Transcendence Bases and Noether Normalization

Suppose $k \subset K = k(x_i)$ is a field extension. An easy Zorn's Lemma argument implies that there exist subsets $\{y_j\} \subset \{x_i\}$ such that
(1) $\{y_j\}$ is algebraically independent over k and
(2) $k(y_j) \subset K$ is an algebraic extension.
Such a subset $\{y_j\}$ is called a **transcendence base** of K over k.

Proposition 1 *All transcendence bases for K over k have the same cardinality. (This cardinality is called the **transcendence degree** of K over k.)*

Proof The general case requires something like a well-ordering argument or Zorn's Lemma to handle large sets. Here is a proof that works in the finite case. Note the 'replacement lemma' below, and its proof, is completely parallel to standard arguments in linear algebra dealing with linearly independent sets and spanning sets in a vector space. ∎

Lemma 1 *Suppose the set $\{x_1, x_2, \ldots, x_m\} \subset K$ is algebraically independent over k and suppose the set $\{y_1, y_2, \ldots, y_n\} \subset K$ has the property that $k(y_j) \subset K$ is an algebraic extension. Then $m \leq n$ and we may reorder the ys so that $k(x_1, \ldots, x_m, y_{m+1}, \ldots, y_n) \subset K$ is an algebraic extension.* □

Reversing the roles of $\{x_i\}$ and $\{y_j\}$ in the lemma, you see that any two finite transcendence bases have the same cardinality. The lemma also implies that if one transcendence base is finite then so is any other.

Proof By the hypothesis on $\{y_j\}$, x_1 satisfies some non-trivial polynomial $P(y_j, x_1) = 0$ with coefficients in k. Choose such a P that involves the fewest number of ys. At least one y occurs, say y_1. (Otherwise x_1 would be algebraic over k.) Now rewrite P as a polynomial in y_1 whose coefficients are formally polynomials in x_1 and some of the y_j with $j > 1$. These coefficients cannot be 0 in K. This is because we chose P involving the fewest number of y's, so any coefficient polynomial that is formally not the 0 polynomial cannot represent the 0 element of K. Therefore y_1 is algebraic over $k(x_1, y_2, \ldots, y_n)$, and hence K is also algebraic over this field.

Repeat the procedure with x_2, which now satisfies a polynomial $Q(x_1, y_2, \ldots, y_n, x_2) = 0$. Choose Q involving the fewest number of y's. Since the $\{x_i\}$ are algebraically independent over k, at least one y_j, say y_2, occurs in Q. Rewriting Q as a polynomial in y_2, one concludes just as before that y_2 and hence K is algebraic over $k(x_1, x_2, y_3, \ldots, y_n)$. Continue until all x's replace y's. You cannot run out of y's first because $\{x_i\}$ is algebraically independent over k, so K cannot be algebraic over k with a proper subset of x's adjoined. ∎

The Noether Normalization Theorem provides a refinement of a choice of transcendence base so that certain ring extensions are integral extensions, not just algebraic extensions.

Proposition 2 *Suppose $k[x_1, \ldots, x_n]$ is a finitely generated integral domain over a field k, of transcendence degree r over k. Then there exist transcendence bases $\{y_1, \ldots, y_r\} \subset k[x_1, \ldots, x_n]$ so that $k[y_1, \ldots, y_r] \subset k[x_1, \ldots, x_n]$ is an integral extension. If k is an infinite field, the y's can be chosen to be linear combinations of the x's.* □

Example 1 Consider $k[x, z]$ where $xz - 1 = 0$. $\{z\}$ is a transcendence base, but x is not integral over $k[z]$. However, $x^2 + (z - x)x - 1 = 0$, so if $y = z - x$ then $k[x, z] = k[x, y]$ and $k[x, y]$ is integral over $k[y]$. □

PROOF We can certainly choose a set $\{y_1, \dots, y_s\}$ so that $k[x_1, \dots, x_n]$ is integral over $k[y_1, \dots, y_s]$, for example $\{x_i\}$ itself. But we will show that if we choose such $\{y_j\}$ with *s least*, then $\{y_j\}$ is algebraically independent over k. Hence $\{y_j\}$ is a transcendence base and $s = r$.

Suppose the y_j satisfy a polynomial equation $P(y_j) = 0$ with coefficients in k. WLOG, assume y_s occurs. The strategy will be to replace the y_j, $j < s$, by elements z_j so that $k[z_1, \dots, z_{s-1}, y_s] = k[y_1, \dots, y_s]$ and so that when written in terms of the new variables the polynomial $P(y_j)$ becomes a monic polynomial in y_s, or at least a polynomial with leading term a constant in k, which is just as good as monic. We then get two integral extensions $k[z_1, \dots, z_{s-1}] \subset k[z_1, \dots, z_{s-1}, y_s] = k[y_1, \dots, y_s] \subset k[x_1, \dots, x_n]$, so by transitivity of integral extensions we contradict the minimality of s.

First assume k is infinite. Set $z_j = y_j - u_j y_s$ for $j < s$, where $u_j \in k$ are constants to be determined. Note that if the y's are linear combinations of the original x's then so are the z's. Let $\sum_I c_I y^I$ be the sum of monomial terms of highest total degree N occurring in polynomial P, where y^I means $y_1^{i_1} y_2^{i_2} \cdots y_s^{i_s}$ with $i_1 + \cdots + i_s = N$. Look at $\sum_I c_I y^I = \sum c_I (z_1 + u_1 y_s)^{i_1} \cdots (z_{s-1} + u_{s-1} y_s)^{i_{s-1}} y_s^{i_s}$. Collect the coefficient of y_s^N, which is $c = \sum_I c_I u_1^{i_1} u_2^{i_2} \cdots u_{s-1}^{i_{s-1}}$. Since k is an infinite field, we can choose u_j so that $c \neq 0$. Obviously none of the homogeneous terms of P of degree $< N$ can contribute anything involving y_s^N. Therefore, the relation $P(y_j) = 0$ yields a relation $Q(z_j, y_s) = 0$ which is monic of degree N in y_s.

If k is finite, a polynomial in $s - 1$ variables can be identically 0 as a function on k^{s-1}. So we need to construct our monic polynomial for y_s over suitable $k[z_1, \dots, z_{s-1}]$ by a different method. The idea is to exploit the fact that if M is a large positive integer than all positive integers have a *unique* M-adic expansion $i_s + i_1 M + \cdots + i_{s-1} M^{s-1}$ with $0 \leq i_j < M$.

Write a presumed relation $P(y_j) = \sum d_I y^I = 0$, a sum over monomial terms of various total degrees. Again we assume y_s occurs. Let M be an integer greater than all exponents that occur in P for any of the y_j. Set $z_j = y_j - y_s M^j$ for $j < s$. In a typical monomial $d_I y^I$, with $y^I = y_1^{i_1} y_2^{i_2} \cdots y_s^{i_s}$, replace y_j by $z_j + y_s M^j$ for $j < s$. The pure power of y_s that occurs after expanding will have exponent $i_s + i_1 M + \cdots + i_{s-1} M^{s-1}$. All other terms involving y_s occurring in this monomial after expanding will have smaller exponent of y_s. By choice of M, these exponents of pure powers of y_s are distinct for all the monomial terms occurring in P. One of these exponents is greatest, and thus greater than any other power of y_s seen. Thus the relation $P(y_j) = 0$ yields a relation $Q(z_j, y_s) = 0$ which is monic in y_s, and we contradict the minimality of s just as before. ■

Remark 1 This proof by contradiction, starting with minimal s, is in reality somewhat more constructive than it might appear. One starts with all the $\{x_1, \dots, x_n\}$. If they are algebraically independent, there is nothing to do. Otherwise, using an explicit algebraic dependence, replace $n-1$ of the x's by appropriate elements z_j so that the remaining x is integral over $k[z_1, \dots, z_{n-1}]$. If the z's are algebraically independent, you are done. Otherwise replace $n - 2$ of the z's by appropriate elements so that the remaining z is integral over these. Continue the process until an algebraically independent set is reached. □

Remark 2 The normalization theorem can be used to eliminate one step in the proof of the Nullstellensatz, and give a slightly more satisfactory conclusion. Suppose $k[x_1, \dots, x_n]$ is a finitely generated integral domain over k of transcendence degree r, and suppose K is an algebraically closed field containing k. The Nullstellensatz asserts that there exist homomorphisms $k[x_1, \dots, x_n] \to K$ over k. Choose a transcendence base $\{y_1, \dots, y_r\}$ so that $k[y_1, \dots, y_r] \subset k[x_1, \dots, x_n]$ is an integral extension. Now, by the Going Up Theorem, any homomorphism $k[y_1, \dots, y_r] \to K$ over k, which is nothing more than just a point of K^r, will extend to a homomorphism $k[x_1, \dots, x_n] \to K$. There is no need to avoid points in some hypersurface in K^r. □

Example 2 Look at the equation $xz - 1 = 0$ again. For all values of x except $x = 0$, you can find a point (x, z) on this curve. With $y = z - x$, the equation becomes $x^2 + yx - 1 = 0$. For any value of y, you can find points (x, y) on this curve, at least over an algebraically closed field. $\square$