5. Transcendental field extensions

Throughout, $K$ is an extension field of $F$.

Def: A set $S \subseteq K$ is algebraically dependent over $F$ if there are distinct elements $a_1, \ldots, a_k \in S$ and a nonzero polynomial $f(x_1, \ldots, x_k) \in F[x_1, \ldots, x_k]$ with $f(a_1, \ldots, a_k) = 0$.

Otherwise, $S$ is algebraically independent.

Remark: 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 and results from linear algebra have similar versions in this setting.

Example 1: If $S = \{a_3\}$, then $S$ is algebraically dependent over $F$ iff $a$ is algebraic over $F$.

Example 2: 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 transcendence set over $F$.

Exercise: Show that $S \subseteq K$ is algebraically dependent over $F$ iff there is some $a \in S$ that is algebraic over $F(S \setminus \{a_3\})$.

Think: Formulate an analogous statement for linear dependent sets over $V$. 


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

Example 3: $K=F(x)$ is purely transcendental.

Example 4: $R/Q$ is transcendental, but not purely transcendental.

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

Compare: 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 $F$.

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

Prop 5.1: 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 $F(S)$.

Remark: 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 \( S = \{ b_1, \ldots, b_k \} \) (possibly empty), and let
\( f(x_0, x_1, \ldots, x_k) \in F[x_0, x_1, \ldots, x_k] \) be a nonzero polynomial with \( f(a, b_1, \ldots, b_k) = 0 \).
Note that \( x_0 \) occurs in \( f(X) \), since \( S \) is a transcendental set.
Define \( g(x_0) = f(x_0, b_1, \ldots, b_k) \in F(S)[x_0] \).
Then \( g(x_0) \neq 0 \) but \( g(a) = 0 \Rightarrow a \) is algebraic over \( F(S) \).

PF: \( \Leftarrow \) Suppose \( g(a) = 0 \) for some \( 0 \neq g(x) \in F(S) \).
We may assume WLOG that \( g(x) \in F[b_1, \ldots, b_k][x] \) for some \( \{ b_1, \ldots, b_k \} \subseteq S \).
Then \( g(a) = 0 \) is a nontrivial algebraic dependence relation
over \( F \) for \( \{ a, b_1, \ldots, b_k \} \), and hence for \( S \cup \{ a \} \).

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
\( \Omega(S) = \Omega_{K,F}(S) = \{ a \in K : a \text{ is algebraic over } F(S) \} \)
is the algebraic closure of \( F(S) \) in \( K \).

This is the analog of the span of a set of vectors \( S \subseteq V \).

Easily verifiable facts:

(i) \( S \subseteq \Omega(S) \);
(ii) If \( S \subseteq T \subseteq K \), then \( \Omega(S) \subseteq \Omega(T) \);
(iii) If $a \in \sigma_2(S)$, then $a \in \sigma_2(S')$ for some finite set $S \subseteq S$;
(iv) $\sigma_2(\sigma_2(S)) = \sigma_2(S)$.

Prop 5.2: Suppose $S \subseteq K$, $a, b \in K$, and $b \notin \sigma_2(S \cup \{a, 3\})$.
Then $a \in \sigma_2(S \cup \{b, 3\})$.

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

By Prop 5.1, $\{a, b, 3\}$ is algebraically dependent over $L$.
Choose $f(x_1, x_2) \neq 0$ in $L[x_1, x_2]$ with $f(a, b) = 0$.

Note: $x_1$ must occur in $f(x_1, x_2)$, since $b$ is transcendental over $L$.
Thus, $0 \neq g(x_1) = f(x_1, g) \in L(b)[x_1] = F(S \cup \{b, 3\})[x_1]$,
and $g(a) = 0$. Therefore, $a \in \sigma_2(S \cup \{b, 3\})$.

Thm 5.3: If $A$ and $B$ are transcendence bases for $K/F$,
then $|A| = |B|$.

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

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

Note: $B \notin \sigma_2(A \setminus \{a, 3\})$; in particular, $a_i \in \sigma_2(B)$ but $a_i \notin \sigma_2(A \setminus \{a, 3\})$.
Choose $b_i \in B \setminus \sigma_2(A \setminus \{a, 3\})$.

Prop 5.1 $\Rightarrow A_i = \{b_i, a_2, ..., a_n\}$ is a transcendence set.
Prop 5.2 $\Rightarrow a_i \in \sigma_2(A_i)$. 


Therefore, $A_1$ is a transcendence basis.

Inductively, define $A_k = \{b_1, \ldots, b_k, A_{k+1}, \ldots, A_n\}$, which is also a transcendence basis.

Consider $k = n$: $A_n = \{b_1, \ldots, b_n\} \subseteq B$, 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 $a \in \sigma(B_a)$.

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

If this set was $C \subseteq B$, then $B \subseteq K \subseteq \sigma(A) \subseteq \sigma(C)$, contradicting algebraic independence of $B$.

Thus, $|B| = |\bigcup_{a \in A} B_a| \leq \sum_{a \in A} |B_a| \leq \aleph_0 |A| = |A|$. √

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

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

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

Motivating example: Over $\mathbb{Q}$, $\{\sqrt{3}, \sqrt{2}, \sqrt{3} \sqrt{2}\}$ are linearly independent, but $\{\pi, e, \pi e\}$ are algebraically dependent.
Proof: Let A be a transcendence basis for L/F, and let B be a transcendence basis for K/L.

Clearly, \( A \cap B = \emptyset \), 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, \( \text{tr.deg}(K/F) \leq |A \cup B| \).

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 \( F(a_1, \ldots, a_m, b_1, \ldots, b_n) = 0 \) with \( a_i \in A, b_j \in B \).

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

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

But then \( g_i(x_1, \ldots, x_m) = 0 \in F[X] \), 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

\( \text{tr.deg}(K/F) = |A \cup B| = |A| + |B| = \text{tr.deg}(L/F) + \text{tr.deg}(K/L) \).
If $K/F$ is purely transcendental and $\text{trdeg}(K/F) = 1$, 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 $B = \{x\}$.

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

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

Pf: Say $\deg \alpha = n > 0$, and write $\alpha = \frac{f(x)}{g(x)}$ with $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ and $g(x) = b_0 + b_1 x + \ldots + b_n x^n \in F[x]$, 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 $\alpha$ 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 \( h_x(y) \) were reducible in \( F(x)[y] \), it would be reducible in \( F[x][y] = F[x, y] \). (Contrapositive to Gauss' lemma; Thm 3.13 Rings).

Since \( \deg h_x(y) = 1 \) in \( x \), if \( h_x(y) \) factored, then

\[
h_x(y) = u(y) \cdot v(x, y), \quad \deg u(y) = 0 \text{ in } x \Rightarrow u(y) \in F[y],
\]
and \( v(x, y) \in F[x, y] \) has degree 1 in \( x \).

Let \( \phi : F[x, y] \to F[y] \), \( \phi(x) = 0 \), \( \phi(y) = y \).

Apply \( \phi \) to \( x \cdot g(y) - f(y) = u(y) \cdot v(x, y) \)

\[
\Rightarrow \frac{-f(y)}{u(y)} \cdot v(0, y) \Rightarrow u(y) \mid f(y) \text{ in } F[y].
\]

Also, \( u(y) \mid x \cdot g(y) = h_x(y) + f(y) \Rightarrow u(y) \mid g(y) \).

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

\( h_x(y) \) is reducible over \( F(x) \).

Since \( K = F(x) = F(x)(x) \), \( [K : F(x)] = \deg h_x(y) = n = \deg x \).

\[\square\]

Cor 1: The minimal polynomial \( m(y) \) for \( x \) over \( F(x) \) is an

\( F(x) \)-multiple of \( x \cdot g(y) - f(y) \).

Cor 2: If \( K = F(x) \) and \( x \in K \setminus F \), then \( K = F(x) \) iff \( \deg x = 1 \),

i.e., if \( x = (ax+b)/(cx+d) \), with \( a, b, c, d \in F \) and \( ad \neq bc \).

\[\text{PF:} \] Since \( [K : F(x)] = \deg x \), we have \( K = F(x) \) iff \( \deg x = 1 \),

i.e., \( x = (ax+b)/(cx+d) \). If \( ad = bc \), then either \( x = \gamma c \) or \( b/d \in F \).

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

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

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

Conversely, defining $\phi(x) = \frac{(ax+b)}{(cx+d)}$ completely determines 
$\phi \in \text{Gal}(K/F)$ since $K = F(x)$.

Define $f : \text{GL}(2,F) \rightarrow \text{G}$ 

$$
\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto \phi \quad \text{where} \quad \phi(x) = \frac{(ax+b)}{(cx+d)}.
$$

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

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

By the FHT theorem, $\text{G} \cong \text{GL}(2,F)/\mathbb{Z}(\text{GL}(2,F)) = \text{PGL}(2,F) \quad \Box$

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

$$
\begin{align*}
    f_y(x) &= (y-y^3) x + y x^3 + y^2 x^5 \quad \deg f_y(x) = 4 \\
    f_x(y) &= (x+x^3) y + x^4 y^2 - x y^3 \quad \deg f_x(y) = 3.
\end{align*}
$$
Thm 5.7 (Lüroth's Theorem): Suppose \( K = F(x) \) with \( x \) transcendental over \( F \), and \( F \subset L \subset K \). Then \( L = F(\tau) \) for some \( \tau \in K \) that is transcendental over \( F \).

\( \text{Pf.} \) 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 \( m_x(y) = a_0 + a_1 y + \ldots + y^n \) 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 \( a_i = a_i(x) = \tau \in L \setminus F \).

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

*It suffices to show that \( k = n\).

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

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

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

\( h_x(y) = 0 \Rightarrow m_x(y) \mid h_x(y) \) in \( L[y] \), say \( m_x(y) p_x(y) = \tau g(y) - f(y) = [f(x)/g(x)] g(y) - f(y) \), \( p_x(y) \in L[y] \).

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

Note: \deg r_x(y) = \deg \Gamma_y(x) = k.
Also, \( m_x(y) p_x(y) q(x) = f(x) g(y) - f(y) g(x) = r_x(y) \). (1)

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 (1) as

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

Now, 
\[ k = \deg r_x(x) = \deg u_y(x) + \deg q_y(x) \geq k + \deg q_y(x). \]

So, 
\[ \deg q_x(x) = 0, \quad q(x, y) = q(y) \in F[y] \quad \text{(and} \quad \deg u_y(x) = k). \]

Note: \( q(y) \) 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

\[ n = \deg u_x(y) = \deg r_x(y) = k. \]

Remark: There is an analog of Lüroth's theorem for purely transcendental extensions of degree 2 (Castelnuovo i; Zariski), if \( F \) is algebraically closed and \( K/L \) separable. Almost nothing is known for degree-3 transcendental extensions.