INTEGRAL DEPENDENCE

ZHAN JIANG

Contents

1. Integral dependence

Definition 1.1. Let S be an R-algebra with structure homomorphism $f : R \to S$. An element $s \in S$ is **integral** over R if there is a monic polynomial $h(x) \in R[x]$ such that $h(s) = 0$.

If we assume that $h(x) = x^d + r_1 x^{d-1} + \cdots + r_d$, then $h(s) = 0$ implies that

$$s^d = -r_1 s^{d-1} - \cdots - r_d$$

So the submodule $f(R)[s]$ inside S is a finite module over R (more precisely, $f(R)$). We have following definitions:

Definition 1.2.
- S is **integral over** R if every element of S is integral over R.
- If $R \subseteq S$ and S is integral over R, then S is called an **integral extension** of R.
- S is **module-finite over** R is S finitely generated as an R-module.
- If $R \subseteq S$ and S is module-finite over R, then S is called a **module-finite extension** of R.

Next we discuss the relation between module-finite extensions and integral extensions, for that we need a technical lemma:

Lemma 1.3. *Let $A = (r_{ij})$ be an $n \times n$ matrix over R and let V be an $n \times 1$ column vector such that $AV = 0$, then* $\det(A)$ *kills every entry of V.*

Proof. $\det(A)V = \det(A)I_n V = \operatorname{adj}(A)AV = 0$ □

Theorem 1.4. *If S is module-finite over R, then S is integral over R.*

Proof. For any element $s \in S$, we want to show that s is integral over R. Let $s_1, ..., s_n$ be a set of generators of S as an R-module. Without loss of generality we can assume that $s_1 = 1$. For each s_i we have

$$ss_i = \sum_j r_{ij} s_j$$

Let $V = \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix}$ and $A = sI_n - (r_{ij})$, then we have $AV = 0$. By Lemma 1.3 we know that $\det(A)$ kills s_i. In particular, it kills $s_1 = 1$. So $\det(sI_n - B) = 0 \Rightarrow s$ is integral over R. □

Proposition 1.5. *Let $R \to S \to T$ be ring homomorphisms such that S is module-finite over R with generators $s_1, ..., s_m$ and T is module-finite over S with generators $t_1, ..., t_n$. Then the composition $R \to T$ is module-finite with generators $s_i t_j$ where $1 \leq i \leq m$ and $1 \leq j \leq n$.*

Proof. Every element $t \in T$ can be written as

$$t = \sum_{i=1}^{n} a_i t_i$$

where $a_i \in S$. Then each a_i could be written as

$$a_i = \sum_{j=1}^{m} r_{ij} s_j$$

where $r_{ij} \in R$. So

$$t = \sum_{i,j} r_{ij} s_j t_i$$

completes the proof. □

Corollary 1.6. *The elements of S integral over R form a subring of S*

Proof. Replace R by its image in S and assume that $R \subseteq S$. Let s_1, s_2 be two elements of S integral over R, then $R[s_1]$ is module-finite over R and $R[s_1, s_2]$ is module-finite over $R[s_1]$. So by Prop 1.5 we see that $R[s_1, s_2]$ is module-finite over R, hence $s_1 \pm s_2$ and $s_1 s_2$ are integral over R. □

Next theorem shows us the key relation between module-finiteness and integralness.

Theorem 1.7. *Let S be an R-algebra, then S is module-finite over R iff S is finitely generated as an R-algebra.*

Proof. The direction that "module-finite" ⇒ "integral" and "finitely generated" has been shown. For the converse, suppose that S is generated by $s_1, ..., s_n$, all of which are integral over R. Then we have a module-finite chain:

$$R \to R[s_1] \to R[s_1, s_2] \to \cdots \to R[s_1, ..., s_n] = S$$

Hence by Prop 1.5, S is module-finite over R. □

Corollary 1.8. *S is integral over R iff it is a directed union of module-finite extensions of R.*

Proof. "If" part is clear, for the "only if" part, notice that S is the directed union of its finitely generated R-subalgebras, each of which is module-finite extension of R. □

Let $f : R \to S$ be the structure map and suppose V is a multiplicative set in R. Let $W = f(V)$ be the image of V in S. Then we have a natural map $V^{-1}f : V^{-1}R \to W^{-1}S$.

Lemma 1.9. *With notations above,*

1. *If S is module-finite (resp. integral) over R, then $W^{-1}S$ is module-finite (resp.integral) over $V^{-1}R$.*
2. *If $R \subseteq S$ (then $W = V$) and T is the integral closure of R in S, then $V^{-1}R \subseteq V^{-1}T \subseteq V^{-1}S$ and $V^{-1}T$ is the integral closure of $V^{-1}R$ in $V^{-1}S$.*

Proof. (1) If S is integral over R, for any element $\frac{s}{w} \in W^{-1}S$, there is some polynomial in R such that

$$s^d + a_1 s^{d-1} + \cdots + a_d = 0$$

There is some v maps to w, hence the polynomial

$$x^d + \frac{a_1}{v} x^{d-1} + \cdots + \frac{a_d}{v^d}$$

is satisfied by $\frac{s}{w}$. So $W^{-1}S$ is integral over $V^{-1}R$.

If S is finitely generated as an R-module by $s_1, ..., s_m$. Then $\frac{s_1}{1}, ..., \frac{s_m}{1}$ generates $W^{-1}S$ over $V^{-1}R$ as well.

(2) The inclusion is trivial. By the result of (1), we see that $V^{-1}T$ is integral over $V^{-1}R$. For any element in $V^{-1}S$ that is integral over $V^{-1}R$, the denominator comes from V while the numerator is integral over R in S. So the numerator is in T therefore the element is in $V^{-1}T$. So $V^{-1}T$ continue to be the integral closure. □

2. Lying over and going up theorems

Definition 2.1. If $R \subseteq S$ are rings, a prime $Q \subseteq S$ is said to **lie over** $P \subseteq R$ if $Q \cap R = P$.

Lemma 2.2. *Let $R \subseteq S$ be domains and let $s \in S - \{0\}$ be integral over R, then s has a nonzero multiple in R.*

Proof. Look at the integral relation of s over R:

$$s^d + a_1 s^{d-1} + \cdots + a_d = 0$$

Since S is a domain, $a_d \neq 0$. So we have

$$s(s^{d-1} + a_1 s^{d-2} + \cdots + a_{d-1}) = -a_d$$

which shows that $-a_d$ is a nonzero multiple of s in R. □

Theorem 2.3. *Let S be an integral extension of R, $I \subseteq R$ an ideal and $u \in IS$. Then u satisfies a monic polynomial equation $u^n + i_1 u^{n-1} + \cdots + i_n = 0$ where $i_t \in I^t$ for $1 \leq t \leq n$.*

Proof. We have that $u = \sum_{t=1}^n s_t i_t$ with $s_t \in S$ and $i_t \in I$. We may replace S by the smaller ring generated by $s_1, ..., s_n$ and u. This ring is module-finite over R. So we may assume WLOG that S is module-finite over R. We may assume further that $s_1 = 1$.

Since $us_j \in IS$, we have

$$us_j = \sum_{t=1}^{n} i_{jt} s_t$$

Let V be the $n \times 1$ column matrix with entries $s_1, ..., s_n$ and let B be the $n \times n$ matrix (i_{jt}). Then the determinant of $\det(uI_n - B)$ kills every s_j, in particular, it kills $s_1 = 1$. So it's zero, which has the form

$$u^n + i_1 u^{n-1} + \cdots + i_n$$

where $i_t \in I^t$. □

Theorem 2.4 (Lying Over Theorem)**.** *Let S be an integral extension of R.*

1. *For every ideal I of R, the contraction of IS to R is contained in $\sqrt{I}$. If I is radical, then $IS \cap R = I$.*
2. *For every prime P of R, there are primes of S that contarct to P, and they are mutually incomparable.*

Proof. (1) let $u \in IS \cap R$, by Thm 2.3 above it satisfies a monic equation with all terms expect u^n has coefficients in I. So $u^n \in I \Rightarrow u \in \sqrt{I}$.

(2) Now assume that $I = P$ is prime. Consider the extension $R_P \to (R-P)^{-1}S$, it's still an integral extension by part (1) of Lem 1.9. So we have $P(R-P)^{-1}S \cap R_P = PR_P$. Then any maximal ideal, say Q' of $(R-P)^{-1}S$ containing $P(R-P)^{-1}S$ will contract to PR_P: the contraction is a prime ideal of R_P containing R_P, which must be PR_P. But then the contraction Q of Q' to S will lie over P.

Now we have to show that if two primes lying over P, then they are not comparable, i.e. one doesn't contain the other. Suppose we have two primes $Q_1 \subseteq Q_2$ in S lying over P, then passing to S/Q_1 and R/P we still have integral extension. Now Q_2S/Q_1 lies over (0). But by Lem 2.2 we see that any nonzero $s \in Q_2S/Q_1$ has a nonzero multiple in R/P, which shows that $Q_2S/Q_1 \cap R/P \neq (0)$. □

Corollary 2.5 (Going UP Theorem)**.** *Let $R \hookrightarrow S$ be an integral extension and let*

$$P_0 \subseteq P_1 \subseteq \cdots \subseteq P_d$$

be a chain of prime ideals of R. Let Q_0 be a prime ideal of S lying over P_0. Then there is a chain of prime ideals

$$Q_0 \subseteq Q_1 \subseteq \cdots \subseteq Q_d$$

of S such that for all t, Q_t lies over P_t.

Proof. It sufficies to construct $Q_1 \supseteq Q_0$ lying over P_1: the result then follows by a straight-forward induction on d. Consider $R/P_0 \subseteq S/Q_0$. This is an integral extension and P_1R/P_0 is a prime ideal. So there is a prime ideal Q_1S/Q_0 lying over it. Then we're done. □

Corollary 2.6. *If $R \hookrightarrow S$ is an integral extension then* $\dim(R) = \dim(S)$.

Proof. Let $Q_0 \subseteq \cdots \subseteq Q_d$ be a chain of ideals of S, then the contraction to R will be a chain of primes in R of the same length: they are all distinct ensured by lying over theorem. Hence we have $\dim(S) \leq \dim(R)$.

On the other hand, given a prime chain in R. The lying over theorem ensures that we have a starting point in S and the going up theorem shows that we have a prime chain of the same length. So $\dim(S) \geq \dim(R)$.

Therefore $\dim(R) = \dim(S)$. □

Next we discuss the number of primes lying over a given prime in the module-finite case, first we need two preliminary results:

Definition 2.7. Two ideals $I, J \subseteq R$ are called comaximal if $I + J = R$.

Lemma 2.8 (Chinese Remainder Theorem)**.** *If $I_1, ..., I_n$ are pairwise comaximal in R, then*

(1) $I_1I_2, I_3, ..., I_n$ are also pairwise comaximal.
(2) $I_1 \cdots I_n = I_1 \cap \cdots \cap I_n$.
(3) Let $J = I_1 \cdots I_n$, then the natural map

$$R/J \to R/I_1 \times \cdots \times R/I_n$$

is a ring isomorphism.

Proof. (1) We only need to show that $I_1I_2 + I_j = R$ for any j. Suppose we have $a_1 + u = 1$ for $a_1 \in I_1$ and $u \in I_j$; $a_2 + v = 1$ for $a_2 \in I_2$ and $v \in I_j$. Then $(a_1 + u)(a_2 + v) = 1 \Rightarrow a_1a_2 + (a_1v + a_2u + uv) = 1$. Note that $a_1a_2 \in I_1I_2$ and $(a_1v + a_2u + uv) \in I_j$.

For (2) and (3): By (1) we only need to prove this for $n = 2$, the general case will follow from the induction on n. Clearly we have $I_1I_2 \subseteq I_1 \cap I_2$. Let $u \in I_1 \cap I_2$, choose $a_1 \in I_1$ and $a_2 \in I_2$ such that $a_1 + a_2 = 1$. Then $u = u(a_1 + a_2) = ua_1 + ua_2$. But both ua_1 and ua_2 are in I_1I_2. So $u \in I_1I_2$.

Now consider the map $R \to R/I_1 \times R/I_2$: It induces an injection $R/I_1I_2 = R/(I_1 \cap I_2) \hookrightarrow R/I_1 \times R/I_2$. To see surjectivity, for any $(u_1, u_2) \in R/I_1 \times R/I_2$, again choose $a_1 \in I_1$ and $a_2 \in I_2$ such that $a_1 + a_2 = 1$. Note that a_1 maps to 1 in R/I_2 and a_2 maps to 1 in R/I_1. Then $u_1a_2 + u_2a_1$ maps to (u_1, u_2) as desired. □

Theorem 2.9. *Let R be a reduced K-algebra that is module-finite over the field K. Then R is a product of finite algebraic field extensions $L_1 \times \cdots \times L_n$ of K. In particular, R has n maximal ideals, i.e. the kernels of the n projections $R \to L_i$ and $n \leq \dim_K R$.*

Proof. Since K is of dimension zero, so is R as it's integral over K. Hence every prime ideal of R is maximal and minimal. R can only have finitely many minimal primes, call them $m_1, ..., m_n$. Then $m_1 \cap \cdots \cap m_n$ is the nilradical of R. So $m_1 \cap \cdots \cap m_n = (0)$ as R is reduced. By Chinese Remainder thoerem, we have

$$R = R/(0) = R/m_1 \cap \cdots \cap m_n = R/m_1 \cdots m_n = R/m_1 \times \cdots \times m_n$$

Each $L_i = R/m_i$ is a field module-finite over K, hence it's a finite algebraic field extension of K. The rest follows easily. □

3. Prime heights, normality and going down theorem

Definition 3.1. Given a prime $P \subseteq R$, the supremum of lengths of finite strictly ascending chains of primes contained in P is called the **height** of P, denoted by $\mathrm{ht}(P)$.

Corollary 3.2. *If $R \subseteq S$ is an integral extension and Q is a prime ideal of S lying over $P \subseteq R$, then $\mathrm{ht}_R(P) \geq \mathrm{ht}_S(Q)$.*

Proof. Any prime chain in S contained in Q restricts to a prime chain in R contained in P by Lying over theorem. □

Then we are natural to ask when the equality holds. That is, suppose you have a prime chain

$$P_0 \subseteq P_1 \subseteq \cdots \subseteq P_n = P$$

and a prime Q lying over P, can you construct a prime chain in S:

$$Q_0 \subseteq Q_1 \subseteq \cdots \subseteq Q_n = Q$$

such that each Q_i lies over P_i?

This turns out to need additional hypotheses even when R is a domain. For this purpose, we need the notion of **integral closure**.

Definition 3.3. (1) The set of elements in $S \supseteq R$ that are integral over R was shown earlier to be a ring. This ring is called the **integral closure of** R **in** S.
(2) The integral closure of a domain R in its fraction field $\mathrm{Frac}(R)$ is called the **integral closure** or **normalization** of R. A domain R is **integrally closed** or **normal** if it is its own normalization.

Example 3.4. (1) A unique factorization domain is a normal domain: Let $\frac{a}{b} \in \mathrm{Frac}(R)$ be integral over R where a, b have no common nonunit divisors, then $\frac{a}{b}$ satisfies a monic equation

$$x^d + c_1 x^{d-1} + \cdots + c_d = 0$$

So we have an equality in R:

$$a^d + c_1 a^{d-1} b + \cdots + c_d b^d = 0$$

Every term except a^d is divisible by b, hence a^d is divisible by b, which implies that a is divisible by b, a contradiction!
(2) $\mathbb{Z}[\sqrt{5}]$ is not integrally closed. The element $\frac{1+\sqrt{5}}{2}$ satisfies the equation $x^2 - x - 1 = 0$.
(3) If $R \subseteq S$ are domains and R is a direct summand of S as an R-module, then R is normal whenever S is.
(4) The d^{th} Vernonse subring of $K[x_1, ..., x_n]$ is normal.

We need some preliminaries before we can prove the going down theorem.

Proposition 3.5 (Division Algorithm)**.** *Let R be rings and $R[x]$ be the polynomial rings in one variable over R. Let g be any polynomial in $R[x]$ and f a monic polynomial in $R[x]$. Then one can write uniquely $g = fq + r$ where $q, r \in R[x]$ and either $r = 0$ or $\deg(r) < \deg(f)$.*

Proof. We can perform the long divison: Suppose $g = ax^n + \cdots$ and $f = x^d + \cdots$. If $n < d$ then we can choose $q = 0$ and $r = g$. If not, let $g_1 = g - ax^{n-d} f$. Then g_1 has lower degree and by induction on degree we can write $g_1 = q_1 f + r_1$. Hence $g = (q_1 + ax^{n-d}) f + r_1$.

To prove uniqueness, suppose that $qf + r = q'f + r'$. Then $(q - q')f = r' - r$. The degree of LHS is larger than RHS unless they are both zero. So $q = q'$ and $r = r'$. □

Proposition 3.6. *Let R be a normal domain with fraction field K. Let S be a domain containing R. Suppose that $s \in S$ is integral over R. Let $f(x) \in K[x]$ be the minimal monic polynomial of s. Then $f(x) \in R[x]$ and for any polynomial $g(x) \in R[x]$ such that $g(s) = 0$, $f(x) | g(x)$ in $R[x]$.*

Proof. Since s satisfies some monic polynomial $h(x)$ over R. We have $f(x)|h(x)$ in $K[x]$. Hence every root of $f(x)$ is integral over R, the coefficient of $f(x)$ are elementary polynomials of roots of $f(x)$. Therefore they are integral over R. Since R is normal, they are in R. Therefore $f(x) \in R[x]$.

If $g(s) = 0$, then $f(x)|g(x)$ in $K[x]$. But we can do the division algorithm in $R[x]$ and get the same result. So $q(x) \in R[x]$ and $f(x)|g(x) \in R[x]$. □

Now we are ready to prove

Theorem 3.7 (Going Down Theorem)**.** *Let R be a normal domain and let S be integral over R. Suppose that no nonzero element of R is a zerodivisor in S, i.e. that S is torsion-free as an R module. Let*

$$P_n \supseteq P_{n-1} \supseteq \cdots \supseteq P_0$$

be a chain of primes in R. Let Q_n be a prime ideal lying over P_n, then there is a chian of primes

$$Q_n \supseteq Q_{n-1} \supseteq \cdots \supseteq Q_0$$

of S such that Q_i lies over P_i for each i.

Proof. The general case follows by induction if we can prove this for two primes, i.e. given $P_0 \subseteq P_1$ in R and Q_1 lies over P_1, we want to find Q_0 lies over P_0 such that $Q_0 \subseteq Q_1$.

First we show that we can assume WLOG that S is a domain by showing that there is a prime $q \subseteq Q_1$ lying over $(0) \subseteq R$. Consider the multiplicative system $W = (R - \{0\})(S - Q_1)$ in S. $0 \notin W$ as S is torison-free as an R-module. So there is a prime ideal q in S disjoint from W. $q \cap R = 0$ as $R - \{0\} \subseteq W$. Since $S - Q_1 \subseteq W$ we also have $q \subseteq Q_1$. We now replace S by S/q. Since q doesn't meet R, we still have injection $R \to S/q$. This extenison is still integral. If we can find a prime ideal Q_0S/q lying over P_0, then the contraction of Q_0 will lie over P_0.

Now we can assume that S is also a domain. Let $A = R - P_0$ and $B = S - Q_1$. To complete the proof, we shall show that the multiplicative system AB does not meet the ideal P_0S. This implies that there is a prime ideal Q_0 of S containing P_0S and disjoint from $AB \supset A \cup B$. $Q_0 \cap B = \emptyset \Rightarrow Q_0 \subseteq Q_1$ and $Q_0 \cap A = \emptyset \Rightarrow P_0 \subseteq Q_0 \cap R \subseteq P_0$.

Suppose that $ab \in P_0S$ where $a \in A$ and $b \in B$. Since ab is integral over R, it satisfies a monic equation $g_1(x)$ with all but the leading coefficients in P_0. Let $g(x) = g_1(ax) \in R[x]$, then $g(b) = 0$. Let $K = \text{Frac}(R)$ and $L = \text{Frac}(S)$ be the corresponding coefficients field. Then b is algebraic over K and has a minimal monic polynomial $f(x)$ in $K[x]$. Since $b \in S$ is integral over R, by Prop 3.6 we see that $f(x) \in R[x]$ and $f(x)$ divides $g(x)$ in $R[x]$, that is, we have $g(x) = f(x)q(x)$ in $R[x]$.

Now we pass to R/P_0, the leading coefficient of $g(x)$ is a^d while all other coefficients are in P_0. So $\bar{g}(x) = \bar{a}^d x^d$. Hence $\bar{f}(x) = x^k$, which means that $f(x)$ should have the form

$$f(x) = x^k + p_1x^{k-1} + \cdots + p_k$$

where all $p_i \in P_0$. So $b^k \in P_0S \subseteq Q_1 \Rightarrow b \in Q_1$, a contradiction! So AB doesn't meet P_0S and we're done. □

Corollary 3.8. *Let R be a normal domain and S an integral extension of R that is torsion free over R. Let $Q \subseteq S$ be a prime lying over $P \subseteq R$, then* $\text{ht}(Q) = \text{ht}(P)$.

4. Graded Case

Theorem 4.1. *Let $R \subseteq S$ be an inclusion of $\mathbb{N}$ graded (or $\mathbb{Z}$ graded) rings compatible with the gradings, i.e. $R_h \subseteq S_h$ for each h. Then the integral closure of R in S is also compatible graded, i.e. every homogeneous component of an element of S integral over R is integral over R.*

Proof. First we 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 deg d forms 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, i.e. we have a commutative diagram

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

Let T be the integral closure of R in S, then θ_u preserves T: If $s \in S$ is integral over R, then one may apply θ_u to the equation of integral dependence to obtain an equation of integral dependence for $\theta_u(s)$ over R.

Now suppose that $s = s_h + \cdots + s_{h+k}$ is the decomposition into homogeneous components, each s_j has degree j. We choose units $u_1, ..., u_n$ such that $u_i - u_j$ is a unit for $i \neq j$. By applying θ_{u_i} we get n equations:

$$u_i^h s_h + \cdots + u_i^{h+k} s_{h+k} = t_i \quad 1 \leq i \leq n$$

Let $M = (u_i^{j+h})_{k\times k}$, $V = \begin{pmatrix} s_h \\ \vdots \\ s_{h+k} \end{pmatrix}$ and $W = \begin{pmatrix} t_1 \\ \vdots \\ t_k \end{pmatrix}$, then we have $W = MV$ and $W \in T$. But M is invertible: it's a Van der Monde matrix with determinant $\prod_{i<j}(u_i - u_j)$. So $V = M^{-1}W \in T$.

In the general case, let t be an indeterminate over R and S. Assign degree zero to t so that $R[t]$ is again a graded ring. Then $R[t] \subseteq S[t]$ is still compatible. Let U be the set of t^n's and all their differences. We have an inclusion of graded rings $U^{-1}R[t] \subseteq U^{-1}S[t]$. Now we have those desired units hence for any $s = s_h + \cdots + s_{h+k}$ integral over R we can show that each s_j is integral over $U^{-1}R[t]$.

Consider an equation of integral dependence

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

where $f_i \in U^{-1}R[t]$. Then we can pick an element $G \in U$ to clear all denominators, and we get

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

The coefficients of t^m where m is the highest degree of t in G must be zero. Therefore we get an equation of s_j with coefficients in R, as required. □

Corollary 4.2. *If R is integrally cloesd in S, then $R[t]$ is integrally closed in $S[t]$. If R is a normal domain, then so is $R[t]$*

Proof. The integral closure of $R[t]$ in $S[t]$ is graded and spanned by elements of the form st^k. Now consider the equation that st^k satisfies: Since t is an indeterminate, the coefficients of the equation must be zero. So s is integral over R. □

In the Noetherian case, we can give an alternate proof: Since R is normal, it's an intersection of Noetherian DVR's V. Therefore $R[t]$ is the intersection of $V[t]$'s. V is a PID, hence UFD. So $V[t]$ is also UFD, hence normal. Therefore their intersection is normal.