Lecture 11 Preliminaries for transcendence bases

This lecture and the next one follow 9.1 – 9.13 of Milne's *Fields and Galois Theory*. Let E/K be a field ext'n. We say that $\{\alpha_1, \dots, \alpha_n\} \subseteq E$ is *algebraically independent* over K if the ring homomorphism

$$\begin{aligned} K[X_1, \dots, X_n] &\xrightarrow{\varphi} K[\alpha_1, \dots, \alpha_n] \\ f(X_1, \dots, X_n) &\longmapsto f(\alpha_1, \dots, \alpha_n) \end{aligned}$$

is an isomorphism. If so, then $K(\alpha_1, \dots, \alpha_n)$ is called a *pure transcendental* field ext'n of K.

More generally, we say that $S \subseteq F$ is algebraically independent over K is every finite subset of S is algebraically independent over K.

With the help of Baker's theorem* we may prove that many numbers are trascendental over $\mathbb{Q}$. But we still don't know whether $S = \{\pi, e\}$ is algebraically independent $/ \mathbb{Q}$.

---

* Baker A., *Linear forms in logarithms of algebraic numbers I*, Mathematika 13, pp. 204 – 216, 1966.

<u>Lemma 1</u> Let $\gamma \in E$ and $S \subseteq E$. The following are equivalent

(a) γ is algebraic over $K(S)$

(b) $\exists\ \beta_0, \dots, \beta_{n-1} \in K(S)$ s.t.

$$\gamma^n + \beta_{n-1}\gamma^{n-1} + \dots + \beta_1\gamma + \beta_0 = 0$$

(c) $\exists\ \beta_0, \dots, \beta_n \in K[S]$ not all 0 s.t.

$$\beta_n\gamma^n + \beta_{n-1}\gamma^{n-1} + \dots + \beta_1\gamma + \beta_0 = 0 \qquad \star$$

(d) $\exists\ F \in K[X_1, \dots, X_m, Y]$ and $\alpha_1, \dots, \alpha_m \in S$ s.t.

$$F(\alpha_1, \dots, \alpha_m, Y) \neq 0 \ \& \ F(\alpha_1, \dots, \alpha_m, \gamma) = 0. \qquad \star'$$

Proof

(a) $\Rightarrow$ (b) $\Rightarrow$ (c) $\Rightarrow$ (a) is clear.

(d) $\Rightarrow$ (c): Any $F \in K[X_1, \dots, X_m, Y]$ may be expressed as

$$F = f_n(X_1, \dots, X_m)Y^n + \dots + f_1(X_1, \dots, X_m)Y + f_0(X_1, \dots, X_m).$$

Just put for $i \in \{0, \dots, n\}$:

$$\beta_i := f_i(\alpha_1, \dots, \alpha_m),$$

which are not all 0 because $F(\alpha_1, \dots, \alpha_m, Y) \neq 0$, and (c) follows.

(c) $\Rightarrow$ (d): $\forall\, i \in \{0, \dots, n\}$ we have $\beta_i \in K[S_i]$ s.t. $|S_i| < \infty$.

Thus $\beta_0, \ldots, \beta_n \in K[\alpha_1, \ldots, \alpha_m] =: E'$, where

$$\{\alpha_1, \ldots, \alpha_m\} := \bigcup_{i=0}^{n} S_i$$

So eq'n ($\bigstar$) says that γ is a root of

$$\beta_n(\alpha_1, \ldots, \alpha_m) Y^n + \ldots + \beta_0(\alpha_1, \ldots, \alpha_m) \in E'[Y].$$

Hence the polynomial $F \in K[X_1, \ldots, X_m, Y]$ defined by

$$F := \beta_n(X_1, \ldots, X_m) Y^n + \ldots + \beta(X_1, \ldots, X_m)$$

satisfies ($\bigstar'$), thus (d) follows $\square$

We say that $\gamma \in E$ is algebraically dependent on S over K if it satisfies any of (a), ..., (d) and write $\gamma \prec S$. A set B is algebraically dependent on S over K if $x \prec S$, for each $x \in B$ and we write $B \prec S$.

<u>Lemma 2</u> (Exchange Property) Let $\{\alpha_1, \dots, \alpha_m\} \subseteq E$. If $\beta \in E$ is s.t.

- $\beta \prec \{\alpha_1, \dots, \alpha_{m-1}, \alpha_m\}$,
- $\beta \not\prec \{\alpha_1, \dots, \alpha_{m-1}\}$,

then $\alpha_m \prec \{\alpha_1, \dots, \alpha_{m-1}, \beta\}$, *Proof*

As $\beta \prec \{\alpha_1, \ldots, \alpha_m\}$, $\exists\, F \in k[X_1, \ldots, X_m, Y]$ s.t.

$$F(\alpha_1, \ldots, \alpha_{m-1}, \alpha_m, Y) \neq 0 \qquad \text{☆}$$

$$F(\alpha_1, \ldots, \alpha_{m-1}, \alpha_m, \beta) = 0 \qquad \text{☆}'$$

by Lemma 1 (d). Note that

$$F = \sum_k a_k(X_1, \ldots, X_{m-1}, Y)\, X_m^k, \qquad *$$

so (☆) implies

$$F(\alpha_1, \ldots, \alpha_m, Y) = \sum_k a_k(\alpha_1, \ldots, \alpha_{m-1}, Y)\, \alpha_m^k \neq 0.$$

This means that for some k_0 we have

$$a_{k_0}(\alpha_1, \ldots, \alpha_{m-1}, Y) \neq 0.$$

But $\beta \not< \{\alpha_1, \ldots, \alpha_{m-1}\}$, so

$$a_{k_0}(\alpha_1, \ldots, \alpha_{m-1}, \beta) \neq 0.$$

This and $(*)$ give

$$F(\alpha_1, \ldots, \alpha_{m-1}, X_m, \beta) \neq 0.$$

Lemma 1 (d) with the latter and $(*')$ imply that

$$\alpha_m < \{\alpha_1, \ldots, \alpha_{m-1}, \beta\} \quad \square$$

Lemma 3 Algebraic dependence is transitive, that is, if

- $C \prec B$,
- $B \prec A$,

then $C \prec A$.

Proof

For each algebraic field extn E_1 / E_2 and each $\alpha \in E_1$ let

$$P_{\alpha / E_2}(X) = X^d + a_{d-1} X^{d-1} + \ldots + a_0 \in E_2[X]$$

be its minimal polinomial / E_2. Recall that any finitely generated algebraic ext'n is of finite degree. In particular, if E_2 / E_3 is algebraic, then

$$\begin{array}{c} E_3(a_0, \dots, a_{d-1}) =: L \\ | \\ E_3 \end{array} \Bigg\} \text{ degree } \delta < \infty$$

Thus α is algebraic over E_3 as $\alpha \in L(\alpha)$ and $L(\alpha)$ is finite over E_3, a fact which follows from the diagram

$$
\begin{tikzcd}
E_2(\alpha) \arrow[d, dash, "d"'] \arrow[dr, dash] & & \\
E_2 \arrow[dr, dash] & L(\alpha) \arrow[d, dash, "d"'] & \\
& L \arrow[d, dash, "\delta"'] & d\delta < \infty \\
& E_3 &
\end{tikzcd}
$$

The lemma follows if we invoke (a) of Lemma 1 $\square$