Math 145. Integral closure

This handout aims to show the following important finiteness theorem for integral closures in the context of algebraic geometry.

Theorem 0.1. *Let A be a domain finitely generated over an infinite perfect field k. Let L be a finite extension of the fraction field K of A. Then the integral closure of A in L is a finite A-module. In particular, the integral closure of A in its own fraction field K is a finite A-module.*

The "infinite" condition on k is only there because we proved Noether normalization under this hypothesis. Also, the result is true for arbitrary k, not necessarily perfect. However, if k has characteristic $p > 0$ and k is of infinite degree over the subfield k^p of pth powers (e.g., $k = \mathbf{F}_p(X_1, \ldots,)$ with infinitely many indeterminates) then one needs more sophisticated tools than we have. We only need the case when k is algebraically closed, and the proof works if you make this assumption throughout.

The plan of the proof is to embed the integral closure inside a finite A-module, so by the *noetherian* property of A, the module-finiteness of the integral closure follows. One can ask if the conclusion of the theorem is valid for any noetherian domain A, even with just $L = K$ (i.e., is the integral closure of A in its own fraction field module-finite over A?). This is false in general, but deep work of Nagata, Zariski, and Grothendieck shows that nearly all noetherian domains that arise "in nature" have this finiteness property.

Proof. By Noether normalization (!), there is a finite injection $k[T_1, \ldots, T_d] \hookrightarrow A$. The integral closure of A in any finite extension L/K is the integral closure of $k[T_1, \ldots, T_d]$ in the finite extension $L/k(T_1, \ldots, T_d)$. Thus, we may rename $k[T_1, \ldots, T_d]$ as A and so can assume that A is a polynomial ring in d variables over k. If L'/L is any finite extension, then the integral closure of A in L is contained in the integral closure of A in L'. Since A is *noetherian*, to prove the theorem for a given L/K we may therefore replace L by any finite extension L' and prove the result for L'/K.

Let's first take care of the case where L/K is a separable extension (which is automatic for characteristic 0). This step does not use that k is perfect and all we use about A is that it is an integrally closed noetherian domain. We will have to use a trick exploiting perfectness of k and the nature of polynomial rings to reduce the general case to this separable case. For separable L/K of degree n, we may replace L by a finite extension to reduce to the case where L/K is *Galois*. Now pick a primitive element e so that $L = K(e)$ is the splitting field of the minimal (separable) polynomial f of e over K. Multiplying e by a suitable non-zero element of A to kill denominators in its minimal polynomial over K, we may choose e to be integral over A, so e lies in the integral closure $\widetilde{A}$ of A in L. We will find a non-zero $D \in K^\times$ so that

$$D \cdot \widetilde{A} \subseteq \sum_{i=0}^{n-1} Ae^i.$$

This implies $\widetilde{A} \subseteq \sum A \cdot (e^i/D)$, whence module finiteness of $\widetilde{A}$ follows by the noetherian property of A.

Choose any

$$x = \sum_{j=0}^{n-1} c_j e^j \in \widetilde{A},$$

with $c_j \in K$. For each $\sigma \in \Gamma = \mathrm{Gal}(L/K)$ we have $\sigma(x) = \sum c_j \sigma(e)^j$. Thus, we get the matrix equation

$$(\sigma(x))_\sigma = (\sigma(e)^j) \cdot (c)_j,$$

where $(c)_j$ denotes the vertical vector of c_j's, the left side is the vertical vector of $\sigma(x)$'s labelled by the $\sigma \in \Gamma$, and the matrix has entries labelled by Γ for the rows and j's for the columns. Of course, to make this matrix equation we have to choose an ordering on the set Γ. Since $e \in \widetilde{A}$, certainly all $\sigma(e) \in \widetilde{A}$, so $\sigma(e)^j \in \widetilde{A}$ for all j. Multiplying through our matrix equation by the adjoint matrix of $(\sigma(e)^j)$,

$$(\sigma(e)^j)^{\mathrm{adj}}(\sigma(x))_\sigma = \Delta \cdot (c)_j,$$

where the enormous adjoint matrix on the left has all entries as universal polynomials in the $\sigma(e)^j$'s with $\mathbf{Z}$ coefficients, and so all its entries lie in $\widetilde{A}$, while $\Delta = \det(\sigma(e)^j) \in \widetilde{A}$. Multiplying through by Δ on both

sides, we see that for each j,

$$\Delta^2 c_j \in \widetilde{A}.$$

But Δ is a vanderMonde determinant, so we can explicitly compute $\Delta = \prod(\sigma(e)-\tau(e))$ where the product is taken over pairs of distinct elements $\sigma, \tau \in \Gamma$ with $\sigma < \tau$ relative to the ordering of Γ chosen in the matrix equations above. Thus, $\Delta^2 = \prod(\sigma(e) - \tau(e))$ where the product is taken over all ordered pairs (σ, τ) of *distinct* elements in Γ, irrespective of any non-canonical ordering. Writing $\tau = \sigma(\sigma^{-1}\tau)$ with $\sigma^{-1}\tau \neq 1$, we can therefore write

$$\Delta^2 = \prod_{\sigma\in\Gamma} \sigma\left(\prod_{\tau\neq 1}(e-\tau(e))\right),$$

where the inner product is nothing other than $f'(e)$, where $f \in K[T]$ is the minimal (separable) polynomial of f over K. Thus,

$$\Delta^2 = \prod_{\sigma\in\Gamma} \sigma(f'(e)).$$

But f is an irreducible separable polynomial over K with root e, so $D \stackrel{\text{def}}{=} \Delta^2 \neq 0$. Also, since D is visibly invariant under the action of Γ, it follows from the fundamental theorem of Galois theory that $D \in K$.

As we noted earlier, $Dc_j = \Delta^2 c_j \in \widetilde{A}$ for all j. But $D, c_j \in K$, so $Dc_j \in \widetilde{A} \cap K = A$ since A is *integrally closed*. We finally conclude that for our arbitrarily chosen $x = \sum c_j e^j \in \widetilde{A}$, we have $Dx = \sum (Dc_j)e_j \in \sum Ae^j$. Thus, $D \cdot \widetilde{A} \subseteq \sum Ae^j$, as desired. This settles the case where L/K is separable.

Now suppose L/K is not separable, or more generally that we are in characteristic $p > 0$. In order to reduce back to the separable case, we need to introduce some auxiliary fields as follows. Let $\overline{K}$ be an algebraic closure of K containing L (at the expense of introducing some awkwardness, we could get by without the use of this algebraic closure below). Define the rising chain of subfields $K_r = k(T_1^{1/p^r}, \ldots, T_d^{1/p^r})$ inside of $\overline{K}$, for $r \geq 0$. Note that there is no ambiguity about the meaining of pth-power roots, as we are in characteristic $p > 0$. Also, since $k = k^p$ (as k is perfect!), we see easily that the subfield K_r^p of pth powers in K_r is exactly K_{r-1} for $r > 1$ and is K when $r = 1$. In fact, the pth power maps define surjective maps, hence *isomorphisms*, of fields $K_r \simeq K_{r-1}$ for $r > 0$; beware these are not maps over k (but rather, over the pth power map on k). These isomorphisms take $k[T_1^{1/p^r}, \ldots, T_d^{1/p^r}]$ onto $k[T_1, \ldots, T_d]$, with $T_j^{1/p^r} \mapsto T_j$. Thus, we may view K_r as the fraction field of a polynomial ring over k in indeterminates denoted T_j^{1/p^r}. In particular, the subalgebra $k[T_1^{1/p^r}, \ldots, T_d^{1/p^r}]$ of K_r is a UFD finite over $k[T_1, \ldots, T_d]$ and hence is the integral closure of $k[T_1, \ldots, T_d]$ in K_r. That is, K_r is a *finite* extension of K in which the integral closure is an explicitly computed $k[T_1, \ldots, T_d]$-module which is itself a polynomial ring over k in d variables T_j^{1/p^r} (and so is a finite $k[T_1, \ldots, T_d]$-module, as each T_j^{1/p^r} satisfies a monic relation $X^{p^r} - T_j$ over this ring).

Let $K_\infty \subseteq \overline{K}$ be the union of the K_r's. As this is a rising union of subfields K_r, K_∞ is a subfield. By construction, any element of K_∞ lies in some K_r and hence has a pth root in $K_{r+1} \subseteq K_\infty$. That is, every element in K_∞ has a pth root in K_∞. We conclude that K_∞ is a *perfect* field. Thus, the *finite* composite extension LK_∞ of K_∞ inside of $\overline{K}$ is a separable extension, so it has a primitive element b with a minimal polynomial $g \in K_\infty[T]$ which is *separable*. Since g has only finitely many coefficients, for a sufficiently large r we have $g \in K_r[T]$, and in here g is separable and irreducible, as this is true when viewed over the algebraic extension K_∞. If L/K has generators $a_1, \ldots, a_m$, then each $a_j \in LK_\infty = K_\infty(b) = K_\infty[b]$ can be expressed as a polynomial in b with coefficients in K_∞. Only finitely many such coefficients arise, so by choosing r sufficiently large we can suppose that $a_j \in K_r[b]$ for all j. That is, $L \subseteq K_r[b] = K_r(b)$.

Now we may replace L with the *finite* extension $K_r(b)$, which is itself finite separable over K_r (as b has minimal polynomial g over K_r which is separable). Recalling that the integral closure R of $k[T_1, \ldots, T_d]$ in K_r is a polynomial ring over k in d variables, and is finite over $k[T_1, \ldots, T_d]$, we see that the integral closure of $k[T_1, \ldots, T_d]$ in L is equal to the integral closure of R in L. It suffices to show that this is a finite R-module, as it is then clearly a finite $k[T_1, \ldots, T_d]$-module (since composites of finite ring maps are finite). But the situation L/K_r with polynomial ring R in K_r is *exactly* the separable case we treated above! ■