5.1 & 7.5.2

4. Provide statement and proof of theorem – 7.6.3