Math 210B. Separating transcendence basis

In this handout we prove that if K/k is a finitely generated extension of a *perfect* field k then there exists a separating transcendence basis (i.e., a transcendence basis $\{y_1, \dots, y_m\}$ such that the finite extension $K/k(y_1, \dots, y_m)$ is separable). In characteristic 0 this is trivial (every transcendence basis works!), so we now assume without further comment that $\mathrm{char}(k) = p > 0$.

1. An induction

Writing $K = k(x_1, \dots, x_n)$ for some elements $x_1, \dots, x_n \in K$ with $n \geq 1$, we shall induct on n. If $n = 1$ then $K = k(x)$ where either x is algebraic over k or is transcendental over k. In the first case K/k is a finite extension and as such must be separable since k is perfect. In the second case $\{x\}$ is clearly a separating transcendence basis. Thus, we now assume $n > 1$ and that the result is known for all finitely generated extensions of k with at most $n-1$ generators (as a field extension).

If $\{x_i\}$ is algebraically independent over k then it is clearly a separating transcendence basis for K/k, so we may assume there is a nontrivial algebraic dependence relation over k. That is, there exists a nonzero $f \in k[X_1, \dots, X_n]$ such that $f(x_1, \dots, x_n) = 0$ in K. Since K is a domain, the same vanishing must hold for some irreducible factor of f, so we may and do assume f is irreducible.

The gritty part of the argument, which we now carry out, is to exploit the induction to reduce to the case in which *every* non-empty proper subset of $\{x_1, \dots, x_n\}$ is algebraically independent over k. Suppose to the contrary that some non-empty proper subset is algebraically dependent over k. By relabeling we can assume this proper subset is contained in $\{x_1, \dots, x_{n-1}\}$, so there exists a nonzero $h \in k[X_1, \dots, X_{n-1}]$ (not necessarily involving all of the X_j's for $j < n$) such that $h(x_1, \dots, x_{n-1}) = 0$. Hence, $F := k(x_1, \dots, x_{n-1})$ has transcendence degree over k equal to some value $m \leq n-2$. But F has at most $n-1$ generators over k, so by induction F admits a separating transcendence basis $y_1, \dots, y_m$.

Since F is *finite separable* over $E := k(y_1, \dots, y_m)$, it admits a primitive element α over E. Thus,

$$K = F(x_n) = (E(\alpha))(x_n) = (E(x_n))(\alpha)$$

is finite separable over $E(x_n) = k(y_1, \dots, y_m, x_n)$ (as the minimal polynomial of α over $E(x_n)$ must divide the minimal polynomial for α over E that is separable by design). Since $E(x_n)/k$ with transcendence degree m (why?) is generated by $m + 1 \leq n - 1$ elements, *by induction* it admits a separating transcendence basis! That is, there exist $Z_1, \dots, Z_m \in E(x_n)$ algebraically independent over k such that $E(x_n)$ is finite separable over $k(Z_1, \dots, Z_m)$. But then clearly $K/k(Z_1, \dots, Z_m)$ is a tower of finite separable extensions and hence is finite separable. That is, $\{Z_j\}$ is a separating transcendence basis for K/k.

We have disposed of the cases in which $\{x_1, \dots, x_n\}$ admits a non-empty proper subset algebraically dependent over k, so for the rest of the argument we may assume that every non-empty proper subset of $\{x_1, \dots, x_n\}$ is algebraically independent over k. In particular, if we remove any single x_i from the collection then what remains is algebraically independent over k. Up to now we have used the perfectness of k only in the most trivial part of the case $n = 1$; its real purpose is yet to come.

2. Keeping track of pth-powers

As we have seen, we may find an irreducible $f \in k[X_1, \dots, X_n]$ such that $f(x_1, \dots, x_n) = 0$. Note that every X_i must occur in f, since we have reduced to the situation in which every non-empty proper subset of $\{x_1, \dots, x_n\}$ is algebraically independent over k. The key observation is that *some*

X_i must occur in f not entirely through X_i^p (i.e., some monomial in f involves X_i^e with $e > 0$ and $p \nmid e$). Indeed, otherwise since $k = k^p$ (!) we would have

$$f \in k[X_1^p, \ldots, X_n^p] = (k[X_1, \ldots, X_n])^p,$$

which is to say f is a pth power, contradicting that f is irreducible. Thus, by relabeling we can assume that X_n does not occur in f entirely through X_n^p.

Since f is irreducible $k[X_1, \ldots, X_n] = k[X_1, \ldots, X_{n-1}][X_n]$ and involves X_n, it is also irreducible when viewed in $k(X_1, \ldots, X_{n-1})[X_n]$ due to considerations with Gauss' Lemma (arguing similarly to Exercise 2 in HW1, using that $k[X_1, \ldots, X_{n-1}]$ is a UFD). But as an irreducible polynomial over the field $k(X_1, \ldots, X_{n-1})$ it doesn't involves X_n entirely through X_n^p, so f is *separable* over $k(X_1, \ldots, X_{n-1})$. By the algebraic independence of $\{x_1, \ldots, x_{n-1}\}$ we have

$$k[X_1, \ldots, X_{n-1}] \simeq k[x_1, \ldots, x_{n-1}]$$

as k-algebras via $X_j \mapsto x_j$, so passing to fraction fields gives $k(X_1, \ldots, X_{n-1}) \simeq k(x_1, \ldots, x_{n-1})$.

We conclude that the polynomial

$$f(x_1, \ldots, x_{n-1}, T) \in k(x_1, \ldots, x_{n-1})[T]$$

is irreducible and separable with x_n as a root (as $f(x_1, \ldots, x_n) = 0$!), so the field extension $K/k(x_1, \ldots, x_{n-1})$ is finite separable! By induction we can find a separating transcendence basis $\{Z_j\}$ for $k(x_1, \ldots, x_{n-1})$ over k, and by the *separability* of $K/k(x_1, \ldots, x_{n-1})$ it is clear that $\{Z_j\}$ is also a separating transencendence basis for K/k. This completes the proof.