5. Transcendental field extensions

Throughout, K is an extension field of F.

<u>Def</u>: A set $S \subseteq K$ is <u>algebraically dependent</u> over F if there are distinct elements $a_1, \dots, a_k \in S$ and a nonzero polynomial $f(X_1, \dots, X_k) \in F[X_1, \dots, X_k]$ with $f(a_1, \dots, a_k) = 0$. Otherwise, S is <u>algebraically independent</u>.

<u>Remark</u>: This is a "generalization" of the notion of linear dependence; replace "nonzero polynomial" with "nonzero linear polynomial" to get the definition of linear dependence.

A lot of the ideas & results from linear algebra have similar versions in this setting.

<u>Example 1</u>: If $S = \{a\}$, then S is algebraically dependent over F iff a is algebraic over F.

<u>Example 2</u>: The set $\{\pi, \pi^2 - 3\pi + 5\}$ is algebraically dependent over $\mathbb{Q}$; consider the polynomial $f(x,y) = x^2 - y + 3x + 5$.

An algebraically independent set $S \subseteq K$ is called a <u>transcendence set</u> over F.

<u>Exercise</u>: Show that $S \subseteq K$ is algebraically dependent over F iff there is some $a \in S$ that is algebraic over $F(S \setminus \{a\})$.

<u>Think</u>: Formulate an analogous statement for linear dependent sets over V.

<u>Def</u>: If K/F is not algebraic, then K is a <u>transcendental extension</u>. If $K = F(S)$ for some transcendence set S over K, then K is a <u>purely transcendental extension</u>.

<u>Example 3</u>: $K = F(x)$ is purely transcendental

<u>Example 4</u>: $\mathbb{R}/\mathbb{Q}$ is transcendental, but not purely transcendental.

<u>Def</u>: A transcendence set $B \subseteq K$ over F is called a <u>transcendence basis</u> if it is maximal w.r.t. set inclusion.

<u>Compare</u>: Vector space basis = "maximal linearly independent set"

Transcendence basis = "maximal algebraically independent set."

By Zorn's lemma, every transcendence set $S \subseteq K$ is contained in a transcendence basis B.

In particular, K has a transcendence basis over F.

<u>Remark</u>: K/F is algebraic iff $B = \emptyset$.

<u>Prop 5.1</u>: Suppose $S \subseteq K$ is a transcendence set and $a \in K \setminus S$. Then $S \cup \{a\}$ is algebraically dependent over F iff a is algebraic over $F(S)$.

<u>Remark</u>: Compare again to linear algebra: If $S \subseteq V$ is a linear independent set and $a \in K \setminus S$, then $S \cup \{a\}$ is linearly dependent iff a is in the span of S.

Pf: ($\Rightarrow$) Let $S = \{b_1, \dots, b_k\}$ (possibly empty), and let

$f(x_0, x_1, \dots, x_k) \in F[x_0, x_1, \dots, x_k]$ be a nonzero polynomial with $f(a, b_1, \dots, b_k) = 0$.

Note that x_0 occurs in $f(X)$, since S is a transcendental set.

Define $g(x_0) = f(x_0, b_1, \dots, b_k) \in F(S)[x_0]$.

Then $g(x_0) \neq 0$ but $g(a) = 0 \Rightarrow a$ is algebraic over $F(S)$. ✓

($\Leftarrow$) Suppose $g(a) = 0$ for some $0 \neq g(x) \in F(S)$.

We may assume WLOG that $g(x) \in F[b_1, \dots, b_k][x]$ for some $\{b_1, \dots, b_k\} \subseteq S$.

Then $g(a) = 0$ is a nontrivial algebraic dependence relation over F for $\{a, b_1, \dots, b_k\}$, and hence for $S \cup \{a\}$. ✓ $\square$

Cor: If S is a transcendence set for K/F, then S is a transcendence basis iff $K/F(S)$ is algebraic.

Def: If $S \subseteq K$, then the set

$$\sigma(S) = \sigma_{K,F}(S) = \{a \in K : a \text{ is algebraic over } F(S)\}$$

is the <u>algebraic closure</u> of $F(S)$ in K.

* This is the analog of the span of a set of vectors $S \subseteq V$.

<u>Easily verifiable facts</u>:

(i) $S \subseteq \sigma(S)$;

(ii) If $S \subseteq T \subseteq K$, then $\sigma(S) \subseteq \sigma(T)$;

(iii) If $a \in \mathcal{R}(S)$, then $a \in \mathcal{R}(S')$ for some finite set $S' \subseteq S$;

(iv) $\mathcal{R}(\mathcal{R}(S)) = \mathcal{R}(S)$.

<u>Prop 5.2</u>: Suppose $S \subseteq K$, $a, b \in K$, and $b \in \mathcal{R}(S \cup \{a\})$.

Then $a \in \mathcal{R}(S \cup \{b\})$.

<u>Pf</u>: Set $L = F(S)$, so b is transcendental over L but algebraic over $L(a)$.

By Prop 5.1, $\{a, b\}$ is algebraically dependent over L.

Choose $f(X_1, X_2) \neq 0$ in $L[X_1, X_2]$ with $f(a, b) = 0$.

<u>Note</u>: X_1 must occur in $f(X_1, X_2)$, since b is transcendental over L.

Thus, $0 \neq g(X_1) = f(X_1, g) \in L(b)[X_1] = F(S \cup \{b\})[X_1]$,

and $g(a) = 0$. Therefore, $a \in \mathcal{R}(S \cup \{b\})$. $\square$

<u>Thm 5.3</u>: If A & B are transcendence bases for K/F, then $|A| = |B|$.

<u>Pf</u>: WLOG, assume $0 < |A| \leq |B|$.

<u>Case 1</u>: $|A| < \infty$. Say $A = \{a_1, \ldots, a_n\}$.

<u>Note</u>: $B \nsubseteq \mathcal{R}(A \setminus \{a_1\})$; in particular, $a_1 \in \mathcal{R}(B)$ but $a_1 \notin \mathcal{R}(A \setminus \{a_1\})$.

Choose $b_1 \in B \setminus \mathcal{R}(A \setminus \{a_1\})$.

Prop 5.1 $\Rightarrow A_1 = \{b_1, a_2, \ldots, a_n\}$ is a transcendence set.

Prop 5.2 $\Rightarrow a_1 \in \mathcal{R}(A_1)$.

Therefore, A_1 is a transcendence basis.

Inductively, define $A_k = \{b_1, \dots, b_k, a_{k+1}, \dots, a_n\}$, which is also a transcendence basis.

Consider $k = n$: $A_n = \{b_1, \dots, b_n\} \subseteq B$, and A_n and B are transcendence basis (maximal algebraically independent set), then $A_n = B$. Since $|A_n| = |A|$, $|A| = |B|$. ✓

Case 2: $|A| = \infty$.

For each $a \in A$, $\exists$ finite set $B_a \subseteq B$ with $a \in \mathcal{R}(B_a)$.

Claim: $B = \bigcup_{a \in A} B_a$.

If this set was $C \subsetneq B$, then $B \subseteq K \subseteq \mathcal{R}(A) \subseteq \mathcal{R}(C)$, contradicting algebraic independence of B.

Thus, $|B| = \left|\bigcup_{a \in A} B_a\right| \leq \sum_{a \in A} |B_a| \leq \aleph_0 |A| = |A|$. ✓ $\square$

Def: The cardinality of a transcendence basis for K/F is called the transcendence degree of K/F, denoted $\operatorname{trdeg}(K/F)$.

Prop 5.4: If $F \subseteq L \subseteq K$, then $\operatorname{trdeg}(K/F) = \operatorname{trdeg}(K/L) + \operatorname{trdeg}(L/F)$.

Remark: This is different than for vector spaces: $[K:F] = [K:L][L:F]$.

Motivating example: Over $\mathbb{Q}$, $\{\sqrt{3}, \sqrt[3]{2}, \sqrt{3}\sqrt[3]{2}\}$ are linearly independent, but $\{\pi, e, \pi e\}$ are algebraically dependent.

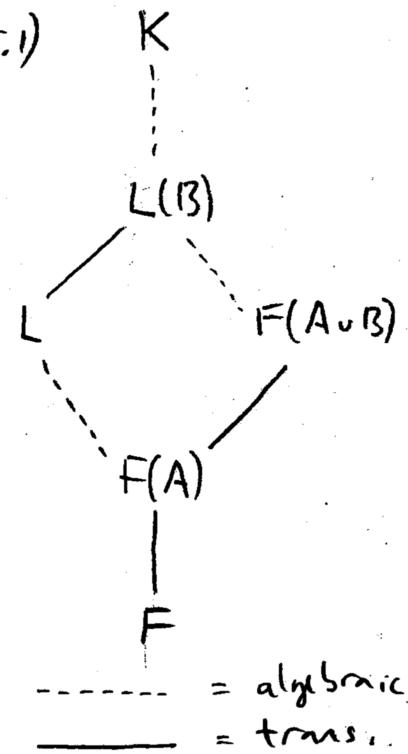
6

$F(A \cup B) \subseteq L(B) \subseteq K$
$|$
$F(A) \subseteq L$
$|$
F

Pf: Let A be a transcendence basis for L/F, and let B be a transcendence basis for K/L.

Clearly, $A \cap B = \phi$, so $L/F(A)$ is algebraic, thus $L(B)/F(A)(B)$ is algebraic (note: $F(A)(B) = F(A \cup B)$)

We also have $K/L(B)$ algebraic (Cor. to Prop 5.1) and $L(B)/F(A \cup B)$ algebraic (similar), so by Prop 1.5, $K/F(A \cup B)$ is algebraic.



Thus, $\operatorname{trdeg}(K/F) \leq |A \cup B|$.

* We need to show equality, i.e, verify that $A \cup B$ is algebraically independent over F.

Suppose that $0 \neq f(X, Y) \in F[X, Y]$ and $f(a_1, \dots, a_m, b_1, \dots, b_n) = 0$ with $a_i \in A$, $b_j \in B$.

Consider $f(a_1, \dots, a_m, Y) \in F[a_1, \dots, a_m][Y]$; the coefficients are "polynomials" $g_i(a_1, \dots, a_m) \in F[a_1, \dots, a_m]$.

Since B is a transcendence set over $L \supseteq F(A)$, all the coefficients $g_i(a_1, \dots, a_m) = 0$.

But then $g_i(x_1, \dots, x_m) = 0 \in F[X]$, since A is a transcendence set over $F \Rightarrow f(X, Y) = 0$ in $F[X, Y]$.

Thus, $A \cup B$ is a transcendence basis for K/F, and so

$$\operatorname{trdeg}(K/F) = |A \cup B| = |A| + |B| = \operatorname{trdeg}(L/F) + \operatorname{trdeg}(K/L).$$ □

If K/F is purely transcendental and $\operatorname{trdeg}(K/F)=1$, then we can take assume that $K=F(x)$ for some indeterminate x.

$F(x)$ is the field of rational functions in x over F, and has transcendence basis $\mathcal{B}=\{x\}$.

<u>Def</u>: If $0 \neq \alpha \in F(x)$, and say $\alpha = f(x)/g(x)$, $(f(x), g(x))=1$, then define the <u>degree</u> of α to be $\deg \alpha = \max\{\deg f(x), \deg g(x)\}$.

<u>Prop 5.5</u>: If $K=F(x)$ and $\alpha \in K \setminus F$, then α is transcendental over F, and $[K:F(\alpha)] = \deg \alpha$.

$$\begin{tikzcd} K = F(x) \arrow[d, dash, dashed, "\text{alg.}"] \\ F\left(f(x)/g(x)\right) = F(\alpha) \arrow[d, dash, "\text{trans.}"] \\ F \end{tikzcd}$$

<u>Pf</u>. Say $\deg \alpha = n > 0$, and write

$\alpha = f(x)/g(x)$ with

$f(x) = a_0 + a_1 x + \dots + a_n x^n$

$g(x) = b_0 + b_1 x + \dots + b_n x^n \in F[x]$,

at least $a_n \neq 0$ or $b_n \neq 0$.

Let y be another indeterminate over K, and set

$$h(y) = h_\alpha(y) = \alpha\, g(y) - f(y) \in F[\alpha][y] \subseteq K[y]$$

The leading coefficient of $h(y)$ is $\alpha b_n - a_n$, so $\deg h(y) = n$ and $h(x) = 0$.

Therefore, x is algebraic of degree $\leq n$ over $F(\alpha)$, and so α is transcendental over F.

* It suffices to show that $h(y)$ is the minimal polynomial of x (i.e, that $h(y)$ is irreducible over $F(\alpha)$).

If $h_\alpha(y)$ were reducible in $F(\alpha)[y]$, it would be reducible in $F[\alpha][y] = F[\alpha, y]$. (Contrapositive to Gauss' lemma; Thm 3.13 Rings).

Since $\deg h_\alpha(y) = 1$ in α, if $h_\alpha(y)$ factored, then

$h_\alpha(y) = u(y)\, v(\alpha, y)$, $\deg u(y) = 0$ in α $\Rightarrow u(y) \in F[y]$,

and $v(\alpha, y) \in F[\alpha, y]$ has degree 1 in α.

Let $\phi : F[\alpha, y] \longrightarrow F[y]$, $\phi(\alpha) = 0$, $\phi(y) = y$.

Apply ϕ to $\alpha g(y) - f(y) = u(y)\, v(\alpha, y)$

$\Longrightarrow$ $-f(y) = u(y)\, v(0, y) \Rightarrow u(y) \mid f(y)$ in $F[y]$.

Also, $u(y) \mid \alpha g(y) = h_\alpha(y) + f(y) \Rightarrow u(y) \mid g(y)$.

Since $(f(y), g(y)) = 1$ in $F[y]$, $\deg u(y) = 0$, and thus

$h_\alpha(y)$ is reducible over $F(\alpha)$.

Since $K = F(x) = F(\alpha)(x)$, $[K : F(\alpha)] = \deg h_\alpha(y) = n = \deg \alpha$. $\square$

<u>Cor 1</u>: The minimal polynomial $m(y)$ for x over $F(\alpha)$ is an $F(\alpha)$-multiple of $\alpha g(y) - f(y)$.

<u>Cor 2</u>: If $K = F(x)$ and $\alpha \in K \setminus F$, then $K = F(\alpha)$ iff $\deg \alpha = 1$, i.e., if $\alpha = (ax+b)/(cx+d)$, with $a, b, c, d \in F$ and $ad \neq bc$.

<u>Pf</u>: Since $[K : F(\alpha)] = \deg \alpha$, we have $K = F(\alpha)$ iff $\deg \alpha = 1$, i.e., $\alpha = (ax+b)/(cx+d)$. If $ad = bc$, then either $\alpha = a/c$ or $b/d \in F$.

$\square$

Def: If V is an n-dimensional vector space, then the projective linear group is the quotient $PGL(n,F) = GL(n,F)/Z(GL(n,F))$, i.e, $n \times n$ invertible matrices, quotient by $\{kI : k \in F\}$.

Thm 5.6: If $K = F(x)$, x transcendental over F, then $Gal(K/F) \cong PGL(2,F)$.

Pf: Any $\phi \in G := Gal(K/F)$ must take x to a primitive element, i.e, $\phi(x) = (ax+b)/(cx+d)$ for some $a,b,c,d \in F$, $ad \neq bc$, by Cor 2.

Conversely, defining $\phi(x) = (ax+b)/(cx+d)$ completely determines $\phi \in G$ since $K = F(x)$.

Define
$$f : GL(2,F) \longrightarrow G$$
$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \longmapsto \phi \quad \text{where } \phi(x) = (ax+b)/(cx+d).$$

If $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL(2,F)$ and $f(A) = 1 \in G$, then
$$(ax+b)/(cx+d) = x \Rightarrow ax+b = cx^2+dx \Rightarrow b=c=0,\ a=d.$$

Thus, $\ker f = \{aI : a \in F \setminus \{0\}\} = Z(GL(2,F))$

By the FHT for Rings, $G \cong GL(2,F)/Z(GL(2,F)) = PGL(2,F)$. $\square$

Notation: If $f(x,y) \in F[x,y]$, then we can think of $f(x,y)$ as a polynomial $f_y(x) \in F[y][x]$ or $f_x(y) \in F[x][y]$.

Example: $f(x,y) = xy - yx^3 + x^3y + x^4y^2$

$f_y(x) = (y - y^3)x + yx^3 + y^2x^4 \qquad \deg f_y(x) = 4$

$f_x(y) = (x + x^3)y + x^4y^2 - xy^3 \qquad \deg f_x(y) = 3.$

Thm 5.7 (Lüroth's Theorem): Suppose $K = F(x)$ with x transcendental over F, and $F \subsetneq L \subsetneq K$. Then $L = F(\gamma)$ for some $\gamma \in K$ that is transcendental over F.

Pf: If $\beta \in L \setminus F$, then x is algebraic over $F(\beta) \subseteq L$ by Prop 5.5. In this case x is also algebraic over L.

Let $m_x(y) = a_0 + a_1 y + \cdots + y^n$ be the minimal polynomial of x over F, and so $[K:L] = [L(x):L] = n$.

At least one a_i is not in F, say $a_i = a_i(x) = \gamma \in L \setminus F$.

By Prop 5.5, $[K : F(\gamma)] = k \geq n$ (since $F(\gamma) \subseteq L \subseteq K$).

* It suffices to show that $k = n$.

By "clearing denominators" (multiplying through by $b_n := \operatorname{lcm}(a_1, \ldots, a_n)$) we may replace $m_x(y) \in F(x,y)$ with a primitive element $u_x(y) = b_0 + b_1 x + \cdots + b_n x^n \in F[x,y]$, $b_j = b_j(x) \in F[x]$.

Since $\gamma = a_i = b_i / b_n = f(x)/g(x)$, $\deg u_y(x) \geq k$.

Set $h_x(y) = \gamma g(y) - f(y) \in L[y]$.

$$h_x(x) = 0 \implies m_x(y) \mid h_x(y) \text{ in } L[y], \text{ say}$$

$$m_x(y)\, p_x(y) = \gamma g(y) - f(y) = [f(x)/g(x)]\, g(y) - f(y), \quad p_x(y) \in L[y].$$

Set $r(x,y) = f(x) g(y) - f(y) g(x) \in F[x,y]$

Note: $\deg r_x(y) = \deg r_y(x) = k$.

Also, $m_x(y)\, p_x(y)\, g(x) = f(x)g(y) - f(y)g(x) = r_x(y)$. $(*)$

View the LHS of this as an element in $F(x)[y]$.

The denominators of coefficients cancel, and since $u_x(y)$ is primitive, we may rewrite $(*)$ as

$$u(x,y)\, q(x,y) = r(x,y) \quad \text{for some } q(x,y) \in F[x,y].$$

Now, $k = \deg r_y(x) = \deg u_y(x) + \deg q_y(x) \geq k + \deg q_y(x)$.

So, $\deg q_y(x) = 0$, $q(x,y) = q(y) \in F[y]$ (and $\deg u_y(x) = k$).

<u>Note</u>: $q(y)$ is primitive (its nonzero coefficients are units), so by Gauss' Lemma (Thm 3.13 Rings), so is $u_x(y)\, q(y)$.

Thus, $r_x(y) = u_x(y)\, q(y)$ is primitive over $F[x]$.

But $r(x,y) = -r(y,x) \Rightarrow r_y(x) = u_y(x)\, q(y)$ is primitive over $F[y]$

Therefore $q(y)$ is constant, i.e., $q(y) = q \in F \setminus \{0\}$, so

$n = \deg u_x(y) = \deg r_x(y) = k$. $\square$

<u>Remark</u>: There is an analog of Lüroth's theorem for purely transcendental extensions of degree 2 (Castelnuovo & Zariski), if F is algebraically closed and K/L separable.

Almost nothing is known for degree-3 transcendental extensions.