DIRECTORATE OF DISTANCE EDUCATION

UNIVERSITY OF NORTH BENGAL

MASTER OF SCIENCES- MATHEMATICS

SEMESTER -IV

FIELD EXTENSION AND GALOIS THEORY

DEMATH4ELEC5

BLOCK-2

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-I

BLOCK-2

BLOCK-2 FIELD EXTENSION AND GALOIS THEORY

The main questions of ruler and compass constructions left unanswered by the ancient Greeks, such as whether an arbitrary angle can be trisected, are resolved. We combine analytic and algebraic arguments to prove the transcendence of π and e. we prove that no algebraic formula exists for the roots of an arbitrary polynomial of degree 5 or larger. In order to prove an analog of the fundamental theorem for infinite extensions, we need to put a topology on the Galois group. It is through this topology that we can determine which subgroups show up in the correspondence between sub extensions of a Galois extension and subgroups of the Galois group. The latter topic, among other things, allows us to extend to arbitrary extensions the idea of separability. The remaining sections of this chapter introduce some of the most basic ideas of algebraic geometry and show the connections between algebraic geometry and field theory, notably the theory of finitely generated non algebraic extensions.

UNIT-8 TRANSCENDENTAL EXTENSIONS

STRUCTURE

8.0 OBJECTIVES

Understand the Algebraic independence and Transcendence bases

Enumerate Luroth's theorem

How to Separating transcendence bases

Understand the Transcendental Galois Theory

8.1 INTRODUCTION

In this chapter we consider fields $\Omega \supset F$ with Ω much bigger than F. For example we could have $\mathbb{C} \supset \mathbb{Q}$

8.2 ALGEBRAIC INDEPENDENCE

Elements $\alpha_1, \ldots, \alpha_n$ of Ω give rise to an F – homomorphism

$$f \mapsto f(\alpha_1, \ldots, \alpha_n) : F[X_1, \ldots, X_n] \to \Omega$$

If the Kernel of this homomorphism is zero, then the α_i are said to be algebraically independent over F. and otherwise, they are algebraically dependent over F. Thus, the α_i are algebraically dependent over F if there exists a nonzero polynomial $f(X_1, \ldots, X_n) \epsilon F[X_1, \ldots, X_n]$ such that $f(\alpha_1, \ldots, \alpha_n) = 0$ and they are algebraically independent if

$$a_{i_1,\ldots,i_n} \epsilon F, \quad \sum a_{i_1,\ldots,i_n} \alpha_1^{i_1} \ldots \alpha_n^{i_1} = 0 \Rightarrow a_{i_1,\ldots,i_n} = 0 \; all \; i_1, \ldots, i_n$$

Note the similarity with linear independence. In fact, if f is required to be homogeneous of degree 1, then the definition becomes that of linear independence

Example:

(a) A single element α is algebraically independent over F if and only if it is transcendental over F

(b) The complex number π and e are almost certainty algebraically independent over $\mathbb{Q}$. But this has not been proved

An infinite set A is **algebraically independent** over F if every finite subset of A is **algebraically independent** ; otherwise, it is algebraically dependent over F

8.2.1 Remark: If $\alpha_1, \ldots, \alpha_n$ are algebraically independent over F, then the map

$$f(X_1, \ldots, X_n) \mapsto f(\alpha_1, \ldots, \alpha_n) : F[X_1, \ldots, X_n] \to \mathrm{F}[\alpha_1, \ldots, \alpha_n]$$

Is an injection, and hence an isomorphism. This isomorphism then extends to the field of fractions

$$X_i \mapsto \alpha_i : F[X_1, \ldots, X_n] \to \mathrm{F}[\alpha_1, \ldots, \alpha_n]$$

In this case, $F(\alpha_1, \ldots, \alpha_n)$is called a pure transcendental extension of F. The polynomial

$$f(X) = X^n - \alpha_1 X^{n-1} + \ldots + (-1)^n \alpha_n$$

Has Galois group $S_n$over $F(\alpha_1, \ldots, \alpha_n)$.

8.2.2 LEMMA : Let $\gamma \epsilon\ \Omega$ and let $A\ \subset\ \Omega$ the following conditions are equivalent:

(a) γ is algebraic over F(A):

(b) there exists $\beta_1, \ldots, \beta_n\ \in F(A)$ such that $\gamma^n + \beta_1\gamma^{n-1} + \cdots + \beta_n = 0$

(c) there exists $\beta_0, \beta_1, \ldots, \beta_n\ \in F(A)$, not all 0 such that $\beta_0\gamma^n + \beta_1\gamma^{n-1} + \ldots + \beta_n = 0$;

(d) there exists an $f(X_1, \ldots, X_m, Y)\ \in F\ [X_1, \ldots, X_m, Y]\ and\ \alpha_1, \ldots, \alpha_m\ \in A$ such that $f\left(\alpha_1, \ldots, \alpha_{m,} Y\right) \neq 0$ but $f\left(\alpha_1, \ldots, \alpha_{m,} \gamma\right) = 0$

Proof:$(a) \Longrightarrow (b) \Longrightarrow (c) \Longrightarrow$ are obvious

$(d) \Longrightarrow (c)$. Write $f\ (X_1, \ldots X_m, Y)$ as a polynomial in Y with coefficients in the ring $F\ [X_1, \ldots, X_m,]$

$$f\ (X_1, \ldots X_m, Y) = \sum f_i(X_1, \ldots, X_m)Y^{n-i}$$

Then (c) holds with $\beta_i = f_i\ (\alpha_1, \ldots, \alpha_m)$

$(c) \Longrightarrow (d)$ The β_i in (c) can be expressed as polynomials in a finite number of elements $\alpha_1, \ldots, \alpha_m$ of A, says $\beta_i = f_i\ (\alpha_1, \ldots, \alpha_m)\ with\ f_i\ \in F\ [X_1, \ldots X_m]$. Then (d) holds with $f = \sum f_i(X_1, \ldots, X_m)Y^{n-i}$

8.2.3 Definition: When γ satisfies the equivalent condition of Lemma 9.3, it is said to be algebraically dependent on A (over F). A and B is algebraically dependent on A if each element B is algebraically dependent on A

The theory in the remainder of this chapter is logically very similar to a part of linear algebra. It is useful to keep the following correspondences in mind:

Linear algebra	Transcendence
Linearly independent	Algebraically independent
A ⊂ span(B)	A algebraically dependent on B
Basis	Transcendence basis

Dimension	Transcendence degree

8.3 TRANSCENDENCE BASES

8.3.1 Theorem: (FUNDAMENTAL RESULT) Let $A = \{\alpha_1, \dots, \alpha_m\}$ and B = $\{\beta_1, \dots, \beta_n\}$be two subsets of Ω. Assume

(a) A is algebraically independent (over F)

(b) A is algebraically dependent on B (over F)

Then $m \leq n$.

We first prove two lemmas

8.3.2 LEMMA: (THE EXCHANGE PROPERTY): Let $\{\alpha_1, \dots, \alpha_m\}$ be a subset of Ω; if β is algebraically dependent on $\{\alpha_1, \dots, \alpha_m\}$ but not on $\{\alpha_1, \dots, \alpha_{m-1}\}$, then α_m is algebraically dependent on $\{\alpha_1, \dots, \alpha_{m-1}, \beta\}$.

Proof: Because β is algebraically dependent on $\{\alpha_1, \dots, \alpha_m\}$ there exists a polynomial $f\ (X_1, \dots X_m, Y)$ with coefficient in F such that

Write f as a polynomial in X_m

$$f\ (X_1, \dots X_m, Y) = \sum_i a_i(X_1, \dots, X_{m-1}, Y)X_m^{n-i}$$

And observe that because $(X_1, \dots, X_{m-1}, Y) \neq 0$, at least one of the polynomials

$\alpha_i(\alpha_1, \dots, \alpha_{m-1}, Y)$

Say $a_{i_{0,}}$ *is* not the zero polynomial. Because β is not algebraically dependent on

$\{\alpha_1, \dots, \alpha_{m-1}\}$,

$a_{i_{0,}}(\alpha_1, \dots, \alpha_{m-1}, \beta) \neq 0$ Therefore, $f\ (\alpha_1, \dots, \alpha_{m-1}, \beta) \neq 0$ Since $f\ (\alpha_1, \dots, \alpha_m, \beta) = 0$, this shows that α_m is algebraically dependent on $\{\alpha_1, \dots, \alpha_{m-1}, \beta\}$.

8.3.3 LEMMA (TRANSIVITY OF ALEBRAIC DEPENDENCE) If C is algebraically dependent on B, and B is algebraically dependent on A, then C is algebraically dependent on A.

PROOF: The argument in the proof of Proposition shows that if γ is algebraically over a field E which is algebraic over a field F, then γ is algebraic over F (if $a_1, \ldots, a_n$ are the coefficients of the minimum polynomial of γ over E, then the field F $[a_1, \ldots, a_n, \gamma)$ has finite degree over F) Apply this with E = A (A ∪ B) and F = F(A)

PROOF (OF THEOREM 8.3.1): Let k be the number of elements that A and B have in common. If $k = m$ then $A \subset B$ and certainly $m \leq n$ suppose that $k < m$, and write B = $\{\alpha_1, \ldots, \alpha_k, \beta_{k+1}, \ldots, \beta_n\}$ since α_{k+1} is algebraically dependent on $\{\alpha_1, \ldots, \alpha_k, \beta_{k+1}, \ldots, \beta_n\}$ but not on $\{\alpha_1, \ldots, \alpha_k\}$, there will be a $\beta_j, k+1 \leq j \leq n$, such that α_{k+1} is algebraically dependent on $\{\alpha_1, \ldots, \alpha_k, \beta_{k+1}, \ldots, \beta_j\}$ but not

$$\{\alpha_1, \ldots, \alpha_k, \beta_{k+1}, \ldots, \beta_{j-1}\}$$

The exchange lemma then shows that β_j is algebraically dependent on

$$B_1 \stackrel{\text{def}}{=} B \cup \{\alpha_{k+1}\} \setminus \{\beta_j\}$$

Therefore B is algebraically dependent on B_1, so A is algebraically dependent on B_1(by 9.7). If $k + 1 < m$, repeat the argument with A and B_1. Eventually we'll achieve $k = m$, and $m \leq n$

8.3.4 Definition: A **transcendence basis** for Ω over F is an algebraically independent set A such that Ω is algebraically over F(A)

8.3.5 LEMMA : If Ω is algebraic over F(A), and A is minimal among subsets of Ω with this property, then it is a transcendence basis for Ω over F

PROOF: If A is not algebraically independent, then there is an $\alpha \epsilon A$ that is algebraically dependent on A $\setminus \{\alpha\}$. It follows from Lemma 9.7 that Ω is algebraic over F(A $\setminus \{\alpha\}$)

8.3.6 THEOREM: If there is a finite subset A ⊂ Ω such that Ω is algebraic over F (A), then Ω has a finite transcendence basis over F.

Moreover, every transcendence basis is finite, and they all have the same number of elements.

PROOF: In fact, every minimal subset A' of A such that Ω is alebraic over $F(A')$ will be a transcendence basis. The second statement follows from Theorem 8.3.1

8.3.7 LEMMA: Suppose that A is algebraically independent, but that $A \cup \{\beta\}$ is algebraically dependent. Then β is algebraic over F(A)

PROOF: The hypothesis is that there exists is nonzero polynomial

$$f\ (X_1, \dots X_n, Y)\ \in F\ f\ (X_1, \dots X_n, Y)$$

Such that $f\ (\alpha_1, \dots, \alpha_n, \beta) = 0$ some distinct$\alpha_1, \dots, \alpha_n\ \in A$. Because A is algebraically independent, Y does occur in f. Therefore

$$f = g_0 Y^m + g_1 Y^{m-1} + \cdots + g_m, \qquad g_i \in F\ [X_1, \dots X_n],$$
$$g_0 \neq 0\ , m \geq 1$$

As $g_0 \neq 0$ and the $\alpha_i$are algebraically independent, $g_0\,(\alpha_1, \dots, \alpha_n) \neq 0$ Because β is a root of

$$f = g_0\,(\alpha_1, \dots, \alpha_n) X^m + g_1(\alpha_1, \dots, \alpha_n) X^m + \dots + g_m(\alpha_1, \dots, \alpha_n)$$

It is algebraic over $F(\alpha_1, \dots, \alpha_n\ \subset F(A)$

8.3.8 PROPOSITION: Every maximal algebraically independent subset of Ω over F.

PROOF: We have to prove that Ω is algebraic over F(A). If A is maximal among algebraically independent subsets. But the maximality implies that, for every $\beta \epsilon$ Ω \ A. A ∪{β}is algebraically dependent, and so the lemma shows that β is algebraic over F(A)

Recall that (except in δ7), We use an asterisk to signal a result depending on Zorn's lemma

8.3.9 THEOREM: Every algebraically independent subset of Ω is contained in a transcendence basis for Ω over F; in particular, transcendence bases exist.

PROOF: Let S be the set of algebraically independent subsets of

Ω containing the given set. We can partially order it by inclusion. Let T be a totally ordered subsets of S, and let B = $\cup\{A|A \epsilon T\}$ I claim that $B \epsilon S$, i.e. that B is algebraically independent. If not, there exists a finite subset B' of B that is not algebraically independent. But such a subset will be contained in one of the sets in T, which is a contradiction. Now Zorn's lemma shows that there exists a maximal algebraically independent containing S, which Proposition 9.12 shows to be a transcendence basis for Ω over F.

It is possible to show that any two (possible infinite) transcendence bases for Ω over F have the same cardinality. The cardinality of a transcendence basis for Ω over F is called the transcendence degree of Ω over F. For example, the pure transcendental extension $F\ (X_1, \dots, X_n)$has transcendence degree n over F

EXAMPLE: Let $p_1, \dots, p_n$ be the elementary symmetric polynomials in $X_1, \dots, X_n$. The field F$(X_1, \dots, X_n)$ is algebraic over F $(p_1, \dots, p_n)$ and so $\{p_1, p_2, \dots, p_n\}$ contains a transcendence basis of F$(X_1, \dots, X_n)$ because F$(X_1, \dots, X_n)$ has transcendence degree n, the $p_i's$ must themselves be a transcendence basis

EXAMPLE: Let Ω be the field of meromorphic functions on a compact complex manifold M

(a) The only meromorphic functions on the Riemann sphere are the rational functions in z. Hence, in this case Ω is a pure transcendental extension of ℂ of transcendence degree 1.

(b) If M is a Riemann surface, then the transcendence degree of Ω over ℂ is 1, and Ω is a pure transcendental extension of ℂ $\Leftrightarrow M$ is isomorphic to the Riemann sphere

(c) If M has complex dimension n, then the transcendence degree is $\leq n$, with equality holding if M is embeddable in some projective space.

8.3.10 PROPOSITION: Any two algebraically closed fields with the same transcendence degree of F and F – isomorphic

PROOF: Choose transcendence bases A and A' for the two fields. By assumptions, there exists a bijection $A \rightarrow A'$. Which extends uniquely to an F- isomorphism $F[A] \rightarrow F[A']$, and hence to an F- isomorphism of the fields of fractions $F(A) \rightarrow F([A'])$, Then the two fields in question are algebraic closures of the same field. And hence are isomorphic.

8.3.11 REMARK : Any two algebraically closed field with the same uncountable cardinality and the same characteristics are isomorphic. The idea of the proof is as follows. Let F and F' be the prime subfields of Ω and Ω'; we can identify F and F'. Then show that when Ω is uncountable the cardinality of Ω is the same as the cardinality of a transcendence basis over F. Finally, apply the proposition.

8.3.12 REMARK: What are the automorphisms of ℂ? There are only two continuous automorphisms (cf. Exercise A – 8 and solution). If we assume Zorn's lemma, then it is easy to construct many: choose any transcendence basis A for ℂ over ℚ, and choose any permutation α of A; then α defines an isomorphism $\mathbb{Q}(A) \rightarrow \mathbb{Q}(A)$ that can be extended to an automorphism of ℂ. Without Zorn's lemma, there are only two, because the noncontinuous automorphisms are non-measurable, $\frac{1}{2}$ and it is known that the Zorn's lemma is required to construct non-measurable functions

Check your Progress-1

1. Define algebraically dependent

____
____
____

2. State and prove the Exchange Property

____
____
____

8.4 LÜROTH'S THEOREM

8.4.1THEOREM (LÜROTH): Let L = F(X) with X transcendental over F. Every subfield E of L properly containing F is of the form E = $F(u)$ for some $u \epsilon L$ transcendental over F.

We first sketch a geometric proof of Lüroth's theorem. The inclusion of E into L corresponds to a map from the projective line $\mathbb{P}^1$. Onto a complete regular curve C. Now the Riemann – Hurwitz formula shows that C has genus 0. Since it has an F – rational point (the image of any F – rational point of $\mathbb{P}^1$), it is isomorphic to $\mathbb{P}^1$. Therefore E = $F(u)$ for some $u \epsilon L$ transcendental over F.

Before giving the elementary proof, we review Gauss's lemma and its consequences.

8.4.2 GAUSS'S LEMMA:

Let R be a unique factorization domain. And let Q be its field of fraction, for example, R = F[X] and Q = F[X] A polynomial $f(T) = \sum a_i T^i$ in R[T] is said to be primitive if its coefficients a_i have no common factor other than units. Every polynomial f in Q[X] can be written $f = c(f).f_1$ with $c(f) \in Q$ and f_1 primitive (write $f = af/a$ with a a common denominator for the coefficients of f, and then write $f = (b/a)\, f_1$ with b the greatest common divisor of the coefficients of $a\,f$). The element $c(f)$ is uniquely determined up to a unit, and $f \in R[X]$ if and only if $c(f) \in R$:

8.4.3 If f, g $\in R\,[T]$ are primitive, so also is fg

Let $f = \sum a_i T^i$ and g = $\sum b_i T^i$ let p be a prime element of R. Because f is primitive, there exists a coefficient $a_i$not divisible by p - let a_{i_1}be the first such coefficient. Similarly, let b_{i_2}be the first coefficient of g not divisible by p then the coefficient of $T^{i_1+i_2}$ in fg is not divisible by p This shows that fg is primitive

8.4.4 : for any f, g $\in$ R[T], c (fg) = c (f)c(g) and $(fg)_1 = f_1 g_1$

Let $f = c\,(f) f_1$ and g = c(g) g_1 with f_1 and g_1 primitive. Then fg = $c(f)c\, f_1 g_1$ with $f_1 g_1$ primitive, and so $f(f$g) = c(f)c(g) and $(fg)_1 = f_1 g_1$

8.4.5 : Let f be a polynomial in R[T]. If f factors into the product of two non-constant polynomials in Q[T], then it factors into the product of two non-constant polynomials in R[T]

Suppose that $f = gh$ in Q[T] then $f_1 = g_1 h_1$ in R[T], so if $f = c(f).f_1 = (c(f).g_1)\, h_1$ with $c(f).g_1$ and h_1 in R[T]

8.4.6 : Let f, g $\in R[T]$. If f divides g in Q[T] and f is primitive, then it divides g in R[T]

Let $fq =$ g with $q \in Q[T]$. Then $c(q) = c(\text{g}) \in R$ and so $q \in R[T]$

PROOF OF LÜROTH'S THEOREM:

We define the degree deg (u) of an element u of $F(X)$ to be the larger of the degrees of the numerator and denominator of u when it is expressed in its simplest form.

8.4.7 LEMMA: Let $u \in F(X) \setminus F$ Then u is transcendental over F, X is algebraic over $F(u)$, and [F(X) : F(u)] = deg(u)

PROOF: Let $u(X) = a(X)/b(X)$ with $a(X)$ and $b(X)$ relatively prime polynomials. Now $a(T) - b(T)u \in F(u)[T]$, and it has X as a root, and so X is algebraic over $F(u)$. It follows that u is transcendental over F.

The polynomial $a(T) - b(T)Z \in F[Z,T]$ is clearly irreducible. As u is transcendental over F

$$F[Z,T] \simeq F[u,T], Z \leftrightarrow u, \qquad T \leftrightarrow T$$

And so $a(T) - b(T)u$ is irreducible in $F[u,T]$, and hence also in $F(u)[T]$ by Gauss's lemma (8.4.5). It has X as a root, and so, up to a constant, it is the minimum polynomial of X over $F(u)$, and its degree is $\deg(u)$, which proves the lemma

EXAMPLE: We have F(X) = $F(u)$ if and if

$$u = \frac{aX + b}{cX + d}$$

With $ac \neq 0$ and neither $aX + b$ nor $cX + d$ a constant multiple of the other These conditions are equivalent to $ad - bc \neq 0$

We know prove Theorem **8.4.1**: Let u be an element of E not in F. Then

$$[F(X): E] \leq [F(X): F(u)] = \deg(u)$$

And so X is algebraic over E. Let

$f(T) = T^n + a_1T^{n-1} + \cdots + a_n, a_i \in E,$

Be its minimum polynomial. As X is transcendental over F. Some $a_j \notin F$, and we'll show that E = $F(a_j)$

Let $d(X) \epsilon F([X]$ be a polynomial of least degree such that $d(X)a_i(X) \in F[X]$ for all i, and let

$$f_1(X,T) = df(T) = dT^n + da_1T^{n-1} + \cdots + da_n \in F[X,T].$$

Then f_1 is primitive as a polynomial in T, i.e. , $\gcd(d, da_1, \ldots, da_n) = 1$ in F[X]. The degree m of f_1 in X is the largest degree of one of the polynomials $da_1da_2, \ldots.$, say $m = \deg(da_i)$. Write $a_i = b/c$ with b, c relatively prime polynomials in F[X]. Now $b(T) - c(T)a_i(X)$ is a polynomial in $E[T]$ having X as a root, and so it is divisible by f, say

$$f(T).q(T) = b(T) - c(T).a_i(X), \qquad q(T) \in E[T]$$

On multiplying through by $c(X)$, we find that

$$c(X).f(T).q(T) = c(X).b(T) - c(T).b(X)$$

As f_1 differs from f by a non zero element of $F(X)$, the equation shows that f_1 divides $c(X).b(T) - c(T).b(X)$ in F(X)[T]. But f_1 is primitive in $F[X][T]$, and so it divides $c(X).b(T) - c(T).b(X)$ in $F[X][T] = F[X,T]$ (by 8.4.6), i.e., there exists a polynomial $h \in F[X,T]$ such that

$$f_1(X,T).h(X,T) = C(X).b(T) - c(T).b(X)$$

In (18), the polynomial c(X).b(T) – c(T).b(X)has degree at most m in X, and m is the degree of $f_1(X,T)$ in X. Therefore, $c(X).b(T) - c(T).b(X)$ has degree exactly m in X, and $h(X,T)$has degree 0 in X i.e. $h \in F[T]$ It now follows from that $c(X).b(T) - c(T).b(X)$ is not divisible by a nonconstant polynomial in F[X]

The polynomial $c(X).b(T) - c(T).b(X)$ is symmetric in X and T, i.e., it is unchanged when they are swapped. Therefore, it has degree m and T and it is not divisible by a non constant polynomial in F[T]. It now follows from (18) that h is not divisible by a non constant polynomial in F[T], and so it lies in $F^{\times}$. We conclude that $f_1\,(X,T)$ is a constant multiple of $c(X).b(T) - c(T).b(X)$.

On comparing degrees in T we see that $n = m$ Thus

$$[F(X): F(a_i)]^{9.24} \deg(a_i) \leq \deg(da_i) = m = n = [F(X): E] \leq [F(X): F(a_i)]$$

Hence, equality holds throughout, and so E = $F[a_i]$

Finally, if $a_j \notin F$, then

[F(X): E] $\leq [F(X): F(a_j)^{9.24} \deg(a_j) \leq \deg(da_j) \leq \deg(da_i) = m = [F(X): E]$

And So $E = F(a_j)$ as claimed

8.4.4 REMARK: Lüroth’s theorem fails when there is more than one variable – see Zariski’s example and Swan’s example. However, the following is true: if [F (X, Y): E] $< \infty$ and F is algebraically closed of characteristic zero, then E is a pure transcendental extension of F (Theorem of Zariski, 1958)

NOTES: Lüroth proved this theorem over $\mathbb{C}$ in 1876. For general fields, it was proved by Steinitz in 1910, by the above argument.

8.5 SEPARATING TRANSCENDENCE BASES

Let $E \supset F$ be fields with E finitely generated over F. A subset $\{x_1, \ldots, x_d)$ of E is a separating transcendence basis for E/F if it is algebraically independent over F and E is a finite separable extension of F$(x_1, \ldots, x_d)$

8.5.1 THEOREM: If F is perfect, then every finitely generated extension E and F admits a separating transcendence basis over F.

PROOF: If F has characteristic zero, then every transcendence basis is separating, and so the statement becomes that of (9.10). Thus, we may assume F has characteristic $p \neq 0$. Because F is perfect, every polynomial in $X_1^p, \ldots, X_n^p$ with coefficients in F is a pth power in $F[X_1, \ldots, X_n]$:

$$\sum a_{i_1} \ldots\ i_n X_1^{i_1 p} \ldots X_n^{i_1 p} = \left(\sum a_{i_1 \ldots i_n}^{\frac{1}{p}} X_1^{i_1}\right)^P.$$

Let$E = F(x_1, \ldots., x + 1_n)$, and assume $n > d + 1$ where d is the transcendence degree of E over F. After renumbering, we may suppose that $x_1, \ldots, x_d$ are algebraically independent (9.9). Then $f(x_1, \ldots, x_{d+1}) = 0$ for some non zero irreducible polynomial $f(X_1, \ldots, X_{d+1})$ with coefficients in F. Not all $\partial f / \partial X_{d+1}$are zero, for otherwise f would be a polynomial in $X_1^p, \ldots, X_{d+1}^p$ which implies that it is a p the power. After renumbering $x_1, \ldots x_{d+1}$, we may suppose that $\partial f / \partial X_{d+1} \neq 0$ Then x_{d+1} is separately algebraic over F $(x_1, \ldots x_d)$ and $F(x_1, \ldots x_{d+1}, x_{d+2})$ is algebraic over F $(x_1, \ldots x_{d+1})$ hence over F $(x_1, \ldots x_d)$ (1.31) and so, by the primitive element theorem (5.1), there is an element y such that $F(x_1, \ldots, x_{d+2}) = F(x_1, \ldots x_d, y)$.Thus E is generated by $n - 1$ elements (as a field) containing F). After repeating process, possibly several times, we will have E = $F(z_1, \ldots\ z_{d+1})$ with z_{d+1} separable over $F(z_1, \ldots, z_d)$

ASIDE: In fact, we showed that E admits a separating transcendence basis with $d+1$ elements where d is the transcendence degree. This has the following geometric interpretation: every irreducible algebraic variety of dimension d over a perfect field F is birationally equivalent with a hypersurface H in $\mathbb{A}^{d+1}$ for which the projection $(a_1, \ldots, a_{d+1}) \longmapsto (a_1, \ldots, a_d)$ realizes $F(H)$ as a finite separable extension of F($\mathbb{A}^d$) (See my notes on Algebraic Geometry).

8.6 TRANSCENDENTAL GALOIS THEORY

8.6.1 THEOREM: Let Ω be an algebraically closed field and let F be a perfect subfield of Ω. If $\alpha \in$ Ω is fixed by all F – automorphisms of Ω, then $\alpha \in$ F, i.e $\Omega^{Aut(\Omega/\mathrm{F})} = F$

PROOF: Let $\alpha \in \Omega \setminus$ F. If α is algebraic over F, then there is an F – homomorphism F[∝] → Ω sending α to a conjugate of α in Ω in different from α. This homomorphism extends to a homomorphism from the algebraic closure F^{al} of F in Ω to Ω (by 6.8). Now choose a transcendence basis A for Ω over F^{al}. We can extend our homomorphism to a homomorphism F(A) → Ω by mapping each element of A to itself. Finally, we can extend this homomorphism to a homomorphism from the algebraic closure Ω of F(A) to Ω, The F - homomorphism Ω → Ω we obtain is automatically an isomorphism (cf 6.8)

If α is transcendental over F, then it is part of a transcendence basis A for Ω over F. If A has at least two elements, then there exists an automorphism σ of A such that $\sigma(\alpha) \neq \alpha$ Now σ defines an F - homomorphism F(A) → Ω which extends to an isomorphism Ω → Ω as before. If A = $\{\alpha\}$, then we let F(α) → Ω be in F – homomorphism sending α to $\alpha + 1$. Again, this extends to an isomorphism Ω → Ω.

Let $\Omega \supset F$ be fields and G = Aut$(\Omega/$F) For any finite subset S of Ω., let

$$G(S) = \{\sigma \in G \mid \sigma s = s \text{ for all } s \in S\}$$

Notes

Then, as in §7, the subgroups G(S) of G form a neighbourhood base for a unique topology on G, which we again call the Krull topology. The same argument as in §7 shows that this topology is Hausdorff (but it is not necessarily compact)

8.6.2 THEOREM : Let $\Omega \supset F$ be fields such that $\Omega^G = F, G = Aut(\Omega/\mathrm{F})$

(a) For every finite extension E of F in $\Omega, \Omega^{Aut(\Omega/\mathrm{E})} = E$

(b) The maps

$$H \mapsto \Omega^H, \mathrm{M} \mapsto \mathrm{Aut}(\Omega/\mathrm{M}) \qquad (19)$$

Are inverse bijections between the set of compact subgroups of G and the set of intermediate fields over which Ω is Galois (possible infinite)

$$\{compact\ subgroups\ of\ G\} \leftrightarrow \{fields\ M\ such\ that\ F \subset M \overset{Galois}{\subset} \Omega\}.$$

(c) If there exists an M finitely generated over F such that Ω is Galois over M, then G is locally compact, and under (19):

$$\{open\ compact\ subgroups\ of\ G\} \overset{1:1}{\leftrightarrow} \{fields\ M\ such\ that\ F \overset{finitely\ generated}{\subset} M \overset{Galois}{\subset} \Omega\}.$$

(d) Let H be a subgroup of G , and let M = Ω^H. Then the algebraic closure M_1 of M is Galois over M. If moreover H = Auto (Ω/M), then $\mathrm{Aut}(\Omega/\mathrm{M}_1)$ is a normal subgroup of H and $\sigma \mapsto \sigma|M_1$ maps H / Aut (Ω/M_1) is isomorphically onto a dense subgroup of Aut (M_1/M)

Check your Progress-2

3. Discuss: If F is perfect, then every finitely generated extension E and F admits a separating transcendence basis over F.

____

____

____

4. State and prove Transcendental Galois Theory

____
____
____

8.7 LET US SUM UP

We have discussed the Algebraic independence and Transcendence bases. We have understood the Luroth’s theorem and Transcendental Galois Theory. We have discussed the concept of Separating transcendence bases.

8.8 KEYWORDS

Injection: An injective function (also known as **injection**, or one-to-one function) is a function that maps distinct elements of its domain to distinct elements of its codomain.

Non- constant Polynomial : If a **polynomial** is not a constant, then the **polynomial** is a **non-constant polynomial**.

Greatest Common Divisor (gcd) : of two or more integers, which are not all zero, is the **largest** positive integer that divides each of the integers.

8.9 QUESTIONS FOR REVIEW

1. Find the centralizer of complex conjugation in Aut(C/ℚ)

2. State and prove **Separating transcendence bases**

8.10 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.

8.11 ANSWERS TO CHECK YOUR PROGRESS

Provide definition – 8.2.3

Provide statement and proof – 8.3.2

Provide proof – 8.5.1

Provide statement and proof – 8.6.1

UNIT- 9 TRANSCENDENTAL EXTENSIONS & ALGEBRAIC CLOSURES

STRUCTURE

9.0 OBJECTIVES

Understand the concept and application of Linear Disjointness

Enumerate Zorn's lemma and its three proofs.

9.1 INTRODUCTION

In this section, we study linear disjointness, a technical condition but one with many applications. One way that we use this concept is to extend the definition of separability in a useful way to non-algebraic extensions. In this chapter, we use Zorn's lemma to show that every field F has an algebraic closure Ω.

9.2 LINEAR DISJOINTNESS

We tacitly assume that all of our field extensions of a given field *F* lie in some common extension field *C* of *F*. Problem 6 shows that this is not a crucial assumption. We will also make use of tensor products. By phrasing some results in terms of tensor products, we are able to give cleaner, shorter proofs. However, the basic results on linear disjointness can be proved without using tensor products.

9.2.1 Definition : *Let K and L be subfields of a field C, each containing a field F. Then K and L are linearly disjoint over F if every F-linearly independent subset of K is also linearly independent over L.*

Let *A* and *B* be subrings or a commutative ring *N. Then* the ring *A[B]* is the subring of *R* generated by A and *B;* that, is, *A[B]* is the smallest subring of *R* containing $A \cup B$. It is not hard to show that

$$A[B] = \left\{ \sum a_i b_i : a_i \in A, b_i \in B \right\}.$$

If A and *B* contain a common field *F*, then the universal mapping property of tensor products shows that there is a well-defined F-linear transformation $\varphi : A \otimes_F B \to A[B]$ given on generators by $\varphi(a \otimes b) = ab$.

We refer to the map φ as the natural map from $A \otimes_F B$ to *A[B]*. We give a criterion in terms of tensor products for two fields to be linear disjoint over a common subfield.

9.2.2 Proposition : *Let K and L be field extensions of a field F. Then K and L are linearly disjoint over F if and only if the map* $\varphi : K \otimes_F L \to K[L]$ *given on generators by* $a \otimes b \mapsto ab$ *is an isomorphism of F-vector spaces.*

Proof. The natural map $\varphi : K \otimes_F L \to K[L]$ is surjective by the descriptionof *K[L]* given above. So, we need to show that *K* and *L* are linearly disjoint over *F* if and only if φ is injective. Suppose first that *K* and L are linearlydisjoint over F. Let $\{k_i\}_{i\in I}$, be a basis for K as an F-vector space. Eachelement of $K \otimes_F L$ has a unique representation in the form $\sum ki \otimes l_i$, withthe $l_i \in L$. Suppose that $\sum ki \otimes l_i \in \ker(\varphi)$, so $\sum kil_i = 0$. Then each $l_i = 0$, since K and L are linearly disjoint over F and $\{ki\}$ is F-linearlyindependent. Thus, φ is injective, and so φ is an isomorphism.

Conversely, suppose that the map φ is an isomorphism. Let $\{a_j\}_{j\in J}$ be an F-linearly independent subset of K. By enlarging J, we may assume thatthe set $\{aj\}$is a basis for K. If $\{aj\}$ is not L-linearly independent, then there are $l_i \in L$with $\sum ajlj = 0$, a finite sum. Then $\sum aj \otimes lj \in \ker(\varphi)$, $\sum aj \otimes lj = 0$ by the injectivity of φ. However, elements of $K \otimes_F L$ can be represented uniquely in the form $\sum aj \otimes mj$ with mi $\in L$. Therefore, each $l_i = 0$, which forces the set $\{aj\}$to be L-linearly independent. Thus, K and L are linearly disjoint over F.

9.2.3 Corollary: *The definition of linear disjointness is symmetric; that is, K and L are linearly disjoint over F if and only if L and K are linearly disjoint over F.*

Proof. This follows from Proposition 20.2. The map $\varphi : K \otimes_F L \rightarrow K[L]$ isan isomorphism if and only if $T : L \otimes_F K \rightarrow L[K] = K[L]$ is an isomorphism,since $'T = i \circ \varphi$, where i is the canonical isomorphism $K \otimes_F L \rightarrow L \otimes_F K$that sends $a \otimes b$ to $b \otimes a$.

9.2.4 Lemma: *Suppose that K and L are finite extensions of F. Then K and L are linearly disjoint over F if and only if [K L : F] = [K: F] [L : F].*

Proof. The natural map $\varphi : K \otimes_F L \rightarrow K[L]$that sends $k \otimes l$ to k_l is surjective and

$$\dim(K \otimes_F L) = [K : F] \cdot [L : F].$$

Thus, φ is an isomorphism if and only if $[KL : = [K: [L : F]$. The lemma then follows from Proposition 9.2.2.

Example : Suppose that K and L are extensions of F with $[K :$
and $[L : F]$ relatively prime. Then K and L are linearly disjoint over F. To see this, note that both $[K : F]$ and $[L : F]$ divide $[KL : F]$, so their product divides $[KL : F]$ since these degrees are relatively prime. The linear disjointness of K and L over F follows from the lemma.

Example : Let K be a finite Galois extension of F. If L is any extensionof F, then K and L are linearly disjoint over F if and only if $K \cap L = F$. This follows from the previous example and the theorem of natural irrationalities, since

$$[KL : F] = [L : F][K : K \cap L],$$

so $[KL : F] = [K : F][L : F]$ if and only if $K \cap L = F$.

The tensor product characterization of linear disjointness leads us to believe that there is a reasonable notion of linear disjointness for rings, notjust fields. Being able to discuss linear disjointness in the case of integral domains will make it easier to work with fields.

9.2.5 Definition: *Let A and B be subrings of a field C, each containing a field F. Then A and B are linearly disjoint over F if the natural map* $A \otimes_F B \to C$ *given by* $a \otimes b \mapsto ab$ *is injective.*

9.2.6 Lemma: *Suppose that F is a field,* and$F \subseteq A \subseteq A'$ *and* $F \subseteq B \subseteq B'$ are *all subrings of a field C. If A' and B' are linearly disjoint over F, then A and B are linearly disjoint over F.*

Proof. This follows immediately from properties of tensor products. Thereis a natural injective homomorphism $i : A \otimes_F B \to A' \otimes_F B'$ sending $a \otimes b$ *to* $a \otimes b$ for $a \in A$ and $B \in B$. If the natural map $\varphi : A' \otimes_F B' \to A'[B']$ is injective, then restricting φ to the image of i shows that the map p: $A \otimes_F B \to A[B]$ is also injective.

Example : Let K and L be extensions of a field F. If $K \cap L$ is larger than F, then K and L are not linearly disjoint over F by the preceding lemma since $K \cap L$ is not linearly disjoint to itself over F. However, K and$L$ may not be linearly disjoint over F even if $K \cap L = F$. As an example, let $F = \mathbb{Q}$, $K = F(\sqrt[3]{2})()$, and $L = F(w\sqrt[3]{2})$, where w is a primitive third root of unity. Then $K \cap L = F$, but $KL = F(\sqrt[3]{2}),\omega)$ has dimension 6 over F, whereas $K \otimes_F L$ has dimension 9, so the map A $\otimes_F L \rightarrow KL$ is not injective.

9.2.7 Lemma: *Suppose that A and B are subrings of a field C, each containinga field F, with quotient fields K and L, respectively. Then A andB are linearly disjoint over F if and only if K and L are linearly disjointover F.*

Proof. If K and L are linearly disjoint over F, then A and B are also linearly disjoint over F by the previous lemma. Conversely, suppose that Aand B are linearly disjoint over F. Let $\{k_i ,... ,k_n\} \subseteq K$ be an F-linearly independent set, and suppose that there are $l_i \in L$ with $\sum k_i l_i = 0$. There are nonzero s $\in$ A and $t \in B$ with $sk_i \in$A and $t_i \in B$ for each $_i$. The set $\{a_i, ...,a$n $\}$ is also F-linearly independent; consequently, $\sum ai \otimes bi \neq 0$, since it maps to the nonzero element $\sum ai \otimes bi \in K \otimes_F L$ under the natural map A $\otimes_F B \rightarrow K \otimes_F B$. However, $\sum ai \otimes bi$ is in the kernel of the mapA $\otimes_F B \rightarrow A[B];$ hence, it is zero by the assumption that A and B are linearly disjoint over F. This shows that $\{k_i\}$ is L-linearly independent, so$K$ and L are linearly disjoint over F.

Example : Suppose that K/F is an algebraic extension and that *L/F* is a purely transcendental extension. Then K and L are linearly disjoint over F; to see this, let X be an algebraically independent set over F with $L = F(X)$. From the previous lemma, it suffices to show that K and F[X] are linearly disjoint over F. We can view F[X] as a polynomial ring in the variables $x \in X$. The ring generated by K and F[X] is the polynomial ring $K[X]$. The standard homomorphism $K \otimes_F$ F[X]→ K[X] is an isomorphism because there is a ring homomorphism $_T : K[X] \rightarrow K$ $\otimes_F$ F[X]induced by x $1 \otimes x$ for each $x \in X$, and this is the inverse of φ.

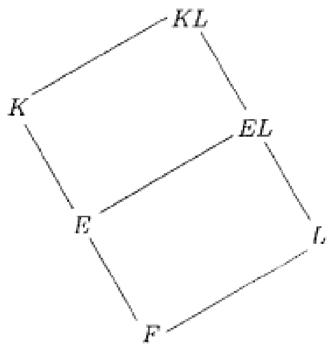
Notes

Thus, *K* and F[X] are linearly disjoint over *F*, so *K* and *L* are linearly disjoint over *F*.

The following theorem is a transitivity property for linear disjointness.

9.2.8 Theorem : *Let K and L be extension fields of F, and let E be a field with F⊆E⊆K. Then K and L are linearly disjoint over F if and only if E and L are linearly disjoint over F and K and EL are linearly disjoint over E.*

Proof. We have the following tower of fields.



Consider the sequence of homomorphisms

$$K \otimes_F L \xrightarrow{f} K \otimes_E (E \otimes_F L) \xrightarrow{\varphi_1} K \otimes_E EL \xrightarrow{\varphi_2} K[L],$$

where the maps f, φ_1, and φ_2 are given on generators by

$$f(k \otimes l) = k \otimes (1 \otimes l),$$
$$\varphi_1(k \otimes (e \otimes l)) = k \otimes el,$$
$$\varphi_2(k \otimes \sum e_i l_i) = \sum k e_i l_i,$$

respectively. Each can be seen to be well defined by the universal mapping property of tensor products. The map *f* is an isomorphism by counting dimensions. Moreover, $\varphi_1$and φ_2 are surjective.

The composition of these three maps is the standard map $\varphi : K \otimes_F L \to K[L]$. First, suppose that *K* and *L* are linearly disjoint over *F. Then* φ is an isomorphism by Proposition 9.2.2. This forces both $\varphi_1$and φ_2 to be isomorphisms, since allmaps in question are surjective.

The injectivity of φ_2 implies that *K* and*EL* are linearly disjoint over *E.* If $\sigma : E \otimes_F L \to E[L]$ is the standard map,then φ_1 is given on generators by

φ_1 *(k ⊗(e ⊗l)) = k ⊗σ- (e ⊗l);* hence, ais also injective. This shows that *E* and *L* are linearly disjoint over *F*.

Conversely, suppose that *E* and *L* are linearly disjoint over *F* and that *K* and *EL* are linearly disjoint over *E*.

Then $\varphi_2$and a are isomorphisms by Proposition 9.2.2. The map $\varphi_1$is also an isomorphism; this follows from the relation between φ_1 and σ above. Then φ is a composition of three isomorphisms; hence, φ is an isomorphism. Using Proposition 20.2 again, we see that *K* and *L* are linearly disjoint over *F*.

Separability of field extensions

One of the benefits of discussing linear disjointness is that it allows us to give a meaningful notion of separability for arbitrary field extensions. We first give an example that will help to motivate the definition of separability for non algebraic extensions.

Example : Let *KIF* be a separable extension, and let *LIF* be a purely inseparable extension. Then *K* and *L* are linearly disjoint over *F*. To prove this, note that if char(F) = 0, then *L = F,* and the result is trivial. So, suppose that char(F) = *p* >0. We first consider the case where *K/F*is a finite extension.

By the primitive element theorem, we may write$K = F(a)$ for some $a \in K$. Let *f (x)* = min(F, *a*) and *g(x)* = min(L, *a*).Then *g* divides *f* in *L[x]*. If $g(x) = \alpha_0 + \cdots + \alpha n\text{-}_1 x^{n-1} + x^n$, then for each *i* there is a positive integer r_i with $\alpha_i^{p^{ri}} \in F$. If r is the maximum of the r_i , then $(\alpha_i^{p^{ri}} \in F$ for each *i*, so *g(x)P* ∈ *F*. Consequently, $g(x)^{p^r}$is a polynomial over *F* for which a is a root. Thus, *f* divides $g)^{p^r}$in *F[x]*.

Viewing these two divisibilities in *L[x]*, we see that the only irreducible factor of *f* in *L[x]* is *g*, so *f* is a power of *g*. The field extension *KtP* is separable; hence, *f* has no irreducible factors in any extension field of *F*. This forces *f* = *g*, so

$$\begin{aligned}[KL:L] &= [L(a):L] = \deg(g) \\ &= \deg(f) = [K:F].\end{aligned}$$

From this, we obtain *[KL : F]= [K: F] • [L: F],* so *K* and *L* are linearly disjoint over *F* by Lemma 9.2.4.

If *K/F* is not necessarily finite, suppose that $\varphi : K \otimes_F L \to K[L]$ is not injective. Then there are $k_1, \ldots, k_n \in K$ and $l_1, \ldots, l_n$, /72 $\in L$ with $\varphi(\sum x_i \otimes l_i)$ = 0. If K_0 is the field generated over *F* by the k_i , then the restriction of φ to $K_0 \otimes_F L$ is not injective, which is false by the finite dimensional case.Thus, φ is injective, so *K* arid *L*, are linearly disjoint over *F*.

9.2.9 Definition: *Let F be a field of characteristic p* >0, *and let* F_{ac}*be analgebraic closure of F. Let*

$$F^{1/p^n} = \left\{ a \in F_{ac} : a^{p^n} \in F \right\}$$

and

$$\begin{aligned}F^{1/p^\infty} &= \left\{ a \in F_{ac} : a^{p^n} \in F \text{ for some } n \geq 0 \right\} \\ &= \bigcup_{n=1}^{\infty} F^{1/p^n}.\end{aligned}$$

The field F^{1/P^∞} is the composite of all purely inseparable extensions of *F* in F_{ac}. It is, therefore, the maximal purely inseparable extension of *F* in F_{ac}, *so* $F^{1/P^\infty}$is the purely inseparable closure of *F* in *Fac.*

9.2.10 Definition: A transcendence basis X for a field extension K/F is said to be a separating transcendence basis for K / F if K is separable algebraic over F(X). If K has a separating transcendence basis over F, then K is said to be separably generated over F.

Example : Let $K = F(x)$ be the rational function field in one variable over a field F of characteristic p. Then $\{x\}$ is a separating transcendence basis for K/F'. However, $\{x^p\}$ is also a transcendence basis, but$K/F(x^p)$ is not separable. This example shows that even if $K/F$is separably generated, not all transcendence bases of K/F are separating transcendence bases.

Example : If $K/F$is algebraic, then K is separable over F if and only if $K/F$is separably generated, so the definition of separably generatedagrees with the definition of separable for algebraic extensions. We now prove the result that characterizes separability of arbitrary extensions.

9.2.11 Theorem: *Let K be a field extension of F. Then the following statements are equivalent:*

1. Every finitely generated subextension of K/F is separably generated.
2. The fields K and $F^{1/P^{\infty}}$ are linearly disjoint over F.
3. The fields K and $F^{1/P}$ are linearly disjoint over F.

Proof. (1)⇒ (2): To show that K and $F^{1/P^{\infty}}$ are linearly disjoint over F, it suffices to assume that K is a finitely generated extension of F. By statement I, we know that K is separably generated over F, so there is a transcendence basis $\{t_1,...,t_n\}$ of K/F for which K is separable over $F(t_1,...,t_n)$. By Example 9.2.7 , the fields $F(t_1,...t_n)$ and $F^{1/P^{\infty}}$ are linearly disjoint over F. Also, K and $F^{1/P^{\infty}}(t_1,...,t_n)$ are linearly disjoint over $F(t_1,...,t_n)$ by Example below theorem 9.2.7 , since $F^{1/P^{\infty}}(t_1,...,t_n)$ is purely inseparable over $F(t_1,...,t_n)$ and K is separable over $F(t_1,...,t_n)$. Therefore, by Theorem 9.2.7, the fields K and $F^{1/P^{\infty}}$are linearly disjoint over F.

(2) ⇒ (3): This is clear since $F^{1/P}$ is a subfield of $F^{1/P^{\infty}}$.

(3)⇒ (1): Suppose that K and $F^{1/P}$ arc linearly disjoint over F.

Let $L = F(a_1,\ldots,a_n)$ be a finitely generated sub extension of K. We use induction on n to show that $\{a_1,\ldots,a_n\}$ contains a separating transcendence basis for L/F. The case $n = 0$ is clear, as is the case where $\{a_1,\ldots,a_n\}$ is algebraically independent, since then $\{a_1,\ldots,a_n\}$ is a separating transcendence basis for L/F. We may then assume that $n > 0$ and that $\{a_1,\ldots,a_n\}$is a transcendence basis for L/F, with $m < n$. The elements $a_1,\ldots,a_{m+1}$are algebraically dependent over F , so there is a nonzero polynomial $f \in F[x_1,\ldots,x_{m+1}]$ of least total degree with $f(a_1,\ldots,a_{m+1}) = 0$.

The assumption that f is chosen of least degree forces f to be irreducible. Wefirst claim that f is not a polynomial in $x_1^p,\ldots x_{m+1}^p$ If $f(x_1,\ldots x_{m+i}) = g(x_1^p,\ldots x_{m+1}^p)$ for some $g \in F[x_1,\ldots,x_{m+1}]$ then there is an $h \in F^{1/P}[x_1,\ldots,x_{m+1}]$ with $f = h(x_1,\ldots,x_{m+1})^p$, since we are assuming that char(F) = p and every coefficient of g is a p^{th} power in $F^{1/P}$. But this implies that $h(a_1,\ldots,a_{m+1}) = 0$. Write $h(x_1,\ldots,x_{m+1})$where the m_j are the monomials occurring in h and the $a_j \in F^{1/P}$. Then$\sum \alpha_j m_j (a_1,\ldots,a_{m+1}) = 0$, so the $m_j(a_1,\ldots,a_{m+1})$ are linearly dependent over $F^{1/P}$.

However, since each m_j is a monomial in the x_k , each mi $(a_1,\ldots,a_{m+1}) \in L \subseteq K$. The assumption that K and $F^{1/P}$ are linearly disjoint over F then forces the $m_j(a_1,\ldots,a_{m+1})$ to be linearly dependent over F.IF$\sum_j \beta_j m_j(a_1,\ldots,a_{m+1}) = 0$ with $\beta_j \in F$, then $h' = \sum_j \beta_j m_j$isa polynomial with $h'(a_1,\ldots,a_{m+1}) = 0$ and deg(h') < deg(f). This contradiction verifies our claim that f is not a polynomial in $x_1^p,\ldots x_{m+1}^p$Therefore, for some i the polynomial f is not a polynomial in x_1^p.Let

$$\begin{aligned} q(t) &= f(a_1,\ldots,a_{i-1},t,a_{i+1},\ldots,a_{m+1}) \\ &\in F[a_1,\ldots,a_{i-1},a_{i+1},\ldots,a_{m+1}][t]. \end{aligned}$$

Then $q(a_i) = 0$, and q is not a polynomial in t^P. If we can show that q is irreducible over M7 then we will have proved that a_i is separable over M. To see this, the set $\{a_1,\ldots,a_{i-1},a_{i+1},\ldots,a_{m+1}\}$is a transcendence basis for L/F, so

$$F[x_1, \ldots, x_{m+1}] \cong F[a_1, \ldots, a_{i-1}, t, a_{i+1}, \ldots, a_{m+1}]$$
$$= F[a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_{m+1}][t]$$

as rings. Under the map that sends a_j to $x_i$and t to x_i, the polynomial q is mapped to f. But f is irreducible over F, so q is irreducible in $F[a_1,\ldots,a_{i-1},a_{i+1},\ldots,a_{m+1}]$[t]. By Gauss' lemma, this means that q is irreducible over M7 the quotient field of $F[a_1,\ldots,a_{i-1},a_{i+1},\ldots,a_{m+1}]$. Thus, we have shown that ai is separable over M so a_i is separable over $L = F(a_1,\ldots,a_{i-1},a_{i+1},\ldots,a_n)$. The induction hypothesis applied to *L'* gives us a subset of $\{a_1,\ldots,a_{i-1},a_{i+1},\ldots,a_n\}$ that is a separating transcendence basis for *Li/F.* Since a_i is separable over *L'*, this is also a separating transcendence basis for *L/F.*

9.2.12 Definition: *A field extension K/F is separable if* char(F) = 0 *or if* char(F) = *p* >0 *and the conditions in Theorem* 9.2.9 *are satisfied; that is, K is separable if every finitely generated subextension of K/F is separably generated.*

We now give some immediate consequences of Theorem 9.2.9.

9.2.13 Corollary : *If K is separably ge7ierated, then K/F is separable. Conversely, if K/F is separable and finitely generated, then K/F is separably generated.*

9.2.14 Corollary: *Suppose that* $K = F(a_1,\ldots, a_n)$ *is finitely generated and separable over F. Then there is a subset Y of* $\{a_1,\ldots, a_n\}$ *that is a separating transcendence basis of K F.*

Proof. This corollary is more accurately a consequence of the proof of (3)⇒(1) in Theorem 20.18, since the argument of that step is to show thatif *K* is finitely generated over *F*, then any finite generating set contains aseparating transcendence basis.

Corollary 20.22*Let F be a* perfect field. Then any finitely generated extensionof F is separably generated.

Proof. This follows immediately from part 3 of Theorem 9.2.9, since $F^{1/P}=F$if F is perfect.

9.2.15 Corollary: *Let* $F \subseteq E \subseteq K$ *be fields.*

1. If K/F is separable, then E/F is separable.

2. If E/F and K/E are separable, then K/F is separable.

3. If K/F is separable and E/F is algebraic, then K/E is separable.

Proof. Part 1 is an immediate consequence of condition 2 of Theorem 9.2.9 . For part 2 we use Theorems 9.2.9 and 9.2.6. If *E/F* and *K/E* are separable, then *E* and $F^{1/P}$) are linearly disjoint over *F*, and *K* and $E^{1/P}$ are linearly disjoint over *E*. However, it follows from the definition that $F^{1/P} \subseteq E^{1/P}$, so $EF^{1/P} \subseteq E^{1/P}$.

Thus, *K* and $EF^{1/P}$are linearly disjoint over *E*. Theorem 9.2.6 then shows that *K* and $F^{1/P}$ are linearly disjoint over *F*, so *K* is separable over *F*.

To prove part 3, suppose that *K/F* is separable and *E/F* is algebraic. We know that *E/F* is separable by part 1. Let $L = E(a_1,\ldots, a_n)$ be a finitely generated subextension of *K/E*. If $L' = F(a_1,\ldots, a_n)$, then by the separability of *K/F* there is a separating transcendence basis $\{t_1,...,t_m\}$ for *L'/F*. Because *E/F* is separable algebraic, $EL' = L$ is separable over L', so by transitivity, *L* is separable over $F(t_1,...,t_m)$.

Thus, *L* is separable over $E(t_1,...,t_m)$, so $\{t_1,...,t_m\}$ is a separating transcendence basis for *L/E*. We have shown that *L/E* is separably generated for every finitely generated subextension of *K/E*, which proves that *K/E* is separable.

Example 20.24 Let *F* be a field of characteristic p, let $K = F(x)$, the rational function field in one variable over *F*, and let $E= F(x^P)$. Then *K/F* is separable, but *K/E* is not separable. This example shows the necessity for the assumption that *E/F* be algebraic in the previous corollary.

Example : Here is an example of saparable extension that is not separably generated. Let F be a field of characteristic p, let x be transcendental over F, and let $K = F(x)(\{x^{1/P^n} : n \geq 1\})$. Then K *is* the union of the fields $F(x^{1/P^n})$, each of which is purely transcendental over *F, and hence* is separably generated. Any finitely generated subextension E is a subfield of $F(x^{1/P^n})$ for some n and hence is separably generated over F by the previous corollary. Therefore, K/F is separable. But K is not separably generated over F, since given any $f \in K$, there is an n with $f \in F(x^{1/P^n})$, so $K/F(f)$ is not separable, since $K/F(x^{1/P^n})$ is a nontrivial purely inseparable extension.

Check your Progress-1

1. Define *linearly disjoint* .

____
____
____

2. State *field extension*

____
____
____

9.3 ZORN'S LEMMA

9.3.1 DEFINITION: (a) A relation ≤ on a set S is a partial ordering if it reflexive, transitive, and anti-symmetric (a ≤ b and b ≤ a ⇒ a = b).

(b) A partial ordering is a total ordering if, for all s, t ∈T , either s ≤ t or t ≤ s.

(c) An upper bound for a subset T of a partially ordered set (S,≤) is an element s ∈ Ssuch that t ≤ s for all t ∈ T .

(d) A maximal element of a partially ordered set S is an element s such that s ≤ s'⇒s = s'.

A partially ordered set need not have any maximal elements, for example, the set of finite subsets of an infinite set is partially ordered by inclusion, but it has no maximal elements.

9.3.2 LEMMA (ZORN): Let (S,≤) be a nonempty partially ordered set for which every totally ordered subset has an upper bound in S. Then S has a maximal element.

Zorn's lemma is equivalent to the Axiom of Choice, and hence independent of the axioms of set theory.

9.3.3 REMARK : The set S of finite subsets of an infinite set doesn't contradict Zorn's lemma, because it contains totally ordered subsets with no upper bound in S.

The following proposition is a typical application of Zorn's lemma—we shall use a * to signal results that depend on Zorn's lemma (equivalently, the Axiom of Choice).

9.3.4 PROPOSITION (*) Every nonzero commutative ring A has a maximal ideal (meaning, maximal among proper ideals).

PROOF. Let S be the set of all proper ideals in A, partially ordered by inclusion. If T is a totally ordered set of ideals, then $J = \bigcup_{I \in T} I$ is again an ideal, and it is proper because if $1 \in J$ then $1 \in I$ for some I in T, and I would not be proper. Thus J is an upper bound forT. Now Zorn's lemma implies that S has a maximal element, which is a maximal ideal in A.

9.4 FIRST PROOF OF THE EXISTENCE OF ALGEBRAIC CLOSURES

An F -algebra is a ring containing F as a subring. Let$(A_i)_{i \in I}$ be a family of commutative F -algebras, and define $\otimes_F A_i$ to be the quotient of the F - vector space with basis$\prod_{i \in I} A_i$ by the subspace generated by elementsof the form:

$(x_i) + (y_i) - (z_i)$ with $x_j + y_j = z_j$ for one $j \in I$ and $x_i = y_i = z_i$ for all $i \neq j$;
$(x_i) - a(y_i)$ with $x_j = ay_j$ for one $j \in I$ and $x_i = y_i$ for all $i \neq j$,

It can be made into a commutative F -algebra in an obvious fashion, and there are canonical homomorphisms $A_i \to \otimes_F A_i$ of F -algebras.

For each polynomial $f \in F[X]$, choose a splitting field E_f, and let Ω. $(\otimes_F E_f)/M$ where M is a maximal ideal in $\otimes_F E_f$ (whose existence is ensured by Zorn's lemma).

Note that $F \subset \otimes_F E_f$ and $M \cap F = 0$. As Ω has no ideals other than (0) and Ω, it isa field (see 1.2). The composite of the F –homomorphisms $E_f \to \otimes_F E_f \to \Omega$ being a homomorphism of fields, is injective. Since f splits in E_f, it must also split in the larger field Ω . The algebraic closure of F in Ω is therefore an algebraic closure of F.

9.5 SECOND PROOF OF THE EXISTENCE OF ALGEBRAIC CLOSURES

We may assume F to be infinite. This implies that the cardinality of every field algebraic over F is the same as that of F. Choose an uncountable set Ξ of cardinality greater than that of F, and identify F with a subset of Ξ. Let S be the set of triples $(E,+,\cdot)$ with $E \subset \Xi$ and $(+,\cdot)$a field structure on E such that$(E,+,\cdot)$ contains F as a subfield and is algebraic over it. Write $(E, +,\cdot) \leq (E', +',\cdot')$if the first is a subfield of the second.

Apply Zorn's lemma to show that S has maximal elements, and then show that a maximal element is algebraically closed.

9.6 THIRD PROOF OF THE EXISTENCE OF ALGEBRAIC CLOSURES

Notes

Consider the polynomial ring $F[\ldots,x_f,\ldots]$ in a family of symbols x_f indexedby the nonconstant monic polynomials $f \in F[X]$. If 1 lies in the ideal I of $F[\ldots,x_f,\ldots]$generated by the polynomials $f(x_f)$, then

$$g_1 f_1(x_{f_1}) + \cdots + g_n f_n(x_{f_n}) = 1 \qquad (\text{in } F[\ldots,x_f,\ldots])$$

for some $g_i \in F[\ldots,x_f,\ldots]$ and some nonconstant monic f_i 2 F[X]. Let E be an extensionof F such that each f_i, $i = 1,\ldots,n$, has a root α_i in E. Under the F –homomorphism$F[\ldots,x_f,\ldots] \rightarrow E$ sending

$$\begin{cases} x_{f_i} \mapsto \alpha_i \\ x_f \mapsto 0, \quad f \notin \{f_1,\ldots,f_n\} \end{cases}$$

the above relation becomes 0 = 1. From this contradiction, we deduce that 1 does not lie inI , and so Proposition 6.4 applied to $F[\ldots,x_f,\ldots]/I$shows that I is contained in a maximalideal M of $F[\ldots,x_f,\ldots]$. Let $\Omega = F[\ldots,x_f,\ldots]/M$. Then is a field containing (a copyof) F in which every nonconstant polynomial in F[X] has at least one root.

Repeat the process starting with E_1 instead of F to obtain a field E_2. Continue in this fashion to obtaina sequence of fields

$$F = E_0 \subset E_1 \subset E_2 \subset \cdots,$$

and let $E = \bigcup_i E_i$. Then E is algebraically closed because the coefficients of any nonconstantpolynomial g in E[X] lie in E_i for some i, and so g has a root in E_{i+1}. Therefore, the algebraic closure of F in E is an algebraic closure of F.

9.7 LET US SUM UP

The difficulty in showing the existence of an algebraic closure of an arbitrary field F is in the set theory. After reviewing the statement ofZorn's lemma, we sketch three solutions to the problem.

9.8 KEYWORDS

Tensor product - The **tensor product** of V and W is the vector space generated by the symbols v ⊗ w, with v ∈ V and w ∈ W, in which the relations of bilinearity are imposed for the **product** operation ⊗, and no other relations are assumed to hold.

Counting Dimension : In the study of fractals, Minkowski **dimension** (a.k.a. box-**counting dimension**) is a notion of **dimension** for fractals, measuring how complexity of detail changes with the scale at which one views the fractal.

Extension : A Galois **extension** is a field **extension** that is both normal and separable

9.9 QUESTIONS FOR REVIEW

1. Let {x, y} be algebraically independent over *F*. Show that *F(x)* and F(y) are linearly disjoint over *F*.

2. Let *F* be a perfect field, and let *K/F* be a field extension of transcendence degree 1. If *K* is not perfect, show that *K/F* is separably generated.

9.10 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.

9.11 ANSWERS TO CHECK YOUR PROGRESS

Provide definition – 9.2.1

Provide definition – 9.2.12

Provide statement– 9.3.2

Provide explanation and proof – 9.6

UNIT-10 APPLICATION OF TRANSCENDENTAL EXTENSIONS I

STRUCTURE

10.0 OBJECTIVES

Understand the concept and example of Algebraic Varieties

Understand the concept and application of Algebraic Function Fields

10.1 INTRODUCTION

The most fundamental concept in transcendental field theory is that of a transcendence basis. In this section, we investigate this concept. We shall see that the notion of a transcendence basis is very similar to that of a basis of a vector space.

10.2 ALGEBRAIC VARIETIES

Field extensions that are finitely generated but not algebraic arise naturally in algebraic geometry. In this section, we discuss some of the basic ideas of algebraic geometry, and in this Section we describe the connection between varieties and finitely generated field extensions.

Let k be a field, and let $f \in k[x_i ,... ,x_n]$ be a polynomial in the n variables $x_1 , . . x_n$. Then f can be viewed as a function from k^n to k in the obvious way; if P = (a_1,…. a_n) ∈ k^n , we will write $f (P)$ for f (a_1,… a_n).

It is possible for two different polynomials to yield the same function on k^n. For instance, if $k = \mathbb{F}_2$, then $x^2 — x$ is the zero function on k^1 , although it is not the zero polynomial. However, if k is infinite, then $f \in k[x_1 ,...,x_n]$ is the zero function on k^n if and only if f is the zero polynomial.

10.2.1 Definition:

Let k be a field, and let C be an algebraically closed field containing k. If S is a subset of $k[x_1,...,x_n]$, then the zero set of S is

$$Z(S) = \{(a_1 ,..., a_n) \in C^n: f (a_1 , ..., a_n) = 0 \text{ for all } f \in S\}.$$

10.2.2 Definition:

Let k be a field, and let C be an algebraically closed field containing k. Then a set $V \subseteq C^n$ is said to be a k-variety if V = Z(S) for some set S of polynomials in $k[x_1 ,...,x_n]$. The set

$$V(k) = \{P \in k^n : f (P) = 0 \text{ for all } f \in S\}$$

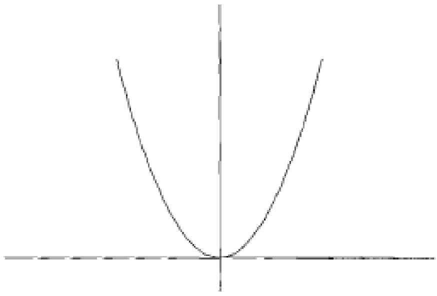
called the set of k-rational points of V.

Before looking at a number of examples, we look more closely at the definitions above. The reason for working in C^n instead of k^n is that a polynomial $f \in k[x_1, ... ,x_n]$ may not have a zero in k^n but, as we shall see below, f does have zeros in C^n.

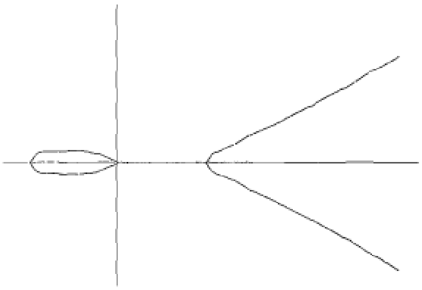
For example, if $f = x^2 + y^2 +1 \in \mathbb{R}[x, y]$, then f has no zeros in $\mathbb{R}^2$, while f has the zeros (0, ±i), among others, in $\mathbb{C}^2$. Classical algebraic geometry is concerned with polynomials over $\mathbb{C}$. On the other hand, zeros of polynomials over a number field are of concern in algebraic number theory. Working with polynomials over a field k but looking at zeros inside C^n allows one to handle both of these situations simultaneously.

We now look at some examples of varieties. The pictures below show theℝ -rational points of the given varieties.

Example: Let $f(x,y) = y - x^2$. Then $Z(f) = \{(a,a^2) : a \in C\}$, a k-variety for any $k \subseteq C$.



Example: Let $f(x, y) = y^2 — (x^3 — x)$. Then $Z(f)$ is a k-variety for any $k \subseteq C$. This variety is an example of an *elliptic curve,* a class of curvesof great importance in number theory.



Example: Let $f(x, y) = x^n + y^n — 1 \in Q[x, y]$, the *Fermat curve.* Fermat's last theorem states that if V = $Z(f)$ and $n \geq 3$, then V has no Q-rational points other than the "trivial points," when either $x = 0$ or y= O.

Example: Let $V = \{(t^2 , t^3) : t \in C\}$. Then V is the k-variety $Z(y^2 - x^3)$. The description of V as the set of points of the form (t^2, t^3) is called a *parameterization* of V. We will see a connection between parameterizing varieties and field extensions in Section 22.

Example: Let V — $(t^3 , t^4 , t^5) : L \in C\}$. *The, it V* is a k-variety, since V is the zero set of $\{y^2 — xz, z^2 — x^2y\}$. To verify this, note that each point of V does satisfy these two polynomials. Conversely, suppose that $(a, b, c) \in C^3$ is a zero of these three polynomials. If a = 0, then a quickcheck of the polynomials shows that $b c = 0$, so $(a, b, c) \in V$. If $a \neq 0$then define $t = b/a$. From $b^2 = ac$, we see that $c = t^2a$. Finally, the equation$c^2 = a^2b$ yields $t^4a^2 = a^3$ t, so $a = t^3 \in V$.

Example: Let $S^n = \{(a_1,\ldots, a_n) \in C^n: \sum_{i=1}^{n} a_i^2\ 1\}$. Then V = $Z(-1 + \sum_{i=1}^{n} x_i^2\}.)$, so -V is a k-variety.

Example: Let V be a C-vector subspace of C^n. We can find a matrix A such that V is the null space of A. If A = (α_{ij}), then a point $(a_1,\ldots, a_n)$ is in V if and only if $\sum_j \alpha_{ij} a_j = 0$ for each *i*. Thus, V is the zero set of the set of linear polynomials $\sum_j \alpha_{ij} x_j$, so V is a C-variety. If each α_{ij} lies in a subfiekl *k*, then V is a k-variety.

Example: Let $SL_n(C)$ be the set of all n x n matrices over *C* of determinant 1. We view the set of all n xn matrices over *C* as the set C^{n^2} of n^2-tuples over *C*. The determinant det = det(x_{ij}) is a polynomial in the n^2 variables x_{ij}, and the coefficients of the determinant polynomial are ±1. We then see that $SL_n(C)$ = Z(det -1) is a k-variety for any sub field*k* of *C*. For instance, if n = 2, then

$$SL_2(C) = \{(a,b,c,d) \in C^4 : ad - bc - 1 = 0\}$$

We can define a topology on C^n, the *k-Zariski topology*, by defining a subset of $C^n$to be closed if it is a k-variety. The following lemma shows that this does indeed define a topology on C^n. Some of the problems below go into more detail about the k-Zariski topology.

10.2.3 Lemma *The sets $\{Z(S): S \subseteq k[x_1,\ldots,x_n)\}$ are the closed sets of a topology on C^n; that is,*

1. *$C^n = Z(\{0\})$ and $\varnothing = Z(\{1\})$.*
2. *If S and T are subsets of $k[x_1,\ldots,x_n]$, then $Z(S) \cup Z(T) = Z(ST)$, where $ST = \{fg : f \in S, t \in T\}$.*
3. *If $\{S_\alpha\}$ is an arbitrary collection of subsets of $k[x_1,\ldots,x_n]$, then $\bigcap_\alpha Z(S_\alpha) = Z(\bigcup_\alpha S_\alpha)$.*

Proof. The first two parts are clear from the definitions. For the third, let $P \in Z(S)$. Then $f(P) = 0$ for all $f \in S$, so $(fg)(P) = 0$ for all $fg \in ST$.

Thus, $Z(S) \subseteq Z(ST)$. Similarly, $Z(T) \subseteq Z(ST)$, so $Z(S) \cup Z(T) \subseteq Z(ST)$.
For the reverse inclusion, let $P \in Z(ST)$. If $P \notin Z(S)$, then there is an $f \in 5$ *with PI') ,L* O. If $g \in T$, then 0 = *(f O (P) f(P)g(P)*, so $g(P) = 0$, which forces $P \in Z(T)$. Thus, $Z(ST) \subseteq Z(S) \cup Z(T)$. This proves that $Z(S) \cup Z(T) = Z(ST)$.

For the fourth part, the inclusion $Z(\cup_\alpha S_\alpha) \subseteq \cap_\alpha Z(S_\alpha)$ follows from part 1. For the reverse inclusion, take $P \in \cap_\alpha Z(S_\alpha)$. Then $P \in Z(S_\alpha)$ for each α, so $f(P) = 0$ for each $f \in S_\alpha$. Thus, $P \in Z(\cup_\alpha S_\alpha)$.

Example : Let $GL_n(C)$ be the set of all invertible n×n matrices over C. Then $GL_n,(C)$ is the complement of the zero set Z(det), so $GL_n(C)$ is an open subset of C^{n^2} with respect to the k-Zariski topology. We can view $GL_n(C)$ differently in order to view it as an algebraic variety. Let t be a new variable, and consider the zero set $Z(t$ det -1) in C^{n^2+1} .

Then the map $GL_n(C)$ $Z(t$ det -1) given by P $(P$, 1/ det(P)) is a bijection between $GL_n(C)$ and $Z(t$ det -1). If we introduce the definition of a morphism ofvarieties, this map would turn out to be an isomorphism. Starting with an ideal I of $k[x_1, ...x_n]$, we obtain a k-variety $Z(I)$. We can reverse this process and obtain an ideal from a k-variety.

10.2.4 Definition : Let $V \subseteq C'^n$. The ideal of V is

$$I(V) = \{f \in k[x_1, \ldots, x_n] : f(P) = 0 \text{ for all } P \in V\}.$$

The coordinate ring of V is the ring $k[V] = k[x_1, \ldots, x_n]/I(V)$.

If $f \in k[x_i, ..., x_n]$ and $V \subseteq C'^n$, then f can be viewed as a function from V to k. Two polynomials f and g yield the same polynomial function on V if and only if $f - g \in I(V)$; hence, we see that k[V] can be thought of as the ring of polynomial functions on V.

One of the main techniques of algebraic geometry is to translate back and forth from geometric properties of varieties to algebraic properties of

Notes

their coordinate rings. We state Hilbert's Nullstellensatz below, the most fundamental result that connects the geometry of varieties with the algebra of polynomial rings.

Let *A* be a commutative ring, and let *I* be an ideal of *A.* Then the *radical* of *I* is the ideal

$$\sqrt{I} = \{f \in A : f^r \in I \text{ for some } r \in \mathbb{N}\}.$$

If *I* = *Ï,* then *I* is said to be a *radical ideal.* A standard result of commutative ring theory is that f_i is the intersection of all prime ideals of A containing T

10.2.5 Lemma :*If V is any subset of* C^n*, then I(V) is a radical ideal of* $k[x_1, \ldots, x_n]$

Proof. Let $f \in k[x_1,... x_n]$ with *fr* ∈ *I(V)* for some r. Then $f^r(P) = 0$ for all *P* ∈V. But $f^r.(P) = (f(P))^r$ so *f (P)* = O. Therefore, *f* ∈*I(V);* hence, *.T(V)* is equal to its radical, so */(V)* is a radical ideal.

10.2.6 Lemma: *The following statements are some properties of ideals of subsets of* C^n

1. *If X and Y are subsets of* C^n *with* $X \subseteq Y$*, then* $I(Y) \subseteq I(X)$.
2. *If J is a subset of* $k[x_1, \ldots, x_n]$*, then* $J \subseteq I(Z(J))$.
3. *If* $V \subseteq C^n$*, then* $V \subseteq Z(I(V))$*, and* $V = Z(I(V))$ *if and only if V a k-variety.*

Proof. The first two parts of the lemma are clear from the definition of *I(V).* For the third, let *V* be a subset of *C.* lf *f* ∈ *I(V),* then *f(P)* = 0 for all *P* ∈ V, so *P* ∈ *Z(I(V)),* which shows that V ⊆*Z(/(V)).* Suppose that V = *Z(S)* for some subset *S* ∈ $k[x_1, \ldots, x_n]$. Then *S* ⊆ *I(V),* so *Z(/(V))* ⊆ *Z(S)* = *V* by the previous lemma. Thus, V = *Z(/(V)).* Conversely, if V = *Z*(I*(V)),* then V is a k-variety by definition.

In the lemma above, if J is an ideal of $k[x_1, \ldots, x_n]$, we have $J \subseteq I(Z(J))$, and actually $\sqrt{J} \subseteq I(Z(J))$, since $/(Z(J))$ is a radical ideal. The following theorem, Hilbert', Nullstellensatz, shows that $T(Z(J))$ is always equal to $\sqrt{J}$

10.2.7 Theorem (Nullstellensatz) *Let J be an ideal of* $k[x_1, \ldots, x_n]$, *and let* $V = Z(J)$. *Then* $I(V) = \sqrt{J}$

10.2.8 Corollary : *There is a* 1-1 *inclusion reversing correspondence between the k-varieties* C^n *and the radical ideals of* $[x_1, \ldots, x_n]$ *given by* $V \mapsto 1(V)$. *The inverse correspondence is given by* $J \mapsto Z(J)$

Proof. If V is a k-variety, then the previous lemma shows that $V = Z(I(V))$. Also, the Nullstellensatz shows that if I is a radical ideal, then $J = I(Z(J))$. These two formulas tell us that the association V $\mapsto I(V)$ is a bijection and that its inverse is given by $J \mapsto Z(J)$.

Another consequence of the Nullstellensatz is that any proper ideal definesa nonempty variety. Suppose that / is a proper ideal of $k[x_1, \ldots, x_n]$.If $V = Z(J)$, then the Nullstellensatz shows that $I(V) = \sqrt{J}$. Since J is a proper ideal, the radical is also proper. However, if $Z(J) = \emptyset$, then $I(Z(J)) = k[x_1 , x_n]$. Thus, $Z(J)$ is nonempty.

Example : Let $f \in k[x_i ,\ldots ,x_n]$ be a polynomial, and let V = $Z(f)$.
If $f = p_1^{r1} \ldots p_t^{rt}$ is the irreducible factorization of f, then I(V) $= \sqrt{(f)}$ by the Nullstellensatz. However, we show that $\sqrt{(f)} = (p_1 \cdots p_t)$ for, if $g \in \sqrt{(f)})$, then $g^m = fh$ for some $h \in k[x_i ,\ldots ,x_n]$ and some in > O. Each p_i then divides g^m; hence, each pi divides g. Thus, $g \in (p_1 \cdots p_t)$. For the reverse inclusion, $p_1 \cdots p_t \in \sqrt{(f)}$, since if r is the maximum of the r_i, then $(p_1 \cdots p_t)^r \in (f)$.

If $f \in k[x_i ,\ldots ,x_n]$ is irreducible, then $\sqrt{(f)}) = (f)$, so the coordinate ring of $Z(f)$ is $k[x_i ,\ldots ,x_n]/(f)$. For example, the coordinate ring of Z(y - x^2) $\subseteq C^2$ is $k[x, y]/(y - x^2)$. This ring is isomorphic to the polynomial ring$k[t]$. Similarly, the coordinate ring of Z(y^2-x3) is $k[x, y]/(y^2-x^3)$. Thisring is isomorphic to the subring $k[t^2, t^3]$ of the polynomial ring $k[t]$; anisomorphism is given by sending x to t^2 and y to t^3.

10.2.9 Definition *Let V be a k-variety. Then V is said to be irreducible if V is not the union of two proper k-varieties.*

Every k-variety can be written as a finite union of irreducible subvarieties,as Problem 7 shows. This fact reduces many questions about varieties tothe case of irreducible varieties.

Example : Let V be an irreducible k-variety. By taking complements,we see that the definition of irreducibility is equivalent to the conditionthat any two nonempty open sets have a nonempty intersection.

Therefore, if U and U' are nonempty open subsets of V, then $U \cap U' \neq \emptyset$. One consequence of this fact is that any nonempty open subset of V is dense in V, as we now prove. If U is a nonempty open subset of V, and if C is the closure of U in V, then $U \cap (V - C) = \emptyset$. The set V -$C$ is open, so one of U or V - C is empty. Since U is nonempty, this forces V -C = $\emptyset$,so C = V. But then the closure of U in V is all of V, so U is dense in V. This unusual fact about the Zariski topology is used often in algebraic geometry.

10.2.10 Proposition: *Let V be a k-variety. Then V is irreducible if and only if I(V) is a prime ideal, if and only if the coordinate ring k[V] is an integral domain.*

Proof. First suppose that V is irreducible. Let $f, g \in k[x_i ,\ldots, x_n]$ with $fg \in I(V)$. Then $I = I(V)+ (f)$ and $J = I(V) + (g)$ are ideals of $k[x_i ,\ldots ,x_n]$containing I(V); hence, their zero sets Y = $Z(I)$ and $Z = Z(J)$ are contained in $Z(I(V))$ = V. Moreover, $IJ \subseteq I(V)$, since $fg \in I(V)$, so Y $\cup Z=Z(IJ)$ contains V. This forces V = Y $\cup Z$, so either Y = V or Z = V, since V is irreducible. If Y = V, then $I \subseteq$I(Y) = $I(V)$, and if Z = V, then $J \subseteq I(Z) = I(V)$. Thus, either $f \in I(V)$ or $g \in I(V)$, so $I(V)$ is a prime ideal of $k[x_i ,\dots ,x_n]$.

Conversely, suppose that *(V)* is prime. Cf $V = Y \cup Z$ for sonic k-varieties Y and Z, let I = I(Y) and $J = I(Z)$. Then $IJ \subseteq I(YUZ)$ = I(V), so either I$\subseteq$ I(V) or $J \subseteq I(V)$. This means that V $\subseteq Z(I)$ = Y or V $\subseteq Z(J) = Z$. Therefore, Y = V or $Z = V$, so V is irreducible.

10.2.11 Definition*: Let V be a k-variety. Then the dimension of V, denoted dim(V), is the largest integer n such that there is a chain.*

$$Y_0 \subset Y_1 \subset \cdots \subset Y_n \subseteq V$$

of irreducible k-subvarieties of V.

While it is not obvious, there is indeed a maximum among the lengths of chains of irreducible subvarieties of any variety. In fact, if V $\subseteq C^n$, then dim(V) $\leq$ n.

The definition above is purely topological. However, the dimension of a k-variety can be determined with purely algebraic methods. One way to determine the dimension of a k-variety is given in the proposition below.

10.2.12 Proposition : *Let V be a k-variety. Then dim(V) is the maximum nonnegative integer n such that there is a chain*

$$P_0 \subset P_1 \subset \cdots \subset P_n$$

of prime ideals of k[V].

Proof. Suppose that $Y_0 \subset Y_1 \subset \cdots \subset Y_n \subseteq V$ is a chain Irreducible subsets of V. Then

$$I(V) \subseteq I(Y) \subset \cdots \subset I(Y_0)$$

is a chain of prime ideals of $k[x_i ,\dots ,x_n]$ by the previous proposition. Moreover, the inclusions are proper by the Nullstellensatz. By taking images in the quotient ring k[V] = $k[x_1, \ldots, x_n]/I(V)$, we get a chain of prime idealsof length n. However, if we have a chain of prime ideals of k[V] of length n, then we get a chain $I(V) \subseteq Q_0 \subset Q_1 \subset \cdots \subset Q_n$ of prime ideals of $kk[x_1, \ldots, x_n]$. Taking zero sets gives a chain

$$Z(Q_n) \subset \cdots \subset Z(Q_0) \subseteq Z(I(V)) = V$$

of irreducible k-subvarieties in *V*. The maximum length of a chain of irreduciblek-subvarieties of V is then the maximum length of a chain ofprimeideals of *k[V]*.

If A is a commutative ring, then the supremum of integers n such that there is a chain of prime ideals of *A* of length n is called the *dimension* of A. The proposition says that dim(V) = dim(k[V]) if V is a k-variety. Calculating the dimension of a k-variety by either the definition or by useof the proposition above is not easy.

Check your Progress-1

1. Define the terms a. *zero set*

b. k-rational points

____

____

____

2. State the concept of ideal

____

____

____

3. Explain the concept of Dimension

____

____

____

10.3 ALGEBRAIC FUNCTION FIELDS

In this section, we study one of the most important classes of field extensions,those arising from algebraic geometry. We will continue to use the notation defined in Section 21. The point of this section is to show how fieldtheoretic information can be used to obtain geometric information about varieties.

10.3.1 Definition

Let V be an irreducible k-variety. Then the function field k(V) of V is the quotient field of the coordinate ring k[V].

This definition is meaningful because if V is irreducible, then *I (V)* is a prime ideal, so k[V] = $k[x_i ,... ,x_n]/I(V)$ is an integral domain. The function field *k(V)* of a variety V can be viewed as a field of functions on V in the following way. Each $f \in$ k[V] is a polynomial function from V to*C*.

A quotient *f / g* of elements of k[V] then defines a function from V-*Z(g)*to *C*. Now, V -*Z(g)* is an open subset of V; hence, it is a dense subset of V. The elements of *k(V)* are then rational functions defined on an open, dense subset of V; the density follows.

Example Let V = Z(y - x^2). Then the coordinate ring of V is *k[x,* y]/(y -x^2), which is isomorphic to the polynomial ring *k[t]* by sending*t* to the coset of *x* in k[V]. Therefore, the function field of V is the rationalfunction field *k(t)*.

Example : Let V = Z(y^2-x^3). Then *k(V)* is the field *k(s, t),* where *s* and *t* are the images of *x* and y in k[V] = *k[x,* y]/(y^2-x^3), respectively. Note that $t^2 = 5^3$. Let *z* = *t/s.* Substituting this equation into $t^2 = s^3$ and simplifying shows that *s* = z2 , and so $t = z^3$. Thus, *k(V)* = *k(z).* The element *z* is transcendental over *k*, since if *k(V)/k* is algebraic, then k[V] is a field by the argument in Example 19.11, so (y^2-x^3) is a maximal ideal of *k[x,* y]. However, this is not true, since (y^2-x^3) is properly contained in the ideal *(x,* y). Thus, *k(V)* is a rational function field in one variable over *k*. Note that *k[V] is* isomorphic to $k[x^2 , x^3]$, a ring that is not isomorphic to a polynomial ring in one variable over *k.*

Example: If V is an irreducible k-variety, then V gives rise to a field extension *k(V)* of *k*. We can reverse this construction. Let *K* be a finitely generated field extension of *k*. Say $K = k(a_1,\cdots a_n)$ for some $a_i \in K$. Let

$$P = \in k[x_i ,\ldots ,x_n]: f(a_1,\ldots,a_n) = 0\}.$$

Then *P* is the kernel of the ring homomorphism φ: $k[x_i ,\ldots ,x_n] \to K$ that sends x_i to a_i, so *P* is a prime ideal. If V = *Z(P)*, then *V* is an irreducible k-variety with coordinate ring $k[x_i ,\ldots ,x_n]/P \cong k[a_1,\ldots,a_n]$, so the function field of *V* is *K*. Note that if we start with an irreducible *k* variety V and let *K* = *k(V)*, then the variety we get from this construction may not be V. Therefore, the processes of obtaining field extensions from varieties and vice versa are not inverses of each other.

The next theorem gives the most useful method for computing the dimension of a variety. We do not give the proof, since this would go past the interests of this book.

10.3.2 Theorem : *Let V be an irreducible k-variety. Then the dimension of V is equal to the transcendence degree of k(V)/k.*

Example : The dimension of the k-variety C^n is n, since the function field of C^n is $k[x_i ,\ldots ,x_n)$, which has transcendence degree n over *k*.

Example: If V = Z(y $-x^2$), then $k[V] = k[x, y]/(y - x^2) \cong k[x]$, so $k(V) \cong k(x)$ has transcendence degree 1 over *k*. Thus, dim(V) = 1. More generally, if *f (x, y)* is any irreducible polynomial in *k[x,* y] and V = *Z(f)*, then k[V] = *k[x , (f) = k[s , t]* , where *s* and *t* are the images in *k[V]* of *x* and y, respectively. Therefore, *k(V) = k(s,t)*. The set {s, t} is algebraically dependent over *k*, since *f (s,t)* 0. However, *s* or *t* is transcendental over *k*, for if *s* is algebraic over *k*, then there is a $g \in k[x]$ with *g(s)* = 0.

Viewing *g(x)* as a polynomial in *x* and y, we see that $g \in 1(V) = (f)$. Similarly, if *t* is algebraic over *k*, then there is an h(y) ∈ k[y] with h ∈*(f)*. These two inclusions are impossible, since *g(x)* and h(y) are relatively prime. This proves that either {s} or {t} is a transcendence basis for *k(V)*, so *k(V)* has transcendence degree 1 over *k*.

Example : Let *f* E $k[x_i ,... ,x_n]$ be an irreducible polynomial and set V = *Z(f)*. Then dim(V) = n - 1. To see this, we showed in Example 19.12 that the quotient field of $k[x_i ,... ,x_n]/(f)$ has transcendence degree n - 1 over k. But, this quotient field is the function field *k(V)* of V. Thus, Theorem 22.5 shows that dim(V) = n - 1. Note that the argument in the previous example is mostly a repeat of that given in Example 19.12 in thecase of two variables.

We now give some properties of the function field of an irreducible variety. We first need two definitions. If *Klk* is a field extension, then *K* is a ***regular extension*** of *k* provided that *K/k* is separable and *k* is algebraically closed in *K*. If *P* is a prime ideal of $k[x_1 ,... ,x_n]$, then *P* is *absolutely prime* if for any field extension *L/k* the ideal generated by *P* in $L[x_1 ,... ,x_n]$ is a **prime ideal.**

Example : Let *P* be an absolutely prime ideal of $k[x_i ,... ,x_n]$, and let V = *Z(P)*.Let *L* be any field extension of *k* contained in *C*. Then we can view *V* as an L-variety. The coordinate ring of *V* considered as an L-varietyis $L[x_1 ,... ,x_n]/I$, where *I* is the ideal of V computed in $L[x_1 ,... ,x_n]$. Theideal *I* contains *P*, so *I* contains the ideal generated by *P* in $L[x_i ,... ,x_n]$.

Since *P* is absolutely prime, the Nullstellensatz tells us that *I* is the ideal generated by *P*. Consequently, V is irreducible as an L-variety.

If $k = \mathbb{R}$and $P = (x^2 + y^2) \in \mathbb{R}[x,y]$, then V = *Z(P)* is an irreducible $\mathbb{R}$-variety hut V is not irreducible as a $\mathbb{C}$-variety, since the ideal of V in $\mathbb{C}[x,y]$ is $(x^2 + y^2) = (x + iy)(x - iy)$.

10.3.3 Theorem : *Let V be an irreducible k-variety. Then k(V) is a finitely generated extension of k. Moreover,k(V)/k is a regular extension if I(V) is absolutely prime.*

Proof. The field $k(V)$ is the quotient field of $k[V] = k[x_1 ,\dots ,x_n]/[V]$.The ring k[V] is generated over k as a ring by the images of the x_i, so $k(V)$is generated as a field extension over k by the images of the xi. This provesthat $k(V)$ is a finitely generated extension of k.

Suppose that $I(V)$ is absolutely prime. We need to show that $k(V)/k$ is separable and that k is algebraically closed in $k(V)$. For this, we first showthat if L is any extension of k, then $k(V)$ and L are linearly disjoint over$k$. To see this, note that

$$k[V] \otimes_k L \cong L[x_1, \dots, x_n]/Q,$$ L estensione algebrica

where $Q = I(V)L[x_1 ,\dots ,x_n]$. This isomorphism is given on generators by $(f\, I(V)) \otimes l \mapsto fl + Q$. The ring $L[x_1 ,\dots ,x_n]/Q$ contains an isomorphic copy of $k[V] = k[x_1 ,\dots ,x_n]$/I(V), and it is the ring generated by L and this copy of $k[V]$. By the assumption that $I(V)$ is absolutely prime, Q is a prime ideal, so $L[x_1 ,\dots ,x_n]/Q$ is a domain. If K is the quotient field of this domain, there are isomorphic copies of $k[V]$ and L inside K, and the tensor product $k[V] \otimes_k L$ is isomorphic to a subring of K. Therefore, $k[V]$and L are linearly disjoint over k, so $k(V)$ and L are linearly disjoint over k. To see that $k(V)$ is separable over k, set $L = k^{1/p^\infty}$.

From what we have shown, $k(V)$ and k^{1/p^∞} are linearly disjoint, so $k(V)$ is separable over k. Let k' be the algebraic closure of k in $k(V)$. By setting $L = k'$, since $k(V)$ and k' are linearly disjoint over k, it follows that k' and k' are linearly disjoint over k, so $k' = k$. Thus, k is algebraically closed in $k(V)$. This finishes the proof that $k(V)$ is a regular extension of k.

10.3.4 Corollary *Let f* E *$k[x_1 ,\dots ,x_n]$ be an absolutely irreducible polynomial.If $V = Z(f)$, then V is an irreducible k-variety, and $k(V)$ is a regular extension of k.*

Proof. Since f is irreducible in $k[x_1 ,\dots ,x_n]$, the principal ideal (f) is prime; hence, $I(V) = (f)$ is prime. Thus, V is an irreducible k-variety.

Moreover, *(f)* is absolutely prime, since *f* is absolutely irreducible. By the previous theorem, *k(V)* is a regular extension of *k.*

Example : Let $f = y^2 - (x^3 - x)$ and V = *Z(f).* If *L/k* is any field extension, then *f* is irreducible in *L[x,* yj, since $x^3 - x$is not a square in *L[x]*. Therefore, *k(V)* is a regular extension of *k.*

Example : If $f = x^2 \pm y^2 \in \mathbb{R}[x, y]$ and V = *Z(f)*, then *f* is irreducible over ℝ, but *f* is not irreducible over C, since $f = (x + iy)(x - iy)$.The field extension ℝ(V)/ℝ is therefore not regular. This extension is separable, since char(R) = O. In ℝ(V), we have $x^2 + y^2 = 0$, so $(x/y)^2 = -1$.Thus, C is a subfield of ℝ(V), which shows that R is not algebraically closed in ℝ(V).

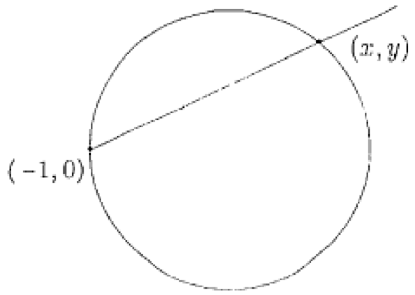
A natural question to ask is what geometric information about a variety can be determined from field theoretic information about its function field. We now investigate another.

10.3.5 Definition : *An irreducible k-variety V is said to be rational if k(V) is a purely transcendental extension of k.*

Recall that a purely transcendental extension with finite transcendence degree is often called a rational extension. Thus, a k-variety *V* is rational if *k(V)/k* is a rational extension. A fundamental problem of algebraic geometry is to determine when a variety is rational. The problem of rationality has a more geometric formulation. Recall from vector calculus that a curve in $\mathbb{R}^2$ can be parameterized in the form $x = f(t)$ and y = g(t), where *f* and *g* are real-valued functions; that is, the curve consists of the points *(Pt), g(t))* as *t* ranges over R. The functions *f* and *g* can be completely general, and even with a curve defined by polynomial equations, the functions *f* and *g* may be transcendental. For example, the most commonparameterization of the unit circle is $x = \cos t$ and $y = \sin t$.

In the case of algebraic varieties, we are interested in parameterizations involving polynomial or rational functions.

Example : Let V be the zero set of x^2+ y^2- 1, an irreducible *k*varietyin C^2 . As noted above, if $k = \mathbb{R}$, then the curve V has a transcendental parameterization. We wish to find a parameterization of V in terms of rational functions. We can do this as follows.



Pick a point on V, for instance *P = (-1,0).* For a point *(x,* y) on V, let *t* be the slope of the line connecting these two points. Then t y/(*x* + 1). If we solve for y and substitute into the equation $x^2 + y^2 - 1 = 0$, we can solve for *x* in terms of *t.* Doing this, we see that

$$x = \frac{1-t^2}{1+t^2}, \quad y = \frac{2t}{1+t^2}.$$

Moreover, we can reverse this calculation to show that

$$\left\{\left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right) : t \in C, t^2 \neq -1\right\} = V - \{P\},$$

for, given $(x, y) \in V$ with $(x, y) \neq (-1,0)$, solving for *t* in the equation

$$(1-t^2)/(1+t^2) = x$$

yields

$$t = \pm\sqrt{\frac{1-x}{1+x}},$$

which are elements of *C,* since $1+x \neq 0$ and *C* is algebraically closed, so *C* contains a square root of any element. With either of these values of *t,* we see that $2t/(1+t^2)$ $t(1+x)$, and we can check that $x^2 + (t(1+x))^2 = 1$; hence, $y = 2t/(1+t^2)$ if the sign of the square root is chosen appropriately. So, this parameterization of V picks up all but one point of V. There is no value of *t* that yields the point *P.*

Intuitively, we would need $t = \infty$ to get x = -1 and y = 0. Starting with any point Q on the curve and followingthis procedure will yield a parameterization of V - {Q}.

Example : For another example of a parameterization, let Y = $Z(y^2-x^3)$. If we start with the point (0,0) and follow the procedure of Example 22.15, we obtain the parameterization $x = t^2$ and $y = t^3$ given in Example 21.6. With this parameterization, we get all points of Y; that is,

$$Y = \{(t^2, t^3) : t \in C\} .$$

Not every algebraic curve can be parameterized with rational functions. To give an intuitive feel for why this is true, let V be the zero set of $y^2-(x^3-x)$. Pick P = (0,0) on V. If we follow the procedure above, we would get $t= y/x$, or $y = tx$. Substituting this into the equation $y^2 = x^3-x$yields $t^2x^2 = x^3- x$, or $x^2-t^2x - 1 = 0$. This has the two solutions

$$x = \frac{t^2 \pm \sqrt{t^2+4}}{2},$$

neither of which are rational functions in t. While this does not prove that Y cannot be parameterized, it does indicate that Y is more complicated than the two previous examples. In Proposition 22.18, we show that an Irreducible curve V can be parameterized if and only if the function Field $k(V)$ is rational over k. A proof that $\mathbb{C}(V)/\mathbb{C}$ is not rational if $V = Z(y^2-x^3+x)$ is outlined in Problem 23.6. It is nontrivial to show that, a field extension K/F is not rational when F is algebraically closed. If F is not algebraically closed, then it is easier to prove that an extension of F is not rational.

We now relate the concept of parameterization to that of rationality. We make precise what it means to parameterize a variety. We will restrict to curves. An algebraic variety of dimension 1 is said to be a *curve.*

10.3.6 Definition :

Let $V \subseteq V'$ be a curve defined over k. Then V can *be parameterized if there are rational functions fi (t) ∈k(t) such that {(f i (t),... , f n (t)) : t ∈* 01} *is a dense subset of V with respect to the k-Zariski topology.*

From Theorem 10.3.2, the function field of a curve defined over a Field *k* has transcendence degree 1 over *k.* We could define what it means to parameterize a variety of dimension greater than 1, although we will not do so.

To clarify the definition above, if *f(t)* is a rational function, say *f(t) g(t)/h(t)* with *g, h ∈k[t]*. Then *f (a)* is defined for a ∈*C* only if *h(a)*≠O. The polynomial *h* has at most finitely many roots, so *f(a)* is defined at all but finitely many a ∈*C.* In the definition of parameterization of a curve, it is being assumed that the point (f_1*(t), ,* f_n *(t))* exists only when each f_i *(t)* is defined.

10.3.7 Proposition: *Let V be an irreducible curvedefined over k. Then V can be parameterized if and only if the function field k(V) is rational over k.*

Proof. First, suppose that V $\subseteq C^n$can be parameterized. Let*f (t),….* f_n *(t)* ∈*k(t)* such that *U* = {(f_i*(t), ,* f_n *(t))* : *t* ∈C} is a dense subset of V. Define *cio : k[*x_i *,... ,*x_n*] (t)* by sending x i to *fi (t).* Then φ uniquely defines a k-hornomorphism. The kernel of φ consists of all polynomialsh, *(*x_i *,... ,*x_n*)*with *h(* f_i *(t),….,* f_n *(t))* = 0. For such an *h,* we have *h(P)* = 0 for all *P* ∈*U.* Therefore, *U* ⊆ *Z(h),* so by density we have V ⊆*Z(h).* Thus, *h* ∈*I(V).* It is clear that *1(V)* ⊆ ker(φ); hence, we see thatker(φ) = *1(V),* so cio induces an injective k-homomorphism φ': k[V] *k(t).*

The map φ' then induces a k-homomorphism *k(V) k(t),* so *k(V)* is isomorphicto an intermediate field of *k(t)/k.* By Liiroth's theorem, which weprove below, *k(V)* is a rational extension of *k.*

For the converse, suppose that *k(V) = k(t)* for some *t* We abuse notation by writing x i for the image of x i in k[V]. We have $x_i = f_i$ *(t)* for some rational function f_i , and we can write t = $g(x_i ,... ,x_n)/h(x_i ,... ,x_n)$for some polynomials g, h. If $P \in$ V, let a = $g(P)/h(P)$, provided that $h(P)\neq$O. Then $P = (f_1(a),...f_n(a))$ by the relations between the x, and t. On the other hand, given a $\in C$, if each f_1 (a) is defined, let Q = (fi (a), . . , f_n(a))

Then u(Q) = 0 for all u$\in(V)$, again by the relations between the x_i and t. Thus, Q E $Z(I(V))$ = V. The points of V not of the form (fi (a), . . , f_n(a)) all satisfy $h(P)$ = O. This does not include all points of V, or else $h \in I(V)$, which is false by the choice of h. Thus, V $\cap Z(h)$ is a finite set, so $\{(f$ (t), , fri $(t))$: t E C} contains all but finitely many points of V, so it is a dense subset of V. The equations $x_i= f_i\ (t)$ thus give a parameterization of V.

We now finish the proof of above Proposition by proving Liiroth's theorem.

Theorem 10.3.8 (Liiroth): *Let k(t) be the rational function field in one variable over a field k, and let F be a field with* $k \subseteq F \subseteq$ *kW, Then* $F = k(u)$ *for some* $u \in F$. *Thus, F is purely transcendental over k.*

Proof. Let $K = k(t)$, and take $v\in F—k$. We know that $[K: k(v)] < \infty$, so $[K: F] < \infty$. Let $f(x) = x^n + l^{n-1}\ x^{n-1} + \cdots + l_0$ be the minimal polynomial of t over F. Then $[K:F]$ =n.

Since t is transcendental over k, some $t_i \in k$. Let u = l_i, and set m $[K : k(u)]$. Therefore, m $\geq$ n, since $k(u) \subseteq F$. If we show m $\leq$ n, then *we* will have proved that $F = k(u)$. All $l_i \in k(t)$, so there are polynomials $c_1(t)$, , $c_n(t)$ and $d(t)$ in $k[t]$ with $l_i = c_j(t)/d(t)$, and such that $\{d, c_1, . . . , c_n\}$ is relatively prime. Note that c_n, $(t) = d(t)$, since f is monic, and u = $c_i(t)/d(t)$, so m $\leq$ max {deg(c_i), deg(d)} by Example 1.17. This may be an inequality instead of an equality because ci and d may not be relatively prime. Let

$$f(x, t) = d(t)\, f(x) = c_n\ (t)x^n + c_{n-1}\ (t)x^{n-1} + \cdots + c_0\ (t).$$

Then $f\ (x ,t) \in k[x, t]$, and f is primitive as a polynomial in x. Moreover,

Notes

Deg x (f(x, t)) = n, where deg„ refers to the degree in x of a polynomial, and deg t ($f(x,t)$) ≥m, since c_i and d are both coefficients of f. By dividing out gcd(c_i, d), we may write u = $g(t)/ h(t)$ with $9, h, \in k[t]$ relatively prime. Now t is a root of' $g(x) - uh(x) \in$ P(x), so we may write

$$g(x) - uh(x) = q(x) f (x) \qquad (A)$$

with $q(x) \in F[x]$. Plugging u = $g(t) / h(t)$ into Equation (A), we see that $g(x)h(t) - g(t)h(x)$ is divisible by $f (x, t)$ in $k(t)[x]$ as $F \subseteq k(t)$. These polynomials are in $k[x, t]$, and f is primitive in x, so we can write

$$g(x)h(t) - g(t)h(x) = r(x , t) f (x , t)$$

with $r(x , t) \in k[x,t]$. The left-hand side has degree in t at most m, since m = max {deg(g), deg(h)}. But we know that the degree of f in t is at least rn. Thus, $r(x,t) = r(x) \in k[x]$.In particular, r is primitive as a polynomial in $k[t][x]$. Thus, rf is primitive in $k[t][x]$ by Proposition 4.3 of Appendix A, so $l(x, t) = g(x)h(t) - g(t)h(x)$is a primitive polynomial in $k[t][x]$. By symmetry, it is also primitive in$k[x][t]$. But $r(x)$ divides all of its coefficients, so r $\in k$. Thus,

$$\begin{aligned} n &= \deg_x(f) = \deg_x(g(x)h(t) - g(t)h(x)) \\ &= \deg_t(g(x)h(t) - g(t)h(x)) \\ &= \deg_t(f) \geq m. \end{aligned}$$

Therefore, n > m. Since we have already proved that n ≤ m, we get n = m,and so $F = k(u)$.

Check your Progress-2

4.State the definition of ***regular extension & prime ideal***

____

____

____

5.. State the condition for parametrization

____

____

____

10.4. LET US SUM UP

We have obtain finitely generated field extensions by considering the quotient field of the coordinate ring of an irreducible k-variety as an extension of k .We finish this section with a brief discussion of the dimension of a variety

10.5 KEYWORDS

Parametrization is a **mathematical** process consisting of expressing the state of a system, process or model as a function of some independent quantities called parameters

Null space - If A is your matrix, the **null-space** is simply put, the set of all vectors v such that A·v=0.

10.6QUESTIONS FOR REVIEW

1. Let V and W be k-varieties, and suppose that φ : V →W is a morphism. Show that φ induces a homorphism $Tp\ (V) \rightarrow T_{\varphi\ (p)}$ (W).

2. Let $X \subseteq \mathbb{C}^2$ be the zero set of $y^2 - x^3 + x$. In this problem, we will show that the function field ℂ (Y) is not rational over ℂ. In order to do this, we need the following result: If Y is an irreducible nonsingular curve in $\mathbb{C}^2$ such that ℂ (Y)/ ℂ is rational, then ℂ [Y] is a unique factorization domain. Verify that ℂ (X) is not rational over. ℂ by verifying the following steps.

(a) Show that X is an irreducible nonsingular curve.

(b) Let $\mathbb{F} = \mathbb{C}\ (x) \subseteq K$. Show that K/ F is a degree 2 extension. If a is the nonidentity F -autornorphisin of K, show that σ(y) = - y. Conclude that $\sigma(A) \subseteq A$, where $A = \mathbb{C}\ [X]$.

10.7 SUGGESTED READINGS AND REFERENCES

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

10.8 ANSWERS TO CHECK YOUR PROGRESS

1. Provide definition – 10.2.1 & 10.2.2

2. Provide definition – 10.2.4

3. Provide definition – 10.2.11

4. Provide explanation and proof – 10.3.2

5. Provide definition – 10.3.6

UNIT-11: APPLICATION OF TRANSCENDENTAL EXTENSIONS II

STRUCTURE

11.0 OBJECTIVES

In this section, we discuss algebraic notions of derivation and differential, and we use these concepts to continue our study of finitely generated field extensions.

11.1 INTRODUCTION

We shall see that by using differentials we can determine the transcendence degree of a finitely generated extension and when a subset of a separably generated extension is a separating transcendence basis. As a geometric application, we use these ideas to define the tangent space to a point of a variety. By using tangent spaces, we are able to define the notion of non-singular point on a variety. This is a more subtle geometric concept.

11.2 DERIVATIONS

Let A be a commutative ring, and let *Me* be an A-module. A *derivation of* A into *M* is a map $D: A \rightarrow M$ such that for all a, $b \in A$,

$$D(a + b) = D(a) + D(b),$$
$$D(ab) = bD(a) + aD(b).$$

We write Der (A, *M)* for the set of all derivations of A into *M.* Since the sum of derivations is easily seen to be a derivation, Der(A, *M)* is a group. Furthermore, Der(A, *M)* is an A-module by defining $aD : A \rightarrow M$ by $(aD)(x) = a(D(x))$.

Example : The simplest example of a derivation is the polynomial derivative map $d/dx : k[x] \rightarrow k[x]$ defined by

$$\frac{d}{dx}\left(\sum_{i=0}^{n} a_i x^i\right) = \sum_{i=1}^{n-1} i a_i x^{i-1},$$

where *k* is any commutative ring. The term ia_iin the formula above is, of course, the sum of a_i with itself *i* times.

Example : If *k* is a field, then the derivation *d/dx* on *k[x]* can be extended to the quotient field *k(x)* by use of the quotient rule; that is, the formula

$$\frac{d}{dx}\left(\frac{f(x)}{g(x)}\right) = \frac{g(x)\frac{d}{dx}f(x) - f(x)\frac{d}{dx}g(x)}{g(x)^2}$$

defines a derivation on *k(x).* We shall see a generalization of this example in Lemma ahead.

Example: Let *k* be any commutative ring, and let A = $k[x_i ,... ,x_n]$
be the polynomial ring in n variables over k . Then the partial derivative snaps $\partial/\partial x_i$are each derivations of A to itself.

Example: Let K be a field, and let $D \in$ Der (K,K). If a $\in K^*$, we prove that $D(a^{-1}) = - a^{-2} D(a)$. To see this, note that D(1) = 0 by an application of the product rule. Thus,

$$\begin{aligned} 0 &= D(1) = D(a \cdot a^{-1}) \\ &= a^{-1}(D(a)) + aD(a^{-1}). \end{aligned}$$

Solving for $D(a^{-1})$ gives $D(a^{-1}) = - a^{-2}D(a)$, as desired.
Other familiar facts from calculus can be verified for arbitrary derivations. For instance, if K is a field and a, b E K with b 0, and if D E Der (K,K), then

$$D\left(\frac{a}{b}\right) = \frac{bD(a) - aD(b)}{b^2}.$$

To see this, we have

$$\begin{aligned} D(ab^{-1}) &= b^{-1}D(a) + aD(b^{-1}) \\ &= b^{-1}D(a) - ab^{-2}D(b) \\ &= b^{-2}(bD(a) - aD(b)) \end{aligned}$$

from the previous calculation. This proves the validity of the quotient rulefor derivations on a field.

Let D be a derivation of a ring A into an A-module M. An element a $\in A$ is said to be a *constant* for D if $D(a) = 0$. It is not hard to see that the set of all constants for D is a subring of A. If B is a subring of A, let Der_B (A, M) be the set of all derivations $D : A \to M$ for which $D(b) = 0$ for all $b \in B$. By studying Der_B (A, A), we will obtain information about the extension A/B when A and B are fields. To simplify notation, let Der_B (A) = Der_B (A, A). We will call an element of Der_B (A) a B-derivationon A.

Let K be a field extension of F. We wish to see how the vector space Der_F (K) gives information about the field extension K/F, and vice versa. We first consider algebraic extensions. The following lemma, which can bethought of as the chain rule for derivations, will be convenient in a number of places.

11.2.1 Lemma : *Let K be a field extension of k, and let D* e $\mathrm{Der}_k(K)$. *If a* ∈ *K and f (x)* ∈*k[x], then D(f (a)) = (a)D(a), where f' (x) is the ordinary polynomial derivative of f. More generally, if f* $(x_1, \ldots, x_n)$ ∈ k$[x_1, \ldots, x_n]$ *and* $a_1, \ldots, a_n \in K$, *then*

$$D(f(a_1, \ldots, a_n)) = \sum_{i=1}^{n} \frac{\partial f}{\partial x_i}(a_1, \ldots, a_n) D(a_i).$$

Proof. Suppose that $f(x) = \sum \alpha_i x^i$. Then

$$\begin{aligned} D(f(a)) &= D\left(\sum \alpha_i a^i\right) \\ &= \sum \alpha_i D(a^i) = \sum \alpha_i i a^{i-1} D(a) \\ &= f'(a) D(a). \end{aligned}$$

The second statement follows from much the same calculation. If *f* $\sum_i \alpha_i x_1^{i_1} \cdots x_n^{i_1}$, where i = ($i_1$, , i_n), applying the property *D(ab) = bD(a)+ aD(b)* repeatedly, we see that

$$\begin{aligned} D(f(a_1, \ldots, a_n) &= \sum_{j=1}^{n} \sum_{\mathbf{i}} i_j \alpha_{\mathbf{i}} a_1^{i_1} \cdots a_{j-1}^{i_{j-1}} a_j^{i_j - 1} D(a_j) a_{j+1}^{i_{j+1}} \cdots a_n^{i_n} \\ &= \sum_{j=1}^{n} \frac{\partial f}{\partial x_i}(a_1, \ldots, a_n) D(a_j). \end{aligned}$$

11.2.2 Proposition:

Let K be a separable algebraic field extension of F.
Then Der_F (K) = 0.

Proof. Suppose that *D* ∈ Der_F (K). If a ∈*K*, let *p(x)* = min(F, a), a separable polynomial over *F.* Then

$$0 = D(p(a)) = p'(a)D(a)$$

by Lemma 11.2.1. Since *p* is separable over *F*, the polynomials *p* and *p'* are relatively prime, so *p' (a)* O. Therefore, *D (a)* = 0, so *D* is the zero derivation.

11.2.3 Corollary: *Let k* ⊆ *F* ⊆ *K be fields, and suppose that K / F is a finite separable extension. Then each k- derivation on F extends uniquely to a k-derivation on K.*

Proof. The uniqueness is a consequence of Proposition 11.2.2. If D_1 and D_2 are k-derivations of *K* with the same restriction to *F*, then $D_1 - D_2 \in \mathrm{Der}_F(K)$, so D_1 = D. We now show that any derivation $D \in \mathrm{Der}_k(F)$ can be extended to a derivation *D'* on *K*. We can write *K = F (u)* for some u separable over *F*. Let *p(x)* = min(F, u), and say $p(t) = \sum \beta_i t_i$. We first define *D'(u) by*

$$D'(u) = -\frac{\sum_i D(\beta_i)u^i}{p'(u)}.$$

To define *D'* in general, if y ∈*K*, say *v = f(u)* for some *f(t)* ∈*F[tl.* If $f(t) = = \sum a_i t^i.$, define *D'* on *K* by

$$D'(v) = f'(u)D'(u) + \sum_i D(a_i)u^i.$$

These formulas are forced upon us by the requirement that *D'* is an extensionof *D.* The verification that *D'* is indeed a well-defined derivation on*K* is straightforward but tedious and will be left to the reader.
The converse of this proposition is also true, which we will verify shortly.To do this, we must look at inseparable extensions.

11.2.4 Proposition :

Suppose that char(F) = *p* >0, *and let K = F(a) be purely inseparable over F. If K≠ F, then* $\mathrm{Der}_F(K)$ *is a one-dimensional K -vector space.*

Proof. Define *D : K→K* by *D(f (a)) = f' (a).* We need to show that *D* is well defined. Let *p(x)* = min(F, a). Then $p(x) = xP^m - \alpha$ for some $m \in$ N and some a ∈*F.* If *f (a) = g(a),* then *p* divides *f - g,* so *f(x) -g(x) = p(x)q(x)* for some *q.* Taking derivatives, we have *f ′(x) -g(x) = p(x)q' (x),* since *p' (x)* = 0. Therefore, *f ′(a) = g ′(a),* so *D* is well defined.

A short calculation shows that *D* is an F-derivation on *K.* If *E* is any derivation of *K,* then *E(f (a)) =f ′(a)E(a)* by Lemma 11.2.1, so *E* is a scalar multiple of *D*, namely *E* = *β*f *β = E(a).* Therefore, $\mathrm{Der}_F(K)$ is spanned by *D,* so $\mathrm{Der}_F(K)$ is one dimensional as a K-vector space.

Notes

We can now prove the converse of Proposition 11.2.2. This converse gives a test for separability by using derivations.

11.2.5 Corollary: *If K is an algebraic extension of F with* $\mathrm{Der}_F(K) = 0$, *then K / F is separable.*

Proof. Suppose that $\mathrm{Der}_F(K) = 0$, and let *S* be the separable closure of *F* in *K.* If *K S,* then there is a proper subfield *L* of *K* containing *S* and an $a \in K$ with $K = L(a)$ and *K/L* purely inseparable. The previous proposition shows that $\mathrm{Der}_L(K) \neq 0$, so $\mathrm{Der}_F(K)$ is also nonzero, since it contains $\mathrm{Der}_L(K)$. This contradicts the assumption that $\mathrm{Der}_F(K) = 0$, so *K* is separable over *F.*

We now consider transcendental extensions. First, we need a lemma that will allow us to work with polynomial rings instead of rational function fields.

11.2.6 Lemma: *Let A be an integral domain with quotient field K. Then any derivation on A has a unique extension to K. If* $D \in \mathrm{Der}_B(A)$ *for some subring B of A, then the unique extension of D to K lies in* $\mathrm{Der}_F(K)$, *where F is the quotient field of B.*

Proof. Let $D \in \mathrm{Der}(\ I)$. Define $D' : K \to K$ by

$$\begin{aligned} D(\alpha) &= D(ab^{-1}) \\ &= b^{-1}D(a) + aD(b^{-1}) \\ &= b^{-1}D(a) - ab^{-2}D(b), \end{aligned}$$

if $a,b \in$ A and *b* O. We first note that *D'* is well defined. If $a/b = c/d$, then $ad = Sc$, so

$$aD(d) + dD(a) = 5D(c) + cD(5).$$

Thus, by multiplying both sides by *bd* and rearranging terms, we get

$$bd^2D(a) - bcdD(b) = b^2dD(c) - abdD(d).$$

Using the relation $ad = bc$, we can simplify this to

$$d^2(bD(a) - aD(b)) = b^2(dD(c) - cD(d)),$$

so

$$\frac{bD(a) - aD(b)}{b^2} = \frac{dD(c) - cD(d)}{d^2},$$

proving that *D′* is well defined. Checking that *D′* is a derivation is straight forward.

To verify uniqueness of extensions, suppose that *D* is a derivation on *K*. If *a*∈*K,* we may write a = *a/b* with *a,b* ∈ A. Then

$$\begin{aligned} D(\alpha) &= D(ab^{-1}) \\ &= b^{-1}D(a) + aD(b^{-1}) \\ &= b^{-1}D(a) - ab^{-2}D(b), \end{aligned}$$

the final equality coming from above Example. This formula shows that *D* is determined by its action on A.

The following proposition determines the module of derivations for a purely transcendental extension of finite transcendence degree.

11.2.7 Proposition: *Suppose that K –k* $(x_1, \ldots, x_n)$ *is the 'rational function field over a field k in n variables. Then* $\mathrm{Der}_k(K)$ *is an n-dimensional K -vector space with basis* $\{\partial/\partial x_i : 1 \le i \le n\}$.

Proof. Let $f \in k[x_1, \ldots, x_n]$. If $D \in \mathrm{Der}_k(K)$, then by Lemma 11.2.1, we have $D(f) = \sum_i D(x_i)(\partial f/\partial x_i)$. Therefore, the n partial derivations $\partial/\partial x_i$ span $\mathrm{Der}_k(k[x_1, \ldots, x_n])$. Moreover, they are K-linearly independent; if

$$\sum_j a_j (\partial/\partial x_i) = 0,$$

then

$$0 = \sum_j a_j \frac{\partial x_i}{\partial x_j} = a_i.$$

This proves independence, so the $\partial/\partial x_i$ form a basis for Der (k*[*$x_1,\ldots,x_n$*])* Finally, a use of the quotient rule shows that the $\partial/\partial x_i$forma basis for $\mathrm{Der}_k(K)$.

We can generalize this theorem to any finitely generated, separable extension.

11.2.8 Theorem : *Suppose that K/ k is a finitely generated, separable extension. Then* trdeg (K/k) = $\dim_k(\mathrm{Der}_k(K))$. [*f*$\{x_1,\ldots,x_n\}$ *is* a separating transcendence basis for *K k and if* $F = k(x_1,\ldots,x_n)$*, then there is a basis* $\{\delta_i : 1 \le i \le n\}$ *for* $\mathrm{Der}_k(K)$ *with* $\delta_i|F = \partial/\partial x_i$ *for each i.*

Proof. Let $\{x_1,\ldots,x_n\}$ be a separating transcendence basis for *K/k*, and set $F = k(x_1,\ldots,x_n)$. The extension *K/F* is finite and separable. By Corollary 11.2.3 , for each i the derivation $\partial/\partial x_i$extends uniquely to a derivationδ_i on *K.*

We show that the *Si* form a basis for Der k (K). It is easy to see that the *6i* are K-linearly independent, for if $\sum_i a_i\delta_i = 0$ with the $a_i \in K$, then

$$0 = \left(\sum_i a_i\delta_i\right)(x_j) = \sum_i a_j \frac{\partial x_j}{\partial x_i} = a_j$$

for each *j*. To show that the $\delta_i$span $\mathrm{Der}_k(K)$, let *D* be a k-derivation of *K*,and let $a_i = D(x_i)$. Then $D - \sum_i a_i\delta_i$ is a derivation on *K* that is trivial on *F*. But $\mathrm{Der}_F(K) = 0$ by Proposition 11.2.2, so $D = \sum_i a_i\delta_i$

Check your Progress-1

1. Explain Derivation

____

____

____

2. *Discuss: Let $k \subseteq F \subseteq K$ be fields, and suppose that K / F is a finite separable extension. Then each k- derivation on F extends uniquely to a k-derivation on K.*

11.3 DIFFERENTIALS

Let $B \subseteq A$ be commutative rings. Then the *module of differentials* $\Omega_{A/B}$ is the A-module spanned by symbols *da*, one for each $a \in A$, subject to therelations

$$d\alpha = 0,$$
$$d(ab) = adb + bda$$

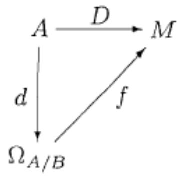
for $a \in$ Band $a\ b \in$ A*;* that is, $\Omega_{A/B}$ is the A-module M/N, where *M* is the free A-module on the set of symbols { d*a* :$a \subset$ A} and *N* the sub-module generated by the elements

$$d\alpha,$$
$$d(a+b) - da - db,$$
$$d(ab) - (adb + bda)$$

for $a \in$ B and $a\ b \in$ A. The map $d: A \to \Omega_{A/B}$ given by $d(a) = da$ is a B-derivation on A by the definition of $\Omega_{A/B}$.

The module of differentials is determined by the following universal mapping property.

11.3.1 Proposition : *Suppose that $D : A \to M$ is a B-derivation from A to an A-module M. Then there is a unique A-module homomorphism $f : \Omega_{A/B} \to M$ with $f \circ d = D$; that is, $f(da) = D(a)$ for all $a \in A$. In other words, the following diagram commutes:*



Proof. Given *D,* we have an A-module homomorphism *f* defined on the free A-module on the set {d*a* : *a*∈ A} into *M* that sends *da* to *D(a).* Since *D* is a B-derivation, *f* is compatible with the defining relations for hence, *f* factors through these relations to give an A-module homomorphism

$$f : \Omega_{A/B,} M \text{ with } f(da) = D(a) \text{ for all } a \in \text{A}.$$

The uniqueness of *f* is clear from the requirement that $f(da) = D(a)$, since $\Omega_{A/B}$ is generatedby {d*a* : *a*∈ A}.

11.3.2 Corollary : *If B* ⊆ A *are commutative rings and, M is an A-module, then* $\text{Der}_{\text{B}}(A,M \cong hom_A(\Omega_{A/B,}M).$

Proof. This is really just a restatement of the universal mapping property for differentials. Define φ : Der_{B} (A, *M)* homA($\Omega_{A/B}$,M) by letting $\varphi(D)$ be the unique element *f* of $\text{hom}_{\text{A}}(\Omega_{A/B},\text{M})$ that satisfies $f \circ d = D.$
A short computation using the uniqueness part of the mapping property shows that φ is an A-module homomorphism.

For injectivity, if $\varphi(D) = 0$,then the condition that $\varphi(D) \circ d = D$ shows that D = O. Finally, for surjectivity, if $f \in$ horn_{A} ($\Omega_{A/B}$,M), then setting $D = f \circ d$ yields $(p(D) = f.$

If .M = A, then the corollary shows that Der_{B} (A) $\text{hom}_{\text{A}}(\Omega_{A/B},A),$
the dual module to $\Omega_{A/B}$,. The next corollary follows immediately from this observation.

11.3.3 Corollary: *If K is a field extension of F, then*

$$\dim_K(\Omega_{K/F}) = \dim_K(\text{Der}_F(K)).$$

The following corollary is a consequence of the previous corollary together with Theorem 11.2.8.

11.3.4 Corollary

If $\{x_1 ,\dots ,x_n\}$ is a separating transcendence basis foran extension K/ k, then $\{dx_1 ,\dots ,dx_n\}$ is a K -basis for $\Omega_{k/k}$.

Proof. Suppose that $\{x_1 ,\dots ,x_n\}$ is a separating transcendence basis for *K/k.* By Theorem 11.2.8 , there is a basis $\{\delta_1 ....,\delta_n \}$ of $\mathrm{Der}_k(K)$ such that δ_i extends the derivation $\partial/\partial x_i$on $k(x_1 ,\dots ,x_n)$. By the universal mapping property for differentials, there are $f_i \in hom_K (\Omega_{k/k} ,K)$ with $f_i(dx_j) =\delta_i(x_j)$ for each j.

But, $\delta_i(x_j) = 0$ if $i\neq j$, and $\delta_i(dx_i) = 1$. Under the isomorphism $\mathrm{Der}_k(K)\cong \hom_K(\Omega_{k/k}, K)$, the δ_i arc sent to the *f.*, so the fi form a basis for $\hom_K (\Omega_{k/k} ,K)$. The dual basis of $\Omega_{k/k}$, to the f_i is then $\{dx_1 ,\dots, dx_n\}$, so this set is a basis for $\Omega_{k/k}$.

The converse of this corollary is also true, and the converse gives us a way to determine when a set of elements form a separating transcendence basis.

11.3.5 Proposition: *Suppose that K is a separably generated extension of k. If $x_1 ,\dots, x_n \in K$ such that $dx_1 ,\dots,dx_n$, is a K-basis for $\Omega_{k/k}$, then $\{x_1 ,\dots, x_n\}$ is a separating transcendence basis for K /k.*

Proof. Since *K/k* is separably generated, r_i = trdeg (K/k) by Theorem 11.2.8 and Corollary 11.3.5. Let $\{y_1,\dots,y_n\}$ be a separating transcendence basis for *K/k.* We will show that $\{x_1 ,\dots, x_n\}$ is also a separating transcendence basis by replacing, one at a time, a y_1, by an x_j and showing that we still have a separating transcendence basis.

The element x_1 is separable over $k(y_1,\dots,y_n,)$, so there is an irreducible polynomial $p(t) \in k(y_1,\dots,y_n)[t]$ with $p(x_1) = 0$ and $pi (x_1)$O. We can write *p(t)* in the form

Notes

$$p(t) = \frac{f_0}{g_0} + \frac{f_1}{g_1}t + \cdots + \frac{f_n}{g_n}t^n$$

with each f_i, $g_i \in k[y_1, \ldots, y_n]$. By clearing denominators and dividing out the greatest common divisor of the new coefficients, we obtain a primitive irreducible polynomial $f(y_1, \ldots, y_n, t)$ with $f(y_1, \ldots, y_n, x_i) = 0$ and $(\partial f/\partial t)(y_1, \ldots, y_n, x_i) \neq 0$. Let $P = (y_1, \ldots, y_n, x_i)$. Taking differentials and using the chain rule yields

$$0 = \frac{\partial f}{\partial t}(P)dx_1 + \sum_{j=1}^{n} \frac{\partial f}{\partial y_j}(P)dy_j.$$

Consequently,

$$dx_1 = \sum_{j=1}^{n} -\frac{(\partial f/\partial y_j)(P)}{(\partial f/\partial t)(P)}dy_j.$$

The differential $dx_1 \neq 0$, so some $(\partial f/\partial y_i)(P) \neq 0$. By relabeling if necessary, we may assume that $(\partial f/\partial y_1)(P) \neq 0$. The equation $(y_1, \ldots, y_n, x_1) = 0$ shows that y_1 is algebraic over $k(x_1, y_2, \ldots, y_n)$.

Moreover, the condition $(\partial f/\partial y_1)(P) \neq 0$ implies that y_1 is separable over $k(x_1, y_2, \ldots, y_n)$- Thus, each y_i is separable over $k(x_1, y_2, \ldots, y_n)$ and since K is separable over $k(x_1, y_2, \ldots, y_n)$, by transitivity the set $\{x_1, y_2, \ldots, y_n\}$ is a separating transcendence basis for K/k.

Now, assume that for some i ≥ 1, $\{x_1, \ldots x_i y_{i+1} \ldots, y_n\}$ is a separating transcendence basis for K/k. Repeating the argument above for x_{i+1} in place of x_1, there is an irreducible primitive polynomial equation $g(Q) = 0$with $(\partial g/\partial t_{n+1})(Q) \neq 0$, if $Q = (x_1, \ldots x_i y_{i+1} \ldots, y_n x_{1+1})$. this yields an equation

$$dx_{i+1} = \sum_{j=1}^{i} -\frac{(\partial g/\partial x_j)(Q)}{(\partial g/\partial t)(Q)}dx_j - \sum_{j=i+1}^{n} \frac{(\partial g/\partial y_j)(Q)}{(\partial g/\partial t)(Q)}dy_j.$$

The differentials $dx_1, \ldots, dx_n$are K-independent, so some $(\partial g/\partial y_j)(Q) \neq 0$. Relabeling if necessary, we may assume that $(\partial g/\partial y_{i+1})(Q) \neq 0$.

Consequently, y_{i+1} is separable over $k(x_1, \ldots x_{1+1} y_{i+2} \ldots, y_n)$. As above, this means that $\{x_1, \ldots x_{1+1} y_{i+2} \ldots, y_n\}$ is a separating transcendence basis for *K/k.* Continuing this procedure shows that $\{x_1, \ldots x_n\}$ is a separating transcendence basis for *K/k.*

Example : Let *k o* be a field of characteristic p, let $K = k_0(x\,y)$ be the rational function field in two variables over ok_0 , and let $k = k_0\,(x^P, y^P)$.Then {*x*, y} is algebraically dependent over *k;* in fact, *K/k* is algebraic.

However, *dx* and dy are K-independent in $\Omega_{k/kj}$*;* to see this, suppose that $adx+bdy = 0$ for some a, $b \in K$. The k_0 -derivations $\partial/\partial x$ and $\partial/\partial y$are actually k-derivations by the choice of *k.* By the universal mapping property for differentials, there are $f, g \in hom_K\,(\Omega_{K/F};,K)$ with $f \circ d = \partial/\partial x$ and $g \circ d = \partial/\partial y$. Then $f\,(adx_+\,bdy) = a\,f\,(dx) + b\,f\,(dy) = a$ and $g(adx + bdy) = b$. Thus, a = b = 0, so *dx* and dy are K-independent.

This shows that Proposition 11.3.5 is false if *K/k* is not separably generated.

11.4 THE TANGENT SPACE OF A VARIETY

Let *f(x,* y) be a polynomial in $\mathbb{R}[x, y]$. The equation $f\,(x\,,\,y) = 0$ defines y implicitly as a function of *x.* If $P = (a, b)$ is a point on the carve $f = 0$, then, as long as the tangent line to the curve at *P* is not vertical, we have

$$\frac{dy}{dx}(a) = -\frac{\partial f/\partial x}{\partial f/\partial y}(P),$$

so the tangent line to the curve at P can be written in the form

$$\frac{\partial f}{\partial x}(P)(x-a) + \frac{\partial f}{\partial y}(P)(y-b) = 0.$$

This formula is valid even if the tangent line at *P* is vertical. To deal with vector subspaces, we define the *tangent space* to the curve $f = 0$ at P to be the set of solutions to the equation

$$\frac{\partial f}{\partial x}(P) \cdot x + \frac{\partial f}{\partial y}(P) \cdot y = 0.$$

This tangent space is a vector subspace of $\mathbb{R}^2$.

The curve $f = 0$ is nothing more than the set of $\mathbb{R}$-rational points of the R-variety $Z(f)$. We can give a meaningful definition of the tangent space to any k-variety, for any field *k, by* mimicking the case of real plane curves. Let V be a k-variety in C^n, where, as usual, C is an algebraically closed extension of k, and let $P \in V$. For $f \in k[x_1,...,x_n]$, let

$$d_P f = \sum_{i=1}^{n} \frac{\partial f}{\partial x_i}(P) x_i.$$

The linear polynomial $dp\, f$ is called the *differential* of f at P.

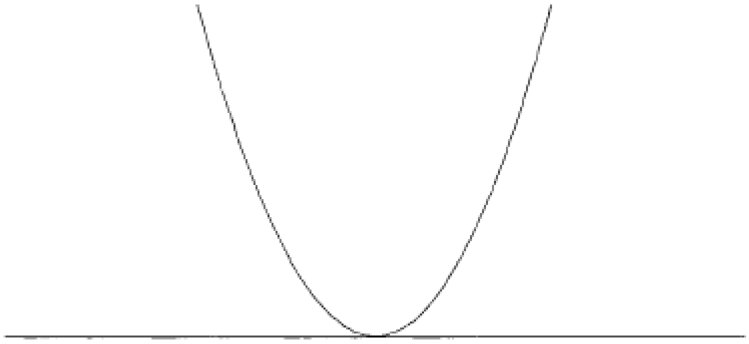
11.4.1 Definition : *If V is* a *k-variety, then the tangent space $T_P(V)$ to V at P is the zero set Z ($\{d_P f : f \in I(V)\}$).*

Example : By the Hilbert basis theorem, any ideal of $k[x_1,...,x_n]$ can be generated by a finite number of polynomials. Suppose that $I(V)$ is generated by $\{f_1,\ldots, f_r\}$. Then we show that $T_P(V) = Z(\{dpf_1,...,dpf_r\}$. If $h = \sum g_i f_i$, then by the product rule,

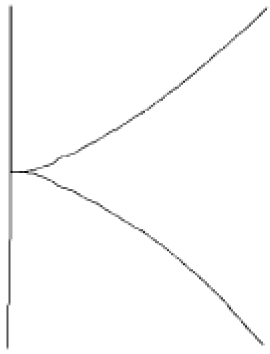
$$\begin{aligned} d_P h &= \sum g_i(P) d_P f_i + \sum d_P g_i \cdot f_i(P) \\ &= \sum d_i(P) d_P f_i. \end{aligned}$$

This shows that $d_P h$ is a linear combination of the $d_P f_i$for any $h \in I(V)$.

Example : If $V = Z(y - x^2)$ and $P = (a, a^2)$, then $Tp(V) = Z(y + 2ax)$. If $P = (0,0)$ is the origin, then $T_P(V)$ is the x-axis.



Example : Let V = Z(y^2-x^3). If *P* = (0,0), then *dp f* = 0 for all $f \in I(V)$. Consequently, $T_P(V)$= C^2.



Example : Let $V = Z(x^2+ y^2+ z^2 - 1)$, and assume that char(k)≠ 2. If *P* = (a, *b, c)* and! x^2+y^2 + $z^2$1, then *dp f = 2ax* + 2by *2cz ,* *so Tp(V) = Z(ax + by + cz).* Since (a, b, *c)*≠(0, 0, 0) for all $P \in V$, the tangent space *Tp(V)* is a 2-dimensional vector space over *C.*

One of the uses of the tangent space is to define non singularity. To keep things as simple as possible, we first consider *hypersurfaces;* that is, varieties of the form *Z(f)* for a single polynomial *f.*

11.4.2 Definition : *Let V = Z(f) be a k-hypersurface. A point $P \in V$ is non-singular, provided that at least one of the partial derivatives $\partial f/\partial x_i$ does not vanish at P; that is, P is non-singular, provided that $d_p f \neq 0$. Otherwise, P is said to be singular. If every point on V is non-singular, then V is said to be non-singular.*

We can interpret this definition in other ways. The tangent space of V = *Z(f)* at *P* is the zero set of $d_p f = \sum_i (\partial f/\partial x_i)(P)x_i$ *, so* $T_p(V)$ is the zero set of a single linear polynomial. If $f \in k[x_1,...,x_n]$, then $T_p(V)$ is either an (n- 1)-dimensional vector space or is all of C^n, depending on whether $d_p f \neq 0$ or not. But, the point $P \in V$ is nonsingular if and only if $dp\, f \neq 0$,so P is non singular if and only if $\dim_k(Tp(V)) = \dim(V) = n - 1$, the latter equality from above Example, and P is singular if $\dim_k(Tp(V)) > \dim(V)$.

Example : The parabola $Z(y - x^2)$ is a nonsingular curve, whereas $Z(y^2 - x^3)$ has a singularity at the origin. Every other point of $Z(y^2 - x^3)$ is nonsingular by an easy calculation. The sphere $Z(x^2 + y^2 + z^2 - 1)$ is also a nonsingular variety, provided that $\mathrm{char}(k) \neq 2$.

For one application of the notion of nonsingularity, we point to Problem 6, which outlines a proof that the function field of the $\mathbb{C}$-variety $Z(y^2 - (x^3 - x))$ is not rational over $\mathbb{C}$.

We now look into nonsingularity for an arbitrary variety. Suppose that V is a k-variety, and let $f_i, \ldots, f_m$, be polynomials that generate the ideal $I(V)$. Let $P \in V$, and consider the Jacobian matrix

$$J(f_1, \ldots, f_m) = \begin{pmatrix} \frac{\partial f_1}{\partial x_1}(P) & \cdots & \frac{\partial f_1}{\partial x_n}(P) \\ \vdots & \ddots & \vdots \\ \frac{\partial f_m}{\partial x_1}(P) & \cdots & \frac{\partial f_m}{\partial x_n}(P) \end{pmatrix}$$

One interpretation of the definition of a nonsingular point on a hypersurfaceis that a point $P \in Z(f)$ is nonsingular if $\mathrm{rank}(J(f)) = 1$, and P is singular if $\mathrm{rank}(J(f)) = 0$. In other words, P is nonsingular if the rank of $J(f)$ is equal to $n - \dim(V)$.

11.4.3 Definition: *Suppose that V is an irreducible k-variety in C^n, and let $f_i, \ldots, f_m$* be generators *of $I(V)$. If $P \in V$, then P is nonsingular if the rank of $J(f_i, \ldots, f_m)$ is equal to $n - \dim(V)$.*

The following proposition shows that $n - \dim(V)$ is an upper bound for the rank of the Jacobian matrix. Thus, a point is nonsingular, provided that the Jacobian matrix has maximal rank. We will call an irreducible k-variety *V absolutely irreducible* if the ideal *I(V)* is an absolutely prime ideal of $k[x_1 ,..., x_n]$.

11.4.4 Proposition : *Suppose that V is an absolutely irreducible k-variety in* C_n *. Let P* ∈ V*, and let fi,…..,fm be generators of the ideal I(V). Then* rank(J(*fi,…..,fm))* ≤ *n* -dim(V).

Proof. We will prove this in a number of steps. Let *K* be the function field of V. The assumption that V is absolutely irreducible means that *K/ k* is a regular extension, by Theorem 22.10. Therefore, *K/k* is separably generated, so

$$\text{trdeg } (K/k) = \dim(\text{Der}_k(K)), \text{ and so } \dim(V) = \dim(\text{Der}_k(K)).$$

The coordinate ring of V is $k[V] = k[x_1,…,x_n]/I(V) = k[s_1,... ,s_n]$, where $s_i = x_i + I(V)$. Thus, $K = k(s_1,... ,s_n)$. Let $Q = (s_1,... ,s_n) \in K^n$. We first point out that

$$I(V) = \{f \in k[x_1, \ldots, x_n] : f(s_1, \ldots, s_n) = 0\}.$$

For $f \in I(V)$, let $d_Q f = \sum_{i=1}^{n} x_i\}(\partial f/\partial x_i)(Q)$. *We* view $d_Q f$ as a linear functional on K^n; that is, we view $d_Q f$ as a linear transformation from K^n to *K* defined by

$$(d_Q f)(\alpha_1, \ldots, \alpha_n) = \sum_{i=1}^{n} \alpha_i \frac{\partial f}{\partial x_i}(Q).$$

Let *M* be the subspace of homK $(K^n\ K)$ spanned by the $d_Q f$ as *f* ranges over *I(V).* Now that we have given an interpretation of the differentials $d_Q f$ as linear functionals, we interpret derivations as elements of *I('*. For $D \in \text{Der}_k(K)$, we obtain an n-tuple $(D(s_1),... ,D(s_n))$. A k-derivation on *K* is determined by its action on the generators $s_1,... ,s_n$of *K/k.*

Therefore, the map $D \to (D(s_1),... ,D(s_n))$ is a K-vector space injection from $\mathrm{Der}_k(K)$ to K^n . We denote by D the image of this transformation. Next, we verify that an n-tuple $(\alpha_1,\ldots,\alpha_n)$ lies in D if and only if $d_Q f(\alpha_1,\ldots,\alpha_n) = 0$. One direction of this is easy. By the chain rule, we see that

$$\sum_{i=1}^{n} \frac{\partial f}{\partial x_i}(Q)D(s_i) = D(f(s_1,\ldots,s_n)) = 0$$

if $f \in I(V)$. For the other direction, suppose that $d_Q f(\alpha_1,\ldots,\alpha_n) = 0$. We define a derivation D on K with $D(s_i) = \alpha_i$ as follows. First, let D' bethe derivation $D' : k[x_1,\ldots,x_n] \to K$ defined by $D' = \sum_i \alpha_i(\partial f/\partial x_i)(Q)$; that is, $D'(f) = \sum_i \alpha_i(\partial f/\partial x_i)(Q)$;.

The condition on the α_I shows that $D'(f) = 0$ if $f \in I(V)$, so D' induces a k derivation $D : k[V] \to K$ defined by $D(g + I(V)) = D'(g)$. The quotient rule for derivations shows that D extends uniquely to a derivation on K, which we also call D. The definition of D' gives us $D(s_i) = \alpha_i$, so $(\alpha_i ,\ldots, \alpha_n) \in D$ as desired. Now that we have verified our claim, we use linear algebra. The subspace D of $K^n$is the set

$$\mathcal{D} = \{v \in K^n : d_Q f(v) = 0 \text{ for all } d_Q f \in M\}.$$

From linear algebra, this implies that $\dim(\mathcal{D}) + \dim(M) = n$. Since

$$\dim(M) = \dim(\mathrm{Der}_k(K)) = \dim(V),$$

we get $\dim(D) = n - \dim(V)$.

The final step is to verify that $\dim(D) = \mathrm{rank}(J')$, where J' is the matrix $((\partial f_i/\partial x_j)(Q))$, and that $\mathrm{rank}(J') \geq \mathrm{rank}(J)$, if J is the Jacobian matrix $((\partial f_i/\partial x_j)(P))$. This will show that

$$\mathrm{rank}(J) \leq \mathrm{rank}(J') = n - \dim(V),$$

our desired result. The first of these claims is easy. The space *D* is spanned by the $d_Q f_i$, since the fi generate the ideal *I (V).*

The i[th] row of *J'* is the matrix representation of the linear transformation $d_Q f_i$,so the rank of *J'* is the dimension of the space spanned by the $d_Q f_i$; in other words, rank(J) =dim(D). For the inequality rank(J') ≥ rank(J), let $P = (a_1,...,a_n) \in V$.

There is a homomorphism $\varphi : k[x_1,...,x_n] \to C$ with $\varphi(x_i) = a_i$. Since *P* ∈V, we have *f (P)* = 0 for all *f* ∈*(V),* so *1(V)* C ker(φ). We get an induced map $\bar{\varphi}: k[V] \to C$ that sends s_i to a_i. Under this map $((\partial f_i/\partial x_j)(Q))$is sent to $(\partial f_i/\partial x_j)(Q)$. If rank(*J'*) r, then the rows of *J'* are linear combinations of some r rows of *J'*.

Viewing $\bar{\varphi}$as a map on matrices, since$\bar{\varphi}(J') = J$ the rows of *J* are linear combinations of the corresponding *r* rows of *J.* Thus, the rank of *J* is at most r, so rank(J') ≥ rank(J). This finishes the proof.
As a consequence of the proof of this proposition, we obtain a relation between the dimension of the tangent space T_P(V) and of V.

11.4.5 Corollary : *Let V be an absolutely irreducible k- variety, and let P ∈V. Then* $\dim(T_P(V)) \geq \dim(V)$, *and* $\dim(T_P(V)) = \dim(V)$ *if and only if P is nonsingular.*

Proof. The tangent space $T_P(V)$ is the set

$$T_P(V) = \{Q \in C^n : d_P f(Q) = 0 \text{ for all } f \in I(V)\}.$$

Using the notation of the proof of the previous proposition, the map induces a map on differentials that sends $d_Q f$ to $d_P f$. If $N = \{d_P f : f \in I(V)\}$, viewed as a subspace of $\hom_C (C^n, C)$, then by linear algebra, we have dim(N) + dim(T_P(V)) = *n* However, $\bar{\varphi}$ sends *M* to *N*, so dim(M)≥ dim(N); hence,

$$\dim(T_P(V)) = n - \dim(N) \geq n - \dim(M)$$
$$= n - \dim(V).$$

Moreover, $\dim(T_P(V)) = \text{rank}(J)$ by the same argument that shows $\dim(D) = \text{rank}(J')$. Therefore, we get equality above exactly when $\text{rank}(J') = \text{rank}(J)$ or when $\text{rank}(J) = n - \dim(V)$. However, this is true if and only if *P* is nonsingular, by the definition of nonsingularity.

Let *k* be a field, and let *C* be an algebraically closed extension of *k.* In One of the above Example, we showed how one can obtain an irreducible k-variety from a finitely generated field extension of *k.* This map is not the inverse of the map that associates to each irreducible k-variety V the function field *k* (V).

In that example, we saw that the nonsingular curve $y = x^2$ has the same function field as the singular curve $y = x^3$. However, nonsingularity is not the only problem. We have only talked about *affine* varieties; that is, varieties inside the affine space C^m. In algebraic geometry, one usually works with *projective* varieties. It is proved in many algebraic geometry books that there is a 1-1 correspondence between finitely generated regular extensions of *k* of transcendence degree 1 and nonsingular projective curves.

Moreover,if we work over ℂ then there is also a 1-1 correspondence between finitely generated extensions of ℂ of transcendence degree 1 and Riemann surfaces. The interested reader can find the correspondence between non-singular projective curves and extensions of transcendence degree 1.

Check your Progress-2

3. What do you understand by Differentials

___

___

___

4. Explain the concept of tangent space of a variety

____
____
____

5. Define Non- singular

____
____
____

11.5 LET US SUM UP

We have seen the concept of derivatives and differential and their geometric application that can be used to define the tangent space to a point of a variety. By using tangent spaces, we are able to define the notion of non-singular point on a variety

11.6 KEYWORDS

Quotient Rule : A **Quotient Rule** is stated as the ratio of the quantity of the denominator times the derivative of the numerator function minus the numerator times the derivative of the denominator function to the square of the denominator function.

Computation : To **compute** is to calculate, either literally or figuratively.

11.7 QUESTIONS FOR REVIEW

1. Let *K* be a separable extension of *F* that is not necessarily algebraic. Show that any derivation on *F* extends to a derivation on *K*.

2. If *K* is a finite separable extension of *F*, show that there is a K-vector space isomorphism $\mathrm{Der}_k(F) \otimes_f K \cong \mathrm{Der}_k(K)$.

11.8 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.*

11.9 ANSWERS TO CHECK YOUR PROGRESS

1. Provide explanation – 11.2

2. Provide proof – 11.2.3

3. Provide explanation –11.3

4. Provide explanation – 11.4

5. Provide explanation and definition – 11.4.2

UNIT-12 DISCRIMINANTS AND TRANSCENDENCE OF Π AND E

STRUCTURE

12.0 OBJECTIVES

Understand the concept of Discriminants and its bilinear form

Comprehend the The Transcendence of π and e

12.1 INTRODUCTION

In this section, we define discriminants and give methods to calculate them. The two best known and most important non rational real numbers areπ and e. In this section, we will show that both of these numbers are transcendental over $\mathbb{Q}$

12.2 DISCRIMINANTS

The discriminant of a polynomial is a generalization to arbitrary degree polynomials of the discriminant of a quadratic. If $K = F(a)$ is a Galois extension of a field F, and if f = min(F, a), then the Galois group

Gal(K/F) can be viewed as a subgroup of the group of permutations of the roots of *f*.

The discriminant determines when this subgroup consists solely of even permutations. We will use this information to describe the splitting field of a polynomial of degree 4 or less. First, there are some are interesting relations L that make calculation discriminants manageable, and there are notions of discriminants in a number of other places, such as algebraic number theory, quadratic form theory, and noncommutative ring theory. While the different notions of discriminant may seem unrelated, this is not the case, as we point out in the following discussion.

The discriminant of a polynomial and an element

The type of discriminant we need in Section 13 is the discriminant of a polynomial. To motivate the definition, consider a quadratic polynomial $f(x)\ x^2 + bx + c$ whose discriminant is $b^2 - 4c$.

The roots of f are = $\alpha_1 = \frac{1}{2}\left(-b + \sqrt{b^2 - 4c}\right)$ and $\alpha_2 = \frac{1}{2}\left(-b - \sqrt{b^2 - 4c}\right)$ Therefore $\sqrt{b^2 - 4c} = \alpha_1 - \alpha_2$, so $b^2 - 4c = (\alpha_1 - \alpha_2)^2$This indicates a way to generalize the notion of the discriminant of a quadratic to higher degree polynomials.

12.2.1 Definition: *Let F be a field with* char(F) $\neq 2$, *and let* $f(x) \in F[x]$. *Let* $\alpha_1, \ldots, \alpha_n$ *be the roots of f in some splitting field K of f over F, and let* $\Delta = \prod_{i<j}(\alpha_i - \alpha_j) \in K$ *Then the discriminant disc(f) of f is the element*

$$D = \Delta^2 = \prod_{i<j}\left(\left(\alpha_i - \alpha_j\right)\right)^2$$

12.2.2 Definition : If *K is an algebraic extension of F with* char(F) $\neq 2$ *and* $\alpha \in K$, *then the discriminant disc(α) is* disc (min(F, α)).

The discriminant disc(α) defined above is dependent on the base field *F*. Also, the element Δ is dependent on the labeling of the roots of *f*, in that a different labeling can change Δ by -1. However, the discriminant does not depend on this labeling. Note that if $f(x) \in F[x]$, then $D = disc(f) =$

0 if and only if *f* has a repeated root. The discriminant thus will give us information only when *f* has no repeated roots. It is in this case that we concentrate our investigation. The discriminant D clearly is an element of *K*. We can say more than that. If *K* is the splitting field of a separable, irreducible polynomial $f \in F[x]$ of degree *n* over *F*, then we view Gal(K/F) as a subgroup of *S*,, by viewing the elements of Gal(K/F) as permutations of the roots of *f*.

12.2.3 Lemma: Let *F be a field with* char(F) ≠ 2, *let* $f(x) \in F[xl$ *be an irreducible, separable polynomial, and let* K *be the splitting field of* $f(x)$ *over F. If* Δ *is defined as in Definition* 10.2.2, *then* $a \in$ Gal(K/F) *is an even permutation if and only if* $\sigma(\Delta) = \Delta$, *and* σ *is odd if and only if* $\sigma(\Delta) = -\Delta$,. *Furthermore,* disc(*f*) $\in F$.

Proof: Before we prove this, we note that the proof we give is the same as the typical proof that every permutation of $S_n$is either even or odd. In fact, the proof of this result about $S_n$is really about discriminants. It is easy to see that each $\sigma \in G =$ Gal(K/F) fixes disc(f), so disc(f) $\in F$. For the proof of the first statement, if $n = \deg(f)$, let $M = F(x_1, \ldots, x_n,,)$. We know that S_n acts as field automorphisms on *M* by permuting the variables. Let $\prod_{i<j}(\alpha_i - \alpha_j)$Suppose that $\sigma \in S_n$ is a transposition, say $\sigma = (ij)$ with $i < j$. Then *a* affects only those factors of *h* that involve i or *j*. We break up these factors into four groups:

$$x_i - x_j$$

$$x_k - x_i, x_k - x_j \text{ for } k < i,$$

$$x_i - x_l, x_j - x_l \text{ for } j < l,$$

$$x_i - x_m, x_m - x_j \text{ for } i < m < j$$

For $k < i$, the permutation $\sigma = (ij)$ maps $x_i - x_j$ to $x_k - x_j$ and vice versa and σ maps $x_i - x_l$ and vice versa for $j < l$ if $i < m < j$, then

$$\sigma(x_i - x_m) = x_j - x_m = -(x_m - x_j)$$

And

$$\sigma\left(x_m - x_j\right) = x_m - x_i = -(x_i - x_m)$$

Finally

$$\sigma\left(x_i - x_j\right) = x_j - x_i = -(x_i - x_j)$$

Multiplying all the terms together gives $\sigma(h) = -h$. Thus, we see for an arbitrary $\sigma \in S_n$ that $\sigma(h) = h$ if and only if σ is a product of an even number of permutations, and $\sigma(h) = -h$ if and only if σ is a product of an odd number of permutations. By substituting the roots α_i of f for the x_i we obtain the desired conclusion.

Recall that the set A_n of all even permutations in S_n is a subgroup; it is called the *alternating* group.

12.2.4 Corollary: *Let F, K, and f be as in Lemma* 10.2.3, *and let* G = Gal(K/F). *Then $G \subseteq A_n$ if and only if disc(f) $\in F^2$. Under the correspondence of the fundamental theorem, the field $F(\Delta) \subseteq K$ corresponds to the subgroup $G \cap A_n$, of G.*

Proof. This follows from the lemma, since $G \subseteq A_n$, if and only if each $\sigma \in G$ is even, and this occurs if and only if $\sigma(\Delta) = \Delta$. Therefore, $G \subseteq A_n$ if and only if disc(f) $\in F^2$.

One problem with the definition of a discriminant is that in order to calculate it we need the roots of the polynomial. We will give other descriptions of the discriminant that do not require knowledge of the roots and lend themselves to calculation. We first obtain a description of the discriminant in terms of determinants.

Let K be a field and let $\alpha_1 \ldots \alpha_n \in K$ Then the *Vandermonde matrix* $V(\alpha_1 \ldots \alpha_n)$ is the $n \times n$ matrix

$$V\left(\alpha_1 - \alpha_n\right) = \begin{bmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^{n-1} \end{bmatrix}$$

12.2.5 Lemma: If *K is* a *field and a , an* E *K, then the determinant of the Vandermonde matrix* V$(\alpha_1 - \alpha_n)$ is $\prod_{i<j}\big((\alpha_1 - \alpha_n)\big)$*.Consequently, if f* ∈ *F[x] has roots* $\alpha_1 - \alpha_n \in K$ *in some extension K of F, then the - discriminant of f is equal to (det* $(V\ (\alpha_1 - \alpha_n))^2$

Proof: Let A = V $(\alpha_1 - \alpha_n)$That det(*A*) = $\prod_{i<j}\big((\alpha_1 - \alpha_n)\big)$ is a moderately standard fact from linear algebra. For those Who have not seen this, we give a proof. Note that if $\alpha_i = \alpha_j$ with $I \neq j$, then det(A) = 0, since two rows of A are the same, so the determinant formula is true in thiscase. We therefore assume that the α_i are distinct, and we prove the result using induction on *n*.

If *n* = 1, this is clear, so suppose that *n* >1. Let *h(x)* = det (V$(\alpha_1, \alpha_2, ... \alpha_{n-1}, x)$*)*. Then *h(x)* is a polynomial of degree less than *n*. By expanding the determinant about the last row, we see that the leading coefficient of *h* is det(V$(\alpha_1, \alpha_2, ... \alpha_{n-1},)$)Moreover, h$(\alpha_i)$ = det(V$(\alpha_1, \alpha_2, ... \alpha_{n-1}, \alpha_i)$ so *h* (α_i)) = 0 if 1 <*i*<*n* — 1. Therefore, *h(x)* is divisible by each *x* - α_i. Since deg(h) <*n* and *h* has $n - 1$ distinct factors, *h(x)* = c $(x - \alpha_1) \ldots (x - \alpha_{n-1})$where *c* = det(V$(\alpha_1, \alpha_2, ... \alpha_{n-1})$). By evaluating *h* at an and using induction, we get.

$$h\ (\alpha_n) = \det \alpha_1, \alpha_2, ... \alpha_n))$$

$$= \prod_{i<j\ \leq n-1} (\propto_j - \alpha_i) \prod_{i<n} (\alpha_n - \alpha_i)$$

$$\prod_{i<n} (\alpha_n - \alpha_i)$$

This finishes the proof that det (V $(\alpha_1, \alpha_2, ... \alpha_n)) = \prod_{i<j}(\alpha_j - \alpha_j)$ The last statement of the lemma is an immediate consequence of this formula and the definition of discriminant.

The discriminant of a polynomial can be determined by the coefficients without having to find the roots, as we proceed to show. This is à convenient fact to describe polynomials of degree 3 and 4. Let A = V$(\alpha_1 \ldots, \alpha_n)$. Then $\det(A)^2 = \det(A^t\ A)$. Moreover,

$$A^tA = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \cdots & \alpha_n^{n-1} \end{bmatrix} \cdot \begin{bmatrix} 1 \alpha_1 \alpha_1^2 \cdots \alpha_1^{n-1} \\ 1 \alpha_2 \alpha_2^2 \cdots \alpha_2^{n-1} \\ \vdots \ \vdots \ \vdots \ \ddots \ \vdots \\ 1 \alpha_n \alpha_n^2 \cdots \alpha_n^{n-1} \end{bmatrix}$$

$$= \begin{bmatrix} t_0 & t_1 \cdots & t_{n-1} \\ t_1 & t_2 \cdots & t_n \\ \vdots & \vdots \ddots & \vdots \\ t_{n-1} & t_n \cdots & t_{2n-2} \end{bmatrix}$$

where $t_i = \Sigma_j \alpha_j^i$. for $i \geq 1$, and $t_0 = n$. Therefore, det $(A)^2$is the determinant of this latter matrix. This is helpful because if the roots of *f(x)* are $\propto_1, \ldots \alpha_n$, then there are recursive relations between the t_i and the coefficients of *f* and so the determinant of the $t_i$can be found in terms of the coefficients of *f*. These relations are called *Newton's identities.* Note that $t_i = T_{K/F} (\alpha_l^i)$if *K* is the splitting field of min(*F*, α_1)

12.2.6 Proportion (Newton's Identities): Let $f(x) = a_0 + a_1 x + \ldots + a_{n-1} x^{n-1} + x^n$ be a monic polynomial over F with roots $\alpha_1, \ldots \alpha_n$ If $t_i = \Sigma_j \alpha_j^i$, then

$$t_m + a_{n-1} t_{m-1} + \ldots + a_{n-m+1} t_1 + m a_{n-m} = 0 \text{ for } m \leq n$$

$$t_m + a_n - t_{m-1} + \ldots + a_0 t_{m-n} = 0 \text{ for } m > n$$

Proof: An alternative way of stating Newton's identities is to use the elementary symmetric functions S_i in the a_i instead of the a_i Since $S_i = (-1)^i a_{n-i}$ Newton's identities can also be written as

$$t_m - s_1 t_{m-1} + S_2 t_{m-2} - + \ldots (-1)^m m a_{n-m} = 0 \text{ for } m \leq n$$

$$t_m + a_n - t_{m-1} + \ldots + a_0 t_{m-n} = 0 \text{ for } m > n$$

The proof we give here is from Mead [21]. The key is arranging the terms in the identities in a useful manner. We start with a bit of notation. If $(a_1, a_2, \ldots a_r)$ is a sequence of non increasing, non-negative integers, let

$$f_{(a_1, a_2, \ldots, a_r)} = \sum \alpha_{\sigma(1)}^{\alpha_1} \ldots \alpha_{\sigma(n)}^{\alpha_r},$$

Where the sum is over all permutations σ of { 1, 2, … , n} that give distinct terms Then $S_i = f_{(1,1,\dots,1)}$ (i ones) and $t_i = f_{(i)}$ To simplify the notation a little, the sequence of $i$once will be denoted (l_i), and the sequence $(\alpha, 1, \dots, 1)$ of length $i + 1$ will be denoted $(a, 1_i)$ It is then straight forward to see that

$$f_{(m-1)}f_{(1)} = f_{(m)} + f_{(m-1,1),}$$

$$f_{(m-2)}f_{(1,1)} = f_{(m-1,1)} + f_{(m-2,1),}$$

$$f_{(m-3)}f_{(1,1,1)} = f_{(m-2,1,1)} + f_{(m-3,1,1,1),}$$

And in general

$f_{(m-i)}, f_{(1i)} = f_{(m-i+1,1,)} + f_{(m-i,1,)}$ for $1 \le i <$ min $\{m-1, n\}$. (12.1)

Moreover, if $m \le n$ and $i = m - 1$ then

$$f_{(1)}f_{(1_{m-1})} = f_{(2,1_{m-2})} + m\, f_{(1_m)}$$

If $m > n = i$, then

$$f_{(m-n)}f_{(1_n)} = f_{(m-n+1,1_{n-1})}$$

Newton's identities then follow from these equations by multiplying the ith equation in (12.1) by $(-1)^{i-1}$ and summing over i

Newton's identities together with Lemma 12.5 give us a manageable way of calculating discriminates of polynomials. As an illustration, we determine the discrimination of a quadratic and a cubic. The calculation of the discriminant of a cubic will come up in Section 13

Example: Let $f(x) = x^2 + bx + c$ then $t_0 = 2$ Also, Newton's identities yield $t_1 + b = 0,$ so $t_1 + b = 0$, so $t_1 = -b$ for t_2 , we have $t_2 + bt_1 + 2c = 0$, so $t_2 = -bt_1 - 2c = b^2 - 2c$ therefore,

Disc $(f) = \begin{vmatrix} 2 & -b \\ -b\ b^2 & -2C \end{vmatrix} = 2\,(b^2 - 2c) - b^2 = b^2 - 4c,$

the usual discriminant of a monic quadratic

Example : Let, $f(x) = x^3 + px + q$ then $a_0 = q, a_1 = p$ and $a_2 = 0$ so by Newton's identities we get

$$t_1 = 0,$$

$$t_2 = -2p,$$

$$t_3 = -3q,$$

$$l_4 = 2p^2,$$

Therefore

$$\text{disc } (f) = \begin{vmatrix} 3 & 0 & -2p \\ 0 & -2p & -3q \\ -2p & -3q & 2p^2 \end{vmatrix} = -4p^3 - 27q^2$$

For an arbitrary monic cubic, we could do a similar calculation. For, if $g(x) = x^3 + ax^2 + bx + c$, let $y = x - a/3$ By Taylor expansion, we have

$$g(x)$$
$$= g(a/3) + g'(a/3)\,(x - a/3) + \frac{g''(a/3)}{2!}(x - a/3)^2 + \frac{g'''(a/3)}{3!}(x - a/3)^3$$

The choice of y was made to satisfy $g''(a/3) = 0$If $p = g'(a/3)$ and $q = g(a/3)$, then $g(x) = y^3 + py + q$ If the roots of g and $\alpha_1 - a/3$, $\alpha_2 - a/3$ and $\alpha_3 - a/3$. Therefore, the definition of discriminant shows that disc $g(x) = disc\ (y^3 + pq + q)$ The interested reader can check that disc $g(x) = a^2(b^2 - 4ac) - 4b^3 - 27c^2 + 18abc$

We give a further description of the discriminant, this time in term of norms

12.2.7 Preposition: Let L = F(α) be a field extension of F If $f(x) = \min(F, \alpha)\ then\ discf = (-1)^{n(n-1)/2} N_{L/F}\big(f'(\alpha)\big)$, Where $f'(x) is\ the\ formal\ derivative\ of\ f$

Proof. Let K be a splitting filed for f over F, and write $f(x) = (x - \propto_1) \ldots (x - \alpha_n) \in K\,[x]$ Set $\alpha = \alpha_1$ then a short calculation shows that $f'(\alpha_j) = \prod_{i=1, i \neq j}^{n} (\alpha_j - \alpha_i)$ If $\sigma_1, \ldots, \sigma_n$ are the F homomorphisms of L to K that satisfy $\sigma_i(\alpha) = \alpha_i$ then by Proportion 8.12

$$N_{L/F}(f'(\alpha)) = \prod_j \sigma_j(f'(\alpha)) = \prod_j f(a_j)$$

Using the formula above for $f'(\propto_j)$ we see by checking signs carefully that

$$N_{L/F}(f'(\alpha)) = \prod_j f'(\alpha_j) = \prod_j \prod_{\substack{i=1 \\ i \neq j}}^{n} (\alpha_{j-} \alpha_i) = (-1)^{\frac{n(n-1)}{2}} disc(f)$$

Example : Let p be an odd prime, and let ω be a primitive pth root of unity in $\mathbb{C}$. We use the previous result to determine disc (ω) Let K= $\mathbb{Q}(\omega)$, the pth cyclotomic extension of $\mathbb{Q}$ If $f(x) = \min(\mathbb{Q}, \omega)$, then $f(x) = 1 + x + \cdots + x^{p-1} = (x^p - 1)/\, x - 1)$ We need to calculate $N_{k/\mathbb{Q}}(f'(\omega))$

First,

$$f'(x) = \frac{px^{p-1}(x-1) - (x^p - 1)}{(x-1)^2},$$

So $f'(\omega) = p\omega^{p-1}/(\omega - 1)$. We claim that $N_{k/\mathbb{Q}}(\omega) = 1$ and $N_{k/\mathbb{Q}}(\omega - 1) = p$ To prove that first equality, by the description of Gal (K/$\mathbb{Q}$) given in corollary 7, 8, we have

$$N_{k/\mathbb{Q}}(\omega) = \prod_{i=1}^{p-1} \omega^i = \omega^{p(p-1)/2} = 1$$

Since p is odd. For the second equality, note that

$$1 + x + \cdots + x^{p-1} = \prod_{i=1}^{p-1} (x - \omega^i)$$

Since $p = \prod_{i=1}^{p-1} (1 - \omega^i)$ However,

$$N_{k/\mathbb{Q}}(\omega - 1) = \prod_{i=1}^{p-1} (\omega^i - 1)$$

So $N_{k/\mathbb{Q}}(\omega - 1) = p$, Where again we use p odd. From this, we see that

$$N_{k/\mathbb{Q}} = (f'(\omega)) = N_{k/\mathbb{Q}}\left(\frac{p\omega^{p-1}}{\omega - 1}\right) = \frac{N_{k/\mathbb{Q}}(p) N_{k/\mathbb{Q}}(\omega)^{p-1}}{N_{k/\mathbb{Q}}(\omega - 1)}$$

$$= \frac{p^{p-1}.1}{p} = p^{p-2}$$

The discriminant of an n tuple and of a field extension

We now define the discriminant of a field extension of degree n and ofan n-tuple in the field extension. We shall see that our definition of the discriminant of an element is a special case of this new definition. Let *K* be a separable extension of *F* with *[K : F] = n.* As we know that *[K : F]* is equal to the number of F-homomorphisms from *K* into an algebraic closure of *F*.

12.2.8 Definition: *Let K be a separable extension of F of degree n, and let* $\sigma_1, \sigma_2, \ldots, \sigma_n$ *be the* distinct F-homomorphisms from K to an algebraic closure of F.

If $\alpha_1, \alpha_2, \ldots, \alpha_n$are any n elements of K, then the discriminant of the n tuple $(\alpha_1, \ldots, \alpha_n)$ is disc $(\alpha_1, \ldots, \alpha_n) = \det(\sigma_i(\alpha_j))^2$If $\beta_1,\ldots, \beta_n$ is any F basis of K, then the discriminant of the field extension K/F is disc (K/F) = disc $(\beta_1, \ldots, \beta_n)$.

The definition of disc(K/F) depends on the choice of basis. We will show just how it depends on the basis. But first, we give another description of the discriminant of an n-tuple, which will show us that this discriminant is an element of the base field *F*.

12.2.9 Lemma : Let K be a separable field extension of F of degree n, and let $\alpha_1, \ldots, \alpha_n \in K$ Then disc $(\alpha_1, \ldots, \alpha_n) = \det(Tr_{K/F}(\alpha_i\alpha_j))$ Consequently, disc $(\alpha_1, \ldots, \alpha_n) \in F$.

Proof. Let $\sigma_1, \ldots, \sigma_n$be the distinct F homomorphisms from K to an algebraic closure of F. If A = $\sigma_i(\alpha_j)$), then the discriminant of the n tuple $\alpha_1, \ldots, \alpha_n$ is the determinant of the matrix A^tA whose ij entry is

$$\sum_k \sigma_k(\alpha_i)\sigma_k(\alpha_j) = \sum_k \sigma_k(\alpha_i\alpha_j)$$

$$= Tr_{K/F}(\alpha_i \alpha_j)$$

Therefore, disc $(\alpha_1, \ldots, \alpha_n)$ = det $(Tr_{K/F}\ (\alpha_i\alpha_j))$

The next result shows that the discriminant can be used to test whether or not an n tuple in K forms a basis for K

12.2.10 Proposition: Let K be a separable field extension of F of degree n, and let $\alpha_1, \ldots, \alpha_n \in$ K. Then disc $(\alpha_1, \ldots, \alpha_n) = 0$ if and only if $\alpha_1, \ldots, \alpha_n$ and linearly dependant over F. Thus $\{\alpha_1, \ldots, \alpha_n\}$ is an F – basis for K if and only if disc $(\alpha_1, \ldots, \alpha_n) \neq 0$

Proof . Suppose that the α_i are linearly depenant over F. Then one of the α_i is an F – linear combination of the others If $\alpha_i = \sum_{k \neq i} a_k a_k$ with $a_j \in$ F , then

$$Tr_{K/F}(\alpha_i \alpha_j) = \sum_k a_k Tr_{K/F}\ (\alpha_i \alpha_j)$$

Therefore, the columns of the matrix $(Tr_{K/F}\ (\alpha_i\alpha_j))$ are linearly dependant over F, so det $(Tr_{K/F}\ (\alpha_i\alpha_j)) = 0$

Conversely, Suppose that det $(Tr_{K/F}\ (\alpha_i\alpha_j)) = 0$ then the rows $R_{1,\ldots} R_n$ of the matrix $(Tr_{K/F}\ (\alpha_i\alpha_j)$ are dependent over F, so there are $a_i \in F$, not all zero, with $\sum_i a_i R_i = 0$ The vector equation $\sum_i a_i R_i = 0$ means that $\sum_i a_i\ (Tr_{K/F}\ (\alpha_i\alpha_j)) = 0$ for each j Let $x = \sum_i a_i \alpha_i$ By linearity of the trace, we see that $Tr_{K/F}(x\alpha_i) = 0$ for each j. If the α_i are independent over F, then they form a basis for K.

Consequently, linearity of the trace then implies that $Tr_{K/F}(xy) = 0$ for all $y \in K$. This means that the trace map is identically zero, which is false by the Dedekind independence lemma. Thus, the α_i are dependent over F

We now see exactly how the discriminant of a field extension depends on the basis chosen to calculate it.

12.2.11 : Let $\{\alpha_1, \ldots, \alpha_n\}$ and $\{\beta_1, \ldots, \beta_n\}$ be two F bases for K. Let A = (a_{ij}) be the $n \times n$ transition matrix between the two bases; that is, $\beta_j = \sum_i a_{ij}\alpha_i$ Then disc $(\beta_1, \ldots, \beta_n)$ = det $(A)^2$ disc $(\alpha_1, \ldots, \alpha_n)$ consequently the coset of disc (K/F) in F^*/F^{*2} is well defined independent of the basis chosen

Proof since $\beta_j = \sum_k a_{kj}\alpha_k$, we have $\sigma_i(\alpha_k)$ In terms of matrices says that

$$\left(\sigma_j(\beta_j)\right) = \left(a_{ij}\right)^t \left(\sigma_j(\alpha_j)\right) = A^t \left(\sigma_j(\alpha_j)\right)$$

Therefore, by taking determinants, we obtain

Disc $(\beta_1, \ldots, \beta_n) = \det(A)^2 \, disc \ (\alpha_1, \ldots, \alpha_n)$.

The final statement of the proposition follows immediately from this relation together with the fact that the discriminant of a basis is non zero, by Preposition 12.13

To make the definition of discriminant of a field extension well defined, one can define it to be the coset in F^*/F^{*2} represented by disc $(\alpha_1, \ldots, \alpha_n)$ for any basis $\{\alpha_1, \ldots, \alpha_n\}$of K. This eliminates ambiguity although it is not always the most convenient way to work with discriminants.

Example : In this example, we show that the discriminant of a polynomial is equal to the discriminant of an appropriate field extension. Suppose that K = $F\ (\alpha)$ is an extension of F of degree n. Then 1, $\alpha, \alpha^2, \ldots, \alpha^{n-1}$ is a basis for K. We calculate disc (K/F) relative to this basis. We have disc (K/F) = det $(\sigma_i(\alpha^{j-1}))^2$ consequently, if $\alpha_i = \sigma_i(\alpha)$, then disc (K/F) = det $\begin{pmatrix} 1\sigma_1(\alpha)\cdots\sigma_1(\alpha^{n-1}) \\ 1\sigma_2(\alpha)\cdots\sigma_2(\alpha^{n-1}) \\ \vdots \quad \vdots \quad \ddots \quad \vdots \\ 1\sigma_n(\alpha)\cdots\sigma_n(\alpha^{n-1}) \end{pmatrix}^2$

= det $\left(V(\alpha_1, \alpha_2, \ldots, \alpha_n)\right)^2$

Therefore, disc (K/F) = disc $(\alpha) = disc$ (min(F, α))

Example: Let K = ($\mathbb{Q}$ $(i)/\mathbb{Q}$) = det $\begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}^2 = (-2i)^2 = -4$

More generally, if K = $\mathbb{Q}(\sqrt{d})$ with d a square free integer, then using 1, $\sqrt{d}$ as a basis, we see that the discriminant is $4d$

12.3 THE DISCRIMINANT OF BILINEAR FORM

We now extend the idea of discriminant to its most general form that we consider. The two previous notions of discriminant will be special cases of this general form. If V is an F – vector space, a bilinear form an V is a mapping B : V $\times V \rightarrow F$ that is linear each variable. In other words, for all $u, v, w \in V$ and all $\alpha\ \beta \in F$, we have

$$B\ (u, \alpha v + \beta\omega) = \alpha B(u, v) + \beta B\ (u, w),$$

$$B\ (\alpha u + \beta v, \omega) = \alpha B(u, w) + \beta B\ (u, w),$$

12.3.1 Definition : If V is an F vector space and if B : V × V→ F is bilinear form then the discriminant of B relative to a basis V = {v_1, . . ., v_n} of V is disc (B)v = det (B(v_i, v_j))

As with the discriminant of a field extension, this definition depends on the choice of basis. If W = {w_1, . . ., w_n} is another basis, let A be the matrix describing the basis change, that is, if A = $\left(a_{ij}\right)$, then $w_j = \sum_i a_{ij} v_i$

By the bilinearity of B, we have

B $(w_i, w_j) = B\left(\sum_k a_{ik} v_k \sum_l a_{jl} v_l\right) = \sum_{k,l} a_{ik} B\,(v_k, v_l) a_{jl}$

Therefore, if follows that (B $(w_i, w_j) = A^t\big(B(v_k v_l)\big)A$ Taking determinants gives

Disc $(B)_w = \det(A)^2\ disc\ (B)_{v1}$

The same relation that was found for field extension

A bilinear form is non degenerate if B $(v, w) = 0\ for$ all w only if $v = 0,$ if B (v, w) = 0 for all v only if $w = 0$ As in Section 11, if we define $B_v : V \rightarrow F$ by $B_v(\omega) = B\ (v, w)$ then the map $v \rightarrow B_v$ is a homomorphism from V to $hom_F\ (V, F)$ The form B is nondegenerate if and only if this homomorphism is injective. If we represent this homomorphism by a matrix, using the basis V and the dual basis for $hom_F(V, F),$ then this matrix is (B $(v_i v_j)$). Therefore B is non degenerate if and only if disc $(B)_v \neq 0$ This condition is independent of the basis, by the change of basis formula above for the discriminant

Example: We now show that the discriminant of a field extension is the discriminant of the trace form. Let K be a finite separable extension of F Let B : $K \times K \rightarrow F$ be defined by B $(a, b) = T_{K/F}(a$b) Then B is a bilinear form because the trace is linear. The discriminant of B relative to a basis V = $\{v_1, \ldots, v_n\}$ is det $(T_{K/F}\ (v_i v_j))$. But, by Lemma 12.12 this is the discriminant of K/F Therefore, the previous notion of discriminant are special cases of the notion of discriminant of a bilinear form.

Check your Progress-1

1. Explain The concept of Discriminant

2. State and prove **Newton's Identities**

12.4 THE TRANSCENDENCE OF Π AND E

12.4.1 Theorem: (Lindemann – Weierstrauss) –Let $\alpha_1, \dots \alpha_m$ be distinct algebraic number. Then the exponentials $e^{\alpha_1}, \dots e^{\alpha_m}$ are linearly independent over $\mathbb{Q}$

12.4.2 Corollary : The numbers π and e are transcendental over $\mathbb{Q}$

Proof: of the corollary: Suppose that e is algebraic over $\mathbb{Q}$ Then there are rational r_i with $\sum_{i=0}^{n} r_i e^i = 0$ This mean that the numbers e^0, e^1, …, e^{n-1} are linearly dependant over $\mathbb{Q}$ By closing $m = n + 1$ and $\alpha_i = i - 1$ this dependence is false by the theorem. Thus e is transcendental over $\mathbb{Q}$ for π we note that if π is algebraic over $\mathbb{Q}$ then so, is πi; hence $e^0, e^{\pi i}$ are linearly independent over $\mathbb{Q}$, which is false since $e^{\pi i} = -1$ thus, π is transcendental over $\mathbb{Q}$

Proof of the Theorem: Suppose that there are $a_j \in \mathbb{Q}$ with

$$\sum_{j=1}^{m} a_j e^{\alpha_j} = 0$$

By multiplying by a suitable integer, we may assume that each $a_j \in \mathbb{Z}$, moreover , by eliminating terms if necessary, we may also assume that each $a_j \neq 0$ Let K be the normal closure of $\mathbb{Q}(\alpha_1, \dots \alpha_m)$ Then K is a Galois extension of $\mathbb{Q}$ suppose that Gal $(K/\mathbb{Q}) = \{\sigma_1, \dots \sigma_m\}$ Since $\sum_{j=1}^{m} a_j e^{\alpha_j} = 0$ we have

$$0 = \prod_{k=1}^{n}\left(\sum_{j=1}^{b} a_j e^{\sigma_k(\alpha_j)}\right) = \sum_{j=0}^{r} c_j e^{\beta_j}$$

Where $c_j \in \mathbb{Z}$, and then β_j can be chosen to be distinct elements of K by gathering together terms with the same exponent. Moreover, some $c_j \neq 0$ (See problem 4); without loss of generality say $c_0 \neq 0$ If $\sigma \in$ Gal (K/$\mathbb{Q}$) then the n terms $\sum_{j=1}^{n} a_j e^{\sigma\sigma_k(\alpha_j)}$ for $1 \leq k \leq n$ are the terms $\sum_{j=1}^{n} a_j e^{\sigma_k(\alpha_j)}$ in some order, so the product is unchanged when replacing $\sigma_k(\alpha_j)$ by $\sigma\sigma_k(\alpha_j)$ since both $\beta_j$is a sum of terms of the form $\sigma_k(\alpha_l)$ the exponents in the expansion of $\prod_{k=1}^{n}\left(\sum_{j=1}^{n} a_j e^{\sigma\sigma_k(\alpha_j)}\right)$ are the various σ (β_j) thus we obtain equations

$$0 = \sum_{j=0}^{r} c_j e^{\sigma_i(\beta_j)}$$

For each i Multiplying the ith equation by $e^{\sigma_i(\beta_0)}$, we get

$$0 = c_0 + \sum_{j=1}^{r} c_j e^{\sigma_i(\gamma_j)} \qquad (1)$$

Where $\gamma_j = \beta_j - \beta_0$ Note that $\gamma_j \neq 0$ since the β_j are all distinct. Each $\gamma_j \in K$; hence γ_j is algebraic over $\mathbb{Q}$ thus, for a fixed j, the elements $\sigma_j(\gamma_j)$ are roots of a polynomial $g_i(x) \in \mathbb{Q}[x]$ where the leading coefficient $b_j g_i(x)$can be taken to be a positive integer. Moreover we may assume that $g_i(0) \neq 0$ by using an appropriate multiple of min ($\mathbb{Q}$, γ_j) for $g_i(x)$

We now make estimates of some complex integrals. If $f(x)$ is a polynomials, let

$$F(x) = \sum_{i=0}^{\infty} f^{(i)}(x)$$

Where $f^{(i)}(x)$ is the ith derivative of f. This sum is finite since f is a polynomial, so F is also a polynomial. Note that $F(x) - F'(x) = f(x)$, so

$$\frac{d}{dx} = (e^{-x}F(x) = -e^{-x}f(x)$$

Therefore

$$\int_0^a e^{-x} f(x)dx = F = 0 - e^{-a} F(a)$$

Or

$$F(a) - e^a F(0) = -e^a \int_e^a e^{-x} f(x)dx$$

By setting $a = \sigma_i(\gamma_j)$, multiplying by c_j and summing over i and j we get

$$\sum_{j=1}^{r}\sum_{i=1}^{n} c_j F(\sigma_j(\gamma_j)) - F(0)\sum_{j=1}^{r}\sum_{i=1}^{n} c_j e^{\sigma_i(\gamma_j)}$$
$$= -\sum_{j=1}^{r}\sum_{i=1}^{n} c_j e^{\sigma_i(\gamma_j)} \int_0^{\sigma_i(\gamma_j)} e^{-z} f(z)dz$$

Using Equation (1) and rearranging the second sum gives us an equation

$$nc_0 F(0) + \sum_{j=1}^{r} c_j \sum_{i=1}^{n} F\left(\sigma_j(\gamma_j)\right)$$
$$= -\sum_{j=1}^{r}\sum_{i=1}^{n} c_j e^{\sigma_i(\gamma_j)} \int_0^{\sigma_i(\gamma_j)} e^{-z} f(z)dz \qquad (2)$$

We define f by

$$f(x) = \frac{(b_1 \dots b_r)^{prn}}{(p-1)!} x^{p-1} \left(\prod_{j=1}^{r} g_j(x)\right)^p$$

Where p is a prime yet to be specified. Recall that b_i is the leading coefficient of $g_i(x)$ and that each b_i is a positive integer. From this definition, we see that

$$0 = f(0) = f'(0) = \cdots = f^{(p-2)}(0)$$

Notes

While $f^{(p-2)}(0) = (b_1 \dots b_r)^{pnr} \prod_{j=1}^{r} g_j(0)^p \neq 0$ We choose p to be any prime larger than $max_j\{b_{j,}g_j(0)\}$, so that p does not divide $f^{(p-1)}$ (0) However, for $t \geq p$, the polynomial $f^{(t)}(x)$ can be written the form

$$f^{(t)}(x) = p(b_1 \dots b_r)^{pnr} h_t(x),$$

Where $h_j(x) \in \mathbb{Z}[x]$ has degree at most $rn-1$. Thus $f^{(t)}(0)$ is divisible by p for $t \geq p$ hence, $F(0) = f^{(p-1)}(0) + \sum_{j \neq p-1} f^{(j)}(0)$ is not divisible by p If we further restrict p so that $p > n$ and $p > c_0$, then p does not divided $nc_0 F(0)$ We will complete the proof by showing that the first sum in Equation (14.2) is an integer divisible by p and that the right hand side of Equation 14.2 goes to 0 as p gets large. Thus will show that the left hand side in at least 1 in absolute value, which will then give a contradiction

We now show that $\sum_{j=1}^{r} c_j \sum_{i=1}^{n} F(\sigma_j \gamma_j))$ is an integer divisible by p. We do this by showing that each term $\sum_{i=1}^{n} F(\sigma_j \gamma_j))$ is an integer divisible by p now,

$$\sum_{i=1}^{n} F\left(\sigma_j(\gamma_j)\right) = \sum_{k} \sum_{i=1}^{n} f^{(k)}\left(\sigma_j(\gamma_j)\right)$$

Since $g_j(x)^p \; divides \; f(x)$ and each $\sigma_j(\gamma_j)$ is a root of $g_j(x)$ we see that

$$0 = f\left(\sigma_j(\gamma_j)\right) = f'\left(\sigma_j(\gamma_j)\right) = \cdots f^{(p-1)}\left(\sigma_j(\gamma_j)\right)$$

For $t \geq p$ since $f^{(t)}(x) = p\,(b_1 \dots b_r)^{pnr} h_j(x)$,

$$\sum_{i=1}^{n} f^{(t)}\left(\sigma_j(\gamma_j)\right) = p \sum_{i=1}^{n} (b_1 .. b_r)^{pnr} h_t\left(\sigma_j(\gamma_j)\right) \qquad (3)$$

However, this sum is invariant under the action of Gal (K/ℚ), so it is a rational number. Moreover $\sum_{i=1}^{n} (b_1 \dots b_r)^{pnr} h_j(x_i)$, is a symmetric polynomial in $x_1, \dots x_n$ of degree at most $prn - 1$ The $\sigma_j(\gamma_j)$ are roots of the polynomial $g_i(x)$ whose leading coefficient is b_j so the second sum in Equation 14.3 is actually an integer by an application of the symmetric function theorem (see Problem 5) this shows that

$\sum_{j=1}^{r} c_j \sum_{i=1}^{n} F(\sigma_j \gamma_j))$ is an integer divisible by p hence the left hand side of Equation (2) is a nonzero integer. This means that

$$\left| \sum_{j=1}^{r} \sum_{i=1}^{n} c_j e^{\sigma_i(\gamma_j)} \int_0^{\sigma_i(\gamma_j)} e^{-z} f(z) dz \right| \geq 1$$

Let

$$m_1 = \max_j \{ |C_j| \},$$

$$m_2 = \max_{i,j} \{ |e^{\sigma_i(\gamma_j)}| \},$$

$$m_3 = \max_{i,j} \{ |\sigma_j{}^{\sigma_i(\gamma_j)}| \},$$

And

$$m_4 = \max_{s \in [0,1]} \{ |e^{-z}| : z = s\sigma_i(\gamma_j) \},$$

$$m_5 = \max_{s \in [0,1]} \left\{ \prod_{j=1}^{r} |gi^{(z)}| : z = s\sigma_i(\gamma_j) \right\}$$

On the straight line path from 0 to $\sigma_i(\gamma_j)$ we have the bound $|z^{p-1}| \leq$

$|\sigma_i(\gamma_j)|^{p-1} \leq$

m_3^{p-1} This yields the inequality

$$\left| \int_0^{\sigma_i(\gamma_j)} e^{-z} f(z) dz \right| \leq m_3 m_4 \frac{(b_1 \cdots b_r)^{prn}}{(p-1)!} m_3^{p-1} m_5^p$$

$$= m_4 \frac{(b_1 \cdots b_r)^{prn}}{(p-1)!} m_3^p m_5^p.$$

Combing this will the previous inequality gives

$$1 \leq \left| \sum_{j=1}^{r} \sum_{i=1}^{n} \right.$$

$$\leq rnm_1 m$$

$$= rnm_1 m$$

Since $u^p/(p-1)! \to 0$ as $p \to \infty$ the last term in the inequality above can be made arbitrarily small by choosing p large enough This gives a contradiction, so our original hypothesis that the exponentials $e^{\alpha_1}, \ldots, e^{\alpha_m}$ are linearly dependant over $\mathbb{Q}$ is false. This proves the theorem

While we have proved that π and e are transcendental over $\mathbb{Q}$, it is unknowns if π is transcendental over $\mathbb{Q}(e)$ or if e is transcendental over $\mathbb{Q}(\pi)$ To discuss this further, we need a definition from Section 19. If K is a field extension of F, then $a_1, \ldots\ldots a_n \in K$ are algebraically independent over F if whenever $f \in F\,[x_1, \ldots.\, x_n]$ is a polynomial with $f\,(a_1, \ldots\ldots a_n) = 0$, then $f = 0$ It is not hard to show that π and e are algebraically independent over $\mathbb{Q}$ if and only if is transcendental over $\mathbb{Q}(e)$, if and only if e is transcendental over $\mathbb{Q}(\pi)$; see Problem 2 A possible generalization of the Lindemann – Weierstrauss theorem in Schanuel's conjecture, which states that if $y_1, \ldots.\, y_n$ are $\mathbb{Q}$ linearly independent complex numbers, then at least n of the numbers $y_1, \ldots, y_n$ are $\mathbb{Q}$ - linearly independent complex numbers, then at least n of the numbers $y_1, \ldots, y_n, e^{y_1}, \ldots., e^{y_n}$ are algebraically independent over $\mathbb{Q}$ If Schanuel's conjecture is true, then $e \; and \; \pi$ are algebraically independent over $\mathbb{Q}$; this is left to Problem 3

Check your Progress-2

3. State Lindemann – Weierstrauss theorem

____

____

____

4. *Prove :* The numbers π and e are transcendental over $\mathbb{Q}$

____

____

____

12.5 LET US SUM UP

We have discussed about the determinant of a polynomial is a generalization to arbitrary degree polynomials of the discriminant of a quadratic. We have seen that using the transcendence of π to prove that it is impossible to square the circle, one of the ruler and compass construction questions of ancient Greece that remained unsolved for 2500years

12.6 KEYWORDS

Generalizations - are where students tell about the pattern they see in the relationship of a certain group of numbers. It's a pattern than is always true.

Inequality - compares two values, showing if one is less than, greater than, or simply not equal to another value

12.7 QUESTIONS FOR REVIEW

1. If B is a nondegenerate bilinear form on V, show that any basis has a dual basis.

2. Let { *ei* } be a basis for *Fn* , and choose an ai E *F* for each i. Define B on this basis by $B(e_i, e_j) = 0$ if $i \neq j$ and $B(e_i , e_i) = a_i \in F$. Prove that this function extends uniquely to a bilinear form $B : Fn$ x Fn F, and determine the discriminant of B.

12.8 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

12.9 ANSWERS TO CHECK YOUR PROGRESS

1. Provide explanation – 12.2
2. Provide statement and proof – 10.2.6
3. Provide statement –12.4.1
4. Provide proof – 12.4.2

UNIT-13 SOLVING POLYNOMIALS BY RADICALS

STRUCTURE

13.0 OBJECTIVES

Understand the Method of Ruler and Compass Constructions

Comprehend Solvability by Radicals

13.1 INTRODUCTION

In the days of the ancient Greeks, some of the major mathematical questions involved constructions with ruler and compass. In spite of the ability of many gifted mathematicians, a number of questions were left unsolved. It was not until the advent of field theory that these questions could be answered. The full story of solvability of polynomials was then discovered by Galois, who proved a necessary and sufficient condition for a polynomial to be solvable. His work introduced the notion of a group and was the birth of abstract algebra.

13.2 METHODS OF RULER AND COMPASS CONSTRUCTIONS

We consider in this section the idea of constructibility by ruler and compass, and we answer the following four classical questions:

1. Is it possible to trisect any angle?
2. Is it possible to double the cube? That is, given a cube of volume V, a side of which can be constructed, is it possible to construct a line segment whose length is that of the side of a cube of volume 2V?
3. Is it possible to square the circle? That is, given a constructible circle of area A, is it possible to construct a square of area A?
4. For which n is it possible to construct a regular n-gon?

The notion of ruler and compass construction was a theoretical one to the Greeks. A ruler was taken to be an object that could draw perfect, infinitely long lines with no thickness but with no markings to measure distance. The only way to use a ruler was to draw the line passing through two points. Similarly, a compass was taken to be a device that could draw a perfect circle, and the only way it could be used was to draw the circle centered at one point and passing through another. The compass was sometimes referred to as a "collapsible compass"; that is, after drawing a circle, the compass could not be Lifted to draw a circle centered at another point with the same radius as that of the previous circle. Likewise, given two points a distance d apart, the rulercannot be used to mark a point on another line a distance d from a given point on the line.

The assumptions of constructibility are as follows. Two points are given and are taken to be the initial constructible points. Given any two constructible points, the line through these points can be constructed, as can the circle centered at one point passing through the other. A point is constructible if it is the intersection of constructible lilies and circles.

The first thing we note is that the collapsibility of the compass is not a problem, nor is not being able to use the ruler to mark distances. Given two constructible points a distance d apart, and a line $l$with a point P on l, we can construct a point Q on la distance d from P. Also, if we can construct a circle of radius r, given any constructible point P, we can construct the circle of radius r centered at P. These facts are indicated in Figure 13.1 .It is left as an exercise (Problem 4) to describe the construction indicated by the figure.

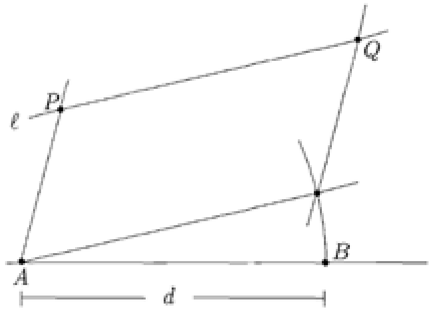


FIGURE 13.1. Construction of Q on ℓ a distance d from P.

There are some standard constructions from elementary geometry that we recall now. Given a line and a point on the line, it is possible to construct a second line through the point perpendicular to the original line. Also, given a line and a point not on the line, it is possible to construct a second line parallel to the original line and passing through the point. These facts are indicated in Figure 13.2.

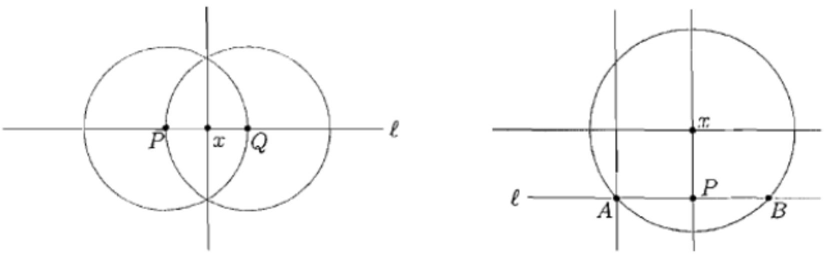


Figure 13.2 Construction of lines perpendicular and parallel to l passing through x

So far, our discussion has been purely geometric. We need to describe ruler and compass constructions algebraically in order to answer our four questions. To do this, we turn to the methods of analytic geometry. Given our original two points, we set up a coordinate system by defining the x-axis to be the line through the points, setting one point to be the origin and the other to be the point (1, 0).We can draw the line perpendicular to the x-axis through the origin to obtain the y-axis.

Let $a \in \mathbb{R}$ We say that a a constructible number if we can construct two points a distance $|a|$ apart. Equivalently, a is constructible if we can construct either of the points $(a, 0)$ or $(0, a)$. If a and b are constructible numbers, elementary geometry tells us that $a + b, a - b, ab,$ and a/b (if $b \neq 0$) are all constructible. Therefore, the set of all constructible

FIGURE 13.3. Construction of $a + b$ and $a - b$.

numbers is a subfield of $\mathbb{R}$ Furthermore, if $a < 0$ is constructible, then so is $\sqrt{a}$ These facts are illustrated in Figures $13.3 - 13.5$

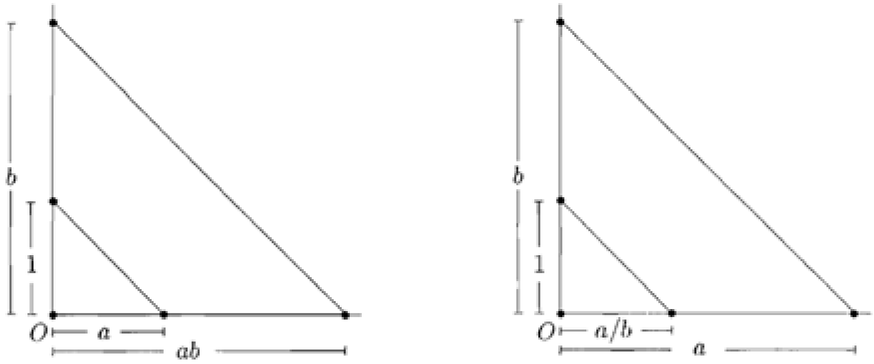


FIGURE 13.4. Construction of ab and a/b.

Suppose that *P* is a constructible point, and set *P* = *(a, b)* in our coordinates system. We can construct the lines through *P* perpendicular to the x-axis and y-axis; hence, we can construct the points (a, 0) and (0, *b).*Therefore, a and *b* are constructible numbers. Conversely, if a and *b* are constructible numbers, we can construct (a, 0) and (0, *b),* so we can construct *P* as the intersection of the line through (a, 0) parallel to the y-axis with the line through (0, *h)* parallel to the x-axis. Thus, *P* = *(a, b)* is constructible if and only if a and *b* are constructible numbers.

In order to construct a number *c,* we must draw a finite number of lines and circles in such a way that $|c|$ is the distance between two points ofintersection. Equivalently, we must draw line and circles so that *(c*, 0) isa point of intersection. If we let *K* be the field generated over ℚ by all the numbers obtained in some such construction, we obtain a subfield of the field of constructible numbers. To give a criterion for when a number

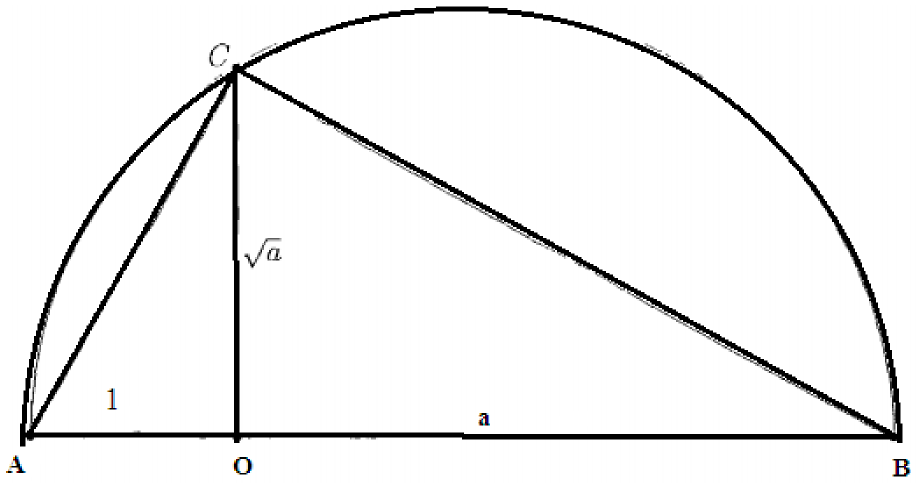


FIGURE 13 .5. Construction of $\sqrt{a}$.

is constructible, we need to relate constructible to properties of the field extension K/ℚ. We do this with analytic geometry. Let *K* be a subfield of ℝ. Given any two points in the plane of *K*, we obtain a line through these points. This will be called a *line in K.* It is not hard to show that a line in *K* has an equation of the form $ax + by + c = 0$ with a, *b, c* ∈*K.* If *P* and *Q* are points in the plane of *K*, the circle with center *P* passing through *Q* is called a *circle in K.* Again, it is not hard to show that the equation of a circle in *K* can be written in the form $x^2 + y^2 + ax + by + c = 0$ for some a, *b, c* ∈ *K.* The next lemma gives us a connection between constructability and field extensions.

Lemma 13.2.1 Let K be a subfield of ℝ

1. The intersection of two lines in K is either empty or is a point in the plane of K.
2. The intersection of a line and a circle in. K is either empty or consists of one or two points in the plane of K($\sqrt{u}$) for some $u \in K$ with $u > 0$

3. The intersection of two circles in K is either empty or consists of oneor two pointsin the plane of $K(\sqrt{u})$ for some $u \in K$ with $u \geq 0$

Proof: The first statement is an easy calculation. For the remaining two statements, it suffices to prove statement 2, since if $x^2 + y^2 + ax + by + c = 0$and $x^2 + y^2 + a'x + b'y + c' = 0$are the equations of circles *C* and *C′*,respectively, then their intersection is the intersection of *C* with the line$(a - a')x + (b - b')y + (c - c') = 0$. So, to prove statement 2, suppose thatour line *L* in *K* has the equation $dx + ey + f = 0$. We assume that $d \neq 0$,since if *d* = 0, then $e \neq 0$. By dividing by *d*, we may then assume that *d* = 1. Plugging $-x = ey + f$into the equation of *C*, we obtain

$$(e^2 + 1)y^2 + (2ef - ae + b)y + (f^2 - af + c) = 0$$

Writing this equation in the form of $\alpha y^2 + \beta y + \gamma = 0$ if $\alpha = 0$ then $y \in K$ If $\alpha \neq 0$ then completing the square shows that either $L \cap C = \emptyset$ or $y \in K\sqrt{\beta^2 - 4\alpha\gamma}$ with $\beta^2 - 4\alpha\gamma \geq 0$

From this lemma, we can turn the definition of constructability into a property of field extension of $\mathbb{Q}$, and in doing so obtain a criterion for when a number is constructible

13.2.2 A real number c is constructible if and only if there is a tower of fields $\mathbb{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_r$ Such that $c \in K_r \, and \, [K_{i+1} : K_i] \leq 2$ for each i Therefore, if c is constructible, then c algebraic over $\mathbb{Q}$, and $[\mathbb{Q}(c) : \mathbb{Q}]$ is power of 2

Proof: If *c* is constructible, then the point *(c,* 0) can be obtained from a finite sequence of constructions starting from the plane of $\mathbb{Q}$. We thenobtain a finite sequence of points, each an intersection of constructible linesand circles, ending at *(c,* 0). By Lemma 15.1, the first point either lies in$\mathbb{Q}$ or in $\mathbb{Q}(\sqrt{u})$ for some u. This extension has degree either 1 or 2. Eachtime we construct a new point, we obtain a field extension whose degreeover the previous field is either 1 or 2 by the lemma. Thus, we obtain asequence of fields

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq K_2 \subseteq \ldots \subseteq K_r$$

With $[K_{i+1} : K_i] \leq 2$ and $c \in K_r$ Therefore $[K_r : \mathbb{Q}] = 2^n$ for some n. However, $[\mathbb{Q}(c): \mathbb{Q}]$ divides $[K_r : \mathbb{Q}]$, so $[\mathbb{Q}(c): \mathbb{Q}]$ is also a power of 2

For the converse suppose that we have a tower $\mathbb{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_r$ with $c \in K$ and $[K_{i+1} : K_i] \leq 2$ for each i We show that c is not constructible by induction on r. If $r = 0$ then $c \in \mathbb{Q}$ so c is constructible Assume that the $r > 0$ and that elements of K_{r-1} are constructible since $[K_r : K_{r-1}] \leq 2$ the quadratic formulas shows that we may write $K_r = K_{r-1}(\sqrt{a})$ for some $a \in K_{r-1}$ Since a is constructible by assumption, so is $\sqrt{a}$. Therefore, $K_r = K_{r-1}(\sqrt{a})$ lies in the field of constructible numbers, hence c is constructible.

With this theorem, we are now able to answer the four questions posed earlier. We first consider trisection of angles. An angle of measure θisconstructible if we can construct two intersecting lines such that the angle between them is θ. For example, a 60° angle can be constructed because the point ($\sqrt{3}$/2, 1/2) is constructible, and the line through this point and (0, 0) makes an angle of 60° with the x-axis.

Suppose that P is the point of intersection on two constructible lines. By drawing a circle of radius 1centered at P, Figure 13.6 shows that if $\theta$is the angle between the two lines, then sin θ and cos θ are constructible numbers. Conversely, if sin $\theta$and cos θ are constructible, then $\theta$is a constructible angle (see Problem2). In order to trisect an angle of measure θ, we would need to be able to construct an angle of θ /3.

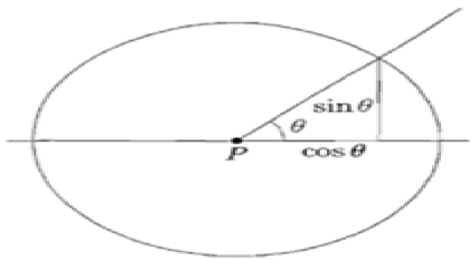


FIGURE 13 .6. Construction of sines and cosines.

Notes

13.3.3 Theorem: It is impossible to trisect a $60°$ angle by ruler and compass construction.

Proof: As noted above, a $60°$ angle can be constructed. If a $60°$ angle can be trisected, then it is possible to construct the number $\alpha = cos20°$ However, the triple angle formula $cos3\theta = 4cos^3\theta - 3\,cos\theta$ gives $4\alpha^3 - 3\alpha = \cos 60° = 1/2$ Thus, α is algebraic over $\mathbb{Q}$. The polynomial $8x^3 - 6x - 1$ is irreducible over $\mathbb{Q}$ because it has no rational roots. Therefore $[\mathbb{Q}(r): \mathbb{Q}] = 3$, so α is not constructible. A $20°$ angle cannot then be constructed, so $60°$ degree angle cannot be trisected.

This theorem does not say that no angle can be trisected. A $90°$ angle can be trisected, since a $30°$ angle can be constructed. This theorem only says that not all angles can be trisected, so there is no method that will trisect an arbitrary angle.

The second classical impossibility we consider is the doubling of a cube.

13.3.4 Theorem: It is impossible to double a cube of length 1by ruler and compass construction

Proof: The length of a side of a cube of volume 2 is $\sqrt[3]{2}$ The minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$ is $x^3 - 2$ Thus, $[\mathbb{Q}\left(\sqrt[3]{2}\right) : \mathbb{Q}] = 3$ is not a power of 2, so $\sqrt[3]{2}$ is not constructible

The third of the classical impossibilities is the squaring of a circle. For this, we need to use the fact that π is transcendental over $\mathbb{Q}$

13.5.5 Theorem: It is impossible to square a circle of radius 1

Proof: We are asking whether we can construct a square of area πTo doso requires us to construct a line segment of length$\sqrt{\pi}$, which is impossiblesince $\sqrt{\pi}$ is transcendental over $\mathbb{Q}$ by last question concerns construction of regular $n - gons$. To determinewhich regular r $n - gons$ can be constructed, we will need information aboutcyclotomic extensions. Recall from Section 7 that if ω is a primitive $n$throot of unity, then $[\mathbb{Q}(\omega) : \mathbb{Q}] = \emptyset(n)$, where $\emptyset$is the Euler phi function.

13.5.6 Theorem : A regular n – gon is constructible if and only if $\emptyset(n)$is a power of 2

Proof : We point out that a regular n – gon is constructible if and only if the central angles $2\pi/n$ are constructible, and this occurs if and only if $\cos(2\pi/n)$ is a constructible number. Let $\omega = e^{2\pi i/n} = \cos(2\pi/n) + isin(2\pi/n)$ is primitive nth root of unity. Then $\cos\left(\frac{2\pi}{n}\right) + \frac{1}{2}(\omega + \omega^{-1})$, Since $\omega^{-1} = \cos(2\pi/n)$ Thus$\cos(2\pi/n) \in \mathbb{Q}(\omega)$. However$\cos(2\pi/n) \in \mathbb{R})$ And $\omega \notin \mathbb{R}$ so $\mathbb{Q}(\omega) \neq \mathbb{Q}\cos(2\pi/n)$ But ω is not root of $x^2 - 2\cos(2\pi/n)x + 1$as an easy calculation shows. So $[\mathbb{Q}\omega : \mathbb{Q}(\cos(2\pi/n))] = 2$ Therefore, if $\cos(2\pi/n)$ is constructible, then $[\mathbb{Q}\cos(2\pi/n) : \mathbb{Q}]$ is a power of 2. Hence, $\emptyset(n) = [\mathbb{Q}\omega : \mathbb{Q}]$ is also power of 2.

Conversely, suppose that $\emptyset(n)$ is a power of 2. The field $\mathbb{Q}(\omega)$ is a Galois extension of $\mathbb{Q}$ with Abelian Galois group by Proposition 7.2. If $H = Gal\,(\mathbb{Q}\omega)/\,\mathbb{Q}(\cos(2\pi/n)\,))$ by the theory of finite Abelian groups there is a chain of subgroups

$$H_0 \subseteq H_1 \subseteq \cdots \subseteq H_r = H$$

With $|H_{i+1} : H_i| = 2$ If $L_i = \mathcal{F}(H_i)$ then $|L_{i+1} : L_i| = 2$, thus $L_i = L_{i+1}(\sqrt{u_i})$ for some u_i. Since $L_i \subseteq \mathbb{Q}\ (\cos(2\pi/n)) \subseteq \mathbb{R}$, each of the $u_i \geq 0$ Since the square root of a constructible number is constructible, we see that everything in $\mathbb{Q}(\cos(2\pi/n)$ is constructible. Thus, $\cos(2\pi/n)$ is constructible, so a regular n - gon is constructible

This theorem shows, for example, that a regular 9 – gon is not constructible and a regular 17 – gon is constructible. An explicit algorithm for constructing a regular 17-gon was given by Gauss in 1801.

If $n = p_1^{m_1} \ldots p_r^{m_r}$ is the prime factorization of n, then $\emptyset(n) = \prod_i p^{m_i - 1}(p_i - 1)$. Therefore $\emptyset(n)$is a power of 2 if and only if $n = 2^s q_1 \ldots q_r$, where $r, s \geq 0$, and the q_i are primes of the form $2^m + 1$. In order to determine which regular n gons are constructible, it then reduces to determining the primes of the form $2^m + 1$

Check your Progress-1

1. Explain The assumptions of constructibility

2. Provide statement of lemma related to **subfield of** $\mathbb{R}$

13.3 SOLVABILITY BY RADICALS

Consider, for example, the polynomialx^4-6x^2 +7. Its roots are $\pm\sqrt{3\pm\sqrt{2}}$ all of which lie in the extension $\mathbb{Q}$ ($\sqrt{2}$, $\sqrt{3\pm\sqrt{2}}$ of $\mathbb{Q}$. Thisextension gives rise to the chain of simple extensions

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

where each successive field is obtained from the previous one by adjoining the root of au element of the previous field. This example motivates the following definitions.

13.3.1 Definition: *A field extension K of F is a radical extension if K = F(a_1 ,...,a_r), such that there are integers n_1 , .. ,n_r, with* $a_1^{n_1}$∈*F and* $a_1^{n_i}$∈ F(a_1 ,...,a_{i-1}) *for all i > 1. If* n_1 = ···· = n_r, = *n, then K is called an n-radical extension of F.*

13.3.2 Definition *If f(x) ∈F [xj, then f is solvable by radicals if there is a radical extension L/ F such that f splits over L.*

If *K* and *F* are as in the first definition, then *K* is an *n* -radical extension of *F* for $n = n_1 \cdots n_r$since a_i^n∈ F(a_1 ,...,a_{i-1}) for each *i*. The definition of radical extension is equivalent to the following statement: *K* is a radicalextension of *F* if there is a chain of fields

$$F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_r = K,$$

where $F_{i+i} = F_i(a_i)$ for some $a_i \in F_{i+i}$ with $a_1^{n_i}$ $F_i$for each *i*. From the definition, it follows easily that if *K/ F* is a radical extension and *L/K* is a radical extension, then *L/F* is a radical extension.

Example : Any 2-Kummer extension of a field *F* of characteristic not 2 is a 2-radical extension of *F* by Theorem 11.4. Also, if *K/F* is a cyclic extension of degree *n* , and if *F* contains a primitive nth root of unity, then *K* is an n-radical extension of *F* .

Example : If $K = \mathbb{Q}(\sqrt[4]{2})$, then *K* is both a 4-radical extension and a 2-radical extension of $\mathbb{Q}$. The second statement is true by considering the Tower

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2})(\sqrt{\sqrt{2}}) = \mathbb{Q}(\sqrt[4]{2}).$$

Example : Let $c \in \mathbb{R}$. By Theorem 15.2, *c* is constructible if and only if there is a tower $\mathbb{Q} = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_r$ such that for each i, $F_{i+1} = F_i(\sqrt{a_i})$ for some $a_i \in F_i$, and $c \in F_r$. Therefore, *c* is constructible if and only if *c* lies in a subfield *K* of $\mathbb{R}$ such that *K* is a 2-radical extension of $\mathbb{Q}$.

The definition of solvability by radicals does not say that the splitting field of *f* over *F* is itself a radical extension. It is possible for *f* to be solvable by radicals but that its splitting field over *F* is not a radical extension. However, if *F* contains "enough" roots of unity, then the splitting field ofa solvable polynomial is a radical extension of *F.* For an example of the first statement, see Example 16.13. The second statement is addressed in Problem 3.

The next lemma is the key technical piece of the proof of the characterization of solvability by radicals.

Notes

13.3.3 : *K be an n-radical extension of F, and let N be the normal closure of K/F. Then N is an n-radical extension of F.*

Proof. Let $K = F(\alpha_1,\ldots,\alpha_r)$ with $\alpha_i^n \in F(\alpha_1,\ldots,\alpha_{i-1})$. We argue by induction on r. If r = 1, then $K = F(\alpha)$ with $\alpha^n = \alpha \in F$. Then $N = F(\beta_1,\ldots,\beta_m)$, where the β_i are the roots of min(F, α). However, this minimal polynomial divides x^n-α, so $\beta_i^n = \alpha$. Thus, N is an n-radical extension of F. Now suppose that r > 1.

Let N_0 be the normal closure of $F(\alpha_1,\ldots,\alpha_{r-1})$ over F. By induction, N_0 is an n-radical extension of F.

Since N_0 is the splitting field over F of $\{\min(F, \alpha_i) : 1 \leq i \leq r - 1\}$, and $N$is the splitting field of all min(F, α_i), we have $N = N_0(\gamma_1,\ldots,\gamma_m)$, where the γ_i are roots of min(F, α_r). Also, $\alpha_r^n = b$ for some $b \in F$, $(\alpha_1,\ldots,\alpha_{r-1}) \subseteq N_0$. By the isomorphism extension theorem, for each i there is a $\sigma_i \in$ Gal(N/F) with $\sigma_i(\alpha_r) = \gamma_1$Therefore, $-\gamma_i^n = \sigma_i(b)$.

However, $N_0$is normal over F, and $b \in No$, so $\sigma_i(b) \in N_0$. Thus, each is an nth power of some element of N_0 , so N is an n-radical extension of N_0. Since No is an n-radical extension of F, we see that N is an n-radical extension of F.

We need some group theory in order to state and prove Galois' theorem on solvability by radicals. The key group theoretic notion is that of solvability of a group.

13.3.4 Definition : A group G is solvable if there is a chain of subgroups

$$\langle e \rangle = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_n = G$$

such that for all i, the subgroup Hi is normal in Hi+1 and the quotient group H_{i+1} / H_i is Abelian.

The following two propositions are the facts that we require about solvability.

13.3.5 Proposition : *Let G be a group and N be a normal subgroup of G. Then G is solvable if and only if N and G/N are solvable.*

13.3.6 Proposition : *If* $n \geq 5$, *then* S_n *is not solvable.*

We now prove Galois' theorem characterizing polynomials that are solvableby radicals.

13.3.7 Theorem (Galois) *Let* char(F) = 0 *and let f (x)* ∈ *F[x]. If K isa splitting field of f over F, then f is solvable by radicals if and only if* Gal(K/F) *is a solvable group.*

Proof. Suppose that *f* is solvable by radicals. Then there is an n-radical extension *M/F* with $K \subseteq M$. Let ω be a primitive nth root of unity in some extension field of *M.* The existence of co follows from the assumption that char (F) = 0. Then $M(\omega)/M$ is an n-radical extension, so $M(\omega)/F$ is an *n*-radical extension. Let *L* be the normal closure of $M(\omega)/F$. By Lemma16.6, *L* is an *n*-radical extension of *F.* Thus, *L* is also an *n* -radical extension of $F(\omega)$. Therefore, there is a sequence of fields

$$F = F_0 \subseteq F_1 = F(\omega) \subseteq F_2 \subseteq \cdots \subseteq F_r = L,$$

where $F_{i+1} = F_i(\alpha_i)$ with $\alpha_i^n \in F_i$. For $i \geq 1$, the extension F_{i+1}/F_i is Galois with a cyclic Galois group, since F_i contains a primitive nth root of unity. Also, F_1/F_0 is an Abelian Galois extension, since F_1 is a cyclotomic extension of *F*. Because char(F) = 0 and *L/F* is normal, *L/F* is Galois. Let *G* = Gal(L/F) and H_i = Gal(L/F_i). We have the chain of subgroups

$$\langle \text{id} \rangle = H_r \subseteq H_{r-1} \subseteq \cdots \subseteq H_0 = G.$$

By the fundamental theorem, $H_{i+1}$is normal in Hi since F_{i+1} is Galois over F_i . Furthermore, H_i/H_{i+1} Gal(F_{i+1}/F_i), so Hi/Hi ±i is an Abelian group. Thus, we see that *G* is solvable, so Gal(K/F) is also solvable, sinceGal(K/F) ≅*G/* Gal(L/K).

For the converse, suppose that Gal(K/F) is a solvable group. We have a Chain

$$\mathrm{Gal}(K/F) = H_0 \supseteq H_1 \supseteq \cdots \supseteq H_r = \langle \mathrm{id} \rangle$$

with H_{i+1} normal in H_i and H_i / H_{i+1} Abelian. Let $K_i = ,F(H_i)$. By the fundamentaltheorem, K_{i+1} is Galois over K_i and $\mathrm{Gal}(K_{i+1}]/K_i) \cong H_i / H_{i+1}$.Let n be the exponent of Gal(K/F), let ω be a primitive nth root of unity,and set $L_i = K_i(w)$. We have the chain of fields

$$F \subseteq L_0 \subseteq L_1 \subseteq \cdots \subseteq L_r$$

with $K \subseteq L_r$. Note that $L_{i+1} = L_i K_{i+1}$. Since K_{i+1} / K_i is Galois, by the theorem of natural irrationalities, L_{i+1} / L_i is Galois and $\mathrm{Gal}(L_{i+1}/L_i)$ is isomorphic to a subgroup of $\mathrm{Ga1}(K_{i+1} / K_i)$. This second group is isomorphic to H_i / H_{i+1}, an Abelian group. Thus, $\mathrm{Gal}(L_{i+1}, /L_i)$ is Abelian, and its exponent divides n. The field L_{i+1} is an n-Kummer extension of L_i, so L_{i+1} is an n -radical extension of L_r. Since Lo $F(\omega)$ is a radical extension, transitivity shows that L_r is a radical extension of F.As $K \subseteq L_r$., the polynomial f is solvable by radicals.

Our definition of radical extension is somewhat lacking for fields of characteristic p, in that Theorem 16.10 is not true in general for prime characteristic. However, by modifying the definition of radical extension in an appropriate way, we can extend this theorem to fields of characteristic p. This is addressed in Problem 2. Also, note that we only needed that char(F)does not divide n in both directions of the proof.

Therefore, the proof above works for fields of characteristic p for adequately large p.

Let k be a field. The general nth degree polynomial over k is the polynomial

$$f(x) = (x - t_1)(x - t_2) \cdots (x - t_n) = x^n - s_1 x^{n-1} + \cdots + (-1)^n s_n \in k(t_1, \ldots, t_n)[x],$$

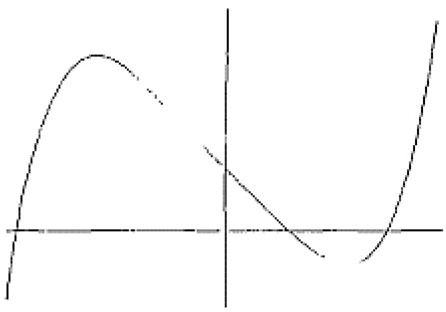
where the s, are the elementary symmetric functions in the t_i . Tf we could find a formula for the roots of f in terms of the coefficients of f, we could use this to find a formula for the roots of an arbitrary nth degree polynomial over k. If $n \leq 4$, we found formulas for the roots of f .For $n \geq$

5, the story is different. The symmetric group S_n is a group of automorphismson $K = k(t_i ,...,t_n)$ and the fixed field is$F = k(s_1,...,s_n)$.

Therefore, Gal(K/F) = S_n . Theorem 13.3.7 shows thatno such formula exists if n ≥ 5.

13.3.8 Corollary : *Let f (x) be the general nth degree polynomial over a fieldof characteristic O. If n ≥5, then f is not solvable by radicals.*

Example 16.12 Let $f(x) = x^5 - 4x + 2 \in \mathbb{Q}[x]$. By graphing techniques of calculus, we see that this polynomial has exactly two nonreal roots, as indicated in the graph below.



Furthermore, *f* is irreducible over $\mathbb{Q}$ by the Eisenstein criterion. Let *K* be the splitting field of *f* over $\mathbb{Q}$. Then $[K: \mathbb{Q}]$ is a multiple of 5, since any root of *f* generates a field of dimension 5 over Q. Let *C;* = Gal(K/$\mathbb{Q}$). We can view $G \subseteq S_5$. There is an element of *G;* of order 5 by Cayley's theorem, since 5 divides |G|. Any element of S_5 of order 5 is a 5-cycle. Also, if σis complex conjugation restricted to *K*, then *a* permutes the two nonreal roots of *f* and fixes the three others, so σ is a transposition. The subgroup of S_5 generated by a transposition and a 5-cycle is all of S_5 so $G = S_5$ is not solvable. Thus, *f* is not solvable by radicals.

Example : Let $f (x) = x^3 - 3x + 1$ E $\mathbb{Q}$ [*x*], and let *K* be the splitting field of *f* over $\mathbb{Q}$. We show that *f* is solvable by radicals but that *K* is nota radical extension of $\mathbb{Q}$. Since *f* has no roots in $\mathbb{Q}$ and deg(f) = 3, the polynomial *f* is irreducible over $\mathbb{Q}$. The discriminant of *f* is $81 = 9^2$, so the Galois group of K/$\mathbb{Q}$ is A_3 and $[K : \mathbb{Q}] = 3$.Therefore, Gal(K/F) is solvable, so *f* is solvable by radicals by Galois' theorem. If *K* is a radical extension of $\mathbb{Q}$, then there is a chain of fields

$$\mathbb{Q} \subseteq F_1 \subseteq \cdots \subseteq F_r = K$$

with $F_i = F_{i-1}(\alpha_i)$ and $\alpha_i^n \in F_{i-}$ for some n. Since $[K : \mathbb{Q}]$ is prime, we see that there is only one proper inclusion in this chain. Thus, $K = \mathbb{Q}(b)$ with $b^n = u \in \mathbb{Q}$ for some n. The minimal polynomial *p(x)* of *b* over $\mathbb{Q}$ splits in *K*, since K/$\mathbb{Q}$ is normal. Let *b′* be another root of *p(x)*. Then $b^n = (b')^n = u$, so b'/b is an *n*th root of unity. Suppose that $\mu = b'/b$ is a primitive mth root of unity, where *m* divides *n*. Then $\mathbb{Q}(\mu) \subseteq K$, so $[\mathbb{Q}(\mu) : = \mathbb{Q}] = \phi(m)$ is either 1 or 3. An easy calculation shows that $\phi(m) \neq 3$for all m. Thus, $[\mathbb{Q}(\mu) : \mathbb{Q}] = 1$, so $\mu, \in \mathbb{Q}$. However, the only roots of unity in $\mathbb{Q}$ are ±1, so $\mu = \pm 1$. Therefore $b' = \pm b$. This proves that *p(x)* has atmost two roots, so $[\mathbb{Q}(b) : \mathbb{Q}] \leq 2 \leq [K : \mathbb{Q}]$, a contradiction to the equality$\mathbb{Q}(b) = K$. Thus, *K* is not a radical extension of $\mathbb{Q}$.

Check your Progress-2

3. Define n-radical extension

____

____

____

4. Define solvable group

____

____

____

13.4 LET US SUM UP

We have discussed the methods in details about Ruler and Compass Constructions. We have also understood solvability by radicals in details with example.

13.5 KEYWORDS

Constructible Number. A **number** which can be represented by a finite **number** of additions, subtractions, multiplications, divisions, and finite square root extractions of integers

Elementary geometry. : the part of Euclidean **geometry** dealing with the simpler properties of straight lines, circles, planes, polyhedrons, the sphere, the cylinder, and the right circular cone

13.6 QUESTIONS FOR REVIEW

1. Use the figures in this section to describe how to construct a+ *b*, *a*— *b*,
   ab, *a/b*, and $\sqrt{a}$, provided that a and *b* are constructible.

2. If sin θ and cos θ are constructible numbers, show that θ is a constructible angle.

3. Let *f (x) E F[x]* be solvable by radicals. If *F* contains a primitive nth root of unity for all n, show that the splitting field of *f* over *F* is a radical extension of *F.* After working through this figure out just which roots of unity *F* needs to have for the argument to work.

13.7 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

13.8 ANSWERS TO CHECK YOUR PROGRESS

1. Provide explanation – 13.2
2. Provide statement– 13.2.1
3. Provide definition –13.3.1
4. Provide proof – 13.3.4

UNIT-14 SOLVING POLYNOMIALS BY RADICALS

STRUCTURE

14.0 OBJECTIVES

Understand the concept of Topological groups

Understand the concept of the krull topology on the Galois group

Enumerate The fundamental theorem of infinite Galois theory

Comprehend Galois groups as inverse limits & Non open subgroups of finite index

14.1 INTRODUCTION

In this chapter, we investigate infinite Galois extensions and prove an analog of the fundamental theorem of Galois theory for infinite extensions. The key idea is to put a topology on the Galois group of an infinite dimensional Galois extension and then use this topology to determine which subgroups of the Galois group arise as Galois groups of intermediate extensions.

14.2 TOPOLOGICAL GROUPS

14.2.1 DEFINITION 7.1 A set G together with a group structure and a topology is a ***topological group*** if the maps

$$(g,h) \mapsto gh: G \times G \to G,$$
$$g \mapsto g^{-1}: G \to G$$

are both continuous.

Let a be an element of a topological group G. Then

$$a_L: G \xrightarrow{g \mapsto ag} G$$

is continuous because it is the composite of

$$G \xrightarrow{g \mapsto (a,g)} G \times G \xrightarrow{(g,h) \mapsto gh} G.$$

In fact, it is a homeomorphism with inverse $(a^{-1})_L$. Similarly a_R:g ↦ga and g ↦g^{-1} are both homeomorphisms. In particular, for any subgroup H of G, the coset aH of H is open or closed if H is open or closed. As the complement of H in G is a union of such cosets, this shows that H is closed if it is open, and it is open if it is closed and of finite index.

Recall that a ***neighbourhood base*** for a point x of a topological space X is a set of neighbourhoods *N* such that every open subset U of X containing x contains an N from *N* .

14.2.2 PROPOSITION :*Let* G *be a topological group, and let N be a neighbourhood base for the identity element* e *of* G. *Then*

(a) *for all* $N_1;N_2 \in \mathcal{N}$*, there exists an* $N' \in N$ *such that* $e \in N' \subset N1 \cap N_2$*;*

(b) *for all* $N \in \mathcal{N}$*, there exists an* $N' \in N$ *such that* $N'N' \subset N$*;*

(c) *for all* $N \in \mathcal{N}$*, there exists an* $N' \in N$ *such that* $N' \subset N^{-1}$*;*

(d) *for all* $N \in \mathcal{N}$ *and all* $g \in G$*, there exists an* $N' \in N$ *such that* $N' \subset gNg^{-1}$;

(e) for all $g \in G$, $\{gN \mid N \in \mathcal{N}\}$ is a neighbourhood base for g.

Conversely, if G is a group and N is a nonempty set of subsets of G satisfying (a, b, c, d), then there is a (unique) topology on G for which (e) holds.

PROOF. If N is a neighbourhood base at e in a topological group G, then (b), (c), and (d) are consequences of the continuity of $(g, h) \mapsto gh$, $g \mapsto g^{-1}$, and $h \mapsto ghg^{-1}$ respectively. Moreover, (a) is a consequence of the definitions and (e) of the fact that gL is a homeomorphism.

Conversely, let $\mathcal{N}$ be a nonempty collection of subsets of a group G satisfying the conditions (a)–(d). Note that (a) implies that e lies in all the N in $\mathcal{N}$. Define U to be the collection of subsets U of G such that, for every $g \in U$, there exists an $N \in \mathcal{N}$ with gN U . Clearly, the empty set and G are in U, and unions of sets in U are in U. Let U_1, $U2 \in U$, and let $g \in U_1 \cap U_2$; by definition there exist $N_1, N_2 \in N$ with gN_1 , $gN_2 \subset U$, on applying (a) we obtain an $N' \in \mathcal{N}$ such that $gN' \subset U_1 \cap U_2$, which shows that $U_1 \cap U_2 \in U$. It follows that the elements of U are the open sets of a topology on G. In fact, one sees easily that it is the unique topology for which (e) holds.

We next use (b) and (d) to show that $(g, g') \mapsto gg'$ is continuous. Note that the sets $g_1N_1 \times g_2N_2$ form a neighbourhood base for (g_1, g_2) in

Notes

$G \times G$. Therefore, given an open U ⊂ G and a pair (g_1 , g_2) such that g_1g_2 2 U , we have to find N_1;N_2 ∈ N such that $g_1N_1g_2N_2$ ⊂ U . As U is open, there exists an N ∈ $\mathcal{N}$ such that g_1g_2N ⊂ U. Apply (b) to obtain an N' such that N' N' ⊂ $\mathcal{N}$; then $g_1g_2N'N' \subset$ U. But $g_1g_2N'N' = g_1(g_2N'\ g_2^{-1})g_2N'$ and it remains to apply (d) to obtain an N_1 ∈ N such that N_1 ⊂ g ∈ $N'\ g_2^{-1}$.

Finally, we use (c) and (d) to show that g ↦g $^{-1}$ is continuous. Given an open U ⊂ G and a g ∈ G such that g $^{-1}$ ∈ U , we have to find an N ∈ $\mathcal{N}$ such that gN ⊂ U^{-1}. By definition, there exists an N ∈ $\mathcal{N}$ such that g $^{-1}$ N ⊂ U. Now N $^{-1}$ g⊂ U^{-1}, and we use (c) to obtain an N' ∈ $\mathcal{N}$ such that N' g ⊂ U^{-1}, and (d) to obtain an $N"$ ∈ $\mathcal{N}$ such that $gN" \subset g(g^{-1}N'g) \subset U^{-1}$

14.2 THE KRULL TOPOLOGY ON THE GALOIS GROUP

Recall that a finite extension Ω of F is Galois over F if it is normal and separable, i.e., if every irreducible polynomial f ∈ F [X] having a root in Ω has deg f distinct roots in Ω. Similarly, we define an algebraic extension Ω of F to be Galois over F if it is normal and separable.

For example, F^{sep} is a Galois extension of F. Clearly, Ω is Galois over F if and only if it is a union of finite Galois extensions.

14.3.1 PROPOSITION: *If* Ω *is Galois over* F *, then it is Galois over every intermediate field* M.

PROOF. Let f (X) be an irreducible polynomial in M [X] having a root a in Ω. The minimum polynomial g(X) of a over F splits into distinct degree-one factors in Ω [X]. As *f* divides g (in M [X]), it also must split into distinct degree-one factors in Ω [X].

14.3.2 PROPOSITION: *Let* Ω *be a Galois extension of* F *and let* E *be a subfield of* Ω *containing* F *. Then every* F *-homomorphism* E → Ω *extends to an* F *-isomorphism* Ω → Ω.

PROOF. The same Zorn's lemma argument shows that every F -homomorphism E → Ω extends to an F -homomorphism α : Ω → Ω. Let a ∈ Ω, and let *f* be its minimum polynomial over F. Then Ω contains exactly deg (f) roots of *f* , and so therefore does α (Ω). Hence a ∈ α (Ω) which shows that α is surjective.

14.3.3 COROLLARY: *Let* Ω ⊃ E ⊃ F *be as in the proposition. If* E *is stable under* Aut(Ω / F) *then* E *is Galois over* F .

PROOF. Let f (X) be an irreducible polynomial in F [X] having a root a in E. Because Ω is Galois over F , f (X)has n = deg (f) distinct roots $a_1,\dots, a_n$ in Ω. There is an F -isomorphism F [a] → F [a_i] ⊂ Ω sending a to a_i (they are both stem fields for *f*), which extends to an F -isomorphism Ω → Ω . As E is stable under Aut(Ω / F), this shows that $a_i \in E$.

Let Ω be a Galois extension of F , and let G = Aut(Ω / F), For any finite subset S of Ω, let

$$G(S) = \{\sigma \in G \mid \sigma s = s \text{ for all } s \in S\}.$$

14.3.4 PROPOSITION: *There is a unique structure of a topological group on* G *for which the sets* G(S) *form an open neighbourhood base of* 1. *For this topology, the sets* G(S) *with* S G-*stable form a neighbourhood base of* 1 *consisting of open normal subgroups.*

PROOF. We show that the collection of sets G.S/ satisfies (a, b, c, d) of (14.2.1). It satisfies (a) because $G(S_1) \cap G(S_2) = G(S_1 \cap S_2)$. It satisfies (b) and (c) because each set G(S) is a group. Let S be a finite subset of Ω. Then F(S) is a finite extension of F , and so there are only finitely many F -homomorphisms F(S) → Ω. Since σS = τS if σ | F(S) = τ | F(S) this shows that $\bar{S} = \bigcup_{\sigma \in G} \sigma S$ is finite. Now $\sigma S = \bar{S}$ for all σ ∈ G, and it follows that G($\bar{S}$) is normal in G. Therefore, σ G($\bar{S}$) σ^{-1} = G($\bar{S}$) = G(S) which proves (d). It also proves the second statement.

The topology on Aut (Ω / F) defined in the proposition is called the ***Krull topology***. We write Gal(Ω / F) for Aut(Ω / F) endowed with the Krull topology, and call it the ***Galois group*** of (Ω / F). The Galois group of F^{sep} over F is called the ***absolute Galois group*** of F. If S is a finite set stable under G, then F(S) is a finite extension of F stable under G, and hence Galois over F (14.3.3). Therefore,

$$\{\mathrm{Gal}(\Omega/E) \mid E \text{ finite and Galois over } F\}$$

is a neighbourhood base of 1 consisting of open normal subgroups.

14.3.5 PROPOSITION 7.7 *Let* Ω *be Galois over* F . *For every intermediate field* E *finite and Galois over* F, *the map*

$$\sigma \mapsto \sigma|E : \mathrm{Gal}(\Omega/F) \to \mathrm{Gal}(E/F)$$

is a continuous surjection (discrete topology on Gal (E/F *).*

PROOF: Let σ ∈ Gal(E / F) and regard it as an F -homomorphism E → Ω''. Then σ extends to an F -isomorphism Ω → Ω (see 14.3.2), which shows that the map is surjective. For every finite set S of generators of E over F , Gal (Ω /E) = G(S), which shows that the inverse image of $1_{\mathrm{Gal}\,(E/F)}$ is open in G. By homogeneity, the same is true for every element of Gal (E/ F).

14.3.6 PROPOSITION: *The Galois group* G *of a Galois extension* Ω/F *is compact and totally disconnected.*

PROOF. We first show that G is Hausdorff. If σ ≠ τ , then σ^{-1}≠ G, and so it moves some element of Ω, i.e., there exists an a ∈ Ω such that σ (a) ≠ τ (a). For any S containing a, σG(S) and G(S) are disjoint because their elements act differently on a. Hence they are disjoint open subsets of G containing σ and τ respectively. We next show that G is compact. As we noted above, if S is a finite set stable under G, then G(S) is a normal subgroup of G, and it has finite index because it is the kernel of

$$G \rightarrow \mathrm{Sym}(S)$$

Since every finite set is contained in a stable finite set, the argument in the last paragraph shows that the map

$$G \rightarrow \prod_{S \text{ finite stable under } G} G/G(S)$$

is injective. When we endow $\prod G/G(S)$ with the product topology, the induced topology on G is that for which the G(S) form an open neighbourhood base of e, i.e., it is the Krull topology.

According to the Tychonoff theorem, $\prod G/G(S)$ is compact, and so it remains to show that G is closed in the product. For each S1 ⊂ S_2, there are two continuous maps $\prod G/G(S) \rightarrow G/G(S_1)$ namely, the projection onto $G/G(S_1)$ and the projection onto $G/G(S_2)$ followed by the quotient map $G/G(S_2) \rightarrow G/G(S_1)$ Let $E(S_1, S_2)$ be the closed subset of $\prod G/G(S)$ on which the two maps agree. Then $\bigcap_{S_1 \subset S_2} E(S_1, S_2)$ is closed, and equals the image of G.

Finally, for each finite set S stable under G, G(S) is a subgroup that is open and hence closed. Since $\bigcap G(S) = \{1_G\}$, this shows that the connected component of G containing 1_G is just $\{1_G\}$. By homogeneity, a similar statement is true for every element of G.

14.3.7 PROPOSITION: For every Galois extension Ω/F , $\Omega^{\mathrm{Gal}(\Omega/F)} =$ F.

Notes

PROOF. Every element of Ω \ F lies in a finite Galois extension of F , and so this follows from the surjectivity in Proposition 14.3.5

Check your Progress-1

1. State the definition of **topological group**

____
____
____

2. Define solvable group

____
____
____

14.4 THE FUNDAMENTAL THEOREM OF INFINITE GALOIS THEORY

14.4.1 PROPOSITION : LetΩ be Galois over F, with Galois group G.
(a) Let M be a subfield of Ωcontaining F. Then Ω is Galois over M, the Galois group Gal(Ω/ M) is closed in G, and Ω Gal(Ω/M) = M.
(b) For every subgroup H of G, Gal (Ω/ Ω^H) is the closure of H.

PROOF. (a) The first assertion was proved in (14.3.1). For each finite subset S⊂M, G(S) isan open subgroup of G, and hence it is closed. But Gal(ΩM) = $\bigcap_{S\subset M}$ G(S), and so italso is closed. The final statement now follows from (14.3.7).

(b) Since Gal(Ω/Ω^H)contains H and is closed, it certainly contains the closure $\bar{H}$ ofH. On the other hand, let σ∈ 2 G\$\bar{H}$; we have to show that σ moves some element of Ω^H.
Because σ is not in the closure of H,

$$\sigma G\,(\Omega/E) \cap H = \emptyset$$

for some finite Galois extension E of F in Ω (because the sets Gal(Ω / E) form a neighbourhoodbase of 1; see above). Let ∅ denote the surjective map Gal(Ω/ F) →Gal(E / F).

Then $\sigma|E \notin \emptyset H$, and so σ moves some element of $E^{\emptyset H} \subseteq \Omega^H$ _ H

14.4.2 THEOREM : Let Ω be Galois over F with Galois group G. The maps

$$H \mapsto \Omega^H, \quad M \mapsto \mathrm{Gal}(\Omega/M)$$

are inverse bijections between the set of closed subgroups of G and the set of intermediatefields between and F :

$$\{closed\ subgroups\ of\ G\} \leftrightarrow \{intermediate\ fields\ F \subset M \subset \Omega\}.$$

Moreover,

(a) the correspondence is inclusion-reversing: $H1 \supset H2 \Leftrightarrow \Omega^{H1} \subset \Omega^{H2}$;

(b) a closed subgroup H of G is open if and only if ΩH has finite degree over F, inwhich case $(G:H) = [\Omega^H : F]$;

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

(d) a closed subgroup H of G is normal if and only if Ω^H is Galois over F , in whichcase $\mathrm{Gal}(\Omega^H/F) \simeq G/H$.

PROOF. For the first statement, we have to show that $H \to \Omega^H$ and $M \to \mathrm{Gal}(\Omega/M)$ are inverse maps. Let H be a closed subgroup of G. Then Ω is Galois over H and $\mathrm{Gal}(\Omega/\Omega^H) = H$ (see 14.4.1).

Let M be an intermediate field. Then $\mathrm{Gal}(\Omega/M)$ is a closed subgroup of G and $\Omega^{\mathrm{Gal}(\Omega/M)} = M$ (see 14.4.1).

(a) We have the obvious implications:

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

But $\mathrm{Gal}(\Omega/\Omega^{Hi}) = Hi$ (see 14.4.1).

(b) As we noted earlier, a closed subgroup of finite index in a topological group is alwaysopen. Because G is compact, conversely an open subgroup of G is always of finite index.

Let H be such a subgroup. The map $\sigma \longleftrightarrow \sigma|\Omega^H$ defines a bijection

$$G/H \to \mathrm{Hom}_F(\Omega^H, \Omega)$$

(apply 14.2.2) from which the statement follows.

(c) For $\tau \in G$ and $\alpha \in \Omega$, $\tau\alpha = \alpha \Leftrightarrow \sigma\tau\sigma^{-1}(\sigma\alpha) = \sigma\alpha$. Therefore, $\mathrm{Gal}(\Omega/\sigma M) = \sigma \mathrm{Gal}(\Omega/M)\sigma^{-1}$, and so σ $\mathrm{Gal}(\Omega/M)\sigma^{-1}\sigma M$.

(d) Let $H \leftrightarrow M$. It follows from (c) that H is normal if and only if M is stable underthe action of G. But M is stable under the action of G if and only it is a union of finiteextensions of F stable under G, i.e., of finite Galois extensions of G. We have alreadyobserved that an extension is Galois if and only if it is a union of finite Galois extensions.

14.4.3 REMARK : As in the finite case (3.17), we can deduce the following statements.

(a) Let $(M_i)_{i\in I}$ be a (possibly infinite) family of intermediate fields, and let $H_i \leftrightarrow M_i$.

Let $\prod Mi$ be the smallest field containing all the M_i ; then because $\bigcap_{i\in I} H_i$ is the largest(closed) subgroup contained in all the H_i,

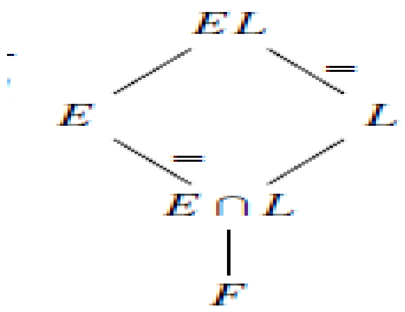
$$\mathrm{Gal}(\Omega/\prod M_i) = \bigcap_{i\in I} H_i.$$

(b) Let $M \leftrightarrow H$. The largest (closed) normal subgroup contained in H is $N = \bigcap_\sigma \sigma H \sigma^{-1}$(cf. GT 4.10), and so Ω^N, which is the composite of the fields σM, is thesmallest normal extension of F containing M.

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

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

is an isomorphism of topological groups.



PROOF. We first prove that the map is continuous. Let G_1= Gal(EL/L) and let G2 = Gal(E/E⋂ L/. For any finite set S of elements of E, the inverse image of $G_2(S)$ in $G_1$is $G_1(S)$.

We next show that the map is an isomorphism of groups (neglecting the topology). As in the finite case, it is an injective homomorphism (3.18). Let H be the image of the map.

Then the fixed field of H is E⋂L, which implies that H is dense in Gal(E/E⋂ L). But His closed because it is the continuous image of a compact space in a Hausdorff space, and so
H /   Gal(E/E ⋂ L)

Finally, we prove that it is open. An open subgroup of Gal(EL/L) is closed (hencecompact) of finite index; therefore its image in Gal(E/E ⋂ L) is compact (hence closed) offinite index, and hence open.

14.4.5 COROLLARY 7.15 Let Ω be an algebraically closed field containing F, and let E and Lbe as in the proposition. If ρ: E → *Ω and* σ : L → *Ω are F* -homomorphisms such thatρ|E ⋂ L= σ|E ⋂ L, then there exists an F -homomorphism τ:EL →*Ω*such that τ| E = ρand τ|L = σ.

PROOF. According to (14.2.2), σ extends to an F -homomorphism s:EL→Ω As s| E ⋂ L = ρ| E ⋂ L, we can write s|E = ρo*ε* for some *ε* ∈ Gal (E/E ⋂ L). According to the proposition,there exists a unique e ∈ Gal(EL/L) such that e|E = *ε*. Define τ = soe^{-1}

EXAMPLE : Let *Ω* be an algebraic closure of the finite field 𝔽ρ. Then G D Gal.=Ω/𝔽ρ) contains a canonical Frobenius element, σ = (*a*→*a*ρ), and it is generated by it as a topological group, i.e., G is the closure of ⟨σ⟩. We now determine the structure of G.

Endow $\mathbb{Z}$ with the topology for which the groups $n\mathbb{Z}$, $n \geq 1$, form a fundamental system of neighbourhoods of 0. Thus two integers are close if their difference is divisible by a large integer.

As for any topological group, we can complete $\mathbb{Z}$ for this topology. A Cauchy sequence in $\mathbb{Z}$ is a sequence $(a_i)_{i\geq 1}$, $a_i \in \mathbb{Z}$, satisfying the following condition: for all $n \geq 1$, there xists an N such that $a_i \equiv a_j \bmod n$ for $i,j > N$. Call a Cauchy sequence in $\mathbb{Z}$ trivial if$a_i \rightarrow 0$ as $i \rightarrow \infty$, i.e., if for all $n \geq 1$, there exists an N such that $a_i \equiv 0 \bmod n$ for all i > N. The Cauchy sequences form a commutative group, and the trivial Cauchy sequences form a subgroup. We define $\hat{\mathbb{Z}}$ to be the quotient of the first group by the second. It has aring structure, and the map sending $m \in \mathbb{Z}$ to the constant sequence $m,m,m,\ldots$ identifies $\mathbb{Z}$with a subgroup of $\hat{\mathbb{Z}}$.

Let $\alpha \in \hat{\mathbb{Z}}$be represented by the Cauchy sequence (a_i). The restriction of the Frobenius element σ to $\mathbb{F}_{\rho}{}^{n}$ has order n. Therefore $(\sigma|\mathbb{F}_{p}{}^{n})^{ai}$ is independent of i provided it is sufficiently large, and we can define $\sigma^{\alpha} \in \mathrm{Gal}(\Omega/\mathbb{F}_p)$ to be such that, for each n,$\sigma^{\alpha}|\mathbb{F}_{p^n} = (\sigma|\mathbb{F}_{p}{}^{n})^{ai}$ for all i sufficiently large (depending on n). The map $\alpha \rightarrow \sigma^{\alpha}$: $\hat{\mathbb{Z}}\mathrm{Gal}(\Omega/\mathbb{F}_p)$
is an isomorphism.
The group $\hat{\mathbb{Z}}$ is uncountable. To most analysts, it is a little weird—its connectedcomponents are one-point sets. To number theorists it will seem quite natural — theChinese remainder theorem implies that it is isomorphic to $\prod_{p\ prime} \mathbb{Z}_p$where $\mathbb{Z}_p$ is the ringof p-adic integers.

EXAMPLE : Let $\mathbb{Q}^{al}$ be the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$. Then $\mathrm{Gal}(\mathbb{Q}^{al}/\mathbb{Q})$ is one of themost basic, and intractable, objects in mathematics. It is expected that every finite groupoccurs as a quotient of it. This is known, for example, for Sn and for every sporadic simple group except possibly M_{23}. See (5.41) and mo80359.

On the other hand, we do understand Gal(F^{ab}/F) where F $\subset \mathbb{Q}^{al}$ is a finite extensionof $\mathbb{Q}$ and F ab is the union of all finite abelian extensions of F contained in $\mathbb{Q}^{al}$. For example, Gal$\mathbb{Q}^{ab}/\mathbb{Q}/ \simeq \widehat{\mathbb{Z}}^{\times}$This is abelian class field theory—see my notes Class Field Theory.

14.4.6 ASIDE : A ***simple Galois correspondence*** is a system consisting of two partially ordered sets P and Q and order reversing maps f :P → Q and g: Q → P such that gf (p) ≥ p for all p∈ P and f g(q) ≥ q for all q ∈ Q. Then *f g f* = *f*, because *fg* (*f p*) ≥ fp and gf (p) ≥ p implies f (*g f p*) ≤ *f* (p) for all p ∈ P . Similarly, *g f g* = g, and it follows that f and g define a one-to-one correspondence between the sets g(Q) and f (P).

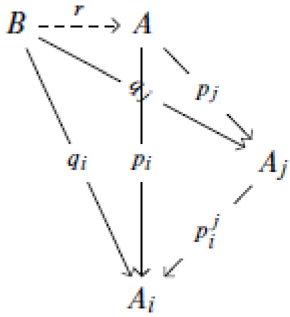
14.5 GALOIS GROUPS AS INVERSE LIMITS

14.5.1 DEFINITION: A partial ordering ≤ on a set I is directed, and the pair (I, ≤) is adirected set, if for all $i,j\in$ I there exists a k ∈ I such that i, $j\leq$ k.

14.5.2 DEFINITION : Let (I, ≤) be a directed set, and let C be a category (for example, the category of groups and homomorphisms, or the category of topological groups and continuous homomorphisms).

(a) An inverse system in C indexed by (I, ≤) is a family $(A_i)_{i\in I}$ of objects of C together with a family (p_i^jo : $A_j \to A_i)_{i\leq j}$ of morphisms such that p_i^jo $p_j^k = p_i^k$all $i\leq j\leq$ k.

(b) An object A of C together with a family (pj : A → $A_j)_{i\in I}$ of morphisms satisfyingp_i^jo p_j=p_i all $i\leq j$ is an inverse limit of the system in (a) if it has the following universal property: for any other object B and family q_j: (B →A_j) of morphisms such p_i^jo q_j=q_i all $i\leq j$, there exists a unique morphism r : B → A such that p_jo r =q_j for j,



Clearly, the inverse limit (if it exists), is uniquely determined by this condition up to a unique isomorphism. We denote it by $\overset{lim}{\longleftarrow}(A_i, p_i^j)$,or just $\overset{lim}{\longleftarrow}A_{i.}$

Example : Let (G_i , p_i^j: $G_j \to G_i$) be an inverse system of groups. Let

$$G = \{(g_i) \in \prod G_i \mid p_i^j(g_j) = g_i \text{ all } i \leq j\},$$

and let p_i:$G \to G_i$ be the projection map. Thenp_i^j o q_j=q_i is just the equation p_i^j(g_i) = g_i. Let (H,q_i) be a second family such that p_i^j o q_j=q_i . The image of the homomorphism

$$h \mapsto (q_i(h)): H \to \prod G_i$$

is contained in G, and this is the unique homomorphism H →G carrying *qi to pi . Hence (G,pi)* $=\overset{lim}{\longleftarrow}$*(Gi,*$p_i^j$*).*

EXAMPLE : Let (G_i,p_i^j: $G_j \to G_i$ be an inverse system of topological groups and continuous homomorphisms. When endowed with the product topology, $\prod G_i$ becomes at opological group

$$G = \{(g_i) \in \prod G_i \mid p_i^j(g_j) = g_i \text{ all } i \leq j\},$$

and G becomes a topological subgroup with the subspace topology. The projection mapsp_i are continuous. Let H be (H,q_i) be a second family such that p_i^j o q_j=q_i. Thehomomorphism

$$h \mapsto (q_i(h)): H \to \prod G_i$$

EXAMPLE : Let. (G_i, p_i^j:Gj→Gi) be an inverse system of finite groups, and regard it as an inverse system of topological groups by giving each Gi the discrete topology. A topological group G arising as an inverse limit of such a system is said to be profinite

If $(x_i) \notin G$, say $p_{i_0}^{j_0}(x_{j_0}) \neq x_{i_0}$, then

$$G \cap \{(g_j) \mid g_{j_0} = x_{j_0}, \quad g_{i_0} = x_{i_0}\} = \emptyset.$$

As the second set is an open neighborhood of (xi), this shows that G is closed in∏Gi. By Tychonoff's theorem, ∏Gi is compact, and so G is also compact. The map p_i:G →Gi is continuous, and its kernel Ui is an open subgroup of finite index in G (hence also closed). As⋂Ui={e}, the connected component of G containing e is just {e}. By homogeneity, the same is true for every point of G: the connected components of G are the one-point sets — G is totally disconnected.

We have shown that a profinite group is compact and totally disconnected, and it is an exercise to prove the converse

EXAMPLE : Let Ω be a Galois extension of 𝔽. The composite of two finite Galois extensions of in Ω is again a finite Galois extension, and so the finite Galois sub extensions of Ω form a directed set *I*. For each *E* in *I* we have a finite group Gal(*E*/ 𝔽), and for each *E*⊂*E′* we have a restriction homomorphism

$p_E^{E'}$:Gal$(E'/F) \to$ Gal(E/F).

In this way, we get an inverse system of finite groups

(Gal(E/F), $p_E^{E'}$) indexed by I.

For each E, there is a restriction homomorphism

p_E:Gal$(\Omega/F) \to$ Gal(E/F)

and, because of the universal property of inverse limits, these maps define a homomorphism

$$\mathrm{Gal}(\Omega/F) \to \varprojlim \mathrm{Gal}(E/F).$$

This map is an isomorphism of topological groups. This is a restatement of what we showed in the proof of (14.2.6).

14.6 NON-OPEN SUB-GROUPS OF FINITE INDEX

Non-open sub-groups of finite index We apply Zorn's lemma10 to construct a non-open subgroup of finite index in Gal.($\mathbb{Q}^{al}/\mathbb{Q}$).

14.6.1 LEMMA: Let V be an infinite-dimensional vector space. For all n ≥1, there exists a subspace Vn of V such that V/V_n has dimension n.

PROOF. Zorn's lemma shows that V contains maximal linearly independent subsets, and then the usual argument shows that such a subset spans V, i.e., is a basis. Choose a basis, and take Vn to be the subspace spanned by the set obtained by omitting n element from the basis.

14.6.2 PROPOSITION: The group Gal.($\mathbb{Q}^{al}/\mathbb{Q}$). has non-open normal subgroups of index 2n for all n> 1.

PROOF.

Let E be the subfield$\mathbb{Q}$ [$\sqrt{-1}$;$\sqrt{-2}$;……$\sqrt{-p}$;….]p prime, of$\mathbb{C}$

For each p, Gal($\mathbb{Q}$ [$\sqrt{-1}$;$\sqrt{-2}$;……$\sqrt{-p}$] /$\mathbb{Q}$) is a product of copies of$\mathbb{Z}$ =2$\mathbb{Z}$indexed by the set {primes≤p}∪{∞}. As

$$\mathrm{Gal}(E/\mathbb{Q}) = \varprojlim \mathrm{Gal}(\mathbb{Q}[\sqrt{-1}, \sqrt{2}, \ldots, \sqrt{p}]/\mathbb{Q}),$$

it is a direct product of copies of$\mathbb{Z}/2\mathbb{Z}$indexed by the primesl of $\mathbb{Q}$ (including l=∞) endowed with the product topology. Let G = Gal.E/$\mathbb{Q}$ and let

$H = \{(a_l) \in G \mid a_l = 0 \text{ for all but finitely many } l\}.$

This is a subgroup of G (in fact, it is a direct sum of copies of$\mathbb{Z}=2\mathbb{Z}$indexed by the primes of $\mathbb{Q}$), and it is dense in G because clearly every open subset of G contains an element of H. We can regard G/H as vector space over $\mathbb{F}_2$ and apply the lemma to obtain subgroups Gn of index 2^n in G containing H. If Gn is open in G, then it is closed, which contradicts the fact that H is dense. Therefore, Gn is not open, and its inverse image in Gal.($\mathbb{Q}^{al}/\mathbb{Q}$)is the desired subgroup1

14.6.3 ASIDE: Let G = Gal.($\mathbb{Q}^{al}/\mathbb{Q}$)We showed in the above proof that there is a closed normal sub-group N = Gal. ($\mathbb{Q}^{al}/E$)ofG suchthatG/N is an uncountable vector space over $\mathbb{F}_2$. Let (G/N) be the dual of this vector space (also uncountable). Every nonzero $f \in$(G/N) defines a surjective map G→ $\mathbb{F}_2$ whose kernel is a subgroup of index 2 in G. These subgroups are distinct, and so G has uncountably many subgroups of index 2. Only countably many of them are open because $\mathbb{Q}$ has only countably many quadratic extensions in a fixed algebraic closure.

14.6.4 ASIDE: Let G be a profinite group that is finitely generated as a topological group. It is a difficult theorem, only recently proved, that every subgroup of finite index in G is open.

Check your Progress-2

3. Define **Simple Galois correspondence**

____

____

____

4. State Directed Set and Inverse system

____

____

____

14.7 LET US SUM UP

Notes

We have discussed infinite Galois extensions and prove an analog of the fundamental theorem of Galois theory for infinite extensions.

14.8 KEYWORDS

Homomorphism is a structure-preserving map between two algebraic structures of the same type (such as two groups, two rings, or two vector spaces).

Restriction - In **mathematics**, the **restriction** of a function is a new function, denoted or , obtained by choosing a smaller domain A for the original function .

14.9 QUESTIONS FOR REVIEW

1. Let p be a prime number, and let Ω be the subfield of ℂ generated over ℚ by all p^mth
   roots of 1 for m ∈ N. Show that Ω is Galois over Q with Galois group

   $$\mathbb{Z}_p \stackrel{\text{def}}{=} \varprojlim \mathbb{Z}/p^m\mathbb{Z}.$$

   (Hint: Use that Ω is the union of a tower of subfields

   $$\mathbb{Q} \subset \mathbb{Q}[\zeta_p] \subset \cdots \subset \mathbb{Q}[\zeta_{p^m}] \subset \mathbb{Q}[\zeta_{p^{m+1}}] \subset \cdots .)$$

2. Let F be an algebraic closure of $\mathbb{F}_p$, and let $\mathbb{F}_{p^m}$ be the subfield of F with p^m elements.
   Show that

   $$\varprojlim_{m \geq 1} \mathrm{Gal}(\mathbb{F}_{p^m}/\mathbb{F}_p) \simeq \varprojlim_{m \geq 1} \mathbb{Z}/m\mathbb{Z}$$

14.10 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.

14.11 ANSWERS TO CHECK YOUR PROGRESS

1. Provide definition – 14.2.1

2. Provide statement– 13.2.1

3. Provide definition –Refer ASIDE 14.4.6

4. Provide definition – 14.5.1 & 14.5.2