Transcendental Extenstions and Lüroth's theorem

Devesh Rajpal

May 15, 2020

Introduction

In this presentation I will discuss field extensions which are not algerbaic. Such extensions are called transcendental extensions. We will define a number associated to a transcendental extension called transcendental degree. I will also present Lüroth's theorem which states that sublfields of rational functions in one variable are simple.

Definition

Let Ω/F be a field extension. A set of elements $\{\alpha_1, ..., \alpha_n\} \in \Omega$ is algebraically independent over F if the map

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

is injective or equivalently

$$a_{i_1,...,i_n} \in F, \quad \sum a_{i_1,...,i_n} \alpha_1^{i_1}, ..., \alpha_n^{i_n} = 0 \Rightarrow a_{i_1,...,i_n} = 0 \text{ for all } a_{i_1,...,i_n}$$

Otherwise the set is called algebraically dependent over F.
Note : An infinite set A is algebraically independent over F if every finite subset of A is algebraically independent.

Definition

Definition : Let A be a subset of Ω. An element $\gamma \in \Omega$ is said to be algebraically dependent on $F(A)$ if it is algebraic over $F(A)$.
A set B is algebraically dependent on $F(A)$ if each element of B is algebraically dependent on A.
Definition : A transcendence basis for Ω over F is an algebraically independent set A such that Ω is algebraic over $F(A)$.

Transcendence basis

Lemma : Let $A = \{\alpha_1, ..., \alpha_n\}$ and $B = \{\beta_1, ..., \beta_m\}$ be two subsets of Ω where Ω is an extension of F. Assume

(a) A is algebraically independent over F.

(b) A is algebraically dependent over $F(B)$.

Then $m \leq n$.

Proof : Use exchange lemma and transitivity of algebraic independence.

Transcendence basis

- Let $P_1 = \{C : \Omega \text{ is algebraic over } F(C)\}$ and $P_2 = \{C : C \text{ is algebraicailly independent over } F\}$.
  Then any minimal element of P_1 is a maximal element of P_2 and vice versa. Any subset satisfying that property is a transcendental basis of Ω over F.
- If there exists a finite transcendence basis of Ω/F then using previous lemma any other transcendence basis is also finite of same cardinality.

Existence

Theorem : Every algebraically independent subset of Ω is contained in a transcendence basis for Ω over F; in particular transcendence basis exists.
Proof : Let S be an algebraically independent set. We consider the subset of P_2 containing elements of which S is a subset and ordering it by inclusion. Let T be a chain in it and let $Z = \bigcup\{A : A \in T\}$.
We claim that Z is upper bound of T. Assume not, then Z is not algebraically independent, so there exists a finite subset Z' of Z which is algebraically dependent. But such a subset will be contained in one of the sets in T, which is a contradiction. Now Zorn's lemma implies there exists a maximal algebraically independent subset which contains S which is also a transcendence basis.

Analogy between Linear Algebra and Transcendental Extensions

linearly independent	algebraically independent
$A \subset \text{span} B$	A is algebraically dependent on B
basis	transcendence basis
dimension	transcendence degree

Lüroth's Theorem

Theorem : Let $L = F(X)$ with X transcendental over F. Every subfield E of L is of the form $E = F(u)$ for some u transcendental over F.

Degree of a fraction

Definition : Let $u \in F(X) \setminus F$. Suppose $u = \frac{a(X)}{b(X)}$ where $a(X), b(X) \in F[X]$ and $\gcd(a(X), b(X)) = 1$. Define

$$\deg(u) = \max\{\deg(a), \deg(b)\}$$

Lemma on degree

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 $u = \frac{a(X)}{b(X)}$ with $\gcd(a(X), b(X)) = 1$. Now $a(T) - b(T)u$ is a polynomial in $F(u)[T]$ with X as a root. So $F(X)$ is algebraic over $F(u)$ and u is transcendental over F (otherwise X will be algebraic over F).

The polynomial $a(T) - b(T)Y \in F[T, Y]$ is irreducible because $a(T)$ and $b(T)$ are relatively prime. As u is transcendental over F, we have isomorphisms

$$F[T, Y] \simeq F[T, u], \quad T \leftrightarrow T, \quad Y \leftrightarrow u$$

so $a(T) - b(T)u$ is irreducible in $F[u, T]$, and hence is irreducible in $F(u)[T]$ by Gauss's lemma. It follows that

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

Proof of Lüroth's Theorem

Proof : Let $u \in F(X) \setminus F$. From the lemma

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

Let $[F(X) : E] = n$ and

$$f(T) = T^n + a_1 T^{n-1} + ... + a_n, \quad a_i \in E$$

be the minimal polynomial of X over E. Since X is transcendental over E, there exists i such that $a_i \notin F$.

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

$$f_1(X, T) = df(T) = dT^n + da_1 T^{n-1} + ... + da_n \in F[X, T]$$

Then f_1 is primitive as a polynomial in T.

Proof of Lüroth's Theorem

Let $\deg(f_1) = \deg(da_i) = m$ in X. Suppose $a_i = \frac{b}{c}$ with b,c relatively prime polynomials in $F[X]$. Now X is a root of $b(T) - c(T)a_i(X) \in E[T]$, so it is a factor of f, say

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

Multiplying the equation by $c(X)$, we get

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

As f_1 is the primitive part of f, it divides $c(X)b(T) - c(T)b(X)$ in $F[X, T]$, so there exists a polynomial $h(X, T) \in F[X, T]$ such that

$$f_1(X, T)h(X, T) = c(X)b(T) - c(T)b(X) \qquad -(*)$$

In the above equation, 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.

Proof of Lüroth's Theorem

Therefore $c(X)b(T) - c(T)b(X)$ has degree exactly m in X and because it is symmetric in X and Y it has degree m in T also. It follows that $h(X, T)$ has degree 0 in X, so $h \in F[T]$. We claim that h is non-zero constant. Assume not, divide $h(T)$ from $b(T)$ and $c(T)$ to obtain

$$b(T) = \lambda_1(T)h(T) + r_1(T)$$

and

$$c(T) = \lambda_2(T)h(T) + r_2(T)$$

substituting this in $(*)$ we obtain

$$f_1(X, T)h(T) = h(T)[c(X)\lambda_1(T) - b(X)\lambda_2(T)] + [c(X)r_1(T) - b(X)r_2(T)]$$

where $h(T)$ divides $[c(X)r_1(T) - b(X)r_2(T)]$ which has less degree in T than $h(T)$ so $[c(X)r_1(T) - b(X)r_2(T)] = 0$ but $\gcd(b(X), c(X)) = 1$ so we get a contradiction. (Notice r_1, r_2 cannot be simultaneously 0 as b and c are coprime.)

So equation $(*)$ becomes

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

so

$$\begin{aligned}[F(X):E] = n = \deg_T(f_1) &= \deg_T(c(X)b(T) - c(T)b(X)) \\ &= m = \deg(a_i) = [F(X):F(a_i)]\end{aligned}$$

Hence $E = F(a_i)$.

An Application

- Luroth's theorem states that subfields of $F(X)$ have transcendence degree equal to 1 so given any two rational functions $u, v \in F(X)$ one is algebraic over the other.

References

1. James Milne, Fields and Galois Theory