Lecture 5: transcendence and Pell

Friday, February 10, 2017 2:32 PM

Transendence Bases

If K/k is a field extension, we say $s_1, \ldots, s_n \in K$ are algebraically indep $\iff$ $k[x_1, \ldots, x_n] \longrightarrow K$, $x_i \longmapsto s_i$ is injective.

we say that $S \subset K$ is a transendence basis if $K/k(S)$ is algebraic. & S are algebraically independent

Thm transendence bases exist and have the same size.

Pf: (in the case of a finite transendence basis)

Aside: Matroid

Def: If X is a set, M a collection of (finite) subsets w/ at least one finite of X is a matroid if

- $m, m' \in M \Rightarrow m \not\subset m'$
- if $m, m' \in M$, $b \in m$ then $\exists\, b' \in m'$ s.t. $(m \setminus \{b\}) \cup \{b'\} \in M$.
- $m \in M \Rightarrow m \neq \emptyset$

Lemma: if M is a matroid then all elements of M ("bases") have the same size.

Pf: let $m \in M$ w/ $|m|$ minimal

if $m' \in M$ induct on $|m' \cap m|$

if $m' \subset m$ then $m' = m$ by Axiom 1

else, can find $b' \in m' \setminus m$

$\exists\, b \in m$ s.t. $(m' \setminus \{b'\}) \cup \{b\} \in M$ ← m''

so switching m for ↗, get new basis

w/ # elmts = $|m|$, such that $|m'' \cap m'|$ $\overset{\shortparallel}{|m \cap m'|+1}$

"induction" ☐

Pf of thm:

Suffices to show that $\overset{\text{max'l.}}{\vee}$ alg. indep sets are a matroid.

Let $S = \{s_1, \ldots, s_m\}$ $S' = \{s'_1, \ldots, s'_n\}$ are tr. bases.

know that each $s_1, \ldots, s_m$ are alg over $k(S')$ ⇒ ∃ polynomial w/ coeffs in $k[S']$ p_i

for which s_i is root

$K / k(s'_1, \ldots, s'_n)$ algebraic $s_i \in K$ satisfies a poly w/ coeffs in

$p_i(s_i) = 0$

poly expressions in $s'_1, \ldots, s'_n, s_i$

goal: want to show $\{s_i, s_2', \ldots, s_n'\}$ is a tr. basis.

consider all p_i's. at least one involves s_1'

else, s_i alg. over $s_2', \ldots, s_n'$ $\Rightarrow$ $L(s_1, \ldots, s_n)$ alg. over K, alg. over $L = k(s_2', \ldots, s_m')$

so WLOG p_i involves s_1'

claim $\{s_i, s_2', \ldots, s_m'\}$ tr. basis

know $p_i(s_i) = 0$

$\uparrow$ poly in $s_1', \underbrace{s_2', \ldots, s_m', s_i}$

s_1' alg. over $k(s_2', \ldots, s_m', s_i)$

if $\underbrace{s_2', \ldots, s_m'}_{\text{indep}}, s_i$ dependent $\Rightarrow$ s_i alg. over $s_2', \ldots, s_m'$

K /alg $L(s_1')$, alg $k(s_1', \ldots, s_n')$, $L(s_1') \supseteq k(s_1', \ldots, s_n')$

| alg

$L = k(s_i, s_2', \ldots, s_m')$ contradiction.

| alg

$k(s_2', \ldots, s_m')$ $\square$.

<u>Def</u>: K/k is separably generated if $\exists$ transcendence basis $\{s_\lambda\}$ of K/k s.t.

$K/k(s_\lambda)$ is separable.

Def K/k is separable ~~(regular)~~ if every intermediate field $K/L/k$ is separably generated.

Thm/Fact: separably generated $\Rightarrow$ separable.

moreover: K/k separable $\Longleftrightarrow$ K & k^{1/p^∞} are linearly disjoint. in an algebraic closure $\bar{K}$

where $p = \mathrm{char}\, k$

$$\begin{tikzcd}
 & \bar{K} \arrow[dl, dash] \arrow[dr, dash] & \\
\bar{k} \arrow[dr, dash] & & K \arrow[dl, dash] \\
 & k^{1/p^\infty} \arrow[d, dash] & \\
 & k &
\end{tikzcd}$$

Def: If $k \subset L, L' \subset K$, we define $[L, L']$ to be the field gen. by L, L' "composition"

Note: we always have a natural hom

$$L \otimes L' \longrightarrow [L, L']$$

$$\sum l_i \otimes l_i' \longmapsto \sum l_i l_i'$$

we say L, L' are linearly disjoint if this is injective.

i.e. note if $V \subset L'$ a k-vector subspace, then $L \otimes V \subset L \otimes L'$ is a L-vector subspace of same size.

if $\sum l_i \otimes l_i' \longmapsto 0$, let $V = \langle l_1', \dots, l_n' \rangle$

then we're saying that a basis for V, is not a basis for some in $[L, L']$ over L.

Said backwards: L, L' linearly disjoint $\Longleftrightarrow$ if $l_1, \dots, l_n'$ are k-independent in L' then they are L-independent in K.

Def k^{1/p^∞} = field ext. of k in $\bar{k}$ gen by all $\sqrt[p^n]{a}$, $a \in k$.

(or in above in $\bar{K} \supset \bar{k}$

Main tool: p-basis:

Given K/k field extension, char $k = p$, we say that B is a p-basis if the monomials in B of degree $< p$ in each elmt of B form a basis for K over $[k, K^p]$

The Frobenius:

If F is a field of char p, then the map

$$\begin{aligned} \text{frob}: F &\longrightarrow F \\ \lambda &\longmapsto \lambda^p \end{aligned}$$ is a ring homomorphism. "The Frobenius"

$(\lambda + \mu)^p = \lambda^p + \mu^p$

we can consider the image of this map: $F^p \simeq F$

$F/_{F^p \simeq F}$

Def F is perfect if frob is an isom (surjective)

$k(x,y) = K$ look at $K/[K^p; k]$

note: $x, y \notin K^p$

$K^p = k^p(x^p, y^p)$ $K/[K^p, k]$

$[K^p, k] = k(x^p, y^p)$

$1, x, x^2, \ldots, x^{p-1}, y, xy, x^2 y \ldots$

Principle: If K/k f.g. separable (~~regular~~) then p-basis = tr basis.

BACK TO FINITE

If E/F is a finite field extension, and $\alpha \in E$ then we define the char. poly of α to be the char poly of the linear transformation

$$m_\alpha : E \longrightarrow E$$
$$\beta \longmapsto \alpha\beta$$

in particular we define $\underset{\text{tr}_{E/F}(\alpha)}{\text{tr}(\alpha)} = \text{tr}(m_\alpha)$

$N(\alpha) = \det(m_\alpha)$

$N_{E/F}(\alpha)$

<u>Note:</u> $tr(\alpha+\beta) = tr(\alpha) + tr(\beta)$ $\quad N(\alpha\beta) = N(\alpha)N(\beta)$

why?: $m_{\alpha+\beta} = m_\alpha + m_\beta$ $\quad m_{\alpha\beta} = m_\alpha m_\beta$

In the case of a Galois extension $\begin{array}{c} E \\ |\,G \\ F \end{array}$, if $\alpha \in E$

then $tr(\alpha) = \sum_{\sigma \in G} \sigma(\alpha)$ $\quad N(\alpha) = \prod_{\sigma \in G} \sigma(\alpha)$

<u>moreover:</u> if $s_d(\alpha) = \sum_{i_1 < i_2 < \dots < i_d} \prod_j \sigma_{i_j}(\alpha)$

where $\{\sigma_1, \dots, \sigma_n\} = G$

then

$$\chi_\alpha(t) = t^n - \underbrace{s_1(\alpha)}_{tr(\alpha)} t^{n-1} + s_2(\alpha)\, t^{n-2} - \dots \mp \underbrace{s_n(\alpha)}_{N(\alpha)}$$

<u>Pf sketch:</u> • if α is a generator: $E = F(\alpha) = \frac{F[x]}{f(x)}$

then will check by hand.

• In generic, consider that entries in m_α (i.e. so coeffs of χ_α) are poly fcns in coeffs of $\alpha \in E$ (as an F space)

consider field extension $E(t_1, \dots, t_N)$ $\quad$ χ agrees

- contin...

$$F(t_1, \ldots, t_N)^G \quad \text{on} \quad \bar{F}^G$$

- consider elmt $\alpha = \sum t_i b_i$ $\{b_i\}$ basis for E/F

  it suffices to show that formula holds for α

  why? since α generates $E(t_1, \ldots, t_N)/F(t_1, \ldots, t_N)$

  if not, $\alpha \in$ a sub ext. $E(\vec{t})/F(\vec{t})$ $\Leftrightarrow$ subgps of G $\updownarrow$ subexts E/F

  $\Rightarrow \alpha$ is an ext. of frm $L(\vec{t})$

  $\Rightarrow$ so do all ways of specializ t! but

  these give all of E. Δ

Only need $F(\alpha) = E = F[x]/f(x)$

e.g. suppose we want to show $N(\alpha) = \prod_{\sigma \in G} \sigma(\alpha)$

$\min_\alpha(x) \in E[x]$

$\prod_{\sigma \in G} (x - \sigma(\alpha))$ so formulas hold in E i.e. true as elmts of E. so true in F.

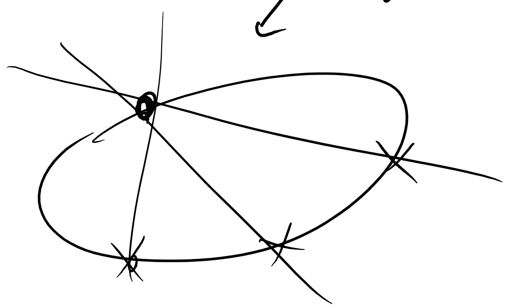
Pell's Equation:

$x^2 - ay^2 = b$ Can you solve it? maybe.

Can you describe solns?

direct, geometric

indirect, deep



Consider $F(\alpha) = \dfrac{F[t]}{t^2-a}$

$\alpha^2 = a$

suppose this is a field.

$$N(x+\alpha y) = (x+\alpha y)(x-\alpha y)$$
$$= x^2 - ay^2$$

i.e. Pell: $N(\beta) = b$.

if β is a soln, β' another then

$$N(\beta) = N(\beta') = b$$

$$N(\beta)N(\beta')^{-1} = N(\beta\beta'^{-1}) = 1$$

if $u^{-1} = \beta\beta'^{-1}$, $N(u) = 1$ then

$$\beta u = \beta'$$

i.e. $N(\beta') = b \iff \beta' = u\beta,\ N(u) = 1$

so, suffices to describe all elmts of Norm 1.

<u>Aside</u>: Norm 1 elements (in what kind of extension?)

$E/F \quad E = F(\alpha)\ \alpha^2 = a \qquad (\mathrm{char} \neq 2)$

Harmless to go to cyclic extensions

Thm (Hilbert's theorem 90) if $E \,|\, C_n = \langle \sigma \rangle \, F$ cyclic Galois extension

then $u \in E$ has $N(u) = 1$
iff $u = \sigma(v)/v$ for some $v \in E^*$.

$$E^* \longrightarrow \{u \in E \mid N(u) = 1\}$$
$$v \longmapsto \sigma(v)/v$$
$$vv' \longmapsto \sigma(vv')/vv' = \left(\sigma(v)/v\right)\left(\sigma(v')/v'\right)$$

kernel:
$$v \longmapsto \sigma(v)/v = 1 \qquad \sigma(v) = v \Rightarrow v \in E^\sigma = F$$

$$E^*/F^* \cong \{u \in E \mid N(u) = 1\}$$

Pf of Hilbert's theorem 90.

Given $u \in E^*$, define map $\psi : G \longrightarrow E^*$, where $G = \langle \sigma \mid \sigma^n = 1 \rangle$

$$e \longmapsto 1$$ "partial norms"
$$\sigma \longmapsto u$$
$$\sigma^2 \longmapsto \sigma(u)u$$
$$\sigma^3 \longmapsto \sigma^2(u)\sigma(u)u$$
$$\sigma^i \longmapsto \sigma^{i-1}(u)\sigma^{i-2}(u)\cdots u$$

$$\psi(\sigma^i) \cdot \sigma^i(\psi(\sigma^j))$$
$$= \sigma^{i-1}(u)\sigma^{i-2}(u)\cdots\sigma(u)u \cdot \sigma^i(\sigma^{j-1}(u)\cdots\sigma(u)u)$$
$$=$$

$\psi(\sigma^{i+j}) = \sigma^{i+j-1}(u) \cdots \sigma(u)u$

$\psi(\sigma^i\sigma^j) = \psi(\sigma^i)\sigma^i(\psi(\sigma^j))$ (only checked this if $i+j<n$!)

what if $i+j \geq n$??

$\psi(\sigma^i\sigma^j) = \psi(\sigma^{i+j-n}) = \sigma^{i+j-n-1}(u) \cdots \sigma(u)u$,

$\overset{?}{=}$ $\psi(\sigma^i)\sigma^i(\psi(\sigma^j)) = \sigma^{i+j-1}(u) \cdots \sigma(u)u$

$\cdot\, \sigma^{i+j-1}(u) \cdots \sigma^{i+j-n}(u)$

$\sigma^{i+j-n}(\sigma^{n-1}(u) \cdots \sigma(u) \cdot u)$ n things

$= \sigma^{i+j-n}(N(u))$ $= N(u)$

Def: $\psi : G \longrightarrow A$, A an abelian gp (write mult) w/ an action by G

$G \to \mathrm{Aut}(A)$

we say ψ is a crossed homomorphism

if $\psi(gh) = \psi(g)\, g(\psi(h))$

Ex: $E \,|\, \langle\sigma\rangle = G \,|\, F$ then $\psi : G \longrightarrow E^*$ is crossed hom

$\Longleftrightarrow$ $\psi(\sigma^i) = \sigma^{i-1}(u) \cdots \sigma(u)u$

some u, $N(u)=1$

Pf: let $u = \psi(\sigma)$

$\psi(e) = \psi(e^2) = \psi(e)\, e(\psi(e))$

$= \psi(e)^2$

$\Rightarrow \psi(e) = 1$

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

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

$= u\,\sigma(\sigma^{i-2}(u) \cdots \sigma(u)u) = \sigma^{i-1}(u) \cdots \sigma(u)u$.

induction

& as above xed hom $\Leftarrow$ $N(u)=1$

induction $\quad$ & as ~~above~~ above $\quad$ Xed hom $\Leftrightarrow$ $N(u)=1$

<u>So:</u> Let's describe the crossed homomorphisms.

why not make
$$\begin{array}{c} E \\ \big|\, G \\ F \end{array}$$
arb.? finite.

Xed homs: $G \longrightarrow E^{\times}$

<u>Thm</u> if $\psi: G \longrightarrow E^*$ is a crossed hom, then $\exists\, u \in E^*$ s.t. $\psi(\sigma) = \sigma(u)/u$

What are crossed homomorphism about, anyways?

<u>Descent:</u>
$$\begin{array}{c} E \\ \big|\, G \\ F \end{array}$$
how to compare vectr spaces over E & F?

given a vectr space $V/F \rightsquigarrow$ get v.space $V \otimes_F E / E$

observation: $V \otimes_F E$ has an added bonus: action of G!