Integral Closures in a Finite Separable Algebraic Extension

We want to prove that certain integral closures are module-finite: see the Theorem just below. We also give, at the end of this supplement, an example of a Noetherian discrete valuation domain of characteristic $p > 0$ whose integral closure is not module-finite.

Theorem. *Let R be a normal Noetherian domain and let $\mathcal{L}$ be a finite separable algebraic extension of the fraction field $\mathcal{K}$ of R (separability is automatic if $\mathcal{K}$ has characteristic 0). Then the integral closure S of R in L is a module-finite over R, and, hence, a Noetherian normal ring.*

When $\mathcal{K} \subseteq \mathcal{L}$ is a finite algebraic extension of fields, for any $\lambda \in \mathcal{L}$, we define $\mathrm{Tr}_{\mathcal{L}/\mathcal{K}}(\lambda)$ to be trace of the $\mathcal{K}$-linear map $\mathcal{L} \to \mathcal{L}$ given by λ: it may be computed by choosing a basis for L over K, finding the matrix of the map given by multiplication by λ, and summing the entries of the main diagonal of this matrix. It is independent of the choice of basis. If the characteristic polynomial is $x^n - cx^{n-1}+$ lower degree terms, where $n = [\mathcal{L} : \mathcal{K}]$, the trace is c. It is also the sum of the eigenvalues of the matrix (calculated in a splitting field for f or any larger field, such as an algebraic closure of $\mathcal{K}$), i.e., the sum of the roots of f (where if a root has multiplicity k, it is used a summand k times in the sum of the roots). We give a further discussion of the properties of trace following the proof of the theorem.

A key element of the proof is that a finite algebraic extension $\mathcal{L}$ of $\mathcal{K}$ is separable if and only if some element of $\mathcal{L}$ has nonzero trace in $\mathcal{K}$. This fact is quite trivial in characteristic 0, since the trace of the identity element is $[\mathcal{L} : \mathcal{K}] \neq 0$. This implies that the function $B : L \times L \to K$ that maps $(a,\, b)$ to the trace of ab is a non-degenerate symmetric bilinear form: it is non-degenerate because if c has nonzero trace, given $a \in L - \{0\}$, $B(a, c/a)$ is the trace of c, and so is not 0. Here, $n = [\mathcal{L} : \mathcal{K}]$. This non-degeneracy tells us that if $b_1, \, \ldots \, , b_n$ is any basis for $\mathcal{L}$ over $\mathcal{K}$, then the matrix $(Tr_{\mathcal{L}/\mathcal{K}} b_i b_j)$ is invertible over $\mathcal{K}$, and we shall assume this in proving the theorem. After we give the proof we discuss further the facts about bilinear forms and about trace that we are using, including the characterization of separability using trace in positive characteristic.

We next prove a preliminary result of great importance in its own right.

Theorem. *Let R be a normal domain with fraction field $\mathcal{K}$, and let $\mathcal{L}$ be a finite algebraic extension of $\mathcal{K}$. Let $s \in \mathcal{L}$ be integral over R. Multiplication by s defines a $\mathcal{K}$-linear map of $\mathcal{L}$ to itself. The coefficients of the characteristic polynomial of this $\mathcal{K}$-linear map are in R. In particular, $\mathrm{Tr}_{\mathcal{L}/\mathcal{K}}(s) \in R$.*

Proof. We first consider the case where $\mathcal{L} = \mathcal{K}[s]$. Let f be the minimal polynomial of s over $\mathcal{K}$, which has degree d. We showed earlier that f has all of its coefficients in R: this is the first Proposition in the Lecture Notes from Octboer 1. Suppose that f has degree d. Then $[\mathcal{L} : \mathcal{K}] = d$, and the characteristic polynomial of the matrix of multiplication by s has degree d. Since the matrix satisfies this polynomial, so does s. It follows that the characteristic polynomial is equal to the minimal polynomial of s over $\mathcal{K}$.

In the general case, let $\mathcal{L}_0 = \mathcal{K}[s] \subseteq L$, and let $v_1, \dots, v_d$ be a basis for $\mathcal{L}_0$ over $\mathcal{K}$, and let $w_1, \dots, w_h$ be a basis for $\mathcal{L}/\mathcal{L}_0$. Let A be the matrix of multiplication by s on $\mathcal{L}_0$ with respect to $v_1, \dots, v_d$. Then the span of $v_1w_j, \dots, v_dw_j$ is $\mathcal{L}_0w_j$ and is stable under multiplication by s, whose matrix with respect to this basis is also A. Therefore, the matrix of multiplication by s with respect to the basis

$$v_1w_1, v_2w_1, \dots, v_dw_1, \dots, v_1w_h, v_2w_1, \dots, v_dw_h$$

is the direct sum of h copies of A, and its characteristic polynomial is f^h, where f is the characteristic polynomial of A. We already know that f has coefficients in R. $\square$

Corollary. *Let R be a normal domain that contains $\mathbb{Q}$, and let S be a module-finite extension of R. Then R is a direct summand of S as an R-module. Hence, for every ideal I of R, $IS \cap R = I$.*

Proof. $R - \{0\}$ is a multiplicative system in S, and so there is a prime ideal P of S disjoint from $R - \{0\}$. Then R embeds in the domain S/P, which is still module-finite over R. It suffices to show that $R \hookrightarrow S/P$ splits, for if $\phi : S/P \to R$ is R-linear and restricts to the identity map on R, then the composition of ϕ with $S \twoheadrightarrow S/P$ will be an R-linear map $S \to R$ that restricts to the identity on R. Thus, we have reduced to the case where S is a module-finite extension domain of R. Let $\mathcal{K}$ and $\mathcal{L}$ be the fraction fields of R and S, respectively, and let $n = [\mathcal{L} : \mathcal{K}]$. Then $(1/n)\mathrm{Tr}_{\mathcal{L}/\mathcal{K}}$, when restricted to S, takes values in R (by the preceding Theorem), is R-linear, and is the identity when restricted to R. $\square$

Proof of the Theorem. Consider $\mathcal{K} \otimes_R S = (R - \{0\})^{-1}S \subseteq (S - \{0\})^{-1}S = \mathcal{L}$. This domain is module-finite over $\mathcal{K}$ and so has dimension 0. Therefore, it is a field containing S, and so must be $\mathcal{L}$. It follows that every element of $\mathcal{L}$ can multiplied in S by an element of $R - \{0\}$. Choose a basis for $\mathcal{L}$ over $\mathcal{K}$, and multiply each basis element by a nonzero element of R so as to get a basis for $\mathcal{L}$ over $\mathcal{K}$ consisting of elements of S. Call this basis $b_1, \dots, b_n$, where $n = [\mathcal{L} : \mathcal{K}]$. Because the field extension is separable, the matrix $A = \big(\mathrm{Tr}_{\mathcal{L}/\mathcal{K}}(b_ib_j)\big)$ is invertible. By the preceding theorem, each entry of this matrix is in R, and so the determinant D of this matrix is a nonzero element of R. We shall prove that $DS \subseteq Rb_1 + \cdots + Rb_n = G$. Since R is a Noetherian ring, G is a Noetherian R-module, and this implies that DS is a Noetherian R-module. But $S \cong DS$ as R-modules, via $s \mapsto Ds$.

It remains to show that $DS \subseteq R$. Let $s \in S$. Then $s \in L$ and so can be written uniquely in the form $\alpha_1b_1 + \cdots + \alpha_nb_n$. We may multiply by $b_i \in S$ and take the trace of both sides:

$$\mathrm{Tr}_{\mathcal{L}/\mathcal{K}}(sb_i) = \sum_{j=1}^{n} \alpha_j \mathrm{Tr}_{\mathcal{L}/\mathcal{K}}(b_ib_j),$$

Let $r_i = \mathrm{Tr}_{\mathcal{L}/\mathcal{K}}(sb_i)$, let W be the column vector whose entries are the r_i (which are in R, by the preceding Theorem), and let V be the column vector whose entries are the α_j. Then $W = AV$, where A and W have entries in R. Let B be the classical adjoint of A, i.e., the transpose of the matrix of cofactors. Then B also has entries in R, and $BA = D(I)$, where I is the size n identity matrix. It follows that $BW = BAV = DV$, so that each $D\alpha_j$ is in R. But then $Ds = (D\alpha_1)b_1 + \cdots + (D\alpha_n)b_n \in G$, as required. $\square$

We next backtrack and review some facts about bilinear forms. Let $\mathcal{K}$ be a field and V a vector space of finite dimension n over $\mathcal{K}$. A bilinear form is simply a bilinear map $B : V \times V \to \mathcal{K}$, and giving V is the same a giving a linear map $T : V \otimes V \to K$. If $v_1, \ldots, v_n$ is a basis for V, then the elements $v_i \otimes v_j$ are a basis for $V \otimes_{\mathcal{K}} V$, and so B is completely determined by the matrix $A = (B(v_i,\, v_j) = T(v_i \otimes v_j)$. If the matrix $A = (a_{ij})$. Suppose that we use this basis to identify V with $\mathcal{K}^n$, with standard basis $e_1, \ldots, e_n$, then $B(e_i, e_j) = a_{ij}$. If v and w are the $n \times 1$ column matrices with entries $c_1, \ldots, c_n$ and $d_1, \ldots, d_n$, respectively, then

$$B(v,\, w) = B(\sum_i c_i e_i, \sum_j d_j e_j) = \sum_{i,j} c_i d_j B(e_i,\, e_j) = \sum_{i,j} c_i a_{ij} d_j = \sum_i c_i (\sum_j a_{ij} d_j)$$

which is the unique entry of the 1×1 matrix $v^{\mathrm{tr}}\, Aw$.

To see the effect of change of basis, let C be an $n \times n$ matrix whose columns $w_1, \ldots, w_n$ are a possibly new basis for $V = K^n$. Then $w_i^{\mathrm{tr}}\, Aw_j$ is the i, j entry of the matrix $C^{\mathrm{tr}}\, AC$ (which is called *congruent* or *cogredient* to A). The invertibility of A is unaffected by the choice of basis. If A is invertible, the bilinear form is called *non-degenerate*.

Let B be a bilinear form and fix a basis $v_1, \ldots, v_n$ for V. Let V^* be the dual vector space. Then B gives a linear map $L : V \to V^*$ by the rule $L(v)(w) = B(v,\, w)$. fix a basis $v_1, \ldots, v_n$ for V. There is a *dual basis* for the dual vector space V^* of V, whose i th element f_i is the linear functional whose value on v_i is 1 and whose value on v_j is 0 for $j \neq i$. Since the value of $L(v_i)$ on $w = \sum_j c_j v_j$ is

$$B(v_i, \sum_j c_j v_j) = \sum_j c_j B(v_i, v_j) = \sum_j B(v_i, v_j) f_j(w),$$

we have that $L(v_i) = \sum_j B(v_i, v_j) f_j$. Thus, the matrix of B with respect to $c_1, \ldots, c_n$ is the same as the matrix of L with respect to the two bases $v_1, \ldots, v_n$ and $f_1, \ldots, f_n$. Hence, the matrix of B is invertible if and only if $L : V \to V^*$ is an isomorphism. This shows that B is non-degenerate if and only if L is one-to-one, which means that B is non-degenerate if and only if for all $v \in V - \{0\}$ there exists $w \in V$ such that $L(v,\, w) \neq 0$.

B is called *symmetric* if $B(v,\, w) = B(w,\, v)$ for all $v,\, w \in V$, and this holds if and only if its matrix A is symmetric.

We next give some further discussion of the notion of trace, and prove the trace characterization of separability discussed earlier.

Let R be any ring and $F \cong R^n$ a free R-module. Consider any R-linear endomorphism $T : F \to F$. We define the *trace* of T as follows: choose a free basis for F, let $M = (r_{ij})$ be a matrix for T, and let $\mathrm{Tr}(T)$ be the sum $\sum_{i=1}^n r_{ii}$ of the entries on the main diagonal of M. This is independent of the choice of free basis for F: if one has another free basis, the new matrix has the form AMA^{-1} for some invertible $n \times n$ matrix A over R, and the trace is unaffected.

If $S \neq 0$ is a free R-algebra that has finite rank as an R-module, so that $S \cong R^n$ as an R-module for some positive integer n, then for every element $s \in S$ we define $\mathrm{Tr}_{S/R} s$ to be the trace of the R-linear endomorphism of S given by multiplication by s. Then $\mathrm{Tr}_{S/R} : S \to R$ is an R-linear map. If $r \in R$, $\mathrm{Tr}_{S/R}(r) = nr$, since the matrix of multiplication by r is r times the $n \times n$ identity matrix. We are mainly interested in the case where R and S are both fields. We first note:

Lemma. *If T is a free S-algebra of finite rank $m \geq 1$ and S is free R-algebra of finite rank $n \geq 1$, then $\mathrm{Tr}_{T/R}$ is the composition $\mathrm{Tr}_{S/R} \circ \mathrm{Tr}_{T/S}$.*

Proof. Let $u_1, \ldots, u_n$ be a free basis for S over R, and let $v_1, \ldots, v_m$ be a free basis for $\frac{T}{S}$. Let $A = (s_{ij})$ be the $m \times m$ matrix over S for multiplication by $t \in T$ with respect to the free basis $v_1, \ldots, v_m$ over S. Let B_{ij} be the $n \times n$ matrix over R for multiplication by s_{ij} acting on S with respect to the basis $u_1, \ldots, u_n$ for S over R. Then

$$t(u_h v_k) = u_h(t v_k) = u_h(\sum_j s_{jk} v_k) = \sum_j (s_{jk} u_h) v_k$$

and $s_{jk} u_h$ is the dot product of the h column of B_{ij} with the column whose entries are $u_1, \ldots, u_n$. It follows that a matrix for multiplication by t acting on T over R with respect to the basis $u_h v_k$ is obtained, in block form, from (s_{ij}) by replacing the i, j entry by the block B_{ij}. Then $\mathrm{Tr}_{T/R}(t)$ is the sum of the diagonal entries of this matrix, which is sum over i of the sums of the diagonals of the matrices B_{ii}. Now, $Tr_{T/S}(t)$ is the sum of the s_{ii}, and when we apply $Tr_{S/R}$ be get the sum over i of the elements $\tau_i = Tr_{S/R}(s_{ii}$. But τ_i is the same as the sum of diagonal elements in B_{ii}, and the result follows. $\square$

Theorem. *Let cL be a finite algebraic extension field of $\mathcal{K}$. Then the extension is separable if and only if there is a (nonzero) element $\lambda \in \mathcal{L}$ such that $\mathrm{Tr}_{\mathcal{L}/\mathcal{K}}(\lambda) \neq 0$.*

Proof. We have already observed that the trace of 1 is $n = [\mathcal{L} : \mathcal{K}]$ which will be nonzero if $\mathcal{K}$ has characteristic 0, and every finite algebraic extension is separable in characteristic 0. Now suppose that $\mathcal{K}$ (and, hence, $\mathcal{L}$) have positive prime characteristic p.

If the extension if not separable, let $\mathcal{F}$ be the largest separable extension of $\mathcal{K}$ within $\mathcal{L}$. Since we must have an element $\theta \in \mathcal{L}$ such that $\theta^p \in \mathcal{F}$ but $\theta \notin \mathcal{F}$. Let $\mathcal{G}$ be the field $\mathcal{F}[\theta]$. Since

$$\mathrm{Tr}_{\mathcal{L}/\mathcal{K}} = \mathrm{Tr}_{\mathcal{F}/\mathcal{K}} \circ \mathrm{Tr}_{\mathcal{G}/\mathcal{F}} \circ \mathrm{Tr}_{\mathcal{L}/\mathcal{G}}$$

it will suffice to show that $\mathrm{Tr}_{\mathcal{G}/\mathcal{F}}$ vanishes identically. We have therefore reduced to the case where $\mathcal{L}$ is purely inseparable over $\mathcal{K}$, generated by a single element θ such that $\theta^p \in cK$. For an element $c \in \mathcal{K}$, $\mathrm{Tr}_{\mathcal{L}/\mathcal{K}}(c) = pc = 0$. For an element $\lambda \in \mathcal{L} - \mathcal{K}$, we have that $\lambda^p = c \in \mathcal{K}$. Since $[\mathcal{L} : \mathcal{K}] = p$ is prime, there are no strictly intermediate fields, and so $\mathcal{K}[\lambda] = \mathcal{L}$, and λ has degree p over $\mathcal{K}$. It follows that the minimal polynomial of λ over $\mathcal{K}$ is $x^p - c$, and that the elements λ^t, $0 \leq t \leq p-1$, are a basis for $\mathcal{L}$ over $\mathcal{K}$. Multiplication by λ. maps each basis vector to the next, except for λ^{p-1}, which is mapped to $c \cdot 1$. The matrix for multiplication by λ therefore has only zero entries on the main diagonal, and so $Tr_{\mathcal{L}/\mathcal{K}}(\lambda) = 0$, as required. (The matrix has a string of entries equal to one just below the main diagonal, and the element c occurs in the upper right hand corner. All other entries are 0.)

It remains to show that if $\mathcal{L}/\mathcal{K}$ is separable, then some element has trace different from 0. By the theorem on the primitive element, we may assume that $\mathcal{L} = \mathcal{K}[\theta]$. (Even without knowing this theorem, we can think of $\mathcal{L}$ as obtained from $\mathcal{K}$ by a finite sequence of field extensions, each of which consists of adjoining just one element, and so reduce to the case where one has a primitive element.) Let f be the minimal polynomial of θ: the hypothesis of separability implies that the roots of f are n distinct elements of the algebraic closure $\overline{\mathcal{L}}$ of $\mathcal{L}$: call them $\theta_1, \ldots, \theta_n$. Let A be the matrix for multiplication by θ with respect to some basis for $\mathcal{L}$ over $\mathcal{K}$. Then for every t, A^t gives a matrix for multiplication by θ^t. We shall show that for some i, $0 \leq i \leq n-1$, $\mathrm{Tr}_{cL/\mathcal{K}}(\theta^i) \neq 0$. Assume otherwise.

Since A satisfies its characteristic polynomial, call it g, which is monic of degree n, θ satisfies g. Thus, $f \mid g$. Since f and g are monic of the same degree, $g = f$. Thus, the eigenvalues of A are distinct: they are the elements θ_j. Therefore, A is similar over $\overline{(}\mathcal{L})$ to diagonal matrix with the θ_j on the diagonal, and it follows that, for every i, A^i is similar to a diagonal matrix with the entries θ_j^i on the diagonal. Therefore,

$$\mathrm{Tr}_{\mathcal{L}/\mathcal{K}}(\theta^i) = \sum_{j=1}^{n} \theta_j^i = 0.$$

Thus, the sum of the columns of the matrix $\Theta = (\theta_j^{i-1})$ is 0, which implies that the determinant is 0. We conclude the proof by showing that the determinant cannot be zero. (This is the well-known Van der Monde determinant, and its value can be shown to be the product of the $\binom{n}{2}$ differences $\theta_j - \theta_i$ for $j > i$. It will not vanish because the θ_j are distinct. But we argue differently, without assuming this.) If the determinant is 0 there is an $\overline{\mathcal{L}}$-linear relation on the rows as well: suppose that $\gamma = (c_0 \;\; c_1 \;\; \ldots \;\; c_n)$ is a vector such that $\gamma\Theta = 0$, giving a relation on the rows. This simply says that for every j,

$$\sum_{i=0}^{n-1} c_i \theta_j^i = 0.$$

But if

$$h(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1},$$

this says that all of the θ_j are roots of $h(x)$, a polynomial of degree at most $n-1$. This is a contradiction unless all of the c_i are 0. $\square$

This completes our treatment of separability and trace.

A non-module-finite integral closure in a finite inseparable extension field

The result of Problem 4. from the fourth problem set for Math 614, Fall 2013 is as follows:

Let $K_1 \subset \cdots \subset K_n \subset \cdots$ be an infinite chain of proper field extensions. Let x be a power series indeterminate over all the K_n. Let $R = \bigcup_{n=1}^{\infty} K_n[[x]]$. Then R is a local (Noetherian) domain in which every nonzero proper ideal is generated by a power of x.

That is, R is a Noetherian discrete valuation domain.

Now let k be a perfect field of characteristic $p > 0$, e.g., either $\mathbb{Z}/pZ$ or any algebraically closed field of positive characteristic. Let $t_0, t_1, \ldots, t_n \ldots$ be an infinite sequence of indeterminates over k, let $K = k(t_k^p : k \in \mathbb{N})$, and for $n \in \mathbb{N}$, let $K_n = K_0(t_1, \ldots, t_n)$, $n \geq 0$. Let $L = \bigcup_{n=0}^{\infty} K_n = K(t_n : n \in \mathbb{N})$. Note that $L^p = K$. Construct the ring R as in Problem 4. using this sequence of fields (the numbering starts with 0 instead of 1, which is not an essential difference). Since R is a DVR, it is normal. Note that $K[[x]] \subseteq R \subseteq L[[x]]$ and that if $f \in L[[x]]$, then $f^p \in R$. In fact, $f^p \in K[[x^p]]$. Let $u = \sum_{i=0}^{\infty} t_i x^i$. Then $u^p \in R$ but $u \notin R$. Let $\mathcal{F}$ be the fraction field of R and let $\mathcal{L} = \mathcal{F}(u)$, a purely inseparable extension of R.

Let S be the integral closure of R in $\mathcal{L}$. We shall show that S is not module-finite over R. For $i \in \mathbb{N}$ let $u_i = \sum_{s=0}^{\infty} t_{s+i} x^s = t_i + t_{i+1}x + \cdots$. Note that $u_0 = u$. Let $g_i = \sum_{s=0}^{i-1} t_s x_s \in K_{i-1}[x] \subseteq K_{i-1}[[x]] \subseteq R$. Then $u_i = (u - g_i)/x^i$ is in $\mathcal{L}$, and $u_i^p \in R$, since $u_n \in L[[x]]$. Hence, u_n is a root of the monic polynomial $Z^p - u_n^p = 0$, which is in $R[Z]$. Thus, all of the u_n are in S. To complete the proof, it suffices to show that for every n, u_n is not in the R-span of $u_0, \ldots, u_{n-1}$. (If S were module-finite over R, it would satisfy ACC as an R-module.) To get a contradiction, we assume that we have $r_0, \ldots, r_{n-1} \in R$ such that $(*) \quad u_n = \sum_{i=0}^{n-1} r_i u_i$.

The finitely many $r_i = \sum_{j=0}^{\infty} c_{ij} x^j$ will all have coefficients $c_{ij} \in K_N$ for some sufficiently large choice of N. Choose such an N and choose any M such that $M + n > N$. Compare the coefficients of x^M on the two sides of $(*)$. On the left hand side the coefficient is t_{M+n}. On the right hand side the coefficient is $\sum_{i=0}^{n-1}(\sum_{j+s=M} c_{ij} t_{s+i})$, and the largest value of $s + i$ that occurs is $M + (n - 1)$. Hence, all of the terms in the coefficient of x^M on the right hand side of $(*)$ are in the field K_{M+n-1}, since this is true both for the c_{ij} and the t_{s+i} that occur. Since $t_{M+n} \notin K_{M+n-1}$, we have the desired contradiction, and so S is not module-finite over R. $\square$