Integral Closure of Ideals

We discuss the notion of integral closure of ideals, and prove some basic facts about its behavior. It turns out that in the case of a Noetherian ring R, and ideal I and an element $r \in R$, the following conditions are equivalent:

(1) There is an element c not in any minimal prime of R such that $cr^n \in I^n$ for all $n \gg 0$ (equivalently, for infinitely many values of n).

(2) There is an element c not in any minimal prime of R such that $cr^n \in I^n$ for infinitely many values of n.

(3) For every map of R into a Noetherian discrete valuation domain V, the image of r is IV.

(4) For every minimal prime $\mathfrak{p}$ of R and map Noetherian discrete valuation domain between $R/\mathfrak{p}$ and its fraction field, the image of r is in IV.

(5) rt is integral over the Rees ring $R[It] \subseteq R[t]$ (the latter is the polynomial ring in one variable t over$R$.

(6) For some positive integer n, the element r satisfies a polynomial equation of the form
$$r^n + i_1 r^{n-1} + \cdots i_j r^{n-j} + \cdots + i_{n-1} r + i_n = 0$$
where the coefficient $i_j \in I^j$.

These facts will be established below: see the Theorem on p. 13.

Our first objective is to review some facts about integral elements and integral ring extensions.

Recall that if $R \subseteq S$ are rings then $s \in S$ is *integral* over R if, equivalently, either

(1) s satsifies a monic polynomial with coefficients in R or

(2) $R[s]$ is finitely generated as an R-module.

The elements of S integral over R form a subring of S containing R, which is called the *integral closure* of R in S. If S is an R-algebra, S is called *integral* over R if every element is integral over the image of R in S. S is called *module-finite* over R if it is finitely generated as an R-module. If S is module-finite over R it is integral over R. S is module-finite over R if and only if it is finitely generated as an R-algebra and integral over R. S is integral over R if and only if every finitely generated R-subalgebra is module-finite over R.

Given a commutative diagram of algebras

$$\begin{array}{ccc} S & \xrightarrow{\ f\ } & U \\ \uparrow & & \uparrow \\ R & \longrightarrow & T \end{array}$$

and an element $s \in S$ integral over the image of R, the image of S in U is integral over the image of T. One can see this simply by applying the homomorphism f to the monic equation s satisfies. When the vertical maps are inclusions, we see that the integral closure of R in S maps into the integral closure of T in U.

Note also that if $R \to S$ and $S \to T$ are both module-finite (respectively, integral) then $R \to T$ is also module-finite (respectively, integral).

The total quotient ring of the ring R is $W^{-1}R$, where W is the multiplicative system of all nonzerodivisors. We have an injection $R \hookrightarrow W^{-1}R$. If R is a domain, its total quotient ring is its field of fractions. If R is reduced, R is called *normal* or *integrally closed* if it is integrally closed in its total quotient ring. Thus, a domain R is integrally closed if and only if every fraction that is integral over R is in R.

Let $(H, +)$ be an additive commutative semigroup with additive identity 0. A commutative ring R is said to be *H-graded* if it has a direct sum decomposition

$$R \cong \bigoplus_{h \in H} R_h$$

as abelian groups such that $1 \in R_0$ and for all $h, k \in H$, $R_h R_k \subseteq R_{h+k}$. Elements of R_h are then called *homogeneous elements* or *forms* of *degree* h. If s is the sum of nonzero forms $s_1 + \cdots + s_n$ of mutually distinct degrees h_i, then $s_i \in R_{h_i}$ is called the *homogenous component* of s of degree h_i. The homogeneous components in other degrees are defined to be 0. The most frequent choices for H are the nonnegative integers $\mathbb{N}$ and the integers $\mathbb{Z}$.

Theorem. *Let $R \subseteq S$ be an inclusion of $\mathbb{N}$-graded (or $\mathbb{Z}$-graded) rings compatible with the gradings, i.e., such that $R_h \subseteq S_h$ for all h. Then the integral closure of R in S is also compatibly graded, i.e., every homogeneous component of an element of S integral over R is integral over R.*

Proof. First suppose that R has infinitely many units of degree 0 such that the difference of any two is a unit. Each unit u induces an endomorphism θ_u of R whose action on forms of degree d is multiplication by u^d. Then $\theta_u \theta_v = \theta_{uv}$, and θ_u is an automorphism whose inverse is $\theta_{u^{-1}}$. These automorphisms are defined compatibly on both R and S: one has a commutative diagrams

$$\begin{array}{ccc} S & \xrightarrow{\theta_u} & S \\ \uparrow & & \uparrow \\ R & \xrightarrow[\theta_u]{} & S \end{array}$$

for every choice of unit u. If $s \in S$ is integral over R, one may apply θ_u to the equation of integral dependence to obtain an equation of integral dependence for $\theta_u(s)$ over R. Thus, θ_u stabilizes the integral closure T of R in S. (This is likewise true for $\theta_{u^{-1}}$, from which one deduces that θ_u is an automorphism of T, but we do not really need this.)

Suppose we write

$$s = s_{h+1} + \cdots + s_{h+n}$$

for the decomposition into homogeneous components of an element $s \in S$ that is integral over R, where each s_j has degree j. What we need to show is that each s_j is integral over R. Choose units $u_1, \ldots, u_n$ such that for all $h \neq k$, $u_h - u_k$ is a unit — we are assuming that these exist. Letting the θ_{u_i} act, we obtain n equations

$$u_i^{h+1} s_{h+1} + \cdots + u_i^{h+n} s_{h+n} = t_i, \quad 1 \leq j \leq n,$$

where $t_i \in T$. Let M be the $n \times n$ matrix $\left(u_i^{h+j}\right)$. Let V be the $n \times 1$ column vector $\begin{pmatrix} s_{h+1} \\ \vdots \\ s_{h+n} \end{pmatrix}$ and let W be the $n \times 1$ column vector $\begin{pmatrix} t_1 \\ \vdots \\ t_n \end{pmatrix}$. In matrix form, the displayed equations are equivalent to $MV = W$. To complete this part of the argument, it will suffice to show that the matrix M is invertible over R, for then $V = M^{-1}W$ will have entries in T, as required. We can factor u_i^{h+1} from the i th row for every i: since all the u_i are units, this does not affect invertibility and produces the Van der Monde matrix $\left(u_i^{j-1}\right)$. The determinant of this matrix is the product

$$\prod_{j>i} (u_j - u_i)$$

(see the Discussion below), which is invertible because every $u_j - u_i$ is a unit.

In the general case, suppose that

$$s = s_{h+1} + \cdots + s_{h+n}$$

as above is integral over R. Let t be an indeterminate over R and S. We can give this indeterminate degree 0, so that $R[t] = R_0[t] \otimes_{R_0} R$ is again a graded ring, now with 0 th graded piece $R_0[t]$, and similarly $S[t]$ is compatibly graded with 0 th graded piece $S_0[t]$. Let $U \subseteq R_0[t]$ be the multiplicative system consisting of products of powers of t and differences $t^j - t^i$, where $j > i \geq 0$. Note that U consists entirely of monic polynomials. Since all elements of U have degree 0, we have an inclusion of graded rings $U^{-1}R[t] \subseteq U^{-1}S[t]$. In $U^{-1}R[t]$, the powers of t constitute infinitely many units of degree 0, and the difference of any two distinct powers is a unit. We may therefore conclude that every s_j is integral over $U^{-1}R[t]$, by the case already done. We need to show s_j is integral over R itself.

Consider an equation of integral dependence

$$s_j^d + f_1 s_j^{d-1} + \cdots + f_d = 0,$$

where every $f_i \in U^{-1}R[t]$. Then we can pick an element $G \in U$ that clears denominators, so that every $Gf_i = F_i \in R[t]$, and we get an equation

$$Gs_j^d + F_1 s_j^{d-1} + \cdots + F_d = 0.$$

Let G have degree m, and recall that G is monic in t. The coefficient of t^m on the left hand side, which is an element of S, must be 0, and so its degree jd homogeneous component must be 0. The contribution to the degree jd component of this coefficient from Gs_j^d is, evidently, s_j^d, while the contribution from $F_i s_j^{d-i}$ clearly has the form $r_i s_j^{d-i}$, where $r_i \in R$ has degree ji. This yields the equation

$$s_j^d + r_1 s_j^{d-1} + \cdots + r_d = 0,$$

and so s_j is integral over R, as required. □

Discussion: Van der Monde matrices. Let $u_1, \ldots, u_n$ be elements of a commutative ring. Let M be the $n \times n$ matrix $\big(u_i^{j-1}\big)$.

(a) We want to show that the determinant of M is $\prod_{j>i}(u_j - u_i)$. Hence, M is invertible if $u_j - u_i$ is a unit for $j > i$. It suffices to prove the first statement when the u_i are indeterminates over $\mathbb{Z}$. Call the determinant D. If we set $u_j = u_i$, then D vanishes because two rows become equal. Thus, $u_j - u_i$ divides D in $\mathbb{Z}[u_1, \ldots, u_n]$. Since the polynomial ring is a UFD and these are relatively prime in pairs, the product P of the $u_j - u_i$ divides D. But they both have degree $1 + 2 + \cdots + n - 1$. Hence, $D = aP$ for some integer a. The monomial $x_2 x_3^2 \cdots x_n^{n-1}$ obtained from the main diagonal of matrix in taking the determinant occurs with coefficient 1 in both P and D, so that $a = 1$. □

(b) We can also show the invertibility of M as follows: if the determinant is not a unit, it is contained in a maximal ideal. We can kill the maximal ideal. We may therefore assume that the ring is a field K, and the u_i are mutually distinct elements of this field. If the matrix is not invertible, there a nontrivial relation on the columns with coefficients $c_0, \ldots, c_{n-1}$ in the field. This implies that the nonzero polynomial

$$c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$$

has n distinct roots, $u_1, \ldots, u_n$, in the field K, a contradiction. □

Corollary. *If a R is integrally closed in S, then $R[t]$ is integrally closed in $S[t]$. If R is a normal domain, then $R[t]$ is normal.*

Proof. The integral closure of $R[t]$ in $S[t]$ will be graded and so spanned by integral elements of $S[t]$ of the form st^k, where s is homogenous. Take an equation of integral dependence for st^k of degree, say, n on $R[t]$. The coefficient of t^{kn} is 0, and this gives an equation of integral dependence for s on R. For the second part, $R[t]$ is integrallly closed in $K[t]$, where $K = \mathrm{frac}\,(R)$, and $K[t]$ is integrally closed in $K(t) = \mathrm{frac}\,(R[t])$ since $K[t]$ is a UFD. □

We next want to discuss integral closure of ideals.

Let R be any ring and let I be an ideal of R. We define an element u of R to be *integral over* I or to be in the integral closure $\overline{I}$ of I if it satisfies a monic polynomial $f(z)$ of degree n with the property that the coefficient of z^{n-t} is in I^t, $1 \le t \le n$. We shall use the temporary terminology that such a monic polynomial is *I-special*. Note that the product of two I-special polynomials is I-special, and hence any power of an I-special polynomial is I-special.

Let t be an indeterminate over R and let $R[It]$ denote the subring of the polynomial ring $R[t]$ generated by the elements it for $i \in I$. This ring is called the *Rees ring* of I. It is $\mathbb{N}$-graded, with the grading inherited from $R[t]$, so that the k th graded piece is It^k.

It follows easily that the integral closure of $R[It]$ in $R[t]$ has the form

$$R + J_1t + J_2t^2 + \cdots + J_kt^k + \cdots$$

where, since this is an R-algebra, each J_k is an ideal of R. We note that with this notation, $J_1 = \overline{I}$. To see this, note that if rt, where $r \in R$ is integral over $R[It]$, satisfying an equation of degree n, then by taking homogeneous components of the various terms we may find an equation of integral dependence in which all terms are homogeneous of degree n. Dividing though by t^n then yields an equation of integral dependence for r on I. This argument is reversible. (Exercise: in this situation, show that J_k is the integral closure of I^k.) We note several basic facts about integral closures of ideals that follow easily either from the definition or this discussion.

Proposition. *Let I be an ideal of R and let $u \in R$.*

(a) *The integral closure of I in R is an ideal containing I, and the integral closure of $\overline{I}$ is $\overline{I}$.*

(b) *If $h : R \to S$ is a ring homomorphism and u is integral over I then $h(u)$ is integral over IS. If J is an integrally closed ideal of S then the contraction of J to R is integrally closed.*

(c) *u is integral over I if and only if its image modulo the ideal N of nilpotent elements is integral over $I(R/N)$. In particular, the integral closure of (0) is N.*

(d) *The element u is integral over I if and only if for every minimal prime P of R, the image of u modulo P is integral over $I(R/P)$.*

(e) *Every prime ideal of R and, more generally, every radical ideal of R is integrally closed.*

(f) *An intersection of integrally closed ideals is integrally closed.*

(g) *In a normal domain, a principal ideal is integrally closed.*

(h) *If S is an integral extension of R then $\overline{IS} \cap R = \overline{I}$.*

Proof. That $I \subseteq \overline{I}$ is obvious. If r is in the integral closure of $\overline{I}$ then rt is integral over $R[\overline{I}t]$. But this ring is generated over $R[It]$ by the elements r_1t such that $r_1 \in \overline{I}$, i.e., such that r_1t is integral over $R[It]$. It follows that $R[\overline{I}t]$ is integral over $R[It]$, and then rt is integral over $R[It]$ by the transitivity of integral dependence. This proves (a).

The first statement in (b) is immediate from the definition of integral dependence: apply the ring homomorphism to the equation of integral dependence. The second statement in (b) is essentially the contrapositive of the first statement.

The "only if" part of (c) follows from (b) applied with $S = R/N$. The "if" part follows from (d), and so it will suffice to prove (d).

The "only if" part of (d) likewise follows from (b). To prove the "if" part note that the values of I-special polynomials on u form a multiplicative system: hence, if none of them vanishes, we can choose a minimal prime P of R disjoint from this multiplicative system, and then no $I(R/P)$-special polynomial vanishes on the image of u in R/P.

(e) follows from the second statement in (c) coupled with the second statement in (b), while (f) is immediate from the definition. To prove (g), suppose that b is an element of R and $a \in \overline{bR}$. If $b = 0$ it follows that $a = 0$ and we are done. Otherwise, we may divide a degree n equation of integral dependence for a on bR by b^n to obtain an equation of integral dependence for a/b on R. Since R is normal, this equation shows that $a/b \in R$, and, hence, that $a \in bR$.

Finally, suppose that $r \in R$ is integral over IS. Then rt is integral over $S[ISt]$, and this ring is generated over $R[It]$ by the elements of S, each of which is integral over R. It follows that $S[ISt]$ is integral over $R[It]$, and so rt is integral over $R[It]$ by the transitivity of integral dependence. □

Recall that a domain V with a unique maximal ideal m is called a *valuation domain* if for any two elements one divides the other. This implies that for any finite set of elements, one of the elements divides the others, and so generates the same ideal that they all do together. We shall use the term *discrete valuation ring*, abbreviated DVR, for a Noetherian valuation domain: in such a ring, the maximal ideal is principal, and every nonzero element of the maximal ideal is a unit times a power of the generator of the maximal ideal. A DVR is the same thing as a local principal ideal domain (PID).

We recall the following terminology: (R,m,K) is *quasilocal* means that R has unique maximal ideal m and residue class field $K = R/m$. Sometimes K is omitted from the notation. We say that (R, m, K) is *local* if it is quasilocal and Noetherian.

The next result reviews some facts about integral closures of rings and integrally closed rings.

Theorem. *Let R be an integral domain.*

(a) *R is normal if and only if R is an intersection of valuation domains with the same fraction field as R. If R is Noetherian, these may be taken to be the discrete valuation rings obtained by localizing R at a height one prime.*

(b) *If R is one-dimensional and local, then R is integrally closed if and only if R is a DVR. Thus, a local ring of a normal Noetherian domain at a height one prime is a DVR.*

(c) *If R is Noetherian and normal, then principal ideals are unmixed, i.e., if $r \in R$ is not zero not a unit, then every associated prime of rR has height one.*

Proof. For (a) and (b) see [M.F. Atiyah and I.G. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley, Reading, Massachusetts, 1969], Corollary 5.22, Proposition 9.2

and Proposition 5.19, respectively, and [O. Zariski and P. Samuel, *Commutative Algebra*, D. Van Nostrand Company, Princeton, New Jersey, 1960], Corollary to Theorem 8, p. 17; for (c) see H. Matsumura, *Commutative Algebra*, W.A. Benjamin, New York, 1970], §17. □

For the convenience of the reader we shall give a proof of (a) below in the case where R is not necessarily Noetherian.

Examples of integral closure of ideals. Note that whenever $r \in R$ and $I \subseteq R$ is an ideal such that $r^n = i_n \in I^n$, we have that $r \in \overline{I}$. The point is that r is a root of $z^n - i_n = 0$, and this polynomial is monic with the required form.

In particular, if x, y are any elements of R, then $xy \in \overline{(x^2,\, y^2)}$, since $(xy)^2 = (x^2)(y^2) \in I^2$. This holds even when x and y are indeterminates.

More generally, if $x_1, \ldots, x_n \in R$ are any elements and $I = (x_1^n, \ldots, x_k^n)R$, then every monomial $r = x_1^{i_1} \cdots x_k^{i_k}$ of degree n (here the i_j are nonnegative integers whose sum is n) is in $\overline{I}$, since

$$r^n = (x_1^n)^{i_1} \cdots (x_k^n)^{i_k} \in I^n,$$

since every $x_j^n \in I$ and $\sum_{j=1}^k i_j = n$.

Now let K be any field of characteristic $\neq 3$, and let X, Y, Z be indeterminates over K. Let

$$R = K[X,\, Y,\, Z]/(X^3 + Y^3 + Z^3) = K[x,\, y,\, z],$$

which is a normal domain with an isolated singularity. Here, we are using lower case letters to denote the images of corresponding upper case letters after taking a quotient: we shall frequently do this without explanatory comment. Let $I = (x, y)R$. Then $z^3 \in I^3$, and so $z \in \overline{I}$. This shows that an ideal generated by a system of parameters in a local ring need not be integrally closed, even if the elements are part of a minimal set of generators of the maximal ideal. It also follows that $z^2 \in \overline{I^2}$, where I is a two generator ideal, while $z^2 \notin I$. Thus, the Briançon-Skoda theorem, as we stated it for regular rings, is not true for R. (There is a version of the theorem that *is* true: it asserts that for an n-generator ideal I, $\overline{I^n} \subseteq I^*$, where I^* is the *tight closure* of I. But we are not assuming familiarity with tight closure here.)

Here is another example. Let x, y, u, v be indeterminates over a field K and $R = K[x, y, u, v]$. Let $J = (x, y) \cap (u, v) = (x, y)(u, v) = (xu, yu, xv, yv)$. Then J is integral over $I = (xu, yv, xv + yu)$, since the generators of J not in I, namely xv, yu, are the roots of the equation $z^2 - (xv + yu)z + (xv)(yu) = 0$, where the second coefficient is in I and the third coefficient $= (xu)(yv) \in I^2$.

We next want to give a proof that, even when a normal domain R is not Noetherian, it is an intersection of valuation domains. We first show:

Lemma. *Let L be a field, $R \subseteq L$ a domain, and $I \subset R$ a proper ideal of R. Let $x \in L - \{0\}$. Then either $IR[x]$ is a proper ideal of $R[x]$ or $IR[1/x]$ is a proper ideal of $R[1/x]$.*

Proof. We may replace R by its localization at a maximal ideal containing I, which only makes the problem harder. If $IR[1/x]$ is not proper we obtain an equation

$$(\#) \quad 1 = j_0 + j_1(1/x) + \cdots j_m(1/x^m),$$

where all of $j_i \in I \subseteq m$. This yields

$$(\#\#) \quad (1 - j_0)x^m = j_1 x^{m-1} + \cdots j_m.$$

Since $1 - j_0$ is a unit, this shows that x is integral over R. Hence m lies under a maximal ideal of $R[x]$, and $mR[x]$ is proper. □

Corollary. *Let $R \subseteq L$, a field, and let $I \subset R$ be a proper ideal of R. Then there is a valuation domain V with $R \subseteq V \subseteq L$ such that $IV \neq V$.*

Proof. Consider the set $\mathcal{S}$ of all rings S such that $R \subseteq S \subseteq L$ and $IS \neq S$. This set contains R, and so is not empty. The union of a chain of rings in $\mathcal{S}$ is easily seen to be in $\mathcal{S}$. Hence, by Zorn's lemma, $\mathcal{S}$ has a maximal element V. We claim that V is a valuation domain with fraction field L. For let $x \in L - \{0\}$. By the preceding Lemma, either $IV[x]$ or $IV[1/x]$ is a proper ideal. Thus, either $V[x] \in \mathcal{S}$ or $V[1/x] \in \mathcal{S}$. By the maximality of V, either $x \in V$ or $1/x \in V$. □

We now can prove the result we were aiming for.

Corollary. *Let R be a normal domain with fraction field L. Then R is the intersection of all valuation domains V with $R \subseteq V \subseteq L$.*

Proof. Let $x \in L - R$. It suffices to find V with $R \subseteq V \subseteq L$ such that $x \notin V$. Let $y = 1/x$. We claim that y is not a unit in $R[y]$, for its inverse is x, and if y were a unit we would have

$$x = r_0 + r_1(1/x) + \cdots + r_n(1/x)^n$$

for some positive integer n and $r_j \in R$. Multiplying through by x^n gives an equation of integral dependence for x on R, and since R is normal this yields $x \in R$, a contradiction. Since $yR[y]$ is a proper ideal, by the preceding Corollary we can choose a valuation domain V with $R[y] \subseteq V \subseteq K$ such that yV is a proper ideal of V. But this implies that $x \notin V$. □

We note the following example of a non-Noetherian valuation domain. Let $R = K[x, y]$ be a polynomial ring in two variables over a field K, which has fraction field $L = K(x, y)$. Then we have a chain of polynomial rings $K[x, y] \subseteq K[x, y/x] \subseteq K[x, y/x^2] \subseteq \cdots \subseteq K[x, y/x^n] \subseteq L$. Let S be the union of the rings $R_n = K[x,\, y/x^n]$: since a directed union of normal domains is normal, S is normal. The ideal $m = (x)S + (y/x^n : n \geq 1)S$ is a maximal ideal, and there exists a valuation domain $(V, \mathcal{M})$ with $S \subseteq V \subseteq L$ such that mV is proper ideal, i.e., $m \subseteq \mathcal{M}$. Then V is not Noetherian, since x is in the maximal ideal and y is a nonzero element in the intersection of the ideals $x^n V$.

The following important result can be found in most introductory texts on commutative algebra, including [M.F. Atiyah and I.G. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley, Reading, Massachusetts, 1969], which we refer to briefly as Atiyah-Macdonald.

Theorem. *If R is a normal Noetherian domain, then the integral closure S of R in a finite separable extension $\mathcal{G}$ of its fraction field $\mathcal{F}$ is module-finite over R.*

Proof. See Proposition 5.19 of Atiyah-MacDonald for a detailed argument. We do mention the basic idea: choose elements $s_1, \ldots, s_d$ of S that are basis for $\mathcal{G}$ over $\mathcal{F}$, and then the discriminant $D = \det\bigl(\mathrm{Trace}_{\mathcal{G}/\mathcal{F}}\, s_i s_j\bigr)$, which is nonzero because of the separability hypothesis, multiplies S into the Noetherian R-module $\sum_{i=1}^{d} R s_i$. $\square$

Theorem (Nagata). *Let R be a complete local domain. Then the integral closure of R in a finite field extension of its fraction field is a finitely generated R-module.*

Proof. Because R is module-finite over a formal power series ring over a field, or, if R does not contain a field, over a DVR whose fraction field has characteristic zero, we may replace the original R by a formal power series ring, which is regular and, hence, normal. Unless R has characteristic p the extension is separable and we may apply the Theorem just above.

Thus, we may assume that R is a formal power series ring $K[[y_1, \ldots, y_n]]$ over a field K of characteristic p. If we prove the result for a larger finite field extension, we are done, because the original integral closure will be an R-submodule of a Noetherian R-module. This enables us to view the field extension as a purely inseparable extension followed by a separable extension. The separable part may be handled using the Theorem just above. It follows that we may assume that the field extension is contained in the fraction field of $K^{1/q}[[x_1, \ldots, x_n]]$ with $x_i = y_i^{1/q}$ for all i. We may adjoin the x_i to the given field extension, and it suffices to show that the integral closure is module-finite over $K[[x_1, \ldots, x_n]]$, since this ring is module-finite over $K[[y_1, \ldots, y_n]]$. Thus, we have reduced to the case where $R = K[[x_1, \ldots, x_n]]$ and the integral closure S will lie inside $K^{1/q}[[x_1, \ldots, x_n]]$, since this ring is regular and, hence, normal.

Now consider the set $\mathcal{L}$ of leading forms of the elements of S, viewed in the ring $K^{1/q}[[x_1, \ldots, x_n]]$. Let d be the degree of the field extension from the fraction field of R to that of S. We claim that any $d+1$ or more $F_1, \ldots, F_N$ of the leading forms in $\mathcal{L}$ are linearly dependent over (the fraction field of) R for, if not, choose elements s_j of S which have them as leading forms, and note that these will also be linearly independent over R, a contradiction (if a non-trivial R-linear combination of them were zero, say $\sum_j r_j s_j = 0$, where the r_j are in R, and if F_j has degree d_j while the leading form g_j of r_j has degree d'_j, then one also gets $\sum_j g_j F_j = 0$, where the sum is extended over those values of j for which $d_j + d'_j$ is minimum). Choose a maximal set of linearly independent elements f_j of $\mathcal{L}$. Let K' denote the extension of K generated by all of their coefficients. Since there are only finitely many, $T = K'[[x_1, \ldots, x_n]]$ is module-finite over R. But T contains every element L of $\mathcal{L}$, for each element of $\mathcal{L}$ is linearly dependent over R on the f_j, and so is in the fraction field of T, and has its q th power in $R \subseteq T$. Since T is regular, it is normal, and so must contain L.

Thus, the elements of $\mathcal{L}$ span a finitely generated R-submodule of T, and so we can choose a finite set $L_1, \ldots, L_k \subseteq \mathcal{L}$ that span an R-module containing all of $\mathcal{L}$,. We can then choose finitely many elements $s_1, \ldots, s_k$ of S whose leading forms are the $L_1, \ldots, L_k$.

Let S_0 be the module-finite extension of R generated by the elements $s_1, \dots, s_k$. We complete the proof by showing that $S_0 = S$. We first note that for every element L of $\mathcal{L}$, S_0 contains an element s whose leading form is L. To see this, observe that if we write L as an R-linear combination $\sum_j r_j L_j$, the same formula holds when every r_j is replaced by its homogeneous component of degree $\deg L - \deg L_j$. Thus, the r_j may be assumed to be homogeneous of the specified degrees. But then $\sum_j r_j s_j$ has L as its leading form.

Let $s \in S$ be given. Recursively choose $u_0, u_1, \dots, u_n, \dots \in S_0$ such that u_0 has the same leading form as s and, for all n, u_{n+1} has the same leading form a $s - (u_0 + \cdots + u_n)$. For all $n \geq 0$, let $v_n = u_0 + \cdots + u_n$. Then $\{v_n\}_n$ is a Cauchy sequence in S_0 that converges to s in the topology given by the powers m_T^h of the maximal ideal of $T = K'[[x_1, \dots, x_n]]$. Since S_0 is module-finite over $K[[x_1, \dots, x_n]]$, S_0 is complete. By Chevalley's lemma, which is discussed below, when we intersect the m_T^h with S_0 we obtain a sequence of ideals cofinal with the powers of the maximal ideal of S_0. Thus, the sequence, which converges to s, is Cauchy with respect to the powers of the maximal ideal of S_0. Since, as observed above, S_0 is complete, we have that $s \in S_0$, as required. □

In the proof of the preceding Theorem, we used Chevalley's Lemma:

Theorem. *Let M be a finitely generated module over a complete local ring (R, m, K). Let $\{M_n\}_n$ be a decreasing sequence of submodules whose intersection is 0. Then for all $k \in \mathbb{N}$ there exists N such that $M_n \subseteq m^k M$.*

Proof. For all h, the modules $M_n + m^h M$ are eventually stable (we may consider instead their images in the Artinian module $M/m^h M$, which has DCC), and so we may choose n_h such that $M_n + m^h M = M_{n'} + m^h M$ for all $n, n' \geq n_h$. We may replace n_h by any larger integer, and so we may assume that the sequence n_h is increasing. We replace the original sequence by the $\{M_{n_h}\}_h$. Thus we may assume without loss of generality that $M_n + m^h M = M_{n'} + m^h M$ for all $n, n' \geq h$. We claim $M_k \subseteq m^k M$ for all k: if not, choose k and $v_k \in M_k - m^k M$. Now choose $v_{k+1} \in M_{k+1}$ such that $v_{k+1} \equiv v_k \bmod m^k M$, and, recursively, for all $s \geq 0$ choose $v_{k+s} \in M_{k+s}$ such that $v_{k+s+1} \equiv v_{k+s} \bmod m^{k+s} M$: this is possible because $M_{k+s} \subseteq M_{k+s+1} + m^{k+s} M$. This gives a Cauchy sequence with nonzero limit. Since all terms are eventually in any given M_n, so is the limit (each M_n is m-adically closed), which is therefore in the intersection of the M_n. □

We have been assuming that valuation domains V are integrally closed. It is very easy to see this: if f is in the fraction field L of V but not in V, then $x = 1/f$ is in the maximal ideal m of V. Some maximal $\mathcal{M}$ of the integral closure V' lies over m, and so x is not a unit of V', i.e., $f \notin V'$. Thus, $V' = V$.

It is also easy to see that if $K \subseteq L$ are fields and V is a valuation domain with fraction field L, then $V \cap K$ is a valuation domain with fraction field K. Moreover, if V is a DVR, then $V \cap K$ is a DVR or is K. For the first statement, each $f \in K - \{0\}$ has the property that f or $1/f$ is in V, and, hence, in $V \cap K$, as required. Now suppose that V is a DVR and that x generates the maximal ideal. Let $W = V \cap K \neq K$. Each nonzero element of the maximal ideal m of W has the form ux^k in V, where k is a positive integer. Choose an element y of the maximal ideal of W such that k is minimum. Then every $z \in m$ is a multiple of y in V, and the multiplier is in W. Thus, m is principal. It follows that every nonzero element m has the form uy^t, where $t > 0$, since it is clear that the intersection of the powers of m is zero.

We next want to prove:

Theorem. *Let R be a Noetherian domain. Then the integral closure R' of R is the intersection of the discrete valuation rings between R and its fraction field L.*

Proof. Let $f = b/a$ be an element of L not in R', where $a, b \in R$ and $b \neq 0$. It suffices to find a DVR containing R and not b/a: we may then intersect it with L. Localize at a prime of R in the support of the R-module $(R' + Rf)/R'$. Since localization commutes with integral closure we may assume that (R, m, K) is local. Nonzero elements of R are nonzerodivisors in $\widehat{R}$ by flatness, and so the fraction field of R embeds in the total quotient ring of $\widehat{R}$, and we may view b/a as an element of the total quotient ring of $\widehat{R}$. If $b + \mathfrak{p}$ is in the integral closure of $a(R/\mathfrak{p})$ for every minimal prime $\mathfrak{p}$ of $\widehat{R}$, then b is integral over $a\widehat{R}$. If the equation that demonstrates the integral dependence has degree n, we find that $b^n \in (b^{n-1}a,\, b^{n-2}a^2,\, \dots,\, ba^{n-1},\, a^n)\widehat{R}$, and since $\widehat{R}$ is faithfully flat over R, this implies that $b^n \in (b^{n-1}a,\, b^{n-2}a^2,\, \dots,\, ba^{n-1},\, a^n)R$ as well. Dividing by a^n then shows that b/a is integral over R, a contradiction. Thus, we can choose a minimal prime $\mathfrak{p}$ of $\widehat{R}$ such that $b + \mathfrak{p}$ is not integral over $a\widehat{R}/\mathfrak{p}$. It follows that $\overline{b}/\overline{a}$ is not integral over $\widehat{R}/\mathfrak{p}$, where the bars over the letters indicate images in $\widehat{R}/\mathfrak{p}$. Note that R injects into $\widehat{R}/\mathfrak{p}$. Thus, the integral closure $(\widehat{R}/\mathfrak{p})'$ of $\widehat{R}/\mathfrak{p}$ does not contain $\overline{b}/\overline{a}$, and since it is module-finite over $\widehat{R}/\mathfrak{p}$ by the Theorem of Nagata on p. 9, it is a normal Noetherian ring. Thus, it is an intersection of DVR's by part (a) of the Theorem on p. 6, and we can choose a DVR V containing $(\widehat{R}/\mathfrak{p})'$ and not $\overline{b}/\overline{a}$, which is the image of b/a, so that V contains the isomorphic image of R but not the image of b/a. Now we may intersect V with the fraction field of R. □

Theorem. *Let R be any ring and let $I \subseteq J$ be ideals of R.*

(a) *$r \in R$ is integral over I if and only if there exists an integer n such that $(I + rR)^{n+1} = I(I + rR)^n$. Thus, if J is generated over I by one element, then J is integral over I if and only if there exists an integer $n \in \mathbb{N}$ such that $J^{n+1} = IJ^n$.*

(b) *If $J^{n+1} = IJ^n$ with $n \in N$ then $J^{n+k} = I^k J^n$ for all $k \in \mathbb{N}$.*

(c) *If $J^{n+1} = IJ^n$ and $Q \supseteq J$ is an ideal and $r \in \mathbb{N}$ an integers such that $Q^{r+1} = JQ^r$, then $Q^{n+r+1} = IQ^{n+r}$.*

(d) *If J is integral over I and generated over I by finitely many elements, then there is an integer $n \in \mathbb{N}$ such that $J^{n+1} = IJ^n$. If R is Noetherian then J is integral over I if and only if there exists an integer $n \in \mathbb{N}$ such that $J^{n+1} = IJ^n$.*

(e) *If R is a domain and M is a finitely generated faithful R-module such $JM = IM$ then J is integral over I. If R is a Noetherian domain, then J is integral over I if and only if there is a finitely generated faithful R-module M such that $JM = IM$.*

Proof. Note that

$$(I + rR)^n = I^n + rI^{n-1} + \cdots + r^t I^{n-t} + \cdots + r^n R.$$

Comparing the expansions for $(I + rR)^{n+1}$ and $I(I + rR)^n$, we see that the condition for equality is simply that r^{n+1} be in $I(I + rR)^n = r^n I + \cdots + I^{n+1}$, and this is precisely the condition for r to satisfy an equation of integral dependence on I of degree $n + 1$. This proves (a).

We prove (b) by induction on k. The result is clear if $k = 0$ and holds by hypothesis if $k = 1$. Assuming that $J^{n+k} = I^k J^n$, for $k \geq 1$ we have that

$$J^{n+k+1} = J^{n+k} J = (I^k J^n) J = I^k J^{n+1} = I^k I J^n = I^{k+1} J^n,$$

as required. This proves (b).

For (c), note that $Q^{r+n+1} = J^{n+1} Q^r = (IJ^n) Q^r = I(J^n Q^r) = IQ^{n+r}$.

It follows by induction on the number of elements needed to generate J over I that if J is finitely generated over I and integral over I then there is an integer n such that$J^{n+1} = IJ^n$.

Next, we want to show that if R is Noetherian and $J^{n+1} = IJ^n$ then J is integral over I. The condition continues to hold if we consider the images of I, J modulo a minimal prime of R, and so it suffices to consider the case where R is a domain. Moreover, if $I = (0)$ the result is immediate, and so we may assume that $I \neq 0$. Thus, J^n is a faithful R-module, and so the proof will be complete once we have established the first sentence of part (e).

Suppose that $JM = IM$ and let $u_1, \ldots, u_n$ be generators for M. Let r be an element of J. Then for every ν we can write $ru_\nu = \sum_{\mu=1}^n i_{\mu\nu} u_\mu$ where the $i_{\mu\nu} \in I$. Let $\mathbf{1}$ denote the size n identity matrix, and let B denote the size n matrix $(i_{\mu\nu})$. Let U be an $n \times 1$ column vector whose entries are the u_i. Then, in matrix notation, $rU = BU$, so that $(r\mathbf{1} - B)U = 0$. Let C be the transpose of the cofactor matrix of $r\mathbf{1} - B$. Then $C(r\mathbf{1} - B)$ is $D\mathbf{1}$, where $D = \det(r\mathbf{1} - B)$ is the characteristic polynomial of B evaluated at r. It is easy to see that the characteristic polynomial of a matrix with entries in I is I-special. Now, when we multiply the equation $(r\mathbf{1} - B)U = 0$ on the left by C we find that $D\mathbf{1}U = 0$, i.e., that $DU = 0$, and since D kills all the generators of M and M is faithful, it follows that $D = 0$, giving an equation of integral dependence for r on I. This proves the first sentence of part (e), and also completes the proof of (d).

Finally, if R is a Noetherian domain and J is integral over I, then if $I = (0)$ we have that $J = (0)$ and we may choose $M = R$, while if $I \neq (0)$ then $J \neq (0)$. In this case we can choose n such that $J^{n+1} = IJ^n$, and we may take $M = J^n$. □

The next Theorem gives several enlightening characterizations of integral closure. We first note:

Lemma. *Let I be an ideal of the ring R, $r \in \overline{I}$, and $h : R \to S$ a homomorphism to a normal domain S such that IS is principal. Then $h(r) \in IS$.*

Proof. By persistence of integral closure, $h(r) \in \overline{IS}$. But IS is a principal ideal of a normal domain, and so integrally closed, which implies that $r \in IS$. $\square$

Theorem. *Let R be a ring, let I be an ideal of R, and let $r \in R$.*

(a) *$r \in \overline{I}$ if and only if for every homomorphism from R to a valuation domain V, $r \in IV$.*

(b) *$r \in \overline{I}$ if and only if for every homomorphism f from R to a valuation domain V such that the kernel of f is a minimal prime P of R, $f(r) \in IV$. (Thus, if R is a domain, $r \in \overline{I}$ if and only if for every valuation domain V containing R, $r \in IV$.) Moreover, it suffices to consider valuation domains contained in the fraction field of R/P.*

(c) *If R is Noetherian, $r \in \overline{I}$ if and only if for every homomorphism from R to a DVR V, $r \in IV$.*

(d) *If R is Noetherian, $r \in \overline{I}$ if and only if for every homomorphism f from R to a DVR V such that the kernel of f is a minimal prime of R, $f(r) \in IV$. (Thus, if R is a domain, $r \in \overline{I}$ if and only if for every DVR V containing R, $r \in IV$.) Moreover, it suffices to consider valuation domains contained in the fraction field of R/P.*

(e) *If R is a domain and $I = (u_1, \ldots, u_n)R$ is a finitely generated ideal, let*

$$S_i = R[\frac{u_1}{u_i}, \ldots, \frac{u_n}{u_i}] \subseteq R_{u_i},$$

and let T_i be the integral closure of S_i. Then $r \in R$ is in $\overline{I}$ if and only if $r \in IT_i$ for all i.

(f) *Let R be a Noetherian domain. Then $r \in \overline{I}$ if and only if there is a nonzero element $c \in R$ such that $cr^n \in I^n$ for all $n \in \mathbb{N}$. (Note: I^0 is to be interpreted as R even if $I = (0)$.)*

(g) *Let R be a Noetherian domain. Then $r \in \overline{I}$ if and only if there is a nonzero element $c \in R$ such that $cr^n \in I^n$ for infinitely many values of $n \in \mathbb{N}$.*

Proof. We first observe that in any valuation domain, every ideal is integrally closed: every ideal is the directed union of the finitely generated ideals it contains, and a directed union of integrally closed ideals is integrally closed. In a valuation domain every finitely generated is principal, hence integrally closed, since a valuation domain is normal, and it follows that every ideal is integrally closed.

Now suppose that $r \in \overline{I}$. Then for any map of f of R to a valuation domain V, we have that $r \in \overline{IV} = IV$. This shows the "only if" part of (a). To complete the proof of both (a) and (b) it will suffice to show that if $f(r) \in IV$ whenever the kernel of f is a minimal prime, then $r \in \overline{I}$. But if $r \notin \overline{I}$ this remains true modulo some minimal prime by part (d) of the Proposition on p. 6, and so we may assume that R is a domain, and that rt is not integral over $R[It]$. But then, by the second Corollary on p. 8, we can find a valuation domain V containing $R[It]$ and not rt (in the Noetherian case V may be taken to be a DVR by the first Theorem on p. 11). Then $r \in \sum_{j=1}^{n} i_j v_j$ with the $i_j \in I$ and the $v_j \in V$ implies $rt = \sum_{j=1}^{n} (i_j t) v_j \in V$ (since each $i_j t \in It \subseteq V$), a contradiction. The fact that it suffices to consider only those V within the fraction field of R/P follows from the observation that one may replace V by its intersection with that field.

The proofs of (c) and (d) in the Noetherian case are precisely the same, making use of the parenthetical comment about the Noetherian case given in the paragraph above.

To prove (e) first note that the expansion of I to S_i is generated by u_i, since $u_j = \frac{u_j}{u_i} u_i$, and so $IT_i = u_i T_i$ as well. If $r \in \overline{I}$ then $r \in IT_i$ by the preceding Lemma. Now suppose instead that we assume that $r \in IT_i$ for every i instead. Consider any inclusion $R \subseteq V$, where V is a valuation domain. Then in V, the image of one of the u_j, say u_i, divides all the others, and so we can choose i such that $S_i \subseteq V$. Since V is normal, we then have $T_i \subseteq V$ as well, and then $r \in IT_i$ implies that $r \in IV$. Since this holds for all valuation domains containing R, $r \in \overline{I}$.

Finally, it will suffice to prove the "only if" part of (f) and the "if" part of (g). If $I = (0)$ we may choose $c = 1$, and so we assume that $I \neq 0$. Suppose that $J = I + Rr$ and choose $h \in \mathbb{N}$ so that $J^{h+1} = IJ^h$, so that $J^{n+h} = I^n J^h$ for all $n \in \mathbb{N}$: see parts (a) and (c) of the second Theorem on p. 11. Choose c to be a nonzero element of J^h. Then, for all n, $cr^n \in J^{n+h} = I^n J^h \subseteq I^n$, as required.

Now suppose that c is a nonzero element such that $cr^n \in I^n$ for arbitrarily large values of n. If $r \notin \overline{I}$ we can choose a discrete valuation v such that the value of v on r is smaller than the value of v on any element of I: then $v(r) + 1 \leq v(u)$ for all $u \in I$. Choose $n > v(c)$. Then $nv(r) + n \leq v(w)$ for all $w \in I^n$. But if we take $w = cr^n$ we have $v(w) = v(c) + nv(r) < nv(r) + n \leq v(w)$, a contradiction. $\square$

For those familiar with the theory of schemes, we note that the condition in part (e) can be described in scheme-theoretic terms. There is a scheme, the *blow-up* Y of $X = \operatorname{Spec} R$ along the closed subscheme defined by I, which has a finite open cover by open affines corresponding to the affine schemes $\operatorname{Spec} S_i$. The normalization Y' of Y, i.e., the *normalized blow-up*, has a finite open cover by the open affines $\operatorname{Spec} T_i$. I corresponds to a sheaf of ideals on X, which pulls back (locally, via expansion) to a sheaf of ideals $\mathcal{J}$ on Y'. The integral closure of I is then the ideal of global sections of $\mathcal{J}$ intersected with R.