715: Lecture of December 11, 2002

Lemma (module-finiteness of certain extensions). *Let R be a ring and suppose that $U_1, \ldots, U_n$ are indeterminates over R. Let $G_1, \ldots, G_n$ be polynomials in $R[U_1, \ldots, U_n]$ such that $\deg G_i = d_i$, $1 \le i \le n$, and the degree i term in G_i is $U_i^{d_i}$. Then:*

(a) *The G_i are algebraically independent over R, and the monomials $U_1^{a_1} \cdots u_n^{a_n}$, $1 \le a_i < d_i$, $1 \le i \le n$, are a free basis for $R[U_1, \ldots, U_n]$ over $R[G_1, \ldots, G_n]$. Thus, $R[U_1, \ldots, U_n]$ is module-finite over $R[G_1, \ldots, G_n]$.*

(b) *The ring $R[U_1, \ldots, U_n]/(G_1, \ldots, G_n)$ is module-finite and free over R.*

(c) *The equations $G_i = 0$, $1 \le i \le n$, have a simultaneous solution for the U_i in a module-finite extension of R, which can be taken to be a domain if R is a domain.*

(d) *If one is given elements u_i' in an extension ring T of R that satisfy the equations G_i, the u_i' are integral over R.*

Proof. We prove (a) first: the other parts will then follow easily. Consider the set M of monomials in the G_i which have non-negative degree in each variable, and let N be the specified set of monomials in the U_i. We first claim that the set of products $MN = \{\mu\nu : \mu \in M, \nu \in N\}$ is a free basis for $R[U_1, \ldots, U_n]$ over R. If the exponents occurring in $\mu \in M$ are $a_1, \ldots, a_n$ and the exponents occurring in $\nu \in N$ are $r_1, \ldots, r_n$ then the highest degree term in $\mu\nu$ is $U_1^{a_1 d_1 + r_1} \cdots U_n^{a_n d_n + r_n}$. It follows from the uniqueness of quotient and remainder in the division algorithms for the various d_i that every monomial in the U_i occurs as the highest degree term in a unique element of MN. From this it follows easily that MN is a free basis for $R[U_1, \ldots, U_n]$ over R. (MN spans all polynomials of degree h by induction on h: each monomial of degree h in such a polynomial occurs in just one element of MN: subtracting off a suitable R-linear combination of these elements leaves a polynomial of degree at most $h-1$, which is already in the span by the induction hypothesis. If there were a nontrivial relation, consider a term of highest degree with nonzero coefficient: its unique highest degree term, $rU_1^{e_1} \cdots U_n^{e_n}$ could then be expressed R-linearly in terms of other monomials of the same degree and lower degree monomials, a contradiction.) From this it follows that M is a free basis for $R[G_1, \ldots, G_n]$ over R (i.e., that the G_j are algebraically independent over R) and also that the elements of N are a free basis for $R[U_1, \ldots, U_n]$ over $R[M] = R[G_1, \ldots, G_n]$, as specified. This proves (a).

For part (b), simply apply the base change $R[G_1, \ldots, G_n] \to R$ obtained by killing $G_1, \ldots, G_n$. The first statement in part (c) now follows: use the images of the U_i in $S = R[U_1, \ldots, U_n]/(G_1, \ldots, G_n)$ as the solution. If R is a domain, choose a prime P of S disjoint from the multiplicative system $R - \{0\}$, and replace S by S/P. The statement in part (d) follows from the fact that the $R[u_1', \ldots, , u_n']$ is a homomorphic image of $R[U_1, \ldots, U_n]/(G_1, \ldots, G_n)$. $\square$

Proof of the equational forcing lemma. We return to the notations in the discussion following the statement of the lemma. By the result just proved, R has a module-finite free extension S in which there are elements u_{ih} corresponding that satisfy:

$$(**_{ih}) \qquad u_{ih}^p = r_{ih} + \sum_{j=1}^{s} r'_{ij} y_h u_{jh}$$

for all i, h, and for each i we let $z'_i = \sum_{h=1}^{k} u_{ih} x_h$. Both the z_i and the z'_i then satisfy the equations

$$Z_i^p = \sum_{h=1}^{k} r_{ih} x_h^p + x^{p-1} \sum_{j=1}^{s} r'_{ij} Z_j,$$

Let $w_i = z_i - z'_i$. Subtracting equations we find that

$$w_i^p = x^{p-1} \sum_{j=1}^{s} r'_{ij} w_j$$

for all i, $1 \leq i \leq s$. Since x is a nonzerodivisor on R, it is a nonzerodivisor on the free R-algebra S, and we have $R \subseteq S \subseteq S_x$. Now the elements $w_i/x \in S_x$ satisfy the equations

$$(w_i/x)^p = \sum_{j=1}^{s} r'_{ij} (w_j/x),$$

and these have the right form to guarantee that the $w_i/x \in S_x$ are integral over S. Thus, the ring $S' = S[w_1/x, \ldots, w_n/x]$ is module-finite over S and over R, and in this ring the $z'_i \in (x_1, \ldots, x_k)S'$ and the $w_i \in xS' \subseteq (x_1, \ldots, x_n)S'$, so that it follows that the $z_i \in (x_1, \ldots, x_k)S'$ as well. If R is a domain, simply kill a prime of S' disjoint from the multiplicative system $R - \{0\}$ to get a domain extension. $\square$